Administering Avaya Aura® Session Manager

Release 7.1.3
Issue 11
October 2020

© 2013-2020, Avaya Inc.
All Rights Reserved.

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.

Named User License (NU). End User may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). End User may install and use the Software in accordance with the terms and conditions of the applicable license

agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”) as indicated in the order, Documentation, or as authorized by Avaya in writing.

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.

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.

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 20
Purpose 20
Change history 20
Chapter 2: System Manager Overview 22
Log on to System Manager 24
Turning off the compatibility mode 24
Logging on to the System Manager web console 25
Chapter 3: System Manager Geographic Redundancy 27
Geographic Redundancy scenarios 28
Sunny Day scenario 29
Rainy Day scenario 30
Split-network Scenario 31
Managing Session Manager in a Geographic Redundancy solution 32
Data center failures 39
Managing data center failures Case 1: The primary data center fails 40
Managing data center failures Case 2: Primary System Manager fails 42
Case 3: Replacing the secondary System Manager due to hardware failures 43
Case 4: Shutting down the primary System Manager for maintenance 43
Case 5: The primary System Manager cannot communicate with the secondary System Manager. The system elements can communicate with the primary System Manager and the secondary System Manager 44
Case 6: The primary System Manager cannot communicate with the system elements, but the elements can communicate with the secondary System Manager 44
Case 7: System elements can communicate only with the primary System Manager 45
Case 8: The primary System Manager cannot communicate with the secondary System Manager. Some system elements can communicate only with the primary System Manager while some system elements can communicate only with the secondary System Manager 46
Setting up a Geographic Redundancy enabled system 47
Upgrade to a Geographic Redundancy-enabled system 48
Upgrading simultaneous element method 48
Upgrading selected element method 49
Performing system verification tests 50
Chapter 4: Synchronizing Communication Manager data with the System Manager database 51
Creating a Communication Manager instance in the system 51
Adding a new element 51
Add Communication Manager field descriptions 52
Messaging elements 55
Creating a Messaging instance 55

Synchronizing the Communication Manager data and configuring options 56
Synchronizing the messaging data 57
Manage Elements field descriptions 57
Element details field descriptions 60
Chapter 5: Managing security 69
Extended Security hardening 69
Enabling the Hardened security profile 70
AIDE commands 71
Trust management 71
Certificate management 71
Certificates issued by System Manager 72
Managing certificate revocation list 79
Certificates issued by a third party 84
Demo certificates 88
Trusted Certificates 89
Identity Certificates 96
Enforcing certificate validation for SIP endpoints 111
Chapter 6: Managing users 112
Required procedures before administering a Session Manager profile 113
Adding users 115
Verifying the Primary and Secondary Session Manager sequence 117
Managing communication profiles 118
Session Manager communication profile administration 118
Multi Device Access 118
Communication profiles 119
Adding a communication profile for the user 119
Deleting the communication profile of a user 120
Creating a new communication address for a communication profile 120
Modifying the communication address 121
Deleting a communication address from a communication profile 121
Presence communication profile administration 122
CM Endpoint profile administration 122
Messaging profile administration 127
CS 1000 and CallPilot profile administration 129
IP Office profile administration 133
Viewing details of a user 136
Modifying user accounts 137
Removing user accounts 138
Removing the deleted users from the database 139
Viewing the deleted users 139
Restoring a deleted user 139
Creating duplicate users 140
Managing default contact list of the user 141

Adding a contact in the Default Contact list..... 141
Modifying membership details of a contact in a contact list..... 141
Viewing membership details of a contact in the contact list..... 142
Deleting contacts from the default contact list..... 142
Attach Contacts field descriptions..... 142
Edit Contact List Member field descriptions..... 144
View Contact List Member field descriptions..... 146
Filtering users..... 148
Searching for users..... 149
Multi Tenancy for Avaya SIP AST endpoints..... 149
Managing user provisioning rules..... 149
User Provisioning Rule..... 149
Capabilities and guidelines of user provisioning rules..... 150
Adding User Provisioning Rules..... 152
Creating the user provisioning rule..... 152
Modifying the user provisioning rule..... 153
Viewing the user provisioning rule..... 153
Creating a duplicate user provisioning rule..... 154
Deleting the user provisioning rule..... 154
User Provisioning Rules Management field descriptions..... 155
User Provisioning Rule field descriptions..... 155
Role Based Access Control..... 165
RBAC permissions for Routing Import/Export operations..... 167
RBAC permissions for Local Host Name Resolution imports..... 168
RBAC permissions for Bulk Communication Profile edits..... 168
Creating a Scheduler operation role..... 169
Creating an RBAC role with read-only permissions..... 169
Creating an RBAC role with read and write permissions..... 170
Assigning an RBAC role to a user..... 171
Configuring a user to have access permissions for System Manager web pages..... 172
Copying permission mapping for a role..... 173
Removing access permissions for Session Manager and Routing pages..... 174
Removing the assigned RBAC role from a user..... 174
Managing bulk import and export..... 175
Bulk import and export..... 175
Bulk import and export using the Excel file..... 175
XML Schema definitions and sample XMLs for bulk import..... 177
Examples of bulk import and export of user by using the Excel file..... 177
Hierarchy in communication profile worksheets..... 179
Microsoft Excel data link error..... 180
Data entry warning in Microsoft Excel..... 181
Key features of bulk import and bulk export..... 182
About bulk import of users..... 182

Configuration options for bulk import using Excel 184
Downloading the Excel template file 185
About bulk export of users 186
Exporting users in bulk from web console 187
Configuration options for bulk import of users 189
Bulk importing of partial user attributes for a user 190
Making exported user data compatible for partial user import 191
About Bulk Import Encryption utility 192
Encrypting passwords in user import file using BulkImportEncryptionUtil running on Windows 192
Encrypting passwords in user import file using BulkImportEncryptionUtil running on Linux 193
Import user considerations 194
Scheduling a user import job 195
Aborting a user import job on first error 196
Canceling a user import job 197
Deleting a user import job 198
Viewing a user import job on the Scheduler page 198
Viewing the details of a user import job 199
Bulk import of global user settings 200
Bulk export of global user settings 201
exportUpmGlobalsettings.sh command 201
Scheduling a global user settings import job 202
Viewing details of a global user settings import job 203
Viewing a global user settings import job on the Scheduler page 204
Aborting a global user settings import job on first error 204
Deleting a global user settings import job 205
Canceling a global user settings import job 205
List of XML Schema definitions and sample XMLs for bulk import 206
Import Users field descriptions 206
Import Users – Job Details field descriptions 210
Export Users field descriptions 212
Job Details field descriptions 218
Import Global Settings field descriptions 219
Quick start to importing users 222
New User Profile field descriptions 227
User Profile Edit field descriptions 249
User Profile View field descriptions 271
User Delete Confirmation field descriptions 288
Chapter 7: Session Manager routing 289
Routing 289
Call routing using routing policy data 290
SIP response handling 290
Administering initial setup of the Session Manager 291

Routing element data import and export overview 292
Duplicating Routing entity data 296
Domains 297
Creating domains 297
Modifying domains 297
Deleting domains 298
Domain Management field descriptions 298
Domain Details field descriptions 299
Bulk import for Domains 299
Locations 300
Dial Plan Transparency 301
Call Admission Control 301
Creating Locations 303
Modifying Locations 304
Deleting Locations 304
Location field descriptions 304
Location Details field descriptions 305
Bulk import for Locations 310
Adaptations 312
Adaptation Module parameters 313
Phone context 316
SIP Header Removal 317
Removing SIP header 318
Adaptation examples 319
Creating Adaptations 321
Modifying Adaptations 323
Deleting Adaptations 323
Installed vendor adapters 324
Adaptations field descriptions 329
Adaptation Details field descriptions 330
Adaptation Module Management field description 335
Bulk import for Adaptations 335
SIP Entities 338
Authentication of trusted SIP Entities 339
IP and transport layer validation 339
Transport Layer Security validation 339
SIP Responses to an OPTIONS Request 340
Deny new service for Entity Links 340
SIP Call Loop elimination 341
Creating SIP Entities 342
Modifying SIP entities 344
Deleting SIP Entities 344
Accepting new service for all entity links 345

Denying new service for all Entity Links ... 345
IP address family validations ... 345
SIP Entities field descriptions ... 346
SIP Entity Details — Session Manager type field descriptions ... 348
SIP Entity Details field descriptions for Non-Session Manager SIP Entity types ... 358
Bulk import for SIP Entities ... 368
SIP Entity References ... 373
Displaying SIP Entity References ... 373
Overview of References to SIP Entities field descriptions ... 374
Entity Links ... 374
Creating Entity Links ... 375
Modifying Entity Links ... 375
Deleting Entity Links ... 376
Accepting new service for the selected Entity Links ... 376
Denying new service for selected Entity Links ... 376
Entity Links field descriptions ... 376
Bulk import for Entity Links ... 378
Time Ranges ... 379
Creating Time Ranges ... 380
Modifying Time Ranges ... 380
Deleting Time Ranges ... 381
Time Ranges field descriptions ... 381
Time Range List field descriptions ... 382
Bulk import for Time Ranges ... 382
Routing Policies ... 383
Creating Routing Policies ... 384
Modifying Routing Policies ... 385
Deleting Routing Policies ... 386
Routing Policies field descriptions ... 386
Routing Policy Details field descriptions ... 387
SIP Entity List field descriptions ... 389
Time Range List field descriptions ... 390
Pattern List field descriptions ... 390
Regular Expression List field descriptions ... 391
Bulk import for Routing Policies ... 391
Dial Patterns ... 392
Emergency Numbers ... 394
Dial Plan Ranges ... 395
Multilocation Dial Plan ... 396
Creating Dial Patterns ... 396
Modifying Dial Patterns ... 397
Deleting Dial Patterns ... 397
Dial Patterns field descriptions ... 397

Dial Pattern Details field descriptions..... 399
Denied Originating Location List field descriptions..... 401
Bulk Import for dial patterns..... 401
Regular Expressions..... 403
Regular Expression constructs..... 403
Creating Regular Expressions..... 405
Modifying Regular Expressions..... 405
Deleting Regular Expressions..... 406
Regular Expressions field descriptions..... 406
Regular Expression Details field descriptions..... 407
Routing Policy List field descriptions..... 407
Bulk import for Regular Expressions..... 408
Defaults..... 408
Modifying the Default settings..... 408
Default Settings field descriptions..... 409
Chapter 8: Session Manager Administration..... 411
Session Manager Dashboard..... 411
Session Manager Dashboard field descriptions..... 411
Maintenance Mode Service state..... 414
Session Manager Administration..... 415
Creating a Session Manager SIP Entity..... 416
Adding a Session Manager instance..... 416
Viewing Session Manager administration settings..... 418
Modifying Session Manager administration settings..... 418
Deleting a Session Manager instance..... 419
Add Session Manager page field descriptions..... 419
Enabling IPv6..... 425
Disabling IPv6..... 426
Administering global Session Manager settings..... 426
Failback policy..... 433
Call History..... 433
Call Journaling High Availability..... 435
Cassandra clustering and data replication overview..... 435
Branch Session Manager..... 440
Survivable Branch Configuration..... 441
Administering Branch Session Manager..... 447
Adding a Branch Session Manager instance..... 449
Viewing Branch Session Manager administration settings..... 451
Modifying the Branch Session Manager administration settings..... 451
Deleting a Branch Session Manager instance..... 451
Add Branch Session Manager page field descriptions..... 452
E911 Services..... 457
Emergency Call Notification to Adjunct Emergency Location Server..... 457

Administering the ELIN server ... 458
Communication Profile Editor ... 458
Viewing Communication Profiles ... 459
Customizing column display ... 459
Modifying Communication Profiles ... 460
Viewing background edit job status ... 461
Viewing Communication Profile edit failures ... 461
Stopping Communication Profile editing jobs ... 461
Communication Profile Editor field descriptions ... 462
Communication Profile Edit Confirmation page field descriptions ... 465
Network Configuration ... 465
Failover Groups ... 465
Rules for working with Failover groups ... 474
Local Host Name Resolution ... 474
Remote Access ... 481
SIP Firewall ... 488
Device and Location Configuration ... 505
Device Settings Groups ... 505
Location Settings ... 521
Setting Station Access Code Policy ... 521
Applications ... 523
Filtering of sequenced applications based on media attributes ... 523
Viewing applications ... 525
Creating an application ... 525
Modifying an application ... 525
Deleting applications ... 526
Applications field descriptions ... 526
Application Editor field descriptions ... 527
Application Sequences ... 529
Viewing application sequences ... 529
Creating an Application Sequence ... 529
Modifying an Application Sequence ... 530
Deleting Application Sequences ... 530
Rearranging Applications in an Application Sequence ... 530
Adding Applications to an existing Application Sequence ... 531
Application Sequences field descriptions ... 531
Application Sequence Editor field descriptions ... 532
Conference Factory URI ... 533
How the Conference Factory feature works ... 534
Adding a new Well Known Conference URI ... 536
Editing the Well Known Conference URI entry ... 537
Removing the Well Known Conference URI entry ... 537
Adding a new Conference Factory Set ... 538

Viewing the Conference Factory Set 539
Editing a Conference Factory Set 539
Deleting a Conference Factory Set 540
Conference Factories Field Description 540
Conference Factory Set Page Field Description 541
Implicit Users 543
SIP User Implicit Sequencing 543
Viewing Implicit User Rules 543
Creating an Implicit User Rule 544
Modifying an existing Implicit User Rule 544
Removing existing Implicit User Rules 544
Implicit User Rules field descriptions 545
Implicit User Rule Editor field descriptions 545
Administering Implicit Applications for SIP users 547
NRS Proxy Users 547
Redirecting UNIStim Phones 548
Creating Terminal Proxy Server instance 548
Creating a NRS Proxy User Rule 549
Modifying NRS Proxy User Rule 549
Deleting an NRS Proxy User Rule 550
NRS Proxy Users field descriptions 550
NRS Proxy User Rule Editor field descriptions 551
Chapter 9: System Status 552
Session Manager SIP Entity Monitoring 552
Viewing the SIP Monitoring Status Summary page 553
SIP Entity Link Monitoring Status Summary page field descriptions 553
Managed Bandwidth Usage 556
Viewing Managed Bandwidth Usage 556
Managed Bandwidth Usage page field descriptions 556
Managed Bandwidth Usage errors 558
Security Module Status 558
Viewing the Security Module page 559
Security Module Status page field descriptions 560
Connection Status 561
SIP Firewall Status 563
Viewing SIP Firewall status 563
Auditing SIP Firewall configuration 564
SIP Firewall Status page field descriptions 564
Registration Summary 565
Viewing Registration Summary 566
Registration Summary field descriptions 566
Rebooting of selected AST devices 567
Reloading of selected AST devices 567

Failback of selected AST devices..... 568
Advanced searching..... 568
User Registrations..... 569
Viewing User Registrations..... 569
User Registrations field descriptions..... 569
Customizing column display..... 577
Exporting user registrations..... 578
User registration export field descriptions..... 578
Forcing unregistration of device registration..... 579
Rebooting of selected AST devices..... 580
Reloading of selected AST devices..... 580
Failback of selected AST devices..... 580
Advanced searching..... 581
SIP Sessions count..... 581
Viewing Session Count data..... 582
Exporting analyzed Session Count data..... 582
Session Counts field descriptions..... 582
User Data Storage and Data Center management..... 583
Viewing User Data Storage Status 584
Data Server Status field descriptions..... 584
Administering Data Center..... 586
User Data Storage backup..... 588
Chapter 10: System Tools..... 593
Session Manager maintenance tests..... 593
Maintenance Tests page field descriptions..... 593
Running maintenance tests..... 594
Maintenance Test descriptions..... 594
Tracer Configuration..... 596
Tracer Configuration page field descriptions..... 596
SIP Tracing..... 599
Trace Viewer page field descriptions..... 600
Call Routing Test..... 601
Call Routing Test page field descriptions..... 602
SNMP Management Information Base..... 604
SNMP MIB Download..... 604
Downloading SNMP MIBs..... 605
SNMP MIB Download page field descriptions..... 605
Chapter 11: Performance..... 606
Call Counts..... 606
Viewing call counts data..... 606
Exporting analyzed call counts data..... 606
Call Counts Report Types..... 607
Call Counts field descriptions..... 607

Location Performance 608
Viewing location performance data 609
Exporting analyzed location performance data 609
Location Performance Report Types 610
Location Performance field descriptions 610
SIP Performance 611
Viewing SIP performance data 612
Exporting analyzed SIP performance data 612
SIP Performance field descriptions 616
System Performance 617
Viewing System Performance data 617
Exporting analyzed System Performance data 618
System Performance Report Types 619
System Performance field descriptions 620
Performance Data Collection 621
Using NFS disk space for performance data storage 622
Reverting to local storage after using remote storage 623
Performance Data Collection field descriptions 624
Chapter 12: Managing system events 626
Managing alarms 626
Alarming 626
Viewing alarms 627
Changing the alarm status 627
Exporting alarms 627
Filtering alarms 628
Searching for alarms 628
Managing Geographic Redundancy related alarms 629
Alarming field descriptions 630
Alarming field descriptions 631
Managing log viewer 634
Log Viewer 634
Viewing log details 634
Exporting logs 635
Filtering logs 635
Searching for logs 636
Logging field descriptions 636
Logging field descriptions 640
Managing log settings 642
Log Settings 642
Accessing the Log Settings service 642
Viewing loggers for a log file 642
Logging Settings field descriptions 642
Editing a logger in a log file 643

Managing log harvester 648
Log harvester 648
Accessing the Log Harvester service 648
Creating a new log harvesting profile 649
Editing a log harvesting profile 650
Viewing the harvested log files in an archive 650
Deleting a profile 651
Submitting a request for harvesting log files 651
Viewing details of a log harvesting request 652
Searching for text in a log file 652
Viewing the contents of harvested log files 653
Downloading the harvested log files 653
Filtering log harvesting profiles 654
Filtering log harvesting requests 655
Viewing details of a log harvesting profile 656
Log Harvester field descriptions 656
Create New Profile field descriptions 657
Harvest Criteria Edit field descriptions 658
Profile Criteria View field descriptions 659
Harvest Archives field descriptions 659
Search Archives field descriptions 661
Harvest - View Harvest detail field descriptions 662
Chapter 13: Managing system data 664
Backup and Restore 664
Disk space required for backup 664
Backup and restore on System Manager that is configured for Geographic Redundancy 665
Accessing the Backup and Restore service 666
Viewing list of backup files 666
Creating a data backup on a local server 666
Creating a data backup on a remote server 666
Scheduling a data backup on a local server 667
Scheduling a data backup on a remote server 668
Editing a scheduled backup job 669
Deleting the scheduled backup job 669
Restoring data backup from a local server 670
Restoring a backup from a remote server 671
Restoring the backup through the command line interface 672
Backup and Restore field descriptions 673
Backup field descriptions 674
Schedule Backup field descriptions 675
Restore field descriptions 676
Managing data retention rules 677
Accessing the Data Retention Rules service 677

Data retention rules ... 678
Viewing data retention rules ... 678
Modifying data retention rules ... 678
Data Retention field descriptions ... 679
Data Replication Service ... 679
Viewing replica groups ... 679
Viewing replica nodes in a replica group ... 680
Repairing a replica node ... 680
Repairing all replica nodes in a replica group ... 680
Viewing replication details for a replica node ... 681
Removing a replica node ... 681
Removing a replica node from queue ... 682
Troubleshooting Replica Nodes ... 682
Replica Groups field descriptions ... 683
Replica Nodes field descriptions ... 683
Replication Node Details field descriptions ... 687
Managing scheduled jobs ... 689
Scheduler ... 689
Accessing scheduler ... 690
Assigning permissions to access Scheduler ... 690
Viewing pending jobs ... 691
Viewing completed jobs ... 691
Viewing logs for a job ... 692
Filtering jobs ... 692
Editing a job ... 693
Deleting a job ... 693
Disabling a job ... 694
Enabling a job ... 695
Stopping a job ... 695
Pending Jobs field descriptions ... 696
Completed Jobs field descriptions ... 698
Job Scheduling-View Job field descriptions ... 700
Job Scheduling-Edit Job field descriptions ... 701
Job Scheduling-On Demand Job field descriptions ... 703
Disable Confirmation field descriptions ... 703
Stop Confirmation field descriptions ... 705
Delete Confirmation field descriptions ... 706
Chapter 14: SIP phone pre-configuration template ... 707
Software requirements for the SIP phone pre-configuration template ... 708
Creating a new customized SIP phone template ... 708
Creating a SIP phone template from a default template ... 709
Applying a SIP phone template to an existing user ... 710
Modifying endpoint settings for an existing user ... 710

Modifying endpoint settings for a group of existing users..... 711
Removing a SIP phone template..... 712
Chapter 15: SIP Team button..... 713
Administering the SIP Team button..... 713
Chapter 16: Service Observing from SIP Phone..... 716
Chapter 17: SNMP support for Session Manager..... 717
Serviceability Agents..... 717
Configuring the Session Manager Serviceability Agent..... 718
Verifying the Session Manager serviceability agent registration..... 719
Activating a serviceability agent..... 719
Managing SNMPv3 user profiles for the selected serviceability agents..... 719
Managing target profiles for the selected serviceability agents..... 720
Generating the test alarm from the web console..... 720
Repairing serviceability agents..... 721
Serviceability Agents list..... 721
Managing SNMPv3 user profiles..... 722
Creating an SNMPv3 user profile..... 722
Editing an SNMPv3 user profile..... 722
Viewing an SNMPv3 user profile..... 722
Deleting an SNMPv3 user profile..... 723
Filtering SNMPv3 user profiles..... 723
SNMPv3 user profiles field descriptions..... 724
Managing SNMP target profiles..... 725
Creating an SNMP target profile..... 725
Editing an SNMP target profile..... 726
Viewing an SNMP target profile..... 726
Deleting an SNMP target profile..... 726
Filtering target profiles..... 727
SNMP Target profile list..... 727
SNMP target profiles field descriptions..... 728
Notification Filter Profile..... 728
Creating a Notification Filter Profile..... 729
Viewing a Notification Filter Profile..... 729
Editing a Notification Filter Profile..... 729
Deleting a Notification Filter Profile..... 730
Assigning a Notification Filter Profile to a serviceability agent..... 730
Unassigning a Notification Filter Profile from a serviceability agent..... 731
Filter Profiles field descriptions..... 731
Create, View, Edit, or Delete Filter Profiles field descriptions..... 732
System Manager TrapListener service..... 732
Configuring the TrapListener service..... 733
Viewing the System Manager TrapListener Service settings..... 733
TrapListener service field descriptions..... 733

Session Manager SNMP MIB 734
Chapter 18: Resources 739
Documentation 739
Finding documents on the Avaya Support website 741
Accessing the port matrix document 741
Training 742
Viewing Avaya Mentor videos 742
Support 743
Using the Avaya InSite Knowledge Base 743
Appendix A: Restricted commands for the Security Module 745
Appendix B: Regular Expression constructs 746
Appendix C: Product notifications 748
Viewing PCNs and PSNs 748
Registering for product notifications 749
Appendix D: List of XML Schema Definitions and sample XMLs for bulk import 750
Attribute details defined in Import user XSD 865
Attribute details defined in Delete User XSD 875
Attribute details defined in the CM Endpoint profile XSD 876
Attribute details defined in the Messaging communication profile XSD 905
Attribute details defined in the Session Manager communication profile XSD 914
Attribute details defined in the Avaya Aura® Conferencing profile XSD 919

Chapter 1: Introduction

Purpose

This guide describes how to administer and manage Avaya Aura® Session Manager.

The primary audience for this document is anyone who configures and verifies Session Manager at a customer site. The audience includes and is not limited to implementation engineers, field technicians, business partners, solution providers, and customers.

The audience must have a basic understanding and working knowledge of the following areas:

- Operating systems in general
- TCP/IP
- SSH
- SIP
- FTP and SFTP
- LAN and WAN
- Hostname and DNS

This document does not include optional or customized aspects of a configuration.

Change history

Issue	Date	Summary of changes
11	October 2020	Updated the section Administering Branch Session Manager on page 447 to identify the required steps when a Branch Session Manager is used only for routing purpose.

Table continues…

Issue	Date	Summary of changes
10	August 2020	Updated the following sections: • SIP Identity Certificate attributes on page 107 • HTTPS Identity Certificate attributes on page 108 • Management, Postgres and SPIRIT identity certificates attributes on page 109
9	July 2020	Updated the following sections: • Viewing call counts data on page 606 • Exporting analyzed call counts data on page 606 • Call Counts field descriptions on page 607
8	May 2020	Defined the priority order of IP addresses during Local Host Name resolution in the following sections: • Resolving a local host name on page 475 • Local Host Name Resolution page field descriptions on page 479 • Local Host Name Entries page field descriptions on page 480
7	March 2020	Updated the *Session Manager Administration* chapter.
6	August 2018	Updated path for the `CDR_User` directory.
5	July 2018	Updated the *Bulk Import for dial patterns* section.
4	May 2018	• Updated the *Extended Security hardening* section. • Introduced new AIDE commands in the *AIDE commands* section. • Added support for User-to-User value in CDR. • Introduced an ability to selectively enable or disable security hardening.
3	December 2017	• Introduced Extended Security Hardening. • Added a procedure to export user registrations. • Updated System Performance Report Types to get the CPU Usage report.
2	August 2017	• Introduced Emergency Calling Application Sequence. • Introduced the new field **Enable Application Sequence for Emergency Calls** in Global Settings: • Introduced a new tab for regular expression pattern rules under implicit user administration.
1	May 2017	Initial release.

Chapter 2: System Manager Overview

Avaya Aura® System Manager is the central administration component for Avaya Aura®.

System Manager centralizes provisioning, maintenance, and troubleshooting of Avaya Aura® components.

The System Manager common console is the management interface for Session Manager. You must log on to the System Manager common console to perform any administration or configuration task.

The System Manager common console provides a set of functionality and interfaces that are categorized as follows:

Category	Description
Users	Provides a single interface for provisioning users on most of the Avaya Aura® components. • **Administrators:** Manage administrative users within Avaya Unified Communications Management. • **Directory Synchronization:** Synchronize users with the enterprise directory. • **Groups & Roles :** Manage groups, roles, and assign roles to users. • **User Management:** Manage users and shared resources, and provision users. • **User Provisioning Rule:** Assign user provisioning rules.

Table continues…

Category	Description
Elements	Provides features for managing each component of the solution including the Session Manager element administration. • **Communication Manager:** Manage Communication Manager 5.2 and higher elements. • **Communication Server 1000:** Manage Avaya Communication Server 1000 elements. • **Conferencing:** Manage Conferencing Multimedia Server objects. • **Avaya Breeze:** Manage Avaya Breeze™ elements. • **IP Office:** Manage IP Office elements. • **Media Server:** Manage media server elements. • **Meeting Exchange:** Manage Meeting Exchange and Avaya Aura® Conferencing elements. • **Messaging:** Manage Avaya Aura® Messaging, Communication Manager Messaging, and Modular Messaging. • **Presence:** Manage Presence-based configuration properties, classes, and access levels. • **Routing:** Session Manager Routing administration. • **Session Manager:** Session Manager administration, status, maintenance, and performance management. • **Work Assignment:** Manage work assignments.

Table continues…

Category	Description
Services	Provides a single interface for managing common services. • **Backup and Restore:** Backup and restore the System Manager database. • **Bulk Import and Export:** Bulk Import and Export of users, User Global Settings, Roles, and others. • **Configurations:** Manage system-wide configurations. • **Events:** Manage alarms, view and harvest logs that System Manager and other components of System Manager generate. • **Geographic Redundancy:** Manage the System Manager geographic redundancy. • **Inventory:** Manage and view elements deployed in System Manager. Synchronize the System Manager data with other elements. • **Licenses:** View and configure licenses for one or more Avaya software products. • **Replication:** Track data replication nodes, repair replication nodes. • **Reports:** Generate reports for elements. • **Scheduler:** Schedule, track, cancel update, and delete jobs. • **Security:** Manages Security Certificates. • **Shutdown:** Shutdown System Manager gracefully. • **Software Management:** Upgrade and Patch Management for Communication Manager devices and IP Office. • **Templates:** Manage templates for Communication Manager, Messaging, and IP Office.

For more information about System Manager, see the System Manager documentation on the Avaya Support website at http://support.avaya.com.

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.

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 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 the role that you are assigned with.

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 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 does not match, System Manager displays an error message and prompts you to enter the user name and password again.

   When you log on to the System Manager web console, the system displays the System Manager/AVP License Error window with the following messages.

Note:

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, the system displays the AVP 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.

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)/VM Management/Location/Hosts/
for impacted AVP hosts.
```

6. Click **OK**, and install a valid System Manager license file.

Chapter 3: System Manager Geographic Redundancy

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.

The Geographic Redundancy feature of System Manager consists of two System Manager servers located in geographically remote locations. The Geographic Redundancy feature ensures that the enterprise communications remain unaffected during the failure of a single System Manager server or during network failures.

The Geographic Redundancy feature provides the following replication mechanisms to ensure data synchronization between the primary System Manager server and the secondary System Manager server:

- Database replication
- File replication
- LDAP replication

In a system consisting of geographic redundant System Manager servers, the primary components include:

- Two System Manager servers located in geographically diverse locations. One System Manager server is designated as the primary System Manager. On a sunny day, the primary System Manager manages all elements in the system. The other System Manager server is designated as the secondary System Manager. The secondary System Manager remains in the standby mode. You can administer the secondary server in the active mode if the primary System Manager fails or loses connectivity with the elements in the system.
- One or more elements that can include Session Manager or Branch Session Manager and other Avaya products.

Important:

In an environment of geographic redundant System Manager instances, both the primary System Manager server and the secondary System Manager server *must* reach each other using FQDN. FQDN must be reachable and resolvable through `/etc/hosts` or DNS.

Before configuring a Session Manager in a geographic redundant environment, the following must be true:

- Both the primary and the secondary System Manager can resolve the Session Manager FQDN through `/etc/hosts`.
- The DNS server contains the IP address or the FQDN entry of all the Session Manager instances that are configured with System Manager. This configuration ensures that both the forward and the reverse lookups of Session Manager work from both the primary and the secondary System Manager servers.

Geographic Redundancy scenarios

A network with geographic redundant System Manager instances operates in the following different modes:

- **Sunny day scenario:** The primary System Manager is in the active mode, the secondary System Manager is in the standby mode, and the system is operating normally.
- **Rainy day scenario:** The primary System Manager has failed or has lost connectivity to the elements in the system. The standby System Manager is managing the elements in the system.
- **Split-network scenario:** The administrator administers the secondary System Manager to the active mode when the primary System Manager is also in the active mode.

An **element** is an instance of an Avaya Aura® network entity. System Manager manages elements such as a Session Manager or Communication Manager server in the Avaya Aura® network.

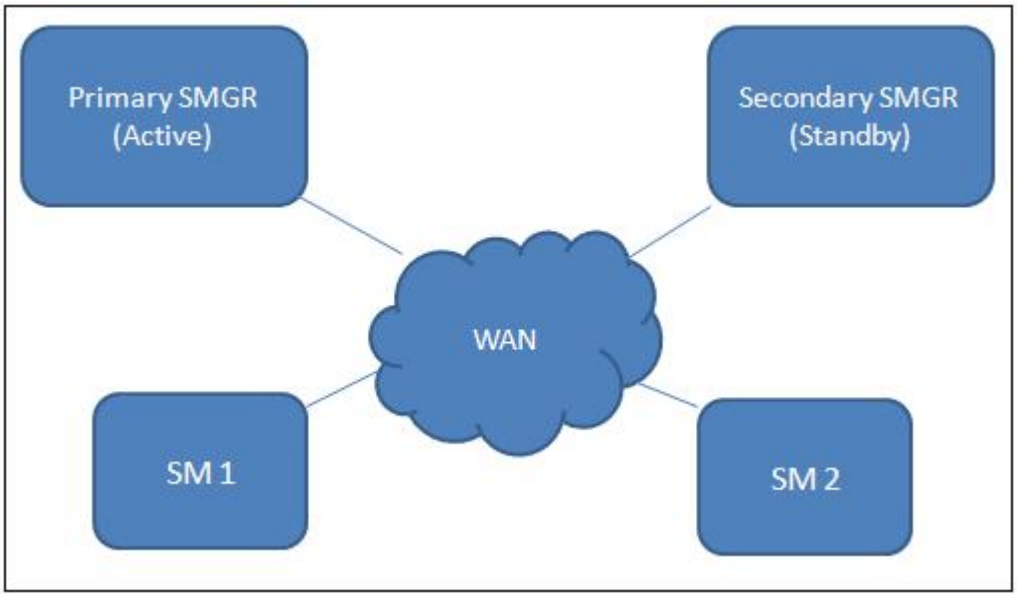
The primary System Manager is always in the **active** mode unless you turn off the server. In failback cases, the primary System Manager might not be in the active mode. The normal mode of operation of the secondary System Manager is the **standby** mode. In a sunny day scenario, the primary System Manager manages all elements of the Avaya Aura® solution, including Session Manager. The secondary System Manager runs a limited set of services.

Geographic Redundancy-aware elements are those elements of the Avaya Aura® solution that support the **Geographic Redundancy** feature, such as Session Manager or Branch Session Manager instances.

Geographic Redundancy-unaware elements are those elements of the Avaya Aura® solution that do not support the **Geographic Redundancy** feature, such as Session Manager or Branch Session Manager instances running releases earlier than 6.3.

Sunny Day scenario

In this scenario, the primary System Manager is in the active mode and manages all elements in the system. The secondary System Manager is running in the standby mode with the database in the read-only mode.

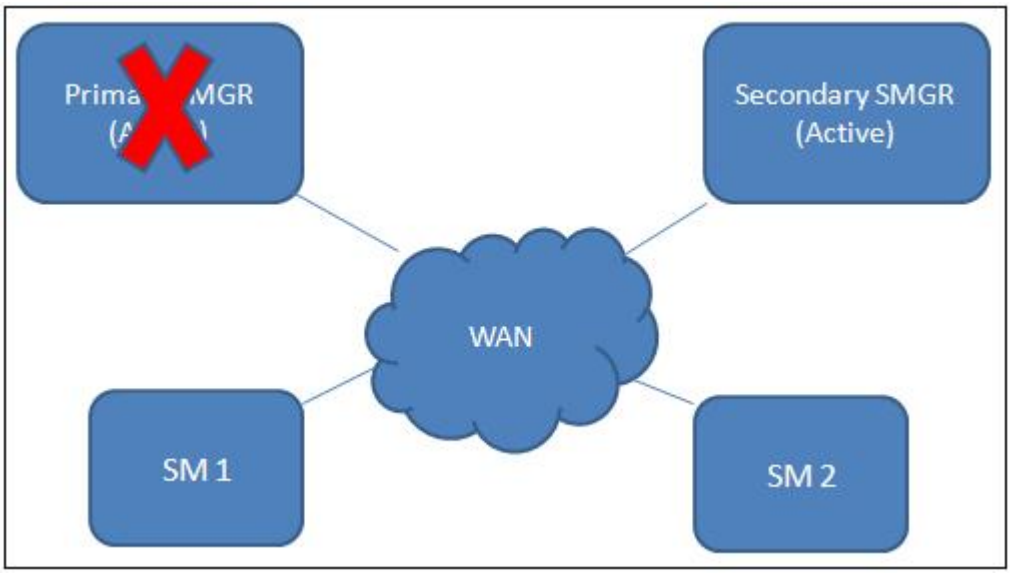


- The primary System Manager is in the active mode and manages the normal System Manager responsibilities including:
  - Providing a web console for the call routing configuration, the user configuration, and the network configuration administration of Session Manager.
  - Replicating the database to the secondary System Manager.
  - Replicating portions of the database to the various elements.
  - Authenticating and authorizing the elements that require System Manager services.
  - Processing SNMP traps and alarms.
  - Responding to System Manager status requests from elements.
  - Performing normal fault management tasks such as handling alarms tests and maintenance tests.
  - Collecting the performance data from the Session Manager elements.
- The secondary System Manager is in the standby mode and performs the following functions:
  - Receiving the database replication data from the primary System Manager, and storing the data in the database.
  - Authenticating and authorizing the elements that require System Manager services.

- Processing SNMP traps and alarms.
- Collecting the performance data from the Session Manager elements.

Rainy Day scenario

In this scenario, the primary System Manager has failed or has lost connectivity to the elements in the system. The system administrator manually administers the secondary System Manager as the active mode. The secondary System Manager manages all elements in the system.



Reasons for the primary System Manager becoming inactive include:

- The primary System Manager or the primary data center fails. You can recover the data by rebooting the System Manager server or the data center.
- The primary System Manager fails and needs hardware replacement.
- Shutting down the primary System Manager for maintenance purposes.

In the Rainy Day scenario:

- The system sends an alarm to the system administrator.
- The system administrator evaluates the situation, verifies that the failure is real, and administers the secondary System Manager to the active mode.
- The secondary System Manager sends notifications to the elements in the network to indicate that the secondary System Manager is in the active mode.
- The elements in the network verify that the secondary System Manager is in the active mode.

  The Session Manager elements automatically connect to the secondary System Manager. For the Session Manager elements that are earlier than release 6.3, you must manually reconfigure these elements with the secondary System Manager.

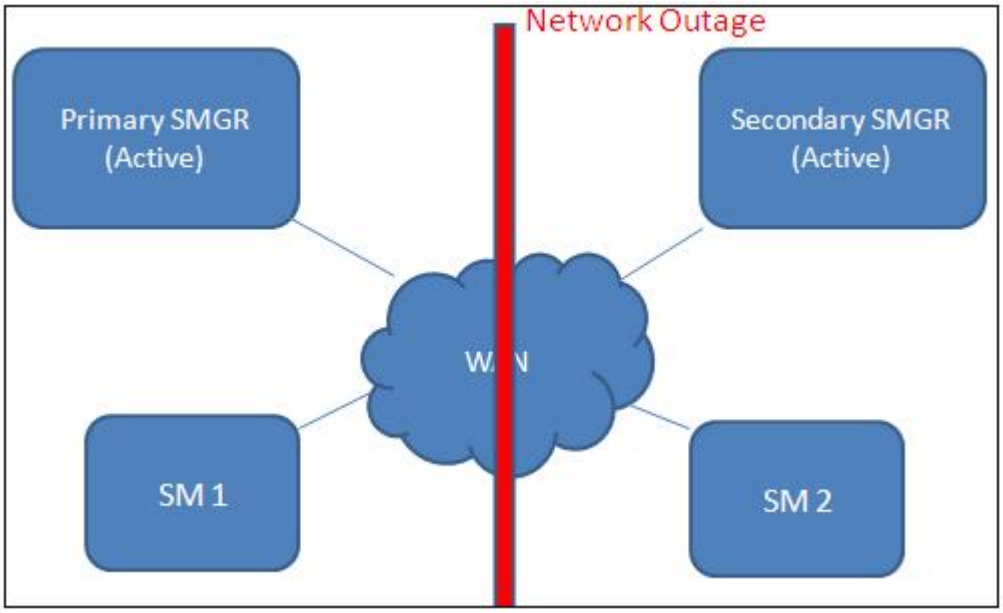
- The secondary System Manager replicates the data to the elements. The network operates with the secondary System Manager as the managing System Manager.

The system remains in this state until the administrator restores the system to the Sunny Day configuration.

Split-network Scenario

In this scenario, the system administrator administers the secondary System Manager to the active mode when the primary System Manager is also in the active mode.

The primary System Manager cannot communicate with the secondary System Manager. Some system elements can only communicate with the primary System Manager while some system elements can communicate only with the secondary System Manager.



In the split WAN or split network scenario:

- The primary System Manager is in the active mode and is communicating with all elements in the network.
- When a connectivity failure occurs in the network, the primary System Manager server and the secondary System Manager server send alarms to the system administrator about the network connectivity failure.
- The system administrator verifies that the network connectivity failure is real and that:
  - Some elements can only communicate with the primary System Manager.
  - Some elements can only communicate with the secondary System Manager.
  - Some elements can communicate with both the primary System Manager and the secondary System Manager.

- The system administrator administers the secondary System Manager to the active mode. Both the primary System Manager and the secondary System Manager are in the active mode.
- The secondary System Manager sends notifications to all elements in the network.
- The elements that can communicate with the primary System Manager function normally. The primary System Manager continues to manage these elements. The elements that cannot communicate with the primary System Manager search for a System Manager in the active mode.
- The elements in the network that cannot communicate with the primary System Manager verify that the secondary System Manager is in the active mode.
- The elements in the network that cannot communicate with the primary System Manager, but can communicate with the secondary System Manager, connect to the secondary System Manager. The secondary System Manager starts to manage these elements.
- Any elements that cannot communicate with the primary System Manager or the secondary System Manager cannot perform data replication. These elements continue to operate with the previously replicated data.

The system remains in this state until you restore the system to the Sunny Day configuration.

Managing Session Manager in a Geographic Redundancy solution

Either the primary or the secondary System Manager server manages Session Manager in different geographic redundancy scenarios.

1. Determining which System Manager manages each Session Manager:

Session Manager Release 6.3

To view the System Manager server that manages a particular Session Manager, see the **Managed By** column in the **Inventory** > **Manage Elements** webpage. The status can be *Primary*, *Secondary*, or *Unknown*. The *Unknown* value means that the System Manager instance cannot get the status from Session Manager. An active System Manager automatically refreshes this status in a periodic manner. Click **Get Current Status** to refresh the status for each Session Manager.

Session Manager releases earlier than 6.3 version

Session Managers of releases earlier than 6.3 version are not Geographic Redundancy-aware. These Session Manager instances can belong to the earlier deployments of System Managers. Usually, this System Manager instance is the primary server but can also be the secondary server. Run the **smconfig** command at the Session Manager command prompt to view the System Manager that manages the Session Manager.

Note:

For Session Managers of releases earlier than 6.3 version, the **Inventory** > **Managed Elements** webpage displays **Not Supported** in the **Managed By** column.

2. Session Manager administration:

This section provides information about the Session Manager administration for different Geographic Redundancy scenarios.

Sunny day scenario

In this case, the primary System Manager manages all Session Manager instances. The primary System Manager replicates administration changes to all Session Manager instances. The secondary server is in the standby mode and you cannot make any administration changes using this server.

Rainy day scenario

In this case, the secondary System Manager manages all Session Manager instances. The secondary System Manager replicates the administration changes to all Session Manager instances. The primary server is offline and you cannot make any administration changes using this server.

Split-network scenario

Caution:

Before making administration changes, you must assess the extent of the enterprise network split. The network split results in partitioning of Session Managers and other elements into two groups. The primary System Manager manages one group and the secondary System Manager manages the other group.

Before making administration changes, the administrator must confirm the group membership using the **Inventory** > **Managed Elements** webpage. The administrator must perform the administration changes on the primary System Manager for the Session Manager instances that the primary server manages. Similarly, the administrator must perform the administration changes on the secondary System Manager for the Session Manager instances that the secondary server manages. Each System Manager replicates the administration changes to the respective Session Manager instances. Administration changes must also be compatible with the non-Session Manager elements in the split network. For example, one System Manager must manage all elements that are referenced in a user Communication Profile.

Split-network warning messages

The call routing administration, the user administration, or the network administration webpages display a warning message when the System Manager server detects that the administrator is configuring for a split-network scenario. The primary System Manager can detect the possibility of a split-network configuration if:

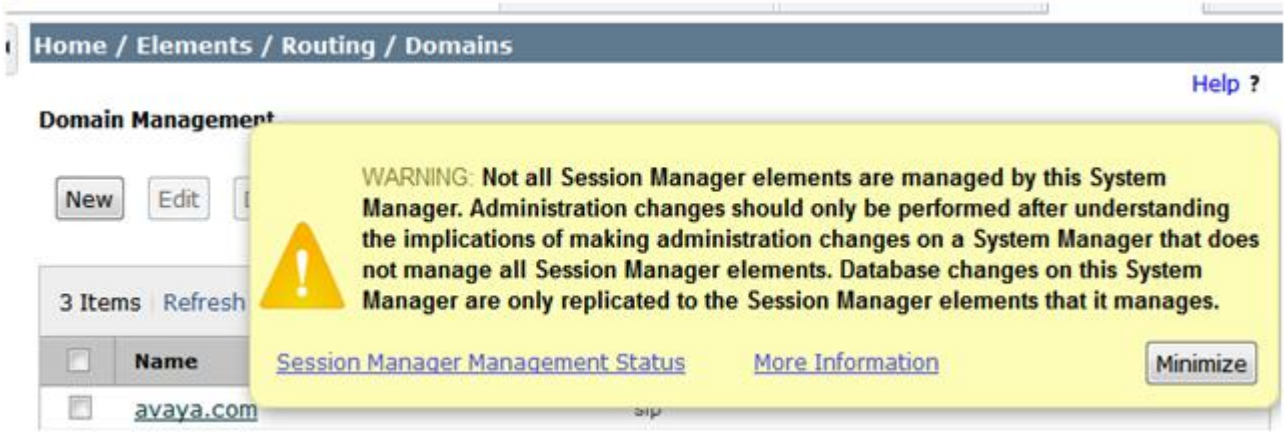
- The primary System Manager does not manage all Session Managers.
- The secondary System Manager is not reachable on the network.

- The secondary System Manager is active.

The secondary System Manager can detect the possibility of a split-network configuration if:

- The secondary System Manager is active.
- The secondary server does not manage all Session Managers.

For example, see the following warning message. When the system displays a warning message, click the **Session Manager Management Status** link to go to the **Inventory** > **Manage Elements** webpage. In this webpage, view the status of the System Manager that manages each Session Manager. Click **Minimize** to hide the warning message.



Applicability

The following table lists all Session Manager administration related functionalities for the respective webpages. When you make administration changes using any of these pages, System Manager replicates these changes only to those Session Manager instances that the System Manager manages.

Webpage	Functionality	Notes
Routing	Change the SIP call routing data.	
Session Manager > **Session Manager Administration**.	Add, edit, delete the Session Manager instances.	
Session Manager > **Communication Profile Editor**	Edit the Session Manager profiles for the administered SIP users.	Only one System Manager must manage all elements that are linked with the Communication Profile of a user. For example, Session Managers and Communication Managers that are referred in a user Communication Profile.
Session Manager > **Network Configuration**	Change the Session Manager network configuration.	

Table continues…

Webpage	Functionality	Notes
Session Manager > **Device and Location Configuration**	Change the device and the location settings.	
Session Manager > **Application Configuration**	Change the Session Manager application sequencing configuration.	
Inventory > **Manage Elements**	Add, edit, or delete the Session Manager instances	
User Management > **Manage Users**	Change the SIP user configuration or the endpoint configuration.	Only one System Manager must manage all elements that are linked with the Communication Profile of a user. For example, Session Managers and Communication Managers that are referred in a user Communication Profile.

3. Session Manager Status and Maintenance :

This section provides information about using a System Manager to view the Session Manager status and perform maintenance operations on Session Managers. For example, you can view the status of Session Manager on the **Session Manager** > **Dashboard** webpage or run the maintenance tests on Session Manager using the **Session Manager** > **Maintenance Tests** webpage. For a full list of applicable status webpages and maintenance webpages, see the *Applicability* section.

Sunny day scenario

In this case, the primary System Manager manages all Session Manager instances. Using the primary System Manager, view the Session Manager system status and perform maintenance operations. The secondary System Manager is in the standby mode. You cannot use the secondary server to view the Session Manager system status or perform maintenance operations.

Rainy day scenario

In this case, the secondary System Manager manages all Session Manager instances. Using the secondary System Manager, view the Session Manager system status and perform maintenance operations. The primary System Manager is offline and you cannot use the primary server to view the Session Manager system status or perform maintenance operations.

Split-network scenario

In this case, the administrator must assess the extent of the enterprise network split before viewing the Session Manager system status or performing maintenance operations on Session Manager. The network split results in partitioning of Session Managers and other elements into two groups. The primary System Manager manages one group and the secondary System Manager manages the other group.

The administrator must confirm the group membership using the **Inventory** > **Managed Elements** webpage. You must view the Session Manager status and perform maintenance operations using the System Manager server that manages the Session Manager instance.

Split-network warning messages

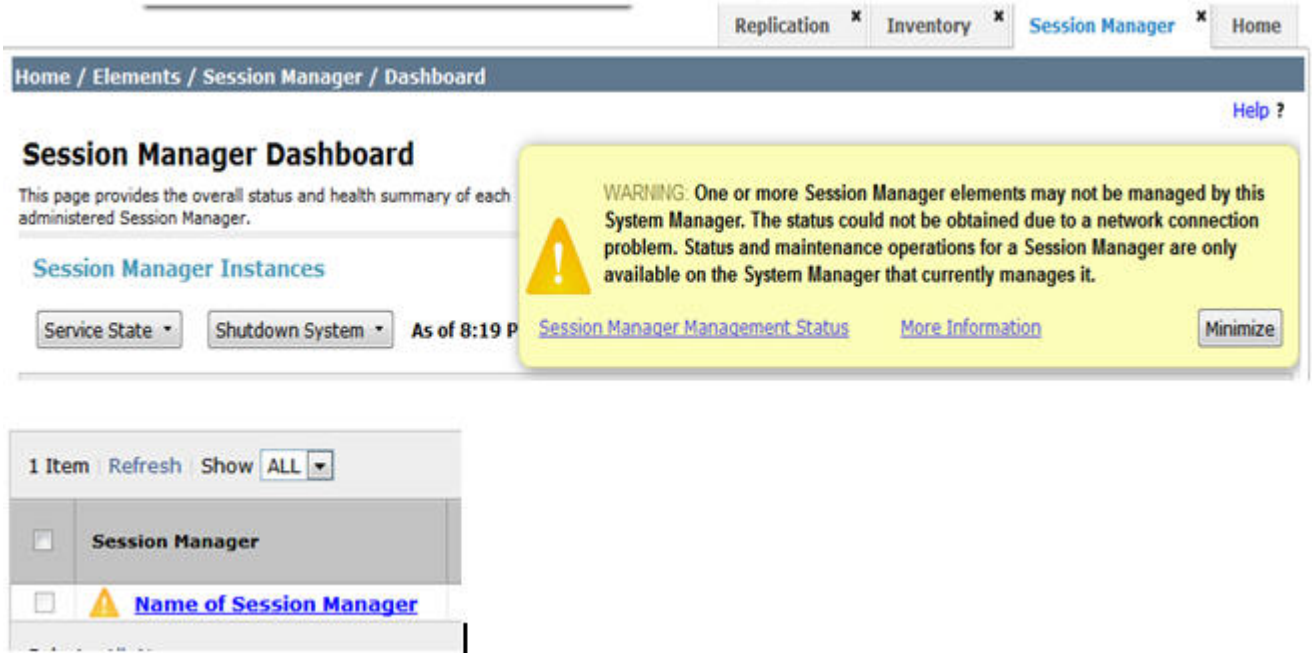
The Session Manager status webpages and the maintenance webpages display a warning message when the current System Manager detects a split-network scenario. The primary System Manager can detect a split-network configuration under the following conditions:

- The primary System Manager does not manage all Session Managers, and
- The secondary System Manager is not reachable on the network, or
- The secondary System Manager is active.

The secondary System Manager can detect a split-network configuration under the following conditions:

- The secondary System Manager is active, and
- The secondary System Manager does not manage all Session Managers.

See the following example of a warning message. If a webpage contains a list of Session Managers, then each Session Manager instance that the System Manager does not manage, remains highlighted with a warning icon. When the system displays a warning message, click the **Session Manager Management Status** link to go to the **Inventory** > **Manage Elements** webpage. In the webpage that contains a list of Session Managers, the system highlights each Session Manager instance that the System Manager does not manage with a warning icon. Click **Minimize** to hide the warning message.



Applicability

The following table lists all system status functions of Session Manager and maintenance operation functions for the respective webpages. The listed functions are only available for Session Managers that the System Manager manages.

Webpage	Functionalities	Notes
Session Manager > **Dashboard**	• View the Session Manager system status. • Accept or deny the new SIP service. • Shut down or restart Session Manager.	
Session Manager > **System Status**	• View the SIP Entity monitoring status. • View the managed bandwidth status. • View the security module status and maintenance operations status. • View the user registration status and maintenance operations status.	
Session Manager > **System Tools**	• Run the maintenance tests for Session Managers. • Configure and view the SIP traces. • Run the Session Manager call routing tests.	
Replication	Perform the Session Manager replica maintenance operations.	You can repair the Session Manager replicas from a System Manager that manages the Session Manager.
Inventory > **Manage Elements**	View and edit the trusted and the identify certificate configuration of Session Manager.	

4. Fault Management (Alarming and Logging):

This section provides information on viewing the Session Manager alarms and the logs using the primary and secondary System Managers.

Sunny day scenario

Both the primary and the secondary System Manager collect alarms from all Session Managers. You can view all Session Manager related alarms from the primary System Manager using the **Events** > **Alarms** webpage. The secondary System Manager runs in the standby mode and you cannot view alarms.

Collect logs from a Session Manager server using the **Events** > **Logs** > **Log Harvester** webpage of the primary System Manager. The secondary System Manager is in the standby mode. You cannot collect logs using the secondary System Manager.

View Session Manager audit logs from the primary System Manager using the **Events** > **Logs** > **Log Viewer** webpage. These logs provide details of administration changes made from the primary System Manager. The secondary System Manager runs in the standby mode. You cannot view these logs on the secondary System Manager.

Rainy day scenario

The secondary System Manager collects alarms from all Session Managers. After you configure the secondary System Manager into the active state, view the following alarms using the **Events** > **Alarms** webpage:

- Alarms collected when the secondary server was in the standby mode.
- New Session Manager related alarms.

The primary System Manager is offline. You cannot view alarms using the primary System Manager.

Collect logs from a Session Manager server using the **Events** > **Logs** > **Log Harvester** webpage of the secondary System Manager. The primary System Manager is offline. You cannot collect logs using the primary System Manager.

View Session Manager audit logs from the secondary System Manager using the **Events** > **Logs** > **Log Viewer** webpage. These logs provide details of the administration changes made after the activation of the secondary System Manager. The primary System Manager is offline. You cannot use the primary System Manager to view these logs.

Split-network scenario

In the split-network scenario, both the primary and the secondary System Manager collect alarms from any Session Manager that are reachable on the enterprise network. View these alarms from the **Events** > **Alarms** webpage. If Session Manager cannot connect to a System Manager because of the network split, the Session Manager forwards all logs to that System Manager when the network connectivity restores. Use the **Inventory** > **Manage Elements** webpage to view the status of the network connectivity from the current System Manager to each Session Manager instance.

View the logs collected from a Session Manager server using the **Events** > **Logs** > **Log Viewer** webpage of the primary or the secondary System Manager that manages the Session Manager server. You cannot collect logs from Session Manager that the current System Manager does not manage.

View the Session Manager audit logs from both the primary and secondary System Manager using the **Events** > **Logs** > **Log Viewer** webpage. Each System Manager displays audit logs for the administration changes made on that System Manager after the server became active.

5. Performance Management:

This section provides information on the performance data collection and the performance data analysis of Session Manager.

Sunny day scenario

The primary and the secondary System Manager collect the performance data from all Session Managers based on the configuration settings. The configuration settings are available on the

Session Manager > **Performance** > **Data Collection** webpage of the primary System Manager. Analyze the data in the primary System Manager using the webpages under **Session Manager** > **Performance**. The secondary System Manager is in the standby mode. You cannot analyze the collected performance data using the secondary System Manager.

Rainy day scenario

The secondary System Manager collects the performance data from all Session Managers based on the configuration settings on the **Session Manager** > **Performance** > **Data Collection** webpage of the secondary System Manager. Analyze the data on the secondary System Manager using the webpages under **Session Manager** > **Performance**. The primary System Manager is offline. You cannot analyze the collected performance data using the primary System Manager.

Split-network scenario

The primary and the secondary System Manager collect the performance data from all Session Managers that are reachable on the enterprise network. The system performs the performance data collection on each System Manager based on the settings configured on the **Session Manager** > **Performance** > **Data Collection** webpage of the System Manager.

Note:

You cannot collect the performance data from Session Manager that is not reachable on the network from System Manager. When the connectivity restores, the system resumes the performance data collection. Use the **Inventory** > **Manage Elements** webpage to view the status of the connectivity from the current System Manager to each Session Manager.

Both the primary and the secondary System Manager can analyze the performance data using the **Session Manager** > **Performance** webpage. A System Manager server cannot collect the performance data from Session Manager that is not reachable. This results in data gaps for the unobtainable data until the connection to all Session Managers restores.

Data center failures

About this task

This section covers all the possible System Manager failures and enterprise network failure scenarios. This section also provides the detailed procedures for restoring the System Manager back into the normal mode of operation.

For more information about system monitoring, see *Geographic Redundancy Health Monitoring* in *Administering Avaya Aura® System Manager*.

Managing data center failures Case 1: The primary data center fails

Procedure

1. Determine whether the System Manager failure is severe.
   - If you can gain access to the primary System Manager in a short duration, restart the primary System Manager and keep the secondary System Manager in the standby mode. In this case, do not follow the procedure in this section.
   - If you cannot gain access to the primary System Manager in a short duration, activate the secondary System Manager and continue to follow the procedures in this section.
2. Manually activate the secondary System Manager using the Geographic Redundancy webpage of the secondary System Manager.

   For more information, see *Activating the secondary System Manager Server* in *Administering Avaya Aura® System Manager*. Manual activation of the secondary System Manager takes between 10 to 20 minutes. Wait until the secondary System Manager is accessible.

   Avoid making any changes to the call routing configuration, the user configuration, or the network configuration administration on the secondary System Manager. Retaining the same configuration as on the primary System Manager simplifies the process of restoring the system back into the sunny day configuration.
3. Verify that the secondary System Manager is active. Confirm this fact by viewing the Geographic Redundancy webpage of the secondary System Manager.
4. Verify that the secondary System Manager is managing all the Session Manager instances that are Geographic Redundancy-aware.

   For more information, see *Determining the System Manager that Manages each Session Manager*.
5. Reconfigure Geographic Redundancy-unaware elements to use the secondary System Manager. Run the **`changeMgmtIP`** command from the Session Manager command line to reconfigure the Session Manager to use the secondary System Manager.

   For more information, see the *Changing the IP address or FQDN in System Manager* section in *Maintaining and Troubleshooting Avaya Aura® Session Manager*.
6. Verify that the data replication from the secondary System Manager to the Session Manager elements is working.

   To verify the data replication, view the Replication page of the secondary System Manager.

   For more information, see the *Managing system data* section in *Administering Avaya Aura® Session Manager*.
7. In the **Session Manager** > **System Status** > **User Registrations** webpage of the secondary System Manager, verify that the endpoints can complete the registrations.

For more information, see the *User Registration* section in *Administering Avaya Aura® Session Manager*.

8. On the secondary System Manager Web Console, using the **Session Manager** > **System Tools** > **Maintenance Tests** webpage, perform the maintenance tests on the Session Manager instances that are managed by the secondary System Manager.

   For more information, see the *Maintenance tests* section in *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

9. After the primary System Manager comes back to service, recover the server and configure the secondary System Manager to the standby mode similar to the sunny day scenario. Follow the steps as mentioned below:

   a. Deactivate the secondary System Manager by using the Geographic Redundancy webpage from the secondary System Manager.

      Note:

      For more information, see the *Deactivating the secondary System Manager server* section in *Administering Avaya Aura® System Manager*.

      Manual deactivation of the secondary System Manager takes between 10 to 20 minutes.

   b. Verify that the secondary System Manager is in the standby mode by checking the Geographic Redundancy webpage of the primary System Manager.

      Logging in to the secondary System Manager Web Console must indicate that the System Manager is in the standby mode.

   c. From the primary System Manager, run the database recovery procedure in the Geographic Redundancy webpage.

      Using this step, you can keep the current primary System Manager database or replace with the secondary System Manager database. For more information, see *Restoring the primary System Manager server* in *Administering Avaya Aura® System Manager*.

   d. Verify that the primary System Manager is managing all the Geographic Redundancy-aware elements.

      For more information, see *Determining the System Manager that Manages each Session Manager*.

   e. Reconfigure the Geographic Redundancy-unaware elements to use the primary System Manager. To reconfigure a Session Manager to use the primary System Manager, run the **`changeMgmtIP`** command from the command line.

      For more information about changing the IP address or the FQDN, see *Changing the IP address or FQDN in System Manager* in *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

Managing data center failures Case 2: Primary System Manager fails

Procedure

1. Shut down the primary System Manager.

   For more information, see *Graceful shutdown* in *Administering Avaya Aura® System Manager*.

2. Activate the secondary System Manager using the Geographic Redundancy webpage of the secondary System Manager.

   For more information about activating the server, see *Activating the secondary System Manager Server* in *Administering Avaya Aura® System Manager*. Manual activation of the secondary System Manager takes between 10 to 20 minutes. Wait until the secondary System Manager is accessible.

   Avoid making any changes to the call routing configuration, the user configuration, or the network configuration administration on the secondary System Manager. Retaining the same configuration as on the primary System Manager simplifies the process of restoring the system back into the sunny day configuration.

3. Verify that the secondary System Manager is active by logging into the Web Console.

4. Verify that the secondary System Manager is managing all Geographic Redundancy-aware elements.

   For more information about determining the System Manager that manages each Session Manager, see *Determining the System Manager that Manages each Session Manager*.

5. If you have not enabled geographic redundancy for some Session Managers, then you must manually reconfigure these elements to use the secondary System Manager. Run the **`changeMgmtIP`** command from the Session Manager command line to reconfigure the Session Manager to use the secondary System Manager.

   For more information about changing the IP address or the FQDN, see *Changing the IP address or FQDN in System Manager* in *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

6. Perform the hardware replacement procedure.

   For more information about the field replacement of the primary System Manager, see the related server documentation from the Avaya support site.

7. Deactivate the secondary System Manager using the Geographic Redundancy webpage of the secondary System Manager.

   For more information about deactivating the secondary System Manager, see *Deactivating the secondary System Manager server* in *Administering Avaya Aura® System Manager*.

Note:

Manual deactivation of the secondary System Manager takes between 10 to 20 minutes.

8. Verify that the secondary System Manager is in the standby mode by checking the *Geographic Redundancy* webpage of the primary System Manager.

   Logging in to the secondary System Manager Web Console must indicate that the System Manager is in the standby mode.

9. From the primary System Manager, run the *database recovery* procedure from the Geographic Redundancy webpage. Using this step, you can keep the current primary System Manager database or replace with the database from the secondary System Manager.

   For more information about restoring the primary System Manager server, see *Restoring the primary System Manager server* in *Administering Avaya Aura® System Manager*.

10. Verify that the primary System Manager is managing all the Geographic Redundancy-aware elements.

    For more information, see the topic *Determining the System Manager that Manages each Session Manager*.

11. Reconfigure the Geographic Redundancy-unaware elements to use the primary System Manager. To reconfigure a Session Manager to use the primary System Manager, run the **`changeMgmtIP`** command from the command line.

    For more information about changing the IP address or the FQDN, see *Changing the IP address or FQDN in System Manager* in *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

Case 3: Replacing the secondary System Manager due to hardware failures

For more information about the field replacement of the secondary System Manager, see *Activating the secondary System Manager Server* in *Administering Avaya Aura® System Manager*.

Case 4: Shutting down the primary System Manager for maintenance

Follow the procedure in Managing data center failures - Case 2 on page 42.

Case 5: The primary System Manager cannot communicate with the secondary System Manager. The system elements can communicate with the primary System Manager and the secondary System Manager

Restore the network connection between the primary System Manager and the secondary System Manager.

Case 6: The primary System Manager cannot communicate with the system elements, but the elements can communicate with the secondary System Manager

Procedure

1. Activate the secondary System Manager using the Geographic Redundancy webpage of the secondary System Manager.

   For more information about activating the secondary System Manager server, see *Activating the secondary System Manager Server* in the book *Administering Avaya Aura® System Manager*. Manual activation of the secondary System Manager takes between 10 to 20 minutes. Wait until the secondary System Manager is accessible.

   Avoid making any changes to the call routing configuration, the user configuration, or the network configuration administration on the secondary System Manager. Retaining the same configuration as on the primary System Manager simplifies the process of restoring the system back into the sunny day configuration.

2. Verify that the secondary System Manager is managing all the geographical redundancy-aware Session Manager instances.

   For more information about determining the System Manager that manages each Session Manager, see *Determining the System Manager that Manages each Session Manager*.

3. Reconfigure the Geographic Redundancy-unaware elements to use the secondary System Manager. Run the **`changeMgmtIP`** command from the Session Manager command line to reconfigure the Session Manager to use the secondary System Manager.

   For more information about changing the IP address or the FQDN , see *Changing the IP address or FQDN in System Manager* in *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

4. Deactivate the secondary System Manager using the Geographic Redundancy webpage of the secondary System Manager.

   For more information, see *Deactivating the secondary System Manager server* in *Administering Avaya Aura® System Manager*.

Note:

Manual deactivation of the secondary System Manager takes between 10 to 20 minutes.

5. Verify that the secondary System Manager is in the standby mode by checking the *Geographic Redundancy* webpage of the primary System Manager. Logging in to the secondary System Manager Web Console must indicate that the System Manager is in standby mode.
6. From the primary System Manager, run the *database recovery* procedure from the Geographic Redundancy webpage. Using this step, you can keep the current primary System Manager database or replace with the database from the secondary System Manager.

   For more information, see *Restoring the primary System Manager server* in *Administering Avaya Aura® System Manager*.
7. Verify that the primary System Manager is managing all the Geographic Redundancy-aware elements.

   For more information, see *Determining the System Manager that Manages each Session Manager*.
8. Reconfigure the Geographic Redundancy unaware-elements to use the primary System Manager. To reconfigure a Session Manager to use the primary System Manager, run the **`changeMgmtIP`** command from the command line.

   For more information about changing the IP address or the FQDN, see *Changing the IP address or FQDN in System Manager* in *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

Case 7: System elements can communicate only with the primary System Manager

Restore the network connection between the system elements and the secondary System Manager.

Case 8: The primary System Manager cannot communicate with the secondary System Manager. Some system elements can communicate only with the primary System Manager while some system elements can communicate only with the secondary System Manager

Procedure

1. Activate the secondary System Manager using the Geographic Redundancy webpage of the secondary System Manager.

   For more information about activating the secondary System Manager server, see *Activating the secondary System Manager Server* in *Administering Avaya Aura® System Manager*. Manual activation of the secondary System Manager takes between 10 to 20 minutes. Wait until the secondary System Manager is accessible.

   Avoid making any changes to the call routing configuration, the user configuration, or the network configuration administration on the secondary System Manager. Retaining the same configuration as on the primary System Manager simplifies the process of restoring the system back into the sunny day configuration.

2. Verify that the secondary System Manager is managing the Geographic Redundancy-enabled Session Manager instances that cannot communicate with the primary System Manager.

   For more information, see *Determining the System Manager that Manages each Session Manager*.

3. Reconfigure the Geographic Redundancy-unaware elements that cannot communicate with the primary System Manager to use the secondary System Manager. Run the **`changeMgmtIP`** command from the Session Manager command line to reconfigure the Session Manager to use the secondary System Manager.

   For more information, see *Changing the IP address or FQDN in System Manager* in *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

4. Restore the network connection between the primary System Manager and the elements that are not connected to the primary System Manager. Restore the network connection between the secondary System Manager and the elements that cannot connect to the secondary System Manager.

5. Deactivate the secondary System Manager using the Geographic Redundancy webpage of the secondary System Manager.

   For more information, see *Deactivating the secondary System Manager server* in *Administering Avaya Aura® System Manager*.

Note:

Manual deactivation of the secondary System Manager takes between 10 to 20 minutes.

6. Verify that the secondary System Manager is in standby mode by checking the *Geographic Redundancy* webpage of the primary System Manager.

   Logging in to the secondary System Manager Web Console must indicate that the System Manager is in the standby mode.

7. From the primary System Manager, run the *database recovery* procedure from the Geographic Redundancy webpage. Using this step, you can keep the current primary System Manager database or replace with the database from the secondary System Manager.

   For more information about restoring the primary System Manager server, see *Restoring the primary System Manager server* in *Administering Avaya Aura® System Manager*.

8. Verify that the primary System Manager is managing all the Geographic Redundancy-aware elements.

   For more information about determining the System Manager that manages each Session Manager, see *Determining the System Manager that Manages each Session Manager*.

9. Reconfigure the Geographic Redundancy-unaware elements to use the primary System Manager. To reconfigure a Session Manager to use the primary System Manager, run the **`changeMgmtIP`** command from the command line.

   For more information about changing the IP address or the FQDN, see *Changing the IP address or FQDN in System Manager* in *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

   For more information about managing Session Manager in a split-network scenario, see *Managing Session Manager in a Geographically Redundant Solution*.

Setting up a Geographic Redundancy enabled system

Before you begin

Ensure that the installed primary and the secondary System Manager servers:

- Contain the same hardware.
- Satisfy the following requirements:
  - Must have the same hardware configuration.
  - Must contain the same version of the System Manager software that includes the template, the software packs, and the patches.
  - Must be able to communicate with each other over the network.

- Must have synchronized network time.

The high-level steps for setting up the Geographic Redundancy-enabled system are as follows:

Procedure

1. Install the primary System Manager with the release 7.1 software or upgrade the System Manager server to the release 7.1.
2. Install the System Manager 7.1 software version on the secondary System Manager.
3. Configure the two System Managers for the Geographic Redundancy operation. For more information, see *Configuring Geographic Redundancy* in *Administering Avaya Aura ® System Manager*.
4. Enable the replication of the primary System Manager data to the secondary System Manager. For more information, see *Enabling the Geographic Redundancy replication* in *Administering Avaya Aura® System Manager*.
5. Conduct the system verification tests to verify the Geographic Redundancy-enabled system. For more information, see *System Verification Tests*.

Upgrade to a Geographic Redundancy-enabled system

About this task

The two basic ways to upgrade an Avaya Aura® solution to a Geographic Redundancy-enabled system, where System Manager is geographically redundant, are:

- Simultaneous element upgrade method
- Selected element upgrade method

Upgrading simultaneous element method

Procedure

1. Upgrade the System Manager server to the release 7.1. The upgraded System Manager server becomes the primary System Manager.
2. Install the System Manager release 7.1 software again for the secondary System Manager server.
3. Log in to the secondary System Manager and enable the Geographic Redundancy feature. This step configures the current System Manager as the secondary and the upgraded System Manager as the primary.

   For more information about configuring the geographic redundancy feature, see *Configuring Geographic Redundancy* in *Administering Avaya Aura® System Manager*.

4. Associate the secondary System Manager and the SAL Gateway with the primary System Manager as the new trap destination. This step ensures that the alarms generated on the various elements are send to both System Managers, associated SAL Gateways, and to any customer designated Network Management Systems (NMS) within the solution.

   For more information about managing alarms, see *Managing Alarms* in *Administering Avaya Aura ® System Manager*.

5. Enable replication from the primary to the secondary System Manager.

   For more information about enabling the geographic redundancy replication, see *Enabling the Geographic Redundancy replication* in *Administering Avaya Aura® System Manager*.

6. Upgrade Session Managers and Branch Session Managers to the release 7.1.

   For more information about upgrading Session Manager, see *Upgrading Avaya Aura® Session Manager*.

7. Now, System Managers and Session Managers operate in the Geographic Redundancy mode.

8. Conduct the system verification tests to verify the Geographic Redundancy-enabled system.

   For more information about the system verification tests, see *System Verification Tests*.

Upgrading selected element method

Procedure

1. Upgrade the System Manager server to System Manager 7.1. This server becomes the primary System Manager. Fresh install a new System Manager 7.1 server as the secondary server.

2. Log in to the secondary System Manager server and enable geographical redundancy. This step configures the current System Manager as the secondary and the upgraded System Manager as the primary.

   For more information about configuring geographic redundancy, see *Configuring Geographic Redundancy* in *Administering Avaya Aura® System Manager*.

3. Associate the secondary System Manager and the SAL Gateway with the primary System Manager as new trap destination. This step ensures that the alarms generated on the various elements are sent to both System Managers, associated SAL Gateways, and to any customer designated Network Management Systems (NMS) within the solution.

   For more information about administering System Manager, see *Administering Avaya Aura ® System Manager*.

4. Enable replication from the primary to the secondary System Manager.

For more information about enabling the Geographic Redundancy replication, see *Enabling the Geographic Redundancy replication* in *Administering Avaya Aura® System Manager*.

5. **(Optional)** Upgrade Session Managers and Branch Session Managers to the release 7.1.
6. Now the upgraded System Managers and Session Managers begin operating in Geographic Redundancy-enabled mode.
7. Conduct the system verification tests to verify the Geographic Redundancy-enabled system.

   For more information about the system verification tests, see *System Verification Tests*.
8. Using this upgrade method, upgrade the remaining elements at a later time.

Performing system verification tests

About this task

Use this procedure to verify that a Geographic Redundancy-enabled systems is operating correctly in a sunny day scenario.

Procedure

1. Check the Geographic Redundancy status of the system.
   a. Go to the Geographic Redundancy web page of the primary System Manager.
   b. Verify the expected configuration settings.
   c. To view the Geographic Redundancy condition, go to the **Geographic Redundancy** > **GR Health** web page of the primary System Manager.
2. Go to the Session Manager Dashboard web page.
3. Verify the status for each Session Manager and Branch Session Manager.
4. **(Optional)** Run the System Manager and Session Manager maintenance tests from the primary System Manager. Go to the **Session Manager** > **System Status** > **Maintenance Tests** web page and run the tests.

Chapter 4: Synchronizing Communication Manager data with the System Manager database

The following sections explain how to synchronize the Communication Manager station data with the System Manager database. The system automatically connects to System Manager and to Communication Manager in the core. The system then synchronizes the provisioning data in the System Manager database with each managed Communication Manager instance.

Synchronize the endpoint data in a scheduled and incremental basis by:

- administering each Communication Manager instance as an entity or application instance.
- initializing the synchronization of Communication Manager and the messaging data with System Manager.

Creating a Communication Manager instance in the system

Adding a new element

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left 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.
6. Click **Commit**.

   The system creates a new element.

Add Communication Manager field descriptions

General Attributes

Field	Description
Name	The name of Communication Manager instance.
Hostname or IP Address	The IP address can be in the IPv4 or IPv6 format. The host name or the IP address of the Communication Manager instance. For the duplicated Communication Manager, this value references the active server IP address.
Login	The login name that you use to connect to the Communication Manager instance. **Note:** craft, craft2, dadmin, inads, init, rasaccess, sroot, and tsc are the restricted logins when you configure a Communication Manager system. Do not use the login name to connect to: • The Communication Manager instance from any other application. • The Communication Manager SAT terminal by using command line interface (CLI).
Authentication Type	The type of password that authenticates the SSH or Telnet login name on the element.
Password	The password that authenticates the SSH or Telnet login name on the element.
Confirm Password	The password that you retype for confirmation. **Note:** **Confirm Password** must match **Password**.
ASG Key	The ASG key that authenticates the SSH or Telnet login name on the element. This field is only available if **ASG Key** is selected in **Authentication Type**.
Confirm ASG Key	The ASG key that you retype for confirmation. This field is only available if **ASG Key** is selected in **Authentication Type**. **Note:** **Confirm ASG key** must match **ASG key**.

Table continues…

Field	Description
SSH Connection	An option to use SSH for connecting to the element. By default, the system selects the check box. If you clear the check box, the system uses Telnet to connect to the element.
RSA SSH Fingerprint (Primary IP)	The RSA SSH key of the Communication Manager server. For duplex servers, the RSA SSH key is the key of the active server.
RSA SSH Fingerprint (Alternate IP)	The DSA SSH key of the standby Communication Manager server. Use the DSA SSH key only for duplex servers.
Description	A description of the Communication Manager server.
Alternate IP Address	The alternate IP address of the element. For duplex servers, the alternate IP address is the IP address of the standby server.
Enable Notifications	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: • Selected: Enables the CM Notify sync feature for this Communication Manager instance. • Cleared: Disables the CM Notify sync feature for this Communication Manager instance. 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. **Note:** Communication Manager 6.2 or later supports this feature.
Port	The port on which the service provided by the element is running. The default SSH port is 5022. **Note:** 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 **SSH Connection** checkbox. When you select this checkbox, the system auto populates the default port value to 5022.
Location	The location of the element.
Add to Communication Manager	An option to select the Communication Manager that you want to view in the communication manager list.

SNMPv1 Attributes

The below fields are available only if **V1** is selected in the **Version** field.

Field	Description
Version	The SNMP protocol type.
Read Community	The read community of the device.
Write Community	The write community of the device.
Retries	The number of times an application polls a device without receiving a response before timing out.
Timeout (ms)	The number of milliseconds an application polls a device without receiving a response before timing out.
Device Type	The Communication Manager application type. The options are: • **Avaya Aura(R) Communication Manager SP** for Communication Manager 6.3.100 on System Platform. • **Avaya Aura(R) Communication Manager VE** for Virtualized Environment-based Communication Manager 6.3.100 and Release 7.1.3.

SNMPv3 Attributes

The below fields are available only if **V3** is selected in the **Version** field.

Field	Description
Version	The SNMP protocol type.
User Name	The user name as defined in the application.
Authentication Protocol	The authentication protocol that authenticates the source of traffic from SNMP V3 protocol users. The possible values are: • **MD5 (default)** • **SHA** • **None**
Authentication Password	The SNMP authentication password.
Confirm Authentication Password	The SNMP authentication password that you retype for confirmation. **Authentication Password** and **Confirm Authentication Password** must match.
Privacy Protocol	The encryption policy for SNMP V3 users. The possible values are: • **AES**: Use the AES encryption for the SNMP-based communication. AES is the default protocol. • **DES**: Use the DES encryption for the SNMP-based communication. • **None**: Do not encrypt traffic for this user.
Privacy Password	The pass phrase used to encrypt the SNMP data.
Confirm Privacy Password	Retype the privacy password in this field for confirmation.
Retries	The number of times the application polls a device without receiving a response before timing out.

Table continues…

Field	Description
Timeout (ms)	The number of milliseconds the application waits for the response from the device being polled.
Device Type	The type of device.

Button	Description
Commit	Adds a Communication Manager instance in the inventory.
Clear	Clears all the entries.
Cancel	Cancels your action and return to the previous page.

Messaging elements

When you create a Messaging element:

- The FQDN or IP address in the **Node** field for a Messaging element must correspond to the Messaging Storage Server (MSS), *not* the Messaging Application Server (MAS).
- The login credentials must be identical between the Messaging server trusted servers screen and the Session Manager application, entity, or attributes for a Messaging type of application.
- The **Trusted Server Name** field on the Trusted Server page maps to the **Login** field in the Attributes section.
- The **Password** field on the Trusted Server page maps to the **Password** field in the Attributes section.

When you add an application entity using the Manage Elements pages, System Manager imports relevant data from the application instance to the Communication System Management database in the background.

Creating a Messaging instance

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Elements**.
2. Click **New**.
3. In the **Type** field, select **Messaging** from the drop-down menu.
4. When the page refreshes, under the **General** section, enter the appropriate information in the **Name** and **Description** fields.
5. In the **Node** field, enter the FQDN or IP address of the Messaging Storage Server (MSS).

6. Click **Commit**.
7. Check the status of the data import:
    a. Navigate to the job scheduler at **System Manager Data** > **Scheduler**
    b. Check the log files on the Communication System Management server.
8. Before you add the Messaging box in System Manager applications:
    a. Navigate to the Messaging Administration/Trusted Servers screen.
    b. In the Trusted Server list on the Messaging box, add the System Manager server or the Communication System Management server information.
    c. Verify the login credentials are identical on the Messaging box trusted servers screen and the Session Manager application, entity, and attributes for a Messaging type of application.
    d. Verify the **Trusted Server Name** field on the Trusted Server page is mapped to the **Login** field in the Attributes section.
    e. Verify the **Password** field on the Trusted Server page is mapped to the **Password** field in the Attributes section.
    f. To allow the LDAP access to the Messaging box from the trusted server, set the **LDAP Access Allowed** field to `yes` on the Trusted Server page.

Synchronizing the Communication Manager data and configuring options

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left 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**.

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.

Manage Elements field descriptions

Field	Description
Name	The name of the element.
Node	The node on which the element runs. The IP address can be in the IPv4 or IPv6 format.
Type	The type of the element to which the element belongs. **Note:** You can view this field only if you gain access to the Manage Elements page from **Inventory**.

Table continues…

Field	Description
Device Type	The device type of the element. For example, for IP Office, the device type can be IP Office or B5800.

The system also provides the following fields when System Manager is configured with Geographic Redundancy.

Field	Description
Reachable	The state that specifies if the element is reachable from the current server. The values are Yes and No.
Managed by	The server that manages this element. The options are Primary and Secondary. For a non-GR element, the field displays Not Supported.
Last Updated Time	The time when the system updates the status of the element.
Error	A red cross icon (✖) if the system generates errors. For more information, you can click the icon.
Warning	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
View	The View <Element-name> page. Use this page to view the details of the selected element.
Edit	The Edit <Element-name> page. Use this page to modify the information of the instance.
New	The New Elements page. Use this page to create a new element.
Delete	The Delete <Element-name> page. Use this page to delete a selected element.

Table continues…

Button	Description
Get Current Status	The real-time connectivity status and the manageability status of elements on the active server. 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. **Note:** • On the secondary System Manager server in the standby mode, the system displays only the connectivity status of elements and not the manageability status. • On a standalone server, the system disables **Get Current Status**.
More Actions > **Manage Trusted Certificates**	The Trusted Certificates page. Use this page to view, add, export, and delete the trusted certificates for the element.
More Actions > **Manage Identity Certificates**	The Identity Certificates page. Use this page to view, export, renew, and replace the identity certificates for the element.
More Actions > **Manage**	An option to set System Manager to start managing the selected element.
More Actions > **Unmanage**	An option to set System Manager to stop managing the selected element.
More Actions > **Import**	The Import Applications page. Use this page to import application data in bulk from a valid XML file.

Table continues…

Button	Description
More Actions > **View Notification Status**	The status of notifications. The valid statuses are Failed and Inprogress. The system displays the progress bar if a notification is pending. The system displays the **Resend Notification** button only when there are no notifications in progress and when you select the rows of the same event type. If you click **Resend Notification**, the system displays a progress bar until the resend operation is complete or fails. 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. **Note:** **View Notification Status** is available only on the primary or the secondary System Manager server that is in the active state.
Filter: Enable	The fields where you can set the filter criteria. **Filter: Enable** is a toggle button.
Filter: Disable	Hides the column filter fields. **Filter: Disable** is a toggle button.
Filter: Apply	Filters elements based on the filter criteria.
Select: All	Selects all elements in the table.
Select: None	Clears the selection for the users that you select.
Refresh	Refreshes the element information in the table.

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. For example, for Presence Services, you can select a standalone Presence Services or Presence Services on Avaya Breeze™.

Field	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. **Note:** The system displays the **Node** field when you select **Other** from the **Node** field.
Device Type	The device type of the element. 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: • **URI**: For system web services API. • **SSH**: For application upgrade functions. • **SNMP**: For discovering elements.
Access Profile Sub Type	The sub type of the URI access profile. The options are: • **EMURL**: To create a URL type access profile. • **WS**: To create a web service access profile. • **GUI**: To create a GUI access profile. • **GRCommunication**: To create a GR-aware element. • **TenantURL**: To create the tenant-related access profile. • **Other**

Table continues…

Name	Description
Protocol	The protocol that the element supports to communicate with other communication devices.
Host	The name of the host on which the element is running.
Port	The port on which the element is running.
Order	The order in which you gain access to access profiles.

Button	Description
View	Displays fields in the Access Profile section that you can use to view access profile details.
New	Displays fields in the Access Profile section that you can use to add access profile details.
Edit	Displays fields in the Access Profile section using which you can modify the access profile details that you select.
Delete	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:

Field	Description
Protocol	The protocol used to access profiles. The options are: • **URI**: For system web services API. • **SSH**: For application upgrade functions. • **SNMP**: For discovering elements. **Note:** The page displays the button only when you click **Add** or **Edit** in the Access Profile section.

Access Profile Details

The page displays the following fields when you click **URI** in the **Protocol** field:

Field	Description
Name	The name of the access profile.

Table continues…

Field	Description
Access Profile Type	The type of the access profile. The options are: • **EMURL**: To create a URL type access profile. • **WS**: To create a web service access profile. • **GUI**: To create a GUI access profile. • **GRCommunication**: To create a GR-aware element. • **TenantURL**: To create the tenant-related access profile. • **Other**
Protocol	The protocol for communicating the element.
Host	The name of the host on which the element is running.
Port	The port on which the element is running.
Path	The path to gain access to the access profile.
Order	The order in which you gain access to access profiles.
Description	A brief description of the access profile.

The page displays the following fields when you click **SSH** in the **Protocol** field:

Field	Description
Name	The name of the access profile.
Login Name	The login name as configured on the element.
Port	The port on which the element is running.
Password	The password to log in to the element.
Confirm Password	The password that you retype.

The page displays the fields when you click **SNMP** in the **Protocol** field and **V3** in the **Type** field:

Field	Description
Profile Name	The name of the profile.
Description	A brief description of the profile.
Type	The SNMP protocol type.
User	The user name as defined in the element.

Table continues…

Field	Description
Authentication Type	The authentication protocol used to authenticate the source of traffic from SNMP V3 users. The possible values are: • **MD5** The default is **MD5**. • **SHA** • **None** **Authorization Type** applies only to the SNMP V3 protocol.
Authentication Password	The password to authenticate the user. The password must contain at least eight characters. **Note:** The password is mandatory.
Confirm Authentication Password	The SNMP V3 protocol authentication password that you retype for confirmation.
Privacy Type	The encryption policy for an SNMP V3 user. The possible values are: • **DES**: For SNMP-based communication. The default is **DES**. • **AES**: For SNMP-based communication. • **None**: Does not encrypt traffic for this user. Set **Privacy Type** only for an SNMP V3 user.
Privacy Password	The password used to enable the **DES** or **AES** encryption. DES passwords must contain at least eight characters.
Confirm Privacy Password	The privacy password that you retype for confirmation.
Privileges	The privileges that determine the operations that you can perform on MIBs. • **Read/Write**: To perform GET and SET operations. • **Read**: To perform only the GET operation. • **None** The default is None.
Timeout	The time in milliseconds for which the element waits for a response from the device being polled during discovery.

Table continues…

Field	Description
Retries	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:

Field	Description
Profile Name	The name of the profile.
Description	A brief description of the profile.
Type	The SNMP protocol type. **Note:** To upgrade Communication Manager using SNMP protocol, you must select SNMPV1.
Read Community	The read community of the device. **Read Community** applies only to the SNMP V1 protocol.
Write Community	The write community of the device. **Write Community** applies only to the SNMP V1 protocol.
Timeout	The time in milliseconds for which the element waits for a response from the device that the element polls.
Retries	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
Save	Saves the access profile details. **Note:** This button is available only when you click **Add** and **Edit** in the Access Profile section.
Cancel	Cancels the operation of creating or editing an access profile and hides the fields where you enter or modify the access profile information. **Note:** This button is available only when you click **Add** and **Edit** in the Access Profile section.

Port

Field	Description
Name	The name of the port.
Port	The port on which the element is running.
Protocol	The protocol for the corresponding port.
Description	A brief description about the port.

Button	Description
New	Displays fields in the Port section that you can use to add a port.
Edit	Displays fields in the Port section with port information. You can change the port details in the port mode.
Delete	Deletes the selected configured port.
Commit	Saves the port details. **Note:** The section displays the **Save** button only when you click **Add** or **Edit** in the Port section.
Cancel	Cancels the current operation of creating or editing an access profile and hides the fields where you add or modify the port information. **Note:** The section displays the **Cancel** button only when you click **Add** or **Edit** 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.

Field	Description
IP	The IP address of System Manager.
FQDN	FQDN of System Manager.
Virtual IP	The virtual IP address of System Manager.
Virtual FQDN	The virtual FQDN of System Manager.
isPrimary	The option to indicate if the element is primary or secondary.

Assign elements

Name	Description
Name	The name of the element.
Type	The type of the application to which the element belongs.
Description	A brief description about the element.

Button	Description
Assign elements	Displays the Assign elements page that you use to assign an element to another element.
Unassign elements	Removes an assigned element.

Button	Description
Commit	Creates or modifies an element by saving the information to the database. **Note:** The system displays the button only when you click **Add** or **Edit** on the Manage Elements page.
Cancel	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.

Field	Description
Login	The name in the **Trusted Server Name** field of the Trusted Servers page on the Messaging server.
Password	The password as given in the **Password** field of the Trusted Servers page on the Messaging server.
Confirm Password	The password that you retype for confirmation.
Messaging Type	The type of the Messaging server. The following types are supported: • **MM**: Modular Messaging • **CMM**: Communication Manager Messaging • **AURAMESSAGING**: Avaya Aura® Messaging
Version	The version of Messaging. Supported versions are 5.0 and later.

Table continues…

Field	Description
Secured LDAP Connection	An option to use the secure LDAP connection. To use the nonsecure LDAP connection, you must clear the check box.
Port	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.
Location	The location of the element.

Chapter 5: Managing security

Extended Security hardening

Using security hardening feature, you can enable different security profiles for Session Manager.

Session Manager supports Standard and Hardened security profiles. Each profile has specific security attributes. The following table describes security attributes for Standard and Hardened profile:

Security attribute	Standard	Hardened
VM Configuration Hardening[1]	Y	Y
Password management	Y	Y (more restrictive)
Login and session management	Y	Y (more restrictive)
System and application files hardening	Y	Y
Certificate management	Y	Y
Support TLS 1.2	Y	Y
FIPS 140-2 Compliance	-	Y
Multifactor Authentication (PIV and CAC support)	Through System Manager	Through System Manager
SELinux enabled	Enforced	Enforced
Audit management	Y	Y
AIDE (File Tampering Prevention)	-	Y

By default, Session Manager is configured with the Standard profile.

Warning:

- The Hardened profile removes certain software components that are not currently FIPS-compliant, including Cassandra. As a result, the Call History and Avaya Aura® Device Services features are not supported with the Hardened profile.
- After you configure Session Manager with Hardened profile, you cannot change the profile. To change the profile, you need to redeploy Session Manager.

[1] VMware ESXi VMX configuration file hardening applied as part of Solution Deployment Manager deployment.

Related links

Enabling the Hardened security profile on page 70
AIDE commands on page 71

Enabling the Hardened security profile

About this task

Use this procedure to enable hardened security profile for Session Manager.

Procedure

1. Log in to the Session Manager command line interface.
2. Run the following command:

   ```
   setSecurityPolicy
   ```

3. At the prompt, select the profile to use.

   ```
   Profiles
   ---------------
   1) Standard
   2) Hardened
   3) Custom

   Select profile:
   ```

4. To select Hardened profile, type `2` and press `Enter`.

   The system displays the following message:

   ```
   This profile will enable FIPS.  This will result in certain
   features being disabled and requires a reboot. Once the hardened
   profile is selected it cannot be reversed. The Session Manager
   would need to be reloaded. Consult documentation for further
   details.

   Do you want to continue? [yes/no]:
   ```

5. At the prompt, type `y` and press `Enter`.

   The Session Manager reboots for changes to take effect.

   Note:

   When you run the **`setSecurityPolicy`** command, you also select the boot password. You must log in to the VMware or KVM console and enter the boot password after the Session Manager restarts.

Related links

Extended Security hardening on page 69

AIDE commands

This section provides information about Advanced Intrusion Detection Environment (AIDE) commands used for updating or creating AIDE database and running an on-demand AIDE report.

aideDBUpdate

This command creates or updates the AIDE database. If the AIDE database already exists, a report is generated prior to refreshing the database.

aideCheck

This command generates the AIDE report and stores the output in the `/var/log/aide/aide_output.log` or `/var/log/messages`. AIDE is configured to generate a report once a day. The user does not have permission to configure the AIDE.

setSecurityPolicy

This command is used to enable or disable AIDE. AIDE can be enabled in the hardened mode and can be turned on through the custom mode.

Related links

Extended Security hardening on page 69

Trust management

The Trust Management module provides certificates to ensure secure communication between elements. Trust Management provides Identity and Trusted (root) certificates to establish mutually authenticated TLS sessions.

Using the Trust Management service, you can perform the following operations for an application instance:

- View installed Trusted and Identity certificates on the Session Manager server.
- Add or remove Trusted certificates on the Session Manager server.
- Replace or renew Identity Certificates on the Session Manager server.

Certificate management

Session Manager uses five unique certificates:

- WebSphere
- SAL Agent
- Management

- SIP
- HTTPS

SIP and HTTPS are the most important because these certificates communicate with outside entities such as Communication Manager and endpoints.

Note:

Session Manager can enforce certificate validation for SIP endpoints communication. Session Manager, establishes communication if the endpoint presents a valid and trusted certificate.

Any changes to these interfaces can cause major service interruptions. *Be very careful when changing these certificates.* The near end and far end use the certificates to trust each other. Each side presents its identity certificate during TLS negotiation. If one side does not trust the identity certificate of the other side, the connection fails. For an entity to trust another certificate, the entity must contain the root CA certificate from the CA that issued the identity certificate. Examples of CAs are VeriSign, Symantec, System Manager, and Avaya's SIP Product CA.

The root CA certificate must be stored in the entity's trusted list, also known as a trust store. To change the SIP or HTTPS identity certificate of a Session Manager, each far-end entity must contain the new root CA certificate in its trusted list. *You must add the new root CA certificate to the trusted list of the far end before changing the identity certificates.*

To handle certificates for a new installation, do one of the following:

- Use the new ID certificates issued by System Manager. This is the default setting.
- Use the ID certificates issued by a third party.

Related links

Certificates issued by System Manager on page 72
Certificates issued by a third party on page 84

Certificates issued by System Manager

System Manager can act as a certificate authority similar to VeriSign and Symantec. Many adopters, such as Communication Manager, Session Manager, and Presence, already use certificates issued by System Manager.

For fresh installations, all Identity Certificates, including SIP and HTTPS, are issued by the System Manager CA. You must install the System Manager trusted root certificates on endpoints that communicate with Session Manager over TLS for the endpoints to trust the Session Manager identity certificate.

Use this checklist for using the Identity Certificates issued by the System Manager.

#	Action	Link	✔
1	Export the System Manager CA.	Exporting the System Manager CA on page 73.	
2	Add the Root Certificate of the System Manager to Communication Manager.	Adding the System Manager CA to Communication Manager on page 73.	
3	Add System Manager Root Certificate to 96xx phones.	Adding the System Manager Root Certificate to 96XX phones on page 74.	
4	Add the System Manager Root Certificate to any other SIP connections, such as CS1K and Radvision.		
5	Replace the Session Manager SIP and HTTP Identity Certificates. **Note:** You must perform this step for all Session Manager and Branch Session Manager servers.	Installing Enhanced Validation Certificates on Session Manager on page 75.	
6	Remove the SIP CA Root Certificate from all trust lists, such as Communication Manager and phones.	Other Session Manager servers administered under the same System Manager will already trust the new Identity Certificate. Removing trusted certificates on page 76.	

Exporting the System Manager CA

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Security** > **Certificates** > **Authority**.
2. On the main page, click **Download pem file**.
3. Save the file.

Note:

To avoid HTTP download issues, save the file with the `.txt` extension.

Adding System Manager CA to Communication Manager

When you configure the Session Manager's SIP Identity Certificate to use System Manager as the CA, links to Communication Manager will go down because the Communication Manager will not trust the System Manager CA. Use this procedure to make Communication Manager trust the System Manager CA certificate.

Procedure

1. Verify you can access the System Manager CA certificate.
2. Log in to the Communication Manager server web interface.
3. Click **Administration** and select **Service (Maintenance)**.
4. In the left menu, under **Miscellaneous**, click **Download Files**.
5. Select **File(s) to download from the machine I'm using to connect to the server**.
6. Click **Browse**.
7. Select the System Manager CA certificate you want to download and click **Open**.
8. Click **Download**.
9. In the left menu, under **Security**, click **Trusted Certificates**.
10. Click **Add**.
11. Enter the name of the downloaded System Manager CA certificate.

    Note:

    You need to enter the full name of the file with extension.
12. Click **Open**.
13. Select the Communication Manager check box.
14. Click **Add**.
15. Restart Communication Manager.

    Warning:

    Select **Delayed Shutdown** and **Restart server after shutdown**. Restarting the Communication Manager server stops the SMI server you are currently using. You will be unable to access the Web pages until the server restarts.

Adding System Manager's Root Certificate to 96xx Phones

This procedure describes how to make phones trust the System Manager CA certificate.

About this task

Important:

To avoid a service outage, perform this procedure before switching Session Manager to certificates issued by System Manager.

Procedure

1. Copy the file to the file server that the 96xx phones are using.
2. On the file server, edit the file `46xxsettings.txt`.
3. **(Optional)** To enforce certificate validation for SIP endpoints, in the file, set **tlssrvid** as `1`.

4. In the file, set the **TRUSTCERTS** option to include the System Manager CA certificate.

   For example:

   ```
   SET TRUSTCERTS "smgr.txt, av_sipca_pem_2027.txt"
   ```

5. Reboot all phones.

   After rebooting, the phones download the System Manager root CA and are ready for replacing the SIP identity certificate of the Session Manager.

Installing Enhanced Validation Certificates for Session Manager

By default, 96xx phones perform enhanced validation of certificates. To make use of these certificates, you need to populate the **Common Name** and **Subject Alternate Name** of the certificate. You need to perform this procedure for all Session Manager servers and Branch Session Manager servers.

Important:

The 96xx phones need to trust the System Manager Root Certificate before you replace an SIP or HTTP certificates. Failure to do so results in the loss of communication with the phones.

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Elements**.
2. Select the appropriate Session Manager from the list and click **More Actions**.
3. Select **Configure Identity Certificates** from the drop-down menu.
4. On the Identity Certificates page, select either **Security Module SIP** or the name associated with **Common Name** security module.
5. Click **Replace**.
6. On the Replace Identity Certificate page, select **Replace this Certificate with Internal CA Signed Certificate**.
7. Select the **Common Name (CN)** check box and enter the host name or IP address of the Security Module.

   The address is the same as the SIP Entity address.

8. Select **RSA** for the **Key Algorithm**.
9. Select **2048** or **4096** as the **Key Size**.
10. Select the **DNS Name** check box and enter the SIP domain.

    You can enter multiple SIP domains using commas (no spaces), such as `avaya.com,company.com,xyz.com`.

11. Click **Commit**.
12. On the Identity Certificates page, select **Security Module HTTP**.

Note:

You must mention IPv6 and IPv4 address in SAN field in HTTP and SIP security certificate when TLSSRVRID is set to 1 on 96X1 phones.

13. Click **Replace**.
14. On the Replace Identity Certificate page, select **Replace this Certificate with Internal CA Signed Certificate**.
15. Select the **Common Name (CN)** check box and enter the IP address of the Security Module.

    The address is the same as the SIP Entity address.
16. Select **RSA** for the **Key Algorithm**.
17. Select **2048** or **4096** as the **Key Size**.
18. Select the **DNS Name** check box and enter the SIP domain.

    You can enter multiple SIP domains using commas (no spaces), such as `abc.com,company.com,xyz.com`.
19. Click **Commit**.
20. Restart all phones.

    After rebooting, the phones download the System Manager Root CA and will be able to communicate with the Session Manager.

Removing trusted certificates

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Elements**.
2. Select a Session Manager instance.
3. Click **More Actions** > **Configure Trusted Certificates**.
4. Select the certificates you want to remove, then click **Remove**.

   The system removes the certificates from the list of trusted certificates in the Session Manager instance.

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 left 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
Username	The name of the certificate holder.
Serial Number	The serial number that identifies the certificate.
Issuer DN	The distinguishing name of the certificate issuer.
Subject DN	The distinguishing name of the certificate holder.
Subject Alt Name	The alternate name of the certificate holder.
Revoked	The option to indicate whether a certificate is revoked.
Revocation Date	The date when the certificate was revoked. The field remains blank if the certificate is not in revoked state.
Revocation Reason	The reason for certificate revocation. The field remains blank if the certificate is not in revoked state.
Valid From	The date and time from when the certificate is valid.
Valid To	The date and time till the certificate is valid.

Button	Description
Done	Closes the View Certificate Detail page and displays the Manage Certificate Revocation page.

Manage Certificate Revocation field descriptions

Name	Description
Select radio button	The option to select a certificate.
Serial Number	The serial number that identifies the certificate.
Issuer DN	The distinguishing name of the certificate issuer.
Valid From	The date and time from when the certificate is valid.
Valid To	The date and time till the certificate is valid.
Subject DN	The distinguishing name of the certificate holder.
Revoked	The option to indicate whether a certificate is revoked.
Last Updated By	The name of the user who last updated or edited the certificate or both.
Revocation Date	The date when the certificate was revoked. The field remains blank if the certificate is not in revoked state.

Table continues…

Name	Description
Revocation Reason	The reason for certificate revocation. The field remains blank if the certificate is not in revoked state.

Button	Description
View Certificate	Displays all details of the selected certificate.
Revoke Certificate	Displays the option to revoke the selected certificate.
Unrevoke Certificate	Displays the option to unrevoke the selected certificate.
Refresh	Refreshes the certificate information in the table.
Filter: Enable	Displays the fields under select columns that you can use to set filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Clear	Clears the filter criteria.
Filter: Apply	Filters certificates based on the filter criteria.
Select: None	Clears the selections.
Previous	Displays the certificates in the previous page. This button is unavailable when you are on the first page.
Next	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 left 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
Serial Number	The serial number that identifies the certificate.
Subject DN	The distinguishing name of the certificate holder.
Valid From	The date and time from when the certificate is valid.
Valid To	The date and time till the certificate is valid.
Revocation Reason	The reason to revoke the certificate.

Button	Description
Revoke	Saves the certificate revocation reason and revokes the certificate.
Cancel	Cancels the certificate revocation and displays the Manage Certificate Revocation page.

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 unrevoke a certificate issued by System Manager as a certificate authority.

Note:

System Manager as a certificate authority does not support Delta CRLs and also the Avaya Aura® elements 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 left 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 left 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**.

Schedule CRL Download field descriptions

Name	Description
Job Details	Expands and collapses the **Job Details** section.
Job Frequency	Expands and collapses the **Job Frequency** section.
Configure CRL Distribution Point	Expands and collapses the **Configure CRL Distribution Point** section.
Expand All	If collapsed, expands all the sections.
Collapse All	If expanded, collapses all the sections.

Job Details

Name	Description
Job Name	The name of the download job.

Job Frequency

Name	Description
Task Time	Options to select the date, time, and time zone.
Recurrence	Options to set the recurrence of the download job.
Range	Options to set the date range for the end of the download job.

Configure CRL Distribution Point

Name	Description
CRL Distribution Point	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
Add	Validates and adds the entered CRL distribution point.
Show	Shows the selected number of CRL distribution points.
Previous	Displays the CRL distribution points on the previous page. This button is unavailable on the first page.
Next	Displays the CRL distribution points on the next page. This button is unavailable on the last page.
Commit	Creates the CRL download job and displays the CRL Download Configuration page.
Cancel	Displays the CRL Download Configuration page with all the details of the download job.

Deleting a CRL download job

Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the left 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 left 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
Select check box	The option to select a download job.
Job Name	The name of 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.
Job State	The current state of the download job.
Frequency	The frequency of the download job.
Scheduled By	The name of the user who scheduled the download job.

Button	Description
Add	Displays the Schedule CRL Download page to create a new download job.
Delete	Displays the Confirm Job Delete dialog box to confirm the deletion of the download job.
View	Displays the CRL Download Job Details page with all the details of the download job.
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. 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.
Revocation Type	The option to select the certificate revocation type. This option cannot be changed if **Certificate Revocation Validation** is set to **NONE**. **Note:** Only System Manager Release 7.1 and later supports **OCSP**. Other elements of Avaya Aura® Suite do not support **OCSP**. Therefore, it is recommended to not change the **Revocation Type** setting to **OCSP**.
Revocation Type Preference	The option to select the certificate revocation type. This option can be edited only if **Revocation Type** is set to **BOTH**.
Check method	The Option to select the checking method for the certificate. This Option cannot be changed if **Certificate Revocation Validation** is set to **NONE**.

SMGR
Cert based authentication

Name	Description
For System Manager User Interface	The option to enable or disable certificate-based authentication for the System Manager user interface.
For Other TLS Ports	The option to enable or disable certificate-based authentication for other TLS ports.

Button	Description
Commit	Saves and commits any changes made in the security configuration with an automatic JBoss restart.

Table continues…

Button	Description
Cancel	Cancels any changes made and reverts the security configuration settings to the last saved setting.

Certificates issued by a third party

The use of third party certificates is optional. Third party certificates are not required.

A third party CA can be a commercial vendor such as VeriSign and Symantec, or an enterprise-run CA that is maintained by the customer's IT department. You can create third party certificates using openssl or open source tools such as EJBCA (http://www.ejbca.org).

Use this checklist for using third party Identity Certificates.

#	Action	Link	✔
1	Add the third party Root Certificate to Communication Manager. Repeat this step for each Communication Manager that is connected to the Session Manager.	Adding a third party Root Certificate to Communication Manager on page 84.	
2	Add the third party Root Certificate CA to 96xx phones.	Adding a third party root certificate CA to 96xx phones on page 85.	
3	Add the third party Root Certificate CA to the trusted list for any other adjunct device that uses TLS to connect to Session Manager through SIP.	For example, Avaya Voice Portal and Meeting Exchange.	
4	Replace the Session Manager SIP and HTTP Identity Certificates.	Installing third party certificates on Session Manager on page 86.	
5	Add the third party certificate to the trusted list.	Adding trusted certificates on page 87.	

Adding a third party CA to Communication Manager

Configure Communication Manager to trust a third party root CA.

When you replace the SIP CA with the third party certificate, all Communication Manager TLS connections will go down.

Perform this procedure for each Communication Manager that is connected to the Session Manager.

Procedure

1. Verify you can access the third party root CA certificate.
2. Log in to the Communication Manager server web interface.
3. Click **Administration** and select **Service (Maintenance)**.

4. In the left menu, under **Miscellaneous**, click **Download Files**.
5. Select **File(s) to download from the machine I'm using to connect to the server**.
6. Click **Browse**.
7. Select the third party CA certificate you want to download and click **Open**.
8. Click **Download**.
9. In the left menu, under **Security**, click **Trusted Certificates**.
10. Click **Add**.
11. Enter the name of the downloaded third party CA certificate.

    Note:

    You only need to enter the name of the file.
12. Click **Open**.
13. Select the Communication Manager check box.
14. Click **Add**.
15. Restart Communication Manager.

    Warning:

    Select **Delayed Shutdown** and **Restart server after shutdown**. Restarting the Communication Manager server stops the SMI server you are currently using. You will be unable to access the Web pages until the server restarts.
16. Repeat this procedure for each Communication Manager connected to the Session Manager.

Adding a third party Root Certificate to 96xx Phones

About this task

This procedure describes how to make phones trust a third party Root Certificate CA.

Important:

To avoid a service outage, perform this procedure before switching the Session Manager to certificates issued by System Manager.

Procedure

1. Copy the third party root certificate file to the file server that the 96xx phones are using.
2. On the file server, edit the file `46xxsettings.txt`.
3. In the file, set the **TRUSTCERTS** option to include the third party CA certificate.

   For example:

   ```
   SET TRUSTCERTS "Third_Party_CA.txt, av_sipca_pem_2027.txt"
   ```
4. Reboot all the phones.

After rebooting, the phones download the System Manager root CA and are ready for replacing the SIP identity certificate of the Session Manager.

Installing third party certificates on Session Manager

This procedure describes how to install a third party certificate for SIP and HTTP on Session Manager.

When the certificate changes to the third party certificate, each SIP Entity must trust the third party CA.

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Elements**.
2. Select the appropriate Session Manager from the list and click **More Actions**.
3. Select **Configure Identity Certificates** from the drop-down menu.
4. Install the SIP third party certificate:
    a. On the **Identity Certificates** page, select **Security Module SIP**, or the name associated with **Common Name** security module.
    b. Click **Replace**.
    c. On the **Replace Identity Certificate** page, select **Import third party PKCS#12 file**.
    d. When the `Please select a file` prompt is displayed, browse for the third party signed certificate and select the certificate file.
    e. Enter the password in the **Password** field.
    f. Click **Retrieve Certificate**. The certificate details section displays the details of the certificate.
    g. Click **Commit**.
5. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Elements**.
6. Select the appropriate Session Manager from the list and click **More Actions**.
7. Select **Configure Identity Certificates** from the drop-down menu.
8. Install the HTTP third party certificate:
    a. On the Identity Certificates page, select **Security Module HTTP**.
    b. Click **Replace**.
    c. On the Replace Identity Certificate page, select **Import third party PKCS#12 file**.
    d. When the `Please select a file` prompt is displayed, browse for the third party signed certificate and select the certificate file.
    e. Enter the password in the **Password** field.

f. Click **Retrieve Certificate**.

The certificate details section displays the details of the certificate.

g. Click **Commit**.

Adding trusted certificates

About this task

You can import a trusted certificate:

- from a file.
- by copying the contents of a PEM file.
- from a list of an existing certificates.
- from a remote location using a TLS connection.

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Elements**.
2. Select a Session Manager instance.
3. Click **More Actions** > **Configure Trusted Certificates**.
4. On the Trusted Certificates page, click **Add**.
5. To import a certificate from a file:
   a. Click **Import from file**.
   b. Click **Browse** and locate the file.
   c. Click **Retrieve Certificate**.
   d. Click **Commit**.
6. To import a certificate in the PEM format:
   a. Select **Import as PEM Certificate**.
   b. Locate the PEM certificate.
   c. Open the certificate using Notepad.
   d. Copy the entire contents of the file. You must include the start and end tags: `-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE----`.
   e. Paste the contents of the file in the box provided at the bottom of the page.
   f. Click **Commit**.
7. To import certificates from existing certificates:
   a. Click **Import from existing**.
   b. Select the certificate from the Global Trusted Certificate section.
   c. Click **Commit**.

8. To import certificates using TLS:
    a. Click **Import using TLS**.
    b. Enter the IP Address of the location in the **IP Address** field.
    c. Enter the port of the location in the **Port** field.
    d. Click **Retrieve Certificate**.
    e. Click **Commit**.

Demo certificates

Previously, Session Manager was shipped with demo certificates issued by the SIP CA to simplify TLS connection setup. Demo certificates are non-unique identity certificates issued by the Avaya SIP Product Certificate Authority. Demo certificates are very insecure and do not meet current NIST standards (SHA256 and 2048 bit keys).

Session Manager no longer uses or supports default demo certificates for new installations. Fresh installations of Session Manager result in SIP and HTTP certificates signed by System Manager. In most cases, existing TLS connections will break until the System Manager CA is installed on the far end. You can reinstall the demo certificates to quickly restore a previously working environment.

For upgrades, Session Manager preserves the previous certificates. If a demo certificate was in use in the previous release, the certificate is preserved through the upgrade.

Determining whether a demo certificate is being used

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Inventory** > **Manage Elements**.
2. Select the Session Manager instance.
3. Click **More Actions** > **Configure Identity Certificates**.
4. Select the **securitymodule**.
5. Check the **Issuer Name**.

    If the **Issuer Name** field contains **CN=SIP Product Certificate Authority, OU=SIP Product Certificate Authority, O=Avaya Inc., C=US**, you have a demo identity certificate.

Installing demo certificates

This procedure reinstalls demo certificates to quickly restore a previously working environment.

About this task

Important:

Avaya does not recommend installing demo certificates. Demo certificates are not secure. Use the System Manager certificates or third party certificates instead.

Procedure

1. Log in to the Session Manager server using the customer login.
2. Enter the command `initTM -d` or `initTM --demo` to install the demo certificates.

   The command displays `Trust Management Initialization started.`, followed by a WARNING message.
3. At the `Do you want to continue? (y/n)` prompt, enter `y`.

   The script installs the demo certificates.

Trusted Certificates

Viewing trusted certificates

Before you begin

You must have permission to view the certificates of an application instance.

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Elements**.
2. Select a Session Manager instance.
3. Click **More Actions** > **Configure Trusted Certificates**.
4. On the Trusted Certificates page, click **View**.

   The View Trust Certificate page displays the details of the selected certificate.

View Trust Certificate field descriptions

Name	Description
Subject Details	The details of the certificate holder.
Valid From	The date and time from which the certificate is valid.
Valid To	The date and time until which the certificate is valid.
Key Size	The size of the key in bits for encryption.
Issuer Name	The name of the issuer of the certificate.
Certificate Fingerprint	The fingerprint that authenticates the entire certificate.

Table continues…

Name	Description
Key Fingerprint	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.
Serial Number	The serial number of the certificate.
Basic Constraints	The extension identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate.
Key Usage Extension	The extension defines the purpose of the key contained in the certificate such as Digital Signature, Key Cert Sign, CRL Sign.
Extended Key Usage	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
Done	Closes the page and returns to the Trusted Certificates page.

Adding trusted certificates

About this task

You can import a trusted certificate:

- from a file.
- by copying the contents of a PEM file.
- from a list of an existing certificates.
- from a remote location using a TLS connection.

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Elements**.
2. Select a Session Manager instance.
3. Click **More Actions** > **Configure Trusted Certificates**.
4. On the Trusted Certificates page, click **Add**.
5. To import a certificate from a file:
    a. Click **Import from file**.
    b. Click **Browse** and locate the file.
    c. Click **Retrieve Certificate**.
    d. Click **Commit**.
6. To import a certificate in the PEM format:
    a. Select **Import as PEM Certificate**.

b. Locate the PEM certificate.
c. Open the certificate using Notepad.
d. Copy the entire contents of the file. You must include the start and end tags: `-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE----`.
e. Paste the contents of the file in the box provided at the bottom of the page.
f. Click **Commit**.

7. To import certificates from existing certificates:
   a. Click **Import from existing**.
   b. Select the certificate from the Global Trusted Certificate section.
   c. Click **Commit**.
8. To import certificates using TLS:
   a. Click **Import using TLS**.
   b. Enter the IP Address of the location in the **IP Address** field.
   c. Enter the port of the location in the **Port** field.
   d. Click **Retrieve Certificate**.
   e. Click **Commit**.

Add Trusted Certificate field descriptions

Name	Description
Store Type	The store type that is based on inbound and outbound connection.
Import from existing	The option to import a certificate from the existing imported certificates.
Import from file	The option to import a certificate from a file. The file format is `.cer` or `.crt`.
Import as PEM Certificate	The option to import a certificate in the PEM format.
Import using TLS	The option to import a certificate if the element requires to contact the certificate provider to obtain the certificate.

Global Trusted Certificate:

The page displays the following fields when you select the **Import from existing** option.

Name	Description
Certificate Name	The fully qualified domain name of the certificate.
Subject Name	The fully qualified domain name of the certificate holder.

Table continues…

Name	Description
Valid To	The date until which the certificate is valid.
Filter: Enable	Displays fields in select columns where you can set the filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Clear	Clears the filter criteria.
Filter: Apply	Filters certificates based on the filter criteria.
Select: All	Selects all the certificates in the table.
Select: None	Clears all the check box selections.
Refresh	Refreshes the certificates information.

The page displays the following fields when you select **Import from file**.

Name/Button	Description
Please select a file	The file that contains the certificates.
Browse	Displays the choose file dialog box where you can choose the file from which you want to import the certificates.
Retrieve Certificate	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
Subject Details	The details of the certificate holder.
Valid From	The date and time from when the certificate is valid.
Valid To	The date and time until when the certificate is valid.
Key Size	The size of the key in bits for encryption.
Issuer Name	The name of the issuer of the certificate.
Certificate Fingerprint	The fingerprint that authenticates the entire certificate.
Key Fingerprint	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.
CA Certificate	The field that specifies whether the certificate is a CA certificate.

The page displays these fields when you select the **Import using TLS** option.

Field/Button	Description
IP Address	The IP address of the certificate provider that is to be contacted for retrieving the certificate.
Port	The port of the server to be used for obtaining the certificate.
Retrieve Certificate	Retrieves the certificate and displays the details of the certificate in the Certificate Details section.

Removing trusted certificates

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Elements**.
2. Select a Session Manager instance.
3. Click **More Actions** > **Configure Trusted Certificates**.
4. Select the certificates you want to remove, then click **Remove**.

   The system removes the certificates from the list of trusted certificates in the Session Manager instance.

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
Certificate Name	The common name of the certificate.
Store Type	The type of the store associated with the certificate.
Subject Name	The name of the certificate holder.

Button	Description
Delete	Deletes the trusted certificate from the corresponding store.
Cancel	Cancels the delete operation and takes you back to the Add Trusted Certificate page.

Exporting a Session Manager Certificate

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Elements**.
2. Select a Session Manager instance.
3. Click **More Actions** > **Configure Trusted Certificates**.
4. Select the appropriate certificate to export.

5. Click **Export**.

Exporting the System Manager root CA certificate

About this task

When Session Manager uses Identity Certificates signed by the System Manager CA , Session Manager must obtain the System Manager root CA certificate to add to the Trust Store of peer devices. Peer devices, such as Communication Manager, SIP Endpoint, and other SIP devices, connect to Session Manager. Use this procedure to obtain the System Manager root CA certificate.

Procedure

1. On System Manager Web Console, go to **Services** > **Security** > **Certificates** > **Authority** > **CA functions** > **CA Structure & CRLs**.
2. Click **Download PEM file** to save the PEM file to the system.

Note:

To avoid HTTP download issues, save the file with a `.txt` extension.

Peer certificate validation

All Session Manager TLS services support validation of peer Identity Certificates consisting of a SHA2 signature and a public key of 2048 bits.

Session Manager verifies whether the peer identity certificate can be traced to a trusted root CA certificate. The root CA certificate must reside in the service Trust Store.

Certificate validations for a System Manager connection

For a TLS connection between Session Manager and System Manager, the system validates the identity certificate using standard path validation, which complies with the *RFC5280 section Certificate Path Validation*. In addition , the system performs hostname validation.

The System Manager identity certificate must have a **Subject Alternate Name** extension with the following DNS name entries:

- The first DNS entry must contain the actual System Manager hostname, for instance, systemmanager-1.example.com.
- The second DNS entry must contain the active.smgr.com value. The hostname active.smgr.com is used because Data Replication) uses this hostname for certificate validation.

Certificate validation for SIP TLS connections

Trusted SIP TLS connections

For trusted SIP TLS connections such as SIP entities, Session Manager applies the following validations:

- Mutual TLS authentication: During TLS handshake, the SIP entity and Session Manager validate certificates for each other and perform mutual TLS authentication.

- Additional validation of the SIP entity identity certificate: If the mutual TLS authentication is successful, further validation is performed using the credential name or the far end IP address of the SIP entity identity certificate. The **Credential name** field of the SIP Entity page is used for further validation.
  - If the credential name (CN) string is empty, the connection is accepted.
  - If the credential name string is not empty, the system searches the credential name and IP address of the SIP entity in the identity certificate provided by the SIP entity. The system looks for the following parameters:
    - CN value from the Subject
    - subjectAltNamedNSName
    - subjectAltName.uniformResourceIdentifier. For IP address comparison, the IP address string is converted to SIP:W.X.Y.Z before comparison. W.X.Y.Z is the remote socket IPV4 address. In this scenario, case insensitive search is performed.

Untrusted SIP TLS connections

For untrusted SIP TLS connections such as SIP endpoints, Session Manager validation depends on the version and its configuration:

- For Session Manager 7.0.0 and earlier, the **Enable TLS Endpoint Certificate Validation** setting on the Session Manager Administration page controls the validation:
  - If the **Enable TLS Endpoint Certificate Validation** check box is selected, Session Manager requests a client certificate through the **TLS Certificate Request** message:
    - If the client provides an identity certificate, its certificate chain must be traced to a trusted CA certificate to establish the connection to
    - If the client does not provide a certificate, the connection is allowed.
  - If the **Enable TLS Endpoint Certificate Validation** check box is cleared, no TLS client authentication is performed.
- For Session Manager 7.0.1 and later, the **TLS Endpoint Certificate Validation** setting on the Session Manager Administration page controls the validation performed on the client certificate. Session Manager requests a client certificate through the **TLS Certificate Request** message, and its validation depends on the configuration value:
  - If **TLS Endpoint Certificate Validation** is set to **Required**.
    - If the client provides a certificate, its certificate chain must be traced to a trusted CA certificate in order to connect.
    - If the client does not provide a certificate, the connection is refused.
  - If the **TLS Endpoint Certificate Validation** field is set to **Optional**:
    - If the client provides a certificate, its certificate chain must be traced to a trusted CA certificate in order to connect.
    - If the client does not provide a certificate, the connection is allowed.
  - If the **TLS Endpoint Certificate Validation** field is set to **None**:
    - If the client provides a certificate, its certificate is saved for reporting but not validated. The connection is allowed.

- If the client does not provide a certificate, the connection is allowed.

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.

Field	Description
Store Description	The purpose of the trusted certificate.
Store Type	The type of the store associated with the certificate.
Subject Name	The name of the certificate holder.

Button	Description
View	Opens the View Trust Certificate page. Use this page to view the certificate details.
Add	Opens the Adds Trusted Certificate page. Use this page to import certificates from the selected resource.
Remove	Removes the selected certificate from the list of trusted certificates.
Export	Exports the selected certificate from the list of trusted certificates to a PEM formatted file.

Identity Certificates

Multiple Identity Certificates exist on Session Manager. This section describes the following Identity Certificates:

- SIP
- HTTPS (PPM_

Important:

In Session Manager, the demo certificates are no longer installed by default. A fresh installation of Session Manager causes the SIP and HTTP certificates to be signed by System Manager. In most cases, existing TLS connections will break until the System Manager CA is installed on the far end.

Identity Certificates field descriptions

Field	Description
Service Name	The name of the service that uses the identity certificate.
Common Name	The common name to identify the service.

Table continues…

Field	Description
Valid To	The date until which the certificate is valid.
Expired	Specifies whether the certificate is expired.
Service Description	A brief description about the service.

Button	Description
Replace	Opens the Replace Identity Certificate page. Use this page to replace a selected identity certificate with a new certificate.
Export	Exports the certificate that you select. The exported certificate is in the form of a PEM file.
Renew	Renews the certificate that you select. After you renew a certificate, the system automatically updates the **Valid To** column.

Viewing Identity Certificates

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Elements**.
2. Select a Session Manager instance.
3. Click **More Actions** > **Configure Identity Certificates**.
4. Click **View**.

Replacing a Session Manager Identity Certificate

Use this procedure to replace the Identity Certificate of a Session Manager.

Before you begin

Make sure you have the following:

- A certificate with the hostname as the Common Name (CN) that is signed by the third party certificate authority (CA). This certificate must be in PKCS#12 format.
- The third-party Root CA certificate.

Procedure

1. Add Root CA to the System Manager Trusted List.
2. Add Root CA to the Session Manager Trusted List.
3. Administer the SIP Identity Certificate.
4. Activate the new Identity Certificate.

Replace Identity Certificate field descriptions

Certificate Details

Name	Description
Subject Details	The certificate holder details.
Valid From	The date and time from when the certificate is valid.
Valid To	The date and time till the certificate is valid.
Key Size	The key size in bits for encryption. The default key size is 2048.
Issuer Name	The name of the certificate issuer.
Certificate Fingerprint	The fingerprint that authenticates the certificate.
Subject Alternative Name	An alternative name of the certificate holder.
Serial Number	The serial number of the certificate.
Basic Constraints	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.
Key Usage Extension	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.
Extended Key Usage	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
Replace this Certificate with Internal CA Signed Certificate	The option to replace the current certificate with the internal CA signed certificate.
Import third party certificate	The option to replace the identity certificate with the PKCS #12 file that you imported from a third-party source.
Generate Certificate Signing Request (CSR) for third party certificate	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
Common Name (CN)	The common name of the certificate holder. You must select the check box to enter the name.

Table continues…

Name	Description
Key Algorithm	The algorithm used to generate the key for the certificate. The option is RSA. System Manager uses the SHA2 hash algorithm for generating certificates.
Key Size	The key size in bits for encryption. The options are: • **1028** • **2048** • **4096** **Note:** Session Manager Release 6.3.12 and later support 4096. Use 2048 as the key size.
Subject Alternative Name	An alternative name of the certificate holder. The options are: • **DNS Name**: The DNS IP address. • **IP Address**: The IP address. • **URI**: The URI address. **Note:** In **DNS Name**, **IP Address**, and **URI** fields, you can enter more than one value separated by a comma. Do not add spaces between comma-separated IP addresses and DNS names.

Button	Description
Commit	Replaces the current identity certificate with the selected certificate.
Generate CSR	Generates a third-party certificate signing request. When you select the **Generate Certificate Signing Request (CSR) for third party certificate** option, the system enables the **Generate CSR** button.
Cancel	Cancels the certificate replacement operation.

When you select **Import third party certificate**, the system displays the following fields.

Name	Description
Please select a file (PKCS #12 format)	The full path of the PKCS #12 file where you saved the certificate.
Password	The password to retrieve the certificate.

Button	Description
Retrieve Certificate	Retrieves the details of the imported certificate and displays them in the Certificate Details section.
Commit	Replaces the current identity certificate with the selected certificate.
Cancel	Cancels the certificate replacement operation.

Adding Root CA to the System Manager Trusted List

About this task

System Manager must trust the third-party certificate that the Session Manager uses.

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Elements**.
2. On the Manage Elements page, select **System Manager**.
3. Click **More Actions** > **Configure Trusted Certificates**.
4. Click **Add**.
5. On the Add Trusted Certificate page, select **Select Store Type to add trust certificate as All**.
6. If the Root CA is in PKCS#12 format:
   a. Select **Import from file**.
   b. Browse for the Root CA certificate using **Please select a file**.
   c. Click **Retrieve Certificate**.
7. If the Root CA is in PEM format, select **Import as PEM Certificate**.
8. Copy and paste the Root CA certificate contents in the space provided.
9. Click **Commit**.

Adding Root CA to the Session Manager Trusted List

For internal communications, Session Manager must trust the third party certificate.

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Elements**.
2. On the Manage Elements page, select **Session Manager**.
3. Click **More Actions** > **Configure Trusted Certificates**.
4. On the Trusted Certificate page, click **Add**.
5. On the Add Trusted Certificate page, select **Select Store Type to add trust certificate as All**.

6. If the Root CA is in PKCS#12 format:
    a. Select **Import from file**.
    b. Browse for the Root CA certificate using **Please select a file**.
    c. Click **Retrieve Certificate**.
7. If the Root CA is in PEM format, select **Import as PEM Certificate**.
8. Copy and paste the Root CA certificate contents in the space provided.
9. Click **Commit**.

Administering a SIP Identity Certificate

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Elements**.
2. Select a Session Manager instance.
3. Click **More Actions** > **Configure Identity Certificates**.
4. Select **securitymodule**.
5. Click **Replace**.
6. Choose one of the following options:
    - If you are replacing the Identity Certificate with an Internal CA Signed Certificate:
        a. Click **Replace this Certificate with Internal CA Signed Certificate**.
        b. Enter the common name, org unit, organization, and country information in the respective fields.
        c. Select the key size/type.
        d. Click **Commit**.
    - If you are replacing the Identity Certificate by importing a third party PCKS # 12 file:
        a. Click **Import third party PCKS # 12 file**.
        b. Enter the file name in the **Please select a file** field.
        c. Enter the password in the **Password** field.
        d. Click **Retrieve Certificate**.
        e. Click **Commit** to replace the certificate with the imported third-party certificate.

Activating a new Identity Certificate

To activate a new Identity Certificate, you reboot the Session Manager and restart the jboss service on System Manager.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager**.
2. Select a Session Manager instance.
3. Select **Shutdown System** > **Reboot**.
4. Click **Confirm**.
5. Login to the System Manager command line interface.
6. Enter the command `service jboss restart`.

Checklist for generating certificate signing request (CSR)

Session Managerdoes not provide a GUI to generate a CSR to replace Session Manager Identity Certificates. An alternate tool such as OpenSSL is used to generate the CSR.

This checklist describes the high level steps to replace Session Manager Identity Certificates with a CSR.

No.	Task	Description	Notes	✔
1	Generate a CSR and its corresponding private key using OpenSSL	Generate a CSR and its corresponding private key using OpenSSL or other adequate tool such as Microsoft Server. Ensure that the CSR contains correct certificate attributes	For more information, see CSR and Private Key generation through OpenSSL on page 103	
2	Get the Identity Certificate signed.	Send the CSR to the PKI administrator to get it signed by the third party CA. The result is a signed Identity Certificate.		
3	Bundle the Identity Certificates and private key into PKCS#12 container using OpenSSL.		For more information see Bundle Identity Certificate and Private Key in aPKCS #12 container on page 106	

Table continues…

No.	Task	Description	Notes	✔
4	Import the PKCS#12 certificate and private key into Session Manager.		For more information see Replacing an identity certificate by a third party CA issued certificate on page 101	

Generating CSR and Private Key through OpenSSL

About this task

Use this procedure to replace the Security Module SIP identity certificate. You can replace other identity certificates similarly.

Procedure

1. Log in to Session Manager CLI with `cust` credentials.
2. Copy and modify the default OpenSSL configuration file to a cust directory by typing: `cp /etc/pki/tls/openssl.cnf /home/cust/openssl_csr.cnf`.
3. Edit the configuration file by typing: `vi /home/cust/openssl_csr.cnf`.

   You must edit the configuration file to meet the certificate attributes required for each Identity Certificate.
4. Edit the following list of certificate attributes with the values assigned.
   - `default_md= sha256`
   - `req_extensions = v3_req # The extensions to add to a certificate request`
   - `keyUsage = nonRepudiation, digitalSignature, keyEncipherment, keyAgreement`
   - `extendedKeyUsage=serverAuth, clientAuth`
   - `subjectAltName= @alt_names`
   - `DNS.1 = example.com # The Session Manager SIP domain`
   - `DNS.2 = sip.example.com # Another Session Manager SIP domain`
   - `IP = 192.168.1.100 # The Session Manager SIP interface (eth1) IP address`
   - `URI.1 = sip:example.com # The Session Manager SIP domain preceded by the sip schema`
   - `URI.2 = sip:sip.example.com # Another Session Manager SIP domain preceded by the sip schema`

The following example shows a configuration file of Security Module SIP identity certificate that meets the Security Module SIP Identity Certificate attributes on page 107.

```
[ req ]
default_bits            = 2048
default_md              = sha256
default_keyfile         = privkey.pem
distinguished_name      = req_distinguished_name
attributes              = req_attributes
x509_extensions = v3_ca # The extentions to add to the self signed cert
…
# WARNING: ancient versions of Netscape crash on BMPStrings or UTF8Strings.
string_mask = utf8only

req_extensions = v3_req # The extensions to add to a certificate request

…
[ v3_req ]

# Extensions to add to a certificate request

basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment, keyAgreement
extendedKeyUsage=serverAuth, clientAuth
subjectAltName= @alt_names

[alt_names]
DNS.1 = example.com              # The Session Manager SIP domain
DNS.2 = sip.example.com          # Another Session Manager SIP domain
IP = 192.168.1.100               # The Session Manager SIP interface (eth1) IP
address
URI.1 = sip:example.com          # The Session Manager SIP domain preceded by the
sip schema
URI.2 = sip:sip.example.com      # Another Session Manager SIP domain preceded by
the sip schema
…
```

Note:

Some public CAs do not allow signing a CSR with a Subject Alternative Name extension entry of type URI and sip scheme, for instance URI=sip:sip.example.com. In such cases, use only the DNS type entry with the corresponding SIP Domain. In the above example, remove the lines that start with URI.1 and URI.2

5. Type `openssl req -out asm1.csr -new -newkey rsa:2048 -keyout asm1.key -config /home/cust/openssl_csr.cnf`.

   The following example shows the system output for this command:

```
$ openssl req -out asm1.csr -new -newkey rsa:2048 -keyout asm1.key -config /home/
cust/openssl_csr.cnf
Generating a 2048 bit RSA private key
....+++
.........................................+++
writing new private key to 'asm1.key'
Enter PEM pass phrase:     <<< Private key pass phrase
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
```

```
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:CO
Locality Name (eg, city) [Default City]:Thornton
Organization Name (eg, company) [Default Company Ltd]:My example company
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:asm1.example.com   <<<
Session Manager hostname
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

The system generates the CSR and private key. The generated CSR file is `asm1.csr` and the private key is `asm1.key`. The private key is protected with a pass phrase to be used at the prompt when the private key is generated. This pass phrase is used to create the PKCS#12 container.

The private key file must stay on the server always and must not be tampered with. If the private key is compromised, it could potentially decrypt TLS traffic or impersonate Session Manager.

6. To view and verify the attributes of the CSR file `asm1.csr`, type `openssl req -in asm1.csr -text`.

   The system displays the following output:

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=US, ST=CO, L=Thornton, O=My example company, OU=IT,
CN=asm1.example.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:f2:d7:35:5a:f9:f7:9f:5f:1e:9e:f5:e0:4f:…
                Exponent: 65537 (0x10001)
        Attributes:
        Requested Extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment, Key
Agreement
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Subject Alternative Name:
                DNS:example.com, DNS:sip.example.com, IP Address:192.168.1.100,
URI:sip:example.com, URI:sip:sip.example.com
    Signature Algorithm: sha256WithRSAEncryption
         1f:64:2a:92:89:ce:bd:ff:80:7a:c8:50:7b:f2:bd:80:57:ce:…
-----BEGIN CERTIFICATE REQUEST-----
MIIDWDCCAkACAQAwcjELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAkNPMREwDwYD…
-----END CERTIFICATE REQUEST-----
```

7. Send the CSR file `asm1.csr` to the PKI administrator to get signature of the third-party CA.

   The result is a signed identity certificate.

Bundling identity certificate and private key in a PKCS #12 container

About this task

Use this procedure to bundle the signed identity certificate and its corresponding private key into a PKCS#12 container using OpenSSL. PKCS#12 is the format required by System Manager to install the identity certificate on Session Manager.

Before you begin

- Generate CSR and a private key through OpenSSL.
- Ensure that you have a signed identity certificate file `asm1_signed.pem` and a private key `asm1.key`.
- Ensure that the identity certificate is in the PEM format. If it is in a different format, use OpenSSL to change the format to PEM.

Procedure

1. Copy the signed identity certificate file `asm1_signed.pem` from your system to the Session Manager and place it in the `/home/cust/` directory.
2. Log in to the Session Manager CLI as `cust`.
3. Run the **`openssl pkcs12 -export -out asm1.p12 -inkey asm1.key -in asm1_signed.pem`** command to generate the PKCS#12 file.

   The system displays the following messages:

   ```
   $ openssl pkcs12 -export -out asm1.p12 -inkey asm1.key -in asm1_signed.pem
   Enter pass phrase for asm1.key:
   Enter Export Password:
   Verifying - Enter Export Password:
   ```

4. Type the private key pass phrase obtained during the generation of the private key `asm1.key`.
5. Type `export password` to protect the PKCS#12 file.

   The password is used to install the identity certificate through System Manager.

   The system generates a PKCS#12 container file `asm1.p12`.
6. Download the file `asm1.p12` to the system.
7. To avoid tampering, type `rm /home/cust/asm1.key` to delete the private key from the Session Manager server.

Next steps

Replacing an Identity Certificate by a third party CA isued certificate.

Identity Certificates lifecycle

All certificates have a limited and valid lifetime. Identity Certificates signed by the root CA of System Manager are valid for two years after being installed. Session Manager auto renews these Identity Certificates 60 days before expiration. For Identity Certificates signed by a third-party CA, the PKI administrator must replace or renew them before expiration.

Session Manager notifies about certificate expiration by generating alarms. These alarms are sent when the auto renew process fails, or a third-party Identity Certificate is about to expire. The following alarms are generated by Session Manager:

- Critical alarm (OP_MMTC20050): if the certificate expires in less than 15 days
- Major alarm (OP_MMTC20049): if the certificate expires between 15 and 29 days
- Warning alarm (OP_MMTC20048): if the certificate expires between 30 and 60 days

For more information about alarms and the certificate expiration process, see *Troubleshooting Avaya Aura® Session Manager*.

SIP Identity Certificate attributes

Generate the Session Manager SIP Identity Certificate with the following X509v3 extensions and attributes.

Attribute	Value	Required?
Authority Information Access	*OCSP - URI:http://{ocsp-server}{:ocsp-port}{/ocsp-path}*	Optional
Authority Key Identifier	*hash*	Required[2]
CRL Distribution Points	*URI:http://{crl-server}{:crl-port}{/crl-path}* *URI:ldap://{crl-server}{:crl-port}{/crl-dn}*[3]	Recommended Recommended
Extended Key Usage	*id-kp-serverAuth = 1.3.6.1.5.5.7.3.2.1* *id-kp-clientAuth = 1.3.6.1.5.5.7.3.2.2* *id-kp-sipDomain = 1.3.6.1.5.5.7.3.20*	Required Optional[4] Contraindicated [5]
Key Usage	*digitalSignature* *nonRepudiation* *keyEncipherment* *dataEncipherment*	All values are Optional. [6]

Table continues…

[2] Authority key identifiers are required elements in end entity certificates to properly establish the trust chain.
[3] URLS and DNs that identify the location of CRLs in LDAP directories can be complex. Entities must be able to handle characters as defined by the LDAP URI specification in RFC 4516.
[4] Required if the same Identity Certificate is used when the server is acting as a client.
[5] Validation of the presence of the `id-kp-sipDomain` extended key usage as described in RFC 5924 is discouraged, as it limits use of the certificate to SIP only and forces certificate proliferation.
[6] Values may vary as specified in RFC 5280 and RFC 3279.

Attribute	Value	Required?
Subject	*CN={fqdn}*	Required
Subject Alternative Name	*IP:{ip}* *URI:sip:{domain}* *DNS:{domain}* *DNS:{fqdn}*	Optional Required [7] Required [8] Required
Subject Key Identifier	*hash*	Recommended
Validity	*validity period*	Required

HTTPS Identity Certificate attributes

Generate the Session Manager HTTPS Identity Certificate with the following X509v3 extensions and attributes.

Attribute	Value	Required?
Authority Information Access	*OCSP - URI:http://{ocsp-server}{:ocsp-port}{/ocsp-path}*	Optional
Authority Key Identifier	*hash*	Required[9]
CRL Distribution Points	*URI:http://{crl-server}{:crl-port}{/crl-path}* *URI:ldap://{crl-server}{:crl-port}{/crl-dn}*[10]	Recommended Recommended
Extended Key Usage	*id-kp-serverAuth = 1.3.6.1.5.5.7.3.2.1* *id-kp-clientAuth = 1.3.6.1.5.5.7.3.2.2*	Required Optional[11]
Key Usage	*digitalSignature* *nonRepudiation* *keyEncipherment* *dataEncipherment*	All values are Optional. [12]
Subject	*CN={fqdn}*	Required

Table continues…

[7] The SIP domain may not be known at install time, so the `URI:sip:{domain}` Subject Alternative Name value suggested by RFC 5922 is not likely to be present.
[8] See Footnote 6. Also, the 96xx endpoints require the SIP domain to be present in the **CN** or as a `DNS:{domain}` entry in the Subject Alternative Name field.
[9] Authority key identifiers are required elements in end entity certificates to properly establish the trust chain.
[10] URLS and DNs that identify the location of CRLs in LDAP directories can be complex. Entities must be able to handle characters as defined by the LDAP URI specification in RFC 4516.
[11] Required if the same Identity Certificate is used when the server is acting as a client.
[12] Values may vary as specified in RFC 5280 and RFC 3279.

Attribute	Value	Required?
Subject Alternative Name	*IP:{ip}* *DNS:{fqdn}*	Optional [13] Required
Subject Key Identifier	*hash*	Recommended
Validity	*validity period*	Required

Management, Postgres and SPIRIT identity certificates attributes

Generate the Management, Postgres or the SPIRIT identity certificates or all with the following **X509v3** extensions and attributes:

Attributes	Value	Required
Subject	*CN={session-manager-fqdn}*	Required
Validity	*validity period*	Required
Authority Key Identifier	*hash*	Required
Subject Key Identifier	*hash*	Recommended
Key Usage	*digitalSignature* *nonrepudiation* *keyEncipherment* *dataEncipherment* *keyAgreement*	Required Required Required Required Required
Extended Key Usage	*id-kp-serverAuth = 1.3.6.1.5.5.7.3.3.1* *id-kp-clientAuth = 1.3.6.1.5.5.7.3.3.2*	Required Required
Authority Information Access	*OCSP - URI:http://{ocsp-server}{:ocsp-port}{/ocsp-path}*	Optional
CRL Distribution Points	*URI:http://{crl-server}{:crl-port}{/crl-path}* *URI:ldap://{crl-server}{:crl-port}{/crl-dn}*	Recommended Recommended

Authority Key Identifiers are required elements in end entity certificates to accurately establish the trust chain. The URLs and DNs used to identify the location of CRLs in LDAP directories are complex. Therefore, entities configuring or consuming them must handle characters as defined by the LDAP URI specification in RFC 4516.

Trust management overview

Multiple Trust Stores exist on Session Manager. Every Trust Store contains a set of CA certificates trusted by a given service. The following table describes the CA certificates trusted by each type of Trust Store:

[13] For 96xx, 1XC SIP, and Avaya communicator SIP endpoints, PPM is defined as an IP address so PPM certificates must contain the `IP:{ip}` Subject Alternative Name entry when endpoints 96xx , 1XC SIP, and Avaya communicator SIP are part of the solution.

Store type	Purpose	Protocol	Notes
SECURITY_MODULE_HTTP	Validates client identity certificates on secure HTTP connections from SIP Endpoints such as Hardphones and Softphones. The endpoints use the HTTP connection for PPM protocol.	HTTPS	
SECURITY_MODULE_SIP	Validates identity certificates for SIP TLS connections between Session Manager and external devices such as Communication Manager, Avaya SBCE, and SIP Endpoints.	SIP	
WEBSPHERE	Used by the WebSphere SIP container to validate the identity certificate of the Security Module.	SIP	The store must contain the Security Module SIP identity certificate signed by the CA certificate. The store does not validate any identity certificate presented by an external TLS connection.
SAL_AGENT	Used by the Spirit Agent to validate the identity certificate of TODO.	HTTPS	
MGMT_JBOSS	Validates the identity certificates of System Manager for management such as RMI/JMX, and DRS replication.	JMX, RMI, HTTPS	

Restoring the default SIP Identity Certificate

Restore the default certificate issued by the SIP CA on the selected Session Manager. You can reinstall demo certificates to quickly restore a previously working environment.

Procedure

1. Log into the Session Manager CLI.
2. Enter the command `initTM --demo`.
3. At the warning message prompt, enter `y`.

   The message `Trust Management initialization completed successfully.` appears when the default certificate has installed.

Enforcing certificate validation for SIP endpoints

About this task

In some high-security environments, it might be necessary to validate whether a device or application being used has trusted credentials. Therefore, the TLS client must provide identity credentials issued by an authority that Session Manager trusts. The endpoint validation setting controls whether the client certificate must be validated.

Procedure

1. On the home page of the System Manager web console, in **Elements**, click **Session Manager** > **Global Settings**.
2. In the **TLS Endpoint Certificate Validation** field, click **Required**.

   When you select the **Required** option, communication occurs only if the endpoint presents a valid certificate trusted by Session Manager.
3. Click **Save**.

Chapter 6: Managing users

This chapter explains Session Manager user administration.

System Manager provides bulk importing of user profiles and user attributes. For more information, see Bulk import and export on page 175.

For information on the Multi Tenancy feature, see *Administering Avaya Aura® System Manager*.

Note:

While administering a user, the secondary Session Manager should not be hosted on the VMware platform unless the primary Session Manager is also hosted on the VMware platform.

When you register a SIP endpoint of a user to the Avaya core, you must assign a communication profile to the user. The communication profile contains a Communication Manager endpoint profile and a Session Manager profile.

The Communication Manager profile associates the user with a station on a Communication Manager that is in the Avaya core network.

The Session Manager profile assigns:

- the primary Session Manager
- the secondary Session Manager
- relevant application sequences
- the survivability server

For application sequencing to Communication Manager, each application in the application sequence must reference the same Communication Manager as the Communication Manager endpoint profile.

For survivability configuration, if a Branch Session Manager is specified as the survivability server, the Branch Session Manager must also reference the same Communication Manager as the Communication Manager endpoint profile.

A user can have more than one Communication Profile.

Required procedures before administering a Session Manager profile

Perform the following steps before administering a Session Manager profile.

Procedure

1. Administer the primary Session Manager by adding a SIP entity of type **Session Manager** with listen ports.

   See:

   - Creating SIP Entities on page 342.
   - Adding a SIP entity as Session Manager Instance on page 416.

2. **(Optional)** For redundancy purposes, administer the secondary Session Manager by adding a SIP entity of type **Session Manager** with listen ports.

   See:

   - Creating SIP Entities on page 342.
   - Adding a SIP entity as Session Manager Instance on page 416.

3. Add SIP domains.

   See Creating domains on page 297.

4. Administer Communication Manager as a Feature Server SIP entity.

   See Creating SIP Entities on page 342.

5. Administer the Communication Manager Feature Server as an application instance.

   See Creating a new element on page 51.

6. Add the Communication Manager Feature Server as an application available for SIP Entities.

   See Creating an application on page 525.

7. Administer and add applications available for SIP Entities. Repeat as needed for each application:

   a. Create the SIP entity.

   b. Create a new element for the application.

   c. Add the application to the list of applications available for SIP Entities.

   See:

   - Creating SIP Entities on page 342.
   - Creating a new element on page 51.
   - Creating an application on page 525.

8. Create an Application Sequence from the existing applications to specify the Origination Application Sequence and Termination Application Sequence. See Creating an Application Sequence on page 529.

   See Creating an Application Sequence on page 529.

9. If you have conference products that support the Conference Factory feature, add Conference Factory Sets.

   See Adding a new Conference Factory Set and setting the respective parameters on page 538.

10. To use a Branch Session Manager server as a Survivability Server, add SIP entities of type **Session Manager** and **Branch Session Manager** with listen ports.

    See:

    - Creating SIP Entities on page 342.
    - Adding a SIP entity as a Branch Session Manager instance on page 449.

11. To modify the Home Location, configure values that are similar to Locations. To add a new value, add a Location.

    See Creating Locations on page 303.

    Note:

    Specify the Home Location to support mobility for a user. Session Manager profiles must be defined only for SIP endpoints. Assign SIP handles to all endpoints registered with Communication Manager.

12. Synchronize Communication Manager station data and messaging data with the System Manager:

    a. Administer each Communication Manager and Messaging application as an application instance.

       See:

       - Creating a new element on page 51.
       - Creating a Messaging instance on page 55.

    b. Synchronize Communication Manager and messaging data with the System Manager.

       See:

       - Synchronizing data and configuring options on page 56.
       - Synchronizing the messaging data on page 57.

Adding users

Use this procedure to add users in Session Manager. Session Manager user administration. You can ignore any input fields that are not necessary.

For information on other sections of the User Management page, see the System Manager online help.

Important:

When you create a user with a user provisioning rule, the system populates the values for user attributes from the user provisioning rule. Do not modify the populated values.

Procedure

1. On the home page of the System Manager Web Console, in **Users**, click **User Management** > **Manage Users**.
2. Click **New**.
3. Verify the Identity tab is selected.
4. **(Optional)** In the User Provisioning Rule field, select a user provisioning rule.

   You can select only one user provisioning rule. For assigning user provisioning rules, see User provisioning rule on page 149.
5. In the Identity section, enter the required information in the appropriate fields.
6. Click the Communication Profile tab.
7. In the **Communication Password** field, enter a password for the user. The user must enter this password to log in to the endpoint.
8. For each SIP handle:
   a. If you are adding a non-SIP endpoint user, for example, a DCP or H.323 endpoint user, verify the communication address of the user conforms to the Avaya E.164 type.
   b. In the Communication Address section, click **New**.
   c. In the **Type** field, select **Avaya SIP** from the drop-down menu.
   d. In the **Fully Qualified Address** field, enter the extension number.
   e. Click **Add**.
9. In the Session Manager Profile section:
   a. Select the **Session Manager Profile** check box.
   b. In the **Primary Session Manager** field, select the appropriate primary Session Manager instance from the drop-down menu.
   c. **(Optional)** For redundancy, in the **Secondary Session Manager** field, select the appropriate secondary Session Manager instance from the drop-down menu.
   d. **(Optional)** For survivability, in the **Survivability Server** field, specify a survivability server. For example, Branch Session Manager.

Note:

When you administer a user with a **Survivability Server**, the system verifies that valid SIP Entity links exist between the Branch Session Manager and the administered Primary and Secondary Session Manager servers.

e. In the **Max. Simultaneous Devices** field, select the appropriate value from the drop-down menu.

f. **(Optional)** Select the check box for **Block New Registration When Maximum Registrations Active?**.

g. In the **Origination Sequence** field, select the origination application sequence from the drop-down menu.

h. In the **Termination Sequence** field, select the termination application sequence from the drop-down menu.

i. In the **Emergency Calling Origination Sequence** field, select the emergency calling origination sequence from the drop-down menu.

j. In the **Emergency Calling Termination Sequence** field, select the emergency calling termination sequence from the drop-down menu.

k. In the **Home Location** field, enter the location. This field is mandatory for mobile users.

l. In the **Conference Factory Set** field, select the Conference Factory Set from the drop-down menu.

m. **(Optional)** Select the check box for **Enable Centralized Call History**.

n. Click **Commit**.

10. Assign the user to a Communication Manager station:

Note:

You can assign a user to a Communication Manager station only after the data synchronization is complete.

a. Select the **CM Endpoint Profile** check box.

b. From the **System** drop-down menu, select **Communication Manager**.

c. If the station already exists on the Communication Manager that is associated with the user, select the **Use Existing Endpoints** check box.

d. In the **Extension** field, enter the extension that is administered on Communication Manager for the existing or new station .

e. If you need to change the Communication Manager station data, click **Endpoint Editor** and make the necessary changes.

f. If the user is not associated with an existing Communication Manager station, in the **Template** field, select a phone template for the station of the user from the drop-down menu.

g. In the **Port** field, enter the port that is associated with the extension.

h. **(Optional)** Select the **Delete Endpoint on Unassign of Endpoint from User or on Delete User** box. This step applies only if you want the system to delete the station when you delete the user or unassign the endpoint.

11. Click **Commit**.
12. Verify the order of the primary and secondary Session Manager servers.

    See Verifying the Primary and Secondary Session Manager sequence on page 117.

Related links

New User Profile field descriptions on page 227

Verifying the Primary and Secondary Session Manager sequence

Compare and verify the primary and secondary Session Manager sequence order of the following with the primary and secondary Session Manager sequence order of the Session Manager communication profile.

- Phone settings file.
- Communication ManagerRoute Pattern administration.
- The user endpoint under SIP proxy settings.

Important:

Errors can occur if the sequence of the primary Session Manager and the secondary Session Manager is not identical to the sequence of the primary Session Manager and the secondary Session Manager in the Session Manager profile, such as Message Waiting Indicator or Presence errors.

Procedure

1. In the phone settings file, verify the sequence of the primary Session Manager and the secondary Session Manager is identical to the sequence of the primary Session Manager and the secondary Session Manager in the Session Manager communication profile.
2. In the Communication Manager Route Pattern administration, verify the sequence of the primary Session Manager and the secondary Session Manager is identical to the sequence of the primary Session Manager and the secondary Session Manager in the Session Manager communication profile.

   The first trunk choice or signaling Group in the route pattern (Far-End Node Name) must be the primary Session Manager, and the second choice is the secondary Session Manager.
3. On the user endpoint under SIP proxy settings, verify the sequence of the primary Session Manager and the secondary Session Manager is identical to the sequence of the primary

Session Manager and the secondary Session Manager in the Session Manager communication profile.

Managing communication profiles

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® network.

All communication addresses of type SIP for the communication profile are associated with the Avaya Aura® 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.

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.

Communication profiles

You can provide communication profiles to associate elements with users. Communication profiles supports communication interactions established through Avaya Communication Services. Communication profiles can be CM Endpoint, Messaging, Officelinx, Session Manager, CS 1000, CallPilot Messaging, IP Office, Presence, Avaya Breeze™, Conferencing, or Equinox Conferencing profile.

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 for the user. A communication subsystem is a service or infrastructure that manages the establishment and controls or routes the communication interactions.

System Manager supports a maximum of five communication profile sets for a user. You can add a maximum of three CM Endpoint profiles and one Messaging profile per user, and 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**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - To create a new user account, click **New**.
   - To add a communication profile to an existing user, select the user and click **Edit**.
4. On the New User Profile or the User Profile Edit page, click the **Communication Profile** tab.

5. In the communication profile section, click **New**.
6. In the **Name** field, enter the name of the new communication profile.
7. To mark the profile as default, select the **Default** check box.
8. Click **Done**.
9. Click **Commit**.

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**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - Select a user and click **Edit**.
   - Select a user and click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the **Communication Profile** section, click a profile.
6. Click **Delete**.
7. Click **Commit**.

Result

When you delete a communication profile, System Manager deletes all the communication addresses associated with the communication profile.

Creating a new communication address for a communication profile

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - To create a new user account, click **New**.
   - To add a communication profile address to an existing user, select the user and click **Edit**.

4. On the New User Profile or the User Profile Edit page, click the **Communication Profile** tab.
5. In the Communication Profile section, click a communication profile.
6. In the Communication Address section, click **New**.
7. In the **Type** field, enter a communication protocol.
8. 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, instant messenger ID, or the SIP address of a SIP-enabled device.
9. Enter the domain name from the field next to **Fully Qualified Address** field.
10. Click **Add**.
11. Click **Commit**.

Modifying the communication address

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - Select a user and click **Edit**.
   - Select a user and click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the **Communication Profile** section, select a profile.
6. In the **Communication Address** section, select a communication address.
7. Click **Edit**.
8. Modify the information in the respective fields.
9. Click **Add**.
10. Click **Commit**.

Deleting a communication address from a communication profile

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.

3. On the User Management page, perform one of the following:
   - Select a user and click **Edit**.
   - Select a user and click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the Communication Profile section, click a communication profile.
6. In the Communication Address section, select a communication address from the table.
7. Click **Delete**.
8. Click **Commit**.

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 and Messaging profiles of a user

With User Profile Management, you can create the following types of communication profiles for a user:

- CM Endpoint Profile, to create an association between an endpoint and a user
- Messaging Profile, to create an association between a subscriber mailbox and a user

You can add, view, modify, and delete endpoint and messaging profiles. You can go to Endpoint or Subscriber Management pages to modify any of the endpoint or subscriber fields that are not available through User Profile Management.

Login name of endpoint or messaging profile

The login name in the Identity section on the New User Profile and Edit User Profile pages is the user name that is associated with the communication profile, CM Endpoint and Messaging. This user name appears in the User column in the Endpoint List or Subscriber 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.

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 CM Endpoint and Messaging profiles

You can create one default or primary Communication Profile for a user. To this default profile, you can add one CM Endpoint and one Messaging profile. In addition, you can add two more CM Endpoint profiles. You can add a maximum of three CM Endpoint profiles and one Messaging 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**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
   - If you are creating a CM Endpoint profile for a new user profile, click **New**.
   - If you are creating a CM Endpoint profile for an existing user, select the user and click **Edit**.
4. Click the **Communication Profile** tab.
5. In the CM Endpoint Profile section, select the check box next to the **CM Endpoint Profile** label.
6. In the CM Endpoint Profile section, enter the relevant information.

Note:

To delete the endpoint from the communication management device after removing the association between the endpoint and the user, select the **Delete Endpoint on Unassign of Endpoint 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**.

   From User Management, you can create or add endpoints. After you select the Communication Manager in which you want to add an endpoint, the system allows you to complete the fields for creating a new endpoint.

   The **Preferred Handle** field specifies numeric only handles, SIP or non SIP, that are administered for a user. If the SIP entity is of Communication Manager type, Session Manager uses the **Preferred Handle** field 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 **Preferred Handle** field to change the phone number entry on the OPS station-mapping table on the Communication Manager.

   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 **Preferred Handle** field to the SIP handle format. After you click **Commit**, System Manager sets the **Phone Number** 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 **Preferred Handle** value to **None**.

Viewing a station profile of a user

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **View**.
4. Click the **Communication Profile** tab.

Modifying a CM Endpoint profile of a user

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the CM Endpoint Profile section, modify the relevant information in the fields.
6. To save the changes to the database, click **Commit**.

   To cancel the action and return to the previous page, click **Cancel**.

Using the automatically generated call routes for SIP routing

About this task

Based on the primary or secondary Session Manager that you have specified in the **Session Manager Communication Profile**, the system automatically determines a route pattern.

Before you begin

In the Communication Manager instance that you have associated with System Manager, make sure that:

1. On the Route Pattern page, you have specified the primary Session Manager.
2. You have selected an SIP endpoint.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. Click **Communication Profile**.
4. In **Session Manager Profile** > **SIP Registration** > **Primary Session Manager**, click a primary session manager.

   Note:

   You must add a primary Session Manager.

   For more information, see *Administering Avaya Aura® Communication Manager*.
5. In **CM Endpoint Profile**, do the following:
   a. In the **Set Type** field, enter the details of an SIP set type.
   b. Select the **Calculate Route Pattern** check box.

Result

For the user that you specified and for the Session Manager that you set as a primary Session Manager, the system automatically generates route patterns.

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**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
   - Click **Edit**.

- Click **View** > **Edit**.

4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the **CM Endpoint Profile** section, clear the check box next to the **CM Endpoint Profile** label.
6. 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**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the **CM Endpoint Profile** section, clear the check box next to the **CM Endpoint Profile** label.
6. 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.

Messaging profile administration

Adding a messaging profile for a user

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management 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**.
4. Click the **Communication Profile** tab.
5. In the Messaging Profile section, select the check box next to the **Messaging Profile** label.
6. 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.
7. Click **Commit** or **Commit & Continue** to add the messaging profile, or click **Cancel** to return 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.

Modifying a messaging profile of a user

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.

5. In the Messaging Profile section, modify the relevant information in the fields.
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**.

Viewing a messaging profile of a user

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **View**.
4. Click the **Communication Profile** tab.

Result

The Messaging Profile section displays the messaging profile information of the user.

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**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the Messaging Profile tab, clear the check box next to the **Messaging Profile** label.
6. 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**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. In the Messaging Profile section, clear the check box next to the **Messaging Profile** label.
6. 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 and CallPilot profile administration

CS 1000 and CallPilot profile administration

With User Management, you can create the following types of communication profiles for a user:

- CS 1000 Endpoint Profile. To create an association between an endpoint and a user.
- CallPilot Messaging Profile. To create an association between a subscriber mailbox and a user.

Note:

You cannot assign the mailbox number in the CallPilot communication profile by using the user provisioning rule. You must add the mailbox number for the CallPilot communication profile.

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 or CallPilot user to Element Manager.

Redirecting the CS 1000 or CallPilot user to Element Manager

Before you begin

A user must exist with at least one communication profile. To create a user, navigate to **User Management** > **New**.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. Select **CS 1000 Endpoint Profile** or **CallPilot Messaging Profile** that you must update and click **Update**.

   The system opens 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.
6. Enter the relevant information and click **Save**.

   The system displays the User Management page.

Adding a CallPilot profile for a user

Before you begin

A user must exist. To create a user, navigate to **User Management** > **New**.

About this task

For a communication profile, you can provide a maximum of one CallPilot mailbox. To add additional mailboxes for a user, you must add another communication profile.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left 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 New User Profile page, click the **Communication Profile** tab.
5. In the CallPilot Messaging Profile section, select the check box and complete the following fields:
   - In the **System** field, select a CallPilot system. The system displays a list of systems that are registered with the element registry.
   - In the **Target** field, select the location of CallPilot, if provisioned.

- In the **Template** field, select a template that CallPilot Element Manager provisions.
- In the **Mailbox Number** field, enter a mailbox number for CallPilot.

Note:

You must enter the mailbox number even if the value is same as Primary DN.

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**.

Adding a CS 1000 profile for a user

Before you begin

A user must exist. To create a new user, navigate to **User Management** > **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**.
2. In the left 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 profile, click **New**.
   - To create a profile for an existing user, select the user and click **Edit**.
4. On the New User Profile page, click the **Communication Profile** tab.
5. 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.

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**.

Modifying a CS 1000 user profile

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user and perform one of the following steps:
   - Click **Edit**.
   - Click **View** > **Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. Click **Update**.
6. 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.

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**.

Modifying a CallPilot user profile

About this task

You cannot modify the CallPilot profile from System Manager User management.

Procedure

1. On the System Manager web console, click **Elements** > **Communication Server 1000**.
2. On the Elements list, click the CallPilot element.
3. Log in to CallPilot Manager.
4. On the CallPilot Manager page, enter the relevant information in the fields.

Note:

- In CallPilot Manager, do not update **Mailbox Number**. The system maps the mailbox number to the System Manager User management user **First Name** and **Last Name**. Use User management from System Manager to update the mailbox number.
- When you update the data for the CS 1000 or CallPilot profiles, the system does not automatically update User management in System Manager. Use Account synchronization to update the data in System Manager User management.

For more details, see the “Communication profiles synchronization” section.

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 left 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 New 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.

Viewing an IP Office endpoint profile of a user

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left 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.

Modifying an IP Office endpoint profile of a user

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left 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.

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 left 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**.

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.

Viewing details of a user

Before you begin

You require appropriate permissions.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.

3. On the User Management page, select a user.
4. 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 field descriptions on page 271

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**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select a user.

   Note:

   At one time, you can edit only one user account.
4. To edit a user account, perform one of the following:
   - Click **Edit**.
   - Click **View** > **Edit**.
5. On the User Profile Edit page, perform 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)** 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 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.

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**.

Related links

User Profile Edit field descriptions on page 249

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**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select one or more users from the table, and click **Delete**.
4. On the User Delete Confirmation page, click **Delete**.

Note:

You cannot delete users:

- With the login name *admin* from the User Management page.
- Synchronized from LDAP.

Removing the deleted users from the database

Using this procedure, you can permanently delete a user from the database.

Before you begin

Permission to delete the selected user.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, click **More Actions** > **Show Deleted Users**.
4. On the Deleted Users page, select the users to delete, and click **Delete**.
5. On the User Delete Confirmation page, click **Delete**.

Viewing the deleted users

When you remove a user from the User Management page using the **Delete** option, the system removes the user temporarily and stores the user in the **Deleted Users** table. To view the temporarily deleted users, use the **Show Deleted Users** option.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, click **More Actions** > **Show Deleted Users**.

   On the Deleted Users page, the system displays the temporarily deleted users in the Deleted Users table.

Restoring a deleted user

You can use this functionality to restore a user that you deleted using the **Delete** option on the User Management page.

Before you begin

You require permission to restore the selected user that is already deleted.

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.

3. On the User Management page, click **More Actions** > **Show Deleted Users**.
4. On the Deleted Users page, select the user you want to restore, and click **Restore**.
5. On the User Restore Confirmation page, click **Restore**.
6. Click **Commit**.

Note:

For a restored user, if you assign a role other than End-User, the system prompts for a password.

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 or CallPilot Messaging Profile communication. You must add the CS 1000 Endpoint Profile or CallPilot Messaging Profile communication 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**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, select the user account that you must duplicate.
4. Click **Duplicate**.
5. On the User Profile Duplicate page, enter the appropriate information.
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**.

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 left 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.

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 left 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.

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 left 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.

Deleting contacts from the default contact list

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left 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

Field	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.
Contact Address	The address of a private or public contact. No contact address is associated with a contact type user.
User Handles	The communication handles associated with the user. These handles are defined in the communication profile of a user.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Enable	Displays fields under selected columns that you can use to set the filter criteria. This is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.
Advanced Search	Displays fields that you can use to specify the search criteria to search for contacts.

Button	Description
Select	Adds the selected contact in the list of associated contacts.
Cancel	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.

Field	Description
Search On	The search options that must base on the **Contact** or **User**.

Table continues…

Field	Description
Criteria	The search criteria for searching the contacts. Displays the following three fields: • 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. • 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. • Field 3 - The value for the search criterion.

Button	Description
+	Adds one more search criteria section.
-	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
Label	The text description for classifying this contact.
Alternative Label	The text description for classifying this contact. The field is similar to **Label**, and is used to store label in an alternate language.
Description	The brief description about the contact.
Presence Buddy	An option to indicate whether to allow monitoring of the presence information of the contact.
Speed Dial	An option to indicate whether to allow speed dial for the contact.
Address/Handle	The fully qualified URI for interacting with the contact. This field is available only if you select the **Speed Dial** check box.
Speed Dial Entry	The reduced number that represents the speed dial number. This field is available only if you select the **Speed Dial** check box.

Contact Details

Field	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	The brief description about the contact.
Company	The name of the company to which the contact belongs.
Localized Display Name	The localized display name of a user. The name is usually the localized full name.
Endpoint Display Name	The endpoint display name of the contact.
Language Preference	The list of languages from which you set a language as the preferred language for the contact.
Update Time	The time when the contact information was last updated.
Source	The source of provisioning the contact.

Postal Address

Field	Description
Name	The name of the contact.
Address Type	The type of mailing address such as, home or office address.
Street	The name of the street.
Locality Name	The name of the city or town.
Postal Code	The postal code of the locality of the city or town.
Province	The full name of the province of the contact.
Country	The name of the country of the contact.

Contact Address

Field	Description
Address	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.
Type	The type of communication medium for interacting with the user.
Category	The categorization of the address based on the location.
Label	The description for classifying this contact.

Table continues…

Field	Description
Alternative Label	The description for classifying this contact. The field is similar to **Label**, and is used to store label in an alternate language.

Button	Description
Add	Saves the modified information in the database.

View Contact List Member field descriptions

Contact Membership Details

Name	Description
Label	Displays a text description for classifying this contact.
Alternative Label	Displays a text description for classifying this contact. The **Alternative Label** field is similar to **Label**, but you use the field to store label in an alternate language.
Description	Displays a brief description about the contact.
Presence Buddy	Provides the option to indicate whether to allow monitoring of the presence information of the contact.
Speed Dial	Provides the option to indicate whether to allow speed dial for the contact.
Address/Handle	Displays a fully qualified URI for interacting with the contact. This field is available only if you select the **Speed Dial** check box.
Speed Dial Entry	Displays the reduced number that represents the speed dial number. This field is available only if you select the **Speed Dial** check box.

Contact Details

Name	Description
Last Name	Displays the last name of the contact.
First Name	Displays the first name of the contact.
Middle Name	Displays the middle name of the contact.
Description	Displays a brief description about the contact.
Company	Displays the name of contact's company
Localized Display Name	Displays the localized display name of a user. It is typically the localized full name.

Table continues…

Name	Description
Endpoint Display Name	Displays the endpoint display name of the contact.
Language Preference	Displays a list of languages from which you set one language as the preferred language for the contact.
Update Time	Displays the time when the contact information was last updated.
Source	Displays the source of provisioning the contact.

Postal Address

Name	Description
Name	Displays the name of the contact.
Address Type	Displays the mailing address type such as, home or office address.
Street	Displays the name of the street.
City	Displays the name of the city or town.
Postal Code	Displays the postal code of the locality of the city or town.
Province	Displays the full name of the contact's province.
Country	Displays the name of the contact's country.

Contact Address

Name	Description
Address	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.
Type	Displays the type of communication medium for interacting with the user.
Category	Displays the categorization of the address based on the location.
Label	Displays a text description for classifying this contact.
Alternative Label	Displays a text description for classifying this contact. This field is similar to **Label**, but it is used to store label in an alternate language.

Filtering users

About this task

You can apply filter to the following user information:

- Last Name
- First Name
- 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**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, click **Filter: Enable**.

   The system displays the **Filter: Enable** button at the upper-right corner of the table that displays users.
4. Enter the information for one or more of the following filter criteria:
   - To filter users by the last name, in the **Last Name** column, enter the last name of the user.
   - To filter users by the first name, in the **First Name** column, enter the 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 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.
5. **(Optional)** To hide the column filters, click **Disable**.

   This action does not clear any filter criteria that you had set.
6. Click **Apply**.

   The table displays the users that match the filter criteria.
7. To clear the filter criteria, click **Clear**.

Searching for users

Procedure

1. On the System Manager web console, click **Users** > **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, click **Advanced Search** at the upper-right corner of the page.
4. In the Criteria section, do the following:
   a. In the first field, select the search criterion.
   b. In the second field, select the operator.
   c. In the third field, enter the search value.
5. To add another search criterion, click plus (**+**) and repeat Step 4a through Step 4c.

   To delete a search criterion, you must click minus (-). The system displays **-** when more than one search criterion is available.
6. Click **Search**.

   The **Users** table lists the users that match the search criteria.

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

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.

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™

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 as admin.
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, perform 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 information.
   c. On the **Organization** tab, select the appropriate information.

   For more information, see User Provisioning Rule field descriptions.
5. Click **Commit** to save the changes.

Modifying the user provisioning rule

Before you begin

Create a user provisioning rule.

Procedure

1. Log on to System Manager as admin.
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, perform one of the following:
   - Click **Edit**.
   - Click **View** > **Edit**.
5. On the Edit User Provisioning Rule page, perform 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**.

Viewing the user provisioning rule

Before you begin

Create a user provisioning rule.

Procedure

1. Log on to System Manager as admin.
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**.

Creating a duplicate user provisioning rule

About this task

You can duplicate a user provisioning rule to create a new user provisioning rule by copying the information from the existing user provisioning rule.

Procedure

1. Log on to System Manager as admin.
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. Click **Duplicate**.
5. On the Duplicate User Provisioning Rule page, perform 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**.

Deleting the user provisioning rule

Procedure

1. Log on to System Manager as admin.
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**.

   The system removes the user provisioning rule from System Manager.

   System Manager disassociates the user provisioning rule from the user if you have already provided the user provisioning rule for the user.

User Provisioning Rules Management field descriptions

Field	Description
Name	The name of the user provisioning rule.
SIP Domain	The name of the configured SIP domain name.
Description	A brief description of the user provisioning rule.

Button/Icon	Description
View	Displays the View User Provisioning Rule page with details of the user provisioning rule that you selected.
Edit	Displays the Edit User Provisioning Rule page where you can modify the selected rule.
New	Displays the New User Provisioning Rule page where you can create a new rule.
Delete	Deletes the user provisioning rule that you selected.
Duplicate	Copies the user provisioning rule that you selected.
	Refreshes the user provisioning rule information in the table.
Select	• All: Selects all user provisioning rules in the table. • None: Clears the check box selections.

User Provisioning Rule field descriptions

Basic

Name	Description
User Provisioning Rule Name	The name of the user provisioning rule.
Description	A description of the user provisioning rule.
SIP Domain	The name of the configured SIP domain name. If **SIP Domain** is nonblank, create an Avaya SIP communication address for the user. The system changes the SIP domain for all selected users with the value that you provide in this field.

Table continues…

Name	Description
Presence/IM Domain	The name of the configured Presence domain name. If **Presence/IM Domain** is nonblank, create an Avaya Presence/IM communication address for the user. The system changes the Presence/IM Domain domain for all selected users with the value that you provide in this field.
Communication Profile Password	The communication profile password. The field is available only if you enable the communication profile. The password policy is configured from **Users** > **User Management** > **Communication Profile Password Policy**. When communication password value is provided during bulk edit of users, the system overwrites any existing communication profile passwords of the user.
Confirm Password	The communication profile password that you must re-enter.
Use Phone Number last ..... digits for Extension	The number of last digits of the phone number that the system uses from the LDAP attribute. E.164 numbers can contain maximum 15 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 **Prefix for Avaya E164 Handle** field. The LDAP attribute is mapped to the `Phone Number` attribute of System Manager on the User Synchronization Datasource page.
Prefix for Avaya E164 Handle	The digits that the system must prefix to the telephone number or Avaya E.164 handle. The default is plus (+).
Language Preference	The preferred written or spoken language of the user. For example, English.
Time Zone	The preferred time zone of the user.

Button	Description
Commit	Creates the user provisioning rule and displays the User Provisioning Rule page.
Cancel	Cancels the create, edit, or delete operation of the user provisioning rule.

Table continues…

Button	Description
Done	Saves the changes that you make to the user provisioning rule. The system displays this button only during the view operation.
Edit	Displays the fields in the edit mode. The system displays this button only during the view operation.

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
Primary Session Manager	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® network. You must select the primary Session Manager server.
Secondary Session Manager	The Session Manager instance that you select as the secondary Session Manager 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
Survivability Server	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. **Note:** 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.
Max. Simultaneous Devices	The maximum number of endpoints that you can register at a time using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.
Block New Registration When Maximum Registrations Active	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.
Origination Application Sequence	The application sequence that the system will invoke when routing the calls from this user. A selection is optional. **Note:** 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.

Table continues…

Name	Description
Termination Application Sequence	The application sequence that will be invoked when the system routes the calls to this user. A selection is optional. **Note:** 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.
Emergency Calling Origination Sequence	The list of application sequences invoked when the system routes emergency call from this user.
Emergency Calling Termination Sequence	The list of application sequences invoked when the system routes emergency call to this user.
Home Location	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 of the location. You must specify a value.
Conference Factory Set	The conference factory set to enable media capability-based call routing to the Conferencing SIP entities. Use the **Session Manager** > **Application Configuration** > **Conference Factories** webpage to administer the Conference Factory Sets.

Communication Profile tab: Avaya Breeze™ Profile

Name	Description
Service Profile	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
Use Next Available Extension	The option to instruct the system to create a new extension for the user. **Note:** For LDAP synchronization, the value in the **Use Phone Number last ..... digits for Extension** field takes priority.
Template	The template, system defined or user defined, that you associate with the endpoint. Select the template based on the set type you add. You must select the template.
Security Code	The security code for authorized access to the endpoint.
Preferred Handle	Avaya SIP or Avaya E.164 handle that is administered for the user. The field is optional. By default, the field is blank.
Password	The password to gain access to the endpoint. The system displays the field if you select **Agent** in **Profile Type**.
Allow H.323 and SIP Endpoint Dual Registration	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 *Avaya Aura® Communication Manager Feature Description and Implementation* on the Avaya Support website at http://support.avaya.com.

Communication Profile tab: CS 1000 Endpoint Profile

Name	Description
System	The system that will be the element manager of the CS 1000 endpoint profile. You must select the system.
Target	The phone or endpoint template that you can choose for the user. The element manager maintains all templates. You must select a template.
Template	The phone or endpoint template that you can choose for the user. The element manager maintains all templates. You must select a template.
Include in Corporate Directory	The option to add this profile to the CS 1000 Corporate Directory feature.
Delete Endpoint on Unassign of Endpoint from User	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
System	The messaging system on which you add the subscriber. You must select the system.
Mailbox Number	The mailbox number of the subscriber. The options are: • Use CM Extension: Use this option only if the Communication Manager profile and Session Manager profile are specified. • Use Next Available Subscriber: Use this option if the system must use the next mailbox number to associate with this profile.
Template	The system-defined or user-defined template that you associate with the subscriber.
Password	The password for logging in to the mailbox. You must provide the password.
Delete Subscriber on Unassign of Subscriber from User or on Delete User	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: Officelinx Profile

Name	Description
System	The Officelinx system to which you add a mailbox.
Refresh	Gets the information about company, departments, and feature groups from Officelinx and saves locally on System Manager for future use. You do not require to refresh for every user.
Use Next Available Mailbox	The option to specify if the system must use the next mailbox number to associate with this profile.
Mailbox Range	The range of mailbox numbers assigned to the Officelinx system. **Note:** This option is available only when you select the **Use Next Available Mailbox** check box.

Table continues…

Name	Description
Numeric Password	The numeric password that is used to log in to the Officelinx system.
Application User Password	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.
Company	The name of the company to which the user belongs.
Department	The department to which the user belongs.
Feature Group	The feature group name that determines the rules for the mailboxes associated with it.
Capability	The type of functionality that the user contains. The values are: • **Standard** • **Fax** • **Messaging** • **Collaboration** • **Messaging and Collaboration**
Domain Account Name	The mailbox NT account name for the Officelinx profile. The options are: • **Same as Login Name** • **Admin Specified**
Synchronization User Name	The account name that is used to gain access to the email server, for example, Microsoft Exchange and Google Gmail. The options are: • **Same as Login Name** • **Admin Specified**

Communication Profile tab: CallPilot Messaging Profile

You cannot assign the mailbox number in the CallPilot communication profile by using the user provisioning rule. You must add the mailbox number for the CallPilot communication profile.

Name	Description
System	The CallPilot system of the messaging profile. The selection is mandatory required.
Target	The field that maps to the CallPilot **Location** field. CallPilot Manager provides the **Target** field. You must select the target.

Table continues…

Name	Description
Template	The mailbox template that you use. Select a template from the drop down list. The element manager maintains all the mailbox templates. You must select the template.

Communication Profile tab: IP Office Endpoint Profile

Name	Description
System	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.
Extension	The extension of the endpoint to which you associate the profile. The options are: • Use CM Extension: Use this option only if Communication Manager profile is specified. • Use Next Available Extension: Use this option if the system must use the next extension to associate with this profile.
Template	A list of user templates from which you can select a template to set the user configurations.
Set Type	The set type for the IP Office endpoint profile. By default, the **Set Type** field is disabled. If you select a template, the system automatically populates the set type value.

Communication Profile tab: Presence Profile

Name	Description
System	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: • Aggregate presence • Archive instant messages if the Instant Messages option is enabled
SIP Entity	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 **System** field. **SIP Entity** is read-only. If the system cannot identify a SIP entity, an appropriate error message is displayed in the field.

Table continues…

Name	Description
IM Gateway SIP Entity	The Presence Services instance for the user.
Publish Presence with AES Collector	The option that determines if Presence Services must publish presence with AES Collector. The options are: • **System Default** • **Off** • **On** The default is **System Default**. 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
Template	The template that you use to set the user configurations.
Location	The location that Conferencing uses when the IP address of the calling phone does not match any IP address pattern of any location. Specify this field to support the mobility of the user.
Select Auto-generated Code Length	The number of digits in the security code that the system generates.
Auto Generate Participant and Moderator Security Codes	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
Equinox User Password	The password that is used to log in to the Avaya Equinox® Management.
Virtual Room Number	The number of a virtual room that is used to create a conference. By default Virtual Room Number serves as Meeting ID when a conference is created. The options are: • **Use Phone Number**: 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. • **Auto Generate Virtual Room Number**: Use this option if the system needs to generate the Virtual Room Number automatically.

Organization

Name/Button	Description
Tenant	The tenant of the user created by the user provisioning rule.
Site	The work site of the user created by the user provisioning rule.
Department	The department of the user created by the user provisioning rule.
Team	The team of the user created by the user provisioning rule.

Button	Description
Commit	Saves the changes and displays the User Provisioning Rules page.
Cancel	Cancels the operation and displays the User Provisioning Rules page.

Role Based Access Control

Role Based Access Control (RBAC) in System Manager supports two types of roles:

- Built-in
- Custom

Built-in roles are the default roles provided by System Manager. You can assign built-in roles to users. You cannot change or delete the permission mappings in the built-in roles.

Some of the important built-in roles and the privileges are as follows:

Role	Privileges and limitations
Auditor	• Read-only access to the system. • Read-only access to logs, configuration information and audit files. Not allowed to run any commands.
Session Manager and Routing Administrator	Read-write access to the Session Manager and Routing web pages.
Session Manager and Routing Auditor	Read-only access to the Session Manager and Routing web pages.

Table continues…

Role	Privileges and limitations
Security Administrator	• Create other logins. • Create, modify, or assign roles. • Install licenses. • Install PKI certificates and keys.
Backup Administrator	Perform backups and restores.
System Administrator	• Read-write access to system parameters. • Modify, assign, or define other roles. • Create and modify logins and all other functionalities.
Avaya Maintenance and Support	• Read-only access to maintenance logs. • Run diagnostics. • View the output of diagnostics tools. Not allowed to run any command that may provide access to another host.

Custom roles access

The administrator can define custom roles to have access to the Session Manager and Routing web pages.

Note:

Only the following built-in roles provide access to the Session Manager and Routing web pages:

- Auditor
- Session Manager and Routing Administrator
- Session Manager and Routing Auditor
- System Administrator
- Avaya Services Administrator

Permissions

With the Session Manager RBAC feature, a system administrator can assign permissions to specific Session Manager and Routing web pages. A user can access or modify only those web pages for which the user is authorized.

The possible permissions include:

- Total read/write permissions. The administrator can view the page and can make modifications to all of the administered fields which are on the page.
- Read-only permissions. The administrator can view the entire page, but cannot make any changes to the fields on the page. The administered fields display the current contents, and the buttons are not operational.

Important:

Providing full access to the Session Manager and Routing web pages does not automatically entitle a user to access the following System Manager elements. You must explicitly grant access permissions to these System Manager web pages:

- Replication
- Inventory > Manage Elements
- User Management

On the Permission Mapping page, the administrator can grant the role:

- Access to all Session Manager and Routing pages.
- Access to specific pages.

RBAC permissions for Routing Import/Export operations

For a user to import Routing data, the administrator must assign one of the following roles:

- System Administrator
- Avaya Services Administrator and Scheduler operation
- Session Manager and Routing Administrator and Scheduler operation

A user with read/write permissions for a specific Routing page cannot import any Routing data. A user with page-level permissions would be able to import any Routing related data, not just data pertaining to the accessible pages. Consequently, the operation is limited to System Administrators.

For a user to export Routing data, the administrator must assign one of the following built-in default roles to the user:

- System Administrator
- Avaya Services Administrator
- Session Manager and Routing Administrator
- Auditor
- Session Manager and Routing Auditor

When exporting data as an Auditor, the user must perform the export operation from the Bulk Import and Export menu.

RBAC permissions for Local Host Name Resolution imports

The administrator must assign one of the following roles for a user to import host name entries on the Local Host Name Resolution page:

- System Administrator
- Avaya Services Administrator
- Session Manager and Routing Administrator

The administrator must assign either of the following permissions to a user to edit more than 15 communication profiles on the Communication Profile Editor page:

- One of the following built-in default roles:
  - System Administrator
  - Avaya Services Administrator
  - Session Manager and Routing Administrator
- Read/write permissions for the Communication Profile Editor page and scheduler operation permissions.

Local Host Name Resolution imports and bulk communication profile edits for more than 15 users are performed as scheduled jobs. Consequently, the tasks can only be performed by a user with permissions to schedule jobs using the System Manager Scheduler.

RBAC permissions for Bulk Communication Profile edits

The administrator must assign one of the following roles to a user to edit more than 15 Communication Profiles on the Communication Profile Editor page:

- System Administrator
- Avaya Services Administrator and Scheduler operation
- Session Manager and Routing Administrator and Scheduler operation

The user must have read/write permissions for the Communication Profile Editor page and scheduler operation permissions.

For more than 15 users, LHNR imports and bulk communication profile edits are performed as scheduled jobs. The operations can only be performed by a user with permissions to schedule jobs using the System Manager Scheduler.

Creating a Scheduler operation role

You must assign the Scheduler operation role to the following roles to use the import operation:

- Avaya Services Administrator
- Session Manager and Routing Administrator

Procedure

1. On the home page of the System Manager Web Console, in **Users**, click **Groups & Roles** > **Roles**.
2. On the Roles page, select **System Administrator**.
3. Click **New**.
4. On the Add New Role page, enter a name in the **Role Name** field.
5. Enter a short description of the role in the **Role Description** field.
6. Click **Commit and continue**.
7. In the Element/service Permissions tab, click **Add mapping**.
8. On the Select Element and/or network Service to Map to Role page, select **Scheduler operation** from the drop-down menu for **Element or Resource Type**.
9. In the **Element or Resource Instance** field, select **ALL** from the drop-down menu.

   Note:

   Group selection is optional.
10. Click **Next**.
11. On the Permission Mapping page, select the **Select/Unselect All** check box.
12. Click **Commit**.

Creating an RBAC role with read-only permissions

You can create an RBAC role with read-only access for all web pages or specific web pages under the Session Manager and Routing tabs.

Procedure

1. On the home page of the System Manager Web Console, in **Users**, click **Groups & Roles** > **Roles**.
2. Select a role or select **System Administrator**.
3. Click **New**.
4. Enter the role name and description.

5. Click **Commit and continue**.
6. In the Element/Service Permissions tab, click **Add mapping** to assign permissions to the role.
7. On the Select Element and/or Network Service to Map to Role page:
   a. In the **Element or Resource Type** field, select **Session Manager and Routing** from the drop-down menu.
   b. In the **Element or Resource Instance** field, select **All** from the drop-down menu.

   Note:

   Group selection is optional.
8. Click **Next**.
9. On the Permission Mapping page, do one of the following:
   - To grant access to all pages, select the **Read-only access to all web pages under the Session Manager and Routing tabs** check box.
   - To grant page-level access:
     a. Expand the section heading on the page corresponding to each of the Session Manager and Routing web pages.
     b. Select the read-only check box for the specific page.
10. Click **Commit**.

    The system displays the Role Details page with the permissions you have chosen.
11. Click **Commit**.

    The system creates the new role that is added to the displayed roles on the Roles page.
12. Assign the role to a user.

    See Assigning an RBAC role to a user on page 171.

Creating an RBAC role with read and write permissions

You can create an RBAC role with read and write permissions for all web pages or specific web pages under the Session Manager and Routing tabs.

To copy the permission mappings of an existing role, see Copying permission mapping for a role on page 173.

Procedure

1. On the home page of the System Manager Web Console, in **Users**, click **Groups & Roles** > **Roles**.
2. On the Roles page, select **System Administrator**.

3. Click **New**.
4. On the Add New Role page, enter a name in the **Role Name** field.
5. Enter a short description of the role in the **Role Description** field.
6. Click **Commit and continue**.
7. In the **Element/Service Permissions** tab, click **Add mapping**.
8. On the **Select Element and/or Network Service to Map to Role** page:
   a. In the **Element or Resource Type** field, select **Session Manager and Routing** from the drop-down menu.
   b. In the **Element or Resource Instance** field, select **All** from the drop-down menu.

   Note:

   Group selection is optional.
9. Click **Next**.
10. On the Permission Mapping page, select the **Full Access or selected permissions** check box.
11. Click **Commit**.

    The system displays the Role Details page with the permissions you have chosen.
12. To confirm your settings, click **Commit**.

    The system creates the new role and adds the role to the displayed roles on the Roles page.
13. Assign the role to a user. See Assigning an RBAC role to a user on page 171.

    Note:

    If the user needs to import Routing data, perform LHNR imports, or edit Communication Profiles, the administrator must assign one more role Scheduler operation.

Assigning an RBAC role to a user

Assign a Role Based Access Control role to a user.

To assign a role to multiple users, see *Assigning users to an RBAC role* in *Administering Avaya Aura® System Manager* on the Avaya Support website at http://support.avaya.com.

Note:

If you assign a new role to a user and do not provide a new password, the system resets the password to match the login name of the user. When the user logs in, the system prompts the user to change the password.

Procedure

1. On the home page of the System Manager Web Console, under **Users**, select **User Management** > **Manage Users**.
2. On the User Management page, do one of the following:
   - To assign a role while setting up a new user account, click **New**.
   - To assign a role to an existing user, select the user and click **Edit** or **View** > **Membership** > **Edit**.
3. On the New User Profile or User Profile Edit page, click the **Membership** tab.
4. Click **Assign Roles**.
5. On the Assign Roles page, select a role from the **Available Roles** section.
6. To assign the role to the selected user, click **Select**.
7. On the New User Profile page or the User Profile Edit page, click **Commit** to save the changes.

Configuring a user to have access permissions for System Manager web pages

This procedure describes how to grant access to the Manage Elements System Manager element for Session Manager administration and maintenance.

Note:

If a user is assigned to a role with read/write access to the Session Manager web pages, the user must also be authorized to add, edit or delete elements on the Manage Elements web page. Likewise, a user assigned to a role with read-only access to the Session Manager web pages must be given read-only permissions on the Manage Elements web page.

Procedure

1. On the home page of the System Manager Web Console, in **Users**, click **Groups & Roles** > **Roles**.
2. On the Roles page, select **System Administrator**.
3. On the Add New Role page, enter a name in the **Role Name** field.
4. Enter a short description of the role in the **Role Description** field.
5. Click **Commit and continue**.
6. In the Element/Service Permissions tab, click **Add mapping**.
7. On the Select Element and/or Network Service to Map to Role page, click **operation** under the Element or Resource Type category.
8. Click **Next**.

9. Select the **Elements/ApplicationManagement** and **Services/Inventory/ManageElements** elements.
10. Do one of the following:
    - For read/write access to the Manage Elements page, select **RTS_Administration** and **RTS_Administration/RTS_Edit_Operation**.
    - For read-only access to the Manage Elements web page, select **RTS_Administration**.
11. Click **Commit**.

    The system displays the Role Details page with the permissions you have chosen.
12. To confirm your settings, click **Commit**.

    The system adds the new role to the displayed roles in the Role page.
13. Assign the role to a user. See Assigning an RBAC role to a user on page 171.

Copying permission mapping for a role

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left 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.

Removing access permissions for Session Manager and Routing pages

For information about disassociating the roles from a user, see *Removing roles from a user* in *Administering Avaya Aura® System Manager* on the Avaya Support website at http://support.avaya.com. You can follow the same procedure as explained below for removing access permissions for other element pages.

To delete a custom role, see *Deleting a role* in *Administering Avaya Aura® System Manager*.

Procedure

1. On the home page of the System Manager Web Console, in **Users**, click **Groups & Roles** > **Roles**.
2. On the Roles page, select a role.
3. On the Role Details page, click the **Element/Service Permissions** tab.
4. Select an Element/Service Permission of type **Session Manager and Routing** from the list and click **Delete Mapping**.

   The system displays the Delete Mapping page.
5. Click **Delete** to delete the selected role mapping.

Removing the assigned RBAC role from a user

Procedure

1. On the home page of the System Manager Web Console, in **Users**, click **User Management** > **Manage Users**.
2. On the User Management page, select the appropriate user and click **Edit**.
3. On the User Profile Edit page, click the **Membership** tab.
4. Select the role you want to remove and click **UnAssign Roles**.
5. Click **Commit**.

Managing bulk import and export

Bulk import and export

In System Manager, you can bulk import and export user profiles and global settings. 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 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, CallPilot Messaging, Conferencing, IP Office, Presence, Avaya Breeze™, Work Assignment, Officelinx, Avaya Equinox profile.

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.

Import and export 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 default
- Handle. The communication address of the user
- Session Manager profile
- Avaya Breeze™ profile
- CM Endpoint profile with all attributes of the station communication profile
- CM Agent profile with all attributes.
- Messaging profile
- Officelinx profile
- CallPilot profile
- IP Office Endpoint profile
- CS 1000 Endpoint profile
- Presence profile
- Conferencing profile
- Work Assignment profile
- Avaya Equinox profile

- Supports more than one communication profile set.
- Supports the creation, updation, and deletion of the user using the same Excel file. However, you can 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 as key 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 change 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.

XML Schema definitions and sample XMLs for bulk import

See List of XML Schema Definitions and sample XMLs for bulk import on page 750.

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	.....	Go to Station Site Data worksheet		Go to Buttons worksheet

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™ 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.

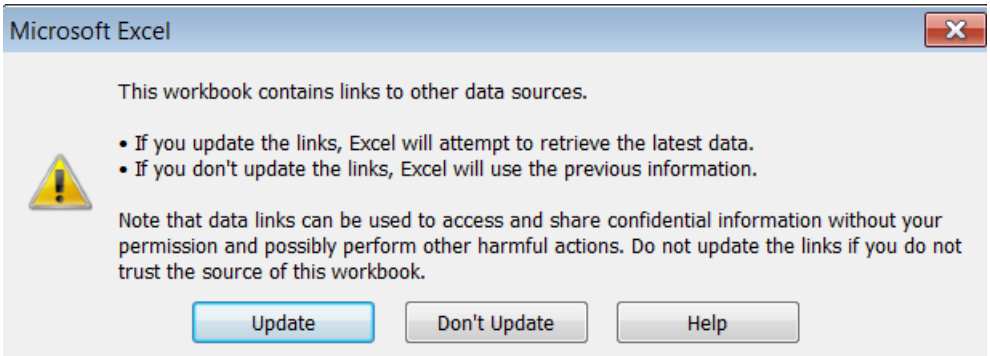
Element	Master worksheet	Child worksheets
Session Manager	Session Manager Profile	None

Table continues…

Element	Master worksheet	Child worksheets
Communication Manager — Endpoint	CM Endpoint Profile	• Station Site Data • Buttons • Feature Buttons • Expansion Module Buttons • Soft Keys • Display Buttons • Station Abbr Dialing Data • Station Data Module • Station Hot Line Data • Native Name Data
Communication Manager — Agent	CM Agent Profile	• CM Agent LoginId Skills Data • CM Agent Native Name Data
Messaging	Messaging Profile	• Messaging MMSpecific • Messaging CMMSpecific • Messaging AAMSpecific
Conferencing	Conferencing Profile	None
IP Office	IP Office Endpoint Profile	None
CS 1000	CS 1000 Endpoint Profile	None
Avaya Breeze™	CE Profile	None
CallPilot	CallPilot	None
Presence	Presence Profile	None
Work Assignment	Work Assignment Profile	• Work Assignmnt Resource Details • Work Assignmnt Agent Attributes
Officelinx	Officelinx Profile	None
Equinox	Equinox Profile	None

Microsoft Excel data link error

Microsoft Excel 2010 displays a data link error.



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.

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.

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 750. See Sample XML for bulk import of users with all attributes on page 757 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 commprofileset 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 commprofileset.

  Note:

  For CS1000 Endpoint Profile and CallPilot Messaging 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 commprofileset 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 commprofileset.
- 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 750. 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 757 and Sample XML for bulk import of users with all attributes on page 757.
- XML schema definition for partial import of users: See XML Schema Definition for partial import of user attributes on page 765. 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 767.

To delete bulk users, a separate XML schema definition is defined. See XML Schema Definition for bulk deletion of users on page 769. For a sample XML that conforms to delete bulk users XML schema definition, see Sample XML for bulk deletion of users on page 770.

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.

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 left 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.

About 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, CallPilot Messaging, Conferencing, IP Office, Presence, Avaya Breeze™, Work Assignment, Officelinx, Avaya Equinox profile.

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 750.

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 the *system administrator* role. For security reasons, the system does not export the **Password** fields to the XML file. Therefore, import of users with the *system administrator* role fails.

To import users with the *system administrator* role, in the XML file for the users, add the following XML tag after the `<username>` tag:

```
<userPassword> provide password for user </userPassword>
```

The system imports the other user records with non system administrator roles and automatically sets the password to `Avaya123$` for **Complete Merge/Replace** import type. 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 deletes the file.

Exporting users in bulk from web console

About this task

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.

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.

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:

   a. An `XML` file with added or updated users in last one week.
   b. An `Excel` file with added or updated users in last one week.
   c. 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.

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 765. For a sample XML file for import of user, see Sample XML for partial import of users on page 767.

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**.

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 750. Partial import type uses a different XML schema definition, for more information, see XML Schema Definition for partial import of user attributes on page 765.

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 ">
     ```

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 ">
     ```

Import user considerations

- If the comprofileset has associated handlelist or commprofilelist, you cannot merge or replace commprofileset attributes name and Isprimary.

  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 the *system administrator* role. For security reasons, the system does not export the **Password** fields to the XML file. Therefore, import of users with the *system administrator* role fails.

To import users with the *system administrator* role, in the XML file for the users, add the following XML tag after the `<username>` tag:

```
<userPassword> provide password for user </userPassword>
```

For **Complete Merge/Replace** import type, the system imports user records with nonSystem Administrator roles and automatically sets the password to `Avaya123$`. 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 does have 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 849. For sample XML file for import global settings, see Sample XML for bulk import of global setting records on page 855.

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 849.

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 859. For a sample XML

conforming to delete bulk global settings XML schema definition, see Sample XML for bulk deletion of users on page 770.

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 849.

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 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. Enter the date in the **Date** field.

      You can use the calender icon to select a date.

   c. Enter time in the **Time** field in the HH:MM:SS format.

   d. From 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

See XML Schema definitions and sample XMLs on page 177 for a list of XML Schema definitions and sample XML snippets for bulk import.

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
Select Import File Type	The type of the file from where you import the users. The options are: • XML • Excel
Select File	The path and name of the XML or Excel file from which you import the users. If you select the Excel file option, use the template that System Manager supports. You can download the template from **User Management** > **Manage Users** > **More Actions** > **Download Excel Template**. If a file type does not match, System Manager displays an error message.

Button	Description
Browse	Displays a dialog box to select the file from which you import the users.

General

Name	Description
Select Error Configuration	The options are: • **Abort on first error**: Aborts importing 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.
Select Import Type	The options are: • **Complete**: Imports users with all the user attributes. • **Partial**: Imports users with specific user attributes. **Select Import Type** is available only for imports using the XML file.

Table continues…

Name	Description
If a matching record already exists	The options are: • **Skip**: 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. **Note:** This option is not available if you select the **Partial** option in **Select Import Type**. • **Replace**: 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. **Note:** **Replace** is available only for imports using the XML file. • **Merge**: 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. • **Delete**: Deletes the user records from the database that match the records in the input file. **Note:** 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.

Job Schedule

Name	Description
Schedule Job	The options for configuring the schedule of the job: • **Run immediately**: Use this option to run the import job immediately. • **Schedule later**: Use this option to run the job at the specified date and time.

Table continues…

Name	Description
Date	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. This field is available when you select the **Schedule later** option for scheduling a job.
Time	The time of running the import users job. The time format is hh:mm:ss and 12 (AM or PM) or 24-hour format. This field is available when you select the **Schedule later** option for scheduling a job.
Time Zone	The time zone of your region. This field is available when you select the **Schedule later** option for scheduling a job.

Button	Description
Import	Imports or schedules the import operation based on the option you selected.

Manage Job

Name	Description
Select check box	Use this check box to select a job.
Scheduled Time	The time and date of scheduling the job.
Status	The current status of the job. The following are the different status of a job: 1. PENDING EXECUTION: The job is in queue. 2. RUNNING: The job execution is in progress. 3. SUCCESSFUL: The job execution is completed. 4. INTERRUPTED: The job execution is cancelled. 5. PARTIAL FAILURE: The job execution has partially failed. 6. FAILED: The job execution has failed.
Job Name	A link to the Scheduler user interface. You can also cancel the job from the Scheduler user interface.
% Complete	The job completion status in percentage.
User Records	The total user records in the input file.
Warnings	The number of user records in the input file with warnings.

Table continues…

Name	Description
Errors	The number of user records in the input file that failed to import.

Button	Description
View Job	Displays the details of the selected job.
Cancel Job	Cancels the import operation for the selected job. You can cancel a job that is in progress or queued for import.
Delete Job	Deletes the selected job.
Refresh	Refreshes the job information in the table.
Show	Provides you an option to view all the jobs on the same page. If the table displaying scheduled jobs are spanning multiple pages, select **All** to view all the jobs on a single page.
Select: All	Selects all the jobs in the table.
Select: None	Clears the check box selections.
Previous	Displays jobs in the previous page.
Next	Displays jobs in the next page.
Done	Navigates to the **User Management** page.

Import Users – Job Details field descriptions

The Import Users-Job Details page displays the details of the selected job.

Name	Description
Name	The import job that the end user initiates.
Scheduled by	The name of the user who initiates or schedules the import job
Scheduled at	The start time of the import job.
Error Configuration	The value that was configured for error while scheduling the Import Job. The values are **Abort on first error** and **Continue processing other records**.
Import Type	The value configured for the **Import Type** field while scheduling the import job. The values are **Complete** and **Partial**.
Import Option	The value that was configured for the **If a matching record already exists** field while scheduling the import job. The values are **Skip**, **Merge**, **Replace**, and **Delete**.

Table continues…

Name	Description
End	The end date and time of the job.
Status	The status of the job.
File	The name of the file that is used to import the user records.
Count	The total number of user records in the input file.
Success	The total number of user records that are successfully imported.
Fail	The total number of user records that failed to import.
Warning	The total number of user records that successfully imported, however, there are warnings generated for the user records.
Message	A message that indicates whether the import is successful or failure.
Completed	The percentage completion of the import.

Name	Description
Line Number	The line number in the file where the error occurred.
Login Name	The login name of the user record that failed to be imported.
Error Message	A brief description of the error.

Button	Description
Download	Exports and saves the user import error records in an XML file to the specified destination. **Note:** This button is not available if there are no error records for user Import Jobs or if the import job type is set to **Abort on first error**.
Cancel	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**.

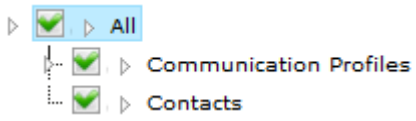
To navigate to the User bulk import configuration page from the System Manager console, click **Services** > **Configurations** > **Settings** > **SMGR** > **User BulkImport profile**.

Export Users field descriptions

Export File Type Options

Name	Description
Select Export File Types	The file type to which you want to export the users. The options are: • **Xml** • **Excel** • **Both**. You can select **Xml** and **Excel**. **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.

User Attribute Options

Name	Description
	User attribute options that an export administrator can choose to export for an export job. The options are: • **All**: The system exports all user attributes that includes all communications profiles and contacts. The default is **All**. • **Communications Profiles**: 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. • **Contacts**: The system exports all contacts. The system does not exports contacts if the check box is clear. **Note:** When you select the **Contacts** 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. **Important:** 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.

Delta Period options

The Delta Period Options section is available only if you select the **Export Delta Users** option.

Name	Description
Select the delta period	Following are the delta period options: • **One Day**: is exact past one day from current system date and time for run immediately or exact past one day from scheduled job time. • **One Week**: is exact past one week from current system date and time for run immediately or exact past one week from scheduled job time. • **One Month**: is exact past one month from current system date and time for run immediately or exact past one month from scheduled job time. **Note:** The system creates the `XML` and `Excel` 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 `XML` and `Excel` files contain zero users data. However, the system creates the `.txt` file only if there are any permanently deleted users in the specified delta period.

Schedule

Name	Description
Schedule Job	The settings to configure the schedule of the job. The options are: • **Run immediately**: To run the export job immediately. • **Schedule later**: To run the job at the specified date and time. **Note:** If you select the **Export All Users** or **Export Delta Users** option, and select the **Schedule Job** as **Schedule later**, the system displays the **Recurrence** and **Range** fields.
Date	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. This field is available when you select the **Schedule later** option for scheduling a job.

Table continues…

Name	Description
Time	The time of running the export job. The time format is hh:mm:ss and 12 (AM or PM) or 24–hour format. This field is available when you select the **Schedule later** option for scheduling a job.
Time Zone	The time zone of your region. This field is available when you select the **Schedule later** option for scheduling a job.

Table continues…

Name	Description
Recurrence	Following are the options: • **Execute task one time only**: The job is executed only once at the specified scheduled start time. • **Tasks are repeated**: The options are **Daily**, **Weekly**, and **Monthly**. The job is repeated as per the selection. **Note:** If you select the **Tasks are repeated**, the system enables the **Range** field. **Note:** The delta period selected for the **Export Delta Users** 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. 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 **One Day**, then the delta of users is identified from December 16, 2017 from 2.00 p.m. For recurrence jobs, if a job is configured to run multiple times then the last exported zip file with the name `<Scheduled Job Name>.zip` will be available on the Export Users page for download. However, the previously exported zip files will be stored in the `/var/avaya/bulkadministration/export/` directory with the name `<Scheduled Job_Date_time_In_UTC>.zip`. Where *Date_time_In_UTC* is the date and time in UTC when the file was last-updated or created in the last run of the job. 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 `/var/avaya/bulkadministration/export/` directory with following names: `users_1503066729239_18-Dec-2017_14:32:37_UTC.zip`, `users_1503066729239_19-`

Table continues…

Name	Description
	`Dec-2017_14:32:32_UTC.zip`, and `users_1503066729239.zip`.
Range	Following are the options: • **No End Date**: The job has no end date and executed as per the selection in the **Tasks are repeated** field. • **End After Occurrences**: The job is executed as per the selection in the **Tasks are repeated** field for the number of occurrences specified in **End After Occurrences**. • **End By Date**: The job is executed and the recurrence ends when the end date is reached.

Button	Description
Export	Exports or schedules the export job based on the option that you selected.

Export List

Name	Description
Select check box	The option to select a job.
Start Time	The date and time when the job was scheduled.
Status	The status of the job. The options are: • PENDING EXECUTION: The job is in queue. • RUNNING: The job execution is in progress. • SUCCESSFUL: The job execution is completed. • INTERRUPTED: The job execution is cancelled. • FAILED: The job execution has failed.
Scheduled Job	A key to the Scheduler page. You can cancel the job from the Scheduler page.
% Complete	The job completion status in percentage.
User Records	The total number of user records that are marked for export.
Failed Records	The number of user records that failed to export.
Download File	The link to download the zip file that contains XML and Excel files.

Button	Description
View	Displays the details of the selected job.

Table continues…

Button	Description
Stop	Stops the export operation for the selected job.
Delete	Deletes the job that you selected.
Refresh	Refreshes the job details.
Select: All	Selects all the jobs from the list.
Select: None	Clears the check box selections.
Previous	Displays jobs in the previous page.
Next	Displays jobs in the next page.
Done	Returns to the User Management page.

Job Details field descriptions

The Job Details page displays the details of the selected Job.

Name	Description
Name	Specifies the name of the import job.
Scheduled by	Name of the user who initiated or scheduled the import job.
Scheduled at	Start time of the scheduled job.
End	End date and time of the job.
Status	Status of the job.
File	Name of the file that is used to import the global user settings records.
Count	Total number of global user settings records in the input file.
Success	Total number of global user settings records that are successfully imported.
Fail	Total number of global user settings records that failed to import.
Message	The message that indicates whether the import is successful or failure.
Completed	Displays the percentage completion of the import.

Name	Description
Record Number	Failed XML element in the input XML file.
Name	Name of the failed XML element.
Error Message	A brief description of the error.

Button	Description
Cancel	Takes you back to the Import Users page.

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
Select File	The path and name of the XML file from which you must import the global settings records. If a file type does not match, System Manager displays an error message.

Button	Description
Browse	Opens a dialog box to select the file from which you must import the global user settings.

General

Name	Description
Select Error Configuration	The options are: • **Abort on first error**: Stops importing the global user settings records when User Management encounters the first error in the import file containing the global user settings records. • **Continue processing other records**: Imports the next global user settings record even if User Management encounters an error while importing a global user settings record.

Table continues…

Name	Description
If a matching record already exists	The options are: • **Skip**: 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. • **Merge**: 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. • **Replace**: 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. • **Delete**: Deletes the global setting records from the database that matches the records in the input XML file.

Job Schedule

Name	Description
Schedule Job	The settings for configuring the schedule of the job: • **Run immediately**: Use this option to run the import job immediately. • **Schedule later**: Use this option to run the job at the specified date and time.
Date	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. This field is available when you select the **Schedule later** option for scheduling a job.
Time	The time of running the import job. The time format is hh:mm:ss and 12 (AM or PM) or 24–hour format. This field is available when you select the **Schedule later** option for scheduling a job.
Time Zone	The time zone of your region. This field is available when you select the **Schedule later** option for scheduling a job.

Button	Description
Import	Imports or schedules the import operation based on the option you selected.

Manage Jobs

Name	Description
Select check box	Use this check box to select a job.
Scheduled Time	The date and time when the job was scheduled.
Status	The current status of the job. The following are the different status of a job: 1. PENDING EXECUTION: The job is in queue. 2. RUNNING: The job execution is in progress. 3. SUCCESSFUL: The job execution is completed. 4. INTERRUPTED: The job execution is cancelled. 5. PARTIAL FAILURE: The job execution has partially failed. 6. FAILED: The job execution has failed.
Job Name	A link to the Scheduler user interface. You can also cancel the job from the Scheduler user interface.
% Complete	The job completion status in percentage.
Records	The total number of global user settings records in the input file.
Error	The number of global user settings records in the input file that failed to import.

Button	Description
View Job	Shows the details of the selected job.
Cancel Job	Cancels the import operation for the selected job. You can cancel a job that is in progress or queued for import.
Delete Job	Deletes the selected job.
Refresh	Refreshes the job information in the table.
Show	Provides you an option to view all the jobs on the same page. If the table displaying scheduled jobs are spanning multiple pages, select **All** to view all the jobs on a single page.
Select: All	Selects all the jobs in the table.
Select: None	Clears the check box selections.
Previous	Displays jobs in the previous page.
Next	Displays jobs in the next page.
Done	Takes you back to the **User Management** page.

Table continues…

Button	Description
Cancel	Cancels the import operation and takes you back to the User Management page.

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 1: Minimal elements

UI field	Description	XML tag	Possible value

Authentication Type	Specifies the type of authentication.	`<authenticationType>`
		...
		`</ authenticationType>`
		>
			Basic or Enterprise

First Name	Specifies the first name of the user.	`<givenName>`
		...
		`</givenName>`
			First name of the user.

Login Name	Specifies the primary handle of user.	`<loginName>`
		...
		`</loginName>`
			User log-in name.

Last Name	Specifies the last name of the user.	`<surname>`
		...
		`</surname>`
			Last name of the user.

Login Password	Specifies the password used to log in to System Manager.	`<userPassword>`
		...
		`</userPassword>`
			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.

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 2: Mapping of Communication Profile for a new SIP user

UI field	Description	XML tag	Possible value
Name	Specifies the name of the communication profile.	`<commProfileSetName>` ... `</commProfileSetName>`	The unique name of this communication profile.
Default	Indicates whether this is a default profile.	`<isPrimary>` ... `</isPrimary>`	True or False.

The attributes to set up the communication address for a user are as follows:

Table 3: User attributes to set up communication address

UI field	Description	XML tag	Possible value
Handle	Specifies the extension number of the user.	`<handleName>` ... `</handleName>`	Extension number.
Type	Specifies the communication type of the user profile.	`<handleType>` ... `</handleType>`	Communication type. For example, sip and smtp.
SubType	Specifies the communication subtype of the user profile.	`<handleSubType>` ... `</handleSubType>`	Communication sub type. For example, username, e164, and msrtc.
Domain	Specifies the domain name of the user.	`<domainName>` ... `</domainName>`	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 4: Mapping of Session Manager Communication Profile elements

UI field	Description	XML tag	Possible value
Primary Session Manager	Specifies the name of the primary Session Manager instance that is used as the home server for a communication profile.	`<sm:primarySM>` ... `</sm:primarySM>`	Enter the name of Session Manager.

Table continues…

UI field	Description	XML tag	Possible value
Origination Application Sequence	Specifies the Application Sequence that is invoked when calls are routed from this user.	<sm:originationAppSequence> ... </sm:originationAppSequence>	True or False.
Termination Application Sequence	Specifies the Application Sequence that is invoked when calls are routed to this user.	<sm:terminationAppSequence> ... </sm:terminationAppSequence>	
Emergency Origination Application Sequence	Specifies the emergency application sequence that is invoked when calls are routed from this user.	<ns6:emergencyOriginationAppSequence>appedpseq</ns6:emergencyOriginationAppSequence>	
Emergency Termination Application Sequence	Specifies the emergency application sequence that is invoked when calls are routed to this user.	<ns6:emergencyTerminationAppSequence>appedpseq</ns6:emergencyTerminationAppSequence>	
Home Location	Specifies the routing home location.	<sm:homeLocation> ... </sm:homeLocation>	

The following is the mapping of CM Endpoint Profile elements with the corresponding user interface fields.

Table 5: Mapping of CM Endpoint Profile elements

UI field	Description	XML tag	Possible value
System	Specifies the SIP Entity of the Communication Manager.	<ipt:cmName> ... </ipt:cmName>	Name of the configured Communication Manager.
Use Existing	Indicates whether the station is already defined in the system.	<ipt:useExistingExtension> ... </ipt:useExistingExtension>	True or False.
Extension	Specifies the extension number for this profile.	<ipt:extension> ... </ipt:extension>	

Table continues…

UI field	Description	XML tag	Possible value
Template	Specifies the template name used for creating the station.	<ipt:template> ... </ipt:template>	
Set Type	Specifies the set type of the station.	<ipt:setType> ... </ipt:setType>	
Port	Specifies the port number from the list for the template you select.	<ipt:port> ... </ipt:port>	

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>
```

New User Profile field descriptions

Use the New User Profile page to create 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
Tenant	The name of the tenant that you must select.
Level 1	The name of the level 1 hierarchy of the tenant organization. For example, Site. The tenant administrator provides the hierarchy on the Tenant Management page.
Level 2	The name of the level 2 hierarchy of the tenant organization. For example, Department.
Level 3	The name of the level 3 hierarchy of the tenant organization. For example, Team.

User Provisioning Rule

Name	Description
User Provisioning Rule	The name of the 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.

Identity tab: Identity

Name	Description
Last Name	The last name of the user. For example, Miller.
Last Name (Latin Translation)	The user-preferred last name that the system must display on the end points. For example, Miller. Typically, the name is the written or spoken language of the user. **Note:** When you create a user, if the **Last Name (Latin Translation)** and **First Name (Latin Translation)** fields are: • Blank, the system displays the last name and first name in the fields. The values change when the last name and first names change. • Filled, the values remain even after you change the values in the **Last Name** and **First Name** fields.
First Name	The first name of the user. For example, John.
First Name (Latin Translation)	The user-preferred first name that the system must display on the end points. For example, John. Typically, the name is the written or spoken language of the user.
Middle Name	The middle name of the user, if any.
Description	A brief description about the user.

Table continues…

Name	Description
Login Name	The login name of the user. 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 JMILLER@AVAYA.COM or jmiller@avaya.com. The login name can be in uppercase or lowercase. If you log in to the system as admin, you cannot edit the login name. **Note:** 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.
User Type	The authentication type that defines how the system performs the authentication of the user. The options are: • **Enterprise**: Directory servers that are external to System Manager authenticate the user login. • **Basic**: Avaya authentication service authenticates the user login. For bulk import of users by using Excel, **User Type** is always Basic. Therefore, the **User Type** field remains invisible in the Excel file.
Password	The password to log in to the System Manager web console.
Confirm Password	The password that you reenter for confirmation.
Localized Display Name	The localized display name of a user. The name is typically the localized full name.
Endpoint Display Name	The full text name of the user represented in ASCII. The display name supports displays that cannot handle localized text, for example, some endpoints.
Title	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.
Language Preference	The preferred written or spoken language of the user. For example, English.

Table continues…

Name	Description
Time Zone	The preferred time zone of the user. For example, (+05:30) Chennai, Kolkata, Mumbai, New Delhi.
Employee ID	The employee number for the user. For example, 20081234.
Department	The department to which the user belongs. For example, Human Resources.
Company	The organization where the user works. For example, Avaya Inc.

Identity tab: Address

Name	Description
Select check box	The option to select an address in the table.
Name	The name of the addressee. For example, Avaya.
Address Type	The type of address. The values are: • **Office** • **Home**
Street	The name of the street. For example, Magarpatta.
City	The name of the city or town. For example, Pune.
Postal Code	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.
Province	The full name of the province. For example, Maharashtra.
Country	The name of the country. For example, India.

Button	Description
New	Displays the Add Address page. Use the page to add the address details.
Edit	Displays the Edit Address page. Use the page to modify the address.
Delete	Deletes the selected address.
Choose Shared Address	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. The section does not apply for Session Manager and Communication Manager.

Name	Description
Language	The localized languages for displaying the user name. For example, English. You must select the language.
Display Name	The user name in the localized language you choose. For example, John Miller.

Button	Description
New	Displays fields that you can use to create a new localized name for the user.
Edit	Displays fields that you can use to modify the localized name for the user.
Delete	Deletes the localized names that you select for the user.
Add	Adds or edits the localized name for the user.
Cancel	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
Communication Profile Password	The communication profile password. The field is available only if you enable the communication profile. The password policy is configured from **Users** > **User Management** > **Communication Profile Password Policy**. When communication password value is provided during bulk edit of users, the system overwrites any existing communication profile passwords of the user.
Confirm Password	The communication profile password that you reenter for confirmation.
Option button	The option to view the details of the selected communication profile.
Name	The name of the communication profile. You must select the name.

Button	Description
New	Creates a new communication profile for the user.
Delete	Deletes the selected communication profile.

Table continues…

Button	Description
Done	Saves the communication profile information that you updated or added for a profile.
Cancel	Cancels the operation for adding of a communication profile.

The system enables the following fields when you click **New** in the **Communication Profile** section.

Name	Description
Name	The name of the communication profile for the user.
Default	The option to select a profile as default or the active profile. At a time, only one active profile can exist.

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
Type	The type of the handle.
Handle	A unique communication address of the user. From Communication Manager Release 7.1.2, alphanumeric handles are also supported.
Domain	The name of the domain with which the handle is registered.

Button	Description
New	The fields for adding a new communication address.
Edit	The button to edit the information of a selected communication address.
Delete	Deletes the selected communication address.

The page displays the following fields when you click **New** and **Edit** in the Communication Address section. The following fields define the communication address for the user.

Name	Description
Type	The type of the handle. The different types of handles are: • **Avaya SIP**: Indicates that the handle supports Avaya SIP-based communication. • **Avaya E.164**: Indicates that the handle refers to an E.164 formatted address. E.164 numbers can have a maximum of fifteen digits and are usually written with a + prefix. • **Microsoft SIP**: Indicates that the handle supports SIP-based communication. • **Microsoft Exchange**: Indicates that the handle is an email address and supports communication with Microsoft SMTP server. • **Lotus Notes**: Indicates that the handle is for Lotus Notes and domino calender. • **IBM Sametime**: Indicates that the handle is for IBM Sametime. The address must be in the DN=IBMHandle format. • **Avaya Presence/IM**: 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. **Note:** To create the Presence communication profile, you must select **Avaya Presence/IM** and provide the communication address. • **GoogleTalk**: Indicates that the handle supports XMPP-based communication with the Google Talk service. • **Other Email**: Indicates that the handle is an email address other than MS Exchange email addresses. • **Other SIP**: Indicates that the handle supports SIP-based communication other than the listed ones. • **Other XMPP**: Indicates that the handle supports XMPP-based communication other than the listed ones.

Table continues…

Name	Description
	• **Work Assignment**: Indicates that the handle supports accounts which can be assigned to an agent for Work Assignment.
Fully Qualified Address	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
Add	Saves the new communication address or modified communication address information in the database.
Cancel	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
Primary Session Manager	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® network. You must select the primary Session Manager server.
Secondary Session Manager	The Session Manager instance that you select as the secondary Session Manager 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
Survivability Server	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. **Note:** 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.
Max. Simultaneous Devices	The maximum number of endpoints that you can register at a time using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.
Block New Registration When Maximum Registrations Active	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. 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 completes.

Table continues…

Name	Description
Origination Application Sequence	The application sequence that the system will invoke when routing the calls from this user. A selection is optional. **Note:** 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.
Termination Application Sequence	The application sequence that will be invoked when the system routes the calls to this user. A selection is optional. **Note:** 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.
Emergency Calling Origination Sequence	The list of application sequences invoked when the system routes emergency call from this user.
Emergency Calling Termination Sequence	The list of application sequences invoked when the system routes emergency call to this user.
Home Location	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 of the location. You must specify a value.
Conference Factory Set	The conference factory set to enable media capability-based call routing to the Conferencing SIP entities. Use the **Session Manager** > **Application Configuration** > **Conference Factories** webpage to administer the Conference Factory Sets.
Enable Centralized Call History	The option to enable the call history feature for SIP users. By default, the system disables the call history feature. The maximum number of call logs per communication profile is 100.

Communication Profile tab: Avaya Breeze™ Profile

Name	Description
Service Profile	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.

Field/Button	Description
System	The Communication Manager system on which you add the endpoint. You must select the system.
Profile Type	The type of the Communication Manager Endpoint profile that you create. You must select the profile type.
Use Existing Endpoints	Select the check box to use the existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions.
Extension	The extension of the endpoint that you associate this profile with. You must select the extension. The field lists the endpoints, existing or available, based on the option you selected in the **Use Existing Endpoints** check box.
Endpoint Editor button	Click to start the Communication Manager application where you can edit or view details of the endpoint. After you save the changes in Communication Manager, the system does not update the modified data on the device or database until you commit the changes on the User Profile Edit page.
Template	The template, system defined or user defined, that you associate with the endpoint. Select the template based on the set type you add. You must select the template.
Set Type	The set type of the endpoint you associate with. When you select a template, the system populates the corresponding set types.
Security Code	The security code for authorized access to the endpoint.

Table continues…

Field/Button	Description
Port	The relevant port for the set type you select. You must select the port. The field lists the possible ports based on the selected set type.
Voice Mail Number	The voice mail number of the endpoint you associate with. **Note:** You must clear Local Device Services Data on all Avaya Aura® Web Gateway nodes in case of changing the value of **Voice Mail Number**.
Preferred Handle	Numeric only handles, SIP handles, or nonSIP handles, that are administered for a user. The **Preferred Handle** field is optional. Select numeric handle for alphanumeric support. By default, the field is blank. If the type of the SIP entity is Communication Manager, Session Manager uses preferred handle in CM Endpoint profile.
Calculate Route Pattern	The option to automatically select the route pattern based on the primary or secondary Session Manager configured in **Session Manager Communication Profile**.
Sip Trunk	The system makes this field available only for the SIP set type. If you select **Calculate Route Pattern** check box, the system: • Populates the **Sip Trunk** field • Makes the **Sip Trunk** field read-only.
Attendant	When you select the 9641SIP template type from **Template**, the system enables the **Attendant** check box. The option to enable the attendant feature on the endpoint. If you select this check box, you can administer the endpoint as an attendant.

Table continues…

Field/Button	Description
Enhanced Callr-Info display for 1–line phones	The option to activate the enhanced Callr-info operation on the phone. The **Enhanced Callr-Info display for 1-line phones** field on the station form is valid for the following set types: • 1603, 1608, 1616, 1408, 1416 • 2402, 2410, 2420 • 4606, 4612, 4612CL, 4624, 4602, 4602+, 4630, 4610, 4622, 4620, 4621, 4625, • 6402D, 6408D, 6408D+, 6416D+, 6424D+, 607A1 • 7506D, 7507D • 8405D+, 8410D, 8405D, 8411D • 9404, 9408, 9601, 9601+, 9610, 9620, 9621, 9608, 9611, 9630, 9640, 9641, 9650 The valid options are: • **No**: Does not change the callr-info interactions with the connected phone. The default setting. • **Yes**: 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 **callr-info** button is not assigned to the phone on the station form, **Enhanced Callr-Info display for 1-line phones** does not apply.
Delete Endpoint on Unassign of Endpoint from User or on Delete User	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 when you delete the user.

Table continues…

Field/Button	Description
Override Endpoint Name and Localized Name	The option to override the following endpoint names: • The endpoint name on Communication Manager with the value you configured on the Manage users page during synchronization. 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. • The localized display name on the Manage Users page in the **Localized Display Name** field of Communication Manager. If you clear the check box, the system does not override the localized display name in the **Localized Display Name** field.
Allow H.323 and SIP Endpoint Dual Registration	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 *Avaya Aura® Communication Manager Feature Description and Implementation* on the Avaya Support website at http://support.avaya.com.

Communication Profile tab: CS 1000 Endpoint Profile

Name	Description
System	The system that will be the element manager of the CS 1000 endpoint profile. You must select the system.
Add new	The option to create a new phone.
Target	The system customer number for the CS 1000 system. You must select the target. The system displays the field only when you select **Add new**.
Template	The phone or endpoint template that you can choose for the user. The element manager maintains all templates. You must select a template. The system displays the field only when you select **Add new**.
Update	Updates the station profile information for the user. When you click **Update**, the system takes you to the element manager cut-through for the updates.

Table continues…

Name	Description
Service Details	The service details of endpoints, such as set type, after phone creation.
Primary DN	The primary directory number of the phone. You can enter only numeric values for this field. The system displays the field only when you select **Add new**.
Terminal Number	The terminal number of the phone. The system displays the field only when you select **Add new**.
Link existing	The option to associate with the existing phone.
Existing TN	The terminal number from the list of existing numbers. The system displays the field only when you select **Link existing**.
Include in Corporate Directory	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
System	The messaging system on which you add the subscriber. You must select the system.
Use Existing Subscriber on System	The option to specify whether to use an existing subscriber mailbox number to associate with this profile.
Mailbox Number	The mailbox number of the subscriber. You must select the mailbox number. The field takes the existing mailbox number that you associate with this profile. This value in the field is valid only if you select the **Use Existing Subscriber on System** check box.
Messaging Editor	Click to start the Messaging application where you can edit or view details of the profile of the messaging endpoint. 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 page.

Table continues…

Name	Description
Template	The system-defined or user-defined template that you associate with the subscriber.
Password	The password for logging in to the mailbox. You must provide the password.
Delete Subscriber on Unassign of Subscriber from User or on Delete User	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: Officelinx Profile

Name	Description
Officelinx System	The Officelinx system to which you add a mailbox.
Refresh	Gets the information about company, departments, and feature groups from Officelinx and saves locally on System Manager for future use. You do not require to refresh for every user.
Mailbox Number	The mailbox number of the subscriber.
Numeric Password	The numeric password that is used to log in to the Officelinx system.
Confirm Numeric Password	The numeric password that you retype to confirm.
Application User Password	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.
Confirm Application User Password	The password that you retype to confirm.
Company	The name of the company to which the user belongs.
Department	The department to which the user belongs.
Feature Group	The feature group name that determines the rules for the mailboxes associated with it.
Capability	The type of functionality that the user contains. The values are: • **Standard** • **Fax** • **Messaging** • **Collaboration** • **Messaging and Collaboration**
Domain Account Name	The mailbox NT account name for the Officelinx profile.

Table continues…

Name	Description
Synchronization User Name	The account name that is used to gain access to the email server, for example, Microsoft Exchange and Google Gmail.

Communication Profile tab: CallPilot Messaging Profile

Name	Description
System	The CallPilot system to which you add a mailbox. You must select the system.
Target	The field that maps to the CallPilot **Location** field. CallPilot Manager provides the **Target** field. You must select the target.
Template	The mailbox template that you use. Select a template from the drop down list. The element manager maintains all the mailbox templates. You must select the template.
Update	Updates the mailbox information for the user. If you click the **Update** button, the system cuts through to the element manager for the updates.
Service Details	Displays mailbox service details from the endpoint after you create the mailbox.
Mailbox Number	The mailbox number or the extension DN of the user. You must select the mailbox number.

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.

Field/Button	Description
System	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.

Table continues…

Field/Button	Description
Template	The list of user templates from which you can select your preferred template to set the user configurations. You must select the template.
Use Existing Extension	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.
Extension	The extension of the endpoint you associate with. You must select the extension. The field lists the endpoints, existing or available, based on the option you selected in the **Use Existing Endpoints** check box.
Endpoint Editor	Starts the IP Office application where you can edit or view the details of the IP Office endpoint. 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 page.
Module-Port	The module port combination list for IP Office analog extensions. You must select **Module-Port** for centralized users with Set Type as **Analog**.
Set Type	The set type for the IP Office endpoint profile. By default, the **Set Type** field is disabled. If you select a template, the system populates the set type.
Delete Extension On User Delete	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 **Analog** and **Digital** set types.

Communication Profile tab: Equinox Conferencing

Name	Description
Equinox User Password	The Equinox user password.
Virtual Room Number	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
System	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: • Aggregate presence • Archive instant messages if the Instant Messages option is enabled
SIP Entity	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 **System** field. **SIP Entity** is read-only. If the system cannot identify a SIP entity, an appropriate error message is displayed in the field.
IM Gateway SIP Entity	The Presence Services instance for the user.
Publish Presence with AES Collector	The option that determines if Presence Services must publish presence with AES Collector. The options are: • **System Default** • **Off** • **On** The default is **System Default**. 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
Select Auto-generated Code Length	The number of characters in PIN. The default is 6. The system displays this field if you select the **Auto Generate Participant and Moderator Security Code** check box.
Auto Generate Participant and Moderator Security Code	Select the check box if the system must generate the participant security code and moderator security code for this user. Clear the check box to assign a specific participant security code or moderator security code for this user.

Table continues…

Name	Description
Participant Security Code	The participant security code that you assign for this user. The system displays this field only when the **Auto Generate Participant and Moderator Security Code** check box is clear.
Moderator Security Code	The moderator security code that you assign for this user. The system displays this field if the **Auto Generate Participant and Moderator Security Code** check box is clear.
Location	The location of the user. This field is mandatory for non-SIP users without a Session Manager profile and optional for SIP users. For SIP users, the system uses the location value from the **Home Location** field in the Session Manager profile.
Template	The Conferencing template that you assign to this user.

Button	Description
Get Templates	Displays the list of Conferencing templates, which you can assign to this user.

Communication Profile tab: Work Assignment Profile

Name	Description
Account	The account name.
Account Address	The account address.
Source	The source name.
Source Address	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
Resource Details	Displays the Assignment Management page where you can configure assignment targets for the user. 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
Account Details	Displays the text box where you can add or modify the account name and account address. You can add attributes to the account only when the account is added to the agent.
Source Details	Displays the text box where you can add or modify the source name and source address. 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.
Presence Buddy	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
Edit	Displays the Edit Contact List Member page. Use this page to modify the information of the selected contact.
Add	Displays the Attach Contacts page. Use this page to select one or more contacts from the list of contacts. 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
Remove	Removes one or more selected contacts from the list of the associated contacts.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.
Filter: Enable	Displays the text fields under the columns that you can use to set the filter criteria. **Filter: Enable** is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Contacts tab: Private Contacts

Use this section to add new private contacts, and edit and delete the existing contacts.

Name	Description
Last Name	The last name of the private contact.
First Name	The first name of the private contact.
Display Name	The display name of the private contact.
Contact Address	The address of the private contact.
Description	A brief description about the contact.

Button	Description
Edit	Displays the Edit Private Contact page. Use this page to edit the information of the contact you selected.
New	Displays the **New Private Contact** page. Use this page to add a new private contact.
Delete	Deletes the selected contacts.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.
Filter: Enable	Displays text fields under the columns that you can use to set the filter criteria. **Filter: Enable** is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Common buttons

Button	Description
Commit & Continue	Creates the user account in the database and retains you on the same page for further modifications.
Commit	Creates the user account and takes you to the User Management page.
Cancel	Cancels the user creation operation.

Related links

Adding users on page 115

User Profile Edit field descriptions

Organization

Name	Description
Tenant	The name of the tenant that you must select.

Table continues…

Name	Description
Level 1	The name of the level 1 hierarchy of the tenant organization. For example, Site. The tenant administrator provides the hierarchy on the Tenant Management page.
Level 2	The name of the level 2 hierarchy of the tenant organization. For example, Department.
Level 3	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
User Provisioning Rule	The user provisioning rule that you must edit.

Identity tab — Identity section

Name	Description
Last Name	The last name of the user. For example, Miller.
Last Name (Latin Translation)	The user-preferred last name that the system must display on the end points. For example, Miller. Typically, the name is the written or spoken language of the user. **Note:** When you create a user, if the **Last Name (Latin Translation)** and **First Name (Latin Translation)** fields are: • Blank, the system displays the last name and first name in the fields. The values change when the last name and first names change. • Filled, the values remain even after you change the values in the **Last Name** and **First Name** fields.
First Name	The first name of the user. For example, John.

Table continues…

Name	Description
First Name (Latin Translation)	The user-preferred first name that the system must display on the end points. For example, John. Typically, the name is the written or spoken language of the user.
Middle Name	The middle name of the user, if any.
Description	A brief description about the user.
Status	The login status of the user
Update Time	The time when the user details were last modified.
Login Name	The login name of the user. 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 JMILLER@AVAYA.COM or jmiller@avaya.com. The login name can be in uppercase or lowercase. If you log in to the system as admin, you cannot edit the login name. **Note:** 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.
Email Address	The email address of the user
User Type	The authentication type that defines how the system performs the authentication of the user. The options are: • **Enterprise**: Directory servers that are external to System Manager authenticate the user login. • **Basic**: Avaya authentication service authenticates the user login. For bulk import of users by using Excel, **User Type** is always Basic. Therefore, the **User Type** field remains invisible in the Excel file.
Change Password	Displays two new fields: **New Password** and **Confirm Password**.

Table continues…

Name	Description
New Password	The new password to log in to the System Manager web console.
Confirm Password	The password that you reenter for confirmation.
Source	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.
Localized Display Name	The localized display name of a user. The name is typically the localized full name.
Endpoint Display Name	The full text name of the user represented in ASCII. The display name supports displays that cannot handle localized text, for example, some endpoints.
Title	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.
Language Preference	The preferred written or spoken language of the user. For example, English.
Time Zone	The preferred time zone of the user. For example, (+05:30) Chennai, Kolkata, Mumbai, New Delhi.
Employee ID	The employee number for the user. For example, 20081234.
Department	The department to which the user belongs. For example, Human Resources.
Company	The organization where the user works. For example, Avaya Inc.

Identity tab — Address section

Name	Description
Time Zone	The preferred time zone of the user. For example, (+05:30) Chennai, Kolkata, Mumbai, New Delhi.
Department	The department to which the user belongs. For example, Human Resources.
Address Type	The type of address. The values are: • **Office** • **Home**
Street	The name of the street. For example, Magarpatta.
City	The name of the city or town. For example, Pune.
Postal Code	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.

Table continues…

Name	Description
Province	The full name of the province. For example, Maharashtra.
Country	The name of the country. For example, India.

Button	Description
New	Displays the Add Address page. Use the page to add the address details.
Edit	Displays the Edit Address page. Use the page to modify the address.
Delete	Deletes the selected address.
Choose Shared Address	Displays the Choose Address where you choose a shared or common address.

Identity tab — Localized Names section

Name	Description
Language	The localized languages for displaying the user name. For example, English. You must select the language.
Display Name	The user name in the localized language you choose. For example, John Miller.

Button	Description
New	Displays fields that you can use to create a new localized name for the user.
Edit	Displays fields that you can use to modify the localized name for the user.
Delete	Deletes the localized names that you select for the user.
Add	Adds or edits the localized name for the user.
Cancel	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
Calculate Route Pattern	The option to automatically select the route pattern based on the primary or secondary Session Managerconfigured in the **Session Manager Communication Profile**.

Table continues…

Name	Description
Sip Trunk	The system makes this field available only for the SIP set type. If you select the **Calculate Route Pattern** check box, the system populates the **Sip Trunk** field, and makes the field read-only.
Allow H.323 and SIP Endpoint Dual Registration	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 *Avaya Aura® Communication Manager Feature Description and Implementation* on the Avaya Support website at http://support.avaya.com.

Button	Description
New	Creates a new communication profile for the user.
Delete	Deletes the selected communication profile.
Done	Saves the communication profile information that you updated or added for a profile.
Cancel	Cancels the operation for adding of a communication profile.

The system enables the following fields when you click **New** in the Communication Profile section.

Name	Description
Name	The name of the communication profile for the user.
Default	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
Type	The type of the handle.
Handle	A unique communication address of the user. From Communication Manager Release 7.1.2, alphanumeric handles are also supported.
Domain	The name of the domain with which the handle is registered.

Button	Description
New	The fields for adding a new communication address.

Table continues…

Button	Description
Edit	The button to edit the information of a selected communication address.
Delete	Deletes the selected communication address.

The page displays the following fields when you click **New** or **Edit** in the Communication Address section.

Name	Description
Type	The type of the handle. The different types of handles are: • **Avaya SIP**: Indicates that the handle supports Avaya SIP-based communication. • **Avaya E.164**: Indicates that the handle refers to an E.164 formatted address. E.164 numbers can have a maximum of fifteen digits and are usually written with a + prefix. • **Microsoft SIP**: Indicates that the handle supports SIP-based communication. • **Microsoft Exchange**: Indicates that the handle is an email address and supports communication with Microsoft SMTP server. • **Lotus Notes**: Indicates that the handle is for Lotus Notes and domino calender. • **IBM Sametime**: Indicates that the handle is for IBM Sametime. The address must be in the DN=IBMHandle format. • **Avaya Presence/IM**: 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. **Note:** To create the Presence communication profile, you must select **Avaya Presence/IM** and provide the communication address. • **GoogleTalk**: Indicates that the handle supports XMPP-based communication with the Google Talk service. • **Other Email**: Indicates that the handle is an email address other than MS Exchange email addresses. • **Other SIP**: Indicates that the handle supports SIP-based communication other than the listed ones. • **Other XMPP**: Indicates that the handle supports XMPP-based communication other than the listed ones.

Table continues…

Name	Description
	• **Work Assignment**: Indicates that the handle supports accounts which can be assigned to an agent for Work Assignment.
Fully Qualified Address	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
Add	Saves the new communication address or modified communication address information in the database.
Cancel	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
Primary Session Manager	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® network. You must select the primary Session Manager server.
Secondary Session Manager	The Session Manager instance that you select as the secondary Session Manager 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
Survivability Server	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. **Note:** 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.
Max. Simultaneous Devices	The maximum number of endpoints that you can register at a time using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.
Block New Registration When Maximum Registrations Active	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.
Origination Application Sequence	The application sequence that the system will invoke when routing the calls from this user. A selection is optional. **Note:** 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.

Table continues…

Name	Description
Termination Application Sequence	The application sequence that will be invoked when the system routes the calls to this user. A selection is optional. **Note:** 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.
Home Location	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 of the location. You must specify a value.
Conference Factory Set	The conference factory set to enable media capability-based call routing to the Conferencing SIP entities. Use the **Session Manager** > **Application Configuration** > **Conference Factories** webpage to administer the Conference Factory Sets.

Communication Profile tab: Avaya Breeze™ Profile

Name	Description
Service Profile	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
System	The Communication Manager system on which you add the endpoint. You must select the system.
Profile Type	The type of the Communication Manager Endpoint profile that you create. You must select the profile type.
Use Existing Endpoints	Select the check box to use 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
Extension	The extension of the endpoint that you associate this profile with. You must select the extension. The field lists the endpoints, existing or available, based on the option you selected in the **Use Existing Endpoints** check box.
Template	The template, system defined or user defined, that you associate with the endpoint. Select the template based on the set type you add. You must select the template.
Set Type	The set type of the endpoint you associate with. When you select a template, the system populates the corresponding set types.
Security Code	The security code for authorized access to the endpoint.
Port	The relevant port for the set type you select. You must select the port. The field lists the possible ports based on the selected set type.
Voice Mail Number	The voice mail number of the endpoint you associate with. **Note:** You must clear Local Device Services Data on all Avaya Aura® Web Gateway nodes in case of changing the value of **Voice Mail Number**.
Preferred Handle	Numeric only handles, SIP handles, or nonSIP handles, that are administered for a user. The **Preferred Handle** field is optional. Select numeric handle for alphanumeric support. By default, the field is blank. If the type of the SIP entity is Communication Manager, Session Manager uses preferred handle in CM Endpoint profile.
Attendant	When you select the 9641SIP template type from **Template**, the system enables the **Attendant** check box. The option to enable the attendant feature on the endpoint. If you select this check box, you can administer the endpoint as an attendant.

Table continues…

Name/Button	Description
Enhanced Callr-Info display for 1–line phones	The option to activate the enhanced Callr-info operation on the phone. The **Enhanced Callr-Info display for 1-line phones** field on the station form is valid for the following set types: • 1603, 1608, 1616, 1408, 1416 • 2402, 2410, 2420 • 4606, 4612, 4612CL, 4624, 4602, 4602+, 4630, 4610, 4622, 4620, 4621, 4625, • 6402D, 6408D, 6408D+, 6416D+, 6424D+, 607A1 • 7506D, 7507D • 8405D+, 8410D, 8405D, 8411D • 9404, 9408, 9601, 9601+, 9610, 9620, 9621, 9608, 9611, 9630, 9640, 9641, 9650 The valid options are: • **No**: Does not change the callr-info interactions with the connected phone. The default setting. • **Yes**: 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 **callr-info** button is not assigned to the phone on the station form, **Enhanced Callr-Info display for 1-line phones** does not apply.
Delete Endpoint on Unassign of Endpoint from User or on Delete User	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 when you delete the user.

Table continues…

Name/Button	Description
Override Endpoint Name and Localized Name	The option to override the following endpoint names: • The endpoint name on Communication Manager with the value you configured on the Manage users page during synchronization. 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. • The localized display name on the Manage Users page in the **Localized Display Name** field of Communication Manager. If you clear the check box, the system does not override the localized display name in the **Localized Display Name** field.

Communication Profile tab - CS1000 Endpoint Profile

Field	Description
System	The system that will be the element manager of the CS 1000 endpoint profile. You must select the system.
Target	The system customer number for the CS 1000 system. You must select the target. The system displays the field only when you select **Add new**.
Template	The phone or endpoint template that you can choose for the user. The element manager maintains all templates. You must select a template. The system displays the field only when you select **Add new**.
Update	Updates the station profile information for the user. When you click **Update**, the system takes you to the element manager cut-through for the updates.
Service Details	The service details of endpoints, such as set type, after phone creation.
Primary DN	The primary directory number of the phone. You can enter only numeric values for this field. The system displays the field only when you select **Add new**.
Include in Corporate Directory	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
System	The messaging system on which you add the subscriber. You must select the system.
Use Existing Subscriber on System	The option to specify whether to use an existing subscriber mailbox number to associate with this profile.
Mailbox Number	The mailbox number of the subscriber. You must select the mailbox number. The field takes the existing mailbox number that you associate with this profile. This value in the field is valid only if you select the **Use Existing Subscriber on System** check box.
Messaging Editor	Click to start the Messaging application where you can edit or view details of the profile of the messaging endpoint. 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 page.
Template	The system-defined or user-defined template that you associate with the subscriber.
Password	The password for logging in to the mailbox. You must provide the password.
Delete Subscriber on Unassign of Subscriber from User or on Delete User	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: Officelinx Profile

Name	Description
Officelinx System	The Officelinx system to which you add a mailbox.
Refresh	Gets the information about company, departments, and feature groups from Officelinx and saves locally on System Manager for future use. You do not require to refresh for every user.
Mailbox Number	The mailbox number of the subscriber.

Table continues…

Name	Description
Numeric Password	The numeric password that is used to log in to the Officelinx system.
Confirm Numeric Password	The numeric password that you retype to confirm.
Application User Password	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.
Confirm Application User Password	The password that you retype to confirm.
Company	The name of the company to which the user belongs.
Department	The department to which the user belongs.
Feature Group	The feature group name that determines the rules for the mailboxes associated with it.
Capability	The type of functionality that the user contains. The values are: • **Standard** • **Fax** • **Messaging** • **Collaboration** • **Messaging and Collaboration**
Domain Account Name	The mailbox NT account name for the Officelinx profile.
Synchronization User Name	The account name that is used to gain access to the email server, for example, Microsoft Exchange and Google Gmail.

Communication Profile tab - CallPilot Messaging Profile

Field	Description
System	The CallPilot system of the messaging profile you edit. The selection is required.
Target	The field that maps to the CallPilot **Location** field. CallPilot Manager provides the **Target** field. You must select the target.
Template	The mailbox template that you use. Select a template from the drop down list. The element manager maintains all the mailbox templates. You must select the template.
Update	Updates the mailbox information for the user. If you click the **Update** button, the system cuts through to the element manager for the updates.

Table continues…

Field	Description
Service Details	Displays mailbox service details from the endpoint after you create the mailbox.
Mailbox Number	The mailbox number or the extension DN of the user. You must select the mailbox number.

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
System	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.
Template	The list of user templates from which you can select your preferred template to set the user configurations.
Use Existing Extension	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.
Extension	The extension of the endpoint you associate with. You must select the extension. The field lists the endpoints, existing or available, based on the option you selected in the **Use Existing Endpoints** check box.

Table continues…

Name/Button	Description
Endpoint Editor button	The option to start the IP Office application, where you can edit or view the details of the IP Office endpoint. 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 page.
Module-Port	The module port combination list for IP Office analog extensions. You must select **Module-Port** for centralized users with Set Type as **Analog**.
Set Type	The set type for the IP Office endpoint profile. By default, the **Set Type** field is disabled. If you select a template, the system populates the set type.
Delete Extension On User Delete	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 **Analog** and **Digital** set types.

Communication Profile tab: Equinox Conferencing

Name	Description
Equinox User Password	The Equinox user password.
Virtual Room Number	The virtual room number of the Equinox user.

Communication Profile tab — Presence Profile

Name	Description
System	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: • Aggregate presence • Archive instant messages if the Instant Messages option is enabled
SIP Entity	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 **System** field. **SIP Entity** is read-only. If the system cannot identify a SIP entity, an appropriate error message is displayed in the field.

Table continues…

Name	Description
IM Gateway SIP Entity	The Presence Services instance for the user.
Publish Presence with AES Collector	The option that determines if Presence Services must publish presence with AES Collector. The options are: • **System Default** • **Off** • **On** The default is **System Default**. 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
Select Auto-generated Code Length	The number of characters in PIN. The default is 6. The system displays this field if you select the **Auto Generate Participant and Moderator Security Code** check box.
Auto Generate Participant and Moderator Security Code	Select the check box if the system must generate the participant security code and moderator security code for this user. Clear the check box to assign a specific participant security code or moderator security code for this user.
Participant Security Code	The participant security code that you assign for this user. The system displays this field only when the **Auto Generate Participant and Moderator Security Code** check box is clear.
Moderator Security Code	The moderator security code that you assign for this user. The system displays this field if the **Auto Generate Participant and Moderator Security Code** check box is clear.
Location	The location of the user. This field is mandatory for non-SIP users without a Session Manager profile and optional for SIP users. For SIP users, the system uses the location value from the **Home Location** field in the Session Manager profile.
Template	The Conferencing template that you assign to this user.

Button	Description
Get Templates	Displays the list of Conferencing templates, which you can assign to this user.

Communication Profile tab: Work Assignment Profile

Name	Description
Account	The account name.
Account Address	The account address.
Source	The source name.
Source Address	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
Resource Details	Displays the Assignment Management page where you can configure assignment targets for the user. You can assign resource details to an agent only when the user has the Work Assignment profile assigned to the user.
Account Details	Displays the text box where you can add or modify the account name and account address. You can add attributes to the account only when the account is added to the agent.
Source Details	Displays the text box where you can add or modify the source name and source address. 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.
Presence Buddy	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
Edit	Displays the Edit Contact List Member page. Use this page to modify the information of the selected contact.

Table continues…

Button	Description
Add	Displays the Attach Contacts page. Use this page to select one or more contacts from the list of contacts. 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
Remove	Removes one or more selected contacts from the list of the associated contacts.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.
Filter: Enable	Displays the text fields under the columns that you can use to set the filter criteria. **Filter: Enable** is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Contacts tab — Private Contacts

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 contact.
Display Name	The display name of the private contact.
Contact Address	The address of the private contact.
Description	A brief description about the contact.

Button	Description
Edit	Displays the Edit Private Contact page. Use this page to edit the information of the contact you selected.
New	Displays the **New Private Contact** page. Use this page to add a new private contact.
Delete	Deletes the selected contacts.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.

Table continues…

Button	Description
Filter: Enable	Displays text fields under the columns that you can use to set the filter criteria. **Filter: Enable** is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Common buttons

Button	Description
Commit & Continue	Saves your changes and retains you on the same page for further modifications.
Commit	Modifies the user account and takes you back to the User Management or User Profile View page. **Note:** While restoring a deleted user, use the **Commit** button to restore a deleted user.
Cancel	Cancels the operation of modifying the user information and takes you back to the User Management or User Profile View page.

Related links

Modifying user accounts on page 137

User Profile View field descriptions

Organization

Name	Description
Tenant	The name of the tenant that you must select.
Level 1	The name of the level 1 hierarchy of the tenant organization. For example, Site. The tenant administrator provides the hierarchy on the Tenant Management page.
Level 2	The name of the level 2 hierarchy of the tenant organization. For example, Department.
Level 3	The name of the level 3 hierarchy of the tenant organization. For example, Team.

User Provisioning Rule

Name	Description
User Provisioning Rule	The name of the 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.

Identity tab — Identity section

Name	Description
Last Name	The last name of the user. For example, Miller.
Last Name (Latin Translation)	The user-preferred last name that the system must display on the end points. For example, Miller. Typically, the name is the written or spoken language of the user. **Note:** When you create a user, if the **Last Name (Latin Translation)** and **First Name (Latin Translation)** fields are: • Blank, the system displays the last name and first name in the fields. The values change when the last name and first names change. • Filled, the values remain even after you change the values in the **Last Name** and **First Name** fields.
First Name	The first name of the user. For example, John.
First Name (Latin Translation)	The user-preferred first name that the system must display on the end points. For example, John. Typically, the name is the written or spoken language of the user.
Middle Name	The middle name of the user, if any.
Description	A brief description about the user.
Status	The login status of the user.
Update Time	The time when the user details were last modified.

Table continues…

Name	Description
Login Name	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. 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 JMILLER@AVAYA.COM or jmiller@avaya.com. The login name can be in uppercase or lowercase. You cannot edit the **Login Name** field for users with the login name admin.
Email Address	The email address of the user.
Authentication Type	Authentication type defines how the system performs user authentication. The options are: • **Enterprise**: The enterprise authenticates the user login. • **Basic**: Avaya Authentication Service authenticates the user login.
Source	The entity that created this user record. The options are IP Address/Port, or a name representing an enterprise LDAP, or Avaya.
Localized Display Name	The localized display name of a user. Usually, the name is the localized full name.
Endpoint Display Name	The full text name of the user represented in ASCII. The field supports display names that cannot handle localized text, for example, some endpoints.
Title	The personal title for address a user. Usually, the title is a social title and not the work title.
Language Preference	The preferred written or spoken language of the user.
Time Zone	The preferred time zone of the user.
Employee ID	The employee number for the user.
Department	The department to which the user belongs.
Company	The organization where the user works.

Identity tab — Address section

Name	Description
Name	The unique label that identifies the address.

Table continues…

Name	Description
Address Type	The type of the address. Types of addresses are: • Office • Home
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 United States, this is Zip code.
Province	The full name of the province.
Country	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	The communication profile password. The field is available only if you enable the communication profile. The password policy is configured from **Users** > **User Management** > **Communication Profile Password Policy**. When communication password value is provided during bulk edit of users, the system overwrites any existing communication profile passwords of the user.

Table continues…

Name	Description
Option button	The option to view the details of the selected communication profile.
Name	The name of the communication profile. You must select the name.

Button	Description
New	Creates a new communication profile for the user.
Delete	Deletes the selected communication profile.
Done	Saves the communication profile information that you updated or added for a profile.
Cancel	Cancels the operation for adding of 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
Type	The type of the handle.
Handle	The unique communication address for the user.
Domain	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
Primary Session Manager	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.
Secondary Session Manager	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.

Table continues…

Name	Description
Survivability Server	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. **Note:** 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.
Max. Simultaneous Devices	The maximum number of endpoints that you can register at a time using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.
Block New Registration When Maximum Registrations Active	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.
Origination Application Sequence	An application sequence that will be invoked when the system routes the calls from this user. A selection is optional. **Note:** 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.

Table continues…

Name	Description
Termination Application Sequence	An application sequence that will be invoked when calls are routed to this user. A selection is optional. **Note:** 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.
Conference Factory Set	The conference factory set to enable media capability-based call routing to the Conferencing SIP entities. Use the **Session Manager** > **Application Configuration** > **Conference Factories** webpage to administer the Conference Factory Sets.
Home Location	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.

Communication Profile tab: Avaya Breeze™ Profile

Name	Description
Service Profile	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
System	Communication Manager on which you add the endpoint. The Communication Manager system on which you add the endpoint. You must select the system.
Profile Type	The type of the profile for the user.
Extension	The extension of the endpoint that you associate this profile with. You must select the extension.
View Endpoint	The list of existing or available endpoints based on the selection of the **Use Existing Endpoints** check box.

Table continues…

Name/Button	Description
Set Type	The set type of the endpoint you associate with. When you select a template, the system populates the corresponding set types.
Security Code	The security code for authorized access to the endpoint.
Port	The relevant port for the set type you select. You must select the port.
Voice Mail Number	The voice mail number of the endpoint you associate with. **Note:** You must clear Local Device Services Data on all Avaya Aura® Web Gateway nodes in case of changing the value of **Voice Mail Number**.
Preferred Handle	Numeric only handles, SIP handles, or nonSIP handles, that are administered for a user. The **Preferred Handle** field is optional. Select numeric handle for alphanumeric support. By default, the field is blank. If SIP entity is of the Communication Manager type, Session Manager uses preferred handle in CM Endpoint profile.
Attendant	When you select the 9641SIP template type from **Template**, the system enables the **Attendant** check box. The option to enable the attendant feature on the endpoint. If you select this check box, you can administer the endpoint as an attendant.

Table continues…

Name/Button	Description
Enhanced Callr-Info display for 1–line phones	The option to activate the enhanced Callr-info operation on the phone. The **Enhanced Callr-Info display for 1-line phones** field on the station form is valid for the following set types: • 1603, 1608, 1616, 1408, 1416 • 2402, 2410, 2420 • 4606, 4612, 4612CL, 4624, 4602, 4602+, 4630, 4610, 4622, 4620, 4621, 4625, • 6402D, 6408D, 6408D+, 6416D+, 6424D+, 607A1 • 7506D, 7507D • 8405D+, 8410D, 8405D, 8411D • 9404, 9408, 9601, 9601+, 9610, 9620, 9621, 9608, 9611, 9630, 9640, 9641, 9650 The valid options are: • **No**: Does not change the callr-info interactions with the connected phone. The default setting. • **Yes**: 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 **callr-info** button is not assigned to the phone on the station form, **Enhanced Callr-Info display for 1-line phones** does not apply.
Delete Endpoint on Unassign of Endpoint from User or Delete User	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 when you delete the user.

Table continues…

Name/Button	Description
Override Endpoint Name	The option to override the following: • The endpoint name on Communication Manager with the value you configured on the Manage users page during synchronization. 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. • The localized display name on the Manage Users page in the **Localized Display Name** field of Communication Manager. If you clear the check box, the system does not override the localized display name in the **Localized Display Name** field.

Communication Profile tab - CS1000 Endpoint Profile

Name	Description
System	The CS 1000 system of the endpoint.
Target	The system customer number for the Communication Server.
Template	The phone or endpoint template that you can choose for the user. The element manager maintains all templates.
Update	The option to update the endpoint profile information for the user. When you click **Update**, the system takes displays the element manager cut through for the updates.
Service Details	The service details, such as set type of endpoints that the system displays after phone creation.
Primary DN	The primary directory number of the phone. You can enter only numeric values.
Include in Corporate Directory	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
System	The messaging system on which you add the subscriber.
Template	The template, system-defined or user-defined, that you associate with the subscriber.
Mailbox Number	The mailbox number of the subscriber.
Password	The password for logging on to the mailbox.
Delete Subscriber on Unassign of Subscriber from User	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: Officelinx Profile

Name	Description
Officelinx System	The Officelinx system to which you add a mailbox.
Refresh	Gets the information about company, departments, and feature groups from Officelinx and saves locally on System Manager for future use. You do not require to refresh for every user.
Mailbox Number	The mailbox number of the subscriber.
Numeric Password	The numeric password that is used to log in to the Officelinx system.
Confirm Numeric Password	The numeric password that you retype to confirm.
Application User Password	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.
Confirm Application User Password	The password that you retype to confirm.
Company	The name of the company to which the user belongs.
Department	The department to which the user belongs.
Feature Group	The feature group name that determines the rules for the mailboxes associated with it.

Table continues…

Name	Description
Capability	The type of functionality that the user contains. The values are: • **Standard** • **Fax** • **Messaging** • **Collaboration** • **Messaging and Collaboration**
Domain Account Name	The mailbox NT account name for the Officelinx profile.
Synchronization User Name	The account name that is used to gain access to the email server, for example, Microsoft Exchange and Google Gmail.

Communication Profile tab - CallPilot Messaging Profile

Field	Description
System	The CallPilot system of the mailbox that you can view.
Location	The location that is mapped to the **CallPilot Location** field. CallPilot Manager provides the **Location** field.
Template	The mailbox template that you apply. The element manager maintains all mailbox templates.
Update	An option to update the mailbox information for the user. The system cuts through to the element manager for the updates.
Service Details	The mailbox service details from endpoint after you create the mailbox.
Mailbox Number	The mailbox number or the extension DN of the user.

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
System	The list of IP Office device names from which you can select the IP Office device you associate with the user.
Template	The list of user templates from which you can select your preferred template to set the user configurations.
Use Existing Extension	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.
Extension	The extension of the endpoint you associate. The field lists the endpoints, existing or available, based on option you selected in the **Use Existing Endpoints** check box.
Endpoint Editor button	Starts the IP Office application, where you can edit or view the details of the IP Office endpoint. 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 page.
Module-Port	The module port combination list for IP Office analog extensions. You must select **Module-Port** for centralized users with Set Type as **Analog**.
Set Type	The set type for the IP Office endpoint profile. By default, the **Set Type** field is disabled. If you select a template, the set type is auto populated.
Delete Extension On User Delete 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 **Analog** and **Digital** set types.

Communication Profile tab: Equinox Conferencing

Name	Description
Equinox User Password	The Equinox user password.
Virtual Room Number	The virtual room number of the Equinox user.

Communication Profile tab — Presence Profile

Name	Description
System	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: • Aggregate presence • Archive instant messages if the Instant Messages option is enabled
SIP Entity	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 **System** field. **SIP Entity** is read-only. If the system cannot identify a SIP entity, an appropriate error message is displayed in the field.
IM Gateway SIP Entity	The Presence Services instance for the user.
Publish Presence with AES Collector	The option that determines if Presence Services must publish presence with AES Collector. The options are: • **System Default** • **Off** • **On** The default is **System Default**. 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
Select Auto-generated Code Length	The number of characters in PIN. The default is 6. The system displays this field if you select the **Auto Generate Participant and Moderator Security Code** check box.
Auto Generate Participant and Moderator Security Code	Select the check box if the system must generate the participant security code and moderator security code for this user. Clear the check box to assign a specific participant security code or moderator security code for this user.

Table continues…

Name	Description
Participant Security Code	The participant security code that you assign for this user. The system displays this field only when the **Auto Generate Participant and Moderator Security Code** check box is clear.
Moderator Security Code	The moderator security code that you assign for this user. The system displays this field if the **Auto Generate Participant and Moderator Security Code** check box is clear.
Location	The location of the user. This field is mandatory for non-SIP users without a Session Manager profile and optional for SIP users. For SIP users, the system uses the location value from the **Home Location** field in the Session Manager profile.
Template	The Conferencing template that you assign to this user.

Button	Description
Get Templates	Displays the list of Conferencing templates, which you can assign to this user.

Communication Profile tab: Work Assignment Profile

Name	Description
Account	The account name.
Account Address	The account address.
Source	The source name.
Source Address	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
Resource Details	Displays the Assignment Management page where you can configure assignment targets for the user. 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
Account Details	Displays the text box where you can add or modify the account name and account address. You can add attributes to the account only when the account is added to the agent.
Source Details	Displays the text box where you can add or modify the source name and source address. You can add properties and attributes to the source only when the source already exists.

Membership tab — Roles section

Name	Description
Name	The name of the role.
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. **False** indicates that you cannot track the presence of the contact.

Button	Description
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.
Filter: Enable	Text fields under the columns that you can use to set the filter criteria. **Filter: Enable** is a toggle button.
Filter: Apply	Filters contacts based on the filter 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.
Display Name	Display name of the private contact.
Contact Address	The address of the private contact.
Description	A brief description about the contact.

Button	Description
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Enable	Text fields under the columns that you can use to set the filter criteria. This is a toggle button.
Filter: Apply	Filters contacts based on the filter criteria.

Common buttons

Button	Description
Edit	Opens the User Profile Edit page. Use the User Profile Edit page to modify the details of the user account.
Done	Closes the User Profile View page and returns to the User Management page.

Related links

Viewing details of a user on page 136

User Delete Confirmation field descriptions

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 a user. It is typically the localized full name.
Login Name	The login name of the you want to delete.
Last login	The date and time of last successful login on to System Manager.

Button	Description
Delete	Deletes the user.
Cancel	Closes the User Delete Confirmation page and returns to the User Management page.

Chapter 7: Session Manager routing

SIP entities send session creation requests to Session Manager. Session Manager routes these requests to other SIP entities using the address specified in the session creation request. Session Manager associates SIP entities with specific locations and makes routing decisions based on the location from which a session creation request arrives.

The addresses specify the identity of the destination of a session creation request and use the SIP Uniform Resource Identifier (URI) format. The identifier consists of a user part and a domain part. Session Manager uses both parts of the identifier to make routing decisions.

- The user part is an alphanumeric string such as a handle. Session Manager has special rules for efficiently routing and manipulating handles that consist of digits such as telephone numbers.
- The domain part specifies a DNS domain.

When you make any configuration changes in Session Manager, System Manager saves the data to the System Manager database. System Manager then synchronizes and distributes the data to all the Session Manager instances in the network. For example, renaming an adaptation changes the data on the SIP Entities Details screen, or changing dial pattern data changes the data in the routing policy where that dial pattern is used.

Routing

Session Manager uses routing to determine which SIP entity receives a call. Routing policies define how Session Manager routes calls between different SIP network elements. The system distributes configuration data from the Routing database to each remote Session Manager instance.

All calls originate either from a SIP entity or an administered user of the system.

Session Manager uses locations for origination-based routing and for specifying bandwidth for Call Admission Control.

Administrators define Session Manager routing:

- by combining several locations.
- by combining several dial patterns and domains.
- for several ToD and rankings.

- for a single routing destination.

Call routing using routing policy data

Administrators define routing policies for forwarding and routing data packets. A routing policy overrides routing protocol decisions. Policy-based routing includes a mechanism for selectively applying policies based on access list, packet size, or other criteria. The routing policy can include actions such as routing packets based on user-defined routes.

Session Manager uses routing policy data in the following manner:

1. First, Session Manager tries to match the domain to one of the authoritative domains.
2. If Session Manager is authoritative for the domain, then the Session Manager tries to match the digit pattern.
3. If a digit pattern is not matched, Session Manager tries to use the regular expression table.
4. If no regular expression match is found, Session Manager sends the request to a Session Manager-provisioned outbound proxy.
5. If no outbound proxy has been administered for the Session Manager and Session Manager is not authoritative for the domain, then Session Manager routes the request to the destination in the request-URI.
6. If the request-URI does not contain an IP address, then Session Manager uses DNS or the Local Host Name Resolution table to determine where to route the request.
7. If the Session Manager cannot resolve the hostname to an IP address, the call fails.

SIP response handling

The following table describes how Session Manager handles SIP responses.

Response	Session Manager action
2xx	Session Manager completes a call.
3xx 422 423 484 5xx (other than 501-504) 6xx	Session Manager sends a response to the caller.

Table continues…

Response	Session Manager action
408 501 to 504	Session Manager maps an alternate IP address or entity link of a SIP entity to determine an alternate route for a call. **Note:** If a SIP message establishes early dialog, Session Manager cannot change the dialog, and therefore cannot alternate route calls. For any SIP 101-199 provisional message that establishes early dialog, Session Manager cannot determine an alternate route for the call.
4xx (except 408)	Session Manager does not try to map the alternate IP addresses or entity link of a SIP entity to establish a call, Session Manager tries to determine an alternate route for the call with another routing policy. **Note:** If a SIP message establishes early dialog, Session Manager cannot change the dialog, and therefore cannot alternate route calls. For any SIP 101-199 provisional message that establishes early dialog, Session Manager cannot determine an alternate route for the call.

IP alternate routing and Call Admission Control

When sending a request, Session Manager sets the timer B or timer F value as specified in the destination SIP entity. If a SIP entity is administered with an FQDN, the Session Manager resolves the FQDN into a list of IP addresses using DNS or the local host name resolution table. The IP address of the final destination determines the egress location. The IP address is compared with IP address patterns on the Location Details page. If a location matches, the location is identified as the destination location. If no IP address pattern matches, the location that is administered on the destination SIP entity, if any, is identified as destination location.

If timer B or timer F expires, Session Manager generates a 408 response to the request. Session Manager then tries other IP addresses for the same SIP entity. If all IP addresses have been tried without success, Session Manager tries the next routing policy on the prioritized list.

If Call Admission Control is administered for the location and the request causes the number of allowed calls to be exceeded, the request is rejected with a 488 response.

Administering initial setup of the Session Manager

Once you have completed the initial setup, you can modify or delete the created entities.

Using the System Manager routing screens, the following is the recommended order for the initial set up of Session Manager.

Procedure

1. Accept or change default settings.
2. Create domains of type SIP.
3. Create locations.
4. Create adaptations.
5. Create SIP entities, some of which are routing destinations:
   - Create SIP entities that are used as Outbound Proxies, such as a particular Gateway or SIP Trunk.
   - Create other SIP entities.
   - Assign locations, adaptations, and Outbound Proxies to the SIP entities.
6. Create entity links:
   - Between Session Manager instances.
   - Between Session Manager instances and other SIP entities.
7. Create time ranges.

   Align with the tariff information received from the Service Providers.
8. Create routing policies.

   Assign the appropriate routing destination and Time Of Day. For Time Of Day, assign the appropriate time range and define the ranking.
9. Create dial patterns and assign the appropriate locations and routing policies to the dial patterns.
10. Create regular expressions and assign them to routing policies.
11. Create Session Manager instances using the Session Manager menus on the System Manager web console.

Routing element data import and export overview

The Routing screens provide administration of the Session Manager SIP routing rules. The management screens consist of configurable elements.

You can import a large number of the elements in System Manager by using XML files. You can export each of the elements or the entire routing configuration to XML files.

System Manager imports the Routing element data in the following order:

1. Domains
2. Locations
3. Adaptations

4. SIP Entities
5. Entity Links
6. Time Ranges
7. Routing Policies
8. Dial Patterns
9. Regular Expressions

Note:

The routing elements depend on each other. An import operation fails if the required elements do not already exist in the database or do not exist in the same import operation. For example, the import of a dial pattern with domain name **avaya.com** will fail if:

- No such domain exists in the database.
- An XML file containing this domain is not imported in the same import operation as the dial pattern.

System Manager Routing Import/Export supports:

- Importing each element separately as a single XML file containing many entries.
- Compressing the XML files using ZIP compression to decrease the size of the files that need to be uploaded to the System Manager server.

  Note:

  File compression is especially important when importing large files exceeding 10 MB or more.
- Importing several elements or all the elements in a single ZIP file containing many XML files.
- Exporting a single type of entity or all of the entities. When exporting all the entities, the exported files are contained in a single ZIP file.
- The Import operation does not halt if one of the elements fails validation. The failed element is not added to the database, and the import operation continues with the next element.
- An audit log provides details of the failed and successful import operations. The log is located at the following location:`/var/log/Avaya/mgmt/nrp/nrpaudit.log`. You can access the file through the System Manager command prompt.
- If an imported element already exists in the System Manager database, the values in the new element will overwrite the older element.
  - For example, if a domain with the name *avaya.com* already exists in the database, the `note`, `type`, and default values are overwritten by the new element.
  - The Dial Pattern is an exception for this rule. You cannot import a dial pattern with elements such as <digitpattern>,<maxdigits>,<mindigits>,<sipdomainName> and <routingoriginationName> already present in the database. The import attempt will fail.

Important:

When adding subcomponents to an existing element, include all the parameters associated with the element in the import XML file. For example, if you add digit patterns to an adaptation, make sure the adaptation import includes all of the patterns and not just the patterns you are adding to the adaptation.

Importing Routing element data

You must import element data as a ZIP file consisting of one or more XML files.

- Do not import data from the later stages in the routing definition process without importing data from the earlier stages. For example, you must import SIP entities either before or with the relevant entity links.
- The import operation can accept XML files of any routing element. For example, you can import **Locations** from the Domains page.
- During the export operation, the XML files contain the following version information:

```
<buildNumber>0</buildNumber>
<implementationVersion>0</implementationVersion>
<specificationVersion>0</specificationVersion>
```

Importing a very large number of elements (thousands and above) can take a very long time. In addition to importing the data, the System Manager server also synchronizes the information with all the Session Manager servers. Perform large imports at a time when the network has low activity, such as at night or during a maintenance window.

Before you begin

- Verify the user who is performing the import operation has administrative privileges.
- Before importing a large amount of data, back up the System Manager database. The backup provides an easy way to restore the original database in case the information you imported is substantially incorrect. For information regarding how to back up the System Manager database, see *Administering Avaya Aura® System Manager*.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing**.
2. Select and click the name of a Routing Element, such as **Locations**.
3. Click **More Actions** > **Import**.
4. Click **Choose File** and select Routing data file you want to import.
5. Do one of the following:
   - To begin the import operation immediately, click **Run immediately**.
   - To begin the import operation at a later time, click **Schedule later** and enter the specific date and time to run the import operation.
6. Click **Import** to start the import operation.

Note:

You can view the job status of the import operation in the **Import Job Status** section.

If the import job contains errors, the **Import Job Status** table provides a link to the failed import objects.

7. To delete a scheduled import job, select the job and click **Delete Job**.
8. To stop a running import job, select the job and click **Stop Job**.

Import Routing Data page field descriptions

File Selection

Button	Description
Select File	Select the file or files containing routing data to import.

Schedule

Name	Description
Run immediately	Run the import operation immediately after clicking **Import**.
Schedule later	Schedule the import operation to run at the specified start time.

Import Job Status

Button	Description
Delete Job	Delete an import job that is scheduled to run.
Stop Job	Stop an import job that is running.

Name	Description
Start Time	The start time of the import job.
Status	The status of the import job. Values are: 1. SUCCESSFUL 2. Waiting to run 3. Manually Stopped 4. FINISHED View errors in `/var/avaya/nrp`.
Files Processed	The number of files imported out of the total number of files.

Table continues…

Name	Description
Failed Entries	The number of errors encountered during the import operation.
Last Updated	The last update time of the import job.
Job Name	The name of the import job in the System Manager scheduler.

Button	Description
Import	Start the import operation of the routing element data file.

Exporting Routing element data

In this procedure, the term *<Any Routing element>* refers to the list of Routing Elements in the list under the **Routing**, such as *Adaptations*. For example, to export adaptations:

1. Select **Routing** > **Adaptations**.
2. Select **More Actions** > **Export Adaptations**.

The system packages the XML files into a zip file.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing**.
2. Click **Routing** > ***<Any Routing element>***.
3. Select a check box for the entity to be exported from the list of entities on the screen.
4. Do one of the following:
   - To export one routing element, click **More Actions** > **Export *<Routing Element>***.
   - To export multiple routing elements, click **More Actions** > **Export all data**.

   The system downloads the zip file.

Duplicating Routing entity data

Use the **Duplicate** button on the relevant Session Manager Routing pages to duplicate routing entities. Duplication of data is useful if you want to:

- Create entities that are similar to an existing entry.
- Copy an entity and make changes to the entity attributes.

For example, you can duplicate a routing policy and add a new dial pattern to the new version.

Domains

Domains determine if the Session Manager Dial Plan can route a particular call and if a SIP user is part of the enterprise SIP network.

For example:

1. Session Manager receives a request to `123@myserver.avaya.com`
2. `myserver.avaya.com` is not administered as a domain.
3. Session Manager checks dial patterns for `avaya.com`

You can create SIP domains and sub-domains on the Domains page.

- A Domain name can be `<organization-name.domain>`. For example, `avaya.com` or `abc.org`.
- A Sub-domain name can be based on the geographical location or any other corporate requirement such as an office location. For example, `us.avaya.com` and `fr.avaya.com` can be sub-domains for Avaya offices in the U.S. and in France.

Creating domains

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Domains**.
2. Click **New**.
3. In the **Name** field, enter the domain or sub-domain name.
4. In the **Type** field, select **sip** as the domain type from the drop-down menu.
5. In the **Notes** field, enter a description or other note as appropriate.
6. Click **Commit**.

Modifying domains

Warning:

Changing the SIP domain name causes a login failure for Communication Address handles that use the domain name.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Domains**.

2. To edit information for existing domains or sub-domains:
   a. Select the domains that you want to edit.
   b. Click **Edit**.
   c. Make the changes to the domain data as required.
   d. Click **Commit**.
3. To copy existing domain data to a new domain:
   a. Select the domain.
   b. Click **Duplicate**.
   c. Edit the duplicate domain data as required.
   d. Click **Commit**.

Deleting domains

You can delete more than one domain at the same time.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Domains**.
2. Select the domain or domains you want to delete.
3. Click **Delete**.
4. Click **Delete** on the confirmation page.

Domain Management field descriptions

Use this page to create, modify, delete, and manage domains.

Button	Description
Edit	Modify the domain details.
New	Create new domains.
Delete	Confirm or cancel the deletion of the domain.
Duplicate	Creates a duplicate of the selected domain.
More Actions > **Import**	Import from XML files or a zip file containing one or more XML files.
More Actions > **Export Domains**	Export the domains data as an XML file to a specified location.
More Actions > **Export all data**	Export all of the routing entities data as a zipped file to a specified location.

Name	Description
Name	Name of the domain.
Type	The type of the domain. Only Domains of type SIP can be used for routing.
Notes	Additional notes about the domain.

Domain Details field descriptions

Name	Description
Name	Name of the domain.
Type	Domain type. Only domains of type SIP can be used for routing.
Notes	Additional notes about the domain.

Button	Description
Commit	Save the domain data and distribute the information to all the Session Manager instances.
Cancel	Cancel the domain creation.

Bulk import for Domains

When creating an XML bulk import file:

- The domain name *must* be unique. The name is referred to by other elements.
- You cannot create a domain with a **<domainType>** of `sip` and the **<defaultDomain>** containing the value `true`.
- The values in **<domainType>** are case-sensitive and must appear exactly the same as the values appear in the System Manager user interface.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<sipdomainFullTOList>
    <SipdomainFullTO>
        <notes>this is a test</notes>
        <defaultDomain>false</defaultDomain>
        <domainName>avaya.com</domainName>
        <domainType>sip</domainType>
        <name>avaya.com</name>
    </SipdomainFullTO>
    <SipdomainFullTO>
        <notes>this is another test</notes>
        <defaultDomain>false</defaultDomain>
        <domainName>avaya2.com</domainName>
        <domainType>sip</domainType>
        <name>avaya2.com</name>
```

```
    </SipdomainFullTO>
</sipdomainFullTOList>
```

Locations

Use the Locations page to configure gateway and user locations. The IP address of the device determines the physical location of the caller or the called user.

1. The Session Manager tries to match the IP address of the bottom-most VIA header of the received INVITE against the IP patterns on the Locations.
2. If no IP address match is found, the Session Manager uses the assigned location on the sending SIP Entity.
3. If no assigned Location is found, the Session Manager uses the assigned location of the Session Manager SIP Entity.

If dial patterns are administered for the specific location, the Session Manager uses the originating location to determine which dial pattern is suitable for routing the call. Locations are also used to limit the number of calls originating from or terminating to a physical location. This is known as Call Admission Control (CAC) and is useful to manage the network bandwidth of locations. CAC provides a level of protection by limiting the impact of multimedia traffic over the most critical network links between enterprise locations, such as the links from branch offices to data centers in the network core. You specify CAC details using the **Overall Managed Bandwidth** and **Per-Call Bandwidth Parameters** sections on the Location Details page.

Note:

The Session Manager logs the result of each rejected multimedia CAC request to help determine the root cause when multimedia calls fail.

You can use the following wildcard characters to specify a location:

- “*” (star) specifies any number of allowed characters at the end of the string.
- “x” specifies a digit.

Note:

The pattern can be an IP address range. For example:

- IPv4: 10.0.0.1-10.0.0.5
- IPv6: - 2a07:2a42:adc0:15:0:0:0:5

The IP address mask is a valid pattern. For example:

- IPv4: 135.9.0.0/16
- IPv6: 2a07:2a42:adc0:15:0:0:0:0/64

The Locations page can contain one or several IP addresses. Each SIP Entity has a particular IP address. Depending on the physical and geographic location of each SIP Entity, some of the SIP Entities can be grouped into a single location. For example, if there are two Communication

Manager servers located in Denver, the Communication Manager servers can form one location named Denver.

The order in which the Session Manager matches the IP address is as follows:

1. Wildcard patterns (* and x)
2. Ranges
3. Netmask

Dial Plan Transparency

Dial Plan Transparency (DPT) is a business continuity feature. During a network outage, DTP preserves the dial plan and reroutes all new calls to the PSTN. Communication Manager and Session Manager support DPT in the Listed Directory Number (LDN)/DTMF method, as follows:

- A PSTN call routes to a single LDN at the far end.
- The PSTN call carries the identity of the calling party.
- The far end answers the call, and the calling side sends identifying DTMF digits of the called party.

For more information about the Dial Plan Transparency feature, see the Communication Manager documentation and Avaya Aura® Dial Plan Transparency White Paper on the Avaya Support website at http://support.avaya.com/.

Note:

- DPT can be triggered by a call between endpoints in different Session Manager locations. However, if a data network failure occurs within a Session Manager location, a DPT call is not supported. Administrators must plan their data network accordingly to decide how to partition users into different locations.
- In a mixed environment with SIP and non-SIP devices, the Session Manager DPT feature does not support DPT calls to non-SIP devices connected to a Communication Manager instance that is different from the Communication Manager instance administered in the Location screen.

Call Admission Control

Audio and multimedia calls require high bandwidth and low latency for best user experience. Call Admission Control (CAC), also known as Bandwidth Management, prevents degradation of call quality by limiting the number of concurrent calls over links that have limited bandwidth.

CAC regulates the total utilized bandwidth, the total number of calls, or the total number of packets or data bits passing a specific point per unit time. If a defined limit is reached or exceeded, a new call may be prohibited from entering the network until at least one current call terminates.

Call Admission Control Behavior

Session Manager CAC limits bandwidth between locations. For CAC, the links between locations can have limited capacity, while calls that take place entirely within a location do not need to be limited. CAC also assumes that all calls entering or leaving a location use the same network link. A link for the location connects the location to the public network, from which every other location can be accessed at equal cost. Any media session between locations involves two links – one link to each location, and another link from each location.

The association of one link to one location means that limits on links can be implemented as limits on locations. No other links are recognized or have limits enforced by CAC. Calls contained entirely within a location involve no links.

CAC enforces limits by allowing calls on a first-come, first-serve basis until a limit is about to be violated. CAC prevents limit violation by either reducing the bandwidth of calls or by denying calls. Bandwidth reduction can mean that audio or video quality is reduced, or that media streams (such as video) are removed. Only calls that would otherwise violate limits will be impacted by CAC. By preventing limits from being exceeded, CAC prevents packet loss degradation from impacting existing calls.

Calls between locations are subject to the limit enforcement of both locations, if limits have been defined for both. In cases when call parties are not mapped to locations, then CAC restrictions do not apply for those parties.

Emergency calls are never impacted by CAC.

Call Admission Control Administration

With CAC, you can specify several types of limits on Locations.

An overall limit, **Total Bandwidth**, constrains the total bandwidth used for calls traversing the link of the location.

The multimedia sub-limit, **Multimedia Bandwidth**, restricts calls that are not audio-only, such as video calls, to less than the full capacity of the location. The sub-limit prevents a few large video calls from exhausting the link and preventing audio calls from being made.

CAC also provides per-call parameters such as **Maximum Multimedia Bandwidth** to be specified at a location level. The **Maximum Multimedia Bandwidth** value limits the bandwidth allowed to a single call to create room for more calls along a link by restricting video quality.

Each of these limits may be specified or left blank for any given location.

CAC operates by inspecting Session Description Protocol (SDP) contained in SIP messaging for calls. SDP identifies both the source of media (by IP address, which maps to Location) and the amount of bandwidth consumed. SDP manipulation is also used to reduce bandwidth consumption for limit enforcement. CAC allows the specification of default bandwidth assumptions for calls with unrecognized SDP, specified per Location (**Default Audio Bandwidth**). CAC also allows a per-location restriction on how much a multimedia stream can have its bandwidth reduced (**Minimum Multimedia Bandwidth**) before it should be removed entirely. This is required for maintaining a minimum level of video quality.

CAC provides alarm notifications when the bandwidth usage of a location remains above a certain threshold for a sustained period of time. Snapshots of current usage are taken every 60 seconds, and if successive snapshots remain above the threshold, the alarm is raised until usage drops below the threshold. For each location and limit type, you can administer the number of snapshots and threshold required to raise the alarm. You can monitor the real-time bandwidth usage in the Managed Bandwidth Usage page.

Two additional settings can change the way Session Manager performs Call Admission Control.

- **Audio Calls Can Take Multimedia Bandwidth**, when not selected, specifies that only multimedia calls will fill the **Multimedia Bandwidth** bucket, while audio-only calls will be limited to the bandwidth specified by **Total Bandwidth – Multimedia Bandwidth**. When selected (default), audio-only calls can consume all of **Total Bandwidth**, and **Multimedia Bandwidth** functions as a sub-limit for calls containing non-audio media.
- Based on the **Ignore SDP for Call Admission Control** option in the Global Settings section on the Session Manager Administration page, all Session Manager instances interpret that all calls lack SDP. This option causes every call to be regarded as an audio call using bandwidth defined as **Default Audio Bandwidth** under the originating location of the call.
  - This setting can be used to transform CAC into a call count enforcer. Because each call is counted equally, the limit enforced is a limit on the number of calls allowed to or from a location. By assigning SIP entities to unique locations, you can limit the number of calls to or from an entity.
  - Session Manager ignores SDP. When upgrading System Manager from 6.0 to later versions, the previous administered behavior will be preserved. Otherwise, this option is disabled by default.

Creating Locations

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Locations**.
2. Click **New**.
3. In the **Name** field, enter the location name.
4. Enter notes about the location as appropriate.
5. In the Dial Plan Transparency in Survivable Mode section, enter the DPT parameters.
6. In the Overall Managed Bandwidth section, specify the parameters for the location.
7. In the Per-Call Bandwidth Parameters section, specify the average bandwidth per call for the location.
8. In the Alarm Threshold section, specify the alarm threshold percentage for audio and multimedia calls for the location.

9. To add a location pattern:
    a. Click **Add** under **Location Pattern**.
    b. Enter an IP address pattern to match.
    c. Enter notes about the location pattern as appropriate.
    d. Continue clicking the **Add** button until you have configured all the required Location Pattern matching patterns.
10. Click **Commit**.

Modifying Locations

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Locations**.
2. Select the check box for the required location.
3. Click **Edit**.
4. Make the required changes to the location or location pattern for the selected location.
5. Make the necessary changes in the different sections.
6. If required, add or remove a **Location Pattern** by clicking **Add** or **Remove** under **Location Pattern**.
7. Click **Commit**.

Deleting Locations

You can delete one or more locations at the same time.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Locations**.
2. Select the location or locations you want to delete.
3. Click **Delete**.
4. Click **Delete** on the confirmation page.

Location field descriptions

Use this page to create, modify, delete, and manage locations.

Button	Description
New	Create a new location.
Edit	Modify information for the selected location.
Delete	Delete the selected location. You can delete more than one location at the same time.
Duplicate	Create a duplicate of the selected location and assign a new state to it.
More Actions > **Import**	Open the Import data page to import data from XML files or compressed files that contain one or more XML files.
More Actions > **Export Locations**	Export the selected location data as an XML file to a specific location.
More Actions > **Export all data**	Export the data for all routing entities as a compressed file to a specific location.

Name	Description
Name	Name of the location.
Correlation	Indication if a Session Manager correlates with a Communication Manager network region or not.
Notes	Notes about the location.

Location Details field descriptions

Use this page to set up and configure locations.

General section

Name	Description
Name	Name of the location.
Notes	Notes about the location.
IP Network Region	IP Network Region that correlates with the Session Manager location.
Communication Manager	The Communication Manager that contains the IP Network Region.

Dial Plan Transparency in Survivable Mode section

Name	Description
Enabled	Enable or disable Dial Plan Transparency (DPT) in Survivable mode.

Table continues…

Name	Description
Listed Directory Number	Far end number where a DPT call gets routed. This number may only contain digits 0-9, '-', '.' or space character and may begin with a leading '+'. This number should be unique and should not match an LDN in any other Location. A Listed Directory Number is required if **Enabled** is selected.
Associated CM SIP Entity	The Communication Manager server used to originate DPT calls from this location. The Communication Manager server should ideally be located in this location to maximize the probability of being reached in the event of a network outage. A SIP Entity name must be selected if **Enabled** is selected.

Overall Managed Bandwidth section

Name	Description
Managed Bandwidth Units	Specifies the bandwidth unit for Overall Managed Bandwidth values.
Total Bandwidth	The total bandwidth available for use by any calls between this location and other locations. Any attempt to exceed this limit results in either • calls either being alternate routed or denied. • requested bandwidth of the calls may be reduced. If no value is specified, the bandwidth limit is infinite.
Multimedia Bandwidth	The bandwidth available for use by multimedia calls between this location and other locations. This is a subset of the Total Bandwidth value. Any attempt to exceed this limit results in either • calls either being alternate routed or denied. • requested bandwidth of the calls may be reduced. If no value is specified, the use of the limit defined for Total Bandwidth depends on the value of Audio Calls Can Take Multimedia Bandwidth. If selected, Total Bandwidth can be used for any call type. If not selected, Total Bandwidth can be used only for audio calls.

Table continues…

Name	Description
Audio Calls Can Take Multimedia Bandwidth	Specifies the use of multimedia call bandwidth for audio calls. If this check box is selected, the bandwidth reserved for multimedia calls may also be used for audio calls. If not, this bandwidth may only be used for multimedia calls.

Per-Call Bandwidth Parameters section

Name	Description
Maximum Multimedia Bandwidth (Intra-Location)	The maximum bandwidth allowed for a single multimedia call within this location. Calls requesting more bandwidth than this value are modified to use less bandwidth. Default value is 1000 Kbit/sec, range is 0-15360 Kbit/sec.
Maximum Multimedia Bandwidth (Inter-Location)	The maximum bandwidth allowed for a single multimedia call between this location and another location. Calls requesting more bandwidth than this value are modified to use less bandwidth. Default value is 1000 Kbit/sec, range is 0-15360 Kbit/sec.
Minimum Multimedia Bandwidth	The minimum bandwidth specified per multimedia media stream that Session Manager uses while reducing the bandwidth request for a call to or from this location to enforce any bandwidth restriction. If a bandwidth restriction requires Session Manager to reduce a media stream below this level, the stream is removed from the call, possibly resulting in the entire call being blocked. Media requests for bandwidth beneath this minimum is not blocked. This is solely a restriction on the ability of Session Manager to modify requests. Default value is 64 Kbit/sec and the range is 64-15360 Kbit/sec.
Default Audio Bandwidth	The audio bandwidth assumed to be used by a call originating in this location that does not explicitly specify its bandwidth needs using the Session Description Protocol (SDP). Such calls are assumed to be of audio type only. Default value is 80 Kbit/sec and the range is 0-15360 Kbit/sec.

Alarm Threshold section

Name	Description
Audio Alarm Threshold	Threshold percentage for the audio portion of the administered **Total Bandwidth** value. When audio usage exceeds this percentage of the limit for the specified latency, an alarm will be raised. Valid range is 0% - 100% in increments of 5%. The default value is 80%. Set the value to 0% to disable the alarm. **Note:** The system displays **Audio Alarm Threshold** field if the **Audio Calls Can Take Multimedia Bandwidth** checkbox is cleared.
Overall Alarm Threshold	Threshold percentage for the administered **Total Bandwidth** value. When audio and multimedia usage exceeds this percentage of the limit for the specified latency, an alarm will be raised. Valid range is 0% - 100% in increments of 5%. The default value is 80%. Set the value to 0% to disable the alarm. **Note:** The system displays **Overall Alarm Threshold** field if the **Audio Calls Can Take Multimedia Bandwidth** checkbox is selected.
Multimedia Alarm Threshold	Threshold percentage for the administered **Multimedia Bandwidth** value. When multimedia usage exceeds this percentage of the limit for the specified latency, an alarm will be raised. Valid range is 0% - 100% in increments of 5%. The default value is 80%. Set the value to 0% to disable the alarm.
Latency before Audio Alarm Trigger	Latency before an alarm is raised for the audio portion of the **Total Bandwidth** value. The units are in minutes, with a range of 0 to 30. The default value is 5 minutes. **Note:** The system displays **Latency before Audio Alarm Trigger** field if the **Audio Calls Can Take Multimedia Bandwidth** checkbox is cleared.

Table continues…

Name	Description
Latency before Overall Alarm Trigger	Latency before an alarm is raised for the **Total Bandwidth** value. The units are in minutes, with a range of 0 to 30. The default value is 5 minutes. **Note:** The system displays **Latency before Overall Alarm Trigger** field if the **Audio Calls Can Take Multimedia Bandwidth** checkbox is selected.
Latency before Multimedia Alarm Trigger	Latency before an alarm is raised for the **Multimedia Bandwidth** value. The units are in minutes, with a range of 0 to 30. The default value is 5 minutes. Latency value specifies the amount of time during which a location exceeds a threshold before an alarm is raised. This specification helps to prevent excessive alarming if the network crosses back and forth over the alarm threshold value over a period of time. Alarm thresholds are sampled every 60 seconds for a given location.

Location Pattern section

Button	Description
Add	Add an IP address pattern to match for the location.
Remove	Remove the IP address pattern to match for the location.

Name	Description
IP Address Pattern	An IP address or IP address pattern that maps IP address(es) to this location. IP addresses should uniquely map to locations. If an address matches several locations' patterns, the address gets assigned to the location with the most specific pattern matched. Pattern examples are: • 135.12x.121.* • 13x.1xx.* • 135.* • 135.12x.121.123 • 2001:d8b::X:X • 2001:d8b0::1xxx • 2001:d8b0:adc0:14:10:10:* **Note:** Pattern can also accept IP address range. Example: • IPv4: 10.0.0.1-10.0.0.5 • IPv6: 2a07:2a42:adc0:15:0:0:0:0 - 2a07:2a42:adc0:15:0:0:0:5 IP address mask is also a valid pattern. Example: • IPv4: 135.9.0.0/16 • IPv6: 2a07:2a42:adc0:15:0:0:0:0/64 This field accepts IPv6 addresses, ranges, and masks. You cannot use the wildcard pattern with a range or a mask.
Notes	Additional notes.

Button	Description
Commit	Save and apply the changes.
Cancel	Do not save and apply the changes.

Bulk import for Locations

When creating an XML bulk import file:

- The import XML refers to **Locations** as **routing origination**.
- The name of a location *must* be unique since other elements refer to the location name.
- You can configure multiple Routing Origination Patterns <routingoriginationpatterns> to one Routing Origination Name.

- The values in <ManagedBandwidthUnitOfMeasurement> are case-sensitive and *must* appear exactly same as the values a in the System Manager user interface.

Example:

```
<routingoriginationFullTOList>
    <buildNumber>0</buildNumber>
    <implementationVersion>0</implementationVersion>
    <specificationVersion>0</specificationVersion>
    <RoutingoriginationFullTO>
            <notes>A complete example</notes>
            <name>New York</name>
            <cac_audio_alarm_latency>5</cac_audio_alarm_latency>
            <cac_audio_alarm_threshold_percent>80</cac_audio_alarm_threshold_percent>
              <AverageBandwidthPerCall>80</AverageBandwidthPerCall>
            <AverageBandwidthPerCallUnitOfMeasurement>Kbit/sec</
AverageBandwidthPerCallUnitOfMeasurement>
            <cac_can_audio_steal_from_video>true</cac_can_audio_steal_from_video>
            <cac_max_bwidth_video_interloc>2000</cac_max_bwidth_video_interloc>
            <cac_max_bwidth_video_intraloc>2000</cac_max_bwidth_video_intraloc>
            <cac_min_acceptable_bwidth_video>64</cac_min_acceptable_bwidth_video>
            <ManagedBandwidthUnitOfMeasurement>Kbit/sec</
ManagedBandwidthUnitOfMeasurement>
            <cac_video_alarm_latency>5</cac_video_alarm_latency>
            <cac_video_alarm_threshold_percent>80</cac_video_alarm_threshold_percent>
            <DptFsSipentityName>testcm</DptFsSipentityName>
            <dpt_in_survivable_mode>true</dpt_in_survivable_mode>
            <listed_directory_number>114</listed_directory_number>
            <routingoriginationpatterns>
            <notes>a test</notes>
            <ipaddresspattern>1.2.3.4-1.2.3.10</ipaddresspattern>
            </routingoriginationpatterns>
            <TimeToLiveInSec>3600</TimeToLiveInSec>
    </RoutingoriginationFullTO>
    <RoutingoriginationFullTO>
            <notes></notes>
             <name>Westminster</name>
            <cac_audio_alarm_latency>5</cac_audio_alarm_latency>
            <cac_audio_alarm_threshold_percent>80</cac_audio_alarm_threshold_percent>
             <AverageBandwidthPerCall>80</AverageBandwidthPerCall>
            <AverageBandwidthPerCallUnitOfMeasurement>Kbit/sec</
AverageBandwidthPerCallUnitOfMeasurement>
             <cac_can_audio_steal_from_video>true</cac_can_audio_steal_from_video>
             <cac_max_bwidth_video_interloc>2000</cac_max_bwidth_video_interloc>
             <cac_max_bwidth_video_intraloc>2000</cac_max_bwidth_video_intraloc>
             <cac_min_acceptable_bwidth_video>64</cac_min_acceptable_bwidth_video>
             <cac_normal_bwidth_video>10000</cac_normal_bwidth_video>
            <ManagedBandwidth>10000</ManagedBandwidth>
             <ManagedBandwidthUnitOfMeasurement>Kbit/sec</
ManagedBandwidthUnitOfMeasurement>
            <cac_video_alarm_latency>5</cac_video_alarm_latency>
            <cac_video_alarm_threshold_percent>80</cac_video_alarm_threshold_percent>
            <dpt_in_survivable_mode>false</dpt_in_survivable_mode>
            <TimeToLiveInSec>3600</TimeToLiveInSec>
        </RoutingoriginationFullTO>
</routingoriginationFullTOList>
```

Adaptations

You can use Adaptations to modify SIP messages that are:

- entering a Session Manager instance (ingress adaptation).
- leaving a Session Manager instance (egress adaptation).

The adaptation function converts strings containing calling and called party numbers from the local dial plan of a SIP entity to the dial plan administered on the Session Manager, and vice-versa. Adaptation also supports special SIP protocol conventions for other SIP entities. Each administered SIP entity can have its own unique adaptation, or one adaptation can be shared among multiple entities.

You can implement adaptations as software modules that you create and deploy to fit the needs of the system.

Session Manager includes a module called DigitConversionAdapter, which can convert digit strings in various message headers as well as hostnames in the Request-URI and other headers. The module also contains adaptation modules which perform protocol conversions such as for AT&T, Verizon, and Cisco systems, as well as the digit conversion. All of these adapters allow for modification of URIs specified using unique name-value pairs for egress adaptation. For example, you can replace the host name in the Request-URI with an administered host name during egress adaptation. An adaptation administered using Routing specifies the module to use as well as the digit conversion that is to be performed on headers in the SIP messages. Different digit conversions can be specified for ingress and egress adaptation.

All adaptation modules provided with Session Manager convert DTMF message bodies in an INFO message between the following formats:

- application/vnd.nortelnetworks.digits
- application/dtmf-relay
- application/dtmf

DTMF message bodies are automatically converted to **application/dtmf-relay** on ingress unless the `noidtmf` parameter is specified. DTMF message bodies are converted on egress to the format specified in the `dtmf` parameter.

Additionally, digit conversion can be specified to modify only **origination** type headers, only **destination** type headers, or both. The origination/source type URIs are:

- From: See #1 below.
- P-Asserted-Identity
- History-Info (calling portion)

The destination type URIs are:

- Request-URI: See #3 below.
- Contact in 3xx response: See #2 below..

- To: See #1 and #3 below.
- Message Account in NOTIFY/message-summary body.
- Refer-To in REFER message: See #2 below.

1. The From and To headers are only modified by adaptation if the `fromto` module parameter is present and has the value of **true**. See *Adaptation Module Administration* below.
2. Adaptations are only applied to the Contact header in a 3xx response and the Refer-To header in a REFER message, if the host-part of the URI is either the IP address of the Session Manager or a domain for which the Session Manager is authoritative.
3. In Session Manager, Request-URI and To headers are not adapted on ingress if the host part of the URI is an IP address that is different from the IP address of the Session Manager. If required, the new adaptation module parameter `adaptForeignURI` can be added to provide the earlier adaptation behavior prior to that of Session Manager 6.2 release.
4. All adaptations strip the port and transport from the Request-URI if the host-part is adapted on egress. This behavior can be overridden with the `keepPortTransport` parameter.

Adaptation Module parameters

All adaptation modules can replace the domain, also known as the host name, part of the URI with a value for source and destination type URIs on outgoing calls (egress). All adaptation modules can also append parameters to the Request URI on for outgoing calls (egress). This adaptation functionality provides flexibility to deployments. The adaptation modules will be preserved during upgrade.

Module Parameter Type

The **Module Parameter Type** displays on the Adaptation Details screen.

The **Module Parameter Type** can contain no parameters, a single parameter, or a list of name-value pairs.

The supported adaptation module parameter values are:

- **fromto:** If set to `true`, the adaptation modifies the From and To headers of the message. If the From and To headers are not present or are set to any other value, the From and To headers are not modified.
- **multipartMIMEsupported:** This option can be abbreviated to `MIME`. This option is applicable to egress processing only. If the parameter is set to `no` , the multipart MIME message bodies are stripped on egress from Session Manager. If the multipart MIME message contains an SDP message body, the message body will be inserted as the only message body in the outgoing message. If omitted or set to any other value, the message bodies will not be modified.
- **adaptForeignURI:** If the value is set to `true`, the INGRESS adaptation is applied to the Request-URI and to the header if the **fromto** parameter is set, even if the host part is an IP address that is different from the IP address of the Session Manager.

- **noidtmf:** If the value is set to `true`, no DTMF message body conversion is performed on ingress.
- **dtmf:** The value of this parameter determines the DTMF message body format that is desired on egress from the Session Manager . If omitted, no conversion is done. Supported values are `nortel`, `relay`, and `dtmf`.
- **keepPortTransport:** If this parameter is present and set to any value, Session Manager does not strip the port and transport when the domain of the Request-URI is modified on egress.
- **noar:** This parameter requires a comma-separated list of SIP response codes. This parameter is applicable to the egress adaptation only. You can use this parameter to override the default alternate routing behavior of Session Manager. Session Manager does not alternate route a request to the next SIP Entity if it receives one of the responses listed in the parameter value. An example of a comma-separated list is `noar = 404,486`.
- **sessionTimeout:** Use this parameter for SIP entities that do not support the session timer, as per RFC 4028, or to send periodic SIP messages to keep the session active for more than one hour. If both entities use the session timer in a call, Session Manager keeps the session active for the negotiated interval. If the entities do not use the session timer in a call, then Session Manager keeps the session active for one hour after the last SIP transaction. In such cases, you can set this parameter (in seconds) to extend the one hour interval. For example, if the session timer is not used, the parameter value of `sessionTimeout=7200` makes the session stay in memory for 7200 seconds (120 minutes) after the last SIP message exchange.
- **noallow:** This parameter requires a comma-separated list of SIP methods. The system strips the methods from the Allow header on egress. Method names are case-insensitive. For example, `noallow=UPDATE` and `noallow=UPDATE,OPTIONS`.
- **iRHdrs:** Remove the specified header or headers during adaptation process from messages in the ingress direction. Separate multiple headers with a comma. For example, `P-Charging-Vector,P-Location`. Header names are case-insensitive. The administrator can remove the headers that Session Manager may add during post adaptation module invocation, for example, P-Location.
- **eRHdrs:** Remove the specified header or headers during adaptation process from messages in the egress direction. Separate multiple headers with a comma. For example, `P-Charging-Vector,P-Location`. The administrator can remove the headers that Session Manager may add during post adaptation module invocation, for example, P-Location.
- **reduceRtHdrs:** The intermediate element adds routing headers when the SIP messages move from one element to other. To reduce the number of routing headers values from the SIP message, use the **reduceRtHdrs** parameter. If you set the value of **reduceRtHdrs** to true, the system reduces the number of routing headers values, such as Via and Record-Route from the SIP message. However, all the outgoing messages from Session Manager will have the Via and Record-Route header with values of Session Manager IP and transport so that all the responses and subsequent requests for that call can be delivered to Session Manager.

  The **reduceRtHdrs** parameter is introduced in Session Manager, to enable the Routing Header Compression feature.
- **addRouteHdrs:** This parameter adds the indicated Route headers to outgoing requests to the entity for dual-Route header support required by Assured Services SIP interface to

SoftSwitch. The **addRouteHdrs** parameter is used in DOD networks to route calls between ESC and LSC utilizing SoftSwitch. The **addRouteHdrs** values must be added within quotation marks. Multiple values must be separated with a comma. For example "<sip:10.129.177.129:5061;transport=tcp;lr>,<sip:10.133.177.129:5061;transport=tcp;lr>"

EGRESS Domain Modification parameters

The EGRESS Domain Modification parameters are:

- `overrideDestinationDomain (` can be abbreviated to `odstd)`: By default, this is the first parameter. The Adaptation module replaces the domain in Request-URI, To header (if administered), Refer-To header, and Notify/message-summary body with the given value for egress only. If the request is a REFER, the domain in the Refer-To header will only be modified if it is the IP address of the Session Manager or a domain for which the Session Manager is authoritative.
- `overrideSourceDomain (` may be abbreviated to `osrcd)`: The Adaptation module replaces the domain in the From header (if administered), P-Asserted-Identity header and calling part of the History-Info header with the given value for egress only. The Module Parameter:`osrcd=dr.avaya.com odstd=ny.avaya.com` is the same as the verbose form `overrideSourceDomain=dr.avaya.com overrideDestinationDomain=ny.avaya.com`.

INGRESS Domain Modification parameters

The INGRESS Domain Modification parameters are:

- `ingressOverrideDestinationDomain (` can be abbreviated to `iodstd)`: Adaptation module replaces the domain in Request-URI, To header (if administered), and Notify/message-summary body with the given value for ingress only. If the request is a REFER, the domain in the Refer-To header will only be modified if it is the IP address of the Session Manager or a domain for which the Session Manager is authoritative.
- `ingressOverrideSourceDomain (` can be abbreviated to `iosrcd)`: Adaptation module replaces the domain in the From header (if administered), P-Asserted-Identity header and calling part of the History-Info header with the given value for ingress only.

EGRESS Display Name Modification

`egressDisplayName` : In Session Manager, if this parameter is present, the adaptation module modifies the display name of the Contact, P-Asserted-Identity, and From/To headers (if fromto = true is specified) of the egress messages.

For outgoing calls, the adaptation module applies the adaptation to the P-Asserted-Identity, Contact, and From headers in both the initial dialog-creating request sent from the Session Manager and in all subsequent in-dialog requests.

For incoming calls, the adaptation module applies the adaptation to the P-Asserted-Identity, Contact, and To headers. If the value of the parameter contains spaces, then the value must be enclosed in double quotes. Additionally, any double quotes that are part of the parameter value must be preceded by a backslash character.

Example values for the egressDisplayName parameter are:

- egressDisplayName=SomeCallingName
- egressDisplayName="My Business"

- egressDisplayName="The \"Best\" Business"

Phone context

Phone Context is an optional field for ingress and egress adaptation rules. The allowed format for the Phone Context string can either be an E.164 number or a domain name (which can contain only alphanumeric characters, a hyphen, and periods).

Ingress message processing:

- If the phone-context field of an ingress adaptation module rule contains a valid value, ingress adaptation is applied only if all four trigger fields (Matching Pattern, Min, Max, and Phone-context) match the header.
- If the phone-context field is empty, ingress adaptation is applied based on the remaining fields (Matching Pattern, Min, and Max).

Egress message processing:

- If the phone-context field of an egress adaptation module rule contains a valid value, the adaptation module modifies the digits and inserts phone-context when the three trigger fields Matching Pattern, Min, and Max) match the criteria.
- If the phone-context field is empty, the egress adaptation module does not insert phone-context.

Precedence Rules

If a request matches the criteria of two rules (one with a valid phone-context and empty phone-context), the rule with valid phone-context string takes precedence. The following is an example of the rule precedence:

Rules	Ingress Adapter Rule
1	Matching pattern: 53853 Min: 7 Max: 7 Phone-Context: Delete Digits: 3 Insert Digits: 538 Address to modify: both

Table continues…

2	Matching pattern: 538 Min: 7 Max: 7 Phone-Context: denver Delete Digits: 0 Insert Digits: +1303 Address to modify: both

If an adapter has the above two rules, a request with `R-URI of 5385335; phone-context=denver@avaya.com; user=phone` matches both the rules. However, Rule 2 is selected for applying the adaptation because Rule 2 matches four fields as compared with three fields in Rule 1.

Presence of URI parameter phone-context and user=

During ingress adaptation, when the phone-context parameter is removed, the adaptation module also removes the URI parameter `user=` if it is present.

During egress adaptation, when the phone-context parameter is inserted, the adaptation module also inserts the URI parameter `user=phone`. However, if the URI parameter `user=phone` is already present, the adaptation module does not insert the parameter. The egress adaptation overwrites the phone-context parameter, if the parameter is present. If the phone-context parameter is present and egress adaptation does not result in a new phone-context, the egress adaptation does not change the original phone-context parameter.

SIP Header Removal

Avaya Aura® Session Manager customers can use the Adaptation Modules to remove specific headers from SIP messages. The administrator defines sets of headers to be removed in the ingress (message entering Session Manager) and egress (messages leaving Session Manager) directions. As part of the Adaptation Module processing, Session Manager removes the specified headers from the messages.

A customer could inadvertently include some of the mandatory and/or required headers in the list of headers to be removed. Session Manager will not remove any mandatory SIP headers, even if the headers are included in the set of exempted headers in adaptations.

The header removal feature does not change the adaptation module selection criteria.

Note:

The SIP Header Removal feature only removes headers. The feature does not remove parameters to decrease the header size. Session Manager removes the headers that are either Avaya proprietary or deemed excessive and unnecessary for non-Avaya elements.

The administrator defines a list of SIP headers to be removed during adaptation module processing on the Adaptation Details page. The list of headers to be removed are defined as

name-value pairs, with multiple headers separated by a comma. The header names in the list are case-insensitive. The maximum length of the **Value** field for the headers list is 1024 characters.

The administrator uses the parameters, **eRHdrs** (egress Remove Headers) and **iRHdrs** (ingress Remove Headers). The **eRHdrs** parameter identities the headers to be removed in messages going in the egress direction (messages leaving Session Manager). The **iRHdrs** parameter identifies the headers to be removed in messages going in the ingress direction (messages entering Session Manager).

As an example: There are two headers: P-Charging-Vector and P-Location headers. To remove these headers from the SIP messages, perform the following:

Note:

If the header removal feature deletes the SIP header **Priority: emergency**, emergency calls may fail in some cases. Also, if the feature removes the headers such as **End Point View** and **Correlation-ID** , some call transfers may fail.

Removing SIP header

About this task

The administrator defines a list of SIP headers to be removed during adaptation module processing on the Adaptation Details page. The list of headers to be removed are defined as name-value pairs, with multiple headers separated by commas. The header names in the list are case-insensitive. The maximum length of the **Value** field for the headers list is 1024 characters.

The administrator uses the parameters, egress Remove Headers (eRHdrs) and ingress Remove Headers (iRHdrs). The eRHdrs parameter identifies the headers to be removed in messages going in the egress direction or messages leaving Session Manager. The iRHdrs parameter identifies the headers to be removed in messages going in the ingress direction or messages entering Session Manager.

Example: The two headers in the SIP messages are: P-Charging-Vector and P-Location headers.

Procedure

1. Navigate to **Home** > **Elements** > **Routing** > **Adaptations**.
2. On the Adaptation Details page, click **New**.
3. In the **Adaptation Name** field, type the adaptation name.
4. In the **Module Name** field, select the DigitConversionAdapter option.
5. In the **Module Parameter Type** field, select the Name-Value Parameter option.
6. Click **Add** to add the name and value parameters.
7. In the **Name** field, type eRHdrs.
8. In the **Value** field, type `"P-Charging-Vector, P-Location"`.
9. Click **Commit**.

Note:

If the header removal feature deletes the SIP header **Priority: emergency**, emergency calls might fail . Also, if the feature removes the headers such as **End Point View** and **Correlation-ID** , some call transfers might fail.

Adaptation examples

Example 1

In the following example, an adaptation is needed for international calls for the AT&T service provider.

For incoming calls, AT&T sends the 11-digit local number in 1 NPA NXX XXXX format. To convert this number into E.164, Session Manager must add a plus sign (+), there by converting the number to +1 NPA NXX XXXX format. Specify the following values:

- Matching pattern = 1
- Min = 11
- Max = 11
- Phone-Context =
- Delete Digits = 0
- Insert Digits = +
- Address to modify = both

For outgoing calls to AT&T, Session Manager must convert the E.164 form to a format that AT&T supports, either 1+10 digits for North America calls or 011+country code + number for international calls. For calls to North America, specify the following values:

- Matching Pattern = +1
- Min = 12
- Max = 12
- Phone-Context =
- Delete Digits = 1
- Insert Digits = <None>
- Notes = Calls to North America

For calls to Germany, specify the following values:

- Matching Pattern = +49
- Min = 13
- Max = 13
- Delete Digits = 1
- Insert Digits = 011

- Address to modify = destination
- Notes = Calls to Germany

Example 2

The following is an example of how to set up an adaptation with phone-context:

Ingress adaptation rule:

- Matching pattern = 53
- Min = 4
- Max = 4
- Phone-Context = site1
- Delete Digits = 0
- Insert Digits = 908
- Address to modify = both

Egress adaptation rule:

- Matching pattern = 908
- Min = 7
- Max = 7
- Phone-Context = site1
- Delete Digits = 3
- Insert Digits =
- Address to modify = both

Input (String prior to the adaptation processing)	Adaptation Processing	Output (String after the adaptation processing)
`5335; phone-context = site1@avaya.com; user = phone`	Ingress adaptation	`9085335@avaya.com`
`9085335@avaya.com`	Egress adaptation	`5335; phone-context = site1@avaya.com; user = phone`

Example 3

Session Manager supports phone-context with a global number prefix, the plus + sign. If the incoming request contains the phone-context parameter with a number starting with +, Session Manager prefixes the user part with the contents of the phone-context before invoking the routing lookup. Session Manager uses the resulting string for routing purposes only and does not modify the user part. The following examples illustrate this point:

R-URI	Ingress Adapter Rule	Resulting R-URI	Routing Notes
`8885335;phone-context=+1303@avaya.com;user=phone`	Matching pattern: 888 Min: 7 Max: 7 Phone-Context: Delete Digits: 3 Insert Digits: 538 Address to modify: both **Note:** Phone-Context string is empty.	`5385335;phone-context=+1303@avaya.com;user=phone`	Session Manager uses the string `+13035385335@avaya.com` for routing purposes.
`5385335;phone-context=+1303@avaya.com;user=phone`	Matching pattern: 538 Min: 7 Max: 7 Phone-Context: +1303 Delete Digits: 0 Insert Digits: +1303 Address to modify: both	`+13035385335@avaya.com`	Session Manager uses the string `+13035385335@avaya.com` for routing purposes.

In the first example (row 1), the phone-context is empty in the ingress adaptation rule. Because the adaptation rule requires matching on three fields (pattern, min and max), the incoming INVITE contains the phone-context parameter. If the phone-context field is empty, the match succeeds and the adaptation is applied. However, the adaptation does not change the phone-context parameter. This example also shows the backward-compatibility case where adaptation is applied on the user part without modifying the phone-context parameter. On receiving this INVITE, Session Manager performs routing lookup based on `+13035383535` to determine the destination. Here, Session Manager only changes the phone number and not the phone-context parameter.

In the second example (row 2), the ingress adaptation rule contains `+1303` in the phone-context field. Also, the incoming INVITE contains the phone-context parameter with value of `+1303`. Because the ingress adaptation rule requires matching all four fields, the match succeeds and the adaptation is applied, which changes the R-URI. On receiving this INVITE, Session Manager performs routing lookup based on the updated R-URI.

Creating Adaptations

You can add URI parameters to the Request-URI. For example, you can append the parameter user=phone for all INVITEs routing to a particular SIP entity. You administer the egress Request-URI parameters on the Adaptation Details page in the **Egress URI Parameters** field.

The format is the string that you need to append to the Request URI. The string must conform to the augmented BNF defined for the SIP Request URI in RFC3261. A leading ';' is optional. The entry `;user=phone;custApp=1` is equivalent to `user=phone;custApp=1`.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Adaptations**.
2. Click **New**.
3. Enter a descriptive name for the **Adaptation Name**.

4. In the **Module Name** field, select an Adaptation module from the drop-down menu.
5. In the **Module Parameter Type** field, select the parameter type from the drop-down menu.
   - If the **Module Parameter Type** is **Single Parameter**, enter the appropriate value in the **Module Parameter** field.
   - If the **Module Parameter Type** is **Name-Value Parameter**:
     a. Click **Add**.
     b. In the **Name** field, enter a module parameter name that does not contain white space.
     c. In the **Value** field, enter the module parameter value.
     d. Repeat adding **Name** and **Value** parameters as needed.
6. In the **Egress URI Parameters** field, enter a name for URI parameters to append to the Request-URI on outgoing calls.
7. In the **Notes** field, enter description about the adaptation module.
8. Ingress adaptation provides digit manipulation for calls coming into the Session Manager instance. To configure ingress digit conversion:
   a. Click **Add** in the Digit Conversion for Incoming Calls to SM section.
   b. Enter the matching pattern. The **Matching Pattern** field can have 1 to 36 characters. Mouse over the input field to view a tool tip describing the valid input.
   c. Enter the number of minimum and maximum digits to be matched in the **Min** and **Max** fields respectively.
   d. Add **Phone Context** as an optional parameter for the ingress adaptation rules.
   e. In the **Delete Digits** field, enter the number of digits that you want to delete from the left side of the dialed number.
   f. In the **Insert Digits** field, enter the digits that you want to insert before the dialed number.
   g. In the **Address to modify** field, select a value from the drop-down menu.
   h. Enter any additional or special adaptation information in **Adaptation Data** field.

      The adaptation data can be up to 20 characters in length including alpha characters, numeric characters 0-9, +, *, #, and -.
   i. Continue clicking the Ingress Adaptation **Add** button until you have configured all the required ingress matching patterns.
9. To remove a matching pattern for ingress adaptations, select the check box next to the pattern and click **Remove**.
10. Egress adaptation provides digit manipulation for calls going out of the Session Manager instance. To configure egress digit conversion:
    a. Click **Add** under the Digit Conversion for Outgoing Calls from SM section.
    b. Enter the **Matching Pattern**. Mouse over the input field to view a tool tip describing the valid input.

c. Enter the number of minimum and maximum digits to be matched in the **Min** and **Max** fields respectively.

d. Add **Phone Context** as an optional parameter for the egress adaptation rules.

e. In the **Delete Digits** field, enter the number of digits that you want to delete from the left side of the dialed number.

f. In the **Insert Digits** field, enter the digits that you want to insert before the dialed number.

g. In the **Address to modify** field, select a value from the drop-down menu.

h. Enter any additional or special adaptation information in **Adaptation Data** field.

Note:

In the case of the Verizon Unscreened ANI feature, the data entered in the outgoing **Adaptation Data** field is verified to ensure that it complies with the required format of a Screened Telephone Number (STN).

i. Continue clicking the Egress Adaptation **Add** button until you have configured all the required egress matching patterns.

11. To remove a matching pattern for egress adaptations, select the check box next to that pattern and click **Remove**.
12. Click **Commit**.

Modifying Adaptations

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Adaptations**.
2. Select the appropriate adaptation.
3. Click **Edit**.
4. Change the appropriate fields as necessary.
5. Click **Commit**.

Deleting Adaptations

You can delete more than one adaptation at the same time.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Adaptations**.
2. Select the adaptation or adaptations you want to delete.

3. Click **Delete**.
4. Click **Delete** on the confirmation page.

Installed vendor adapters

Avaya Media Server Adapter

The Avaya Media Server requires a request URI in the form **<token>@domain**. Typically, you can administer a Session Manager with a regular expression to route calls to a media server. However, regular expression routing does not support location-based routing such as dial pattern routing.

If a customer wants to perform location-based routing or domain routing to an Avaya Media Server, the customer can define a dial pattern and use the AMSAdapter on egress to the AMS to change the request-URI. The AMSAdapter does not perform any digit conversion. The AMSAdapter only converts the request-URI.

You configure the adapter with one parameter, **amsuri**. If the value of the **amsuri** parameter contains a complete URI, for example, **amsuri=user@domain**, both the user and the host parts of the URI will be replaced. If the value of the **amsuri** parameter does not contain the **@** symbol, for example, **amsuri=ce-msml**, then only the user part of the request-URI will be replaced.

AT&T Adapter

AT&T does not handle the History-Info header. On egress to AT&T, the adaptation module, AttAdapter, removes any History-Info headers in a request or response. Messages from AT&T do not change. The AT&T Adapter also performs all the conversions available by the Digit Conversion Adapter.

CS1000 Adapter (CS1000Adapter)

The CS1000 adapter provides the following services:

- Translation between History-Info header formats.
- Origination routing based on the presence of `x-nt-net-feature=x-nt-home` in the Request-URI.

x-nt-home routing

The CS1000 adapter requires special origination based routing when the `x-nt-net-feature` parameter is in the Request-URI with the value of `x-nt-home`. During ingress adaptation, the CS1000 adapter looks for this parameter, value pair. If it is found, the call is routed on the URI in the P-Asserted-Identity header rather than the Request-URI.

History-Info header adaptation

Since the CS1000 adapter uses some different formatting for the History-Info header than other Avaya products, it is necessary to adapt the History-Info header values. Two primary areas of formatting differences requiring adaptation are index values and reason code values.

Index format: The CS1000 adapter increments its indices by adding a value of 1. For example: 1, 2, 3, 4. Avaya products increment its indices after the decimal dot. For example: 1, 1.1, 1.2, 1.3.

The CS1000 adapter on ingress converts the values from the integer format to the decimal format. The CS1000 adapter on egress converts the values from the decimal format to the integer format.

Reason Code adaptation: Avaya uses two reason parameters in its History-Info header format. The second parameter is labeled *Redirection* and must be inserted on ingress and removed on egress by the CS1000 adapter. The *Redirection* phrase also contains a `Cause` parameter. The *Redirection Cause* is inserted to make the CS1000 History-Info look like the call forwarding History-Info sent from Communication Manager according to the following mapping:

SIP Cause	Redirection Reason
302	CFI
486	CFB
480	CFNR

Example

A conversion from Avaya format to CS1000 format:

Avaya History-Info:

```
History-Info:<sip:orig@avaya.com>;index=1
History-Info:"Original Destination"<sip:orig@avaya.com?Reason=SIP%3Bcause%3D302%3Btext
%3D%22Moved%20Temporarily%22&Reason=Redirection%3BCause%3DCFI>;index=1.1
History-Info:"Final Destination"<sip:final@avaya.com>;index=1.2
```

gets converted to:

```
CS 1000 History-Info:
History-Info:<sip:orig@avaya.com?Reason=SIP%3Bcause%3D302%3Btext%3B%22Moved
%20Temporarily%22>;index=1, <sip:final@avaya.com>;index=2
```

Example

A conversion from CS1000 format to Avaya format:

CS1000 History-Info:

```
History-Info: <sip:7521;phone-context=cdp.udp@testbed1.com;user=phone?reason=%20sip
%3bcause%3d480%3btext%3d%20%Temporarily%20Unavailable%22>; index=1,
<sip:5522;phone-context=cdp.udp@testbed1.com;user=phone>;index=2
```

gets converted to:

Avaya History-Info:

```
History-Info:<sip:canonically-adjusted-7521@testbed1.com;user=phone>;index=1
History-Info:<sip:canonically-adjusted-7521@testbed1.com;user=phone? Reason=SIP%3Bcause
%3D480%3Btext%3D%22Temporarily%20Unavailable%22&Reason=Redirection%3Bcause%3DNORMAL
%3avaya-cm-reason%3D%22cover-no-reply%22>;index=1.1
History-Info: <sip:canonically-adjusted-5522@testbed1.com;user=phone>;index=1.2
```

Multiple Diversions:

When CS1000 sends History-Info with multiple diversions, the top History-Info will have the original calling number, and the second History-Info will have the last redirect number (CS1000 can send only 2 diversion History-Infos). In Session Manager, the CS1000 adapter copies the original calling number History-Info to the second-to-last History-Info during ingress adaptation. For example:

CS1000 History-Info:

```
History-Info: <sip:1001;phone-context=cdp.udp@interop.com;user=phone?reason=sip%3bcause
%3d302%3btext%3d%22Moved%20Temporarily%22>;index=1, <sip:1002;phone-
context=cdp.udp@interop.com;user=phone?reason=sip%3bcause%3d480%3btext%3d%22Temporarily
%20Unavailable%22>;index=2, <sip:1003;phone-
context=cdp.udp@interop.com;user=phone>;index=3
```

gets ingress adapted to:

```
History-Info: <sip:canonically-adjusted-1001@interop.com>;index=1
History-Info: <sip:canonically-adjusted-1001@interop.com;user=phone?
reason=SIP;cause=302;text="Moved Temporarily"&Reason=Redirection;Cause="CFI">;index=1.1
History-Info:<sip:canonically-adjusted-1002@interop.com;user=phone?
reason=SIP;cause=480;text="Temporarily
Unavailable"&Reason=Redirection;cause="CFNR">;index=1.2
History-Info: <sip:canonically-adjusted-1001@interop.com;user=phone?
reason=SIP;cause=302;text="Moved Temporarily"&Reason=Redirection;Cause="CFI">;index=1.3
History-Info: <sip:canonically-adjusted-1003@interop.com;user=phone>;index=1.4
```

If `copyOCNHistInfo=false` is given as an adaptation module parameter, then the CS1000 adapter behaves as it did in prior Session Manager releases and does not copy the original calling number History-Info.

On egress, the CS1000 adapter removes the copied History-Info header when a call is routed from one CS 1000 to another CS 1000.

The CS1000 adapter also performs all the conversions available in the *DigitConversionAdapter*.

Cisco Adapter and Diversion Type Adapter

Cisco Adapter (CiscoAdapter) provides two basic header manipulations: converting between Diversion and History-Info headers and converting between P-Asserted-Id and Remote-Party-Id headers. IETF does not accept Diversion and Remote-Party-Id headers. The Diversion and Remote-Party-Id headers are replaced by History-Info and P-Asserted-Identity respectively but are still used in the Cisco products. CiscoAdapter also performs all the conversions available by the Digit Conversion Adapter.

Note:

DiversionTypeAdapter performs the same function as the CiscoAdapter for Avaya Business Communication Manager systems.

Diversion to History-Info Header Adaptation

Cisco requires the use of the Diversion header, rather than the History-Info header to provide information related to how and why the call arrives to a specific application or user. The following examples illustrate the adaptations.

Example 1:

Communication Manager user 66600001 forwards to Cisco user 60025.

The outgoing INVITE of Communication Managerhas this history-info:

```
History-Info: "<sip:66600001@ny.avaya.com>;index=1
History-Info: "stn 66600001" <sip:66600001@ny.avaya.com?
    Reason=SIP%3Bcause%3D302%3Btext%3D%22Moved%20Temporarily%22
    &Reason=Redirection%3Bcause%3DCFI>;index=1.1
History-Info: <sip:600025@ny.avaya.com>;index=1.2
```

In the message sent to Cisco this is converted to:

```
Diversion: "stn 66600001" <sip:66600001@ny.avaya.com>;reason=no-
answer;privacy=off;screen=no
```

Example 2:

Communication Manager user calls Cisco user 60025. This call is routed to Modular Messaging at extension 688810.

The INVITE message from the Cisco server contains the following Diversion Header:

```
Diversion: "Ken's Desk" <sip:600025@ny.avaya.com>;reason=user-
    busy;privacy=off;screen=no
```

The message is adapted and the outgoing INVITE to MM replaces the Diversion header with the following:

```
History-Info: <sip:600025@ny.avaya.com>;index=1
History-Info: "Ken's Desk" <sip:600025@ny.avaya.com?
    Reason=SIP%3Bcause%3D486%3Btext%3D%22Busy%20Here%22
    &Reason=Redirection%3Bcause%3DNORMAL%3Bavaya-cm-reason%3D%22
    cover-busy%22%3Bavaya-cm-vm-address-digits%3D81080000%3Bavaya-cm-vm-address-handle
%3Dsip:80000%40avaya.com>;index=1.1
History-Info: "MM" <sip:688810@ny.avaya.com>;index=1.2
```

Remote-Party-Id to P-Asserted-Identity Header Adaptation

Cisco requires information in the P-Asserted-Identity (PAI) header to be received in the Remote-Party-Id (RPI) header. Any incoming message containing a P-Asserted-Identity header being routed to Cisco replaces that header with the Remote-Party-Id header. Similarly, calls from Cisco containing the Remote-Party-Id header are converted to a P-Asserted-Identity header when routed to non-Cisco entities.

Example 3:

A call is placed from 12345 at Communication Manager and routed to the Cisco PBX.

The INVITE from Communication Manager contains:

```
P-Asserted-Identity: “Ryan” <sip:12345@avaya.com>
```

This header is converted to RPI when the request is sent to the Cisco PBX:

```
Remote-Party-Id: “Ryan”
<sip:12345@avaya.com>;party=called;screen=no;privacy=off
```

Example 4:

A call is placed from 23456 at Cisco PBX and routed to Communication Manager.

The INVITE from Cisco PBX contains:

```
Remote-Party-Id: “Ryan”
<sip:23456@avaya.com>;party=called;screen=no;privacy=off
```

This header is converted to PAI when the request is sent to Communication Manager:

```
P-Asserted-Identity: “Ryan” <sip:23456@avaya.com>
```

Modular Messaging Adapter

The Modular Messaging Adapter (Modular Messaging Adapter) adaptation module is required only if you have the following elements:

- Session Manager Release 6.1.2 and later.
- Modular Messaging system with software earlier than release 5.2 Service Pack 7.
- A SIP entity that uses one of the other adaptations as listed above and that uses Modular Messaging as its voice messaging system.

You do not need this adaptation if the only entity in your network that can send calls to Modular Messaging is Communication Manager.

In Session Manager Release 6.1.2 and later, the CS1000 Adapter and other adaptation modules convert from Diversion to History-Info output. This History-Info format contains call forwarding diversion information instead of what looks like Communication Manager coverage history-info which can be interpreted correctly by Modular Messaging 5.2 Service Pack 7 and higher.

The Modular Messaging Adapter converts this History-Info into a format that looks like the information came from Communication Manager to indicate a covered call, which conforms to the History-Info format supported by earlier releases of Modular Messaging.

Orange Adapter

The Orange Adapter (OrangeAdapter) is a module for the service provider Orange. The OrangeAdapter is derived from the VerizonAdapter and performs the same History-Info to Diversion adaptation as the Verizon adapter and all the digit conversions available by the Digit Conversion Adapter. In addition, the OrangeAdapter looks for SDP on INGRESS only of requests and responses. If the adapter finds an SDP indicating an Orange offer or answer of G.729, such as the m= line contains the payload type 18, and if there is no fmtp:18 line containing the string 'annexb', then it adds or replaces an 'a=fmtp:18 annexb=no' line in the SDP. This is because the Orange network only supports G.729A and signals G.729B. Finally, OrangeAdapter modifies how Session Manager generates the P-Asserted-Identity header in a request or a response if it is not present on ingress from Orange. The default behavior of the Session Manager is overridden and the PAI is generated from the From header in requests and To header in responses.

Note:

This means that anything calling Orange sees what it supplied in the To header as the connected party number.

Orange does not insert PAI in 1xx/2xx responses and their contact header does not contain connected party information.

Verizon Adapter

The Verizon adapter (VerizonAdapter) requires the same History-Info to Diversion adaptations that the Cisco Adapter uses. The Verizon Adapter also performs all the conversions available by the Digit Conversion Adapter.

Verizon egress adapter inserts a special Screened Telephone Number (STN) into the Diversion header of all outgoing calls which utilize Verizon as the Service Provider.

This enables Verizon to identify the physical location of the endpoint that is being used to make an outgoing call and to create the needed billing or tariff data as well as to provide the proper routing of E911 emergency calls.

This feature is called the Verizon Unscreened ANI feature.

Administering Verizon ANI feature

Procedure

1. On the Adaptation Details page, administer the *Module name* field as *VerizonAdapter* so that the adaptation can be associated with the Verizon Adapter.
2. In the *Digit Conversion for Outgoing Calls from SM* section,
   a. Enter one or more *Matching Patterns* that are to be used to identify which origination numbers (PAI) are associated with a given physical location.
   b. Enter the Screened Telephone Number (STN) that corresponds with that location in the *Adaptation Data* field.

   When the Verizon Adapter processes an egress call, the PAI number associated with the call is compared with the various Matching Patterns administered in the *Digit Conversion for Outgoing Calls from SM* section. In addition, the domain of the PAI should be an SM authoritative domain.

   - If there is a match, the data administered in the *Adaptation Data* field is incorporated into the Diversion header for that call and the call continues with its normal routing procedures.
   - If there is no match, the system continues to function as per design.

   Note:

   - If a match occurs on a row with STN filled-in then the History-Info to Diversion header conversion is not done by VerizonAdapter since either a STN or the converted History-Info can be inserted into the Diversion header. So effectively the STN takes precedence in such cases.
   - *Address to modify* field must be set to *origination* or *both* for STN feature to work. Session Manager does not populate STN into the Diversion header on a *destination* address match.
   - If no digit conversion is to be done (that is, matching pattern is there only to specify the STN), then the user should set *Delete Digits* field to 0 and leave *Insert Digits* field as blank.

Adaptations field descriptions

Use this page to create, modify, delete, and manage adaptations.

Button	Description
New	Create a new adaptation.
Edit	Modify the information of an adaptation.
Delete	Delete an adaptation.
Duplicate	Duplicate the selected adaptation and assign a new state to it
More Actions > **Import**	Import data from XML files or zip file containing one or more XML files.
More Actions > **Export Adaptations**	Export the adaptation data as an XML file to a specified location.
More Actions > **Export all data**	Export the routing entities data as a compressed file to a specified location.
More Actions > **Manage Modules**	Provides management of custom adaptation modules. **Note:** For Avaya Professional Services use only.

Name	Description
Name	The name of the adaptation. The name must be unique and be between 3 and 64 characters in length.
Module name	The name of the Adaptation Module.
Module Parameters	The contents of the Adaptation Module.
Egress URI Parameters	The terminating trunk group parameters.
Notes	Other information you wish to add.

Adaptation Details field descriptions

General section

Name	Description
Adaptation name	Name of the adaptation. Must be unique and from 3 to 64 characters in length.
Module Name	Name of the module from the drop-down menu.

Table continues…

Name	Description
Module Parameter Type	The module parameter can be one of the following types: • No parameter. • Single Parameter. The Module Parameter must not contain any white spaces. • Name-Value Parameter. Selecting this option displays a table for you to add or remove multiple lines of Name-Value pairs. **Note:** 1. A module parameter name must not contain any white space. 2. Enclose the value in double quotation marks if the value contains the space character. Within the value field, you can include a double quotation mark by using \" . Supported adaptation module parameters are: • **fromto:** If set to **true**, the adaptation modifies From and To headers of the message. If omitted or set to any other value, From and To headers are not modified. • **multipartMIMEsupported (MIME):** (Optional) This adaptation applies to the egress processing only. If the parameter is present and set to **no**, then multipart MIME message bodies will be stripped on egress from Session Manager. If the multipart MIME message contained an SDP message body, it will be inserted as the only message body in the outgoing message. If omitted or set to any other value, message bodies will not be modified. EGRESS Domain Modification Parameters • `overrideDestinationDomain (` can be abbreviated to `odstd)`**:** {parameter #1 if not named}, replaces the domain in Request-URI, To header (if administered), Refer-To header, and Notify/message-summary body with the given value for egress only. • `overrideSourceDomain (` can be abbreviated to `osrcd)`**:** replaces the domain in the From header (if administered), P-Asserted-Identity

Table continues…

Name	Description
	header and calling part of the History-Info header with the given value for egress only. INGRESS Domain Modification Parameters: • `ingressOverrideDestinationDomain ( iodstd)` : replaces the domain in Request-URI, To header (if administered), and Notify/message-summary body with the given value for ingress only. • `ingressOverrideSourceDomain (` can be abbreviated to `iosrcd)` : replaces the domain in the From header (if administered), P-Asserted-Identity header and calling part of the History-Info header with the given value for ingress only.
Egress URI Parameters	The terminating trunk group parameters. URI parameters can be added to the Request-URI. For example, the parameter “user=phone” can be appended for all INVITEs routing to a particular SIP entity. The egress Request-URI parameters are administered from the Adaptation Details using the Egress URI Parameters field. The field's format is the string that should be appended to the Request URI. The string must conform to the augmented BNF defined for the SIP Request URI in RFC3261. A leading ';' is optional. Entry “;user=phone;custApp=1” is equivalent to “user=phone;custApp=1”.
Notes	Optional information that you wish to add.

Digit Conversion for Incoming Calls to SM section

Button	Description
Add	Adds digit conversion for incoming calls for the adaptations.
Remove	Removes digit conversion from incoming calls for the adaptations.

Name	Description
Select check box	Use this check box to select and use the digit conversion for the incoming calls
Matching Pattern	Pattern to match for the incoming calls. The pattern can have between 1 and 36 characters. Roll over the field for the valid pattern.

Table continues…

Name	Description
Min	Minimum number of digits to be matched. The minimum value can be 1 or more.
Max	Maximum number of digits to be matched. The maximum value can be any number up to 36.
Phone Context	Optional parameter for the ingress adaptation rules. If the phone-context field of an ingress adaptation module rule contains a valid value (not empty), ingress adaptation is applied only if all four trigger fields (Matching Pattern, Min, Max, and Phone-context) match the header. If the phone-context field is empty, ingress adaptation is applied based on the remaining fields (Matching Pattern, Min, and Max). The allowed format for the Phone Context string can either be an E.164 number (which can contain optional hyphens, periods, or parenthesis) or a domain name (which can contain only alphanumeric characters, a hyphen, and periods).
Delete Digits	Number of digits to be deleted from the dialed number.
Insert Digits	Number of digits to be added before the dialed number.
Address to Modify	A setting of both will look for adaptations on both origination and destination type headers. The digit conversion applied to a header will be taken from the entry with the longest matching pattern.
Adaptation Data	Any additional or special adaptation data up to 20 characters. Valid values: numeric characters 0-9, +, *, #, and -. This is a non-mandatory field.
Notes	Any other details that you wish to add.

Digit Conversion for Outgoing Calls from SM section

Button	Description
Add	Adds digit conversion for outgoing calls for the adaptations.
Remove	Removes digit conversion from outgoing calls for the adaptations.

Name	Description
Select check box	Use this check box to select and use the digit conversion for the outgoing calls.

Table continues…

Name	Description
Matching Pattern	Pattern to match for the outgoing calls. The pattern can have between 1 and 36 characters. Roll over the field for the valid pattern.
Min	Minimum number of digits to be matched. The minimum value can be 1 or more.
Max	Maximum number of digits to be matched. The maximum value can be any number up to 36.
Phone Context	Optional parameter in the action fields for the egress adaptation rules. If the phone-context field of an egress adaptation module rule contains a valid value (not empty), the adaptation module modifies the digits and insert phone-context when the three trigger fields match the criteria, that is, Matching Pattern, Min, and Max. On the other hand, if the phone-context field is empty, the egress adaptation module does not insert phone-context.
Delete Digits	Number of digits to be deleted from the dialed number.
Insert Digits	Number of digits to be added before the dialed number.
Address to Modify	A setting of both will look for adaptations on both origination and destination type headers. The digit conversion applied to a header will be taken from the entry with the longest matching pattern.
Adaptation Data	Any additional or special adaptation data up can be up to 20 characters. Valid values: numeric characters 0-9, +, *, #, and -. This is a non-mandatory field. **Note:** In the case of the Verizon Unscreened ANI feature, the data entered in the outgoing **Adaptation Data** field is verified to ensure that it complies with the required format of a Screened Telephone Number (STN).
Notes	Any other details that you want to add.

Button	Description
Commit	Saves the adaptation details and distributes them to the Session Manager instances in the enterprise.
Cancel	Cancels changes to the adaptation details and returns to the Adaptations page.

Adaptation Module Management field description

Name	Description
Details	Details of adaptation module.
Module	The name of the module.
Module Jar	The name of the module jar file.
Version	The version of the module.
Upload Date	The date on which the module is uploaded.
Deploy Completion Date	The date on which the deployment is completed.
Deploy Status	The status of deployment.
Deploy Count	The count of deployment.

Button	Description
Upload	Uploads a module.
Deploy	Deploys a module.
Undeploy	Undeploys a module.
Delete	Deletes a module.
Audit	Performs the audit of a module.
Done	Closes the page.

Bulk import for Adaptations

When creating an XML bulk import file:

- The name of an adaptation must be unique. Other elements refer to the adaptation name.
- The value of <adaptationmodule> is a combination of the fields *Module Name* and *Module Parameters* in the System Manager user interface. The values are separated by a single space.
- You can configure multiple Ingress and Egress configurations <<EgressadaptationFullTO>, <IngressadaptationFullTO>> for one Adaptation name.
- The values in <addressToModify> are case-sensitive and must be the same as they appear in the System Manager user interface.

Warning:

When you add new digit pattern or adaptation entries to an existing adaptation, you must include all the patterns in the adaptation XML file. You cannot import an adaptation that includes only the new adaptation patterns. When you add new patterns to an existing adaptation, ensure that you export the current adaptation, add new patterns, and then re-import the XML file that includes the current and new patterns.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<adaptationFullTOList>
    <buildNumber>0</buildNumber>
    <implementationVersion>0</implementationVersion>
    <specificationVersion>0</specificationVersion>
    <AdaptationFullTO>
        <adaptationmodule>DigitConversionAdapter osrcd=avaya.com odstd=fr.rnd.avaya.com
iosrcd=avaya.com iodstd=fr.rnd.avaya.com</adaptationmodule>
        <egressuriparameters></egressuriparameters>
        <name>frscrush4 Adaptation</name>
        <EgressadaptationFullTO>
            <deletedigits>0</deletedigits>
            <insertdigits></insertdigits>
            <matchingpattern>8223</matchingpattern>
            <maxdigits>5</maxdigits>
            <mindigits>5</mindigits>
            <addressToModify>both</addressToModify>
        </EgressadaptationFullTO>
        <IngressadaptationFullTO>
            <deletedigits>0</deletedigits>
            <insertdigits></insertdigits>
            <matchingpattern>8223</matchingpattern>
            <maxdigits>5</maxdigits>
            <mindigits>5</mindigits>
            <addressToModify>both</addressToModify>
        </IngressadaptationFullTO>
    </AdaptationFullTO>
    <AdaptationFullTO>
        <adaptationmodule>CS1000Adapter iodstd=avaya.com iosrcd=avaya.com</
adaptationmodule>
        <egressuriparameters></egressuriparameters>
       <name>CS_1000_Adaptation</name>
        <EgressadaptationFullTO>
            <deletedigits>8</deletedigits>
            <insertdigits></insertdigits>
            <matchingpattern>+1613</matchingpattern>
            <maxdigits>12</maxdigits>
            <mindigits>12</mindigits>
            <phoneContext>cdp.udp</phoneContext>
            <addressToModify>both</addressToModify>
        </EgressadaptationFullTO>
        <EgressadaptationFullTO>
            <deletedigits>5</deletedigits>
            <insertdigits>+1613</insertdigits>
            <matchingpattern>+1614</matchingpattern>
            <maxdigits>12</maxdigits>
            <mindigits>12</mindigits>
            <addressToModify>both</addressToModify>
        </EgressadaptationFullTO>
        <EgressadaptationFullTO>
            <deletedigits>2</deletedigits>
            <insertdigits></insertdigits>
            <matchingpattern>+1615</matchingpattern>
            <maxdigits>12</maxdigits>
            <mindigits>12</mindigits>
            <phoneContext>+1</phoneContext>
            <addressToModify>both</addressToModify>
        </EgressadaptationFullTO>
        <EgressadaptationFullTO>
            <deletedigits>4</deletedigits>
            <insertdigits></insertdigits>
            <matchingpattern>3333343</matchingpattern>
            <maxdigits>11</maxdigits>
```

```
            <mindigits>11</mindigits>
            <phoneContext>udp</phoneContext>
            <addressToModify>both</addressToModify>
        </EgressadaptationFullTO>
        <EgressadaptationFullTO>
            <deletedigits>8</deletedigits>
            <insertdigits>3</insertdigits>
            <matchingpattern>33333434</matchingpattern>
            <maxdigits>11</maxdigits>
            <mindigits>11</mindigits>
            <phoneContext>cdp.udp</phoneContext>
            <addressToModify>both</addressToModify>
        </EgressadaptationFullTO>
        <EgressadaptationFullTO>
            <deletedigits>2</deletedigits>
            <insertdigits></insertdigits>
            <matchingpattern>603</matchingpattern>
            <maxdigits>6</maxdigits>
            <mindigits>6</mindigits>
            <phoneContext>cdp.udp</phoneContext>
            <addressToModify>both</addressToModify>
        </EgressadaptationFullTO>
        <EgressadaptationFullTO>
            <deletedigits>3</deletedigits>
            <insertdigits></insertdigits>
            <matchingpattern>603</matchingpattern>
            <maxdigits>7</maxdigits>
            <mindigits>7</mindigits>
            <phoneContext>cdp.udp</phoneContext>
            <addressToModify>both</addressToModify>
        </EgressadaptationFullTO>
        <IngressadaptationFullTO>
            <deletedigits>4</deletedigits>
            <insertdigits></insertdigits>
            <matchingpattern>1413</matchingpattern>
            <maxdigits>11</maxdigits>
            <mindigits>11</mindigits>
            <addressToModify>both</addressToModify>
        </IngressadaptationFullTO>
        <IngressadaptationFullTO>
           <deletedigits>5</deletedigits>
            <insertdigits></insertdigits>
            <matchingpattern>+1413</matchingpattern>
            <maxdigits>12</maxdigits>
            <mindigits>12</mindigits>
            <addressToModify>both</addressToModify>
        </IngressadaptationFullTO>
        <IngressadaptationFullTO>
            <deletedigits>5</deletedigits>
            <insertdigits>6</insertdigits>
            <matchingpattern>+141366</matchingpattern>
            <maxdigits>12</maxdigits>
            <mindigits>12</mindigits>
            <addressToModify>both</addressToModify>
        </IngressadaptationFullTO>
        <IngressadaptationFullTO>
            <deletedigits>0</deletedigits>
            <insertdigits>3333</insertdigits>
            <matchingpattern>344</matchingpattern>
            <maxdigits>7</maxdigits>
            <mindigits>7</mindigits>
            <phoneContext>udp</phoneContext>
            <addressToModify>both</addressToModify>
        </IngressadaptationFullTO>
        <IngressadaptationFullTO>
```

```
            <deletedigits>3</deletedigits>
            <insertdigits>6</insertdigits>
            <matchingpattern>413</matchingpattern>
            <maxdigits>10</maxdigits>
            <mindigits>10</mindigits>
            <phoneContext>+1</phoneContext>
            <addressToModify>both</addressToModify>
        </IngressadaptationFullTO>
        <IngressadaptationFullTO>
            <deletedigits>4</deletedigits>
            <insertdigits>6</insertdigits>
            <matchingpattern>4137</matchingpattern>
            <maxdigits>10</maxdigits>
            <mindigits>10</mindigits>
            <phoneContext>udp</phoneContext>
            <addressToModify>both</addressToModify>
        </IngressadaptationFullTO>
        <IngressadaptationFullTO>
            <deletedigits>3</deletedigits>
            <insertdigits>3333344</insertdigits>
            <matchingpattern>500</matchingpattern>
            <maxdigits>7</maxdigits>
            <mindigits>7</mindigits>
            <phoneContext>cdp.udp</phoneContext>
            <addressToModify>both</addressToModify>
        </IngressadaptationFullTO>
    </AdaptationFullTO>
</adaptationFullTOList>
```

SIP Entities

A SIP network consists of a number of SIP entities. Examples of a SIP Entity include:

- Session Manager
- Communication Manager
- Session Border Controller
- SIP trunks

With the Endpoint Concentrator type, you can have up to 1000 connections from a single IP address. The single IP address can be shared by multiple Windows instances running on a virtualized server. SIP Link Monitoring is disabled for this SIP Entity type.

When Session Manager receives a request where the host part of the request-URI is the IP address of the Session Manager, the Session Manager associates one of the administered domains with the port on which the request was received. For more information about failover groups, see Failover Groups on page 465.

In cases when Session Manager cannot associate any administered routing policies, the request is sent to the SIP entity that is administered as an outbound proxy. If no outbound proxy is provisioned, then Session Manager will proxy the request on its own.

The system searches the IP Address by default when any string is configured in the Credential Name. The Credential name is a regular expression string and follows Perl version 5.8 syntax. The following are examples of entering information in the Credential name:

- For `www.sipentity.domain.com`, enter the string `www\.sipentity\.domain\.com`.
- For `192.14.11.22`, enter the string `192\.14\.11\.22`.
- You can search for a subset of the string or you can create a wild card search. For example, to search for `domain.com` as a substring, enter the string `domain\.com`.

Authentication of trusted SIP Entities

Routing uses the following information to authenticate SIP entities by performing validation on the IP/Transport Layer and TLS Layer:

- FQDN or IP Address of the SIP entity.
- Credential name of the SIP entity.
- Protocol of the Entity Links. The protocol is the SIP connection transport type (TCP/TLS/UDP).
- Connection Policy of the Entity Link. The policy defines whether the entity link is trusted or not.

IP and transport layer validation

Session Manager performs the following validation checks when receiving a request from the network:

- The far-end IP address matches the IP address of one of the SIP Entities configured in ‘Routing’ that have entity links with Session Manager. If a SIP Entity is administered with an FQDN instead of an IP address, Session Manager resolves the FQDN to an IP address while doing the comparison.
- The transport on which the request was received matches the administered transport of one of the entity links associated with this SIP entity and the Session Manager. The Connection Policy of the entity link must be configured as trusted, otherwise Session Manager challenges the request.

Transport Layer Security validation

Session Manager applies the following validations for SIP Transport Layer Security (TLS) connections:

1. During a TLS handshake, the Identity Certificate of the SIP Entity is validated against the trusted CA certificate repository in the Session Manager for SIP TLS connections. If this mutual TLS authentication fails, Session Manager does not accept the connection.

Note:

With Session Manager, you can enforce certificate validation for SIP endpoints. Session Manager establishes the connection with the SIP endpoints based on the settings in the TLS Endpoint Certificate Validation field.

2. If the mutual TLS authentication is successful, Session Manager performs further validation on the SIP entity Identity Certificate as per the Credential Name or the far-end IP address.
   - If the Credential Name string is empty, the connection is accepted.
   - If the Credential Name string is not empty, the Credential Name and the IP address of the far-end is searched for in the following fields in the identity certificate provided by the SIP entity:
     - CN value from the subject.
     - subjectAltName.dNSName.
     - subjectAltName.uniformResourceIdentifier. For IP address comparison, the IP address string is converted to SIP:W.X.Y.Z before comparison. W.X.Y.Z is the remote socket IPV4 address. The search is case-insensitive.

SIP Responses to an OPTIONS Request

With OPTIONS messages, Session Manager keeps track of the status of the SIP trunks and forwards calls, without any delay, onto entity links that are up or partially down. A partially down entity link indicates that one of the SIP entities is inaccessible and Session Manager must forward calls to other SIP entities that are accessible. By keeping track of the SIP entities that are inaccessible, Session Manager keeps call performance at an acceptable level and enables load balancing or fail-over configurations without the impact of delayed calls.

Sometimes, especially when interfacing with some third party entities, Session Manager receives nonstandard responses. In these situations, the Session Manager cannot determine whether the SIP entity is up or down. On the SIP Entities Details page, in the **SIP Responses to an OPTIONS Request** section, you can specify the list of specific SIP responses to OPTIONS messages for these SIP Entities so that Session Manager can track the SIP responses.

If you do not set this feature, calls can be delayed. When the Session Manager attempts to route a call over an inaccessible SIP entity, the Session Manager waits a specific time, indicated by “Timer B”, before trying for another SIP entity. If multiple SIP entities are involved, the sum of the wait times can cause substantial delays that might have an impact on service.

Deny new service for Entity Links

When in the deny new service state, Entity Links do not accept new incoming calls and Session Manager does not route outgoing calls over these links. Link monitoring continues over these links but no alarms are generated for the denied links.

When placing an Entity Link into the Deny New Service state, you can:

- Take selected SIP Entities out of service for upgrades and repair without receiving numerous SIP Monitoring alarms.
- Test alternate routing paths by denying the primary link Session Manager uses on a given route.
- Deny selected links during a planned WAN outage.

SIP Call Loop elimination

Session Manager can sometimes receive identical INVITE requests within a short interval.

Session Manager sets up separate sessions for each INVITE. Multiple identical INVITE requests can initiate SIP call loops and deplete network resources. Session Manager provides administration features to track and terminate call looping instances in the network.

Loop Administration

You administer loop parameters when you create a SIP entity that is not of **Type** Session Manager on the SIP Entity Details page under **Elements** > **Routing** > **SIP Entities**.

Session Manager rejects requests if the number of incoming requests that have the same combination of the **R-URI**, **To**, **From**, and **PAI** header values reaches the administered **Loop Count Threshold** value within the **Loop Detection Interval** time. The frequency of the call loops is a function of the latency and the number of network elements in the loop path. An administrator must set the Loop Detection parameters based on the customer network configuration. Setting improper values of **Loop Count Threshold** and **Loop Detection Interval** can result in:

- System performance overhead.
- Non-detection of call looping scenarios in the network.

For example, if the successive loop call arrives at Session Manager after 40 milliseconds (because of the propagation delay of the intermediate hops) and the administrator needs to break the loop on the fifth loop call instance, the recommended Firewall configuration must have **Loop Count Threshold** set to 5 and **Loop Detection Interval** set to 200 milliseconds.

Note:

Set the **Loop Count Threshold** value higher than the default value of 5, if the network has:

- Communication Manager administered as IPv6 with ANAT configured
- The **Loop Detection Mode** set to ON

Alarm Generation

The Session Manager SIP Firewall generates a minor-level alarm for a call loop detection event based on the Loop Detection parameters settings. You can administer Loop Detection alarms on the Session Manager Administration page.

When an alarm is generated for the Loop Detection event, Session Manager does not generate any more alarms for the administered **Loop Detection Alarm Threshold** interval after the event. For example, if the **Loop Detection Alarm Threshold** is set to 24 hours and a Loop Detection alarm is generated, the SIP Firewall does not generate any new Loop Detection alarms for the

next 24 hours. During this interval, the SIP Firewall continues to detect and break loops without generating any new alarms, but continues to log loop detection summary events.

Creating SIP Entities

About this task

Use this procedure to create a SIP entity.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **SIP Entities**.
2. Click **New**.
3. In the General window, do the following:
   a. In the **Name** field, type the name of the SIP entity.
   b. In the **IP Address Family** field, click the address types that the SIP entity supports. For more information see IP address family validations.

      For administering SIP entities by using IPv6 address, ensure that on the Global Settings page, the Enable IPv6 check box is selected. If IPv6 is not enabled, the IPv6 and Both options are not available.

      Depending on the IP Address Family that you select, the system displays:

      - For IPv4 IP address family: **FQDN or IPv4 Address** field.
      - For IPv6 IP address family: **FQDN or IPv6 Address** field.
      - For Both address family: **FQDN or IPv4 Address** and **FQDN or IPv6 Address** fields.

        For SIP entities other than Session Manager, if the FQDNs for IPv4 and IPv6 are separate, you must specify both fields with the corresponding IPv4 and IPv6 FQDNs.

        If one FQDN resolves to both IPv4 and IPv6 addresses, fill the **FQDN or IPv4 Address** field. You can leave the **FQDN or IPv6 Address** field blank.

        For Session Manager SIP entities, you must specify only IP addresses.

      Session Manager supports a mixture of FQDN and IPv6 addresses for SIP entities other than Session Manager.
   c. In the **FQDN or IP4 Address** or **FQDN or IP6 Address** fields, type the FQDN or IP address of the SIP entity.
   d. In the **Type** field, click Session Manager as the type of SIP entity.
   e. In the **Notes** field, type information about the SIP entity.
   f. In the **Location** field, click a location.

g. In **Outbound Proxy**, click a proxy. For Session Manager, you must specify an Outbound Proxy.

Note:

h. In the **Time Zone** field, click the default time zone for the SIP entity.

i. In the **Minimum TLS Version**, click TLS version that you want to configure.

Use this field if you want to set the minimum allowed TLS version to a different setting other than the global setting for this sip entity.

j. In the **Credential name** field, type a regular expression string.

For example: To use `www.sipentity.domain.com`, type the string `www\.sipentity\.domain\.com`.

4. For a non-Session Manager SIP Entity type, click the appropriate mode in **Loop Detection Mode**.

The default value of **Loop Detection Mode** is **On**.

5. In the **SIP Link Monitoring** field, click one of the following:

- **Use Session Manager Configuration**
- **Link Monitoring Enabled**
  - In the **Proactive Monitoring Interval (in seconds)** field, type the time. The range is 1 to 9000 seconds, and the default value is 900.
  - In the **Reactive Monitoring Interval (in seconds)** field, type the time. The range is 1 to 900 seconds, and the default value is 120.
  - In the **Number of Tries** field, type a number. The range is 0 to 15, and the default value is 1.
- **Link Monitoring Disabled**

6. To specify the Entity Links:

a. Click **Add**.

b. In the **Name** field, type the name.

c. In the **SIP Entity 1** field, click the required **Session Manager** SIP Entity.

SIP Entity 1 must always be a Session Manager instance.

d. In the **IP Address Family** field, click the address types that the SIP entity supports.

e. In the **Protocol** field, click the appropriate protocol.

f. In the **Port** field, type the required port.

g. In the **SIP Entity 2** field, click the required non-Session Manager SIP Entity.

h. In the **Port** field, type the required port.

This is the port on which you have configured the remote entity to receive requests for the specified transport protocol.

i. In the **Connection Policy** field, click the appropriate policy.

   Session Manager does not accept SIP connection requests or SIP packets from untrusted SIP entities.

j. Click **Deny New Service** to deny service for the associated entity link.

7. **(Optional)** In the **Failover** field, add ports if the SIP entity is a failover group member.

   This step is applicable only for Session Manager SIP entity type.

8. To specify the Port parameters:
   a. Click **Add** in the Port section.
   b. Enter the necessary port and protocol parameters.
   c. To remove an incorrectly added Port, click the respective **Port** and click **Remove**.
9. For OPTIONS requests, in the **Response Code & Reason Phrase** field, add or remove a SIP code and phrase to mark the SIP entity as up or down, respectively.
10. Click **Commit**.

Modifying SIP entities

Note:

- Changes to the protocol and port in the Port section of a Session Manager SIP entity can cause signalling issues in endpoints.
- Changing a Failover Port on the SIP Entity:
  - affects entity links that are auto-generated during failover.
  - affects any other entity links which are unrelated to failover but share the same failover Port.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **SIP Entities**.
2. Select the SIP entity you want to modify.
3. Click **Edit**.
4. Make the necessary changes to the appropriate fields.
5. Click **Commit**.

Deleting SIP Entities

You can delete more than one SIP Entity at the same time.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **SIP Entities**.
2. Select the SIP Entity or Entities you want to delete.
3. Click **Delete**.
4. Click **Delete** on the confirmation page.

Accepting new service for all entity links

Change the service state to accept new service for all entity links of the selected SIP entity or entities.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **SIP Entities**.
2. Select the SIP entity or entities that need to have the service state changed.
3. Click **More Actions** > **Accept new service for all entity links**.
4. Click **Commit**.

Denying new service for all Entity Links

Change the state to deny new service for all entity links of a selected SIP entity.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **SIP Entities**.
2. Select the SIP entity or entities that need to have the service state changed.
3. Click **More Actions** > **Deny new service for all entity links**.
4. Click **Commit**.

IP address family validations

Entity links support an **IP Address Family**, which can be IPv4, IPv6, or both . The following table summarizes the validation rules for the **IP Address Family**:

IP Address Family Type for SIP Entity 1	IP Address Family Type for SIP Entity 2	IP Address Family value on Entity Links Summary page	IP Address Family field on Entity Links add/edit page
IPv4	IPv4	IPv4	Disabled
IPv6	IPv6	IPv6	Disabled
IPv4	IPv6	Link establishment not allowed	NA
IPv6	IPv4	Link establishment not allowed	NA
Both	IPv4	IPv4	Disabled
Both	IPv6	IPv6	Disabled
IPv4	Both	IPv4	Disabled
IPv6	Both	IPv6	Disabled
IPv4 / Both and Part of failover group	IPv4/Both Part of failover group	IPv4	Disabled
IPv6 / Both	IPv6/Both Part of failover group	Ipv6	Disabled
Both/Part of failover group	Both/Part of failover group	drop down with IPv4 (by default) and IPv6	Enabled

SIP Entities field descriptions

Button	Description
New	Create a new SIP entity.
Edit	Modify the selected SIP entity.
Delete	Delete the selected the SIP entity.
Duplicate	Create a duplicate of the selected SIP entity and assign a new state to it.
More Actions > **Display SIP Entity References**	Display the routing policies, adaptations, and locations that correspond to the SIP entity on the Overview of References to SIP Entities page.
More Actions > **Import**	Import from XML files or zip file containing one or more XML files using the Import data page.

Table continues…

Button	Description
More Actions > **Export SIP Entities**	Export the SIP entity data as an XML file to a specified location using the Export SIP Entities page.
More Actions > **Export all data**	Export data for all routing entities as a zipped file to a specified location using the Export all data page.
More Actions > **Deny new service for all Entity Links**	Deny new service for all entity links associated with the selected SIP entities (busyout condition).
More Actions > **Accept new service for all Entity Links**	Accept new service for all entity links associated with the selected SIP entities (released condition).

Name	Description
Name	SIP entity name. This name must be unique and can have between 3 and 64 characters.
IP Address Family	Type of IP addresses that the SIP entity supports. Depending on the IP Address Family that you select, the system displays: • For IPv4 IP address family: **FQDN or IPv4 Address** field. • For IPv6 IP address family: **FQDN or IPv6 Address** field. • For Both address family: **FQDN or IPv4 Address** and **FQDN or IPv6 Address** fields. For SIP entities other than Session Manager, if the FQDNs for IPv4 and IPv6 are separate, you must specify both fields with the corresponding IPv4 and IPv6 FQDNs. If one FQDN resolves to both IPv4 and IPv6 addresses, fill the **FQDN or IPv4 Address** field. You can leave the **FQDN or IPv6 Address** field blank. For Session Manager SIP entities, you must specify only IP addresses.
FQDN or IPv4 Address	Fully qualified domain name or IPv4 address of the SIP entity.
FQDN or IPv6 Address	Fully qualified domain name or IPv6 address of the SIP entity.

Table continues…

Name	Description
Type	The type of SIP entity, such as **Session Manager**. **Note:** You can select the SIP entity type as **ELIN Server**. This type is used by third party E911 services. The services determine the location of a user based on the IP address to send the new ELIN to Session Manager in case of emergency call. The SIP Entity selected as the ELIN server should be resolved through local host name resolution to use either the primary or secondary IP address.
Notes	Additional notes about the SIP entity.

SIP Entity Details — Session Manager type field descriptions

Use this page to specify SIP entity details for the Session Manager type SIP entity.

General

Name	Description
Name	The SIP entity name. This name must be unique and can have between 3 and 64 characters.
IP Address Family	Type of IP addresses that the SIP entity supports. Depending on the IP Address Family that you select, the system displays: • For IPv4 IP address family: **FQDN or IPv4 Address** field. • For IPv6 IP address family: **FQDN or IPv6 Address** field. • For Both address family: **FQDN or IPv4 Address** and **FQDN or IPv6 Address** fields. For SIP entities other than Session Manager, if the FQDNs for IPv4 and IPv6 are separate, you must specify both fields with the corresponding IPv4 and IPv6 FQDNs. If one FQDN resolves to both IPv4 and IPv6 addresses, fill the **FQDN or IPv4 Address** field. You can leave the **FQDN or IPv6 Address** field blank. For Session Manager SIP entities, you must specify only IP addresses.

Table continues…

Name	Description
FQDN or IPv4 Address	Fully qualified domain name or IPv4 address of the SIP entity.
FQDN or IPv6 Address	Fully qualified domain name or IPv6 address of the SIP entity.
Type	Session Manager type SIP entity.
Notes	Additional notes about the SIP entity.
Location	The SIP entity location.
Outbound Proxy	The outbound proxy if the entity type is Session Manager and you want to specify a proxy. **Note:** In cases when Session Manager cannot associate any administered routing policies, the request is sent to the SIP entity administered as an outbound proxy. If no outbound proxy is provisioned, Session Manager will proxy the request on its own.
Time Zone	The default time zone to be used for the entity.
Minimum TLS Version	Minimum allowed TLS versions for the SIP entity. The options are: • Use Global Setting • 1.0 • 1.1 • 1.2 The default option is **Use Global Setting**.

Table continues…

Name	Description
Credential name	The credential name is used for TLS connection validation by searching for this string in the SIP entity identity certificate. • If you do not want to perform the additional validation on the SIP entity identity certificate or are not using SIP TLS for connecting to the SIP entity, leave this field empty. • If you want to verify that a specific string or SIP entity FQDN is present within the SIP entity identity certificate, enter that string or SIP entity FQDN using the regular expression syntax. • If you want to verify that the SIP entity IP address is present within the SIP entity identity certificate, enter the SIP entity IP address using the regular expression syntax. **Note:** The IP Address is searched by default when any string is configured in the Credential Name. The credential name is a regular expression string and follows Perl version 5.8 syntax. For example: For `www.sipentity.domain.com`, enter the string `www\.sipentity\.domain\.com`. For `192.14.11.22`, enter the string `192\.14\.11\.22`. You can search for a subset of the string or you can create a wild card search. For example, to look for `domain.com` as a substring, enter the string `domain\.com`

SIP Link Monitoring

Name	Description
SIP Link Monitoring	Selects the process for SIP Link monitoring. The options are: • Use Session Manager Configuration • Link Monitoring Enabled: When you click this option, the system displays the following fields: **Proactive Monitoring Interval (in seconds)**, **Reactive Monitoring Interval (in seconds)**, and **Number of Retries**. • Link Monitoring Disabled

Table continues…

Name	Description
Enable CRLF Keep Alive Monitoring	The option to enable the monitoring of SIP entity links using CRLF pings. You must enable the following SIP monitoring fields before you enable the CRLF Keep Alive Monitoring mechanism: • **Enable SIP Monitoring** • **SIP Link Monitoring** on the SIP Entity Details page When you select the checkbox, the **Enable CRLF Keep Alive Monitoring** option displays a drop-down list with the following options: • **Use Session Manager Configuration**: Uses the Session Manager configuration to determine whether to monitor SIP entity links. This is the default selection in the drop-down list. You can select this option only if **SIP Link Monitoring** on the SIP Entity Details page is configured to **Use Session Manager Configuration** or **Link Monitoring Enabled**. • **CRLF Monitoring Enabled**: Overrides the Session Manager configuration and uses the CRLF monitoring option to monitor SIP entity links. You can select this option only if **SIP Link Monitoring** on the SIP Entity Details page is configured to **Link Monitoring Enabled**. • **CRLF Monitoring Disabled**: Disables the CRLF-based monitoring of SIP entity links. You can select this option only if **SIP Link Monitoring** on the SIP Entity Details page is configured to **Link Monitoring Enabled** or **Link Monitoring Disabled**. The **Enable CRLF Keep Alive Monitoring** option is disabled by default.
Proactive Monitoring Interval (in seconds)	This value is used for polling the administered SIP entities by the added Session Manager. Monitoring ensures that the entities are still reachable. Proactive monitoring occurs as long as no outages are detected. A value between 1 and 9000 is required. The default is 900 seconds.

Table continues…

Name	Description
Reactive Monitoring Interval (in seconds)	This value is used when proactive monitoring detects that an administered SIP entity is not reachable and changes to a reactive mode. Reactive monitoring continues till the SIP entity responds again. Typically, the value for reactive monitoring should be less than the value for proactive monitoring. A value between 1 and 900 is required. The default is 120 seconds.
Number of Tries	Specifies the number of times Session Manager polls a SIP entity before the SIP entity link is deemed down. A value between 0 and 15 is required. The default is 1.
Number of Successes	Specifies the number of times Session Manager polls a SIP entity before the SIP entity link is deemed up. A value between 0 and 15 is required. The default is 1.
CRLF Ping Interval	Specifies the ping interval between 1 and 900 seconds. The default value of the ping interval is 120 seconds.

Entity Links

Button	Description
Add	Adds the selected entity link.
Remove	Removes the selected entity link.

Name	Description
Name	System auto populates this field based on the name specified on the SIP Entity Details General section.
SIP Entity 1	The SIP entity from the drop-down list. This entity must always be a Session Manager instance.
Protocol	The protocol to use for the entity link.
Port	The port to use for **SIP entity 1**. The default port for TCP and UDP is 5060. The default port for TLS is 5061.
SIP Entity 2	The SIP entity from the drop-down list. This entity need not be a Session Manager entity.
Port	The port to use for SIP entity 2.
IP Address Family	The address family type of the entity link. The options are: • IPv4 • IPv6

Table continues…

Name	Description
Connection Policy	Specifies the policy to use for the entity link. The choices are: • Trusted • Trusted HA: Connection policy for high availability clustered hosts such as Avaya Aura® Contact Center. It is identical to the Trusted Connection Policy except that the TCP Keep Alive window value is 3 seconds. • Untrusted • endpt conc: connection policy for the SIP Entities hosting endpoint concentrators. **Note:** The system should not use the global TLS policy for SIP when establishing connection policy for the SIP Entities hosting endpoint concentrators.
Deny New Service	Denies new service for the associated entity link.

Failover Ports

Session Manager permits assignment of failover group ports if the **IP Address Family** field is set to IPv6 or Both. If a failover group is already present for the primary and secondary Session Manager, you cannot change the IP address family of the related SIP entity.

Name	Description
IPv4 TCP Failover port	The SIP entity TCP failover port.
IPv6 TCP Failover port	The SIP entity TCP failover port. The IPv6 failover port must be between 1024 and 65535. You cannot delete an IPv6 TCP failover port if a Session Manager is connected to the SIP entity which is part of a failover group.

Table continues…

Name	Description
Ipv4 TLS Failover port	The SIP entity TLS failover port. **Note:** • Each Session Manager instance that becomes a failover group member, must designate one failover port per transport type that it supports. Far-end Session Manager instance and failover group peers use this port to forward all call preservation traffic to the Session Manager instance over the transport type. • If Session Manager is a member of a Failover Group, then changing these port values results in automatically updating the **SIP Entity 1** port value of any Entity Links that have this Session Manager as **SIP Entity 1**. The update ensures that the **SIP Entity 1** port of the entity links matches the new value of **TCP Failover port** if the link has transport protocol TCP or the value of **TCP Failover port** if the transport protocol is TLS. These updates ensure the correct functioning of call preservation routing behavior.

Table continues…

Name	Description
Ipv6 TLS Failover port	The SIP entity TLS failover port. **Note:** • Each Session Manager instance that becomes a failover group member, must designate one failover port per transport type that it supports. Far-end Session Manager instance and failover group peers use this port to forward all call preservation traffic to the Session Manager instance over the transport type. • If Session Manager is a member of a Failover Group, then changing these port values results in automatically updating the **SIP Entity 1** port value of any Entity Links that have this Session Manager as **SIP Entity 1**. The update ensures that the **SIP Entity 1** port of the entity links matches the new value of **TCP Failover port** if the link has transport protocol TCP or the value of **TCP Failover port** if the transport protocol is TLS. These updates ensure the correct functioning of call preservation routing behavior. • You cannot delete an IPv6 TLS failover port if a Session Manager is connected to the SIP entity which is part of a failover group.

Listen Ports

Button	Description
Add	Adds the selected port.
Remove	Removes the selected port.

Name	Description
Listen Ports	Adds a Session Manager listening port for each desired transport type and domain name for the endpoints in the customer network. ASM listens for endpoint connections (or datagrams in the case of UDP) on the ports administered in the **Listen Ports** field. This field is also used for establishing the default domain name associated with incoming requests that contain an IP addresses (not domain) in the R-URI and P-Asserted-Identity headers. This default domain will be associated with such requests whether they originate from endpoints or SIP entities. For security reasons, make sure to administer only those ports and transports that the SIP endpoints will connect within the customer network. The IPv6 failover listen port and the listen port must not have different protocols on the same port number. **Note:** These ports are returned in redirection response (301/302) to SIP Register request or HTTP/PPM getHomeServer and getHomeCapabilities responses to the requests received from the SIP users, based on the domain in the incoming request.
Protocol	The protocol that the SIP entity uses. The options are: • TCP • TLS • UDP
Default Domain	The domain of the SIP entity.
Endpoint	The listen port for SIP endpoints. **Note:** You can select only one entry per transport protocol per domain as the endpoint listen port.

Table continues…

Name	Description
IP Address Family	The address family type of the listen port. The options are: • IPv4 • IPv6 • Both If the SIP Entity IP address family is IPv4 or IPv6, the **IP Address Family** field displays a default value of IPv4 or IPv6.
Notes	Additional notes about the port and port parameters.

SIP Responses to an OPTIONS Request

Button	Description
Add	Adds SIP responses that signifies the SIP entity is up or down.
Remove	Removes the selected SIP response.

Name	Description
Response Code & Reason Phrase	Three digit SIP response code and optional reason code signifying that the SIP entity is up or down.
Mark Entity Up/Down	The SIP entity's up or down state in response to an OPTIONS request as per the administered Response Code & Reason Phrase.
Notes	Additional notes about the responses.

Button	Description
Commit	Saves the SIP entity and distributes it to the Session Managers in the enterprise.
Cancel	Cancels the creation or modification of the SIP entity.

SIP Entity Details field descriptions for Non-Session Manager SIP Entity types

The following tables contain the SIP Entity field descriptions for a SIP Entity that is not of **Type** Session Manager.

Note:

Not all of the fields are applicable to all SIP Entity types.

General

Name	Description
Name	SIP Entity name. The name must be unique and have between 3 and 64 characters.
IP Address Family	Type of IP addresses that the SIP entity supports. Depending on the IP Address Family that you select, the system displays: • For IPv4 IP address family: **FQDN or IPv4 Address** field. • For IPv6 IP address family: **FQDN or IPv6 Address** field. • For Both address family: **FQDN or IPv4 Address** and **FQDN or IPv6 Address** fields. For SIP entities other than Session Manager, if the FQDNs for IPv4 and IPv6 are separate, you must specify both fields with the corresponding IPv4 and IPv6 FQDNs. If one FQDN resolves to both IPv4 and IPv6 addresses, fill the **FQDN or IPv4 Address** field. You can leave the **FQDN or IPv6 Address** field blank. For Session Manager SIP entities, you must specify only IP addresses.
Tolerance	Specifies tolerance for IPv4 and IPv6 addresses. The system displays this field for all non-Session Manager SIP entities. The system uses the address family of the connection and the tolerance level of the peer element to determine the SIP signaling constraints. Tolerance level defines the interworking function behavior of the SIP entity. If the SIP entity is non-IP tolerant and the SIP message contains IP address of the opposite address family from the address family of the connection Session Managerdoes one of the following: • Removes the IP address of the opposite address family from the message. • Shifts the IP address to parameters.

Table continues…

Name	Description
FQDN or IPv4 Address	Fully qualified domain name or IPv4 address of the SIP entity. **Warning:** System does not validate FQDN when: • SIP entity supports IPv4 and IPv6 IP family address is created. • FQDN is referred to IPv4 and IPv6 IP address text box where only IPv6 entry exists in LHNR. If the system is set up such that, only IPv6 entry exists in LHNR and an entity link supporting IPv4 address family is created then the calls may fail. The calls fail because the resolution at the time indicates only IPv6 addresses and the IPv4 entity link can't be used.
FQDN or IPv6 Address	Fully qualified domain name or IPv6 address of the SIP entity. **Warning:** System does not validate FQDN when: • SIP entity supports IPv4 and IPv6 IP family address is created. • FQDN is referred to IPv4 and IPv6 IP address text box where only IPv6 entry exists in LHNR. If the system is set up such that, only IPv6 entry exists in LHNR and an entity link supporting IPv4 address family is created then the calls may fail. The calls fail because the resolution at the time indicates only IPv6 addresses and the IPv4 entity link can't be used.
FQDN or IP Address	Fully qualified domain name or IP address of the SIP Entity.

Table continues…

Name	Description
Type	Non-Session Manager type SIP Entity, such as Communication Manager, SIP trunk, or a gateway. **Note:** • You can select the SIP Entity type as **ELIN Server**. This is used by third party E911 services, which determines a user's location based on IP address, to send the new ELIN to the Session Manager for an emergency call. The SIP Entity selected as the ELIN server should be resolved through local host name resolution to use either the primary or secondary IP address. • You can select SIP Entity type as **Survivability Server** for a B5800 Branch Gateway (or Advanced Gateway / Secure Routers and other non-PPM capable devices) for providing local 96xx / 96x1 SIP survivability.
Notes	(Optional) Notes about the SIP Entity.
Adaptation	Assigned adaptation.
Location	The SIP Entity location. Select from a list of previously defined locations.
Time Zone	The default time zone to be used for the entity.
SIP Timer B/F (in seconds)	Amount of time the Session Manager waits for the response from the SIP Entity. The range is 1–32. The default value is 4 seconds.

Table continues…

Name	Description
Credential name	The Credential name is used for TLS connection validation by searching for this string in the SIP Entity identity certificate. • If you do not want to perform the additional validation on the SIP Entity identity certificate or are not using SIP TLS for connecting to the SIP Entity, leave this field blank. • To verify that a specific string or SIP Entity FQDN is present within the SIP Entity identity certificate, enter the string or SIP Entity FQDN using the regular expression syntax. • To verify that the SIP Entity IP address is present within the SIP Entity identity certificate, enter the SIP Entity IP address using the regular expression syntax. **Note:** The IP Address is searched by default when any string is configured in the Credential Name. The Credential name is a regular expression string and follows Perl version 5.8 syntax. Some examples are: For “www.sipentity.domain.com”, enter the string “www\.sipentity\.domain\.com”. For “192.14.11.22”, enter the string “192\.14\.11\.22”. You can search for a subset of the string or you can create a wild card search. For example, to look for “domain.com” as a substring, use the string “domain\.com”
Securable	A securable SIP entity is one which the administrator believes does not expose the signaling and media streams of a call to unauthorized monitoring or modification. If a SIP entity does not meet the constraints imposed on the Secured SIP entities, the SIP entity is considered unsecured even if it is administratively marked securable.

Table continues…

Name	Description
Call Detail Recording	Call Detail Recording (CDR) settings. If CDR is enabled on a Session Manager, a CDR record is generated for a call originating from a non-Session Manager SIP Entity depending on the following settings: • none: CDR is not generated for the calls involving the entity. • ingress: CDR is generated only for calls from the entity. • egress: CDR is generated only for calls to the entity. • both: CDR is generated for call either to or from the entity. If two entities are involved in a call, the CDR settings are combined to determine whether a record should be generated. For instance, if the Session Manager routes a call from entity1 to entity2, and the CDR setting of entity1 is “none” but the CDR setting of entity2 is “ingress” or “both” then a record is generated. CDRs are captured under the `/data/home/CDR_User` directory.
CommProfile Type Preference	This field is visible for the SIP Entity type *Other* only and displays list of all of the administered **CommProfile** types that can be used with this SIP Entity type.

Loop Detection

Name	Description
Loop Detection Mode	The default value is **On**. The **On** value activates Loop Detection monitoring for all the Entity Links associated with the SIP Entity. The **Test Only** value allows the administrator to test and change the settings without rejecting the live calls.
Loop Count Threshold	The default value is 5. The allowed range is 2 to 10,000.
Loop Detection Interval (in msec)	The default value is 200 msec. The allowed range is 10ms to 10,000ms.

SIP Link Monitoring

Name	Description
SIP Link Monitoring	Select the process for SIP Link monitoring. The options are: • Use Session Manager Configuration • Link Monitoring Enabled: When you select this option, the system displays the following fields: **Proactive Monitoring Interval (in seconds)**, **Reactive Monitoring Interval (in seconds)**, and **Number of Retries**. • Link Monitoring Disabled

Table continues…

Name	Description
Enable CRLF Keep Alive Monitoring	The option to enable the monitoring of SIP entity links using CRLF pings. You must enable the following SIP monitoring fields before you enable the CRLF Keep Alive Monitoring mechanism: • **Enable SIP Monitoring** • **SIP Link Monitoring** on the SIP Entity Details page When you select the checkbox, the **Enable CRLF Keep Alive Monitoring** option displays a drop-down list with the following options: • **Use Session Manager Configuration**: Uses the Session Manager configuration to determine whether to monitor SIP entity links. This is the default selection in the drop-down list. You can select this option only if **SIP Link Monitoring** on the SIP Entity Details page is configured to **Use Session Manager Configuration** or **Link Monitoring Enabled**. • **CRLF Monitoring Enabled**: Overrides the Session Manager configuration and uses the CRLF monitoring option to monitor SIP entity links. You can select this option only if **SIP Link Monitoring** on the SIP Entity Details page is configured to **Link Monitoring Enabled**. • **CRLF Monitoring Disabled**: Disables the CRLF-based monitoring of SIP entity links. You can select this option only if **SIP Link Monitoring** on the SIP Entity Details page is configured to **Link Monitoring Enabled** or **Link Monitoring Disabled**. The **Enable CRLF Keep Alive Monitoring** option is disabled by default.
Proactive Monitoring Interval (in seconds)	This value is used for polling the administered SIP Entities by the added Session Manager. Monitoring ensures that the entities are still reachable. Proactive monitoring occurs as long as no outages are detected. A value between 1 and 9000 is required. The default value is 900 seconds.

Table continues…

Name	Description
Reactive Monitoring Interval (in seconds)	This value is used when proactive monitoring detects that an administered SIP Entity is not reachable and changes to a reactive mode. Reactive monitoring continues till the SIP Entity responds again. Typically, the value for reactive monitoring should be less than the value for proactive monitoring. A value between 1 and 900 is required. The default value is 120 seconds.
Number of Tries	Specifies the number of times the Session Manager polls a SIP Entity before the SIP Entity is considered unreachable.
Number of Successes	Specifies the number of times the Session Manager polls a SIP Entity before the SIP Entity is considered reachable.
Supports Call Admission Control	Enable or disable CAC management for the SIP Entity. If enabled, the Session Manager does not perform CAC on outgoing calls.
Shared Bandwidth Manager	Enable or disable the Shared Bandwidth attribute for this SIP Entity. If you select this option, you must also specify one or two Session Manager instances that support the PUBLISH API to this SIP Entity.
Primary Session Manager Bandwidth Association	Primary Session Manager instances that supports the PUBLISH API to this SIP Entity.
Backup Session Manager Bandwidth Association	Backup Session Manager instances that supports the PUBLISH API to this SIP Entity, in case the primary fails.

Entity Links

Name	Description
Override Port & Transport with DNS SRV	Select the check box to override Local Host Name Resolution or DNS routing. • If you select this option, the transport and port information is determined using DNS information. You must administer entity links for each transport protocol used to connect to or from the remote entity. • If you do not select this option, the transport and port information is determined using the data administered in the Entity Link table. However, FQDNs are resolved to IP addresses using a DNS server and the Local Hostname Resolution table entries, and only the port and transport data is derived from the Entity Link table.

Button	Description
Add	Add the selected entity link.
Remove	Remove the selected entity link.

Name	Description
SIP Entity 1	Select a SIP Entity from the drop-down list.
Protocol	Protocol to use for the entity link. The options are: • TCP • TLS • UDP
Port	Port to use for SIP Entity 1. Range is 1 to 65535.
SIP Entity 2	Select a SIP Entity from the drop-down list.
Port	Port to use for SIP Entity 2. Range is 1 to 65535. **Note:** If you select the **Override Port & Transport with DNS SRV** check box, the port identified in the DNS SRV or LHNR is used.
IP Address Family	The address family type of the entity link. The options are: • IPv4 • IPv6
Connection Policy	Specifies the policy to use for the entity link. • Trusted. • Trusted HA: connection policy for high availability clustered hosts such as Avaya Aura® Contact Center. This policy is identical to the *Trusted* Connection Policy except that the TCP Keep Alive window value is 3 seconds. • Untrusted. • endpt conc: connection policy for the SIP Entities hosting endpoint concentrators.
Deny New Service	Deny new service for the associated entity link.

SIP Responses to an OPTIONS Request

Button	Description
Add	Add SIP responses that signify if the SIP Entity is up or down.
Remove	Remove the selected SIP response.

Name	Description
Response Code & Reason Phrase	SIP response code and optional reason code signifying that the SIP Entity is up or down.
Mark Entity Up/Down	Mark the SIP Entity as up or down when it responds to an OPTIONS request according to the administered Response Code & Reason Phrase.
Notes	Optional notes about the responses.

Button	Description
Commit	Save the SIP Entity and distribute the information to the Session Manager instances in the enterprise.
Cancel	Cancel the creation or modification of the SIP Entity.

Bulk import for SIP Entities

The following rules apply when creating an XML bulk import file:

- The name of a SIP Entity must be unique. Other elements refer to the SIP Entity name.
- <adaptationName> must either be empty or refer to an existing adaptation with the exact same name. The <adapationName> must either appear in the System Manager database or in an import file that exists in the same import operation as the SIP Entity. SIP Entity of type **ASM** <Avaya Session Manager> cannot contain an adaptation entry.
- <adaptationName> contains the adaptation module name and parameters separated by spaces <examples below>.
- Listen ports (<listenports>) are only relevant for SIP Entity of type **ASM**. Do not include these entries for any other type of SIP Entity.
- Multiple listen ports entries (<listenports>) can be configured for one ASM SIP Entity.
  - <sipdomainName> must refer to an existing domain with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the SIP Entity.
  - The values in <transportprotocol> must appear exactly same (being case sensitive) as they appear in the System Manager user interface.
- The values of <timezoneName> should be same (being case sensitive) as that of the field **Time Zone** in the SIP Entity user interface in System Manager.
- The field <userfc3263> corresponds to the `Override Port & Transport with DNS SRV` check box in the SIP entity form.
- The value of <entitytype> must contain one of the following values, being case sensitive, must exactly appear as follows:
  - CM: Communication Manager in the user interface.

  - ASM: Session Manager in the user interface.
  - Messaging: Session Manager in the user interface.
  - VP: Voice Portal in the user interface.
  - Gateway: Gateway in the user interface.
  - SIP Trunk: SIP Trunk in the user interface.
  - OTHER: Other in the user interface.
- The values in <cdrSetting> are case sensitive and must appear exactly as they appear in the System Manager user interface.
- The field <do_monitoring> corresponds to the field `SIP Link Monitoring` in the SIP Entity details form.
  - To enable SIP Link monitoring, set the <do_monitoring> value to**yes**.
  - To disable SIP Link monitoring, set the <do_monitoring> value to **no**.
  - To use the Session Manager configuration, the <do_monitoring> tag must be completely omitted.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<sipentityFullTOList>
    <buildNumber>0</buildNumber>
    <implementationVersion>0</implementationVersion>
    <specificationVersion>0</specificationVersion>
    <SipentityFullTO>
        <notes></notes>
        <entitytype>ASM</entitytype>
        <fqdnoripaddr>10.64.15.6</fqdnoripaddr>
         <fqdnoripaddr2>2a07:2a42:adc0:14:10:64:15:6</fqdnoripaddr2>
        <ipaddrFamilyType>IPv46</ipaddrFamilyType>
        <ipaddrTolerant>true</ipaddrTolerant>
        <name>Lucifer</name>
        <cac_capable>false</cac_capable>
        <cdrSetting>none</cdrSetting>
        <credentialname></credentialname>
        <crlfKeepAliveSecs>0</crlfKeepAliveSecs>
        <do_monitoring>use-instance</do_monitoring>
        <listenports>
```

```
            <notes></notes>
            <portnumber>5061</portnumber>
            <endpoint>true</endpoint>
            <ipaddrFamily>IPv46</ipaddrFamily>
            <sipdomainName>smgr-hollywood.com</sipdomainName>
             <transportprotocol>TLS</transportprotocol>
        </listenports>
        <listenports>
            <notes></notes>
            <portnumber>5060</portnumber>
            <endpoint>true</endpoint>
            <ipaddrFamily>IPv46</ipaddrFamily>
            <sipdomainName>smgr-hollywood.com</sipdomainName>
            <transportprotocol>TCP</transportprotocol>
         </listenports>
        <loop_detect_interval_msec>200</loop_detect_interval_msec>
        <loop_detect_mode>off</loop_detect_mode>
        <loop_detect_threshold>5</loop_detect_threshold>
        <monitor_okresponses>1</monitor_okresponses>
        <monitor_proactive_secs>900</monitor_proactive_secs>
        <monitor_reactive_secs>120</monitor_reactive_secs>
        <monitor_retries>1</monitor_retries>
        <securable>false</securable>
        <tcp_failover_port>5060</tcp_failover_port>
        <tcp_failover_port_v6>5060</tcp_failover_port_v6>
         <timer_bf_secs>4</timer_bf_secs>
        <timezoneName>Australia/Melbourne</timezoneName>
        <tls_failover_port>5061</tls_failover_port>
        <tls_failover_port_v6>5061</tls_failover_port_v6>
        <userfc3263>false</userfc3263>
    </SipentityFullTO>
    <SipentityFullTO>
```

```
        <notes></notes>
        <entitytype>OTHER</entitytype>
        <fqdnoripaddr>10.64.15.200</fqdnoripaddr>
        <fqdnoripaddr2>2a07:2a42:adc0:14:10:64:15:200</fqdnoripaddr2>
        <ipaddrFamilyType>IPv46</ipaddrFamilyType>
        <ipaddrTolerant>false</ipaddrTolerant>
        <name>CUCM</name>
        <adaptationName>cucmadaptation</adaptationName>
        <cac_capable>false</cac_capable>
        <cdrSetting>none</cdrSetting>
        <credentialname></credentialname>
        <crlfKeepAliveSecs>0</crlfKeepAliveSecs>
        <do_monitoring>use-instance</do_monitoring>
        <loop_detect_interval_msec>200</loop_detect_interval_msec>
        <loop_detect_mode>on</loop_detect_mode>
        <loop_detect_threshold>5</loop_detect_threshold>
        <monitor_okresponses>1</monitor_okresponses>
        <monitor_proactive_secs>900</monitor_proactive_secs>
        <monitor_reactive_secs>120</monitor_reactive_secs>
        <monitor_retries>1</monitor_retries>
        <securable>false</securable>
        <timer_bf_secs>4</timer_bf_secs>
        <timezoneName>America/Fortaleza</timezoneName>
        <userfc3263>false</userfc3263>
    </SipentityFullTO>
```

Example: for IPv4

```
<SipentityFullTO>
 <notes> </notes>
 <entitytype>CM </entitytype>
 <fqdnoripaddr>10.15.64.100 </fqdnoripaddr>
 <ipaddrFamilyType>IPv4 </ipaddrFamilyType>
 <ipaddrTolerant>false </ipaddrTolerant>
 <name>comet </name>
```

```
<cac_capable>false </cac_capable>
<cdrSetting>none </cdrSetting>
<commproftype>CM </commproftype>
<credentialname> </credentialname>
<crlfKeepAliveSecs>1900 </crlfKeepAliveSecs>
<do_monitoring>use-instance </do_monitoring>
<loop_detect_interval_msec>200 </loop_detect_interval_msec>
<loop_detect_mode>on </loop_detect_mode>
<loop_detect_threshold>5 </loop_detect_threshold>
<monitor_okresponses>1 </monitor_okresponses>
<monitor_proactive_secs>900 </monitor_proactive_secs>
<monitor_reactive_secs>120 </monitor_reactive_secs>
<monitor_retries>1 </monitor_retries>
<securable>false </securable>
<timer_bf_secs>4 </timer_bf_secs>
<timezoneName>America/Fortaleza </timezoneName>
<userfc3263>false </userfc3263>
</SipentityFullTO>
```

Example: for IPv46

```
<SipentityFullTO>
    <notes></notes>
    <entitytype>OTHER</entitytype>
    <fqdnoripaddr>10.64.1.202</fqdnoripaddr>
    <fqdnoripaddr2>2a07:2a42:adc0:14:10:64:1:202</fqdnoripaddr2>
    <ipaddrFamilyType>IPv46</ipaddrFamilyType>
    <ipaddrTolerant>false</ipaddrTolerant>
     <name>aSiddharth-uas</name>
    <cac_capable>false</cac_capable>
     <cdrSetting>none</cdrSetting>
    <credentialname></credentialname>
    <crlfKeepAliveSecs>1900</crlfKeepAliveSecs>
    <do_monitoring>no</do_monitoring>
```

```
     <loop_detect_interval_msec>200</loop_detect_interval_msec>
      <loop_detect_mode>on</loop_detect_mode>
    <loop_detect_threshold>5</loop_detect_threshold>
    <monitor_okresponses>1</monitor_okresponses>
    <monitor_proactive_secs>900</monitor_proactive_secs>
     <monitor_reactive_secs>120</monitor_reactive_secs>
    <monitor_retries>1</monitor_retries>
    <routingoriginationName>Delhi</routingoriginationName>
    <securable>false</securable>
    <timer_bf_secs>4</timer_bf_secs>
     <timezoneName>Asia/Kolkata</timezoneName>
    <tlsVersion>1.0</tlsVersion>
    <userfc3263>false</userfc3263>
<SipentityFullTO>
```

SIP Entity References

You can view all references to a SIP entity, such as its location, the routing policy that is created for the SIP entity, and adaptations, if any. If a single SIP entity has more than one combination of these references, the system displays each of the combinations on a separate row.

Displaying SIP Entity References

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **SIP Entities**.
2. Select the check box for a specific SIP entity.
3. Click **More Actions**.
4. Select **Display SIP Entity References** from the drop-down menu.
5. Click **Return** to navigate back to the SIP Entities page.

Overview of References to SIP Entities field descriptions

Name	Description
SIP Entity Name	Name of the SIP Entity.
Location Name	Location associated with the specified SIP entity.
Routing Policy Name	Routing policy associated with the specified SIP entity.
Adaptation Name	Name of the adaptation associated with the SIP entity.

Button	Description
Return	Return to the **SIP Entities** page.

Entity Links

Routing entity links connect two SIP entities through the Session Manager to define the network topology for SIP routing.

- Entity Links connect two SIP entities.
- Trusted Hosts are indicated by assigning the **Trust State** to the link that connects the entities.

Session Manager uses an Entity Link to send or receive messages directly from the entity. You must configure an entity link between Session Manager and any administered SIP entity.

To communicate with other SIP entities in the network, each Session Manager instance must identify the port and transport protocol of the entity link to the SIP entities. The Session Manager listens on the local port for connections from the remote entity using the given transport protocol. If the **Override Port & Transport** check box is selected for the SIP entity, Session Manager uses DNS information to determine the port and transport information to the remote entity. If the **Override Port & Transport** check box is not selected for the SIP entity, Session Manager determines the port and transport information to the remote entity using the data administered in the Entity Link table.

Deny new service state

When in the deny new service state, Entity Links do not accept new incoming calls and Session Manager does not route outgoing calls over these links. Link monitoring continues over these links but no alarms are generated for the denied links.

When placing an Entity Link into the Deny New Service state, you can:

- Take selected SIP Entities out of service for upgrades and repair without receiving numerous SIP Monitoring alarms.
- Test alternate routing paths by denying the primary link Session Manager uses on a given route.

- Deny selected links during a planned WAN outage.

Creating Entity Links

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Entity Links**.
2. Click **New**.
3. Type the name in the **Name** field.
4. Enter the SIP entity 1 by selecting the required **Session Manager** SIP entity from the drop-down list and provide the required port.

   SIP entity 1 must always be a Session Manager instance.

   The default port for TCP and UDP is 5060. The default port for TLS is 5061.
5. Enter the SIP entity 2 by selecting the required non-Session Manager SIP entity from the drop-down list and provide the required port.

   The port is the port on which you have configured the remote entity to receive requests for the specified transport protocol.
6. In the **IP Address Family** field, select the IP address family.
7. From the **Connection Policy** drop-down menu, select **Trusted**.

   Session Manager does not accept SIP connection requests or SIP packets from untrusted SIP entities.
8.
9. Click **Commit**.

Modifying Entity Links

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Entity Links**.
2. Select the entity link you need to modify.
3. Click **Edit**.
4. Make the required changes.

   Note:

   SIP Entity 1 *must* always be a Session Manager instance.
5. Click **Commit**.

Deleting Entity Links

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Entity Links**.
2. Select the Entity Link or Links you want to delete.
3. Click **Delete**.
4. Click **Delete** on the confirmation page.

Accepting new service for the selected Entity Links

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Entity Links**.
2. Select the appropriate Entity Link or links.
3. Click **More Actions** > **Accept new service for selected Entity Links**.
4. On the Accept New Service Confirmation page, click **Commit**.

Denying new service for selected Entity Links

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Entity Links**.
2. Select the appropriate Entity Link or links.
3. Click **More Actions** > **Deny new service for selected Entity Links**.
4. On the Deny New Service Confirmation page, click **Commit**.

Entity Links field descriptions

Button	Description
New	Create a new entity link.
Edit	Change the information for the selected entity link.
Delete	Delete the selected entity link.

Table continues…

Button	Description
Duplicate	Duplicate the selected entity link and assign a new state to it.
More Actions > **Import**	Import data from XML files or a zip file containing one or more XML files using the Import data page.
More Actions > **Export Entity Links**	Export the entity links data as an XML file to a specified location using the Export Entity Links page.
More Actions > **Export all data**	Export the data for all routing elements as a zipped file to a specified location using the Export all data page.
More Actions > **Deny new service for selected Entity Links**	Deny new service for selected entity links.
More Actions > **Accept new service for selected Entity Links**	Accept new service for selected entity links.

Name	Description
Name	Name of the SIP entity link. The name must be unique and can have 3 to 64 characters.
SIP Entity 1	Name of the SIP Entity 1. This SIP Entity must be a Session Manager.
Protocol	Protocol to use for the entity link.
Port	Port to be used for SIP Entity 1. The default port for TCP and UDP is 5060. The default port for TLS is 5061.
SIP Entity 2	Name of the SIP Entity 2. These are the non-Session Manager type SIP entities.
DNS Override	Indicates that the **Override Port & Transport with DNS SRV** check box is selected on the SIP Entity Details page.
Port	Port to use for SIP Entity 2.
IP Address Family	Address type of the SIP entity. The options are: • IPv4 • IPv6

Table continues…

Name	Description
Connection Policy	Specifies the connection policy to use for the entity link. The choices are: • Trusted • Trusted HA: Connection policy for high availability clustered hosts such as AACC. It is identical to the Trusted Connection Policy except that the TCP Keep Alive window value is 3 seconds. • Untrusted • endpt conc
Deny New Service	Deny new service for the entity link.
Notes	Additional information about the entity link.

Bulk import for Entity Links

When creating an XML bulk import file:

- The name of an Entity Link must be unique.
- <entityName1> , <entityName2> must refer to an existing SIP Entity with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the Entity Link.
- The values in <transportProtocol> must appear exactly same, being case sensitive, as they appear in the System Manager user interface.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<entitylinkFullTOList>
    <buildNumber>0</buildNumber>
    <implementationVersion>0</implementationVersion>
    <specificationVersion>0</specificationVersion>
    <EntitylinkFullTO>
        <connectionPolicy>trusted</connectionPolicy>
        <listenPortEntity1>5060</listenPortEntity1>
        <listenPortEntity2>5060</listenPortEntity2>
        <name>asm18 to cpv4</name>
        <serviceState>normal</serviceState>
        <transportProtocol>TCP</transportProtocol>
        <trusted>true</trusted>
        <entityName1>asmblade18</entityName1>
        <entityName2>cpvirtual4</entityName2>
    </EntitylinkFullTO>
    <EntitylinkFullTO>
        <notes></notes>
        <connectionPolicy>trusted</connectionPolicy>
        <listenPortEntity1>17000</listenPortEntity1>
        <listenPortEntity2>17000</listenPortEntity2>
        <name>asmblade10_asmblade24_17000_TCP</name>
        <serviceState>normal</serviceState>
        <transportProtocol>TCP</transportProtocol>
        <trusted>true</trusted>
        <entityName1>asmblade10</entityName1>
```

```
        <entityName2>asmblade24</entityName2>
    </EntitylinkFullTO>
    <EntitylinkFullTO>
        <notes></notes>
        <connectionPolicy>trusted</connectionPolicy>
        <listenPortEntity1>5060</listenPortEntity1>
        <listenPortEntity2>5060</listenPortEntity2>
        <name>asmblade10_FakeSM_5060_TCP</name>
        <serviceState>normal</serviceState>
        <transportProtocol>TCP</transportProtocol>
        <trusted>true</trusted>
        <entityName1>asmblade10</entityName1>
        <entityName2>FakeSM</entityName2>
    </EntitylinkFullTO>
</entitylinkFullTOList>
```

Example: for IPv6 and IPv4

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<entitylinkFullTOList>
<buildNumber>0</buildNumber>
<implementationVersion>0</implementationVersion>
<specificationVersion>0</specificationVersion>
<EntitylinkFullTO>
<notes></notes>
<connectionPolicy>trusted</connectionPolicy>
<ipaddr_family>IPv6</ipaddr_family>
<listenPortEntity1>5060</listenPortEntity1>
<listenPortEntity2>5060</listenPortEntity2>
<name>sm-169_cmdummy_5060_UDP</name>
<serviceState>normal</serviceState>
<transportProtocol>UDP</transportProtocol>
<trusted>true</trusted>
<entityName1>sm-169</entityName1>
<entityName2>cmdummy</entityName2>
</EntitylinkFullTO>
<EntitylinkFullTO>
<notes></notes>
<connectionPolicy>trusted</connectionPolicy>
<ipaddr_family>IPv4</ipaddr_family>
<listenPortEntity1>5061</listenPortEntity1>
<listenPortEntity2>5061</listenPortEntity2>
<name>import sm_import cm_5061_TLS</name>
<serviceState>normal</serviceState>
<transportProtocol>TLS</transportProtocol>
<trusted>true</trusted>
<entityName1>import sm</entityName1>
<entityName2>import cm</entityName2>
</EntitylinkFullTO>
</entitylinkFullTOList>
```

Time Ranges

Use the Time Ranges page to create, modify, delete, and manage time ranges for each administered Routing Policy.

You must specify as many Time Ranges as necessary to cover all hours and days in a week for each administered Routing Policy. For example:

- Routing Policy A can be in effect on all weekdays from 9:00 a.m. to 5:59 p.m.
- Routing Policy B can be in effect on all weekdays from 6:00 p.m. to 9 a.m.
- Routing Policy C time ranges can be in effect on weekends.

These three Time Ranges together determine how calls should be routed throughout the week.

Routing Policies that a Session Manager server selects can be prioritized based on time-of-day routing information. Based on this selection, Session Manager:

- determines the current time at the destination entity. The current time on the Session Manager is converted to the time at the destination SIP Entity using the administered time zone.
- finds the Time Range that you administered. The Time Range contains the time at the destination.
- finds the rank that you administered on the Routing Policy for the selected Time Range.

After the selection, Session Manager orders the Routing Policies in ascending order and tries one route in each priority as per the administered order.

Note:

Priorities must not overlap. If the priorities overlap, the order of routing policies that have the same priorities will be random.

Creating Time Ranges

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Time Ranges**.
2. Click **New**.
3. Enter the name, then select the required days by entering the start and end times and notes for the new time range. Start times start with the first second of the hour:minute. End Times go through the last second of the end hour:minute.
4. Click **Commit**.

Modifying Time Ranges

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Time Ranges**.

2. Select the time range you need to change.
3. Click **Edit**.
4. Make the necessary changes.
5. Click **Commit**.

Deleting Time Ranges

You can delete more than one Time Range at a time.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Time Ranges**.
2. Select the Time Range or Ranges you want to delete.
3. Click **Delete**.
4. Click **Delete** on the confirmation page.

Time Ranges field descriptions

Use the Time Ranges page to create, modify, delete, and manage time ranges.

Button	Description
New	Opens the Time Ranges page where you can create new time ranges.
Edit	Opens the Time Ranges page where you can modify the time range details.
Delete	Opens the Delete Confirmation page for confirming or canceling the deletion of the time range.
Duplicate	Creates a duplicate of the selected time range and assigns a new state to it.
More Actions > **Import**	Opens the Import data page where you can import the time ranges from XML files or zip file containing one or more XML files.
More Actions > **Export Time Ranges**	Opens the Export Time Ranges page where you can export the time ranges data as an XML file to a specified location.
More Actions > **Export all data**	Opens the Export all data page where you can export data for all the routing entities as a zipped file to a specified location.

Field	Description
Name	Name for the time range.
Days (Mo to Su)	Days of the week for which the time range is defined.
Start Time	Start time for the time range. Use 24-hour time format.
End Time	End time for the time range. Use 24-hour time format.
Notes	Additional notes.

Time Range List field descriptions

Use this page to define or modify a Time Range.

Name	Description
Name	Name for the Time Range. It can have between three and 64 characters. The name cannot contain the following characters: <, >, ^, %, $, @, #, *
Mon to Sun	Selected check box indicates the days of the week applicable for the Time Range.
Start Time	Start time for the Time Range. For a 24–hour Time Range, the start time is 0.00.
End Time	End time for the Time Range. For a 24–hour Time Range, the end time is 23:59.
Notes	Additional notes about the Time Range.

Button	Description
Select	Selected Time Range is assigned to the Routing Policy.
Cancel	Cancels the changes to the Time Range.

Bulk import for Time Ranges

When creating an XML bulk import file, the name of a Time Range must be unique. Other elements refer to the Time Range name.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<timerangeFullTOList>
    <TimerangeFullTO>
        <notes>this is a test</notes>
```

```
        <includesFriday>true</includesFriday>
        <includesMonday>true</includesMonday>
        <includesSaturday>false</includesSaturday>
        <includesSunday>false</includesSunday>
        <includesThursday>true</includesThursday>
        <includesTuesday>true</includesTuesday>
        <includesWednesday>true</includesWednesday>
        <name>regularweek</name>
        <startTime>00:00:00</startTime>
        <stopTime>23:59:00</stopTime>
    </TimerangeFullTO>
    <TimerangeFullTO>
        <notes></notes>
        <includesFriday>false</includesFriday>
        <includesMonday>false</includesMonday>
        <includesSaturday>true</includesSaturday>
        <includesSunday>true</includesSunday>
        <includesThursday>false</includesThursday>
        <includesTuesday>false</includesTuesday>
        <includesWednesday>false</includesWednesday>
        <name>weekend</name>
        <startTime>00:00:00</startTime>
        <stopTime>23:59:00</stopTime>
    </TimerangeFullTO>
    <TimerangeFullTO>
        <notes>Time Range 24/7</notes>
        <includesFriday>true</includesFriday>
        <includesMonday>true</includesMonday>
        <includesSaturday>true</includesSaturday>
        <includesSunday>true</includesSunday>
        <includesThursday>true</includesThursday>
        <includesTuesday>true</includesTuesday>
        <includesWednesday>true</includesWednesday>
        <name>24/7</name>
        <startTime>00:00:00</startTime>
        <stopTime>23:59:00</stopTime>
    </TimerangeFullTO>
</timerangeFullTOList>
```

Routing Policies

Use the Routing Policies page to create and modify routing policies.

All Routing Policies together form the **Enterprise wide dial plan**.

Routing Policies can include the **Origination of the caller**, the **Dialed digits** of the called party, the **Domain** of the called party and the actual time the call occurs.

Optionally, you can define a **Regular Expression** in place of the **Dialed digits** and the **Domain** of the called party.

Session Manager determines the destination of the call depending on one or more inputs as mentioned above.

If you qualify the destination using the **Deny** option, Session Manager does not route the call.

Session Manager uses the data configured in the routing policy to find the best match against the number or address of the called party.

Note:

If Session Manager cannot match any dial patterns, Session Manager then attempts to find a matching regular expression. Session Manager examines each regular expression in the administered Rank Order and determines if the expression matches the request-URI. During this comparison, user parameters are not stripped; however, the request-URI is compared against each regular expression twice. The first time, the entire request-URI is compared. The second time, if there is no match, only user@host is compared, that is the URI scheme, sip:, sips:, tel:, and any URI parameters appearing after the host-part of the request-URI are stripped. If there is a match, Session Manager selects routing policies according to the administered regular expressions.

Creating Routing Policies

Procedure

1. On the System Manager Web Console, under **Elements**, click **Routing** > **Routing Policies**.
2. Click **New**.
3. Under the General section, type a routing policy name and notes in the relevant fields.
4. In the **Retries** field, type the number of retries for the destination SIP entity.

   Note:

   The default value in **Retries** field is zero. The valid values are 0-5.
5. Select the **Disabled** check box to disable the routing policy.
6. Under the **SIP Entity as Destination** section, click **Select** to select the destination SIP entity for this routing policy.
7. Select the required destination and click **Select**.
8. Under the **Time of Day** section, click **Add** to associate the Time of Day routing parameters with this Routing Policy.
9. Select the Time of Day patterns that you want to associate with this routing pattern and click **Select**.

   If there are gaps in the selected Time of Day coverage pattern, Session Manager displays a warning message. If such gaps exist in the Time of the Day coverage, randomness in routing selections may be observed.
10. Type the relative rankings that you want to associate with each Time Range. Lower ranking values indicate higher priority.
11. Under the Dial Patterns and Regular Expressions sections, click **Add** to associate existing Dial Patterns and Regular Expressions with the Routing Policy.
12. Select a dial pattern from the pattern list or a regular expression from the regular expression list, and click **Select**.

Note:

This field can be left blank. The routing policy can be added to the dial pattern or regular expression when you add it.

13. Under the Dial Patterns and Regular Expressions sections, click **Remove** to dissociate existing Dial Patterns and Regular Expressions with the Routing Policy.
14. Select a dial pattern from the pattern list or a regular expression from the regular expression list, and click **Select**.
15. Click **Commit**.

Modifying Routing Policies

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Routing** > **Routing Policies**.
2. Select a routing policy for modification.
3. Click **Edit**.
4. In the **General** section, modify a routing policy name and add notes in the relevant fields if required.
5. In the **Retries** field, enter the number of retries for the destination SIP entity.

   Note:

   The default value in **Retries** field is zero. The valid values are 0-5.
6. Select the **Disabled** check box to disable the routing policy.
7. In the **SIP Entities as Destination** section, click **Select** to select another destination SIP entity for this routing policy if required.
8. Select the required destination and click **Select**.
9. In the **Time of Day** section, click **Add** to associate another Time of Day routing parameters with this Routing Policy, if required.
10. Select the Time of Day patterns that you want to associate with this routing pattern and click **Select**.

    If there are gaps in the selected **Time of Day** coverage pattern, the Session Manager displays a warning message. If such gaps exist in the Time of the Day coverage, randomness in routing selections may be observed.
11. Enter the relative rankings that you want to associate with each Time Range. Lower ranking values indicate higher priority.
12. If you need to dissociate the Time of Day routing parameters from this Routing Policy, click **Remove** from the Time of Day section.

13. In Dial Patterns or Regular Expressions, click **Add** to associate existing Dial Patterns and Regular Expressions with the Routing Policy. Select a dial pattern from the pattern list or a regular expression from the regular expression list and click **Select**.

    If you have not specified the dial patterns or regular expressions, you can add the routing policy to the dial pattern or regular expression when you add them later.

14. In **Dial Patterns or Regular Expressions**, click **Remove** to dissociate existing Dial Patterns and Regular Expressions with the Routing Policy.
15. Select another dial pattern, if required, from the pattern list or a regular expression from the regular expression list and click **Select**.
16. Click **Commit**.

Deleting Routing Policies

When you delete a routing policy, all dial patterns and regular expressions associated with the routing policy are also deleted.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Routing Policies**.
2. Select the routing policy or policies you want to delete.
3. Click **Delete** on the confirmation page.
4. Click **Delete**.

Routing Policies field descriptions

Use this page to create, modify, delete, and manage routing policies.

Button	Description
New	Create a new routing policy.
Edit	Modify the selected routing policy.
Delete	Delete the selected routing policy.
Duplicate	Create a duplicate of the selected routing policy and assigns a new state to it.
More Actions > **Import**	Import routing policy data from XML files or a zip file containing one or more XML files.
More Actions > **Export Routing Policies**	Export the routing policy data as an XML file to a specified location.
More Actions > **Export all data**	Export data for all the routing entities as a zipped file to a specified location.

Name	Description
Name	Name of the routing policy.
Disabled	Indicates the routing policy is disabled and should not be used.
Retries	Number of retries for the destination SIP entity. Valid values are 0-5. The default is 0.
Destination	SIP Entity as Destination.
Notes	Additional information about the routing policy.

Routing Policy Details field descriptions

Use this page to specify the details for creating or modifying a routing policy.

General section

Name	Description
Name	Name of the routing policy.
Disabled	Indicates that the routing policy is disabled and should not be used.
Retries	Number of retries for the destination SIP entity. The valid values are 0-5. The default value is 0.
Notes	Additional information about the routing policy.

SIP Entity as Destination section

Button	Description
Select	Display the SIP Entity List page to select a SIP Entity as a destination and associate the SIP Entity to the selected routing policy.

Name	Description
Name	SIP Entity name. The name must be unique and can have between 3 and 64 characters.
FQDN or IP Address	Fully qualified domain name or IP address of the SIP entity.
Type	SIP entity type, such as a Session Manager , Communication Manager, SIP trunk, or a gateway.
Notes	Additional information about the SIP entity.

Time of Day section

Button	Description
Add	Add a new time of the day to the selected routing policy.
Remove	Remove the selected time of day entry from the selected routing policy.
View Gaps/Overlaps	Selecting a time of day entry and selecting **View Gaps/Overlaps** generates a Duration Lists report. The report displays any gaps or overlaps in the time of day entries for each day of the week.

Name	Description
Ranking	Ranking of the assigned Time Ranges.
Name	Name of the Time Ranges.
Days (Mo to Su)	Days of the week specified for the time range.
Start Time	Start Time of the Time Range.
End Time	End Time of the Time Range.
Notes	Additional information.

Dial Patterns section

Button	Description
Add	Add a new dial pattern to the selected routing policy.
Remove	Remove the selected dial pattern from the selected routing policy.

Name	Description
Pattern	Dial pattern to match. The pattern can have between 1 and 36 characters.
Min	Minimum number of digits to be matched.
Max	Maximum number of digits to be matched.
Emergency Call	Indicate if this is an emergency call.
SIP Domain	Domain for which you want to restrict the dial pattern.
Originating Location	Origination Location Name.
Notes	Additional information.

Regular Expressions section

Button	Description
Add	Add a new regular expression to the selected routing policy.
Remove	Remove the selected regular expression from the selected routing policy.

Name	Description
Pattern	Regular expression pattern for Session Manager to match.
Rank Order	Priority of the pattern. A lower rank order means higher priority.
Deny	Deny routing for a matched regular expression pattern.
Notes	Additional information.

Button	Description
Commit	Save the routing policy changes and distribute the changes to the Session Manager instances in the enterprise.
Cancel	Cancels changes to the routing policy.

SIP Entity List field descriptions

Name	Description
Name	Select a SIP entity name check box from the list to associate it to the selected routing policy.
FQDN or IP Address	Displays the fully qualified domain name or IP address of the SIP entity.
Type	Displays the type of the SIP entity such as Session Manager, Session Border Controller, Communication Manager, Voice Portal, Gateway, SIP Trunk, or Other entities.
Notes	Additional information.

Button	Description
Select	Confirm selection of the SIP entity for associating to the routing policy.
Cancel	Cancel the changes for the SIP entity.

Time Range List field descriptions

Use this page to define or modify a Time Range.

Name	Description
Name	Name for the Time Range. It can have between three and 64 characters. The name cannot contain the following characters: <, >, ^, %, $, @, #, *
Mon to Sun	Selected check box indicates the days of the week applicable for the Time Range.
Start Time	Start time for the Time Range. For a 24–hour Time Range, the start time is 0.00.
End Time	End time for the Time Range. For a 24–hour Time Range, the end time is 23:59.
Notes	Additional notes about the Time Range.

Button	Description
Select	Selected Time Range is assigned to the Routing Policy.
Cancel	Cancels the changes to the Time Range.

Pattern List field descriptions

Name	Description
Pattern	Dial pattern to match. The pattern can have between 1 and 36 characters.
Min	Minimum number of digits to be matched.
Max	Maximum number of digits to be matched.
Emergency Call	Indicate if this is an emergency call. **Note:** • Up to 100 emergency numbers can be assigned for each location. • This emergency dial number must match the emergency dial number in the 96xx settings file for all SIP phones in the identified location. Failure to follow this guideline can result in users being unable to dial emergency numbers.

Table continues…

Name	Description
SIP Domain	Domain for which you want to restrict the Dial Pattern.
Originating Location	Name of the location associated with the Dial Pattern.
Notes	Additional information.

Button	Description
Select	Associate the selected pattern to the Routing Policy.
Cancel	Cancel the changes.

Regular Expression List field descriptions

Name	Description
Regular Expression	Displays the regular expression to be used for the selected routing policy.
Rank Order	Priority of the regular expression. Lower rank order means a higher priority.
Deny	Deny routing for a matched regular expression.
Notes	Additional information for the regular expression.

Button	Description
Select	Associates the selected regular expression to a routing policy or dissociates it based on the Add or Remove option selected earlier.
Cancel	Cancel the changes for the association or dissociation of the regular expression.

Bulk import for Routing Policies

Use the following rules while creating an XML bulk import file:

- The name of a routing policy <referred to as routing policy> is unique and is referred to by other elements.
- <sipentityName> must refer to an existing SIP element with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the Routing Policy.
- Multiple time of day entries, <timeofdayNames>, can be configured for one Routing Policy.
  - <timerangeName> must refer to an existing Time Range with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the Routing Policy.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<routingpolicyFullTOList>
    <RoutingpolicyFullTO>
        <notes>this is a test</notes>
        <disabled>false</disabled>
        <name>toBerlin</name>
        <sipentityName>BerlinCM</sipentityName>
        <timeofdayNames>
            <rank>1</rank>
            <timerangeName>regularweek</timerangeName>
        </timeofdayNames>
        <timeofdayNames>
            <rank>0</rank>
            <timerangeName>24/7</timerangeName>
        </timeofdayNames>
    </RoutingpolicyFullTO>
</routingpolicyFullTOList>
```

Dial Patterns

A dial pattern specifies routing policies to route a call based on the digits dialed by a user. The system matches a dial pattern and then routes the call based on the dial pattern. Session Manager matches the dialed digits after applying any administered ingress adaptation.

The system also uses the following to determine how to route the call:

- the originating location of the call.
- the domain in the request-URI.
- the Global Settings option of the **Better Matching Dial Pattern or Range in Location ALL Overrides Match in Originator's Location** on the Session Manager Administration page.

The following sections describe the dial pattern look-up method with respect to the Global Setting option.

If the Global Settings option is not selected:

1. Session Manager compares the user-part of the Request-URI with all dial patterns valid for the originating location where the domain matches the domain in the Request-URI. A Dial Pattern is valid for a particular location if :
   - the location in the dial pattern matches the originating location.
   - the dial pattern is for **ALL** locations.
2. Dial patterns that match the originating location are considered before dial patterns for **ALL** locations. If a dial pattern for the originating location matches the digits, dial patterns for **ALL** locations are ignored.
3. If no matching dial patterns are found, the domain in the Request-URI is modified to remove one level of subdomain until only a top-level domain is left. For example, if **dr.avaya.com** does not match, Session Manager attempts to match **avaya.com**. If **avaya.com** does not match, Session Manager then attempts to match **.com**, which fails.

4. If more than one Dial Pattern matches, Session Manager selects the Dial Pattern with the longest matching pattern.

If the Global Settings option is selected:

1. Session Manager compares the user-part of the Request-URI with all dial patterns valid for the originating location where the domain matches the domain in the Request-URI. Only dial patterns matching the location are considered.
2. If no matching dial patterns are found, the domain in the Request-URI is modified to remove one level of subdomain until only a top-level domain is left. For example, if **dr.avaya.com** does not match, Session Manager attempts to match **avaya.com**. If **avaya.com** does not match, Session Manager then attempts to match **.com**, which fails.
3. If more than one dial pattern matches,Session Manager selects the dial pattern with the longest matching pattern.
4. Similarly, dial patterns administered for **ALL** locations are also compared.
5. The comparison may result in two matching dial patterns, one for **ALL** locations and one for a specific location. Session Manager select the longest matching pattern. A longer pattern administered for **ALL** locations overrides a location-specific pattern. If both matching patterns are of the same length, then both patterns are examined for wildcard characters. If one pattern contains a wildcard and the other does not, then the pattern without a wildcard is selected. If both patterns contain a wildcard, then the location-specific pattern is selected.

Examples - Global Settings option is selected:

Location Specific Pattern	ALL Locations Pattern	Chosen Pattern
1303538	1303538	Location-Specific
130353	1303538	ALL Locations
1303538	130353	Location-Specific
130353x	1303538	ALL Locations
1303538	130353x	Location-Specific
1x	1303538	ALL Locations
13035xx	130xxxx	Location-Specific
1303xxxxx	1303538xx	ALL Locations

Session Manager matches patterns using the following algorithm:

- Valid digits are 0-9.
- Valid characters for the leading position are,+, *, and #. Any other characters are not matched.
- A lowercase **x** is a wildcard character that matches a character from the allowed characters mentioned above. Spaces are not allowed.
- Longer matches have a higher priority over shorter matches. For example, +1601555 has a higher priority as compared to +1601.

- For matches of equal length, exact matches have a higher priority over wildcard matches. For example, +1601555 has a higher priority as compared to +1xxx555.
- Longer matches with trailing wildcard character **x** have a higher priority over shorter matches. Therefore you should not use wildcard character **x** as trailing character. For example +650xxxxxxx has a higher priority as compared to +6504.
- For both routing policies and adaptations, the pattern matching rules work in the same manner.

Note:

If multiple Routing Policies have the same destination SIP Entity and are assigned to the same Dial Pattern, Session Manager behaves as if the Route Policy **Retries** field is set. The value is equal to the number of administered Routing Policies. The Route Policy **Retries** value specifies the number of times the Session Manager polls a SIP Entity before timing out.

Emergency Numbers

Session Manager supports up to 100 emergency numbers for each unique location. You administer Emergency Numbers on the Dial Patterns pages of System Manager. The IP address of the endpoint determines the emergency numbers that are downloaded to that endpoint. Only those emergency numbers from the Dial Patterns page where **Originating Locations and Routing Policies** and **Denied Originating Locations** are consistent with the location administered for the user are sent to the endpoint. Emergency numbers that are specific to the location and the general emergency numbers are sent to the endpoint. If the general emergency number is same as that of the local emergency number, the local number description takes precedence over the general emergency number description. Prior to user login, the emergency number related information is downloaded to the endpoint devices upon connection to the network. Emergency numbers are again sent to the endpoint when a user logs in.

A priority number can be assigned or the first number administered is assigned as the priority number, so that the endpoint can associate an emergency number with the emergency softkey of the endpoint.

Important:

- The SIP endpoints administered with more than one emergency number must have software that supports multiple emergency number downloads from Session Manager. If an Avaya endpoint does not support multiple emergency numbers, Session Manager only routes the first administered emergency number.
- You must assign only one priority number to one emergency number and which should be unique.
- A maximum of 300 dial plan entries are sent to the endpoints.
- Emergency numbers are not supported for dial pattern ranges.
- If you define multiple locations in System Manager, you must administer at least one emergency call dial pattern entered with **originating location = ALL**. As an alternative, every location with a location-specific Emergency Number dial pattern must be defined

with an associated IP address pattern. If these criteria are not met, unregistered endpoints cannot make emergency calls.

- Any emergency number can be sequenced with other applications such as Avaya Breeze™ and Communication Manager.

Dial Plan Ranges

Note:

Before enabling the Dial Plan Range feature in an enterprise system, ensure that all Session Manager installations are of version 6.3.4 or later.

Using a Dial Plan Range, you can specify number ranges in the Session Manager Dial Plan.

A valid range has the following characteristics:

- Two integers separated by a colon (:)
- (Optional) A plus sign (+) can precede the numbers. If one number begins with a (+) sign, then the other number must also begin with a (+) sign.
- The number to the left of the colon must be numerically less than the number to the right. These numbers cannot be equal.
- The numbers on the left and right of the colon must be of the same length.

Note:

The Global Settings **Dial Plan Ranges** must be enabled on the Session Manager Administration page.

The valid pattern format is [+0-9][0-9]{0,23}[:][+0-9][0-9]{0,23}. For example, +493420479242000:+493420479242999.

You can enter a range that is a subset or superset of an existing range or pattern. The smaller range is a sub-range. Sub-ranges have the following limitations within the same location and domain:

- Two sub-ranges must not match each other.
- A sub-range must not match a pattern.
- A sub-range must not cross the starting or end of another range.

Dial Plan Range Example

If the Dial Plan Range is 5000:5499, you can specify the sub-ranges as:

- 5002:5011
- 5000:5499 and 5492:5499, where the end of sub-range and range match.
- 5000 (single entry) and 5000:5009, where the beginning of sub-range and range match.

The sub-range 5300:5555 is not valid because the sub-range crosses the end of the range.

Note:

When routing, Session Manager performs more efficiently using a smaller range rather than a larger range or longer pattern.

Multilocation Dial Plan

The Communication Manager location of a user is determined from the Communication Manager station form or from the *ip-address* of the endpoint if this address is administered on the Communication Manager *ip-network-map* form. If a user has a specific location other than the administered global location, then both the global and location specific dial plan entries are sent to the endpoint. If the user is not administered with a Communication Manager location, then only the global dial plan entries are sent to the endpoint. This information is used by the endpoint to determine the permitted dial sequences for a user.

Note:

For Session Manager releases earlier than 6.2, upon user login, endpoints receive all the administered Communication Manager dial plan entries.

Creating Dial Patterns

Use the Dial Patterns page to create Dial Patterns and to associate the Dial Patterns to a Routing Policy and Locations.

Note:

You cannot save a dial pattern unless you add at least a routing policy or a denied location.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Dial Patterns**.
2. Click **New**.
3. Enter the Dial Pattern General information in the General section.

   Note:

   You can provide a Domain to restrict the Dial Pattern to the specified Domain.
4. Under the Originating Locations and Routing Policies section, click **Add**.
5. Select all the required Locations and Routing Policies that you want to associate with the Dial Pattern.
6. When you have finished making your selections, click **Select**.
7. To deny calls from the specified locations:
   a. Click **Add** under the Denied Locations section.

b. Select all the Locations that are to be denied.

c. When you have finished making your selections, click **Select**.

8. Click **Commit**.

Modifying Dial Patterns

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Dial Patterns**.
2. Select the dial pattern you want to modify.
3. Click **Edit**.
4. Modify information as required.
5. Add or remove Locations and click **Select**.
6. Add or remove Routing Policies as required and click **Select**.
7. Click **Commit**.

Note:

You cannot save a dial pattern unless the dial pattern has at least one routing policy or a denied location associated to the dial pattern.

Deleting Dial Patterns

When you delete a Dial Pattern, the system deletes the Dial Pattern from all Routing Policies associated with the Dial Pattern.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Dial Patterns**.
2. Select the Dial Patterns you want to delete.
3. Click **Delete**.
4. Click **Delete** on the confirmation page.

Dial Patterns field descriptions

Use this page to create, modify, delete, and manage dial patterns.

Name	Description
New	Create a new dial pattern.
Edit	Modify information for the selected dial pattern.
Delete	Delete the selected dial pattern or patterns.
Duplicate	Create a copy of the selected dial pattern and assign a new state to it.
More Actions > **Dial Pattern Report**	Display Dial Patterns and the corresponding Locations, Routing Policies, and Domains.
More Actions > **Import**	Import dial pattern data from XML files or a zip file containing one or more XML files. If the dial pattern matches the existing dial pattern during the import, the dial pattern replaces the existing dial pattern. To preserve the existing dial pattern, export and modify the dial pattern before importing it.
More Actions > **Export Dial Patterns**	Export dial pattern data as an XML file to a specified location.
More Actions > **Export all data**	Export data for all the routing entities as a zip file to a specified location.

Name	Description
Pattern	The dial pattern to match. The pattern can have 1 to 49 characters.
Min	The minimum number of digits to be matched.
Max	The maximum number of digits to be matched.
Emergency Call	The status of the call to indicate whether the call is an emergency call.
Emergency Priority	The priority of the emergency number.
Emergency Type	The type of emergency call. For example, medical, fire, and police.
SIP Domain	The domain for which you want to restrict the dial pattern.
Notes	Additional information.

Dial Pattern Details field descriptions

General section

Name	Description
Pattern	The dial pattern to match. The pattern can have 1 to 49 characters. The valid pattern format for different pattern types are as follows: • For regular patterns, [+*#0-9x][0-9x]{0,35} • For pattern ranges, [+0-9][0-9]{0,23}[:][+0-9][0-9]{0,23} • For patterns with Emergency number, [0-9]{0,35} **Note:** If you specify a Dial Pattern Range, the system disables the **Min**, **Max**, and **Emergency Call** fields.
Min	The minimum number of digits to match in the dial pattern.
Max	The maximum number of digits to match in the dial pattern.
Emergency Call	Indicate if the call is an emergency call. **Note:** Important constraints of this feature are: • Each location can have up to 100 emergency numbers assigned. • The emergency dial number must match the emergency dial number in the 96xx settings file for all SIP phones in the identified location. Failure to follow this guideline can result in users being unable to dial emergency numbers.

Table continues…

Name	Description
Emergency Priority	Based on the IP address of the endpoint, up to 100 emergency numbers get downloaded to the endpoint, with each number assigned with a separate priority. **Note:** • PPM sends the emergency number, type, and priority/default to the endpoint. The first number in the list of emergency numbers, sent to the endpoint device, gets assigned with the Emergency soft key on the device. • Do not assign the same priority number for more than one emergency number of a location.
Emergency Type	Type of emergency number. Examples are **medical** and **fire**.
SIP Domain	Domain for which you want to restrict the dial pattern.
Notes	Other information.

Originating Locations and Routing Policies section

Button	Description
Add	Add locations and routing policies for the dial patterns.
Remove	Remove locations and routing policies for the dial patterns.

Name	Description
Select check box	Select and use the digit conversion for the incoming calls.
Originating Location Name	Name of the location to be associated to the Dial Pattern.
Originating Location Notes	Notes about the selected location.
Routing Policy Name	Name of the Routing Policy to be associated to the Dial Pattern.
Rank	Rank order.
Routing Policy Disabled	Name of the Routing Policy that should not be used for the Dial Pattern.
Routing Policy Destination	Destination of the Routing Policy.
Routing Policy Notes	Other information about the Routing Policy.

Denied Originating Locations section

Button	Description
Add	Add denied locations for the dial patterns.
Remove	Remove denied locations for the dial patterns.

Name	Description
Select check box	Select denied locations for the Dial Pattern match.
Originating Location	Name of the location to be associated to the Dial Pattern.
Notes	Notes about the selected location.

Button	Description
Commit	Save the Dial Pattern changes.
Cancel	Cancel changes to the Dial Pattern and return to the Dial Patterns page.

Denied Originating Location List field descriptions

Use this page to specify denied locations for the selected dial pattern

Button	Description
Select	Select the location as a denied location for the Dial Pattern.
Cancel	Cancel the selection of the denied location.

Name	Description
Apply to All Originating Locations	Select to associate all the locations to the Dial Pattern.
Select check box	Select this check box to select denied locations for the Dial Pattern match.
Name	Name of the location associated to the Dial Pattern.
Notes	Notes about the selected location.

Bulk Import for dial patterns

Using System Manager, you can import dial patterns, routing policies, regular expressions, entity links, and SIP entities in bulk. To import data in bulk, you must provide an XML or zip file containing multiple XML files as an input file. System Manager validates any file that you upload during the bulk import operation.

If the dial pattern matches with the existing dial pattern during the import, the dial pattern replaces the existing dial pattern. To preserve the existing dial pattern, export and modify the dial pattern before importing it.

You can associate origination dial pattern sets with the dial patterns.

Use the following rules when creating an XML bulk import file:

- A dial pattern is identified by a combination of the five elements below. This combination must be unique for each dial pattern.
  - <digitpattern>
  - <maxdigits>
  - <mindigits>
  - <sipdomainName>
  - <routingoriginationName>
  - <originationpatternsetName>
- <sipdomainName> must refer to an existing domain with the same name. The element must appear in the System Manager database or in an import file that exists in the same import operation as the dial pattern.
- <routingpolicyNames> must refer to existing Routing Policies with the same name. The element must appear in the System Manager database or in an import file that exists in the same import operation as the dial pattern.
- <routingpolicyNames> must exist if <deny> is false.
- <routingpolicyNames> must exist if <deny> is true.

If the Flexible Routing feature is disabled, and the user imports dial patterns with origination dial pattern sets, the following error message appears:

```
Flexible Routing is not enabled. Dial Pattern 123xx having
importedDigitmapOriginationSetName set2 cannot be imported.
```

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<digitmapFullTOList>
    <DigitmapFullTO>
        <notes>this is a test</notes>
        <deny>true</deny>
        <digitpattern>123</digitpattern>
        <maxdigits>36</maxdigits>
        <mindigits>3</mindigits>
        <originationpatternsetName>set2</originationpatternsetName>
        <routingoriginationName>New York</routingoriginationName>
        <routingpolicyNames>toBerlin</routingpolicyNames>
        <sipdomainName>avaya.com</sipdomainName>
        <treatasemergency>true</treatasemergency>
    </DigitmapFullTO>
    <DigitmapFullTO>
        <notes>this is a test</notes>
        <deny>false</deny>
        <digitpattern>123</digitpattern>
        <maxdigits>36</maxdigits>
```

```
        <mindigits>3</mindigits>
        <originationpatternsetName>set2</originationpatternsetName>
        <routingoriginationName>Berlin</routingoriginationName>
        <routingpolicyNames>toBerlin</routingpolicyNames>
        <sipdomainName>avaya.com</sipdomainName>
        <treatasemergency>true</treatasemergency>
    </DigitmapFullTO>
</digitmapFullTOList>
```

Regular Expressions

You can configure routing in Session Manager by creating regular expressions and associating them with a routing policy.

Regular expression syntax is based on Java syntax. Some of the syntax related rules are:

- The asterisk character "*" matches any character string.
- The dot character "." matches one character.
- The backslash character "\ " makes a character lose its special meaning, if any

Some examples are:

- For “www.sipentity.domain.com”, use the string “www\.sipentity\.domain\.com”
- For “192.14.11.22”, use string “192\.14\.11\.22”.
- The routing policy with a regular expression .*@.*\.de routes all calls requesting a domain in Germany (for example, name@company.de) to a Frankfurt Gateway.

Regular Expression constructs

For more information, see the information regarding patterns at http://download.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html.

Construct	Matches
Characters	
x	The character x
\\	The backslash character
Character classes	
[abc]	a, b, or c (simple class)
[^abc]	Any character except a, b, or c (negation)
[a-zA-Z]	a through z or A through Z, inclusive (range)
[a-d[m-p]]	a through d, or m through p: [a-dm-p] (union)
[a-z&&[def]]	d, e, or f (intersection)

Table continues…

Construct	Matches
[a-z&&[^bc]]	a through z, except for b and c: [ad-z] (subtraction)
[a-z&&[^m-p]]	a through z, and not m through p: [a-lq-z](subtraction)
Predefined character classes	
.	Any character (may or may not match line terminators)
\d	A digit: [0-9]
\D	A non-digit: [^0-9]
\s	A whitespace character: [\t\n\x0B\f\r]
\S	A non-whitespace character: [^\s]
\w	A word character: [a-zA-Z_0-9]
\W	A non-word character: [^\w]
java.lang.Character classes (simple java character type)	
\p{javaLowerCase}	Equivalent to java.lang.Character.isLowerCase()
\p{javaUpperCase}	Equivalent to java.lang.Character.isUpperCase()
\p{javaWhitespace}	Equivalent to java.lang.Character.isWhitespace()
\p{javaMirrored}	Equivalent to java.lang.Character.isMirrored()
Classes for Unicode blocks and categories	
\p{InGreek}	A character in the Greek block (simple block)
\p{Lu}	An uppercase letter (simple category)
\p{Sc}	A currency symbol
\P{InGreek}	Any character except one in the Greek block (negation)
[\p{L}&&[^\p{Lu}]]	Any letter except an uppercase letter (subtraction)
Boundary matchers	
^	The beginning of a line
$	The end of a line
Greedy quantifiers	
X?	X, once or not at all
X*	X, zero or more times
X+	X, one or more times
X{n}	X, exactly n times
X{n,}	X, at least n times
X{n,m}	X, at least n but not more than m times
Logical operators	
XY	X followed by Y
X|Y	Either X or Y

Creating Regular Expressions

Use the Regular Expressions screen to create regular expressions and associate them with routing policies. You cannot save a regular expression unless the regular expression has a routing policy associated with the regular expression.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Regular Expressions**.
2. Click **New**.
3. Enter the regular expression pattern in the **Pattern** field.
4. Specify a rank order for the regular expression. A lower rank order indicates a higher priority.
5. To deny routing for a matched regular expression pattern, select the **Deny** check box.
6. To associate a routing policy for the matched pattern, click **Add** under the Routing Policy section.
7. Select the required routing policies that you want associated with the Regular Expression by selecting the respective check boxes.
8. Click **Select** to indicate that you have completed your selections.
9. To remove an associated routing policy, select the routing policy and click **Remove**.
10. Click **Commit**.

Modifying Regular Expressions

Modify regular expressions and associate the regular expressions with routing policies.

A lower rank order indicates a higher priority.

Note:

You cannot save a regular expression unless the regular expression has a routing policy associated to the regular expression.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Regular Expressions**.
2. Select a regular expression from the list.
3. Click **Edit**.
4. Make the required changes.

5. Click **Commit**.

Deleting Regular Expressions

The system deletes the regular expression from all routing polices associated with the regular expression.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **Regular Expressions**.
2. Select the regular expression or expressions you want to delete.
3. Click **Delete**.
4. Click **Delete** on the confirmation page.

Regular Expressions field descriptions

Button	Description
New	Create a new regular expression.
Edit	Modify the selected regular expression.
Delete	Delete the selected regular expression. You can delete more than one regular expression at the same time.
Duplicate	Create a duplicate of the selected regular expression and assign a new state to it.
More Actions > **Import**	Import regular expression data from XML files or a zip file containing one or more XML files.
More Actions > **Export Regular Expressions**	Export regular expressions data as an XML file to a specified location.
More Actions > **Export all data**	Export data for all entities as a zipped file to a specified location.

Name	Description
Pattern	Regular expression pattern for Session Manager to match.
Rank Order	Priority of the pattern. A lower rank order means higher priority.
Deny	Deny routing for a matched regular expression pattern.
Notes	Additional information about the regular expression pattern.

Regular Expression Details field descriptions

General

Name	Description
Pattern	Regular expression pattern for Session Manager to match.
Rank Order	Priority of the pattern. A lower rank order means higher priority.
Deny	Deny routing for a matched regular expression pattern.
Notes	Additional information about the regular expression pattern.

Routing Policy

Button	Description
Add	Associate a routing policy for the matched pattern.
Remove	Dissociate a routing policy from the matched pattern.

Name	Description
Name	Name of the routing policy.
Disabled	Indicate the routing policy is to be disabled and should not be used.
Destination	SIP Entity as Destination.
Notes	Additional information about the routing policy.

Button	Description
Commit	Save the changes and distribute the information to the Session Manager instances in the enterprise.
Cancel	Cancel and disregard the changes.

Routing Policy List field descriptions

Name	Description
Name	Name of the routing policy to be associated with the selected regular expression.
Disabled	Indicate the associated routing policy is disabled for the selected regular expression.

Table continues…

Name	Description
Destination	Destination SIP entity for the routing policy.
Notes	Additional information about the routing policy.

Button	Description
Select	Confirm the selection of the routing policy for associating it with the regular expression.
Cancel	Cancel the selection of the routing policy.

Bulk import for Regular Expressions

Use the following rules when creating an XML bulk import file:

- The pattern of a Regular Expression, referred to as <regexpmap> must be unique.
- <routingpolicyNames> must refer to an existing Routing Policy with the exact same name. It must either appear in the System Manager database or in an import file that exists in the same import operation as the Regular Expression.
- Multiple Routing Policy entries (<routingpolicyNames>) can be configured for one Regular Expression.

Example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<regexpmapFullTOList>
    <RegexpmapFullTO>
        <notes>this is a test</notes>
        <deny>false</deny>
        <pattern>*.com</pattern>
        <rankorder>0</rankorder>
        <routingpolicyNames>toBerlin</routingpolicyNames>
    </RegexpmapFullTO>
</regexpmapFullTOList>
```

Defaults

Default values are used when creating new Routing entities. You set the default values on the Personal settings page for Defaults.

Changing the values does not change the values of entities that have already been created.

Modifying the Default settings

Use the Defaults screen to change the default values or ranges for parameters that are used by the other Routing entities.

The Default values are used when creating new Routing entities. Modifying these values does not change the values of entities that have already been created.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Routing** > **Defaults**.
2. Make the required changs.
3. Click **Apply**.

Default Settings field descriptions

Specify default settings for all the Routing menus and save the values as your default personal settings.

Adaptations

Name	Description
Matching Pattern Min Length	Minimum length of pattern matched for adaptations. The minimum value is 1.
Matching Pattern Max Length	Maximum length of pattern matched for adaptations. The maximum value is 36.

Dial Patterns

Name	Description
Dial Pattern Min Length	Minimum length of dial pattern to be matched. The minimum value is 1.
Dial Pattern Max Length	Maximum length of dial pattern to be matched. The maximum value is 36.

Entity Links

Name	Description
Listen Port	The port to be used for entity links.
Default Transport Protocol for Entity Links	The default transport protocol for entity links to use . The default is TLS.

Domain Management

Name	Description
Suffix	The default suffix to be used for the domain name.

SIP Entities

Name	Description
Type	Type of the SIP entity, such as ASM, CM, Trunk, and Gateway. The default is ASM.
Time Zone	The default time zone to be used for the entity link.
Default Transport Protocol for Ports	The transport protocol to be used by the ports. The default is TLS.
Override Port & Transport with DNS SRV	Override DNS routing. Selecting this option causes the system to use the port and transport values that are administered in the local host name resolution table. The contents for both the Port and Protocol (Transport) fields on the SIP entity form are ignored. If you select the check box, the system performs a a full DNS lookup (as described in RFC 3263), and the transport and port information specified in the entity link could be overridden.

Time Ranges

Name	Description
Time Range Start Time	Start time for the time range. Default is 00:00.
Time Range End Time	End time for the time range. Default is 23:59.

Application Settings

Name	Description
Show warning message	Display a warning message if: • You try to navigate to another page when the displayed page has unsaved data. • A data import is in progress.

Button	Description
Restore Defaults	Restore vendor defaults.
Revert	Revert to settings before the last applied settings.
Apply	Save and apply the current settings.

Chapter 8: Session Manager Administration

Session Manager Dashboard

The Session Manager Dashboard page displays the overall status and health summary of each administered Session Manager instance. The Dashboard also provides the ability to:

- Change the service state of a Session Manager instance.
- Shut down the Session Manager server.
- Reboot the Session Manager server.
- Enable and disable EASG for selected Session Manager.

Note:

If the **License Mode** of Session Manager or Branch Session Manager displays **Restricted**, you cannot change the service state to **Accept New Service**. The service state cannot be changed until the cause of the license error has been corrected.

Events that cause a license error include:

- No license.
- Expired license.
- Cannot access the WebLM server.
- The number of Session Manager or Branch Session Manager instances administered exceeds the number of servers the license supports.
- The software release installed on the Session Manager or Branch Session Manager instance is not supported by the license version.

Session Manager Dashboard field descriptions

Name	Description
Session Manager	The list of administered Session Manager instances. Clicking the link displays the Session Manager Administration page.

Table continues…

Name	Description
Type	The type of Session Manager instance. The options are: • Core • BSM
Tests Pass	The current results for periodic maintenance tests. • Green indicates the tests passed. • Red indicates at least one test failed. • **Limited Connection** indicates whether Session Manager or Branch Session Manager is in the Maintenance Mode service state. Clicking the link displays the Maintenance Tests page. • **No Connection** indicates failing network connection between System Manager and Session Manager or Branch Session Manager.
Alarms	The number of active Major/Minor/Warning alarms. Clicking the link displays the Alarming page.
Security Module	The state of the Security Module. The state can be: • Up • Down • --- (unknown) Clicking the link displays the detailed summary page of the selected security module.
Service State	The current service state of Session Manager. The options are: • Accept New Service • Deny New Service • Maintenance Mode
Entity Monitoring	The monitoring status of the administered Session Manager instances. The field displays the number of entities with connection problems/ the total entities. Clicking the link displays the Session Manager Entity Link Connection Status page. **Note:** Entity Monitoring does not apply to a Session Manager that is administered as a Branch Session Manager. The monitoring status of a Branch Session Manager is always unknown (---).
Active Call Count	The current number of active calls for the administered Session Manager instances.
Registrations	The current registration summary and the maximum number of registrations in the last 24 hours. Clicking the link displays the Registration Summary page.

Table continues…

Name	Description
Data Replication	The replication status for the replica node. • Green indicates synchronized. • Red indicates not synchronized. • A warning symbol indicates that the system cannot match the Session Manager management host name with the **Replica Node Host Name** on the Replication page. This error indicates a mismatch between the Session Manager configuration for the **Replica Node Host Name** and the information System Manager receives from a DNS lookup. Clicking the symbol displays the Replica Groups page.
User Data Storage Status	The status of the user data storage. • Green indicates the User Data Storage Sanity Test passed. • Red indicates the test failed. Clicking the symbol displays a detailed status report on the User Data Storage Status page. **Note:** The **User Data Storage Status** displays **– –** for: • Branch Session Manager instances. • A Session Manager instance running a release earlier than 6.3.8.
License Mode	Status of the Session Manager or Branch Session Manager license. The status can be: • **Normal:** The license is valid and no errors are detected. • **Error:** The license is not accessible or does not exist. The system displays the time remaining in the 30–day grace period. • **Restricted:** The 30–day grace period has expired. Session Manager or Branch Session Manager, if operational, is now in the **Deny New Service** state. Clicking the link displays the WebLM Home page.
Enhanced Access Security Gateway (EASG)	Status of Session Manager EASG. The status can be: • **Enabled** — EASG is installed and is enabled for Avaya Service access. • **Disabled** — EASG is installed but is disabled for Avaya Service access. • **Removed** — EASG is removed from Session Manager. To enable EASG access Session Manager has to be reinstalled. • **---** — EASG status for Session Manager is not retrievable or is not applicable for the current version of Session Manager.
Version	The version of the installed Session Manager software. Clicking a version string link displays the Session Manager Version Inventory page.

Button	Description
Service State > Deny New Service	Blocks incoming calls for the selected Session Manager or Branch Session Manager instances. Leave active calls connected. **Note:** In the Deny New Service mode, the system denies any new call attempts and service requests. SAL agent is restarted and monitoring is re-enabled. The Deny New Service mode can deny selected entity links during a planned WAN outage.
Service State > Accept New Service	Accepts incoming calls for the selected Session Manager instances.
Service State > Maintenance Mode	Places the selected Session Manager instances in the **Maintenance Mode** state. **Note:** In the Maintenance mode, SAL agent stops working and monitoring is disabled. Maintenance mode does not support GUI-based operations and alarms generation. Maintenance mode supports the repair or upgrade of existing Session Manager and Branch Session Manager.
Shutdown System > Shutdown	Shuts down the selected Session Manager server.
Shutdown System > Reboot	Reboots the selected Session Manager server.
EASG > Enable EASG	Enables EASG for the selected Session Manager. **Note:** The ability to Enable or Disable EASG is also supported when Session Manager is in **Maintenance Mode** and Session Manager is currently displaying **Limited Connection** status.
EASG > Disable EASG	Disables EASG for the selected Session Manager. **Note:** The ability to Enable or Disable EASG is also supported when Session Manager is in **Maintenance Mode** and Session Manager is currently displaying **Limited Connection** status.

Maintenance Mode Service state

To support deployment and maintenance of many Session Manager or Branch Session Manager instances, a non-operational Session Manager or Branch Session Manager can be set to the **Maintenance Mode** service state. The **Maintenance Mode** service state essentially places Session Manager or Branch Session Manager into a dormant state. **Maintenance Mode** is not a SIP service state and is independent of the **Deny** and **Accept New Service** states.

Use the **Maintenance Mode** service state for:

- Staging installations where Session Manager or Branch Session Manager is not provisioned on the network.
- Pre-administering a large number of Branch Session Manager instances before installing or configuring the machines.
- Upgrading an existing Session Manager or Branch Session Manager.
- Preventing large amounts of error logging and alarming during a temporary outage.

When you change the service state to **Maintenance Mode**, the system:

- Changes the service state of Session Manager or Branch Session Manager to the **Deny New Service** state if the service state is **Accept New Service**.
- Does not generate alarms.

You change the service state to **Maintenance Mode** using the Session Manager Administration page or from the Session Manager Dashboard. **Maintenance Mode** is an option on the **Service State** drop-down menu.

Maintenance Mode is enabled by default when adding a new Session Manager or Branch Session Manager instance.

Session Manager Administration

Using the System Manager Web Console, you administer a SIP Entity as a Session Manager or Branch Session Manager instance on the Session Manager Administration page. When you add Session Manager instances, the instances form a link with the Session Manager Element Manager. The Session Manager Element Manager obtains and monitors the status of the Session Manager instances.

Data replication and monitoring operations become operational only after you add and configure Session Manager instances.

Use the Session Manager Administration page to administer Session Manager and Branch Session Manager instances and to configure global settings.

In addition to creating new Session Manager instances, you can use the Session Manager Administration page to view, edit, or delete administered Session Manager instances.

You can also administer Session Manager and Branch Session Manager instances using the **Inventory** > **Manage Elements** pages.

The high-level steps for creating and administering a Session Manager instance are:

1. Create a Session Manager SIP Entity.
2. Administer the Session Manager SIP Entity.

For more information regarding creating and administering SIP Entities, see *Avaya Aura® Session Manager Case Studies* on the Avaya support web site.

Creating a Session Manager SIP Entity

About this task

Use this procedure to create:

- A Session Manager SIP Entity.
- An entity link between a Session Manager and a Communication Manager instance that is connected to a Session Manager instance using SIP trunks.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Routing** > **SIP Entities**.
2. Click **New**.
3. In the **Name** field, enter the name of the Session Manager.
4. In the **FQDN or IP Address** field, enter the IP address of the IP signaling interface for the virtual SM-100 interface on Session Manager.
5. In the **Type** field, click **Session Manager** .
6. In the **SIP Link Monitoring** field, select **Use Session Manager Configuration**.
7. Enter information in the remaining fields as appropriate.
8. In the Entity Links section, click **Add**.

   The information for the new SIP Entity appears in the list.
9. In the **Name** field, enter a name for the entity link. For example, you can use the names of the two SIP entities as a paired name.
10. In the **SIP Entity 1** field, click the name of the Session Manager instance.
11. In the **SIP Entity 2** field, click the appropriate Communication Manager instance.
12. Click **Commit**.

Adding a Session Manager instance

You can add a Session Manager instance using either the:

- Session Manager Administration pages.
- Manage Elements pages.

Note:

If a Version 7 license is installed and the Session Manager server instance count has been reached, the following error message appears after clicking the **New** button: `Cannot add Session Manager instance, maximum instance count reached for license.`

You cannot administer a new Session Manager beyond the license limit until you install a Version 7 license with a higher limit.

Procedure

1. On the home page of the System Manager Web Console, do one of the following:
   - Use the Session Manager Administration page:
     a. Under **Elements**, click **Session Manager** > **Session Manager Administration**.
     b. Click the **Session Manager Instances** tab.
     c. Click **New**.
   - Use the Manage Elements page:
     a. Under **Services**, click **Inventory** > **Manage Elements**.
     b. Click **New**.
     c. From the **Type** field, select **Session Manager**.
     d. When the screen refreshes, from **Select type of Session Manager to add:**, select **Core Session Manager**.
     e. Click **Continue**.
2. On the Add Session Manager page, in the General section, perform the following:
   a. In the **SIP Entity Name** field, type the name of the Session Manager instance.
   b. In the **Description** field, type a description for this entity.

      This field is optional.
   c. In the **Management Access Point Host Name/IP** field, type the IP address of the management interface of the Session Manager server.

      The **Management Access Point Host Name/IP** field accepts only IPv4 addresses even when you create Session Manager instances for entities supporting IPv6 or Both address families.
   d. From the **Direct Routing to Endpoints** drop-down list, select Enable for direct routing to endpoints.
   e. From the **Data Center** drop-down list, select a data center.
   f. From the **Avaya Aura Device Services Server Pairing** drop-down list, select an AADS server.

      AADS is available with Avaya Equinox® 3.0.

      When an AADS server is already paired with a Session Manager instance, the system does not display that AADS Server.

g. **Maintenance Mode** is enabled by default. Deselect **Maintenance Mode** if you are not:

- Staging a non-operational Session Manager or Branch Session Manager.
- Pre-administering Session Manager or Branch Session Manager on System Manager prior to host installation.

3. Specify the appropriate information in the remaining required fields.

   For information about the fields, see Add Session Manager Administration page field descriptions.

4. Click **Commit**.

Related links

Add Session Manager page field descriptions on page 419

Viewing Session Manager administration settings

Procedure

1. On the home page of the System Manager Web Console, do one of the following:
   - Under **Elements**, click **Session Manager** > **Session Manager Administration**.
   - Under **Services**, click **Inventory** > **Manage Elements**.
2. Select a Session Manager from the list of Session Manager instances.
3. Click **View**.
4. After you have viewed the information, click **Return**.

Modifying Session Manager administration settings

Change the configuration settings for an already configured Session Manager.

Procedure

1. On the home page of the System Manager Web Console, do one of the following:
   - Under **Elements**, click **Session Manager** > **Session Manager Administration**.
   - Under **Services**, click **Inventory** > **Manage Elements**.
2. Select a Session Manager from the list of Session Manager instances.
3. Click **Edit**.
4. Make the necessary changes.
5. Click **Commit**.

Deleting a Session Manager instance

Before you begin

Important:

Before you delete a Session Manager instance, you must first do one of the following:

- Dissociate the Session Manager instance from all the related Communication Profiles.
- Delete all associated users on the Session Manager.

Procedure

1. On the home page of the System Manager Web Console, do one of the following:
   - Under **Elements**, click **Session Manager** > **Session Manager Administration**.
   - Under **Services**, click **Inventory** > **Manage Elements**.
2. Select a Session Manager from the list of Session Manager instances.
3. Click **Delete**.
4. Click **Delete** on the confirmation page.

Add Session Manager page field descriptions

General

Name	Description
SIP Entity Name	The name of the SIP Entity that you are adding as a Session Manager instance. The entity must be of the **Session Manager** type and must be in the **Sync** state.
Description	The description of the SIP Entity. This field is optional.
Management Access Point Host Name / IP	The IP address of the management agent of Session Manager. The **Management Access Point Host Name/IP** field accepts only IPv4 addresses even when you create Session Manager instances for entities supporting IPv6 or Both address families.
Direct Routing to Endpoints	The field to assign routing directly to endpoints.
Data Center	The list of data centers that can be associated with a Session Manager instance.
Avaya Aura Device Services Server Pairing	The list of AADS Server to pair a Session Manager instance with an AADS node. **Note:** AADS is available only with Avaya Equinox® 3.0.

Table continues…

Name	Description
Maintenance Mode	The maintenance mode of a Session Manager instance. **Note:** If **Maintenance Mode** is selected for a Session Manager instance earlier than 7.0, the Session Manager instance is in the **Deny New Service** state.

Security Module

Name	Description
SIP Entity IP Address	The IP address of Session Manager as specified on the SIP Entity Details page. The system displays this field only when you select a SIP entity of address family type IPv4 or both IPv4 and IPv6.
SIP Entity IPv6 Address	The IP address of Session Manager as specified on the SIP Entity Details page. The system displays this field only when you select a SIP entity of address family type IPv6 or both IPv4 and IPv6.
Network Mask	The network mask value. The security module configures the network mask and defines the subnet associated with the security module. The system displays this field only when you select a SIP entity of address family type IPv4 or both IPv4 and IPv6.
IPv6 Network prefix length	The network prefix length. This field is displayed only when you select a SIP entity of address family type IPv6 or both IPv4 and IPv6.
Default Gateway	The IP address of the default gateway. The system displays this field only when you select a SIP entity of address family type IPv4 or both IPv4 and IPv6.
IPv6 Default Gateway	The IP address of the default gateway. The system displays this field only when you select a SIP entity of address family type IPv6 or both IPv4 and IPv6.
Call Control PHB	The type of service and priority for SIP traffic from the security module. All packets containing SIP signaling that leave the security module have the specified value in the differentiated service code point (DSCP) field of the IP header. Intervening routers can treat packets containing this value with a different level of precedence. The routers must either support the type by default or be specially configured to do so. Different DSCP values are specified in RFCs 2597 and 2598. To be consistent with Communication Manager, Session Manager uses a default DSCP value of 46 that indicates forwarding with the highest priority.
SIP Firewall Configuration	The SIP Firewall Configuration associated with the Session Manager instance.

NIC Bonding

Note:

The NIC Bonding section appears only if the system was administered using a Session Manager version earlier than 7.0 *and* NIC bonding was enabled.

The NIC Bonding section does not appear for:

- New core Session Manager instances.
- Systems that were administered prior to Session Manager 7.0 without NIC bonding enabled.

Name	Description
Enable Bonding	The NIC bonding bifurcates the interfaces eth2 and eth3 in a bond of interfaces. This ensures that all the Network firewall rules related to SM100 agent public IP Address are applied on the NIC bonding interface.
Driver Monitoring Mode	The ARP Monitoring or MII Monitoring as the modes of NIC bonding. The modes are supported by the NIC bonding driver.
ARP Interval (secs)	The ARP link monitoring frequency. The range is 50 to 1000. The default value is 100.
ARP Target IP	The IP target of the ARP request that is sent to determine the status of the link to the targets. You can configure up to 3 IP Addresses for ARP monitoring.
Link Monitoring Frequency (msecs)	The period of monitoring. The range is 50 to 500. The default value is 100.
Down Delay (msecs)	The wait time for disabling a slave when a link failure is detected. The value is a multiple of the link monitoring frequency value. The range is 50 to 1000. The default value is 200.
Up Delay (msecs)	The wait time for enabling a slave after a link recovery. The value is a multiple of the link monitoring frequency value. The range is 50 to 1000. The default value is 200.

Monitoring

Name	Description
Enable SIP Monitoring	The monitoring of the SIP entities administered to this Session Manager instance. Monitoring ensures that the entities are reachable.
Proactive cycle time (secs)	The time for polling the SIP entities administered to this Session Manager. Proactive monitoring occurs as long as no outages are detected. The default is 900 seconds. The default value is used for each administered SIP entity unless overridden by the **Monitoring** option on the SIP Entities page for a specific entity.

Table continues…

Name	Description
Reactive cycle time (secs)	The time for monitoring if an administered SIP entity is unreachable and detecting changes to a reactive mode. Reactive monitoring continues until the SIP entity responds again. The value for reactive monitoring must be less than the value for proactive monitoring. The default value is 120 seconds. The default value is used for each administered SIP entity unless overridden by the **Monitoring** option on the SIP Entities page for a specific entity.
Number of Tries	The number of times that Session Manager polls a SIP entity before the SIP entity is deemed unreachable. The default value is 1. Session Manager uses the default value for each administered SIP entity unless overridden by the **Monitoring** options on the SIP Entities page for a specific entity.
Number of Successes	The number of times that Session Manager polls a SIP entity before marking the SIP entity link active. You can configure a value between 1 and 10. The default value is 1.
Enable CRLF Keep Alive Monitoring	The option to enable the monitoring of SIP entity links using CRLF pings. You must enable the following SIP monitoring fields before you enable the CRLF Keep Alive Monitoring mechanism: • **Enable SIP Monitoring** • **SIP Link Monitoring** on the SIP Entity Details page When you select the checkbox, the **Enable CRLF Keep Alive Monitoring** option displays a drop-down list with the following options: • **Use Session Manager Configuration**: Uses the Session Manager configuration to determine whether to monitor SIP entity links. This is the default selection in the drop-down list. You can select this option only if **SIP Link Monitoring** on the SIP Entity Details page is configured to **Use Session Manager Configuration** or **Link Monitoring Enabled**. • **CRLF Monitoring Enabled**: Overrides the Session Manager configuration and uses the CRLF monitoring option to monitor SIP entity links. You can select this option only if **SIP Link Monitoring** on the SIP Entity Details page is configured to **Link Monitoring Enabled**. • **CRLF Monitoring Disabled**: Disables the CRLF-based monitoring of SIP entity links. You can select this option only if **SIP Link Monitoring** on the SIP Entity Details page is configured to **Link Monitoring Enabled** or **Link Monitoring Disabled**. The **Enable CRLF Keep Alive Monitoring** option is disabled by default.

Table continues…

Name	Description
CRLF Ping Interval (secs)	The time that the **Enable CRLF Keep Alive Monitoring** option waits before pinging the SIP entity link again. The default value is 120 seconds. You can set a value between 1 and 900 seconds.

CDR

Name	Description
Enable CDR	The CDR activation at the system level for the Session Manager instance. You can then use the **Call Detail Recording** drop-down menu to individually control call detail recording for specific SIP entities.
User	The user login name for CDR access.
Password	The password for CDR access. An external CDR processing adjunct uses this password for connecting to Session Manager and to transfer the generated CDR files.
Confirm Password	The confirmation of the password.
Data File Format	The format of the CDR data file. The options are: • **Standard Flat File (default)**: Applicable for Session Manager 6.3.4 and earlier releases. • **Enhanced Flat File**: Applicable for Session Manager 6.3.4 and later releases. • **Enhanced XML File**: Applicable for Session Manager 6.3.4 and later releases. • **IPv6 Standard Flat File**: Applicable for Session Manager 7.1.2 and later releases. • **IPv6 Enhanced Flat File**: Applicable for Session Manager 7.1.2 and later releases. For URE calls **Enhanced Flat File** or **Enhanced XML File** should be selected.
Include User to User Calls	The CDR records inclusion for user-to-user calls. User-to-user calls are SIP calls that originate and terminate at Session Manager instances that are managed by the same System Manager.

Table continues…

Name	Description
Include Incomplete Calls	The CDR records inclusion for one of the following types of incomplete calls: • Incoming or outgoing calls that are unanswered. • Incoming or outgoing calls that do not have enough media resources to complete the call. • Other incoming and outgoing calls that are not completed for other reasons. • At a SIP level, the call receives any non 2xx response to the initial INVITE associated with that call.

Personal Profile Manager (PPM) - Connection Settings

Note:

Session Manager supports a feature that indicates that Service Observe (SO) is assigned to the SIP endpoint. The button can be activated by registered users.

Name	Description
Limited PPM client connection	The limited mode for the PPM client connection. The default value is **Enabled**.
Maximum Connection per PPM client	The maximum number of connections per PPM client. The valid values are integers between 1 and 10. The default value is 3.
PPM Packet Rate Limiting	The limiting value for the PPM packet rate. The default is **Enabled**.
PPM Packet Rate Limiting Threshold	The number of packets per second that the PPM connection will transfer. This value is applied per PPM client. The range is 1 to 500. The default value is 200.

Event Server

Name	Description
Clear Subscription on Notification Failure	The option to remove the subscription or not when NOTIFY failures occur. The default value is **No**.

Button	Description
Cancel	Cancels the operation.
Commit	Saves the added SIP entity as a Session Manager instance with the selected configuration options.

Related links

Adding a Session Manager instance on page 416

Session Manager Instances field descriptions

Name	Description
Name	The name of the administered Session Manager. If a warning symbol appears after the name, the Session Manager instance is in the Maintenance Mode service state.
License Mode	Status of the Session Manager or Branch Session Manager license. The status can be: • **Normal:** The license is valid and no errors are detected. • **Error:** The license is not accessible or does not exist. The system displays the time remaining in the 30–day grace period. • **Restricted:** The 30–day grace period has expired. Session Manager or Branch Session Manager, if operational, is now in the **Deny New Service** state. Clicking the link displays the WebLM Home page.
Primary Communication Profiles	The number of Communication Profiles that use this Session Manager as the primary SIP controller.
Secondary Communication Profiles	The total number of Communication Profiles that use this Session Manager as the secondary SIP controller.
Maximum Active Communication Profiles	The maximum number of active Communication Profiles supported by this Session Manager instance.
Description	Description of the Session Manager instance.

Button	Description
New	Create a new Session Manager instance.
View	View the specific information for the selected Session Manager.
Edit	Edit the information for the selected Session Manager.
Delete	Delete the selected Session Manager.

Enabling IPv6

About this task

Session Manager provides a global setting to enable IPv6 support. Use this procedure to enable IPv6.

Warning:

If you have a network with Session Manager instances prior to 7.1, and IPv6 is enabled on Session Manager 7.1, you must not change the service state of any Session Manager 7.0.x or earlier out of the maintenance mode.

If you attempt changing the service state to **Accept New Service** or **Deny New Service**, the system displays the following message:

Session Manager xxx service state cannot be changed. IPv6 support is currently enabled and requires all Session Managers to be at version 7.1 or above.

If a Session Manager before 7.1 is not connected, do not change it to **Accept New Service** or **Deny New Service** to prevent data replication failures.

Before you begin

Ensure that all Session Manager and Branch Session Manager instances are release 7.1 or later.

Procedure

1. On the home page of System Manager web console, in **Elements**, click **Session Manager** > **Session Manager Administration**.
2. On the Global Settings page, select the **Enable IPv6** check box.
3. Click **Commit**.

Disabling IPv6

Before you begin

Ensure that all administered IP addresses, patterns, and address family settings are IPv4. When you disable the IPv6 property, you cannot use IPv6 based addresses, patterns, and ranges. When you attempt reverting to IPv4, the system displays errors for areas of administration that are not compatible.

Procedure

1. On the home page of the System Manager web console, in **Elements**, click **Session Manager** > **Session Manager Administration**.
2. On the **Global Settings** tab, clear the **Enable IPv6** check box.
3. Click **Commit**.

Administering global Session Manager settings

About this task

Use this procedure to administer the global settings of all the configured Session Manager instances.

Procedure

1. On the home page of the System Manager web console, in **Elements**, click **Session Manager** > **Global Settings**.
2. Select the following:

- **Allow Unauthenticated Emergency Calls** to allow unauthenticated users to make emergency calls, based on the dial pattern.
- **Allow Unsecured PPM Traffic** to allow PPM traffic over HTTP to process phone login and download button labels, contact lists, and other services.
- **Failback Policy** to specify manual and scheduled failback support for terminals.
- **ELIN SIP Entity** to specify the ELIN server for E911 services.
- **Better Matching Dial Pattern or Range in Location ALL Overrides Match in Originator's Location** to specify how to route the call based on the Dial Pattern settings.
- **Ignore SDP for Call Admission Control** to specify whether Call Admission Control (CAC) uses Session Description Protocol (SDP) in SIP messages to determine the bandwidth used by a call.
- **Disable Call Admission Control Threshold Alarms** to disable the alarms that are generated when the system crosses the alarm thresholds of CAC.
- **Disable Loop Detection Alarms** to disable the generation of loop detection alarms.

3. In the **Loop Detection Alarms Threshold (hours)** field, enter the interval after which an alarm must be generated when the system detects a loop detection error.
4. This field is not active when the Disable Loop Detection Alarms check box is selected.
5. In **TLS Endpoint Certificate Validation**, select the option to validate an endpoint certificate when the connection type is TLS (outbound SIP connection to the endpoint).

   The options are:

   - None: No mutual authentication occurs because there is no certificate validation.
   - Optional: Communication occurs if the endpoint presents a valid certificate. Alternatively, communication occurs even if the endpoint does not have certificate.
   - Required: Communication occurs only if the endpoint presents a valid certificate trusted by Session Manager.

   This setting is applicable to all Session Manager and Branch Session Manager instances in the managed network.
6. In the **Minimum SIP Entity TLS Version**, click the minimum allowed TLS version for SIP entity.
7. In the **Minimum Endpoint TLS Version**, click the minimum allowed TLS version for endpoints.
8. Select **Enable Dial Plan Ranges** to specify dial plan ranges on the Dial Pattern Details page.

Warning:

Before specifying a dial plan range, ensure that all Session Manager instances and Branch Session Manager instances are running Release 6.3.4 or later.

9. Select **Enable Implicit Users Applications for SIP users** to start implicit application sequencing.

   Note:

   This setting is not applicable for Session Manager releases earlier than 6.3.8.

10. Select **Enable Application Sequence for Emergency Calls** to enable application sequencing for emergency calls.
11. Select **Enable End to End Secure Call Indication** to activate the icon that indicates to the end user whether the signaling and the media are end-to-end secure.
12. Do the following to enable the features for military deployments:
    a. Select **Enable Military Support**.
    b. In **MLPP Network Domain(s)**, type the network domain names for Session Manager to give precedence to calls within the domains.

       Enter multiple network domain names by separating the domain names by a comma (,). For instance, uc, dsn.
13. Select **Enable Application Sequence for Emergency Calls** to enable application sequencing for emergency calls.
14. In the **Emergency Call Resource-Priority Headers** field, enter the resource priority header value to define emergency call.

    You can enter multiple values separated by commas.
15. Click **Save**.

Related links

Global settings page field descriptions on page 429

Global settings page field descriptions

Name	Description
Failback Policy	Manual or automatic failback for SIP phones. The options are: • **Auto**: When **Failback Policy** is set to **Auto**, the SIP phones will automatically failback to normal operation when connectivity to their primary Session Manager is restored. • **Manual**: When **Failback Policy** is set to **Manual**, the administrator need to manually initiate the failback to normal operation when connectivity to the primary Session Manager is restored. The default value is **Auto**. **Note:** In the case of Branch Session Manager, the failback policy setting does not apply. Failback from Branch Session Manager is always initiated in coordination with the failback policy of the collocated LSP.
Allow Unauthenticated Emergency Calls	The facility to enable unauthenticated users to make emergency calls.
Allow Unsecured PPM Traffic	The PPM traffic over HTTP to continue to process phone login and download button labels, contact lists, and other services.
ELIN SIP Entity	Identification of a user's location based on the IP address to send the new ELIN to Session Manager in case of an emergency call. This entity is used by third-party E911 services. The SIP Entity selected as the ELIN server must be resolved through local host name resolution to use either the primary or secondary IP address.
Better Matching Dial Pattern or Range in Location ALL Overrides Match in Originator's Location	The patterns associated with ALL locations, taking precedence over the dial patterns associated with a specific location.
Ignore SDP for Call Admission Control	Determination of whether Call Admission Control (CAC) uses the SDP in SIP messages to determine the bandwidth used by a call. When this box is selected, all calls are audio calls using the bandwidth specified as a location's Default Audio Bandwidth. When this box is clear, a call's SDP is evaluated to determine call type and bandwidth use.
Disable Call Admission Control Threshold Alarms	The alarms that are generated when Call Admission Control alarm thresholds are exceeded. Alarms are still generated by call denials due to bandwidth limits being exceeded.
Disable Loop Detection Alarms	The generation of Loop Detection alarms.

Table continues…

Name	Description
Loop Detection Alarms Threshold (hours)	The interval after which the Session Manager generates an alarm for a Loop Detection event. The default value is 24 hours. The allowed range is 1 hour to 168 hours. This field is required if the **Disable Loop Detection Alarms** option is not selected.
Minimum SIP Entity TLS Version	Minimum allowed TLS versions for SIP entity. The options are: • 1.0 • 1.1 • 1.2 For any Session Manager upgrading to Release 7.1, the default value is 1.0. For any new Session Manager deployment to Release 7.1, the default value is 1.2.
Minimum Endpoint TLS Version	Minimum allowed TLS versions for SIP endpoints. The options are: • 1.0 • 1.1 • 1.2 For any Session Manager upgrading to Release 7.1, the default value is 1.0. For any new Session Manager deployment to Release 7.1, the default value is 1.2.
TLS Endpoint Certificate Validation	Validation of an endpoint certificate on a TLS connection. The options are: • **None**: No mutual authentication occurs because there is no certificate validation. • **Optional**: Communication occurs if the endpoint presents a valid certificate. Alternatively, communication occurs even if the endpoint does not have a certificate. • **Required**: Communication occurs only if the endpoint presents a valid certificate trusted by Session Manager. This setting is applicable to all Session Manager and Branch Session Manager instances in the managed network. **Note:** The Optional selection is supported on all Session Manager releases and is the default value for 7.0 and later. The Required setting for releases earlier than 7.0.1 Session Manager results to the Optional setting to support backward compatibility.

Table continues…

Name	Description
Enable Dial Plan Ranges	The dial plan ranges in the Dial Pattern Details page. **Warning:** Before specifying a dial plan range, ensure that all Session Manager and Branch Session Manager instances are Release 6.3.2 or later.
Enable Regular Expression Adaptations	The option to enable regular expression adaptations.
Enable Device Adaptations	The option to enable device adaptations. By enabling this option, you can create device adaptations and device mappings. **Note:** • To enable this option, all Session Manager instances must be on Release 8.1.2 or later. • This setting cannot be disabled until all adaptations of type 'device' are removed and all device mappings are removed.
Enable Flexible Routing	The option to enable flexible routing.
Set Precedence for Routing	The option to set precedence for routing. The options are: • Dial Patterns • Regular Expressions
Set Dial Patterns Precedence	The option to set the precedence order for dial patterns. Use the Up and Down arrows to set the precedence order of dial patterns.
Enable Application Sequence for emergency calls	The application sequencing for emergency calls.
Enable End to End Secure Call Indication	The indication to the end user whether the signaling and the media are end-to-end secure.
Enable IPv6	The option to control support of IPv6 addresses for administering Session Manager. The **Enable IPv6** check box is cleared by default. When you select the **Enable IPv6** check box, Session Manager supports IPv6 addresses for administration.
Enable Military Support	The option to enable the features for military deployments and to configure Session Manager with specific domains to give precedence to calls within those domains. The **Enable Military Support** feature is disabled by default.
MLPP Network Domain(s)	The domains to which Session Manager gives precedence to establish calls. You can enter multiple domain names separated by a comma (,).

Table continues…

Name	Description
Enable Application Sequence for Emergency Calls	The option to enable application sequence for emergency calls.
Emergency Call Resource-Priority Headers	The field to define resource-priority headers used to identify emergency call. When Session Manager receives an invite request with the resource priority header value, Session Manager considers this call as an emergency call.
Enable Implicit User Applications for the SIP users	The Implicit User sequenced applications for SIP users.
Enable SIP Resiliency	The option to enable SIP resiliency.
Log Retention (days)	The field to enter number of days for which logs will be retained.
Centralized Call History Retention (days)	The field to enter number of days for which centralized call history will be retained. A user's Centralized Call History is a collection of information on the 100 most recent calls made and received by the user, which their Avaya SIP Endpoint has access to and can display. **Note:** For this information to be collected by the Session Manager and displayed for the user on the Avaya SIP Endpoints, **Enable Centralized Call History** option must be enabled in the **User Management** > **Manage Users** > **Edit** > **Communication Profile** of the Session Manager Profile User Interface.

Button	Description
Commit	To save the global settings of Session Manager administration.
Cancel	To cancel the changes.
View Defaults	To display the default settings for Session Manager administration.

Related links

Administering global Session Manager settings on page 426

End-to-End Secure Call Indication

In Session Manager, endpoints display an icon that indicates whether a call is secure or not. The call security indication is only for point to point SIP calls. The icon is similar to the icon displayed by web browsers when visiting a secured web site.

A typical two-party call between enterprise SIP endpoints routes through several SIP elements, specifically Session Manager, Communication Manager, and Session Border Controller. All of these elements can impact the end-to-end security of the call.

A SIP entity marked secured is one that does not expose the signaling and media streams to unauthorized monitoring or modification. A call is considered secure if all the signaling hops between the two entities (for example, TLS) and all media streams are secure (for example, SRTP). Any call crossing an entity that is not administered as securable will not be considered a secure call even if the entity meets the rest of the security constraints.

The Session Manager administrator has the option to mark a SIP entity as not secure if the entity is a third party entity or an older version.

Note:

When you administer the SIP entities using System Manager, mark the following Avaya Aura® elements as secure. To mark the elements as secure, click the **Enable End to End Secure Call Indication** check box on the Session Manager Administration page to turn the feature on globally and then mark each element on the Sip Entity page.

If you mark any other element that is not listed here as secured, the End-to-End Secure Call Indication feature might not give correct indication about a call security.

- Communication Manager Release 7.0 or later
- Avaya SBCE Release 7.0 or later

Failback policy

By using the Failback Policy feature, you can determine how the SIP phones failback to normal operation after connectivity to their primary Session Manager is restored. This policy only applies to failback between core Session Managers. You can configure the **Failback Policy** field on the **Elements** > **Session Manager** > **Global Settings** page by using the System Manager web console.

Note:

In the case of Branch Session Manager, the failback policy setting does not apply. Failback from Branch Session Manager is always initiated in coordination with the failback policy of the collocated LSP.

Call History

In Session Manager, logged out missed call information is saved for both H.323 and SIP endpoints.

- For H.323 endpoints, Communication Manager stores logged out missed calls and downloads the Call History logs when the endpoint logs in.
- For SIP endpoints, the primary Session Manager stores all call logs and downloads the logs to the endpoint during login. The endpoint maintains the logs locally while logged in. Call logs are only stored on the primary Session Manager of the user. No call logs are stored on the secondary Session Manager for the user. Call log storage is not redundant.

You control Call History logging for the SIP user by selecting or deselecting the **Enable Centralized Call History** check box on the Session Manager Communication Profile screen. The check box is deselected by default (disabled). The maximum number of call logs for each Communication Profile is 100. You cannot configure the maximum number of call logs.

Administering Call History

Enable or disable call history collection for a user.

Warning:

When a user logs in for the first time after the **Centralized Call History** check box is selected for that user, all calls that were made or received by that user before enabling **Centralized Call History** are lost.

Procedure

1. On the home page of the System Manager Web Console, in **Users**, click **User Management** > **Manage Users**.
2. Do one of the following:
   - If you are adding a new user, click **New** and add the information for the new user.
   - If you are enabling/disabling call history collection for a current user, select the user and click **Edit**.
3. Click the **Communication Profile** tab.
4. Select the **Session Manager Profile** check box.
5. Under the **Call History Settings** section, select or deselect **Enable Centralized Call History?**.
6. Click **Commit**.

Administering Call History for SIP users

You can bulk enable or disable the call history collection for all SIP users or selected SIP users.

Warning:

When a user logs in for the first time after the **Centralized Call History** check box is selected for that user, all calls that were made or received by that user before enabling **Centralized Call History** are lost.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Communication Profile Editor**.
2. Select a user, select multiple users, or select **All**.
3. In the **New Communication Profile Values** section, under **Call History Settings**, select a value from the **Enable Centralized Call History** drop-down menu.
4. Click **Commit**.

Call Journaling High Availability

The Call Journaling feature captures call history data.

Previously, the call logs were captured only on the primary Session Manager server. No call data was stored while the endpoint was failed over to the secondary Session Manager.

In Session Manager, the Call Journaling High Availability feature provides redundancy of the call log data. Call history data is not redundant or highly available when the primary Session Manager for a user is down.

Note:

For Release 7.0, Branch Session Manager does not provide Call Journaling service.

Call data is not redundant for Session Manager user communities that have just one Session Manager. If the Session Manager fails, the data must be restored from a backup. For user communities with more than one Session Manager, the data for the failed Session Manager is restored from the database application running on other Session Manager instances. Although call logs are not maintained on a Branch Session Manager, any missed calls while an endpoint is registered to the Branch Session Manager are recorded by the primary or secondary Session Manager if the primary and secondary Session Manager servers are in service.

Changing the primary Session Manager results in the call logs moved from the old primary Session Manager to the new primary Session Manager. This move is initiated by the new primary Session Manager. The call history is preserved. If the secondary Session Manager is changed for the user, the call log data stored on that Session Manager is moved to the new secondary Session Manager.

The actual deletion of the old call history on the old primary Session Manager occurs within 24 hours, assuming the old Session Manager is running. If the old Session Manager is not running, the deletion occurs during the first nightly audit after the old Session Manager is started. If the secondary Session Manager is changed for a user, any call history data for that user is preserved on the primary Session Manager.

Cassandra clustering and data replication overview

If the **Enable Data Storage Cluster** field on the Session Manager Administration page is selected, all Session Managers are added to the Cassandra database cluster.

If the **Enable Data Storage Cluster** field is not selected, all the Cassandra nodes run in standalone mode.

Cassandra clustering should be done only when Avaya Aura® Device Services servers are configured and paired with Session Manager.

Cassandra data distribution uses the administration on the User Data Storage page to identify the Session Manager instances that are within the same datacenter.

For administering Cassandra data distribution:

1. Enable data storage clustering.
2. Create a data center.
3. Assign co-located Session Managers to the data center.
4. Add the Avaya Aura® Device Services instance to the inventory.
5. Pair a Session Manager instance with an Avaya Aura® Device Services node.

Cluster topology

When the Enable Data Storage Cluster flag is checked, all the Session Manager instances become members of a Cassandra cluster. Each Session Manager instance in the cluster can also be configured as part of a data center.

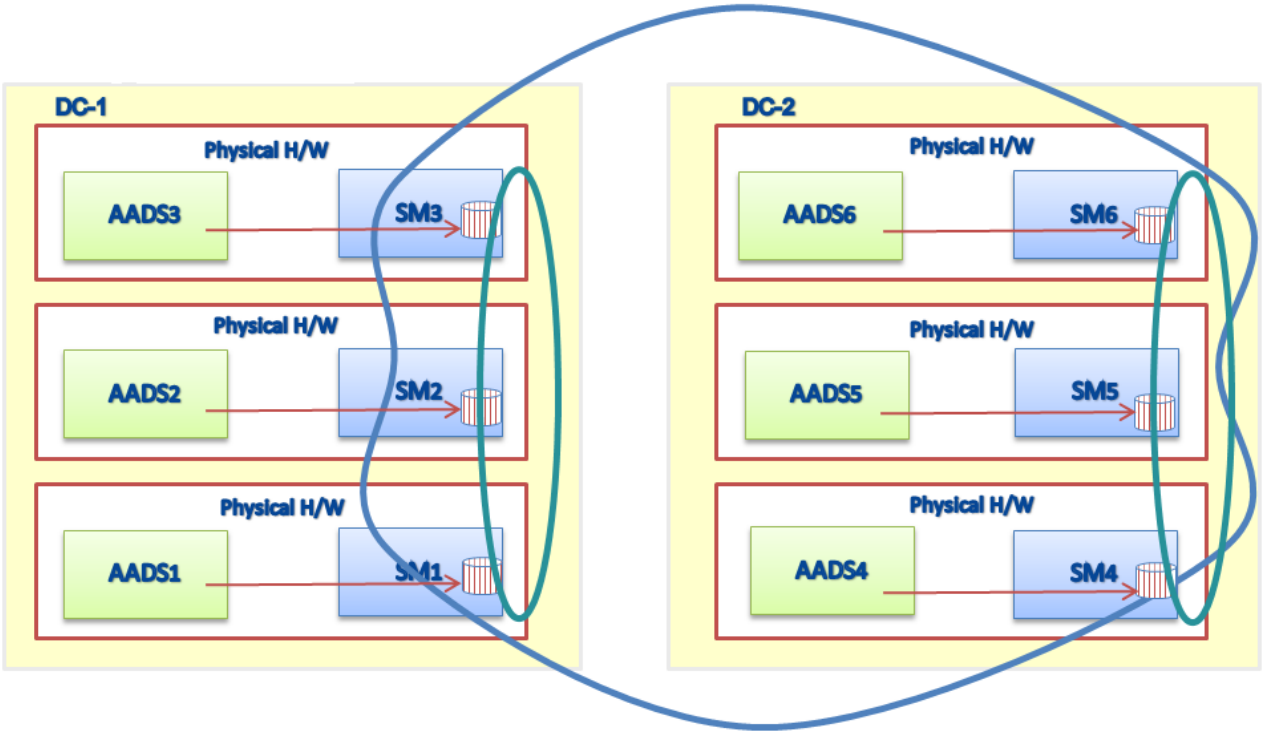


Figure 1: Cassandra Clustering Topology

Enabling data storage clustering

About this task

Use this procedure to enable data storage clustering to activate Cassandra data replication and assign Session Manager instances to discrete data centers for geo-redundancy.

You must use Data Center assignment when Session Manager servers are geographically separated.

Procedure

1. On the home page of the System Manager web console, in **Elements**, click **Session Manager** > **Session Manager Administration**.
2. On the **Global Settings** tab, click **Enable Data Storage Clustering**.
3. Click **Commit**.

Changing the password of a Cassandra admin user

Procedure

1. On the home page of the System Manager web console, in **Elements**, click **Session Manager** > **Session Manager Administration**.
2. Click the **Change Data Storage Password** link.
3. In the **New Data Storage Password** field, type the new password for the Cassandra admin user.
4. In the **Confirm Data Storage Password** field, type the password again to confirm.
5. Click **Commit**.

Adding an Avaya Aura® Device Services instance to System Manager

Repeat these steps for all Avaya Aura® Device Services nodes in the cluster.

Before you begin

Deploy the Avaya Aura® Device Services OVA. For information about deploying and administering the AADS OVA, see *Deploying Avaya Aura® Device Services* and *Administering Avaya Aura® Device Services.*

Note:

is available only with Avaya Equinox® 3.0.

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, click **New**.

   The system displays the New Elements page.
4. In the **General** section, from the **Type** field, select **Avaya Aura Device Services**.

   The system refreshes the page and displays the New Avaya Aura Device Services page.
5. On the **General** tab, perform the following:
   a. In the **Name** field, type the name of the server.
   b. In the **Description** field, type the description of the server.
   c. In the **Node** field, type the IP of the server.

6. On the **Attributes** tab, perform the following:
   a. In the **Login** field, type the admin login name to access the server.
   b. In the **Password** field, type the admin password to access the server.
   c. In the **Confirm Password** field, retype the admin password to access the server.
   d. In the **Version** field, type the version of the server.
   e. In the **Location** field, type the location name of the server.
7. Go back to the General tab.

   Important:

   Access profiles of type GRCommunication and TrustManagement are available by default.
8. Select the TrustManagement access profile, and click **Edit**.
9. In the Access Profile Details section, in the **Name** field, type a name for the access profile.
10. In the **Access Profile Type** field, click **Trust Management** .
11. In the **Protocol** field, click **https**.
12. In the **Host** field, type the FQDN or IP address of the Avaya Aura® Device Services server.
13. Leave the **Container Type** field blank.
14. Leave the other fields unchanged at default values.
15. Click **Save**.

    To enable SSO login, you must add an access profile of type EMURL. Steps 13a to 13k show how to add an access profile of type EMURL.
16. To add an EMURL access profile, on the **General** tab, in the Access Profile section, perform the following:
    a. Click **New**.
    b. In the Application System Supported Protocol section, in the **Protocol** field, click **URI**.
    c. In the Access Profile Details section, in the **Name** field, type a name for the access profile.
    d. In the **Access Profile Type** field, click **EMURL**.
    e. In the **Protocol** field, click **https**.
    f. In the **Host** field, type the server FQDN.
    g. In the **Port** field, type `8445`.
    h. In the **Path** field, type `/admin`.
    i. In the **Order** field, retain the default value.
    j. In the **Description** field, type a description of the access profile.

k. Click **Save**.

17. Click **Commit**.

Next steps

Go to the System Manager home page and click **Device Services** in the Elements section.

The Device Services page displays the element you added. After installation is complete, you can click the name of the element to open the home page.

Adding a Session Manager to a data center

Before you begin

Data Centers need to be added before the Session Manager assigning.

About this task

You can assign a Session Manager instance to a data center while adding a Session Manager instance or after adding the Session Manager instance using the **Edit** button.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Session Manager Administration**.
2. On the Session Manager Administration page, click the **Session Manager Instances** tab.
3. In the Session Manager Instances section, select a Session Manager instance, and click **Edit**.

   The system displays the Edit Session Manager page.
4. From **Data Center**, select a data center.
5. Click **Commit**.

Pairing Session Manager with an Avaya Aura® Device Services node

About this task

You can pair a Session Manager instance to an Avaya Aura® Device Services node while adding a Session Manager instance or after adding the Session Manager instance using the **Edit** button.

Repeat these steps for all Avaya Aura® Device Services nodes in the cluster.

For example, for a Session Manager cluster with two nodes, SM01 and SM02, to deploy an Avaya Aura® Device Services cluster with two nodes, AADS01 and AADS02, you must pair:

- SM01 with AADS01
- SM02 with AADS02

Before you begin

Assign the Session Manager instance to a data center.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Session Manager Administration**.
2. On the Session Manager Administration page, click the **Session Manager** Instances tab.
3. In the **Session Manager Instances** section, select a Session Manager instance, and click **Edit**.

   The system displays the Edit Session Manager page.
4. From **Data Center**, select a data center if one is not already assigned.

   If you do not assign the Session Manager instance to a data center, the system displays the following message: `Session Manager must be assigned to a Data Center to pair with an Avaya Aura Device Services Server.`
5. From **Avaya Aura Device Services Server Pairing**, select an Avaya Aura® Device Services server.

   When an AADS server is already paired with a Session Manager instance, the system does not display that Avaya Aura® Device Services Server in the **Avaya Aura Device Services Server Pairing** drop-down list.
6. Click **Commit**.

Branch Session Manager

Branch Session Manager, also known as Survivable Remote Session Manager, provides a SIP-enabled branch survivability solution. A Branch Session Manager handles emergency calls similar to that of the core Session Manager.

In a typical branch setup,

- A Branch Session Manager provides service to SIP users if a WAN failure occurs between the branch and core.
- A Media Gateway connects the branch to the PSTN and provides media services such as conferencing, tones, and announcements.
- A Survivable Remote Server, also known as a Local Survivable Processor (LSP), is a survivable processor for the branch Media Gateways. The Survivable Remote Server (SRS) provides telephony features to SIP users using application sequencing. The SRS becomes active when a Media Gateway loses connectivity to the main Communication Manager C-LAN or Processor Ethernet.
- End user devices register with the primary Session Manager as a primary controller, and use the Branch Session Manager as a secondary or tertiary controller in case of a WAN failure.

A Branch Session Manager provides service when the branch loses WAN connectivity. When a WAN failure occurs,

- The Branch Media Gateway loses connectivity with the main Communication Manager (procr or C-LAN), and registers with the Branch Communication Manager SRS. As the result, the SRS starts providing service.
- The SIP phones detect connectivity is lost with the core Session Manager and subscribe to the Branch Session Manager.

Configure each Branch Session Manager to support no more than two core Session Managers. You can configure either Session Manager as the primary or the secondary server for a branch user.

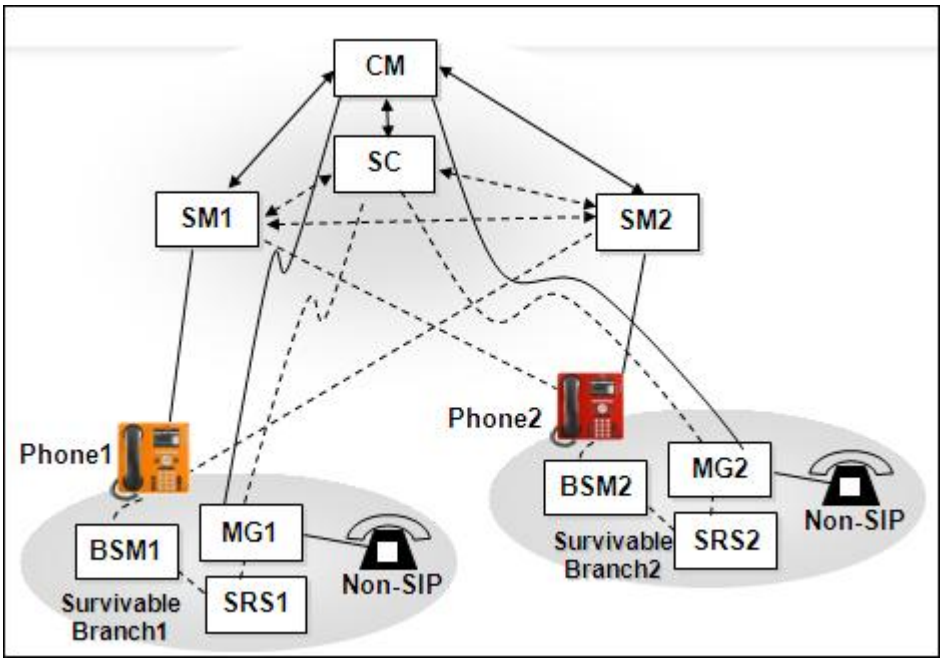
Important:

When a WAN outage occurs, the Branch Session Manager supports the SIP endpoints, possible PSTN access, and the ISDN trunks on the media gateways. The Branch Session Manager does not have access to other adjuncts due to the same WAN outage that caused the Media Gateways to register to the SRS.

For SIP trunks configured with adjuncts, the far-end node name ip-address field displays the Branch Session Manager IP address for the active Survivable Remote server.

Branch Session Manager does not support SIP only users. The Branch Session Managerusers must use the local LSP server along with the appropriate user suite license to support local SIP phones. In addition, SIP only users in the core Session Managers must have a ASM User License.

Survivable Branch Configuration



Comments on this document? infodev@avaya.com

Legend

- BSM: Branch Session Manager (Survivable Remote Session Manager)
- CM: Communication Manager (Feature Server and Evolution Server)
- SRS : Survivable Remote Server (also called as LSP)
- SC: Survivable Core Server
- MG: Media Gateway
- SM: Session Manager

Configuration details

- Phone1 has SM1 as primary, SM2 as secondary, and BSM1 as the local Survivability Server.
- Phone2 has SM2 as primary, SM1 as secondary, and BSM2 as the local Survivability Server.
- Phone1 is served by CM (primary), SC (backup), and SRS (survivable condition).
- Phone2 is served by CM (primary), SC (backup), and SRS (survivable condition).
- MG1 is configured with CM, SC, and SRS1 as reprioritized list of controllers.
- MG2 is configured with CM, SC, and SRS2 as reprioritized list of controllers.

System Behavior

- Phones simultaneously register with multiple SMs in the core and BSM in the branch.
- Gateways connect with the highest priority controller that is reachable.
- If SM1 fails:
  - Phone1 registers with SM2 as the active controller
  - MG1 is served by CM
  - Phone1 is still served by CM
- If Branch1 loses WAN connectivity:
  - MG1 cannot connect with CM or SC. It registers with the SRS1 as the controller.
  - Phone1 cannot connect with SM1 or SM2. It re-registers with the BSM as the active controller.
  - Phones in the branch are served by survivable elements
    - SIP endpoints are served by SRS1 using BSM1.
    - Non-SIP endpoints are served by SRS1 using MG1.
- If CM fails:
  - Media Gateways registers with the SC as the controller.
  - SIP phones are served by SC using SMs in the core.
  - Non-SIP phones are served by SC using Media Gateways.

Remote SIP Trunking

With Public SIP Trunks in a branch location, an enterprise can build network topologies to route SIP traffic to external networks using the branch locations. The network topologies can include the following:

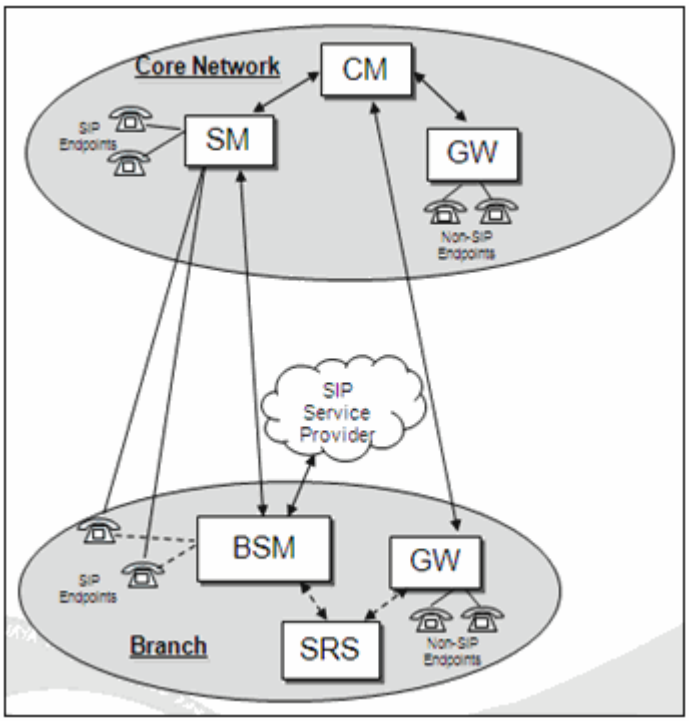
- Intra-enterprise calls such as SIP to SIP, SIP to Non-SIP, Non-SIP to SIP, Non-SIP to Non-SIP.
- Enterprise-bound call from the PSTN (destinations are SIP and non-SIP endpoints).
- Enterprise-originated calls towards the PSTN (SIP and non-SIP originations).

The Branch Session Manager connects with the SIP Service Provider and supports incoming and outgoing SIP Service Provider traffic, irrespective of network connectivity to the data center. For a survivable remote configuration, the following section shows the different branch connectivity scenarios and the associated call flows:

1. Normal Scenario: All provisioned entity link connections between the Branch Session Manager and the core are in service. The Media Gateway is in contact with the primary controller, that is, the core Communication Manager. No error is reported on any of the Branch Session Manager SM links.
2. Failure Scenarios: All provisioned entity link connections between the Branch Session Manager and the core are out of service. When the Media Gateway loses contact with the core Communication Manager, the Media Gateway attempts to re-register with the SRS. The Branch Session Manager is in complete survivable mode due to a full WAN outage of the branch. All the components in the branch such as phones, Media Gateway, and Branch Session Manager , have lost connectivity with all the components in the core, such as Session Manager and Communication Manager.

Call Scenarios

Normal scenarios



- SIP phones in the branch locations are simultaneously registered with core Session Manager and Branch Session Managers (BSM)
- SIP phones are registered with one of the core SMs as the active controller.
- Media Gateways are registered with Communication Manager (CM) in the core.
- BSM has direct connectivity with SIP Service Provider (SP).
- BSM and SM have direct connectivity.

The following are some example call scenarios to illustrate the behavior of the feature. The scenarios listed here are not intended to be a complete list of all possible configurations and call scenarios.

Case 1: Calls incoming from the SP branch SIP trunk to a branch SIP user

1. Request arrives at BSM from SIP SP interface.
2. BSM perform ingress adaptation and routes the request to primary core SM of the called party.
3. SM invokes core CM as the sequenced application and completes sequenced application invocation.
4. SM performs contact resolution and routes the call to the SIP endpoint at the branch.

Case 2: Calls going to the SP branch SIP trunk from a branch SIP user

1. Branch SIP user initiates a call to an external number.

2. Core SM invokes core CM as a sequence application and completes sequenced application invocation.
3. Based on dial patterns, SM routes the request to the SIP SP connected with the BSM.
4. SM performs egress adaptation and Call Admission Control (CAC).
5. SM routes the request to BSM with route-through to SIP SP. Based on route-header, BSM routes the request to SIP SP.

Case 3: Calls incoming from the SP branch SIP trunk to a branch non-SIP user

1. Request arrives at BSM from SIP SP interface.
2. BSM perform ingress adaptation and then routes the request to one of the core SM instances.
3. Based on the dial pattern, SM routes the request to core CM.

   Note:

   CM-ES does CAC for this call.
4. CM processes the request and terminates the request at the branch non-SIP endpoint.

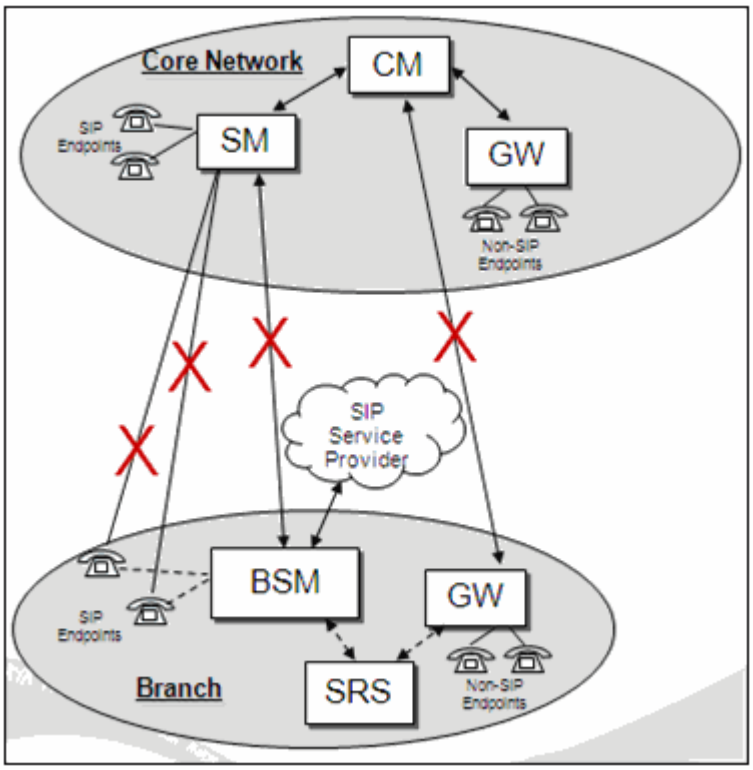
Case 4: Calls going to the SP branch SIP trunk from a branch non-SIP user

1. Branch non-SIP endpoint initiates a call to an external number.
2. CM performs call processing and routes the request to SM.
3. Based on dial patterns, the SM determines the request should be routed to SIP SP connected with BSM. SM performs egress adaptation and CAC. Finally, SM routes the request to BSM with route-through to SIP SP.
4. Based on the Route header, BSM routes the request to SIP SP.

Case 5: Calls incoming from the SP branch SIP trunk for a non-branch SIP user

1. Request arrives at BSM from SIP SP interface.
2. BSM performs ingress adaptation and then routes the request to one of the core SMs.
3. The authoritative SM performs CAC and invokes core CM as the sequenced application and completes sequenced invocation.
4. SM performs contact resolution and routes the call to the non-branch SIP user.

Failure scenarios



- Branch users are provisioned with one core SM (SM-1) and the BSM. There is no secondary SM.
- Branch SIP phones, after losing connectivity with SM-1, mark BSM as the active controller.
- Media Gateways in the branch detect outage and connect with SRS as the controller.
- SRS activates the link with BSM.
- Branch loses connectivity with all the core networks.

The following example call scenarios illustrate the behavior of the feature. The scenarios listed are not intended to be a complete list of all possible configurations and call scenarios.

Case 1: Calls incoming from the SP branch SIP trunk to a branch SIP user

1. Incoming request from the SIP SP arrives at BSM.
2. BSM performs ingress adaptation.
3. BSM detects the outage of the primary controller of the branch SIP user.
4. BSM invokes SRS as the sequenced application and completes application sequencing.
5. BSM terminates the call at the locally registered SIP endpoint.

Case 2: Calls going to the SP branch SIP trunk from a branch SIP user and entire core is unreachable

1. A call originates from branch SIP user.

2. BSM detects the outage of the primary controller of the branch SIP user.
3. BSM invokes SRS as the sequenced application and completes application sequencing.
4. BSM cannot connect with any core SM.
5. BSM performs routing based on partial routing data.
6. Before forwarding the request to SIP SP, BSM performs egress adaptation. No CAC is performed at this step.

Branch SIP Trunk administration for PSTN connectivity

About this task

The following are the high level administration steps for administering branch SIP trunks with SIP Service Provider.

You must first administer the service providers interface as the new SIP entity. You must also create SIP entity links between:

1. The associated Branch Session Manager and one or more core Session Manager instances.
2. The service provider SIP entity and the associated Branch Session Manager.

Note:

You can administer direct SIP Entity Links between Branch Session Manager and other types of SIP Entities – similar to Session Manager. For instance, you can directly connect Messaging Service to Branch Session Manager in Branch.

Procedure

1. Add a new SIP Entity with type **Service Provider**. Use the IP address of the service provider equipment.
2. Modify the Adaptation as needed.
3. Add a SIP Entity link between the **Service Provider** and the Branch Session Manager.
4. Add Entity Links between the Branch Session Manager and the core Session Manager instances.

   Note:

   Links must be available between the Branch Session Manager and any core Session Manager instances that are controllers for users on the branch. For call routing, at least one link must be available between the Branch Session Manager and a core Session Manager to make calls to the core.
5. Administer SIP Monitoring for all Branch SIP Trunks.

Administering Branch Session Manager

The following are the basic steps for administering a Branch Session Manager.

Before you begin

Using System Manager, administer the main Communication Manager Feature Server or Evolution Server (CM-FS/ES) as an Inventory element. For information and procedures, see *Administering Avaya Aura® System Manager* on the Avaya support site.

Procedure

1. Add a SIP Entity for the Branch Session Manager using the IP address of the Branch Session Manager Security Module.
2. Using the System Manager Web Console, administer a Branch Session Manager Instance on the Session Manager Administration page.
3. Create Entity Links between the Branch Session Manager and the main Communication Manager server. The Branch Session Manager uses the administered entity link to the main Communication Manager to internally generate an entity and entity link connection to the survivable remote server. The system uses the connection for survivability mode.
   - If Communication Manager is configured as a Communication Manager Feature Server or Trunk Gateway (CM FS/TG):
     - Create an entity link between the Branch Session Manager and the core Communication Manager Feature Server.
     - Create an entity link between the Branch Session Manager and the core Communication Manager Trunk Gateway.
   - If Communication Manager is configured as a Communication Manager Evolution Server (CM-ES):
     - You can configure a CM-ES using just one entity link. The system uses the entity and entity link for both application sequencing and trunk gateway routing.
     - Each entity link must use the same port and transport as the corresponding link to the primary Session Manager in the core. The ports between the Communication Manager and Session Manager entities must be unique.
4. If required, create a sequence of applications (application sequence). The Communication Manager application you select should be the same as specified on the Branch Session Manager administration page.

   Note:

   If Branch Session Manager is used only for routing purpose with only H.323 (non-SIP station) setup, then administration of application and application sequence is required. If application sequence is not administered, then the link between the LSP and Branch Session Manager will not work as expected.
5. Administer SIP user profiles using the Branch Session Manager as the survivability server.

Branch Session Manager Instances field descriptions

Name	Description
Name	The name of the administered Branch Session Manager. If a warning symbol appears after the name, the Branch Session Manager instance is in the Maintenance Mode service state.
License Mode	Status of the Session Manager or Branch Session Manager license. The status can be: • **Normal:** The license is valid and no errors are detected. • **Error:** The license is not accessible or does not exist. The system displays the time remaining in the 30–day grace period. • **Restricted:** The 30–day grace period has expired. Session Manager or Branch Session Manager, if operational, is now in the **Deny New Service** state. Clicking the link displays the WebLM Home page.
Main CM for LSP	The main Communication Manager for the Local Survivable Processor (LSP) associated with this Branch Session Manager.
SIP Communication Profiles	The number of Communication Profiles assigned to this Branch Session Manager.
Description	Description of the Branch Session Manager.

Button	Description
New	Create a new Branch Session Manager instance.
View	View the information related to the selected Branch Session Manager instance.
Edit	Edit the information for the selected Branch Session Manager instance.
Delete	Delete the selected Branch Session Manager instance.

Adding a Branch Session Manager instance

You can administer a SIP entity as Branch Session Manager instance using:

- Session Manager Administration pages.
- Manage Elements pages.

Endpoints use the listen ports to connect to the Branch Session Manager. You can map different listen ports to different domains. You administer the listen ports on the SIP Entity page.

Procedure

1. Verify the SIP entity exists and is administered as type **Session Manager**.
2. Do one of the following:
   - Use the Session Manager Administration page:
     a. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager** > **Session Manager Administration**.
     b. Click the **Branch Session Manager Instances** tab.
     c. Click **New**.
   - Use the Manage Elements page:
     a. On the home page of the System Manager Web Console, under **Services**, click **Inventory** > **Manage Elements**.
     b. Click **New**.
     c. In the **Type** field, select **Session Manager** from the drop-down menu.
     d. When the screen refreshes, from **Select type of Session Manager to add:**, select **Branch Session Manager**.
     e. Click **Continue**.
3. On the Add Branch Session Manager page, in the General section, perform the following:
   a. Select the **SIP Entity Name** from the drop-down menu.
   b. **(Optional)** Type a description in the **Description** field.
   c. In the **Management Access Point Host Name/IP** field, type the IP address of the management interface of the Branch Session Manager.

      The **Management Access Point Host Name/IP** field accepts only IPv4 addresses even when you create Session Manager instances for entities supporting IPv6 or Both address families.
   d. Select the **Main CM for LSP** form the drop-down menu.

      You can click the **View / Add CM Entities** link to add new Communication Manager applications.
   e. Select **Enable** for **Direct Routing to Endpoints**.
   f. Select the **Maintenance Mode** check box if you are:
      - Staging a non-operational Branch Session Manager.
      - Pre-administering a Branch Session Manager on System Manager prior to host installation.
   g. Select the **Adaptation for Trunk Gateway** from the drop-down menu, if required.
4. Specify the appropriate information in the remaining required fields.

   For information about the fields, see Add Branch Session Manager Administration page field descriptions.

5. Click **Commit**.

Viewing Branch Session Manager administration settings

You can view the administration settings for Branch Session Manager instances using either the:

- Session Manager Administration pages.
- Manage Elements pages.

Procedure

1. On the home page of the System Manager Web Console, do one of the following:
   - Under **Elements**, click **Session Manager** > **Session Manager Administration**.
   - Under **Services**, click **Inventory** > **Manage Elements**.
2. Select a Branch Session Manager instance.
3. Click **View**.
4. After you have viewed the information, click **Return**.

Modifying the Branch Session Manager administration settings

Procedure

1. On the home page of the System Manager Web Console, do one of the following:
   - Under **Elements**, click **Session Manager** > **Session Manager Administration**.
   - Under **Services**, click **Inventory** > **Manage Elements**.
2. Select a Branch Session Manager instance.
3. Click **Edit**.
4. Make the necessary changes.
5. Click **Commit**.

Deleting a Branch Session Manager instance

You can delete more than one Branch Session Manager instance at the same time.

You can delete a Branch Session Manager instance using either the:

- Session Manager Administration pages.
- Manage Elements pages.

Before you begin

Important:

Before deleting a Branch Session Manager instance, you must either:

- Disassociate the Session Manager instance from all of the related Communication Profiles, or
- Delete the associated users.

Procedure

1. On the home page of the System Manager Web Console, do one of the following:
   - Under **Elements**, click **Session Manager** > **Session Manager Administration**.
   - Under **Services**, click **Inventory** > **Manage Elements**.
2. Select a Branch Session Manager instance.
3. Click **Delete**.
4. Click **Delete** on the confirmation page.

Add Branch Session Manager page field descriptions

General

Name	Description
SIP Entity Name	The name of the SIP entity that you are adding as a Branch Session Manager instance. The entity must be of the **Session Manager** type and must be in the **Sync** state.
Description	The description of the SIP entity. This field is optional.
Management Access Point Host Name / IP	The IP address of the management agent of the Branch Session Manager. The **Management Access Point Host Name/IP** field accepts only IPv4 addresses even when you create Session Manager instances for entities supporting IPv6 or Both address families.

Table continues…

Name	Description
Main CM for LSP	Main Communication Manager for the LSP associated with this Branch Session Manager. The options are: • **Refresh**: Updates the list of Communication Manager systems. • **View/Add CM Systems**: Views or adds to the list of currently provisioned Communication Manager systems.
Direct Routing to Endpoints	The direct routing to endpoints.
Maintenance Mode	The maintenance mode of Branch Session Manager.
Adaptation for Trunk Gateway	The digit conversion of the SIP trunk to the Branch Session Manager. Branch Session Manager uses the selected adaptation for routing calls to or from the Communication Manager LSP trunk gateway. **Note:** For the Communication Manager Feature Server (CM-FS) or Communication Manager Trunk Gateway (CM-TG), the adaptation from the core CM-TG is used by default. The adaptation selection overrides the default CM-TG adaptation and applies to all calls routed on the trunk gateway entity to the LSP. For Communication Manager Evolution Server (CM-ES), the default adaptation is taken from the core Communication Manager entity. The adaptation applies to calls that are routed through the gateway to the LSP and also to calls that are application-sequenced.

Security Module

Name	Description
SIP Entity IP Address	The IP address of the Branch Session Manager as specified on the SIP Entity Details page.
Network Mask	The network mask of the domain name of the server that hosts the Branch Session Manager application. The network mask is passed to the security module. The agent configures the network mask to define the subnet that the security module is to be associated with.
Default Gateway	The IP address of the default gateway.

Table continues…

Name	Description
Call Control PHB	The field that specifies the SIP traffic type of service and priority as the SIP traffic travels through the IP network. All packets leaving the security module that contain SIP signaling have the specified value in the differentiated service code point (DSCP) field of the IP header. Intervening routers may or may not treat packets containing this value with a different level of precedence. The routers must either support differentiated service by default or be specially configured to do so. Different DSCP values are specified in RFCs 2597 and 2598. To be consistent with Communication Manager, Branch Session Manager uses a default DSCP value of 46. This value indicates forwarding with the highest priority.
SIP Firewall Configuration	The SIP Firewall Configuration associated with the Branch Session Manager instance.

Monitoring

Note:

Regardless of the administered settings, Branch Session Manager monitors the feature server entity **avaya-lsp-fs** every second. The monitoring settings are important because the system uses links for failover and failback procedures on Branch Session Manager. If an additional connection exists to the LSP for the trunk gateway, these administered monitoring settings also apply.

Button	Description
Enable Monitoring	The monitoring of the administered SIP entities associated with this Branch Session Manager instance.
Proactive cycle time (secs)	The time in seconds for polling the administered SIP entities associated with this Branch Session Manager. Proactive monitoring occurs as long as no outages are detected. The default is 900 seconds. The default value is used for each administered SIP entity unless overridden by the **Monitoring** option on the SIP Entities page for a specific entity.

Table continues…

Button	Description
Reactive cycle time (secs)	The time in seconds for when proactive monitoring detects that an administered SIP entity is unreachable and changes to a reactive mode. Reactive monitoring continues until the SIP entity responds again. The value for reactive monitoring must be less than the value for proactive monitoring. The default value is 120 seconds. The default value is used for each administered SIP entity unless overridden by the **Monitoring** option on the SIP Entities page for a specific entity.
Number of Retries	The number of times that the Branch Session Manager polls a SIP entity before the SIP entity is deemed unreachable. The default value is 1. The Branch Session Manager uses the default value for each administered SIP entity unless overridden by the **Monitoring** options on the SIP Entities page for a specific entity.

Personal Profile Manager (PPM) - Connection Settings

During normal operation, Branch Session Manager receives data from Communication Manager feature server for synchronizing Avaya SIP endpoints.

Note:

Branch Session Manager supports a feature that indicates that the Service Observe (SO) button is assigned to the SIP endpoint. The button can be activated by a registered user.

Name	Description
Limited PPM client connection	The limited mode for the PPM client connection. The default value is **Enabled**.
Maximum Connection per PPM client	The maximum number of connections per PPM client. The valid values are integers between 1 and 10. The default value is 3.
PPM Packet Rate Limiting	The limiting value for the PPM packet rate. The default is **Enabled**.
PPM Packet Rate Limiting Threshold	The number of packets per second that the PPM connection will transfer. This value is applied per PPM client. The range is 1 to 500. The default value is 200.

Event Server

Name	Description
Clear Subscription on Notification Failure	The option to remove the subscription or not when NOTIFY failures occur. The default is **No**.

Button	Description
Commit	Saves the added SIP entity as a Branch Session Manager instance with the selected configuration options.
Cancel	Cancels the changes.

Branch Session Manager Instances field descriptions

Name	Description
Name	The name of the administered Branch Session Manager. If a warning symbol appears after the name, the Branch Session Manager instance is in the Maintenance Mode service state.
License Mode	Status of the Session Manager or Branch Session Manager license. The status can be: • **Normal:** The license is valid and no errors are detected. • **Error:** The license is not accessible or does not exist. The system displays the time remaining in the 30–day grace period. • **Restricted:** The 30–day grace period has expired. Session Manager or Branch Session Manager, if operational, is now in the **Deny New Service** state. Clicking the link displays the WebLM Home page.
Main CM for LSP	The main Communication Manager for the Local Survivable Processor (LSP) associated with this Branch Session Manager.
SIP Communication Profiles	The number of Communication Profiles assigned to this Branch Session Manager.
Description	Description of the Branch Session Manager.

Button	Description
New	Create a new Branch Session Manager instance.
View	View the information related to the selected Branch Session Manager instance.
Edit	Edit the information for the selected Branch Session Manager instance.
Delete	Delete the selected Branch Session Manager instance.

E911 Services

Using the E911 service, you can identify the physical location of a registered user in the event of an emergency call. The system determines the location using the IP address and port level discovery of the E911 administration.

Session Manager interacts with E911 service user registrations to obtain an Emergency Location Identification Number (ELIN). Each Session Manager synchronizes with the E911 services server, stores ELIN records for registered users, and sends the ELIN to the Communication Manager when a user makes an emergency call. Session Manager synchronizes with the E911 services server when:

- You add the ELIN server to the Session Manager.
- The connection between Session Manager and the server is lost and later restored.
- User registration and unregistration causes the Session Manager to synchronize with the E911 service.

E911 services operate in a primary and secondary server mode. The primary server is active, and the secondary server is in standby mode.

Related links

Emergency Call Notification to Adjunct Emergency Location Server on page 457
Administering the ELIN server on page 458

Emergency Call Notification to Adjunct Emergency Location Server

With the Multiple Device Access (MDA) feature, users can register with multiple devices. In the past, the multiple devices usage with one extension number, may have resulted in a problem establishing the exact location of an emergency call. However, in Session Manager, the callers exact location can now be determined. This allows Session Manager to support the tracking of an emergency caller in large campus settings. The advanced communication applications guide the emergency crew to the exact location of the emergency call using LED display units near the main entrance of the site.

The applications use the capabilities of the following Avaya Aura® components:

- Session Manager shares the IP address of the caller's SIP device.
- Communication Manager shares the identity of the emergency caller from the database.

Session Manager adds an Emergency Call (EC) Alert to the existing Adjunct Emergency Location Server (AELS) interface for the SIP users. The AELS establishes the exact location of the emergency caller.

The caller may be a SIP user registered through System Manager or an unregistered/unknown user.

Related links

E911 Services on page 457

Administering the ELIN server

The following are the high-level steps for administering the ELIN server

Procedure

1. On the Local Host Name Resolution page, administer the FQDN for the ELIN Server. You need to administer a Local Host Name entity for two different IP address with different priorities for the primary and secondary servers.
2. Add a SIP Entity of type **ELIN Server** using the administered FQDN.
3. On the Session Manager Administration page, in the Global Settings section, select the administered ELIN Server for the **ELIN SIP Entity** field.
4. Create the Entity Links from ELIN Server to all Session Manager SIP Entities.
5. Import certificates, using a TLS link between the Session Manager and the ELIN server. This step is required only if the entity link is of type **TLS**.

Note:

OPTIONS monitoring is enabled between the Session Manager and the and ELIN Server. Monitoring is applied to all entity links and you should not disable it.

Related links

E911 Services on page 457

Communication Profile Editor

Using the Communication Profile Editor, you can:

- View a list of all Session Manager Communication Profiles using sort and filter options.
- Bulk edit required Communication Profile attributes across selected Communication Profiles. For example, replace a Session Manager instance for the selected Communication Profiles at one time instead of editing individual profiles using the User Profile Edit page.
- View the background edit job status of bulk editing a Communication Profile.
- View the Communication Profile edit failures during bulk editing operations.

Important:

You add a SIP endpoint to the Aura Network by creating a Communication Profile that contains a Communication Manager endpoint profile and a Session Manager profile. The Communication Manager profile associates the user with a station on a Communication

Manager that is in the core network. The Session Manager profile assigns the primary and secondary Session Managers of the user, the application sequences, and the survivability server. For correct application sequencing to Communication Manager, the application sequences must reference the same Communication Manager as the Communication Manager endpoint profile. For correct survivability configuration, if a Branch Session Manager is specified as the survivability server, the Branch Session Manager must also reference the same Communication Manager as the Communication Manager endpoint profile.

Note:

When you change the Primary Session Manager, the Secondary Session Manager or the Survivable Server (Branch Session Manager) for one or more users using the Communication Profile Editor page, the system verifies valid SIP Entity links exist between the components. If any of these links do not exist, the system automatically creates the required links. The default protocol and ports of the generated links are specified in the **Entity Links** section of the **Routing** > **Defaults - Personal Settings** page.

Viewing Communication Profiles

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Communication Profile Editor**.
2. To view using the sorting option, click a column title to sort the information in the table as the primary sorting order.
3. To view using the filtering option, enable the **Filter** option and enter the filter information in the appropriate field. You can use the filter option for one or more fields. The table displays only those results that match all the filtering criteria.

Customizing column display

About this task

You can customize the column display on the Communication Profile Editor page using one of the following methods:

- Select the columns you need to get displayed in the table
- Order the appearance of the columns
- Reset the column appearance to the default columns

Note:

The customization settings are valid for the current user session only. After the user logs out, the customization settings revert to the default appearance.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Communication Profile Editor**.
2. Click the **Customize** link in the upper right of the table.
3. Use the following actions to customize the **Available Columns** and **Display Columns**:
   - **Move:** Select a column entry under **Available Columns** and move it to **Display Columns**.
   - **Move All:** Move all of the entries under **Available Columns** to **Display Columns**.
   - **Remove:** Remove an entry from under **Display Columns**.
   - **Remove All:** Remove all entries from under **Display Columns**.
4. To rearrange the selected columns under **Display Columns**:
   - Click **Top** to move the selected column to the top of the list.
   - Click **Up** to move the selected column one position up on the list.
   - Click **Down** to move the selected entry down one position on the list.
   - Click **Bottom** to move the selected column to the bottom of the list.
5. To restore the default settings, click **Default**.
6. To apply the changed settings, click **Apply**.
7. Click **Close** to close the customization section.

Modifying Communication Profiles

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Communication Profile Editor**.
2. Do one of the following:
   - Select the rows that you need to modify.
   - Click **All** to select all the rows.
3. In the New Communication Profile Values section, all fields initially have the default value as **Use existing values**. Modify the field values to be set as property values for the selected list of Communication Profiles.

   You cannot set the values for the **Primary Session Manager** and **Home Location** fields as **None**. To add a new value for the **Home Location** field, you need to add a location using the **Routing** > **Locations** menu selection.
4. Click **Commit**.
5. Click **Commit** on the confirmation page.

Viewing background edit job status

The Background Edit Job Status section displays the status of all background edit jobs since the last restart of System Manager.

When the number of simultaneous Communication Profile editing operations exceed 15, the operations are queued as batch jobs.

Procedure

On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Communication Profile Editor**.

Viewing Communication Profile edit failures

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Communication Profile Editor**.
2. In the Background Edit Job Status section, select the edit job that did not complete successfully.
3. Click **View Profile Edit Failures** to view the details of all Communication Profiles that cannot be modified in the selected job run.

   The Session Manager Communication Profiles section displays the details of those existing profiles that could not be edited due to the failed job run.
4. Click **Return to View All Profiles** to return to the original Communication Profile Editor screen.

Stopping Communication Profile editing jobs

About this task

This functionality enables termination of the current running Communication Profile background editing jobs.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Communication Profile Editor**.
2. On the Local Host Name Resolution page, in the Background Job Status section, select a running edit job and click **Stop Job**.

Communication Profile Editor field descriptions

Customize Column Display section

List	Description
Available Columns	The list of available columns.
Display Columns	The list of selected columns.

Link	Description
Customize	Expand the **Customize Column Display** section.
Move	Move selected items from the **Available Columns** list to the **Display Columns** list.
Move All	Move all items from the **Available Columns** list to the **Display Columns** list.
Remove	Remove selected items from the **Display Columns** list.
Remove All	Remove all items from the **Display Columns** list.
Top	Move the selected items of **Display Columns** list to the top of the list.
Up	Moves the selected items of **Display Columns** list to one position up in the list.
Down	Move the selected items of **Display Columns** list to one position down in the list.
Bottom	Move the selected items of **Display Columns** list to the bottom of the list.

Button	Description
Default	Restore the default column settings of the **Available Columns** and **Display Columns** lists.
Apply	Apply the changes made in the column customizing lists to the **AST Device Notifications** section.
Close	Collapse the **Customize Column Display** section.

Session Manager Communication Profiles

Name	Description
Login Name	Full unique login name of the user.

Table continues…

Name	Description
Address: Handle	Handle part of the Communication Address. **Note:** The displayed address can be either the “E.164 ” or the “Avaya E.164” address as specified on the User Profile page.
Address: Domain	Domain part of the Communication Address.
Primary Session Manager	The name of the primary Session Manager that is used as the default access point for connecting devices associated with the Communication Profile to the Avaya Aura® network. You must select the Session Manager server.
Secondary Session Manager	The name of the secondary Session Manager that provides continued service to SIP devices associated with the Communication Profile when the primary Session Manager server becomes unavailable. A selection is optional.
Origination Sequence	The list of application sequences that will be invoked when the system routes calls from this user. **Note:** If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, then Communication Manager must be the same in both the sequences.
Termination Sequence	The list of application sequences that will be invoked when the system routes calls to this user. **Note:** If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, then Communication Manager must be the same in both the sequences.
Emergency Calling Origination Sequence	The list of application sequences that will be invoked when the system routes emergency calls from this user.
Emergency Calling Termination Sequence	The list of application sequences that will be invoked when the system routes emergency calls to this user when **Enable Application Sequence for Emergency Calls** is selected under Global Settings..

Table continues…

Name	Description
Conference Factory Set	Name of the Conference Factory Set associated with this user.
Survivability Server	Name of the Survivability Server that provides survivability communication services for devices associated with a Communication Profile when the local connectivity to Session Manager instances in the Avaya Aura® core is lost.
Max. Simultaneous Devices	The maximum number of endpoints that can register at a time using this Communication Profile. If you register more than one endpoint, all the endpoints receive calls simultaneously. The value range is 1–10. The default is 1.
Home Location	The 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 the IP Address Pattern of any of the locations. This is a mandatory field. **Note:** A user's call is routed according to the user's home location except for the following cases: • Call Admission Control routes based on actual location. • Emergency calling routes based on actual location.
Enable Centralized Call History	Enable or disable Call History logging.

The field descriptions for the **New Communication Profile Values** section are the same as above. Click **Commit Changes** to save the field values for the selected Communication Profiles.

Background Edit Job Status

This section provides a list of Communication Profile editing operations that run as background jobs since the last restart of System Manager. When the number of simultaneous Communication Profile editing operations exceed 15, the system queues these operations as batch jobs.

Button	Description
View Profile Edit Failures	Displays editing failure information for all Communication Profiles that could not be modified in the selected job.
Stop Job	Stop the current running background edit job.

Name	Description
Start Time	Start time of the background edit job.
Status	Status of the background edit job.
Percent Completed	Percentage completion of the background edit job.
Total Edits to Perform	Number of background edits to be performed in the job run.
Failed Edits	Number of failed background edits during the job run.
Last Updated	Finish time of the background edit job run.
Job Name	Name of the background edit job.

Communication Profile Edit Confirmation page field descriptions

Button	Description
Commit	Saves the changes to the selected Session Manager Communication Profiles. **Note:** If the Communication Profiles for bulk editing equals 15 or less in number then the edit changes are committed immediately. Otherwise for Communication Profiles numbering more than 15, the edit changes run as background job.
Cancel	Cancels the changes to the selected Session Manager Communication Profiles.

Network Configuration

Failover Groups

A Failover Group is a group of two active Session Manager instances that are interconnected to ensure high availability of Session Manager services.

During normal operations, one Session Manager instance in a Failover Group is active and handles calls. The other Session Manager instance is active as a backup. In cases when the preferred Session Manager instance fails to handle a call or becomes unreachable to the peer SIP entities, the failover mechanism preserves the session information and switches the call control

from the failed Session Manager to the backup Session Manager. The backup Session Manager then uses the preserved session information and resumes the call.

You can associate peer SIP entities with the Failover Group. The peer SIP entities can detect a Session Manager failure and reroute the call to the backup Session Manager.

Each Failover Group has a Group Name and a unique Failover Group Domain Name (FGDN) for each Session Manager instance in the group. The peer SIP entities use the FGDN to resolve the preferred and the backup Session Manager instances at the time of network outage. The Failover Group has two ordered resolution sets, namely **Session Manager 1 Preferred Domain Name** and **Session Manager 2 Preferred Domain Name**.

- The **Session Manager 1 Preferred Domain Name** resolves the preferred Session Manager as high priority and the backup Session Manager as secondary.
- The **Session Manager 2 Preferred Domain Name** resolves the backup Session Manager as high priority and the operational Session Manager as secondary

In some cases, the source and the destination entities in a call do not have the same Failover Group domain associations. To preserve a call in such cases, the Session Manager Failover Group provides a Two-Tier Routing mechanism known as route-through. Two-Tier routing mechanism ensures that during a Session Manager outage, either entity can route responses or mid-dialog requests using alternate Session Manager instances of different Failover Groups.

When you add a Failover Group, the system runs an entity link audit to verify that each Session Manager in a Failover Group is connected to every other Session Manager in the group using a TCP and a TLS entity link and the administered failover ports of each Session Manager. The Entity Link audit process determines:

- If one or more entity links have not yet been added.
- If existing entity links do not use the correct listen ports or are not trusted.

For example:

1. SM1 and SM2 constitute one Failover Group.
2. SM2 and SM3 constitute another Failover Group.
3. Session Manager runs the audit.
4. The audit generates the missing entity links automatically between SM1 and SM2, SM2 and SM3, and SM1 and SM3 for the failover ports for each transport type. The link between SM1 and SM3 is a newly generated link.

For more information regarding system administration for different configurations, see *Call Preservation Feature Description and Administration Guide* on the Avaya support website.

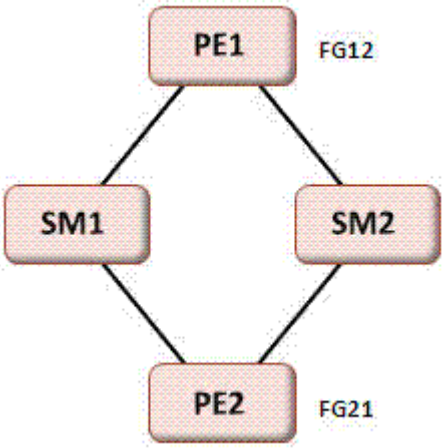
Scenarios for Two-Tier Routing

Two-Tier Routing is a route-through mechanism of the Failover Group feature. Two-Tier Routing provides call preservation even if the source and the destination peer SIP entities in a call are associated with different Session Manager instances of different Failover Groups.

The following sample scenarios describe the call routing process in different situations.

Scenario 1

The source and the destination Peer SIP entities (PE) have different associated failover group domains and are connected to the same set of Session Manager instances.



PE1 prefers SM1 (Failover Group FG12) while PE2 prefers SM2 (Failover Group FG21).

FG12 and FG21 resolve SM1 as well as SM2.

During normal condition, the request and response between PE1 and PE2 are routed as: PE1—SM1—SM2—PE2

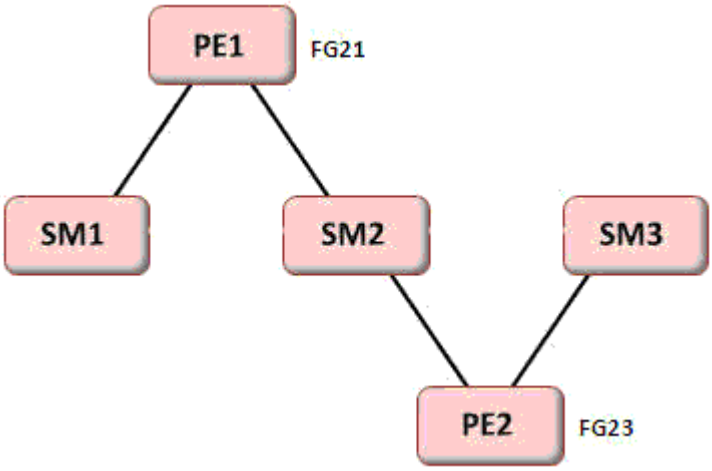
If SM1 fails, the request and response is routed as: PE1—SM2—SM2—PE2

If SM2 fails, the request and response is routed as: PE1—SM1—SM1—PE2

The Failover Group preserves the call between PE1 and PE2.

Scenario 2

The source and the destination Peer SIP entities have different associated failover group domains and are connected to a different set of Session Manager instances. However, both the Peer SIP entities are connected to the common Session Manager instance.



PE1 prefers SM2 (Failover Group FG21) and PE2 also prefers SM2 (Failover Group FG23).

FG21 and FG23 resolve SM2. There is no direct connectivity between SM1 and PE2 as well as SM3 and PE1.

During normal condition, the request and response between PE1 and PE2 is routed as: PE1–>SM2–>SM2–>PE2

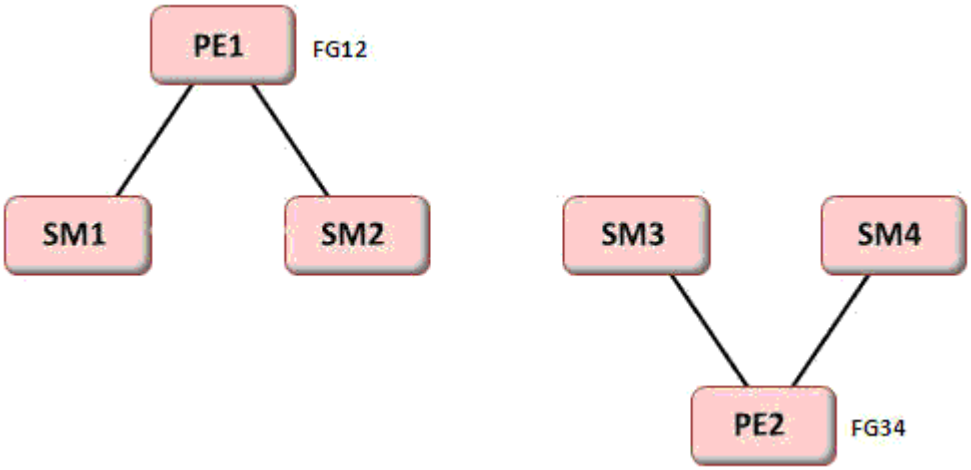
If SM2 fails, the Failover Group feature establishes a connection (Two Tier Routing or route through) between SM1 and SM3.

The request and response is routed as: PE1–>SM1–>SM3–>PE2

The Failover Group preserves the call between PE1 and PE2.

Scenario 3

The source and the destination Peer SIP entities have different associated failover group domains, different set of Session Manager instances, and both the Peer SIP entities are connected to a different Session Manager instance.



PE1 prefers SM1 (Failover Group FG12) while PE2 prefers SM3 (Failover Group FG34).

There is no direct connectivity between SM1 and PE2 as well as SM4 and PE1.

During normal conditions, the request and response between PE1 and PE2 is routed as: PE1–>SM1–>SM3–>PE2

If SM1 fails, the Failover Group feature establishes a connection (Two Tier Routing or route through) between SM2 and SM3.

The request and response is routed as: PE1–>SM2–>SM3–>PE2

If SM3 fails, the Failover Group feature establishes a connection (Two Tier Routing or route through) between SM1 and SM4.

The request and response is routed as: PE1–>SM1–>SM4–>PE2

The Failover Group preserves the call between PE1 and PE2.

Failover Groups Page Field Descriptions

Button	Description
Add	Add a new Failover Group.
Edit	Modify information for an existing Failover Group.
Delete	Delete one or more existing Failover Groups.
Manage Peer Entities	Associate or remove peer SIP entities with a Session Manager instance.

Name	Description
Group Name	Name of the Failover Group.
Session Manager 1	
Preferred Domain Name	A unique and a fully qualified preferred domain name for the preferred Session Manager of the Failover Group.
Session Manager	Name of the operational Session Manager from the drop-down list.
Session Manager 2	
Preferred Domain Name	A unique and a fully qualified preferred domain name for the backup Session Manager instance of the Failover Group.
Session Manager	Name of the backup Session Manager from the drop-down list. **Note:** Do not select the same Session Manager instance for **Session Manager 1** and **Session Manager 2**.

Related links

Adding a new Failover Group in Session Manager on page 469
Editing Failover Group information on page 471
Deleting a Failover Group from Session Manager on page 471
Adding peer SIP entities to a Failover Group on page 472
Removing peer SIP entities from Failover Groups on page 474

Adding a new Failover Group in Session Manager

Note:

Do not use the same Session Manager instance for **Session Manager 1** and **Session Manager 2**.

Before you begin

Verify that you have added Session Manager instances and peer SIP entities to associate with the Failover Group. You must administer failover ports for each Session Manager instance that is a member of a Failover Group. You must administer one port per supported transport type to ensure call preservation flows.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Network Configuration** > **Failover Groups**.
2. Click **Add**.
3. On the Add Failover Group page, enter the required information for the Failover Group.
4. Click **Commit**.

   The screen refreshes. The **Session Manager Entity Link Audit** page displays the list of Trusted Entity Links that must be added for ensuring failover service.
5. Click **Commit**.

Related links

Failover Groups Page Field Descriptions on page 469
Add Failover Group Page Field Description on page 470

Add Failover Group Page Field Description

Fields	Description
Group Name	Name of the Failover Group.
Session Manager 1	
Preferred Domain Name	A unique and a fully qualified preferred domain name for the primary Session Manager instance of the Failover Group.
Session Manager Name	Name of the operational Session Manager instance from the drop-down list.
Session Manager 2	
Preferred Domain Name	A unique and a fully qualified preferred domain name for the backup Session Manager instance of the Failover Group.
Session Manager Name	Name of the backup Session Manager instance from the drop-down list. **Note:** You must not select the same Session Manager instance for **Session Manager 1** and **Session Manager 2**.

Button	Description
Commit	Creates a new Failover Group.
Cancel	Cancels the Failover Group creation.

Related links

Adding a new Failover Group in Session Manager on page 469

Editing Failover Group information

You can edit only one Failover Group at a time.

Note:

Do not use the same Session Manager instance for **Session Manager 1** and **Session Manager 2**.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Network Configuration** > **Failover Groups**.
2. Select the Failover Group you need to modify.
3. Click **Edit**.
4. Change the information as required.
5. Click **Commit**.

   The Session Manager Entity Link Audit page display the list of Trusted Entity Links that must be added for ensuring failover service.
6. Click **Commit**.

Related links

Failover Groups Page Field Descriptions on page 469

Deleting a Failover Group from Session Manager

You can delete more than one Failover Group.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Network Configuration** > **Failover Groups**.
2. Select the Failover Group or Groups from the list you want to delete.
3. On the delete confirmation notice, click **OK**.
4. Click **Delete**.
5. Click **Refresh** to refresh the data.

Related links

Failover Groups Page Field Descriptions on page 469

Managing peer SIP entities for Failover Group

This section describes the basic steps for managing peer SIP entities associated with the respective Failover Group. You can add or remove one or more peer SIP entities within the Failover Group.

When adding SIP entities in a Failover Group, the following display criteria applies:

- One peer SIP entity can be associated with only one Failover Group. When you need to add peer SIP entities, the system displays only those entities that are not associated to any other Failover Group.
- Entities of type Session Manager are not displayed.

Manage Peer SIP Entities Page Field Descriptions

Name	Description
Name	Name of the peer SIP entity.
Address	IP address or FQDN of the peer SIP entity.
Type	SIP entity type.
Location	Location information of the peer SIP entity.

Button	Description
Add	Add the selected peer SIP entities to the Failover Group.
Remove	Remove the selected peer SIP entity from the Failover Group.
Remove All	Remove all the peer SIP entities from the Failover Group.

Related links

Adding peer SIP entities to a Failover Group on page 472
Removing peer SIP entities from Failover Groups on page 474

Adding peer SIP entities to a Failover Group

Session Manager automatically runs an audit process to ensure the existence of entity links between Session Manager instances and the associated peer SIP entities. Based on the audit process:

- If there are no Entity Links between the peer SIP entity and either of the Session Manager instances in the Failover Group, the system displays an error message that the Entity Links must be added in order to perform the operation.
- If there is an Entity Link between the SIP entity (for TCP or TLS) and only one of the Failover Group Session Manager instances, the system displays a message that a trusted Entity Link will be added between the SIP Entity and the other Session Manager before the operation can be completed.

- If none of the Entity Links between the SIP Entity and Failover Group Session Manager instances are trusted or do not use the Failover listen port of Session Manager as the Session Manager listen port, the system displays a message that these Entity Links will be updated before the operation can be completed.

Before you begin

Before starting this procedure:

1. Verify the peer SIP entities exist.
2. Administer entity links between the peer SIP entities and both Session Manager instances in the Failover Group.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Network Configuration** > **Failover Groups**.
2. Select the Failover Group to which you want to add peer SIP entites.
3. Click **Manage Peer Entities**.
4. Click **Add** to view the list of all of the previously administered SIP entities.
5. On the Add Peer SIP Entities page, select the peer SIP entity or entities you want to add to the Failover Group.
6. Click **Add Selected** for associating the selected peer SIP entities with the Failover Group.

Related links

Failover Groups Page Field Descriptions on page 469
Manage Peer SIP Entities Page Field Descriptions on page 472
Add Peer SIP Entities Page Field Descriptions on page 473

Add Peer SIP Entities Page Field Descriptions

Name	Description
Name	Name of the peer SIP entity.
Address	IP address or FQDN of the peer SIP entity.
Type	SIP entity type.
Location	Location information of the peer SIP entity.

Button	Description
Add Selected	Add the selected peer SIP entity or entities to the Failover Group.
Cancel	Cancel the changes.

Related links

Adding peer SIP entities to a Failover Group on page 472

Removing peer SIP entities from Failover Groups

Remove one or more peer SIP entities.

Note:

You must select at least one peer SIP entity to activate the **Remove** and **Remove All** buttons.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Network Configuration** > **Failover Groups**.
2. Select the appropriate Failover Group from the list.
3. Click **Manage Peer Entities**.
4. Do one of the following:
   - Select the peer SIP entity or entities you want to remove and click **Remove**.
   - Click **Remove All** to remove all the peer SIP entities simultaneously.
5. Click **Delete** on the confirmation page.
6. Click **Refresh** to refresh the data.

Related links

Failover Groups Page Field Descriptions on page 469
Manage Peer SIP Entities Page Field Descriptions on page 472

Rules for working with Failover groups

Use the following best practices while working with Failover groups:

- Refresh the page before any further operations for Failover groups, such as add new failover group, edit failover groups, and managing peers.
- Do not add two SIP entities as primary or secondary with different IP address families as part of a single failover group.
- In a failover group if one Session Manager has IP address family set to Both, all related entity links must be established with the IP address family of another Session Manager instance's SIP entity.
- You cannot add two Session Managers with different IP address families as primary and secondary SM in single failover group.
- Existing rules with different combinations of IP address families also apply while creating entity links between SIP entities which are part of failover groups.

Local Host Name Resolution

Session Manager can locally resolve host names into an ordered set of IP address, port, and transport tuples and assigns priority and weights to each tuple. Local Hostname Resolution is only

applied to host names provisioned by the administrator and overrides normal DNS resolution. For example, if Session Manager is attempting to resolve nj.proxy.avaya.com, and the host name is provisioned as a local host name, Session Manager will skip the DNS resolution and instead determine the request target using the tuples for nj.proxy.avaya.com.

To route a SIP INVITE, Session Manager needs the IP addresses corresponding to the Fully Qualified Domain Name (FQDN) in the INVITE. To resolve a host name by replacing it with its IP address, Session Manager checks for the host name on the local network. If the host name cannot be resolved through broadcasting on the local network, Session Manager searches for the host name in the host names file or by querying the DNS server that maintains the host name to IP address mapping.

Note:

The IP address field supports IPv6 addresses if the global settings page has the **Enable IPv6** field selected.

Resolving a local host name

About this task

You can import or export an XML Schema instance file containing Local Host Name entries using the **More Actions** menu on the Local Host Name Resolution page.

Procedure

1. Verify that at least one entity link has been defined for each FQDN and Transport entry.
2. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Network Configuration** > **Local Host Name Resolution**.
3. Click **New**.
4. On the New Local Host Name Entries page, type a maximum of ten host information.
   a. In **Host Name (FQDN)**, type the Fully Qualified Domain Name or IP address of the host.

      The host name entries override the information provided by DNS.
   b. In **IP Address**, type the IP Address that is mapped to the host name.

      A host can be mapped to more than one IP addresses and each of these mappings are a separate entry.
   c. In **Port**, type the port that the host must use for routing the particular IP address.
   d. In **Priority**, type the value for the priority.

      If there are multiple IP address entries for a given host, Session Manager tries the administered IP addresses in the order of the priority. The lowest integer value indicates the highest priority.
   e. In **Weight**, type the value for the weight.

      If there are multiple IP address entries for a given host, and if some entries have the same priority, then for each priority level, the Session Manager chooses a host according to the specified weights.

f. In **Transport**, select the transport protocol for routing.

The default protocol is **TLS**.

5. Click **Commit**.

Related links

Local Host Name Resolution page field descriptions on page 479
Local Host Name Entries page field descriptions on page 480

Viewing import job status

View the job status of importing Local Host Name Resolution entries since the last restart of System Manager.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Network Configuration** > **Local Host Name Resolution**.
2. Under the Background Job Status section, you can view the status of all background import jobs since the last restart of System Manager.

Related links

Local Host Name Resolution page field descriptions on page 479

Viewing failed job entries

View the list of **Local Host Name Resolution** entries that failed to import and the reason for the failure.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Network Configuration** > **Local Host Name Resolution**.
2. Under the Background Job Status section, select a failed import job.
3. Click **View Failures**.

   The **Local Host Name Entries** page displays the list of Local Host Name Resolution entries that failed to import during the selected import job process.
4. Click **Return to View All Entries** to return to the normal view mode.

Related links

Local Host Name Resolution page field descriptions on page 479

Stopping import jobs

Stop current import jobs that are running in the background.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Network Configuration** > **Local Host Name Resolution**.

2. Under the Background Job Status section, select a running import job.
3. Click **Stop Job**.

Related links

Local Host Name Resolution page field descriptions on page 479

Local Host Name Schema

Example

The format of the JAXB-compliant XSD schema of the XML files used by the Local Host Name Import and Export feature is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            xmlns:jxb="http://java.sun.com/xml/ns/jaxb"
            jxb:version="2.0">

<xsd:annotation>
  <xsd:documentation xml:lang="en">
    XML schema definition for 'Local Host Name Resolution' entries.

    Copyright Avaya Inc., All Rights Reserved
    THIS IS UNPUBLISHED PROPRIETARY SOURCE CODE OF AVAYA INC
    The copyright notice above does not evidence any
    actual or intended publication of such source code.
    Some third-party source code components may have been modified from
    their original versions by Avaya Inc.
    The modifications are Copyright Avaya Inc., All Rights Reserved.
  </xsd:documentation>
</xsd:annotation>

<xsd:element name="LocalHostNameEntries" type="LocalHostNameEntryListType"/>

<xsd:complexType name="LocalHostNameEntryListType">
        <xsd:sequence>
                <xsd:element name="LocalHostNameEntry" type="LocalHostNameEntryType"
                                    maxOccurs="unbounded"/>
        </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="LocalHostNameEntryType">
  <xsd:sequence>
    <xsd:element name="hostName" type="hostNameType"/>
    <xsd:element name="ipAddress" type="ipAddressType"/>
    <xsd:element name="port" type="portType"/>
    <xsd:element name="priority" type="priorityType"/>
    <xsd:element name="weight" type="weightType"/>
    <xsd:element name="transport" type="transportType"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:simpleType name="hostNameType">
  <xsd:restriction base="xsd:string">
    <xsd:minLength  value="1"/>
    <xsd:maxLength  value="255"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="ipAddressType">
  <xsd:restriction base="xsd:string">
    <xsd:minLength  value="7"/>
```

```
    <xsd:maxLength  value="15"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="portType">
  <xsd:restriction base="xsd:int">
    <xsd:minInclusive value="0"/>
    <xsd:maxInclusive value="65535"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="priorityType">
  <xsd:restriction base="xsd:int">
    <xsd:minInclusive value="0"/>
    <xsd:maxInclusive value="2147483647"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="weightType">
  <xsd:restriction base="xsd:int">
    <xsd:minInclusive value="0"/>
    <xsd:maxInclusive value="100"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="transportType">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="TLS"/>
    <xsd:enumeration value="TCP"/>
    <xsd:enumeration value="UDP"/>
  </xsd:restriction>
</xsd:simpleType>

</xsd:schema>
```

Example

The following is a sample XML Schema :

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<LocalHostNameEntries>
        <LocalHostNameEntry>
                <hostName>www.domain1.com</hostName>
                <ipAddress>192.168.1.100</ipAddress>
                <port>1024</port>
                <priority>900</priority>
                <weight>50</weight>
                <transport>TLS</transport>
        </LocalHostNameEntry>
        <LocalHostNameEntry>
                <hostName>www.domain2.com</hostName>
                <ipAddress>192.168.1.101</ipAddress>
                <port>1024</port>
                <priority>600</priority>
                <weight>25</weight>
                <transport>TCP</transport>
        </LocalHostNameEntry>
</LocalHostNameEntries>
```

Local Host Name Resolution page field descriptions

Local Host Name Entries

Name	Description
Host Name (FQDN)	Fully Qualified Domain Name of the host. The host name entries override the information provided by DNS. You can add a maximum of ten entries on a page.
IP address	IP address to which the host name is mapped. A host can be mapped to more than one IP addresses and each of these mappings are a separate entry. The host name supports the following IP addresses: • IPv4 address • IPv6 address **Note:** You can enter IPv6 addresses only if the **Enable IPv6** option on the Global Settings page is selected.
Port	Port number that the host uses for routing with the particular IP address.
Priority	If there are multiple IP address entries for a given host, the Session Manager tries the administered IP addresses in the order of the priority. The lowest integer value indicates the highest priority.
Weight	If there are multiple IP address entries for a given host, and if some entries have the same priority, the Session Manager chooses a host according to the specified weights for each priority level.
Transport	The transport protocol to use for routing. The options are: • TLS • TCP • UDP The default protocol is TLS.

Button	Description
New	Add a new local host.
Edit	Modify the selected local host.
Delete	Delete the selected local hosts.

Table continues…

Button	Description
More Actions > **Import Local Host Name Entries**	Import or upload an XML Schema instance file containing a list of Local Host Name entries to add to the Local Host Name resolution table.
More Actions > **Export Local Host Name Entries**	Export (download) an XML Schema instance file containing a list of Local Host Name entries currently in the Local Host Name resolution table.
More Actions > **Get Local Host Name Schema**	Retrieve the XML Schema for the current version of the Session Manager release. You can use the XML schema format as a template for creating a new XML schema instance file for import purposes.

Background Job Status

Name	Description
Start Time	Time the import job process started.
Status	State of the import job.
Percent Completed	Percentage of import job process completion.
Total Entries to Process	Total number of Local Host Name Resolution entries to be imported.
Failed Entries	Number of Local Host Name Resolution entries that failed to be imported.
Last Updated	Time of the last import job process.
Job Name	Name of the import job.

Button	Description
View Failures	View the failed Local Host Name Resolution entries for the selected failed import job.
Stop Job	Stop the selected import job running in background.

Related links

[Resolving a local host name](#) on page 475
[Viewing import job status](#) on page 476
[Viewing failed job entries](#) on page 476
[Stopping import jobs](#) on page 476

Local Host Name Entries page field descriptions

The fields apply to the following pages:

- New Local Host Name Entries
- Edit Local host Name Entries

Name	Description
Host Name (FQDN)	Fully Qualified Domain Name of the host. The host name entries override the information provided by DNS. You can add a maximum of ten entries on a page.

Table continues…

Name	Description
IP address	IP address to which the host name is mapped. A host can be mapped to more than one IP addresses and each of these mappings are a separate entry. The host name supports the following IP addresses: • IPv4 address • IPv6 address **Note:** You can enter IPv6 addresses only if the **Enable IPv6** option on the Global Settings page is selected.
Port	Port number that the host uses for routing with the particular IP address.
Priority	If there are multiple IP address entries for a given host, the Session Manager tries the administered IP addresses in the order of the priority. The lowest integer value indicates the highest priority.
Weight	If there are multiple IP address entries for a given host, and if some entries have the same priority, the Session Manager chooses a host according to the specified weights for each priority level.
Transport	The transport protocol to use for routing. The options are: • TLS • TCP • UDP The default protocol is TLS.

Button	Description
Cancel	Cancel the operation.
Commit	Save the changes.

Related links

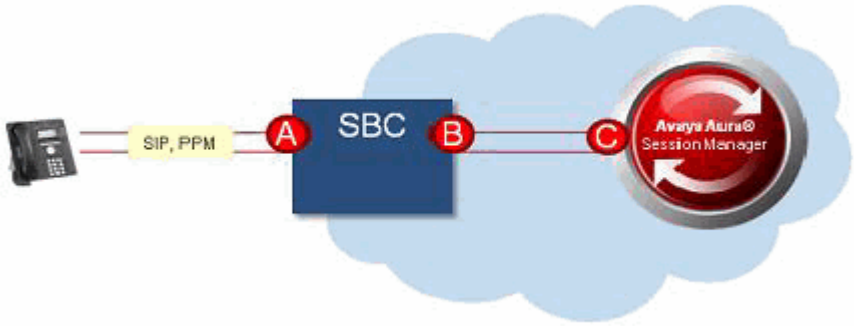
Resolving a local host name on page 475

Remote Access

Enterprises or Hosted Communication Solution Providers can use the Session Manager Remote Access feature to provide fully functional Avaya communication services to a remote user over the public Internet without VPN connectivity.

Reference configuration

A remote endpoint can use a Session Border Controller (SBC) to access a Session Manager deployed in the enterprise network. Remote users can connect over the Internet to the public interface of the SBC, which is at the edge of the enterprise network.



- Reference point A indicates the external, public facing IP address on the SBC.
- Reference point B indicates the internal facing IP address and port on the SBC.
- Reference point C indicates the IP address of Session Manager.

For the list of supported endpoints, see *Avaya Aura® Session Manager Overview and Specification*.

The IP address field for Remote access supports IPv6 addresses if the global settings page has the **Enable IPv6** field selected.

Creating a Remote Access Configuration

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Network Configuration** > **Remote Access**.
2. Click **New**.
3. In the **Name** field, enter a SIP Proxy name.
4. In the **Note** field, enter a note about the SIP Proxy.
5. To add a new SIP Proxy mapping with Session Manager:
   a. In the **SIP Proxy Mapping** table, click **New**.
   b. Enter the **SIP Proxy Public Address** associated with the Session Manager.
6. To add a new SIP Proxy Private IP address:
   a. In the **SIP Proxy Private IP Addresses** table, click **New**.
   b. Enter the private IP address of the SIP Proxy in the enterprise.
   c. Select the **Securable** check box to mark SBC and remote workers as securable.
7. Click **Add**.

Related links

Remote Access page field descriptions on page 485
Remote Access Configuration page field descriptions on page 485

Modifying a Remote Access configuration

You can edit only one Remote Access configuration at one time.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Network Configuration** > **Remote Access**.
2. Select the Remote Access configuration you need to modify.
3. Click **Edit**.
4. Modify the information as required.
5. Click **Commit**.

Related links

Remote Access page field descriptions on page 485

Deleting Remote Access configurations

You can delete more than one Remote Access Configurations simultaneously.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Network Configuration** > **Remote Access**.
2. Select the Remote Access configurations that you want to delete.
3. Click **Delete**.
4. Click **Delete** on the confirmation page.

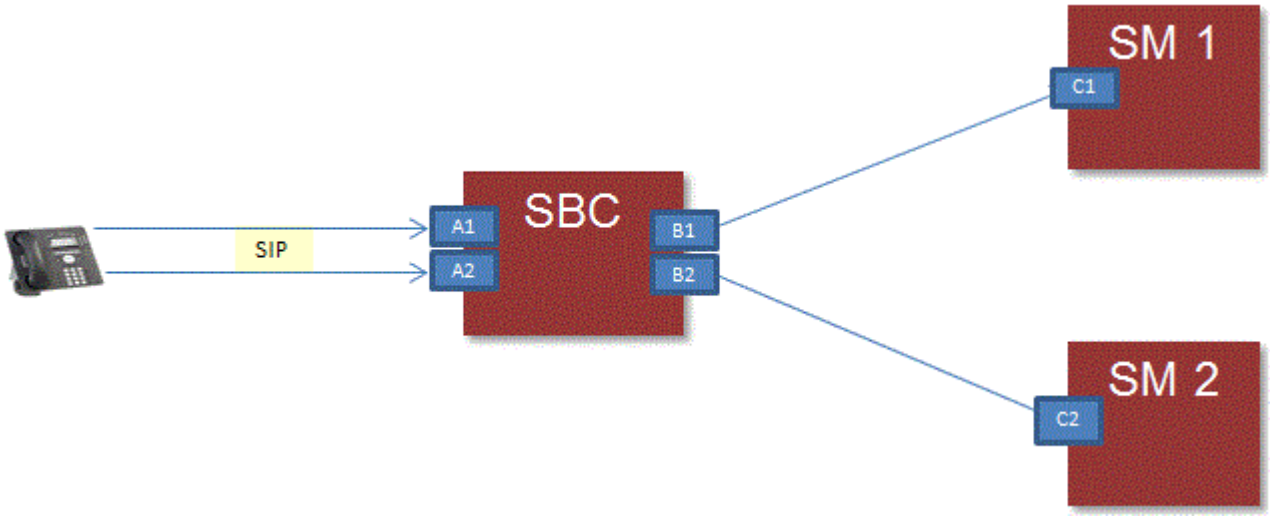
Related links

Remote Access page field descriptions on page 485

Configuring SIP core redundancy

About this task

You can configure Remote Worker solution with multiple core Session Manager instances for added redundancy and resiliency of the Session Manager connection from the endpoint device.



For configuring the core redundancy solution,

1. Configure multiple external facing interfaces, such as *reference point A1* and *reference point A2*, for each SBC.
2. Associate the *reference point A1, A2* with distinct Session Manager instances (SM1 and SM2 with *reference point C1 and C2* respectively) in order to enable the registered endpoints to failover in the case of a loss of connection to the Session Manager.
3. Configure the SIP Private Address (*reference point B1* and *reference point B2*) for the SBC.

The remote endpoint simultaneously registers with:

- core Session Manager (SM1) through *reference point A1*
- core Session Manager (SM2) through *reference point A2*

The SBC in the Remote Worker configuration proxies addresses in both directions. Session Manager interprets all communication, from remote endpoints that traverse the SBC, as having an SBC address (reference point B1 or B2). The remote endpoints interpret Session Manager as having the public address of the SBC (*reference point A1 or A2*).

Where,

- SIP Proxy Public Address (*reference point A*) is the Public IP address of the enterprise SBC.
- Session Manager (*reference point C*) is the IP address of the selected Session Manager instance.
- SIP Private Address (*reference point B*) is the Private IP address of the enterprise SBC.

When SM1 fails or connection to SM1 is lost, the registered SM2 instance can serve the registered endpoints.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Network Configuration** > **Remote Access**.
2. Click **New**.

3. Enter the value of SIP Proxy Private IP Address as *reference point B1* and *reference point B2*.
4. To add a new SIP Proxy mapping with Session Manager, in the SIP Proxy Mapping table, click **New** and enter the required information.

   This step creates a new row in the SIP Proxy Mapping table where Reference point A (A1) and Reference point C (C1) are mapped. Add a second set of addresses if needed to support dual registration to create a SIP Proxy Mapping for Reference point A (A2) and Reference point C (C2). Both SIP Proxy Public IP addresses must be in the phone settings file.
5. To add a new SIP Proxy Private IP address, in the SIP Proxy Private IP Addresses table, click **New** and enter the required information.
6. Click **Commit**.

Verifying user registration details

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **System Status** > **User Registrations**.
2. Verify the user registration status under the **Remote Office** column of the User Registrations page.
3. Click **Refresh** to display the latest user registration summary results.

Remote Access page field descriptions

Button	Description
New	Create a new Remote Access configuration.
Edit	Modify an existing Remote Access configuration.
Delete	Delete the selected Remote Access configuration.

Name	Description
Remote Access Configuration Name	The name of the administered Remote Access configuration.

Related links

Creating a Remote Access Configuration on page 482
Modifying a Remote Access configuration on page 483
Deleting Remote Access configurations on page 483

Remote Access Configuration page field descriptions

Name	Description
Name	Name of the Remote Access configuration.

Table continues…

Name	Description
Note	Optional information of the Remote Access configuration.
Click to open Remote Access Reference Map	The map displays the reference configuration of the remote access solution. • Reference Point A indicates the external, public-facing IP address of the SBC. • Reference Point B indicates the internal facing IP address and port of the SBC. • Reference Point C indicates the IP address of the Session Manager.

SIP Proxy Mapping Table

Button	Description
New	Add a new row in the SIP Proxy Mapping table.
Delete	Delete the selected row in the SIP Proxy Mapping table.

Name	Description
SIP Proxy Public Address (Reference A)	The Public IP address of the enterprise SBC.
Session Manager (Reference C)	The selected Session Manager instance. If on the Session Manager Administration page, the **Enable Military Support** field is selected, the **Session Manager (Reference C)** screen displays branch Session Manager instances along with Session Manager instances.

Table continues…

Name	Description
IP Address Family	The IP address family of the Session Manager instance. Depending on the Session Manager instance the IP address family type is selected as following: • If Session Manager [Reference C] supports IPv4 only, the valid value for the IP address family type is IPv4. • If Session Manager [Reference C] supports IPv6 only, the valid value for the IP address family type is IPv6. • If Session Manager [Reference C] supports IPv6 and IPv4 (both), the valid values for the IP address family type is IPv6 and IPv4 and not both. As part of validation, the following is true: • If Reference C entries in mapping table contains only IPv4 family, then in private addresses table, only IPv4 addresses are allowed in Reference B field. • If reference C entries in mapping table contains only IPv6 family, then in private addresses table, only IPv6 addresses are allowed in Reference B field. • If Reference C entries in mapping table are of mixed IPv4 and IPv6 family types, then in Reference B field both IPv4 and IPv6 address are allowed.

SIP Proxy Private IP Addresses

Button	Description
New	Add a new row in the SIP Proxy Private IP Addresses table.
Delete	Delete the selected row in the SIP Proxy Private IP Addresses table.

Name	Description
SIP Private Address (Reference B)	The Private IP address of the enterprise SBC.
SBC Type	The type of SBC used in the Remote Access configuration.
Securable	Mark SBC and remote workers as securable.
Note	Optional information about the SIP Proxy Private IP address.

Button	Description
Add	Add the Remote Access configuration.
Cancel	Cancel the changes for the Remote Access configuration.

Related links

Creating a Remote Access Configuration on page 482

SIP Firewall

The SIP Firewall controls incoming and outgoing SIP traffic into the Session Manager server based on a set of rules.

The SIP Firewall configuration consists of a collection of Rule Sets. The administrator assigns the SIP Firewall Rule Sets to Session Manager and Branch Session Manager instances in the network. The SIP Firewall routes or drops SIP messages based on the sender, location, and other criteria defined in the Rule Sets.

The IP address field for SIP firewall supports IPv6 addresses if the global settings page has the **Enable IPv6** field selected.

SIP Firewall default Rule Set

A default SIP Firewall Rule Set for the SIP Firewall is automatically provided when Session Manager is installed. The system preserves the default Rule Sets for different Session Manager releases. You can rollback to an earlier release of an Avaya-provided Rule Set by assigning earlier Rule Set versions.

After a system upgrade, the default Rule Sets associated with Session Manager and Branch Session Manager are automatically updated with the latest versions of the Rule Sets. Rule Sets created and assigned by customers remain unaffected after a system upgrade.

Note:

The installation software will only upgrade automatically to the new default rule set if the Session Manager or Branch Session Manager currently has a default rule set assigned. The default rule set s not upgraded when a customer-modified rule set is in place.

SIP Firewall Rule Set

Rules:

SIP Firewall rules can generate log events that are monitored by the serviceability agents. You must enable logging in each SIP Firewall rule to have a record of the actions taken by the SIP Firewall.

Note:

SIP Firewall log messages are rate-limited. Each rule can log a maximum of one log message per second. Rate-limiting of log messages provides protection from flooding the logging system due to a misconfiguration of the SIP Firewall rules.

You can apply SIP filtering and Denial of Service protection to:

- A SIP gateway or proxy connections (SIP Multiplexed connection or trunk). For example, a SIP Firewall rule can set a rate limit on the number of INVITE messages from a specific user without affecting the traffic from other users in that gateway.
- A SIP TLS connection. The Session Manager Security Module decrypts all the incoming SIP TLS packets before any filtering rules are applied by the SIP Firewall.

For more information about the default SIP Firewall rules, see *Avaya Aura® Session Manager Security Design*.

Blacklist

The SIP Blacklist blocks any known bad SIP elements. The SIP Firewall drops any SIP packet that matches a rule in the Blacklist.

Whitelist

The whitelist contains a list of known SIP elements. If a SIP packet matches a whitelist rule, the SIP Firewall:

- Allows the SIP packets unconditionally.
- Does not apply any other filtering rules.

Rule precedence and traversal

The SIP Firewall is a packet-based filtering engine. If a packet matches a rule, the SIP Firewall stops the rule traversal and either permits or drops the packet according to the rule action. The traversal process does not apply to rules defined with an action type of **None**.

The order of precedence for using the rules is:

1. Blacklist
2. Whitelist
3. Rules

Each list can contain more than one rule. The Session Manager traverses the rules from top to bottom within the lists.

Deep inspection filtering

SIP Firewall rules provide the following filters for deep inspection:

- SIP Layer content
- IP and Transport layer parameters such as IP address, protocol, and port.

You can combine both SIP Layer content and IP transport layer parameters in a single Firewall rule. For example, a SIP Firewall rule can limit the high rate of INVITE packets coming from a remote IP address.

Denial of Service protection

The SIP Firewall provides protection from the Denial of Service (DoS) attacks such as:

- Flood Protection from a specified source.
- Advanced Flood Protection. Define a rule to detect or mitigate flood attacks within the live SIP stream without knowing the flood source in advance. You do not need to know the host that is causing the flood when you configure the rule. A high-performance database tracks all matching messages.
- Rate-Limiting. Configure a **Rate Limit** action to limit the number of SIP packets that are forwarded within a specified period.
- Rate-Blocking. Configure a **Rate Block** action to block an offending SIP source when the traffic reaches a specified threshold within a given period. Traffic is then blocked until the configured timeout expires.
- Signature Detection. Configure a rule to perform signature detection and drop packets that match the signature. The rule can support both simple and regular-expression string searching across either the entire SIP header region of the message or across the full message (headers and body).

SIP Firewall status

You can view the status of the SIP Firewalls for each Session Manager and Branch Session Manager deployed across the network. Additionally, you can perform the following operations:

- View the assignment details of specific rule sets for each Session Manager and Branch Session Manager.
- View the SIP Firewall processing status for each Session Manager and Branch Session Manager.
- Perform an audit of the Session Manager Rule Set assignments.
- Reset the processing counters of the selected Session Manager and Branch Session Manager instances.

Related links

Security Module Status page field descriptions on page 560

Creating a new Rule Set

You can define up to 50 rules on the Rules page.

You can create up to 200 blacklist or whitelist rules.

If you create a new blacklist or whitelist rule, you must click **Commit** on the blacklist or whitelist page, then click **Commit** again on the Rule page to save the configuration information for Session Manager.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Network Configuration** > **SIP Firewall**.
2. Click **New**.
3. Enter the name and description of the new Rule Set.
4. On the Rules tab, select or clear the **Enabled** check box to enable or disable all the rules.
5. Do one of the following:
   - To create a new rule, click **New** and enter the required information.
   - To modify a rule, select a rule and click **Edit**.
   - To delete a rule, select a rule and click **Delete**.
   - To move the rule in the order, select a rule from the list and click **Up** or **Down**.
6. On the Blacklist tab:
   a. Select **Enabled** to drop messages from untrusted hosts.
   b. To delete a blacklist rule, select the rule and click **Delete**.
   c. To create a new rule to drop messages from untrusted hosts, click **New**, enter the required information, and click **Commit**.
7. On the Whitelist tab:
   a. Select **Enabled** to allow messages from trusted hosts to bypass the SIP firewall.
   b. To delete a whitelist rule, select the rule and click **Delete**.
   c. To create a new rule to allow messages from trusted hosts, click **New**, enter the required information, and click **Commit**.
8. Click **Commit**.

Related links

SIP Firewall Configuration page field descriptions on page 503

Creating a new SIP Firewall rule

To create the new rule and save the configuration to Session Manager, you must click **Commit** on the Rule Set page. The Rule Set page appears after you click **Done** on the Rule page.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Network Configuration** > **SIP Firewall**.
2. Click **New**.
3. Type the name of the new rule in the **Name** field.
4. Type a description of the rule in the **Description** field.

5. Under the Rules tab, click **New**.
6. Enter or change the information as appropriate on the Rule page.
7. Click **Done**.
8. On the Rule Set page, click **Commit** to save the new rule and send the configuration information to Session Manager.

Creating a duplicate Rule Set

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Network Configuration** > **SIP Firewall**.
2. Select the Rule Set you want to duplicate.
3. Click **Duplicate**.
4. Type a name and description for the duplicate Rule Set.
5. Modify the appropriate information of the duplicate Rule Set.
6. Click **Commit**.

Related links

SIP Firewall Configuration page field descriptions on page 503

Modifying a Rule Set

You cannot modify a Default Rule Set.

After you modify a Rule Set, the system updates the associated Session Manager and Branch Session Manager instances with the changes.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Network Configuration** > **SIP Firewall**.
2. Select the Rule Set you want to modify.
3. Click **Edit**.
4. Modify the appropriate information of the Rule Set.
5. Click **Commit**.

Related links

SIP Firewall Configuration page field descriptions on page 503

Viewing a Rule Set

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Network Configuration** > **SIP Firewall**.

2. Select the Rule Set you want to view.
3. Click **View**.
4. Click **Done** to return to the SIP Firewall Configuration page.

Related links

SIP Firewall Configuration page field descriptions on page 503

Deleting a Rule Set

You cannot delete a default Rule Set.

Procedure

1. If you are deleting an assigned Rule Set, you must first reassign all the associated Session Manager and Branch Session Manager instances to another Rule Set.
2. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Network Configuration** > **SIP Firewall**.
3. Select the Rule Set you want to delete.
4. Click **Delete**.
5. Click **Delete** on the confirmation page.

Related links

SIP Firewall Configuration page field descriptions on page 503

Assigning Rule Sets to all core Session Manager and Branch Session Manager instances

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Network Configuration** > **SIP Firewall**.
2. Select the Rule Set you want to assign to all core Session Manager and Branch Session Manager instances.
3. Click **Assign** > **Assign All (Core SMs and BSMs)**.
4. Click **Confirm**.

Related links

SIP Firewall Configuration page field descriptions on page 503

Assigning Rule Sets to all core Session Manager instances

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Network Configuration** > **SIP Firewall**.
2. Select a Rule Set for assigning to all core Session Manager instances.
3. Click **Assign** > **Assign All Core SMs**.

4. Click **Confirm**.

Related links

SIP Firewall Configuration page field descriptions on page 503

Assigning Rule Sets to all Branch Session Manager instances

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Network Configuration** > **SIP Firewall**.
2. Select the Rule Set that you want to assign to all Branch Session Manager instances.
3. Click **Assign** > **Assign All BSMs**.
4. Click **Confirm**.

Related links

SIP Firewall Configuration page field descriptions on page 503

Assigning Rule Sets to selected Session Manager and Branch Session Manager instances

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Network Configuration** > **SIP Firewall**.
2. Select the rule set that you want to assign to selected Session Manager and Branch Session Manager instances.
3. Click **Assign** > **Select SMs and BSMs for assignment**.
4. On the Assign Rule Set page, click the Session Manager and Branch Session Manager instances.
5. Click **Commit**.

Related links

SIP Firewall Configuration page field descriptions on page 503

Viewing Rule Set assignment for Session Manager and Branch Session Manager instances

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Network Configuration** > **SIP Firewall**.
2. Select the Rule Set you want to view.
3. Click **Assign** > **View Assigned SMs and BSMs**.
4. Click **Done** to return to the SIP Firewall Configuration page.

Related links

SIP Firewall Configuration page field descriptions on page 503

Viewing SIP Firewall status

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Network Configuration** > **SIP Firewall**.
2. Click **Status** to display the SIP Firewall Status page.
3. To view the rules associated with the Session Manager instance, select the Session Manager and click **Show**.

Related links

SIP Firewall Configuration page field descriptions on page 503
SIP Firewall Status page field descriptions on page 504

Auditing SIP Firewall configuration

You can perform a periodic audit of the Firewall configuration to verify the operation of the SIP Firewall. The audit operation checks for Rule Set upgrades and imports the latest default Rule Sets. The system also performs the audit operation automatically every 5 minutes.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Network Configuration** > **SIP Firewall**.
2. Click **Status**.

   The SIP Firewall Configuration page displays the list of Session Manager and Branch Session Manager instances.
3. Click **Audit**.

   The Rule Set Audit and Repair Status page displays the processing results for the Session Manager and Branch Session Manager instances.
4. Click **Done**.

Rule Set page field descriptions

Name	Description
Name	The name of the Rule Set.
Description	The description of the Rule Set.
SM Type	Session Manager or Branch Session Manager.

Button	Description
Commit	Save and apply the changes.
Cancel	Cancel the changes.

Rules tab

Name	Description
Enabled	Enable or disable the rule.
Name	The name of the SIP Firewall rule. The name can have a maximum of 80 characters.
Action Type	The action type for the rule: • **None**: No specific action required. Use this action when you want to only generate a log or alarm for matching SIP traffic. Rule traversal continues when a SIP packet matches a rule with the **None** action. • **Permit**: If the rule conditions are met, allow the SIP message to pass through the SIP Firewall. If the rule conditions are not met, the SIP message is not affected or dropped. • **Drop**: If the rule conditions are met, drop the SIP message. • **Rate Block**: If the packets matching the rule exceed a certain count in a certain period, block the matching SIP packets for the duration of timeout. You define the timeout period using the Threshold parameters. • **Rate Limit**: If the packets matching the rule exceed a certain count in a certain period, drop the additional matching SIP packets for the duration of the period. You define the time period using the Threshold parameters.
Log Type	Specify if you want to generate a log, send an alarm, or take no action.
Log Message	The message that will be logged when the **Log Type** is **Yes** or **Alarm**.

Button	Description
Enabled	Enable or disable all rules in the Firewall Rule Set.
New	Define a new SIP Firewall rule.
Edit	Edit the selected SIP Firewall rule.
Delete	Delete the selected rule or rules.
Up	Move a selected rule up in the list.
Down	Move a selected rule down in the list.

Blacklist tab

Name	Description
Enabled	Enable or disable dropping of messages from untrusted hosts.
Key	Key for filtering messages.
Value	The value of the Key. The **Value** can be one of the following: • **Remote IP address**: IP address of the host from where the messages are sent. • **CONTACT**: The string value to search in the **Contact** SIP Header in the SIP message. The string value can be a complete or partial SIP URI, for example, jdoe@avaya.com for a specific user, or @avaya.com for a domain of users. • **FROM**: The string value to search in the **From** SIP Header in the SIP message. The string value can be a complete or partial SIP URI, for example, jdoe@avaya.com for a specific user, or @avaya.com for a domain of users. When you select **Remote IP Address** in the **Key** field, and select **Enable IPv6**, the **Value** field supports both IPv4 and IPv6 addresses. When you specify an IPv6 address in the **Value** field, you must also specify an IPv6 prefix mask.
IP Address Mask	Subnet mask used for the blacklist operation. This field supports values between 1 and 128 and is mandatory.

Button	Description
New	Create a rule for dropping messages from untrusted hosts.
Delete	Delete the selected Blacklist rule.

Whitelist tab

Name	Description
Enabled	Enable (allow) or disable do not allow) messages from trusted hosts to bypass the SIP Firewall.
Key	Key for filtering messages.

Table continues…

Name	Description
Value	Value of the Key. The **Value** can be one of the following: • **Remote IP address**: IP address of the host from where the messages are sent. • **CONTACT**: The string value to search in the **Contact** SIP Header in the SIP message. The string value can be a complete or partial SIP URI, for example, jdoe@avaya.com for a specific user, or @avaya.com for a domain of users. • **FROM**: The string value to search in the **From** SIP Header in the SIP message. The string value can be a complete or partial SIP URI, for example, jdoe@avaya.com for a specific user, or @avaya.com for a domain of users.
IP Address Mask	Subnet mask used for the whitelist operation.

Button	Description
New	Create a rule for allowing messages from trusted hosts to bypass the SIP Firewall.
Delete	Delete the selected Whitelist rule.

Rule page field descriptions

General

Name	Description
Enabled	Enable or disable the rule.
Name	The name of the SIP Firewall rule. The name can have a maximum of 80 characters.

Table continues…

Name	Description
Action Type	Specify one of the following action types for the rule: • **None**: No specific action required. Use this action when you want to only generate a log or alarm for matching SIP traffic. Rule traversal continues when a SIP packet matches a rule with the **None** action. • **Permit**: If the rule conditions are met, allow the SIP message to pass through the SIP Firewall. If the rule conditions are not met, the SIP message is not affected or dropped. • **Drop**: If the rule conditions are met, drop the SIP message. • **Rate Block**: If the packets matching the rule exceed a certain count in a certain period, block the matching SIP packets for the duration of timeout. You define the timeout period using the Threshold parameters. • **Rate Limit**: If the packets matching the rule exceed a certain count in a certain period, drop the additional matching SIP packets for the duration of the period. You define the time period using the Threshold parameters.
Log Type	Specify if you want to generate a log, send an alarm, or take no action. You must specify a **Log Type** when the **Action Type** is None.
Log Message	The message that will be logged when the **Log Type** is **Yes** or **Alarm**.

IP Layer Match Options

Name	Description
Protocol	The protocol for which the rule is to be used.
Remote IP Address	The options are: • **Any** to use the rule for all IP addresses. • **Specify** to use the rule for a specific IP address.

Table continues…

Name	Description
IP Address	The IP address if you selected **Specify** for **Remote IP Address**. When you select **Specify** in the **Remote IP Address** field, and select **Enable IPv6**, the **IP Address** field supports both IPv4 and IPv6 addresses.
IP Address Mask	Network Mask for the specified IP address. IPv6 supports prefix mask. Valid values for prefix mask, range from 1 to 128. It also supports values in CIDR format such as /64.
Remote Port	The options are: • **Any** • **Specify** a single port. • **Specify Range** for a range of ports.
Start	A single port or the start port for a range. This field appears if you select **Specify** or **Specify Range** for the **Remote Port**.
End	The end port for a range of ports.
Local Port	The options are: • **Any** • **Specify** a single port. • **Specify Range** for a range of ports.
Start	A single port or the start port for a range. This field appears if you select **Specify** or **Specify Range** for the **Remote Port**.
End	The end port for a range of ports.

SIP Layer Match Options

Button	Description
New	Create up to five SIP layer match options for the rule.
Delete	Delete the selected SIP layer match options.

Name	Description
Key Type	The key type that the rule should match. You can add up to five key type match options. Use the logical **AND** to create a search pattern to define more than one match option. • **All SIP Headers:** Search for the Value within all the SIP headers for the SIP packet. • **All SIP Headers/Body:** Search for the Value in the SIP headers and body portions for the SIP packet. • **REQUEST-METHOD, RESPONSE-CODE:** All the remaining entries in the **Key Type** list are SIP headers. This option searches for the Value within the specified SIP header only.
Value Type	Specify whether the key type is a string or a regular expression. You can create regular expressions using the PERL version 5.8 syntax.
Value	Value of the selected key type. The string does not need to be an exact match and can be a subset of the string present in the SIP header being used for the search.

IP/SIP LayerTrack

Name	Description
Track	The option for tracking SIP messages. This field appears only if you have selected either Rate Block or Rate Limit in the Action Type field, or None for the Action Type with Log Type enabled. You cannot use IP/SIP Layer Track with Permit/Drop Actions. This option provides advanced flood tracking in the SIP Firewall. • None: No tracking required • Remote IP address: Tracks messages for a specific IP address of the remote host. • Local Port: Tracks messages for a specific local port • From: Sender of the message • To: Receiver of the message • Contact: Tracks messages for a specific contact. • Request URI: URI of the called party

Threshold

Name	Description
Count (packets)	Threshold for matching packets. The range is 3 to 100000. The default value is 20. You specify this value only for the Rate Block and Rate Limit Action Types.
Period (secs)	Threshold for period for matching packets. The range is 1 to 86400. The default value is 20. You specify this value only for the Rate Block and Rate Limit Action Types.
Timeout (secs)	Action timeout in seconds. The range is 30 to 36000. The default value is 900. Specify this value only for the Rate Block Action Type.

Connection

Name	Description
Connection Type	The connection types are: • **Any :** This is a default option. Session Manager matches the SIP Firewall rule against all incoming SIP Traffic • **SIP UA Connection:** Session Manager matches the SIP Firewall rule against the incoming SIP traffic from entities that are not the Trusted SIP Entity, as defined by the Routing Policy. This option is suitable for creating SIP Firewall filtering rules for SIP telephones that are directly connected to Session Manager. • **NRP SIP Entity:** Session Manager matches the SIP Firewall rule against the incoming SIP traffic from SIP entities. • **NRP Trusted SIP Entity:** Session Manager matches the SIP Firewall rule against the incoming SIP traffic from entities that are marked as Trusted SIP Entity in the Routing Policy. • **NRP Untrusted SIP Entity:** Use this option for entities such as a Session Border Controller (SBC). You can set a firewall rule to monitor traffic coming through an SBC which might have higher thresholds than SIP UA connections.

Button	Description
Commit	Save and apply the changes.
Cancel	Cancel the changes.

SIP Firewall Configuration page field descriptions

Name	Description
Rule Set	The name of the Rule Set.
Type	The name of the Session Manager or Branch Session Manager instance.
Assigned Count	The number of Session Manager and Branch Session Manager instances assigned to a Rule Set.
Avaya Provided	The Rule Set provided by Avaya. The options are: • **Yes**: Provided by Avaya. • **Default:** Provided by Avaya. • **No**: Defined by the customer. During a system upgrade, only the Default Rule Sets are automatically updated.
Description	The Rule Set description.

Button	Description
New	Creates a new SIP Firewall Rule Set.
Duplicate	Duplicates a selected SIP Firewall Rule Set to a new Rule Set.
Edit	Edits a selected SIP Firewall Rule Set.
View	Views a selected SIP Firewall Rule Set.
Assign All (Core SMs and BSMs)	Assigns a SIP Firewall Rule Set to all core Session Manager and Branch Session Manager instances.
Assign All Core SMs	Assigns a SIP Firewall Rule Set to all core Session Manager instances.
Assign All BSMs	Assigns a SIP Firewall Rule Set to all Branch Session Manager instances.
Select SMs and BSMs for assignment	Assigns a SIP Firewall Rule Set to the selected Session Manager or Branch Session Manager instance.
View Assigned SMs and BSMs	Displays a list of Session Manager and Branch Session Manager instances assigned with a selected Rule Set.
Delete	Deletes the selected Rule Set.
Import	Imports a SIP Firewall XML file.
Export	Downloads a SIP Firewall XML file for the selected Rule Set.
Status	Displays the SIP Firewall status for all Session Manager and Branch Session Manager instances.

SIP Firewall Status page field descriptions

Button	Description
Reset	Reset all the processing counters of the selected Session Manager and Branch Session Manager instances to zero, except for the **Loop Detection** counters. This action also resets all the Rule matching counts to zero. **Note:** After a reset operation, the system updates the counts from the last reset time.
Audit	Perform an audit of the Session Manager Rule Set assignments. The Audit process also checks for Rule Set upgrades and imports pending default Rule Sets.
Configure	Navigates to the SIP Firewall Configuration page.

Name	Description
Details	Displays the detailed SIP Firewall processing status for each Rule for the selected Session Manager. The details section displays a **Rule Matching table** with the following columns: • Rule: The name of the rule. • Match: The matched count of the Rule for the selected Session Manager. • Drop: The dropped count of the Rule for the selected Session Manager.
SM	The name of the Session Manager.
Type	The Session Manager type.
Rule Sets	The name of the Rule Set assigned to the Session Manager.
Reset Time	The last reset time of the SIP Firewall processing counts. **Note:** The reset time displays only displays for Session Manager and Branch Session Manager Release 6.3.4 and later.

Table continues…

Name	Description
Processing Counts	Displays the summary of counts for Rules, Whitelist, Blacklist, and Loop Detection. Loop Detection counts do not reset. To view the exact counts, mouse over the **Processing Counts** column. **Note:** The processing counts only display for Session Manager and Branch Session Manager Release 6.3.4 and later.

Related links

Viewing SIP Firewall status on page 495

Device and Location Configuration

Use the Device and Location Configuration page to:

- Configure Avaya terminal settings by terminal or location groups.
- Assign Device Settings Groups to Locations.

Device Settings Groups

Using Device Settings Groups, you can manage some of the configuration data for Avaya terminals. The device settings are associated in groups or in a default group and can be assigned to one or more terminals or locations.

Device Settings Groups of type **Location Groups** can be associated with Locations while Device Settings Groups of type **Terminal Groups** can only be associated with a terminal having a Terminal Group ID. When the terminal is set up for the first time, the terminal is set up with a pre-provisioned group called Default Group. The Default Group provides the global settings across locations and terminals.

A terminal can be individually associated with a set of Device Settings that are downloaded and set according to the following criteria:

- The configuration of a terminal is set as **Default Device Settings** if the terminal:
  - Does not belong to an **Routing Policy Location**
  - Does not belong to the **Network Routing Policy Location** where the terminal is located.
  - Is not associated with a specific set of Personal Profile Manager (PPM) attributes

- The configuration of a terminal is set as the set of attributes defined for a **Routing Policy Location** if the terminal:
  - Is located in that **Routing Policy Location**.
  - Is not individually associated with a specific set of PPM attributes.
- The configuration of a terminal is set as a specific set of PPM attributes if the terminal s individually associated with a set of PPM attributes and the selected set of PPM attributes exists.

Priority ordering of usage of the Device Settings data is as follows:

- Terminal group data – highest priority. This priority is used if a terminal group is configured in the endpoints
- Location based settings. Has priority over default settings
- Default service settings

PPM supports device settings on a per location basis. Session Manager notifies an endpoint when Device Settings modified, including the following settings:

- Timers: Registration, Subscription
- QoS parameters: for Video, Audio and call control
- VLAN ID

Viewing Device Settings Groups

Procedure

On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Device and Location Configuration** > **Device Settings Groups**.

Result

The Device Settings Groups page displays the list of Device Settings Groups.

Related links

Device Settings Groups field descriptions on page 509

Creating a Device Settings Group - Terminal Group

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Device and Location Configuration** > **Device Settings Groups**.
2. Under Terminal Groups, click **New**.
3. Enter the information for the new Terminal Group.
4. Do one of the following:
   a. Click **Restore** to restore the original values.
   b. Click **Cancel** to cancel the changes.

c. Click **Save** to save the changes.

Related links

Device Settings Groups field descriptions on page 509
Device Settings Group - Terminal Group field descriptions on page 517

Modifying a Device Settings Group - Terminal Group

You can modify only one Terminal Device Settings Group at a time.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Device and Location Configuration** > **Device Settings Groups**.
2. Select the appropriate Terminal Group.
3. Click **Edit**.
4. Modify the appropriate information for the Terminal Group.
5. Do one of the following:
   a. Click **Restore** to restore the original values.
   b. Click **Cancel** to cancel the changes.
   c. Click **Save** to save the changes.

Related links

Device Settings Groups field descriptions on page 509
Device Settings Group - Terminal Group field descriptions on page 517

Deleting Device Settings Group - Terminal Group

You cannot delete the default Device Settings Group.

You can delete more than one Terminal Group at the same time.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Device and Location Configuration** > **Device Settings Groups**.
2. Select one or more Terminal Groups.
3. Click **Delete**.

Related links

Device Settings Groups field descriptions on page 509
Device Settings Group - Terminal Group field descriptions on page 517

Creating a Device Settings Group - Location Group

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Device and Location Configuration** > **Device Settings Groups**.
2. Under Location Groups, click **New** .
3. Enter the appropriate information for the Location Group.

   From release 7.1, an IPv6 Settings section is added to administer Signaling and media address family for endpoints.
4. Do one of the following:
   a. Click **Restore** to restore the original values.
   b. Click **Cancel** to cancel the changes.
   c. Click **Save** to save the changes.

Related links

Device Settings Groups field descriptions on page 509
Device Settings Group - Location Group field descriptions on page 513

Modifying a Device Settings Group - Location Group

You can modify only one Location Group at a time.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Device and Location Configuration** > **Device Settings Groups**.
2. Select the appropriate Location Group.
3. Click **Edit**.
4. Modify the information for the Location Group.
5. Do one of the following:
   a. Click **Restore** to restore the original values.
   b. Click **Cancel** to cancel the changes.
   c. Click **Save** to save the changes.

Related links

Device Settings Groups field descriptions on page 509
Device Settings Group - Location Group field descriptions on page 513

Deleting Device Settings Groups - Location Groups

You cannot delete the default Device Settings Group.

You can delete more than one Location Group at the same time.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Device and Location Configuration** > **Device Settings Groups**.
2. Select one or more Location Groups.
3. Click **Delete**.

Related links

Device Settings Groups field descriptions on page 509
Device Settings Group - Location Group field descriptions on page 513

SIP subscriptions

SIP Subscription and Notification requests update connected SIP endpoints on state changes related to services that the endpoints consume. For example, when a new voice message arrives in a mailbox, Session Manager sends a SIP notification request to notify the related endpoints about the arrival of a new voice mail message.

For an endpoint to receive SIP notifications, it first needs to subscribe to the relevant subscription package. Each subscription package is related to a specific service that the network delivers to the endpoint. The SIP endpoints automatically establish all required subscriptions upon logging into the network.

When a subscription to an event package or service, is established, SIP subscription is assigned with a subscription expiration timer. The endpoint continues to receive notifications as long as the expiration timer does not expire. The endpoints automatically refresh any subscriptions before their expiration timer expires. A lower subscription expiration timer generates more SIP traffic related to subscription refresh events. Refreshing a subscription updates the state of the subscription.

Session Manager allows administration of the subscription expiration timer for each type of event package.

Device Settings Groups field descriptions

Button	Description
Default Group	Displays the default Device Settings Group page. You can modify the information on this page.

Terminal Groups

Button	Description
New	Create a new Terminal Group.
Edit	Modify the selected Terminal Group.
Delete	Delete the selected Terminal Group.

Name	Description
Name	Name of the Terminal Group.
Terminal Group Number	A numeric ID for this group. A group ID identifies different phones in the network for easier administration. With the exception of the field Group ID, Group parameters are the same as those for common phone parameters. The Terminal Group Number is a number between 0 and 999.
Description	Optional information regarding the Terminal Group.

Location Groups

Button	Description
New	Create a new Location Group.
Edit	Modify the selected Location Group.
Delete	Delete the selected Location Group.

Name	Description
Name	Name of the Location Group.
Description	Optional information regarding the Location Group.

Related links

Viewing Device Settings Groups on page 506
Creating a Device Settings Group - Location Group on page 508
Modifying a Device Settings Group - Location Group on page 508
Deleting Device Settings Groups - Location Groups on page 508
Creating a Device Settings Group - Terminal Group on page 506
Modifying a Device Settings Group - Terminal Group on page 507
Deleting Device Settings Group - Terminal Group on page 507

Device Settings Group - Default Group field descriptions

General section

Name	Description
Name	Displays **Default Group**.
Description	Displays **Default Group**.
Group Type	The default is **Location Group**.
Terminal Group Number	Non-active field.

Server Timer section

Name	Description
Subscription Expiration Timer (secs)	The length of time in seconds for a SIP server to keep a SIP client as subscribed. The range is 60–86400 seconds.
Registration Expiration Timer (secs)	The length of time in seconds for a SIP server to keep a SIP client as registered. The range is 60–3600 seconds.

Endpoint Timer section

Name	Description
Line Reservation Timer (secs)	Maximum time a SIP server can reserve a SIP line appearance. The range is 30–240 seconds. The default value is 30 seconds.
Reactive Monitoring Interval (secs)	The amount of time a phone should attempt to REGISTER with a proxy server when the proxy server is not reachable or available. The range is 10–3600 seconds. The default is 60 seconds.
Timer B (sec)	The amount of time for a phone to wait before proceeding to another proxy server if the phone does not receive a response to a SIP INVITE. The range is 0 to 32 seconds. 0 disables this feature. The default value is 2.

Maintenance Settings section

Name	Description
IP Address For SNMP Queries	IP address of a server that can query the phone for SNMP messages. The server must have the correct community string. If this field is blank, any server can query the phone.
SNMP Community	SNMP community name. This string is both a challenge and a response for the server specified in the IP addresses for SNMP Queries field and the phone. If a server IP address is specified, both the server and the phone must have the same community name administered. Only alphabetic characters are allowed, and the length cannot exceed 32 characters.

Table continues…

Name	Description
Station Admin Password	Code that an administrator must enter on a SIP phone to log in and administer the phone. Only numeric values are accepted, and the password cannot exceed 32 digits. This is an optional field. **Note:** All End Points except 96x1 with 7.1 firmware use **Station Admin Password** to log in.
Station Access Code	Code that an administrator must enter on a SIP phone to log in and administer the phone. This field accepts numerics, lowercase and uppercase alphabets, and special characters. This is an optional field **Note:** 96x1 phone with 7.1 firmware use **Station Access Code** to log in.
Confirm Station Access Code	Station Access Code retyped for confirmation.
Quick Login Status	Specify whether or not users must enter a password when logging in to the phone. The choices are **Password Entry Required** and **Quick Login Allowed**.

VoIP Monitoring Manager section

Name	Description
IP Address	IP address of the Avaya Voice over IP Monitoring Manager server.
Port	Port used by the Avaya Voice over IP Monitoring Manager server. The range is 1–65,535. The default port is 5005.
Reporting Period	How often an endpoint should send its RTCP packets of endpoints to the Avaya Voice over IP Monitoring Manager server. The range is 5–30 seconds. The default value is 5.

Volume Settings section

Name	Description
Receiver Volume	Set the volume in the handset rather than the speaker. The range is 0-10. The default value is 5.
Ringer Cadence	Set the cadence of the ring tone. The range is 1-8. The default value is 3.

Table continues…

Name	Description
Ringer Volume	Set the ringer setting for the stations bridged appearance buttons. The range is 1-10. The default value is 5.
Speaker Volume	Set the volume on the speaker rather than the handset. The he range is 0-10. The default value is 5.

VLAN Parameters section

Name	Description
VLAN Supported?	Indicates whether VLAN is supported or not. The VLAN ID field does not display if this option is not selected.

DIFFSERV/QOS Parameters section

Name	Description
Call Control PHB Value	The range is 0-63. The default value is 46.
Audio PHB Value	The range is 0-63. The default value is 46.
Video PHB Value	The range is 0-63. The default value is 46.

802.1 P/Q Parameters section

Name	Description
Call Control 802.1p Priority	The range is 0-7. The default value is 6.
Audio 802.1p Priority	The range is 0-7. The default value is 6.
Video 802.1p Priority	The range is 0-7. The default value is 5.

Button	Description
Restore	Restore the previous device settings.
Cancel	Cancel the modified device settings changes.
Save	Save the modified device settings changes.

Device Settings Group - Location Group field descriptions

General section

Name	Description
Name	The name of the Location Device Settings Group.
Description	Information regarding the Location Device Settings Group.
Group Type	Displays the Group Type. This field is display-only.

Server Timer section

Name	Description
Subscription Expiration Timer (secs)	Maximum time for a SIP server to keep a SIP client as subscribed. The range is 60 – 86400 seconds.
Registration Expiration Timer (secs)	Maximum time for a SIP server to keep a SIP client as registered. The range is 60 – 3600 seconds.

Assigned Location section

Name	Description
Name	Name of the location to which the Device Group Settings is associated.

Endpoint Timer section

Name	Description
Line Reservation Timer (secs)	Maximum time a SIP server can reserve a SIP line appearance. The range is 30–240 seconds. The default value is 30 seconds.
Reactive Monitoring Interval (secs)	The amount of time a phone should attempt to REGISTER with a proxy server when the proxy server is not reachable or available. The range is 10–3600 seconds. The default is 60 seconds.
Timer B (sec)	The amount of time for a phone to wait before proceeding to another proxy server if the phone does not receive a response to a SIP INVITE. The range is 0 to 32 seconds. 0 disables this feature. The default value is 2.

Maintenance Settings section

Name	Description
IP Address For SNMP Queries	IP address of a server that can query the phone for SNMP messages. The server must have the correct community string. If this field is blank, any server can query the phone. You can enter IPv4 or IPv6 addresses in the **IP Address for SNMP Queries** field.
SNMP Community	SNMP community name. This string is both a challenge and a response for the server specified in the IP addresses for SNMP Queries field and the phone. If a server IP address is specified, both the server and the phone must have the same community name administered. Only alphabetic characters are allowed, and the length cannot exceed 32 characters.

Table continues…

Name	Description
Station Admin Password	The code that an administrator must enter on a SIP phone to log in and administer the phone. Only numeric values are accepted, and the length cannot exceed 32 digits.
Station Access Code	Code that an administrator must enter on a SIP phone to log in and administer the phone. This field accepts numerics, lowercase and uppercase alphabets, and special characters. This is an optional field
Confirm Station Access Code	Station Access Code retyped for confirmation.
Quick Login Status	Specify whether or not users must enter a password when logging in to the phone. The choices are **Password Entry Required** and **Quick Login Allowed**.

VoIP Monitoring Manager section

Name	Description
IP Address	IP address of the Avaya Voice over IP Monitoring Manager server. You can enter IPv4 or IPv6 addresses in the **IP Address** field.
Port	Port used by the Avaya Voice over IP Monitoring Manager server. The range is 1 – 65,535. The default is 5005.
Reporting Period	How often an endpoint should send its RTCP packets to the Avaya Voice over IP Monitoring Manager server. The range is 5 – 30 seconds. The default is 5.

Volume Settings section

Name	Description
Receiver Volume	Set the volume in the handset rather than the speaker. The range is 0-10. The default value is 5.
Ringer Cadence	Set the cadence of the ring tone. This is a required field. The range is 1-8. The default value is 3.
Ringer Volume	Set the ringer setting for the station's bridged appearance buttons. The range is 1-10. The default value is 5.
Speaker Volume	Set the volume on the speaker rather than the handset. The range is 0-10. The default value is 5.

VLAN Parameters section

Name	Description
VLAN Supported?	Indicates whether VLAN is supported or not. The VLAN ID field does not display if this option is not selected.

DIFFSERV/QOS Parameters section

Name	Description
Call Control PHB Value	The range is 0-63. The default value is 46.
Audio PHB Value	The range is 0-63. The default value is 46.
Video PHB Value	The range is 0-63. The default value is 46.

802.1 P/Q Parameters section

Name	Description
Call Control 802.1p Priority	The range is 0-7. The default value is 6.
Audio 802.1p Priority	The range is 0-7. The default value is 6.
Video 802.1p Priority	The range is 0-7. The default value is 5.

IPv6 Settings section

You can view and update the **Media Address Mode** and **Signaling Address** mode fields only when the **Enabled IPv6** field on the Session Manager Administration page is selected.

Name	Description
Signaling Address Mode	The IP address type supported by end points to set **Signaling Address Mode** to one of the following: . • 4: The value defines the IP address type IPv4. • 6: The value defines the IP address type IPv6. Session Managersets IP address family settings on phone in response to `PPM get-AllEndpointConfiguration` request from phone. The endpoints use the IP address family settings to establish the **Signaling Address Mode**.

Table continues…

Name	Description
Media Address Mode	The IP address type supported by end points to set **Media Address Mode** to one of the following: • 4: The value defines the IP address type IPv4. • 6: The value defines the IP address type IPv6. • 46: The value defines IP address type IPv4 and IPv6 with IP address type IPv4 preferred. • 64: The value defines IP address type IPv6 and IPv4 with IP address type IPv6 preferred. Session Managersets IP address family settings on phone in response to `PPM get-AllEndpointConfiguration` request from phone. The endpoints use the IP address family settings to establish the **Media Address Mode**.

Button	Description
Restore	Restore the previously saved device settings.
Cancel	Cancel the device settings changes.
Save	Save and apply the device settings changes.

Related links

Creating a Device Settings Group - Location Group on page 508
Modifying a Device Settings Group - Location Group on page 508
Deleting Device Settings Groups - Location Groups on page 508

Device Settings Group - Terminal Group field descriptions

General section

Name	Description
Name	Name of the Terminal Device Settings Group.
Description	Information regarding the Terminal Device Settings Group.
Group Type	Displays the Group Type. This field is display-only.
Terminal Group Number	Device Settings Group number

Endpoint Timer section

Name	Description
Line Reservation Timer (secs)	Maximum time a SIP server can reserve a SIP line appearance. The range is 30 – 240 seconds. The default value is 30 seconds.

Table continues…

Name	Description
Reactive Monitoring Interval (secs)	The amount of time a phone should attempt to REGISTER with a proxy server when the proxy server is not reachable or available. The range is 10 – 3600 seconds. The default is 60 seconds.
Timer B (sec)	The amount of time for a phone to wait before proceeding to another proxy server if the phone does not receive a response to a SIP INVITE. The range is 0 to 32 seconds. 0 disables this feature. The default value is 2.

Maintenance Settings section

Name	Description
IP Address For SNMP Queries	IP address of a server that can query the phone for SNMP messages. The server must have the correct community string. If this field is blank, any server can query the phone. You can enter IPv4 or IPv6 addresses in the **IP Address For SNMP Queries** field.
SNMP Community	SNMP community name. This string is both a challenge and a response for the server specified in the IP addresses for SNMP Queries field and the phone. If a server IP address is specified, both the server and the phone must have the same community name administered. Only alphabetic characters are allowed, and the length cannot exceed 32 characters.
Station Admin Password	The code that an administrator must enter on a SIP phone to log in and administer the phone. Only numeric values are accepted, and the length cannot exceed 32 digits.
Station Access Code	Code that an administrator must enter on a SIP phone to log in and administer the phone. This field accepts numerics, lowercase and uppercase alphabets, and special characters. This is an optional field
Confirm Station Access Code	Station Access Code retyped for confirmation.
Quick Login Status	Specify whether or not users must enter a password when logging in to the phone. The choices are **Password Entry Required** and **Quick Login Allowed**.

VoIP Monitoring Manager section

Name	Description
IP Address	IP address of the Avaya Voice over IP Monitoring Manager server. You can enter IPv4 or IPv6 addresses in the **IP Address** field.
Port	Port used by the Avaya Voice over IP Monitoring Manager server. The range is 1 – 65,535. The default is 5005.
Reporting Period	How often an endpoint should send its RTCP packets to the Avaya Voice over IP Monitoring Manager server. The range is 5 to 30 seconds. The default is 5.

Volume Settings section

Name	Description
Receiver Volume	Set the volume in the handset rather than the speaker. The range is 0-10. The default value is 5.
Ringer Cadence	Set the cadence of the ring tone. The range is 1-8. The default value is 3.
Ringer Volume	Set the ringer setting for the stations bridged appearance buttons. The angle is 1-10. The default value is 5.
Speaker Volume	Set the volume on the speaker rather than the handset. The range is 0-10. The default value is 5.

VLAN Parameters section

Name	Description
VLAN Supported?	Indicates whether VLAN is supported or not. The VLAN ID field does not display if this option is not selected.

DIFFSERV/QOS Parameters section

Name	Description
Call Control PHB Value	The range is 0-63. The default value is 46.
Audio PHB Value	The range is 0-63. The default value is 46.
Video PHB Value	The range is 0-63. The default value is 46.

802.1 P/Q Parameters section

Name	Description
Call Control 802.1p Priority	The range is 0-7. The default value is 6.
Audio 802.1p Priority	The range is 0-7. The default value is 6.
Video 802.1p Priority	The range is 0-7. The default value is 5.

IPv6 Settings section

You can view and update the **Media Address Mode** and **Signaling Address** mode fields only when the **Enabled IPv6** field on the Session Manager Administration page is selected.

Name	Description
Signaling Address Mode	The IP address type supported by end points to set **Signaling Address Mode** to one of the following: . • 4: The value defines the IP address type IPv4. • 6: The value defines the IP address type IPv6. Session Managersets IP address family settings on phone in response to `PPM get-AllEndpointConfiguration` request from phone. The endpoints use the IP address family settings to establish the **Signaling Address Mode**.
Media Address Mode	The IP address type supported by end points to set **Media Address Mode** to one of the following: • 4: The value defines the IP address type IPv4. • 6: The value defines the IP address type IPv6. • 46: The value defines IP address type IPv4 and IPv6 with IP address type IPv4 preferred. • 64: The value defines IP address type IPv6 and IPv4 with IP address type IPv6 preferred. Session Managersets IP address family settings on phone in response to `PPM get-AllEndpointConfiguration` request from phone. The endpoints use the IP address family settings to establish the **Media Address Mode**.

Button	Description
Restore	Restore the previously saved device settings.
Cancel	Cancel the device settings changes.
Save	Save the device settings changes.

Related links

[Creating a Device Settings Group - Terminal Group](#) on page 506
[Modifying a Device Settings Group - Terminal Group](#) on page 507

Deleting Device Settings Group - Terminal Group on page 507

Location Settings

Use the Location Settings page to assign a Device Settings Group to a Location.

Viewing location settings

Procedure

On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Device and Location Configuration** > **Location Settings**.

Related links

Location Settings field descriptions on page 521

Modifying Location Settings

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Device and Location Configuration** > **Location Settings**.
2. Associate a location with the respective Device Settings Group.
3. Click **Save** to save the changes.

Related links

Location Settings field descriptions on page 521

Location Settings field descriptions

Button	Description
Save	Save the Location Settings changes.

Name	Description
Name	Name of the Location.
Device Setting Group	Name of the Device Setting Group.

Related links

Modifying Location Settings on page 521
Viewing location settings on page 521

Setting Station Access Code Policy

About this task

From Session Manager Release 7.1, the administrator can define the Complex Station Access Code validation rules using the Station Access Code Policy screen on the Device and Location

Configuration page. The administrator can establish parameters to define the access codes, such as minimum length, allowed characters, and inclusion of minimum character sets.

You can use the Station Access Code Policy page to define the rules for setting a Station Access Code.

Procedure

1. On the home page of System Manager Web Console, in **Elements**,click **Session Manager** > **Device and Location Configuration** > **Station Access Code Policy**.
2. Enter appropriate information in the required fields.

   For more information, see “Station Access Code Policy Field Description”.
3. Click **Commit**.

   The system saves the password policy for Complex Station Access Code.

Station Access Code Policy field descriptions

Name	Description
Minimum required length	The minimum number of characters required in the password. The password can be of 6 to 25 characters. **Note:** The minimum required length must be equal to or greater than the number of characters required from each character set.
Minimum character sets	The minimum number of character sets required in the password. The options are: • 0 • 1 • 2 • 3 For example, if you set the **Minimum character set** field to 2, the password must contain at least two characters from the numeric, upper, or special character sets.
Lower case characters	The minimum number of lowercase characters required in the password.
Upper case characters	The minimum number of uppercase characters required in the password.
Numeric characters	The minimum number of numeric characters required in the password.
Special characters	The minimum number of special characters required in the password.

Note:

You can set either the **Minimum character sets** or the number of characters required from each character set to a value other than 0. You cannot simultaneously specify values in the **Minimum character sets** field and the number of characters required from each character set.

Button	Description
Commit	Saves all updates in the Station Access Code Policy page.
Cancel	Disregards the changes and goes back to the earlier page.

Applications

Session Manager uses media-based filtering when invoking a set of sequenced applications for an originating or terminating call. Before invoking an application, Session Manager ensures the application supports the media type requested in the session request. If an application does not support the requested media, Session Manager skips that application in an application sequence.

The administrator defines the media attributes for each application.

Related links

Application Sequences on page 529

Filtering of sequenced applications based on media attributes

Before invoking a provisioned originating or terminating sequenced application, Session Manager checks for the value of the **Enable Media Filtering** flag of the application.

- If the flag is set, Session Manager applies application filtering based on the provisioned media attributes conditions and the media types requested in the SDP. Session Manager invokes the sequenced application only if it passes the filter condition.
- If the flag is not set, Session Manager unconditionally invokes the sequenced application.

Session Manager applies the media based filtering for both orig-side and term-side applications.

For filtering the requests, Session Manager compares the SDP of the SIP request against the following attributes of the sequenced application: Audio, Video, Text, MatchType, and “If SDP Missing”.

The following table shows some of the possible examples for analysis of the media based filtering treatment:

Audio	Video	Text	MatchType	If SDP Missing	Description
Y	Y	Not Only	Exact	Allowed	Enables: {A,V,T} , {A,V} and request with no SDP only.

Table continues…

Audio	Video	Text	MatchType	If SDP Missing	Description
Y	Y	Not Only	Exact	Skip	Enables: {A,V,T} and {A,V} only. (Does not allow requests without SDP)
N	N	Not Only	Exact	Allowed	Invalid combination.
N	Not Only	Not Only	Not Exact	Skip	Invalid combination. At least one attribute must be Yes.
Y	Y	Not Only	Not Exact	Skip	Enables: {A}, {V}, {A, V}, {A,T}, {V, T}, {A,V,T}
Y	N	Not Only	Not Exact	Skip	Enables: {A} {A,T}

For an application with the Mandatory condition in an application sequence:

If the **Enable Media Filtering** flag is enabled for an application, Session Manager applies application filtering based on media irrespective of the **Mandatory** condition defined for the application.

For example:

1. Setup details
   - An application sequence vector seq-vector-abc consists of three applications app-a, app-b, and app-c in sequence.
   - Only app-a and app-b have the **Mandatory** conditions defined.
   - The media-based applicable filtering is enabled for seq-vector-abc. app-a and app-c support audio whereas app-b does not support audio.
2. Call processing details

   Upon receiving an originating audio request from a user of seq-vector-abc, Session Manager removes app-b from the list based on the media attribute filter processing. Even the **Mandatory** condition is defined for app-b, Session Manager does not invoke app-b because app-b does not meet the media attribute filter condition. Session Manager invokes app-a followed by app-c in the sequence. If the request fails when Session Manager invokes app-a, Session Manager does not proceed with the request because app-a has the **Mandatory** condition.

In survivable condition:

When in the survivable mode, for requests that either originate from or are targeted to the branch SIP endpoint and meet the media attribute filter conditions, Branch Session Manager invokes the

LSP as the sequenced application. If the request does not meet the filter condition of LSP, Branch Session Manager skips the sequenced application invocation step.

Viewing applications

Display the list of applications for available SIP entities.

Procedure

On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Application Configuration** > **Applications**.

Creating an application

Before you begin

You must first administer a non-Session Manager SIP entity before you can create a new application entry.

Procedure

1. Verify the non-Session Manager SIP entity exists.
2. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Application Configuration** > **Applications**.
3. Click **New**.
4. Enter the appropriate information for the new application.
5. Click **Commit**.

Related links

Applications field descriptions on page 526
Application Editor field descriptions on page 527

Modifying an application

You can modify only one application at a time.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Application Configuration** > **Applications**.
2. Select the application you want to modify.
3. Click **Edit**.
4. Change the appropriate information.

5. Click **Commit**.

Related links

Applications field descriptions on page 526
Application Editor field descriptions on page 527

Deleting applications

You cannot delete an application if the application is a part of an Application Sequence. If you try to delete the application, the system displays a warning and the application entry remains.

You can delete more than one application at the same time.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Application Configuration** > **Applications**.
2. Select one or more applications.
3. Click **Delete**.
4. Click **Delete** on the confirmation page.

Related links

Applications field descriptions on page 526

Applications field descriptions

Use the filter feature to sort each field or filter records . Records are filtered by using a partial string match or by a combination of one or more fields.

Button	Description
New	Create a new application entry.
Edit	Modify the information for the selected application entry.
Delete	Delete the selected application entry or entries.

Name	Description
Application Name	Name of the application.
SIP Entity	Name of the associated SIP Entity.
Media Filtering	The status of media filtering for this application entry.
Description	Information about the application.

Related links

Creating an application on page 525
Modifying an application on page 525
Deleting applications on page 526

Application Editor field descriptions

Application section

Name	Description
Name	Name of the application entry.
SIP Entity	List of SIP entities for this application to which Session Manager can sequence calls as part of an Application Sequence.
CM System for SIP Entity	List of the Communication Manager (CM) systems corresponding to the selected CM SIP entity.
Description	Information about the application.

Application Attributes (optional) section

Name	Description
Application Handle	A unique handle for the application. Session Manager inserts the handle in the Route header when Session Manager sequences a call to an application. The Application Handle distinguishes between multiple applications running on the same host.
URI Parameters	List of URI parameters.

Application Media Attributes section

Name	Description
Enable Media Filtering	Indicates whether media filtering is to be applied to this sequenced application. If this check box is cleared, then all the fields in this section become disabled. Media Filtering is disabled for this Application, and the Application will always be invoked irrespective of the media requested in the session requests.

Table continues…

Name	Description
Audio	Specifies whether this Application supports audio media. Valid choices are : YES, NO, NOT_ONLY The NOT_ONLY option specifies that audio may be present with either text or video but not as an audio-only media stream.
Video	Specifies whether this Application supports video media. Valid choices are: YES, NO, NOT_ONLY The NOT_ONLY choice specifies that video may be present with either audio or text but not as a video-only media stream.
Text	Specifies whether this Application supports text media. Valid choices are: YES, NO, NOT_ONLY The NOT_ONLY choice specifies that text may be present with either audio or video but not as a text-only media stream.
Match Type	The options for this field are: • **EXACT:** This option indicates the SDP for this message must contain all of the media type specified with **YES** and none of the media types specified with **NO**. • **NOT_EXACT:** This option indicates that the SDP for this message must contain at least one of the media types specified with **YES**.
If SDP Missing	Specifies whether or not the Application is to be invoked if no SDP is present in the INVITE. • If the field is set to **Allow** and the SDP is not present, the application is invoked. • If the field is set to **Skip** and the SDP is not present, the application is skipped. • If the SDP is present, this field is ignored.

Button	Description
Commit	Save and apply the changes.
Cancel	Cancel the changes.

Related links

[Creating an application](#) on page 525
[Modifying an application](#) on page 525

Application Sequences

Application Sequences define and manage an ordered set of applications for call sequencing. These application sets can be associated as originating and terminating application templates for the Communication Profile of a registered user. Applications are assigned based on the needs of the user and are not related to the location or the device used.

Session Manager provides the capability to create a profile for third party PBX users. You can add applications to apply to these users to provide services such as:

- Block calls based on user preferences.
- Direct calls to a user when the user moves across the enterprise.
- Augment caller ID information for incoming and outgoing calls without upgrades or code modifications to existing third party PBX-equipment.

Related links

Applications on page 523

Viewing application sequences

The Application Sequences page displays the list of Application Sequences.

Procedure

On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Application Configuration** > **Application Sequences**.

Related links

Application Sequences field descriptions on page 531

Creating an Application Sequence

An Application Sequence can contain a maximum of 10 applications.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Application Configuration** > **Application Sequences**.
2. Click **New**.
3. Enter the appropriate information.
4. Click **Commit**.

Related links

Application Sequences field descriptions on page 531
Application Sequence Editor field descriptions on page 532

Modifying an Application Sequence

You can modify only one Application Sequence at a time.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Application Configuration** > **Application Sequences**.
2. Select the application sequence you need to modify.
3. Click **Edit**.
4. Modify the information as required.
5. Click **Commit**.

Related links

Application Sequences field descriptions on page 531
Application Sequence Editor field descriptions on page 532

Deleting Application Sequences

You can delete more than one Application Sequence at a time.

You cannot delete an Application Sequence if the Application Sequence is defined as an originating or terminating application set of a communication profile.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Application Configuration** > **Application Sequences**.
2. Select one or more application sequences.
3. Click **Delete**.
4. Click **Delete** on the confirmation page.

Related links

Application Sequences field descriptions on page 531

Rearranging Applications in an Application Sequence

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Application Configuration** > **Application Sequences**.
2. Select an Application Sequence.

3. Click **Edit**.
4. In the Applications in this Sequence section, do one of the following for each Application you want to move or remove:
   - Select an Application and click the buttons to move the Application to the first or last position in the Application Sequence order, or to remove the Application from the Application Sequence.
   - Select an Application and click the up or down arrows under the **Sequence Order (first to last)** column to change the relative sequence order of the Application, or click the **X** symbol to remove the Application from the Application Sequence.
5. Click **Commit**.

Related links

Application Sequence Editor field descriptions on page 532

Adding Applications to an existing Application Sequence

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Application Configuration** > **Application Sequences**.
2. Select an application sequence.
3. Click **Edit**.
4. In the Available Applications section, click the plus sign (**+**) in front of the application you want to add to the application sequence.
5. **(Optional)** In the Applications in this sequence section, do one of the following:
   - Select the application and use the up and down arrows to move the application in the sequence order.
   - Select the application and click the delete sign (**X**) to remove the application from the sequence.
6. Click **Commit**.

Related links

Application Sequence Editor field descriptions on page 532

Application Sequences field descriptions

Button	Description
New	Create a new application sequence.

Table continues…

Button	Description
Edit	Modify the selected application sequence.
Delete	Delete the selected application sequence.

Name	Description
Name	Name of the application sequence.
Description	Information about the application sequence.

Related links

Viewing application sequences on page 529
Creating an Application Sequence on page 529
Modifying an Application Sequence on page 530
Deleting Application Sequences on page 530

Application Sequence Editor field descriptions

Sequence Name section

Name	Description
Name	Name of the application sequence.
Description	Information about the application sequence .

Applications in this Sequence section

Button	Description
Move First	Move the selected application to become the first application invoked in the sequence.
Move Last	Move the selected application to become the last application invoked in the sequence.
Remove	Remove the selected application from the sequence.

Name	Description
Sequence Order (first to last)	Change the relative sequence order of the applications or remove applications from the application sequence using the up and down arrows or the delete sign (X).
Name	Name of the selected application.
SIP Entity	Name of the SIP entity associated with the selected application

Table continues…

Name	Description
Mandatory	Specifies whether invocation of this application is mandatory or not. If Session Manager fails to reach the application during the sequencing, Session Manager stops sequencing and sends an error response upstream. If the **Enable Media Filtering** flag is selected for an application, Session Manager performs application filtering based on media regardless of the **Mandatory** condition. Session Manager skips the application if the request does not pass the media attribute filters. For requests that pass the application media attribute filter condition, Session Manager performs application sequencing according to the **Mandatory** condition.
Description	Description of the selected application

Available Applications section

Name	Description
+	Add the selected application to the application sequence.
Name	Name of the application.
SIP Entity	Name of the SIP entity associated with the application.
Description	Description of the application

Button	Description
Commit	Save and apply the changes.
Cancel	Cancel the changes.

Related links

Creating an Application Sequence on page 529
Modifying an Application Sequence on page 530
Rearranging Applications in an Application Sequence on page 530
Adding Applications to an existing Application Sequence on page 531

Conference Factory URI

The Conference Factory URI provides seamless integration of the conference capabilities supplied by the conference products such as Avaya Multimedia Messaging and SIP endpoints such as an Avaya Desktop Video Device with Session Manager. This feature provides an enhanced

experience for conferences participants and richer collaboration when using voice, video, and text conference systems.

A Conference Factory Set is a collection of Conference Factory URI mappings that have a unique URI. The URI is referred as the Conference Factory URI. In a Conference Factory URI mapping, a Conference Factory URI is associated with a respective Entity Name (Conference server name), Audio-Video-Text media attributes, Match Type parameters, and SDP parameters. On the User management page, you can associate a Conference Factory Set with the Session Manager Communication Profile of a user.

Session Manager receives a REQUEST URI in the INVITE and compares the Request URI of the Invite with the provisioned Well Known Conference URI list. Session Manager then selects the Conference Factory Set and routes the call towards the associated Conference Server to create a new ad-hoc conference.

How the Conference Factory feature works

The Well Known Conference URI is a unique SIP address used by the endpoint to initiate a conference. The Conference Factory URI is a unique SIP address of the Conference Server. An Avaya phone receives the **Well Known Conference URI** from the settings file.

Session Manager contains a list of all provisioned Well Known Conference URIs and Conference Factory URIs in the database. Session Manager uses information specified in the Session Manager Communication Profile of the user to route the conference call of the participant to the appropriate conference server as follows:

1. When the first participant wants to initiate a conference, the participant either presses the conference button on the phone or drags additional contacts into the spotlight (as applicable for some conferencing products).
2. The endpoint then sends an INVITE to Session Manager with the REQUEST URI set to the Well Known Conference URI.
3. Session Manager receives the INVITE, reads the Well Known Conference URI, and runs the originating application sequence.
4. Session Manager compares the REQUEST URI of the INVITE with the provisioned Well Known Conference URI list.
5. If the URI does not match, Session Manager proceeds with the normal routing process.
6. If the URI matches, Session Manager routes the call towards an appropriate conference server based on the priority level setting of the Conference Factory URI mappings:
    a. Session Manager identifies the Conference Factory Set defined in the Session Manager Communication Profile of the originator and matches the provisioned Conference Factory Sets for evaluation.
    b. Session Manager compares the media type contained in the INVITE (SDP) with the media criteria specified for the first Conference Factory URI mapping of the Conference Factory Set.

c. If the media types match the media attributes, Session Manager replaces the REQUEST URI of the INVITE with the respective Conference Factory URI and routes the call to the respective Conference Server that is the SIP Entity identified in the current Conference Factory URI mappings.

d. If the media types do not match the media attributes, Session Manager compares the media type with the media attributes specified for the next Conference Factory URI mappings in the matched Conference Factory Set and so on.

e. If there is no match between the endpoint media types in the INVITE and the media attributes specified for other Conference Factory URI mappings, Session Manager denies the conference initiation request and send back 403 response to the upstream SIP element.

f. If the SDP is not present in the INVITE message, Session Manager routes the call based on the **If SDP Missing** field setting in the Conference Factory Set Web page,

- If the SDP is not present and the field is set to **Allow**, Session Manager routes the call to the conference server as indicated in the Conference Factory URI mapping.
- If the SDP is not present and the field is set to **Deny**, Session Manager does not route the call to the conference server as indicated in the Conference Factory URI mapping. Instead, Session Manager skips this conference server and goes to the next Conference Factory URI mappings until Session Manager finds an SDP status set to **Allow**.
- If the SDP is present, Session Manager ignores the **If SDP Missing** field.

You can create multiple Conference Factory Sets in Session Manager. You can create a maximum of ten (10) Well Known Conference URIs.

You can add multiple Conference Factory URI mappings in the Conference Factory Set. To each Conference Factory URI mapping, you can assign a particular URI, Entity Name (Conference server name), Audio-Video-Text media attributes, Match Type parameters, and SDP parameters. A conference server, defined as a SIP entity in the Conference Factory URI mapping, can be associated with multiple Conference Factory Sets. You can import and export these Conference Factory Sets and Well Known URIs using the Bulk Importing and Exporting feature. You can assign Conference Factory Sets to the conference servers using the Communication Profile Editor feature.

Session Manager replicates the Well Known Conference URIs table and the Conference Factory URIs table to all the core Session Manager instances and the associated Branch Session Manager instances. If a Branch Session Manager cannot communicate with the core Session Manager, the Branch Session Manager compares the Well Known Conference URI from the REQUEST URI of the INVITE with the provisioned Well Known Conference URI list on the Branch Session Manager. The Branch Session Manager then routes the call to the appropriate conference server or SIP entity that matches the associated user's feature server (LSP) or local trunk gateway.

Adding a new Well Known Conference URI

You can add a maximum of ten (10) Well Known Conference URIs.

Note:

The following restrictions apply to the Well Known Conference URI name:

- The Well Known Conference URI name must contain at least two characters and must not exceed 255 characters.
- You cannot use <, >, $, %, \, ^,*, #
- You can use characters from the UTF-8 character set.
- Do not include the sip: or sips: prefix when entering the Well Known Conference URI.
- Follow the RFC 3261 for more information on SIP URI format.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Application Configuration** > **Conference Factories**.
2. Click the **Well Known Conference URIs** tab.
3. Click **Add**.
4. Type a name in the empty field in the **Well Known Conference URIs** column.
5. Click the empty cell under the **Description** column and type a general description for the Well Known Conference URI.
6. Click **Commit**.
7. Click **Refresh** to refresh the list of URIs.

   Caution:

   Do not click **Refresh** before saving the field entries. You must click **Commit** to save the Well Known Conference URI record.
8. To sort the Well Known Conference URIs in alphabetical order, place the cursor on the **Well Known Conference URIs** column header and click the arrow on the right side of the column header.

Related links

Conference Factories Field Description on page 540

Editing the Well Known Conference URI entry

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Application Configuration** > **Conference Factories**.
2. Click the **Well Known Conference URIs** tab.
3. Click the appropriate cell and make the required changes.
4. Click **Commit**.
5. Click **Refresh** to refresh the list of URIs.

   Caution:

   Do not click **Refresh** before you save the field entries. You must click **Commit** to save the Well Known Conference URI record.

Related links

Conference Factories Field Description on page 540

Removing the Well Known Conference URI entry

You can remove multiple Well Known Conference URIs at the same time.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Application Configuration** > **Conference Factories**.
2. Click the **Well Known Conference URIs** tab.
3. Select the Well Known Conference URI or URIs you want to remove.
4. Click **Remove**.
5. Click **Commit**.
6. Click **Refresh** to refresh the list of URIs.

   Caution:

   Do not click **Refresh** before saving the URI entries. You must click **Commit** to update the Well Known Conference URI record.

Related links

Conference Factories Field Description on page 540

Adding a new Conference Factory Set

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Application Configuration** > **Conference Factories**.
2. Click the **Conference Factory Sets** tab.
3. Click **Add**.
4. Type the **Factory Set Name**.
5. Type a **Description** for the Conference Factory Set.
6. Click **Add**.
7. In the **Conference Factory URI** field, enter the Conference Factory SIP URI. Do not enter the **sip** or **sips** prefix.
8. In the **SIP Entity** field, select an appropriate SIP entity from the drop-down menu.
9. In the **Audio** field, select the appropriate option from the drop-down menu to specify if this URI mapping supports voice conferencing.
10. In the **Video** field, select the appropriate option from the drop-down menu to specify if this URI mapping supports video conferencing.
11. In the **Text** field, select the appropriate option from the drop-down menu to specify whether this URI mapping supports text conferencing.
12. In the **Match Type** field, select the appropriate option from the drop-down menu to specify whether this URI mapping supports selected media types.
    - Select **EXACT** to indicate that SDP for this message should contain all the media types specified with **YES** and none of the media types specified with **NO**.
    - Select **NOT_EXACT** to indicate that SDP for this message should contain at least one media type specified with **YES**.
13. In the **If SDP Missing** field, select the appropriate option from the drop-down menu to specify whether Session Manager should route the INVITE to the Conference Factory URI if the SDP is not present.
    - If the SDP is not present and this field is set to **ALLOW**, Session Manager routes the call to the conference server as indicated in the Conference Factory URI mapping.
    - If the SDP is not present and this field is set to **DENY**, Session Manager does not route the call to the conference server as indicated in the Conference Factory URI mapping. Instead, Session Manager skips this conference server and goes to the next Conference Factory URI mapping until Session Manager finds an SDP status set to **ALLOW**.
    - If the SDP is present, Session Manager ignores the **If SDP Missing** field.
14. In the **Priority** field, set the priority to evaluate INVITE order evaluation. Move up to set as a higher priority and move down to set as a lower priority.

15. Click **Commit**.
16. Click the **Well Known Conference URIs** tab.
17. Click **Refresh** to refresh the list of Conference Factory Sets.

Related links

Conference Factories Field Description on page 540
Conference Factory Set Page Field Description on page 541

Viewing the Conference Factory Set

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Application Configuration** > **Conference Factories**.
2. Click the **Conference Factory Set** tab.
3. Select the Conference Factory Set you want to view.
4. Click **View**.
5. Click **Cancel** to return to the previous page.

Related links

Conference Factories Field Description on page 540
Conference Factory Set Page Field Description on page 541

Editing a Conference Factory Set

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Application Configuration** > **Conference Factories**.
2. Click the **Conference Factory Set** tab.
3. Select the Conference Factory Set you want to edit.
4. Click **Edit**.
5. Modify the appropriate information.
6. Click **Commit**.

Related links

Conference Factories Field Description on page 540
Conference Factory Set Page Field Description on page 541

Deleting a Conference Factory Set

You can delete more than one Conference Factory Set at the same time.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Application Configuration** > **Conference Factories**.
2. Click the **Conference Factory Set** tab.
3. Select the Conference Factory Set or Sets you want to delete.
4. Click **Delete**.
5. Click **OK** in the Delete confirmation dialog box.
6. Click the **Well Known Conference URIs** tab.
7. Click **Refresh** to refresh the list of administered Conference Factory Sets.
8. Verify the Conference Factory Set or Sets have been deleted.

Related links

Conference Factories Field Description on page 540
Conference Factory Set Page Field Description on page 541

Conference Factories Field Description

Well Known Conference URI tab

Button	Description
Add	Add a new entry of Well Known Conference URI to the table.
Remove	Remove the selected Well Known Conference URI entry from the table.
Reset	Discard the changes and restore the saved Well Known URI values.
Commit	Save the Well Known Conference URI entry in the Session Manager database.
Refresh	Refresh the information in the Session Manager database.

Field	Description
Well Known Conference URI	The list of the provisioned Well Known Conference URIs.
Description	The description of the Well Known Conference URI.

Conference Factory Set Tab

Button	Description
Add	Add a new Conference Factory Set.
View	View the details of the selected Conference Factory Set.
Edit	Edit the information of the selected Conference Factory Set.
Delete	Delete the Conference Factory Set entry from the Session Manager database.

Field	Description
Factory Set Name	The name of the provisioned Conference Factory Sets.
Communication Profiles	Number of users with Session Manager Communication Profile references to this Conference Factory Set.
Description	Description of the selected Conference Factory Set.

Related links

Adding a new Well Known Conference URI on page 536
Editing the Well Known Conference URI entry on page 537
Removing the Well Known Conference URI entry on page 537
Adding a new Conference Factory Set on page 538
Viewing the Conference Factory Set on page 539
Editing a Conference Factory Set on page 539
Deleting a Conference Factory Set on page 540

Conference Factory Set Page Field Description

Fields	Description
Factory Set Name	Name of the Conference Factory Set.
Description	Description of the Factory Set.

Conference Factory URIs

Button	Description
Add	Add a new entry for Conference Factory URI in the table.
Remove	Remove the selected entry of the Conference Factory URI from the table.

Fields	Description
Priority	Set the order for evaluating the INVITE for a match.
Conference Factory URI	The Conference Factory URI without the **sip:** or **sips:** prefix.
SIP Entity	The Conference Server SIP Entity linked to this Conference Factory URI.
Audio	Specify whether or not this Conference Factory URI supports voice conferencing.
Video	Specify whether or not this Conference Factory URI supports video conferencing.
Text	Specify whether or not this Conference Factory URI supports text conferencing.
Match Type	Specify whether or not this Conference Factory URI needs to match all the media types. **Exact:** The SDP for this message must contain all the media types specified with **Yes** and none of the media types specified with **No**. **Not Exact:** The SDP for this message should contain at least one media type specified with **Yes**.
If SDP missing	Specify how Session Manager routes the INVITE to the Conference Factory URI if the SDP is not present in the Conference Factory URI. • If the SDP is not present and this field is set to **Allow**, Session Manager routes the call to the conference server as indicated in the Conference Factory URI mapping. • If the SDP is not present and this field is set to **Deny**, Session Manager does not route the call to the conference server as indicated in the Conference Factory URI mapping. Instead, Session Manager skips this conference server and goes to the next Conference Factory URI mapping until Session Manager finds a SDP status set to **Allow**. • If the SDP is present, Session Manager ignores the **If SDP Missing** field.

Button	Description
Commit	Saves the Conference Factory Set in the Session Manager database.
Reset	Discard the changes and restore the saved Conference Factory Set values.
Cancel	Discard the changes and return to the Conference Factories page.

Related links

Adding a new Conference Factory Set on page 538
Viewing the Conference Factory Set on page 539
Editing a Conference Factory Set on page 539
Deleting a Conference Factory Set on page 540

Implicit Users

Use the Implicit Users feature to administer certain dial patterns, originating sequenced applications, and terminating sequenced applications for users who do not register or connect with Session Manager.

SIP User Implicit Sequencing

You can apply origination and termination application sequencing for SIP (explicit) users based on implicit user application sequencing definitions.

During origination, Session Manager sequences through explicit, then implicit origination applications.

During termination, Session Manager sequences through implicit, then explicit termination applications.

For backwards compatibility, implicit sequencing for SIP users is **disabled** by default.

Implicit sequencing for a SIP user is performed from the Session Manager associated with the user only. For non-SIP users, any Session Manager can perform implicit sequencing.

Implicit sequencing can route-through to an alternate Session Manager to reach an application. For a SIP user, route-through is limited to the Session Manager instances in the user's community.

Viewing Implicit User Rules

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager**.
2. Click **Application Configuration** > **Implicit Users**.

   The Implicit Users page displays the list of Implicit User rules.

Related links

Implicit User Rules field descriptions on page 545

Creating an Implicit User Rule

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Application Configuration** > **Implicit Users**.
2. Click **New**.
3. On the Implicit User Rule Editor page, enter the appropriate information.
4. Click **Commit**.

Related links

Implicit User Rules field descriptions on page 545
Implicit User Rule Editor field descriptions on page 545

Modifying an existing Implicit User Rule

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Application Configuration** > **Implicit Users**.
2. Select the Implicit User rule you want to edit.
3. Click **Edit**.
4. Modify the appropriate information.
5. Click **Commit**.

Related links

Implicit User Rules field descriptions on page 545
Implicit User Rule Editor field descriptions on page 545

Removing existing Implicit User Rules

You can delete one or more Implicit User Rules at the same time.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Application Configuration** > **Implicit Users**.
2. Select one or more Implicit User rules you want to delete.
3. Click **Delete**.
4. Click **Delete** on the confirmation page.

Related links

Implicit User Rules field descriptions on page 545

Implicit User Rules field descriptions

Button	Description
New	Create a new Implicit User Rule.
Edit	Modify the selected Implicit User Rule.
Delete	Delete the selected Implicit User Rule. You can delete more than one rule at the same time.

Name	Description
Pattern	Dial pattern with the same pattern format as the Routing Policy Dial pattern.
Min	Minimum number of digits to be matched from the dial pattern of this rule. Valid values are between 1 and 36.
Max	Maximum number of digits to be matched from the dial pattern of this rule. Valid values are between 1 and 36.
SIP Domain	SIP Domain to which this rule is associated.
Origination Application Sequence	Name of the Origination Application Sequence for this rule.
Termination Application Sequence	Name of the Termination Application Sequence for this rule.
Emergency Origination Application Sequence	Name of the Emergency Origination Application Sequence for this rule.
Emergency Termination Application Sequence	Name of the Emergency Termination Application Sequence for this rule.
Description	Description of the rule.

Related links

Viewing Implicit User Rules on page 543
Creating an Implicit User Rule on page 544
Modifying an existing Implicit User Rule on page 544
Removing existing Implicit User Rules on page 544

Implicit User Rule Editor field descriptions

Use the Implicit User Rule Editor page to define a new pattern rule or to modify an existing pattern rule.

Tab	Description
Digit Pattern Rules	Enables the administration of application sequences for emergency calling using digit based pattern rules.
Regular Expression Pattern Rules	Enables the administration of application sequences for emergency calling using regular expression based pattern rules.

The following table lists the fields for **Digit Pattern Rules**:

Name	Description
Pattern	Dial pattern with the digit pattern format.
Min	Minimum number of digits to match in the dial pattern. Valid values are 1-36.
Max	Maximum number of digits to match in the dial pattern. Valid values are 1- 36.
Description	Description of the Rule.
SIP Domain	Name of the SIP Domain associated with the Rule.
Origination Application Sequence	Name of the Origination Application Sequence for this Rule.
Termination Application Sequence	Name of the Termination Application Sequence for this Rule.
Emergency Origination Application Sequence	Name of the Emergency Origination Application Sequence for this Rule.
Emergency Termination Application Sequence	Name of the Emergency Termination Application Sequence for this Rule.

The following table lists the fields for **Regular Expression Pattern Rules**:

Name	Description
Pattern	Dial pattern with the regular expression pattern format.
Origination Application Sequence	Name of the Origination Application Sequence for this Rule.
Termination Application Sequence	Name of the Termination Application Sequence for this Rule.
Emergency Origination Application Sequence	Name of the Emergency Origination Application Sequence for this Rule.
Emergency Termination Application Sequence	Name of the Emergency Termination Application Sequence for this Rule.
Description	Description of the Rule.

Button	Description
Commit	Save and apply the changes.
Cancel	Cancel the changes.

Related links

Creating an Implicit User Rule on page 544
Modifying an existing Implicit User Rule on page 544

Administering Implicit Applications for SIP users

By default, **Enable Implicit User Applications for the SIP users** is not enabled on the Session Manager Administration page.

Procedure

1. On the System Manager web console home page, under **Elements**, click **Session Manager** > **Session Manager Administration**.
2. Under the **Global Settings** section, enable or disable **Enable Implicit User Applications for SIP users**.
3. Click **Save**.

NRS Proxy Users

The Session Manager Network Connect Service (NCS) provides routing services to VoIP endpoints based on Avaya Communication Server 1000 (CS1000). This service is similar to the services provided by the Nortel Network Routing Service (NRS). The NRS provides following three services:

- SIP Proxy Server (SPS): SPS performs two roles in CS1000-based configuration. These roles are SIP routing proxy and SIP registrar.
- Network Connect Server (NCS): NCS supports the centralized CS1000 solution for IP clients (IP phones).
- H.323 Gatekeeper (GK): GK provides typical H.323 gatekeeper functions to H.323 endpoints in the solution.

Session Manager provides both the SIP Proxy Server and Network Connect Server functionality that are provided by Nortel NRS.

Session Manager provides the following information to each UNIStim phone:

- Primary signaling server
- Secondary signaling server

- Branch Office, Survivable Media Gateway, or Survivable Remote Gateway

The Session Manager NCS provides network redirection services for UNIStim phones for several CS1000 network features, such as geographic redundancy, virtual office, branch office, and Survivable Remote Gateway. You can define user patterns that are administered as a NRS Proxy User Rule in Session Manager and associate user patterns with up to three CS1000 Terminal Proxy Servers in priority order. Since a large number of users share the same server set, you can administer a range for the user pattern to match a large set of users.

Redirecting UNIStim Phones

The following are the high-level steps for this procedure.

In normal conditions, configure UNIStim phones so that the Primary Connect Server, (Primary CS1000) points to the local Primary Session Manager and the Secondary Connect Server, (Secondary CS1000), points to the Secondary Session Manager.

Before you begin

Obtain the appropriate Avaya Communication Server 1000 documentation on the Avaya support website.

Procedure

1. Point each SIP Signaling Gateway from the SIP Proxy Server (SPS) to the Session Manager.
2. Reconfigure NCS to point to Session Manager.
3. Create Terminal Proxy Server instances for Primary signaling server and Secondary signaling server according to your system requirements.
4. Create Terminal Proxy Server instances for each Branch Office, Survivable Media Gateway, or Survivable Remote Gateway 50.
5. Create an NRS Proxy User Rule.

Related links

Creating Terminal Proxy Server instance on page 548
Creating a NRS Proxy User Rule on page 549

Creating Terminal Proxy Server instance

When you add an application entity through Runtime Topology Service (RTS), the system starts a synchronization process for the relevant data of the application instances to the Communication System Management database.

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Elements**.
2. Click **New**.
3. In the **Type** field, select **CS 1000 Terminal Proxy Server** from the drop-down menu.

   The screen refreshes with the New CS 1000 Terminal Proxy Server page.
4. In the **Name** field, type the H.323 ID value of the Main or Primary Signaling Server.
5. **(Optional)** Type a description in the **Description** field.
6. In the **Node** field, enter the Node IP address of the Main or Primary Signaling Server.
7. Click **Commit**.
8. **(Optional)** Check the status of the synchronization process. On the home page, under **Services**, click **Scheduler** > **Pending Jobs**.

Creating a NRS Proxy User Rule

Procedure

1. Verify the Terminal Proxy Server is administered on the **Inventory** > **Manage Elements** page.
2. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Application Configuration** > **NRS Proxy Users**.
3. Click **New**.
4. Enter the appropriate information for the new NRS Proxy User Rule.
5. Click **Commit**.

Related links

NRS Proxy Users field descriptions on page 550
NRS Proxy User Rule Editor field descriptions on page 551

Modifying NRS Proxy User Rule

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Application Configuration** > **NRS Proxy Users**.
2. Select the NRS Proxy User Rule you want to modify.
3. Click **Edit**.
4. Make the appropriate changes.

5. Click **Commit**.

Related links

NRS Proxy Users field descriptions on page 550
NRS Proxy User Rule Editor field descriptions on page 551

Deleting an NRS Proxy User Rule

You can delete more than one NRS Proxy User Rule at the same time.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Application Configuration** > **NRS Proxy Users**.
2. Select the NRS Proxy User Rule or Rules you want to delete.
3. Click **Delete**.
4. Click **Delete** on the confirmation page.

Related links

NRS Proxy Users field descriptions on page 550

NRS Proxy Users field descriptions

Button	Description
New	Create a new entry.
Edit	Edit information for the select entry.
Delete	Delete the selected entry.

Name	Description
Pattern	User Pattern type.
Primary Terminal Proxy Server	The administered Primary Terminal Proxy Server.
Secondary Terminal Proxy Server	The administered Secondary Terminal Proxy Server.
Survivable Terminal Proxy Server	The administered Survivable Terminal Proxy Server.

Related links

Creating a NRS Proxy User Rule on page 549
Modifying NRS Proxy User Rule on page 549
Deleting an NRS Proxy User Rule on page 550

NRS Proxy User Rule Editor field descriptions

Name	Description
Pattern	User Pattern. This field is required. The prefix can include the numbers 0 to 9, and the hash (#), hyphen (-), and question mark (?) symbols. The prefix can have a length of up to 30 characters, but the first character *must* be numeric. Routing entries can be categorized as follows: • **Basic digits:** Use any number of digits to make a simple entry. For example, 570 • **Range of digits:** Use two basic digit entries to build a range entry. The range has a dash between the two entries. Each range must have the same number of digits. For example, 467 – 486 is valid. 467 – 4866 is not valid. • **Length delimited:** Terminate a basic digit entry with the hash "#" symbol to force a specific length match. For example, 5703360#. • **Wild card:** Append the wild card digit character "?" to a basic digit entry. Each wild card character matches only one digit, and multiple wild cards can be appended. For example, 57033??
Primary Terminal Proxy Server	Administered Terminal Proxy Server. This field is a required field.
Secondary Terminal Proxy Server	Administered Secondary Terminal Proxy Server.
Survivable Terminal Proxy Server	Administered Survivable Terminal Proxy Server.

Button	Description
Commit	Save and apply the changes.
Cancel	Cancel the changes.

Related links

Creating a NRS Proxy User Rule on page 549
Modifying NRS Proxy User Rule on page 549

Chapter 9: System Status

Session Manager SIP Entity Monitoring

SIP Entity Monitoring provides background detection for monitored connections to improve alternative routing and to minimize the call setup time due to SIP link failures. The SIP Monitor periodically tests the status of the SIP proxy servers. If a proxy fails to reply, SIP messages are no longer routed to that proxy. As a result, call delays are reduced since calls are not routed to the failed servers. The SIP Monitor continues to monitor the failed SIP entity. When the proxy replies, SIP messages are again routed over that link.

SIP monitoring sends OPTIONS requests to SIP entities to determine whether these are in up, partially up, down or deny new service state. An entity is considered up if all of the addresses associated with it are up. An entity is down if all of its addresses are down. An entity is partially up if some, but not all, of its addresses are up. An address is considered down if the response of address to OPTIONS is:

- 408 Request Timeout
- 500 Server Internal Error: Destination Unreachable
- 503 Service Unavailable (with no parenthetical text)
- 503 Service Unavailable (no media resources)
- 504 Server Timeout

All other responses (including "503 Service Unavailable") with other parenthetical text, such as "503 Service Unavailable (Signaling Resources Unavailable)" results in the address to be considered up.

Note:

Any 503 response is displayed as a 500 response on the SIP Monitoring GUI. SIP container converts 503 to 500 before passing the response to Session Manager.

You can turn the monitoring on or off for a given SIP entity. If monitoring is turned off, the SIP entity is not monitored by any instance.

You can also turn monitoring on or off for an entire Session Manager instance. If monitoring is turned off, none of the SIP entities are monitored by that Session Manager instance. If monitoring for the Session Manager instance is turned on, only those SIP entities for which monitoring is turned on are monitored.

SIP Monitoring can only report problems if the Security Module is functional.

SIP Monitoring setup is administered using the SIP Entity and the Session Manager Administration pages.

Viewing the SIP Monitoring Status Summary page

The SIP Entity Link Monitoring Status Summary page displays the status of the entity links for all the administered Session Manager instances. An entity link consists of one or more physical connections between a Session Manager server and a SIP entity.

Procedure

On the System Manager Web Console, under **Elements**, click **Session Manager** > **System Status** > **SIP Entity Monitoring**.

SIP Entity Link Monitoring Status Summary page field descriptions

SIP Entities Status for ALL Monitoring Session Manager Instances

Button	Description
Run Monitor	Starts asynchronous demand monitor test for the selected Session Manager or Branch Session Manager instances.
Refresh	Refreshes the status of the entity links for all administered Session Manager instances.

Field	Description
Session Manager	Name of the Session Manager instance. Clicking any of Session Manager servers in the list opens the Session Manager Entity Link Connection Status page that displays detailed connection status for all entity links from Session Manager. **Note:** An entity link consists of one or more physical connections between a Session Manager server and a SIP entity. If all of these connections are up, then the entity link status is **up**. If one or more connections are down, but there is at least one connection up, then the entity link status is **partially down**. If all the connections are down, the entity link status is **down**.

Table continues…

Field	Description
Type	Instances of type Session Manager and Branch Session Manager.
Monitored Entities / Down	Entity links for Session Manager that are down out of the total number of entity links for Session Manager.
Monitored Entities / Partially Up	Entity links for Session Manager that are partially up.
Monitored Entities / Up	Entity links for Session Manager that are up out of the total number of entity links for Session Manager.
Monitored Entities / Not Monitored	SIP entities that are not monitored by Session Manager.
Monitored Entities / Deny	Number of Deny New Service Entity Links.
Monitored Entities / Total	Number of total Entity Links for a SIP Entity.

All Monitored SIP Entities

Button	Description
Run Monitor	Starts asynchronous demand monitor test for the selected SIP entities. Clicking any of the entities in the list opens the SIP Entity, Entity Link Connection Status page that displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

Session Manager Entity Link Connection Status page field descriptions

All Entity Links with connections to Session Manager

Field	Description
SIP Entity Name	Name of the SIP Entity.
IP Address Family	IP address family of the Entity link.
SIP Entity Resolved IP	Resolved IP address of the SIP entity.
Port	Port used for the connection.
Protocol	Protocol used.
Deny	Deny new service status.
Conn. Status	Connection status.
Reason Code	Reason for the failure. This field explains how the status of a connection is determined irrespective of whether the status is “up” or “down”.
Link Status	Status of the Entity Link.

Button	Description
Summary View	Returns to the SIP Entity Link Monitoring Status Summary page.
Refresh	Refreshes and displays the detailed connection status for all entity links from the selected Session Manager instance.

Details

Field	Description
Time Last Down	Time when the entity link was last down.
Time Last Up	Time when the entity link was last up.
Last Message Sent	Port used for the connection.
Last Message Response	Duration of the last response latency (ms).

SIP Entity Link Connection Status page field descriptions

All Entity Links to SIP Entity

Field	Description
Session Manager Name	Name of the Session Manager instance.
IP Address Family	IP address family of the Entity link.
SIP Entity Resolved IP	Resolved IP address of the SIP entity
Port	Port used for the connection
Protocol	Protocol used
Deny	Deny new service status.
Conn. Status	Connection status
Reason Code	Reason for the failure. This field explains how the status of a connection is determined irrespective of whether the status is “up” or “down”.
Link Status	Status of the Entity Link.

Button	Description
Summary View	Returns to the SIP Entity Link Monitoring Status Summary page.
Refresh	Refreshes and displays the detailed connection status for all entity links from all Session Manager instance to a single SIP entity.

Details

Field	Description
Time Last Down	Time when the entity link was last down

Table continues…

Field	Description
Time Last Up	Time when the entity link was last up
Last Message Sent	Port used for the connection
Last Message Response	Duration of the last response latency (ms)

Managed Bandwidth Usage

The Managed Bandwidth Usage page displays Managed Bandwidth (Call Admission Control) real-time data. Measurement of bandwidth usage helps administrators to manage networks with multimedia calls. It displays a read-only table containing one row for each administered location and provides details on actual call counts and bandwidth usage for audio and video calls respectively.

You can expand each row to display a breakdown of usage and capacity by Session Manager which can be helpful in debugging network utilization or the distribution algorithm.

Viewing Managed Bandwidth Usage

The Managed Bandwidth Usage page displays system-wide bandwidth usage information for locations where usage is managed.

Procedure

1. On the System Manager Web Console, under **Elements**, click **Session Manager** > **System Status** > **Managed Bandwidth Usage**.
2. Click **Show** under the **Details** column to view the bandwidth usage information the Session Manager in that location.
3. Click **Refresh** to refresh the data.

Managed Bandwidth Usage page field descriptions

The Manage Bandwidth Usage page displays system-wide bandwidth usage information for locations where usage is managed. If no bandwidth management is implemented, this table has no information.

Field	Description
Details	Displays the breakdown of usage among the administered instances Session Manager in the enterprise. You can click the **Show** or **Hide** arrow on any row under **Details** to display or hide the detailed usage for that location.
Location	Displays the locations that are administered in the Routing Policy.
Audio Call Count	The total number of audio calls of Session Manager in a given location.
Audio BW Used	The bandwidth used for audio calls of Session Manager in a given location.
Multimedia Call Count	The total number of multimedia calls of Session Manager instances in a given location.
Multimedia BW Used	The bandwidth used for multimedia calls of Session Manager instances in a given location.
Multimedia BW Allow	Administered value, if any, of multimedia Bandwidth allowed for a given location.
Multimedia BW %Used	The bandwidth used for multimedia calls into or out of a given location divided by the value in the **Multimedia BW Allow** column.
Total BW Used	The total audio and multimedia bandwidth into or out of a given location
Total BW Allow	Administered value, if any, of the total bandwidth for a given location.
Total BW %Used	The audio and multimedia bandwidth for calls into or out of a given location divided by the value in the **Total BW Allow** column.

Field	Description
Session Manager	Name of the Session Manager instance. A warning symbol indicates the Session Manager instance is in the **Maintenance Mode** service state.
Audio Call Count	Number of audio calls terminated by the selected Session Manager for the given location.
Audio BW Used	Sum of bandwidth used by audio calls terminated by the selected Session Manager for the given location.
Multimedia Call Count	Number of multimedia calls terminated by the selected Session Manager for the given location.
Multimedia BW Used	The bandwidth used by multimedia calls terminated by the selected Session Manager for the given location.

Managed Bandwidth Usage errors

The following errors may appear on the **Managed Bandwidth Usage** page. They are related to a Session Manager instance being unreachable from System Manager. The diagnosis and resolution steps are similar:

- **Network fragmentation has occurred. Bandwidth limits are not being enforced.** This error indicates that communication is being disrupted among the cluster of Session Managers in the core (non-Branch).
- **Unable to access status information for xxxx — cannot connect to server, internal error.** The Session Manager instance is unreachable from System Manager.
- **Data displayed may be inaccurate due to connection problems to one or more Session Managers.** If one of the Session Managers is not accessible by System Manager, the values may not be accurate.

System Manager may be able to communicate with the Session Manager instance, but the Session Manager instance itself may be isolated from the rest of the core members. During this period, total bandwidth management in the core is unable to be properly enforced.

Causes

Possible causes include:

- An upgrade is in progress among the Session Managers.
- Session Manager is provisioned administratively but is not actively up and running.
- Misadministration could cause the Session Manager to appear to be administered, but the Session Manager is unreachable.
- There is a true network error within the core where connectivity is limited or unavailable between certain Session Managers.
- There is an error among the Session Managers that has limited their ability to maintain a full cluster of core Session Manager nodes.

Solutions

1. The condition should be transient and ultimately resolved on its own if network connections are being limited or disrupted, or if Session Manager is being upgraded.
2. If the condition lasts for longer than 10 minutes, check the administration and verify it is correct.
3. If the condition still exists, contact an Avaya service representative to help resolve the problem.

Security Module Status

The Security Module Status page displays the status and configuration of the security module for each administered Session Manager and Branch Session Manager.

Use the Security Module Status page to perform the following actions:

- **Reset :** Resets the security module for the selected Session Manager or Branch Session Manager. You can reset the security module when a connection cannot be made to the security module.

  Warning:

  Session Manager cannot process calls while the security module is resetting.

- **Synchronize:** Synchronize the administered configuration with the configuration information stored on the security module.
- **Connection Status:** Displays the current status of inbound and outbound links between the Session Manager security module and external hosts. The Connection Status page provides general-purpose monitoring and debugging activities such as:
  - identifying if Session Manager must be taken out of service.
  - determining if links are secure or not.
  - viewing link details and statistics.

Viewing the Security Module page

Possible causes for the Security Module status to be **Down** include:

- The security module may have recently been reset. A reset can take several minutes to complete.
- The security module may not have received security module configuration information from System Manager.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager**.
2. If the Security Module state of Session Manager does not display as **Up**:
   a. Click on the status text of the Security Module for Session Manager to display the Security Module Status page.
   b. Verify the IP address for Session Manager is correct.
   c. Select Session Manager.
   d. Click **Synchronize**.
   e. If the status remains **Down**, click **Reset**.

      Warning:

      Session Manager cannot process calls while the security module is being reset.

Security Module Status page field descriptions

Button	Description
Reset	Resets the selected Session Manager instance.
Synchronize	Synchronizes the security module of the selected Session Manager.
Connections Status	Displays the connection status information for the selected Session Manager instance.

Name	Description
Session Manager	List of administered Session Manager instances. A warning symbol after the name indicates the Session Manager or Branch Session Manager instance is in the **Maintenance Mode** service state.
Type	Type of Session Manager instance (SM or BSM).
Status	Status of the Security Module for Session Manager (up or down).
Connections	Total number of connections for the Security Module.
IP Address	The IP address of the security module used for SIP traffic. This field should match the address administered on the SIP Entity form for the Session Manager instance.
VLAN	The VLAN ID associated with the Security Module.
Default Gateway	The default Gateway used by the Security Module. This value should match the default gateway administered on the Session Manager instance form.
Entity Links (expected / actual)	The number of expected and actual Entity Links. The expected value is the number of configured SIP Entities in the Routing Policy that have Entity Links to Session Manager. The actual value is the number of Entity Links currently configured on the Security Module. These values should match. If these values do not match, there is a synchronization issue that you must investigate.
Certificate Used	Type of certificate in use.

Related links

SIP Firewall status on page 490

Connection Status

Use the Connection Status page to view the current status of inbound and outbound links between the Session Manager security module and external hosts. On the Connection Status page, you can perform general-purpose monitoring and debugging activities such as:

- Identifying if Session Manager needs to be taken out of service.
- Determining if links are secured or not.
- Viewing link details and statistics.

Monitoring Connection Links

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager**.
2. Click **System Status** > **Security Module Status**.
3. Select a system and click **Connection Status**.
4. Apply the required filters using the Connection Filter section. Select the **Non-Compliant NIST TLS Only** check box to display only the TLS connections that are not compliant with NIST standards.
5. Under Connection List, click **Apply Filter** to display the list of connection links.
6. Select a row and click **Show** to view detailed information about the selected connection.
7. Click **Return** to return to the Security Module Status page.

Connections Status field descriptions

Summary section

The Summary section displays the total number of Active Connections and the number of connections that are incoming, outgoing, TCP, and TLS.

Connection Filter section

Use the Connect Filter section to define a filter and to display the connection list based on the defined filters. A filter can be an FQDN or an IP Address and mask.

If you select **Non-compliant NIST TLS Only**, the page displays only the TLS connections having an algorithm that is not compliant with the NIST SP800-131A recommendation.

Connection List section

The Connection List table displays basic information of all the active connections. The following definitions apply to several of the fields:

- **A:** Acceptable. The algorithm and key length are safe to use. No security risk is currently known.
- **D:** Deprecated. The use of the algorithm and key length is allowed, but the user must accept some risk.

- **X:** Disallowed.
- **N:** Not approved.
- **R:** Restricted. The use of the algorithm or key length is deprecated, and there are additional restrictions required to use the algorithm or key length for applying cryptographic protection to data.
- **U:** Unknown. The system cannot determine the status.

Name	Description
Details	Show or hide the detailed information of the selected connection link.
Dir	Link direction (inbound or outbound).
Local Port	Local Security Module port.
Remote IP	Remote IP address.
Remote Port	Remote port.
Remote FQDN/IP	Remote FQDN or IP address.
Transport	Transport protocol (UDP, TCP, TLS).
Policy	Security Policy (Trusted, Default, Instance)
Cert Sign	Certificate Signature. Digital signature algorithms (for example, RSA or DSA) and the cryptographic hash function (for example, SHA) of the certificate in use by the TLS connection.
Key Exch	Key exchange algorithm (for example, RSA, DSA, Diffie-Hellman,) and key bit length (for example, 1024, 2048) to establish symmetric keys between the endpoints on the TLS connection.
Encryption	Cryptographic operation that provides confidentiality of the data being carried on the TLS connection.
MAC	Message Authentication Code algorithm (for example, SHA) that authenticates the TLS data and provides integrity and authenticity assurance on the message.

Connection Details section

The Connection Details section displays detailed information for the selected connection.

Name	Description
Direction	Link direction.
Creation time	Link creation time.
Last message received	Last message received time.
Last message sent	Last message sent time.
Messages/Bytes Received	Received message count and byte count.

Table continues…

Name	Description
Messages/Bytes Transmitted	Transmitted message count and byte count.
Messages/Bytes Dropped	Dropped message count and byte count.
Subject	The subject field identifies the entity associated with the public key stored in the subject public key field of the X.509 certificate.
Alt Subject	Alt subject is an extension to X.509 that allows various values to be associated with a security certificate.
CA	The issuer who signed the certificate.
Cipher	The negotiated TLS cipher suite. The cipher suite includes the Key Exchange, Encryption and MAC algorithms.
Public Key Algorithm	The encryption algorithm of the public key (e.g. RSA, DSA or Diffie-Hellman).
Key Size (bits)	The Public Key length.
q bits size	For DSA public keys, this represents the q parameter size.
Signature Algorithm	The identifier for the cryptographic algorithm used by the CA to sign this certificate.
MAC Algorithm	The Message Authentication Code (MAC) algorithm to verify data integrity.

SIP Firewall Status

Viewing SIP Firewall status

The SIP Firewall Status page displays the SIP Firewall processing status for each administered Session Manager and Branch Session Manager instance.

Procedure

On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **System Status** > **SIP Firewall Status**.

Auditing SIP Firewall configuration

You can perform periodic audit of Firewall configuration to ensure the functioning state of the SIP Firewall. The audit operation checks for Rule Set upgrades and imports the latest default Rule Sets. The system also performs the audit operation automatically at every 5 minutes.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **System Status** > **SIP Firewall Status**.
2. Click **Audit**

   The Rule Set Audit and Repair Status page displays the processing results for the Session Manager and Branch Session Manager instances.
3. Click **Done**.

SIP Firewall Status page field descriptions

Button	Description
Reset	Reset all the processing counters of the selected Session Manager and Branch Session Manager instances to zero, except for the **Loop Detection** counters. This action also resets all the Rule matching counts to zero. **Note:** After a reset operation, the system updates the counts from the last reset time.
Audit	Perform an audit of the Session Manager Rule Set assignments. The Audit process also checks for Rule Set upgrades and imports pending default Rule Sets.
Configure	Navigates to the SIP Firewall Configuration page.

Name	Description
Details	Displays the detailed SIP Firewall processing status for each Rule for the selected Session Manager. The details section displays a **Rule Matching table** with the following columns: • Rule: The name of the rule. • Match: The matched count of the Rule for the selected Session Manager. • Drop: The dropped count of the Rule for the selected Session Manager.
SM	The name of the Session Manager.
Type	The Session Manager type.
Rule Sets	The name of the Rule Set assigned to the Session Manager.
Reset Time	The last reset time of the SIP Firewall processing counts. **Note:** The reset time displays only displays for Session Manager and Branch Session Manager Release 6.3.4 and later.
Processing Counts	Displays the summary of counts for Rules, Whitelist, Blacklist, and Loop Detection. Loop Detection counts do not reset. To view the exact counts, mouse over the **Processing Counts** column. **Note:** The processing counts only display for Session Manager and Branch Session Manager Release 6.3.4 and later.

Related links

Viewing SIP Firewall status on page 495

Registration Summary

Use the Registration Summary page to view the registration status for all Avaya SIP Telephony (AST) devices registered for the selected Session Manager instance. The AST devices are reloaded or rebooted based on the following actions:

- Reset of endpoints.

- Full reload of endpoints.
- Partial reload of endpoints.
- Failback of endpoints to the primary controller.

Viewing Registration Summary

View basic registration information for a particular device.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **System Status** > **Registration Summary**.
2. Click **Refresh** to retrieve the latest Device Summary results.

Registration Summary field descriptions

Button	Description
Reboot	Reboot the selected Avaya SIP Telephony (AST) devices.
Reload Complete	Force complete reload of the selected AST devices.
Reload Config	Reload only the configurations of the selected AST devices.
Reload Contacts	Reload only the contacts of the selected AST devices.
Failback	Ensure that devices failback to Primary Session Manager.

Name	Description
Session Manager	Name of the Session Manager instance. A warning symbol indicates the instance is in the **Maintenance Mode** service state.
Type	Type of Session Manager instance (SM or BSM).
Primary Registered	Number of users registered to this Session Manager as the primary Session Manager.
Primary AST	Number of PPM subscriptions to this Session Manager for users as the primary Session Manager.

Table continues…

Name	Description
Primary Admin	Number of users administered to use this Session Manager as the primary Session Manager. **Note:** A Session Manager instance of type **BSM** does not have any registration status entries in the Primary column group. The system displays the status as “---”.
Secondary Registered	Number of users registered to this Session Manager as the secondary Session Manager.
Secondary AST Failover	Number of PPM subscriptions to this Session Manager for users as the secondary Session Manager. This also indicates the failover users since failover users subscribe to the secondary Session Manager.
Secondary Admin	Number of users administered to use this Session Manager as the secondary Session Manager.
Total Registered	Total number of **Primary Registered** and **Secondary Registered** users.
Total AST	Total number of **Primary AST** and **Secondary AST Failover** users.
Total Admin	Total number of **Primary Admin** and **Secondary Admin** users.

Rebooting of selected AST devices

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **System Status** > **Registration Summary**.
2. Select the AST Device and click **Reboot**.
3. On the Confirm Reboot Notification page, click **Confirm**.

   The screen refreshes with a status page containing detailed information regarding the current state of scheduled and running endpoint actions.

Reloading of selected AST devices

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **System Status** > **Registration Summary**.

2. Click the rows to select SIP AST devices and do one of the following:
   - Click **Reload** > **Reload Complete** to force a complete reload of the selected SIP AST devices for all data.
   - Click **Reload** > **Reload Config** to reload only the configuration information of the selected SIP AST subscribed devices.
   - Click **Reload** > **Reload Contacts** to reload only the contact information of selected SIP AST subscribed devices.
3. Click **Confirm** on the confirmation page.

   The screen refreshes with a status page containing the information regarding the current state of scheduled and running endpoint actions.

Failback of selected AST devices

Procedure

1. On the home page of the System ManagerWeb Console, under **Elements**, click **Session Manager** > **System Status** > **Registration Summary**.
2. Click to select the AST Devices and click **Failback**.
3. On the Confirm Failback Notification page, click **Confirm**.

Advanced searching

Procedure

1. Click the **Advanced Search** in the upper-right corner of the page.
2. Select the search criterion from the first drop-down menu.
3. Select the operator from the second drop-down menu.
4. Enter the search value in the third field.
5. To add another search condition, click the plus sign (+).
6. To delete a search condition, click the minus sign (-) .
7. Do one of the following:
   - Click **Clear** to clear the fields.
   - Click **Search** to search using the entered search criteria.
   - Click **Close** to return to the Registration Summary page.

User Registrations

Use the User Registrations page to send notifications to the selected SIP AST devices and display the summary of the user registration status for the SIP AST Device based on the following actions:

- Forced termination of registrations for selected devices
- Reset of selected devices
- Full reload of selected devices
- Only reload configuration for selected devices
- Only reload contacts for selected devices
- Failback of devices to the primary controller

Viewing User Registrations

View the basic registration information for a particular user or groups of users.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **System Status** > **User Registrations**.
2. Click **View** and select the one of the viewing options form the drop-down menu.
3. To view detailed information for an individual user, select the user and click the **Show** link.
4. Click **Refresh** to retrieve the latest user registration summary results.

User Registrations field descriptions

Customize Column Display section

List	Description
Available Columns	Displays the list of available columns.
Display Columns	Displays the list of selected columns.

Link	Description
Customize	Expand the **Customize Column Display** section.
Move	Move selected items from the **Available Columns** list to the **Display Columns** list.
Move All	Move all items from the **Available Columns** list to the **Display Columns** list.

Table continues…

Link	Description
Remove	Remove selected items from the **Display Columns** list.
Remove All	Remove all items from the **Display Columns** list.
Top	Move the selected item in the **Display Columns** list to the top of the list.
Up	Move the selected item in the **Display Columns** list to one position up in the list.
Down	Move the selected item in the **Display Columns** list to one position down in the list.
Bottom	Move the selected item in the **Display Columns** list to the bottom of the list.

Button	Description
Default	Restore the default column settings in the **Available Columns** and **Display Columns** lists.
Export	Export the SIP registration data to the CSV or XML file.
Apply	Apply the changes made in the column customizing lists to the AST Device Notifications section.
Close	Collapse the **Customize Column Display** section.

AST Device Notifications: section

The **As of (time)** label indicates the time of the last update of information for the **AST Device Notifications** section.

Button	Description
View > **Default**	View the current default view.
View > **User**	View the specific information of the user.
View > **Time Detail**	View the diagnosis of endpoint registration problems.
View > **Device**	View all available device information.
View > **Active Controller**	View registration information of the active controller Session Manager for AST devices. The system displays **AC** under the **Registered** column only for Avaya SIP devices that support PPM through the avaya-css-profile event subscription. Third party devices do not show an Active Controller indication.
View > **SM**	View which Session Manager instances are associated with the user registration.
View > **Customized**	View custom views.

Table continues…

Button	Description
View > **Create Customized**	Customize the display columns for viewing the user registration details.
Force Unregister	Force termination of registrations for selected devices.
Reboot	Reboot the selected AST devices.
Reload Complete	Force a complete reload of selected AST devices.
Reload Config	Reload configurations of the selected AST devices.
Reload Contacts	Reload contacts of the selected AST devices.
Failback	Enable devices to failback to Primary Session Manager.

Default View:

Name	Description
Details	Options for viewing the Registration Detailed section.
Address	SIP registration address.
First Name	Administered first login name.
Last Name	Administered last login name.
Actual Location	Name of the registration location.
IP Address	Indicates numeric IP address of the end point.
Remote Office	Indicates whether the incoming IP Address has been correlated with an administered **Remote Office - SIP Proxy Mapping**.
Shared Control	Indicates this registration, such as Avaya OneX Communicator, controls another endpoint.
Simultaneous Devices	Number of devices registered and the maximum administered devices.
AST Device	Indicates an AST device.
Registered Prim	Indicates as primary registration.
Registered Sec	Indicates as secondary registration.
Registered Surv	Indicates as survivable registration.

User View:

Name	Description
Details	Options for viewing the Registration Detailed section.
Address	SIP registration address.
Login Name	Administered user login name.

Table continues…

Name	Description
First Name	Administered first login name.
Last Name	Administered last login name.
Home Location	Name of the home location as assigned to the user in Session Manager Communication Profile.
IP Address	Indicates numeric IP address of the end point.
Simultaneous Devices	Number of devices registered and the maximum administered devices.
AST Device	Indicates an AST device.
Registered Prim	Indicates as primary registration.
Registered Sec	Indicates as secondary registration.
Registered Surv	Indicates as survivable registration.

Time Detail View:

Name	Description
Details	SOptions for viewing the Registration Detailed section.
Address	SIP registration address.
Login Name	Administered user login name.
IP Address	Indicates numeric IP address of the end point.
PPM Subscription Time (AC)	Indicates the subscription time for PPM services of AST endpoint.
Registration Time Prim	Indicates the registration time for the Primary Session Manager.
Registration Interrupted Prim	Indicates the last time when the registration was interrupted for the Primary Session Manager.
Registration Time Sec	Indicates the registration time for the Secondary Session Manager.
Registration Interrupted Sec	Indicates the last time when the registration was interrupted for the Secondary Session Manager.
Registration Time Surv	Indicates the registration time for the Survivable Session Manager.
Registration Interrupted Surv	Indicates the last time when the registration was interrupted for the Survivable Session Manager.

Device View:

Name	Description
Details	Options for viewing the Registration Detailed section.

Table continues…

Name	Description
Address	SIP registration address.
IP Address	Indicates numeric IP address of the end point.
Remote Office	Indicates whether the incoming IP address correlates with an administered Remote Office — SIP Proxy Mapping.
MAC Address	MAC address of the endpoint.
Device Vendor	Device information from PPM.
Device Type	Device information from PPM.
Device Model	Device information from PPM.
Device Version	Device information from PPM.
Simult. Devices	Number of devices registered to the maximum number administered.

Active Controller View:

Name	Description
Details	Options for viewing the Registration Detailed section.
Address	SIP registration address.
Login Name	Administered user login name.
Actual Location	Name of the registration location.
Active Controller	Name of the Active Controller
Registration Time (AC)	Indicates the registration time for the Active Controller.
Registration Interrupt Time (AC)	Indicates the time duration since the last interruption occurred for the Active Controller.
Registration Interrupted (AC)	Indicates the last time when the registration was interrupted for the Active Controller.
AST Device	Indicates an AST device.
Registered Prim	Indicates as primary registration.
Registered Sec	Indicates as secondary registration.
Registered Surv	Indicates as survivable registration.

SM View:

Name	Description
Details	Options for viewing the Registration Detailed section.
Address	SIP registration address.
Login Name	Administered user login name.

Table continues…

Name	Description
Home Location	Name of the home location as assigned to the user in Session Manager Communication Profile.
Actual Location	Name of the registration location.
Active Controller	Name of the Active Controller
Primary SM	Primary Session Manager of the user profile.
Secondary SM	Secondary Session Manager of the user profile.
Survivable SM	Survivable Session Manager of the user profile.
Registered Prim	Indicates as primary registration.
Registered Sec	Indicates as secondary registration.
Registered Surv	Indicates as survivable registration.

Customized View:

Name	Description
Details	Options for viewing the Registration Detailed section.
Address	SIP registration address.
Login Name	Administered user login name.
First Name	Administered first login name.
Last Name	Administered last login name.
Home Location	Name of the home location as assigned to the user in Session Manager Communication Profile.
IP Address	Indicates numeric IP address of the end point.
Simultaneous Devices	Number of devices registered and the maximum administered devices.
AST Device	Indicates an AST device.
Registered Prim	Indicates as primary registration.
Registered Sec	Indicates as secondary registration.
Registered Surv	Indicates as survivable registration.

`Create Customized view is same as Customize Column Display section as shown above.`

Details section

User Tab:

Name	Description
First Name	Administered first login name.
Last Name	Administered last login name.
Login Name	Administered user login name.

Table continues…

Name	Description
Registration Address	The Communication Address/handle user logged in with.
All Addresses	All of the SIP Communication Addresses the user has administered.
Home Location	Name of the home location as assigned to the user in Session Manager Communication Profile.
Actual Location	Name of the registration location.
Primary SM	Primary Session Manager of the user profile.
Secondary SM	Secondary Session Manager of the user profile.
Survivable SM	Survivable Session Manager of the user profile.
Simultaneous Devices	Number of devices registered to the maximum number administered.
ELIN Number	The ELIN sent from ELIN server associated with the primary controller for a user.
ELIN Last Updated	The date and time that the ELIN was last updated by ELIN server based on the location of Session Manager. Format is: www mmm dd hh:mm:ss TMZ yyyy", where: • www implies day of the week • mmm implies month • dd implies date • hh:mm:ss implies hour (military time):minutes:seconds • TMZ implies time zone • yyyy implies year For example, Fri Feb 11 15:56:36 MST 2011.

Registration Tab:

Name	Description
Registration Address	The Communication Address/handle user logged in with.
IP Address	Indicates numeric IP address of the end point.
Active Controller	Session Manager currently serving the endpoint SIP signaling and event subscriptions.
PPM Subscription Time (AC)	Indicates the subscription time for PPM services of AST endpoint.
Event Subscriptions	Event subscription details.

Table continues…

Name	Description
Instance Id	SIP User Agent Instance Id as URN (Uniform Resource Name):UUID (Universally Unique IDentifier).
Primary Registration Time	Indicates the registration time for the Primary Session Manager.
Primary Registration Interrupted Time	Indicates the time duration since the last interruption occurred for the Primary Session Manager.
Primary Registration Interrupted	Indicates the last time when the registration was interrupted for the Primary Session Manager.
Secondary Registration Time	Indicates the registration time for the Secondary Session Manager.
Secondary Registration Interrupted Time	Indicates the time duration since the last interruption occurred for the Secondary Session Manager.
Secondary Registration Interrupted	Indicates the last time when the registration was interrupted for the Secondary Session Manager.
Survivable Registration Time	Indicates the registration time for the Survivable Session Manager.
Survivable Registration Interrupted Time	Indicates the time duration since the last interruption occurred for the Survivable Session Manager.
Survivable Registration Interrupted	Indicates the last time when the registration was interrupted for the Survivable Session Manager.

Device Tab:

Name	Description
MAC Address	MAC address of the endpoint.
IP Address	Indicates numeric IP address of the end point.
Remote Office	Indicates whether the incoming IP address correlates with an administered Remote Office — SIP Proxy Mapping.
Remote Office SIP Proxy Name	Name of the SIP Proxy.
Active Controller	Name of the Active Controller
Event Subscriptions	Event subscription details.
AST Device	Indicates an AST device.
Device Vendor	Device information from PPM.
Device Type	Device information from PPM.
Device Model	Device information from PPM.
Device Version	Device information from PPM.

Simultaneous Tab:

Shows all other registrations associated with this user.

Name	Description
Address	Shows the SIP registration address.
Login Name	Shows the administered user login name.
IP Address	Indicates numeric IP address of the end point.
MAC Address	MAC address of the endpoint.

History Tab:

Shows up to 10 of the last device registrations performed by this user.

Name	Description
MAC Address	MAC address of the endpoint.
Vendor	Device information.
Type	Device information.
Model	Device information.
Version	Device information.

Customizing column display

About this task

You can customize the column display on the User Registrations page using one of the following methods:

- Select the columns you need to display in the table.
- Order the appearance of the columns.
- Reset the column appearance to the default columns.

Note:

The customization settings are valid for the current user session only. After the user logs out, the customization settings revert to the default appearance.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **System Status** > **User Registrations**.
2. Click the **Customize** link in the upper right of the table.
3. Use the following actions to customize the **Available Columns** and **Display Columns**:
   - **Move:** Select a column entry under **Available Columns** and move it to **Display Columns**.
   - **Move All:** Move all of the entries under **Available Columns** to **Display Columns**.

- **Remove:** Remove an entry from under **Display Columns**.
- **Remove All:** Remove all entries from under **Display Columns**.

4. To rearrange the selected columns under **Display Columns**:
   - Click **Top** to move the selected column to the top of the list.
   - Click **Up** to move the selected column one position up on the list.
   - Click **Down** to move the selected entry down one position on the list.
   - Click **Bottom** to move the selected column to the bottom of the list.
5. To restore the default settings, click **Default**.
6. To apply the changed settings, click **Apply**.
7. Click **Close** to close the customization section.

Exporting user registrations

About this task

Use this procedure to export and download SIP registrations data to a CSV or XML file format. You must schedule an export job if the registration records are more than 100,000.

Procedure

1. On the home page of the System Manager web console, in **Elements**, Click **Session Manager** > **System Status** > **User Registrations**.
2. On the User Registrations page, click **Export**.
3. Select a Session Manager instance.
4. Select **Export Format** and **Registrations for Export**.
5. To download the registrations data, click **Download Now**.
6. To schedule export job, click **Start Export Job**.

User registration export field descriptions

Name	Description
All registrations count	Displays the number of registrations on the selected job.
Current view registration count	Displays the number of registrations that are visible or selected on System Manager User Registrations page.

Table continues…

Name	Description
Export Format	Displays the format of the export job. The options are: • XML • CSV
Registrations For Export	Displays the selected registrations for export. The options are: • All • Current View

Button	Description
Download Now	To directly download the registration details in the XML or CSV file.
Start Export Job	To set a job for downloading user registrations. A link is created which can be used for downloading. When the status of job becomes Running, the link is ready to download
Done	To go back to the User Registrations page.

Forcing unregistration of device registration

About this task

This feature enables forced unregistration of any registered device and is not limited to only AST devices. These devices respond based on device settings.

Note:

Force unregistration of non-AST devices is not supported until the third party do not send the subscription for *reg event*.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **System Status** > **User Registrations**.
2. Select the device and click **Force Unregister**.
3. On the Confirm Force Unregister Notification page, click **Confirm**.

   The status page displays the detailed information of the unregistration action.

Rebooting of selected AST devices

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **System Status** > **User Registrations**.
2. Click select the AST Devices and click **Reboot**.
3. On the Confirm Reboot Notification page, click **Confirm**.

   The screen refreshes with a status page containing detailed information regarding the current state of scheduled and running endpoint actions.

Reloading of selected AST devices

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **System Status** > **User Registrations**.
2. Click the rows to select the SIP AST Devices and do one of the following:
   - Click **Reload** > **Reload Complete** to force a complete data reload of the selected SIP AST Devices.
   - Click **Reload** > **Reload Config** to reload only the configuration information of the selected SIP AST subscribed devices.
   - Click **Reload** > **Reload Contacts** to reload only the contact information of the selected SIP AST subscribed devices.
3. Click **Confirm** on the confirmation page.

   The screen refreshes with a status page containing the information regarding the current state of scheduled and running endpoint actions.

Failback of selected AST devices

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **System Status** > **Registration Summary**.
2. Select the users having AST Devices.
3. Click **Failback**.
4. On the Confirm Failback Notification page, click **Confirm**.

Advanced searching

Procedure

1. Click the **Advanced Search** in the upper-right corner of the page.
2. Select the search criterion from the first drop-down menu.
3. Select the operator from the second drop-down menu.
4. Enter the search value in the third field.
5. To add another search condition, click the plus sign (+).
6. To delete a search condition, click the minus sign (-) .
7. Do one of the following:
   - Click **Clear** to clear the fields.
   - Click **Search** to search using the entered search criteria.
   - Click **Close** to return to the Registration Summary page.

SIP Sessions count

The Session Manager Element Manager collects, monitors, and logs the number of concurrent SIP sessions in the system. Since the total number of session licenses used is equal to the number of concurrent SIP sessions, you can use the SIP sessions count feature to monitor and report the number of session licenses being used by the system.

The system raises an alarm for the following conditions:

- For a single occurrence of an event when the number of concurrent SIP INVITE sessions exceeds the authorized number of session licenses.
- If the number of concurrent SIP INVITE sessions in use continues to exceed the number of authorized licenses. For this condition, the system raises a new alarm once every 24 hours until either the number of concurrent SIP INVITE sessions is reduced below the number of authorized licenses or the number of authorized licenses is increased to be equal to or greater than the number of concurrent SIP INVITE sessions.

Note:

The system raises an alarm if a valid license file is not installed on the system.

The SIP sessions count functionality enables historical analysis of SIP sessions count data for the system or the selected Session Manager instance. Using the SIP session count function, you can:

- generate graphs of the analyzed data.
- export the analyzed data as a report in the comma separated value (CSV) or XML format.

Using the generated reports, you can conduct a time-based analysis of the license use of the system.

Related links

Viewing Session Count data on page 582
Exporting analyzed Session Count data on page 582
Session Counts field descriptions on page 582

Viewing Session Count data

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **System Status** > **Session Counts**.
2. In the **Session Manager** field, select the appropriate Session Manager instance.
3. Specify the date and time for the required period of the session counts data.
4. Click **Generate Graphs** to view the data in graphical format.

Related links

SIP Sessions count on page 581

Exporting analyzed Session Count data

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager** > **System Status** > **Session Counts**.
2. Select a Session Manager instance.
3. Specify the date and time for the required period of the session counts data.
4. Specify **Export Data Range** and **Export Data Format**.
5. Click **Download Data** to save a copy of the generated report.

Related links

SIP Sessions count on page 581

Session Counts field descriptions

Name	Description
Global Session Status as of	Indicates when the session count data was last updated.

Table continues…

Name	Description
Sessions Used	The number of SIP sessions currently used by the system.
Sessions Available	The number of SIP sessions authorized for usage by the system.
Session Manager	The Session Manager instance or all Session Manager instances for which session count data is desired.
Data Available	The period for which session count data is available.
Date and Time	The period of the session count data. Predefined values: 1. all dates and times • last month • last week • today • yesterday 2. Last: 1-99 Days or Hours 3. Between: Specified Date Range
Generate Graphs	Generates session count graphs based on specified parameters.
Export Data Range	The period for which session count data must be exported: • All – Retrieve all data for specified Session Manager. • Selected Range – Retrieve data based on the Date and Time field selection.
Export Data Format	The format of downloaded session count data: CSV or XML.
Download Data	Exports session count data based on the specified parameters.

Related links

SIP Sessions count on page 581

User Data Storage and Data Center management

Use the User Data Storage status screen to manage, monitor, backup, and restore User Data Storage on Session Manager instances.

User Data Storage stores the call logs, contacts and other user-related data for users associated with that Session Manager.

Note:

The User Data Storage backup is *not* related in any way to the System Manager backup.

Viewing User Data Storage Status

Note:

The system displays `No status details while in Maintenance Mode` for those instances that are in the **Maintenance Mode** service state.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **System Status** > **User Data Storage**.
2. Select the Session Manager instance for which you want the system to display the data.

Data Server Status field descriptions

The Data Server Status page displays the status of the User Data Storage data server. The page displays the last ten operation executions and results information.

The history details display the operations status such as:

- Start: the last time that the User Storage was started.
- Cluster: The Session Manager recently added to the database cluster.
- Uncluster: The Session Manager recently removed from the database cluster.
- Restore: The node of the database cluster was restored.
- Backup: On demand or nightly backup of the database cluster node.
- Audt: On demand or nightly audit of the database cluster node.
- Repair: On demand or automatic cluster consistency check and repair.

Name	Description
Details	The details of the last ten operation executions and result information for Session Manager. The most recent operations executed are presented first. Details of the status of User Store/Cassandra to access, read, and write data. **Note:** Operation history is not retained during a host restart. The operation history includes explicit, administrator requested operations, schedules operations, and psuedo-operations executed as a function of other system activities.
SM	Name of the core Session Manager. A warning symbol indicates the Session Manager is in the **Maintenance Mode** service state.
Release	Release of Session Manager. Releases prior to 6.3.8 do not support User Store. Releases prior to 7.0.1 do not support User Store in a clustered configuration.
Connect Test	Status of the maintenance connection test to the User Data Storage server.
Disk Usage	Cumulative disk usage for data storage.
Data Center	The data center that Session Manager is assigned to.
Cluster Status	Clustering details if Session Manager is a part of a storage cluster.

Button	Description
Audit	Audits the call history and remove entries for deleted users, users with deleted Session Manager Communication Profiles, and users who have been reassigned to another Session Manager. Compacts the data storage table after removing the affected files. Audit covers Call Log data, Contact data, and Session Manager data.
Repair	Repairs automatically under most circumstances and redistributes data around the cluster as needed. Supported on clustered Session Manager release 7.0.1 and later.

Administering Data Center

Adding data center

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **System Status** > **User Data Storage**.
2. On the User Data Storage page, click the **Data Center** tab, and then click **New**.

   The system displays the Edit Data Center page.
3. In the **Name** field, type the name of the data center.
4. In the **Description** field, type the description about the data center.
5. Click **Commit**.

   Note:

   A Warning message might display. However, the process is unaffected and you can proceed to add the data center.

Data Center page field descriptions

Name	Description
Data Center	The name of a data center.
Description	The description of a data center.
Details	The details of the Session Manager instances assigned to a data center.
# of assigned SMs	The number of core Session Manager instances assigned to a data center.
SM	The name of the core Session Manager assigned to a data center.
Description	The description of the core Session Manager.

Name	Description
New	Creates a new Data Center. Assigns Core Session Managers to any Data Center.
Edit	Modifies a Data Center name, description, or modifies assignment of Core Session Manager to any Data Center.
Delete	Deletes a data center if the data center is not assigned to a core Session Manager server.
View	Displays the read only view of Data Center.

Assigning Session Manager to a data center

Before you begin

Data Centers need to be added before the Session Manager assigning.

About this task

You can assign a Session Manager instance to a data center while adding a Session Manager instance or after adding the Session Manager instance using the **Edit** button.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **System Status** > **User Data Storage**.
2. On the User Data Storage page, click the **Data Center** tab.
3. Select a data center and click **Edit**.

   The system displays the **Edit Data Center** page.
4. To assign Session Manager to data center, under the **SMs unassigned or assigned to other Data Center** section, from the **Data Center** drop-down list, select the data center name.
   - If you select the same data center name for Session Manager, the system refreshes the page and displays the assigned data center under the **SMs in Data Center** section.
   - If you select the other data center name for Session Manager, the system displays the assigned data center under the **SMs unassigned or assigned to other Data Center** section.
5. Click **Commit**.

   The system displays the Confirm Data Center assignments page.
6. Verify the data center and SM assignment.
7. Click **Confirm**.

Unassigning data center to Session Manager

About this task

Unassign a Session Manager server from a data center as follows.

Note:

This procedure is only applicable to Session Manager servers that are not scheduled to be paired to AADS.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **System Status** > **User Data Storage**.
2. On the User Data Storage page, click the **Data Center** tab.
3. Select a data center and click **Edit**.

   The system displays the **Edit Data Center** page.
4. To un-assign data center to Session Manager, from the **Data Center** drop-down list, select the blank pulldown option.

5. Click **Commit**.

   The system displays the Confirm Data Center assignments page.

6. Verify the data center and SM assignment.
7. Click **Confirm**.

User Data Storage backup

Backups and audits run on a daily basis at 1:15 AM local time on the Session Manager server. The backup server audit removes extra backup files at 2:15 AM local time on System Manager.

The User Data Storage backup feature:

- is *not* related in any way to the System Manager backup.
- does not pre-allocate space. The administrator must administer a location for backup files. 4 GB of space is adequate for this release, but more space will need to be allocated over time.
- makes a backup directly from the Session Manager to the backup location.
- backs up call history data only.

If the user does not configure a backup server:

- a warning message displays until the user configures a backup server location.
- no backups are made.
- the status page displays that no backup server is configured.

Backup and Restore field descriptions

Use this screen to configure and monitor User Data Storage backups and recoveries. The backup server must be in place before configuring the backup information.

The fields display **- -**:

- If the system cannot retrieve the status of a Session Manager.
- If the Session Manager is running a release earlier than 6.3.8.

Name	Description
Backup Host	Name of the backup server.
File Transport	Type of file transport in use.
Directory	Location on the backup server to store the backup files.
Directory Disk Used	Amount of disk space used for the backup file
Retained Copies	Number of backup copies saved on the backup server per Session Manager.

Table continues…

Details	The details for a selected Session Manager (File Name, Backup Date, File Size, Session Manager Release).
SM	The name of the core Session Manager.
Release	The release of Session Manager.
Data Center	The data center to which Session Manager is assigned.
Backup Status	The status of the last backup (Complete or Failed).
Backup Files	The number of backup files that are stored on the backup server for the selected Session Manager.
Last Backup Time	The time a backup was last run on the selected Session Manager.
Last Restore Status	The status of the last Restore request on the selected Session Manager (Complete or Failed).
Last Restore Time	The time a restore request was last run on the selected Session Manager.

Button	Description
Backup	Start the backup process on the selected Session Managers.
Restore	Start the restore process on the selected Session Managers.
Configure Backup	Configure backup server location and directory for backup file storage.
Audit Backup	Audit the backup configuration, status, and directory. Provides an option to remove unnecessary files to reclaim disk space.

Administering Backup Storage Configuration

Use the Backup Storage Configuration screen to create or change the backup server configuration information.

Backups and audits run on a daily basis at 1:15 AM local time on the Session Manager server. The backup server audit removes extra backup files at 2:15 AM local time on System Manager.

Important:

The backup server must support the SSH2 protocol.

Warning:

If you change the server or backup file location directory using this screen, the existing backup files are not automatically moved to the new location and are not available for restoring. The administrator must move the backup files to the new location and remove files from the unused location.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **System Status** > **User Data Storage**.
2. Click **Backup and Restore**.
3. Click **Configure Backup**.
4. Enter the required information.
5. Do one of the following:
   - Click **Commit** to save the configuration changes.
   - Click **Test Connection** to verify the configuration information is correct.
   - Click **Cancel** to cancel the configuration request.

Backup Storage Configuration field descriptions

Name	Description
Hostname or IP Address	The hostname or IP address of the SSH-accessible server.
Login	The login that has SSH privileges and can gain access to the server.
Password	The password associated with the login.
Confirm Password	The confirmation of the password.
Backup File Transfer	The file transfer protocol to be used. The default is SFTP. SCP is a slightly faster transport but can be affected by interrupts.
SSH Port	The SSH port used. The default is 22.
Directory	The directory location where backup files are stored on the backup server.
Retained backup copies per SM	The maximum number of backup file copies retained for each Session Manager on the backup location.

Button	Description
Commit	Accepts and stores the configuration changes to the database.
Test Connection	Tests the SSH connection, directory access for the login, and write/delete permissions.
Cancel	Makes no changes to the existing configuration information.

Backing up user data storage

About this task

Use this procedure to run a backup immediately. Running the backup on demand does not alter the nightly backup schedule.

Procedure

1. On the Home page of the System Manager web console, in **Elements**, click **Session Manager** > **System Status** > **User Data Storage**.
2. Click **Backup and Restore**.
3. Select the Session Manager or multiple Session Manager instances on which you want to run the backup.
4. Click **Backup**.
5. Click **Confirm**.

Restoring user data storage

The restore operation:

- Only restores call history information that exists in the backup file.
- Deletes call history information that exists only in the database.

Procedure

1. On the Home page of the System Manager web console, in **Elements**, click **Session Manager** > **System Status** > **User Data Storage**.
2. Click **Backup and Restore**.
3. Select the Session Manager on which to run the restore operation.
4. Click **Restore**.
5. In the **Restore File** column, select the appropriate file you want to restore from the drop-down menu.
6. Do one of the following:
   - Click **Commit** to accept the selection.
   - Click **Reset** to reload the **Restore File** selection list.
   - Click **Cancel** to cancel the restore request and return to the User Data Storage screen.
7. Click **Confirm** to send a request to each Session Manager to begin the restore operation using the selected file, or click **Cancel** to cancel the restore request.

Auditing a Backup Storage Location

The audit runs on the backup server and provides a summary status of the backup server and files.

The Audit Backup Storage Location screen also displays the files which will be removed in the next nightly audit. If not enough disk space is currently available, the administrator can click **Remove Pending** to immediately remove the pending files on the backup server.

Backups and audits run on a daily basis at 1:15 AM local time on the Session Manager server. The backup server audit removes extra backup files at 2:15 AM local time on System Manager.

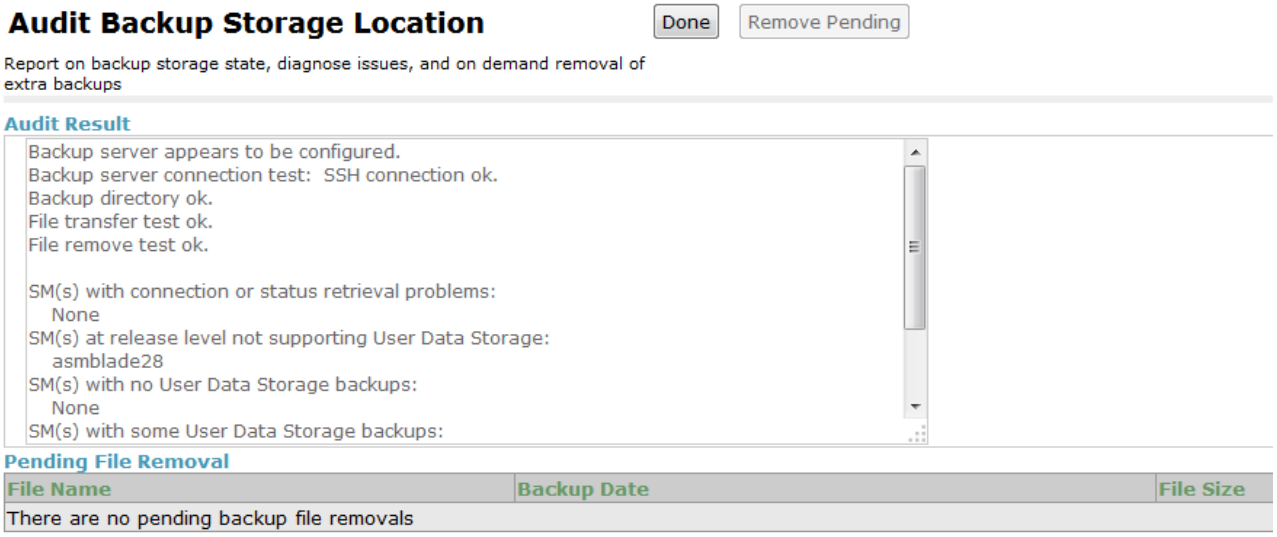
Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **System Status** > **User Data Storage**.
2. Click **Backup and Restore**.
3. Select a Session Manager from the **SM** list.
4. Click **Audit Backup**.

   The system displays the results of the audit.
5. To immediately remove any files listed under **Pending File Removal**, click **Remove Pending**.
6. Click **Done**.

Example

The audit displays results similar to the following:



Chapter 10: System Tools

Session Manager maintenance tests

Use the Maintenance Tests page to perform tests on System Manager server and the administered Session Manager instances. The tests verify functionality such as network connectivity, data replication, and database operation.

The system runs the tests periodically in the background to monitor the status of system components. You can also run the tests on demand.

Note:

Tests can fail if the server under test is out of service or is not responding.

Maintenance Tests page field descriptions

Name	Description
Select System Manager or Session Manager to test:	Select System Manager or a Session Manager from the drop-down menu on which to perform the maintenance tests.

Button	Description
Execute Selected Tests	Run the selected maintenance tests on System Manager or the selected Session Manager.
Execute All Tests	Run all the maintenance tests on System Manager or the selected Session Manager.

Name	Description
Test Description	Description of the test.
Test Result	The outcome of executing the test (pass or fail).
Test Result Time Stamp	The last time the test was run.

Note:

The system loads Maintenance test data asynchronously in the background. The system displays the message **Loading..** when data is loading in the background. The system displays the message **Loading Complete** when data loading finishes. If the wait time exceeds a

certain limit, the system displays the message **Loading failure. Please try again.** and requests the user to try again later.

Running maintenance tests

Run the maintenance tests on System Manager or any administered Session Manager or Branch Session Manager.

Procedure

1. On the System Manager Web Console, under **Elements**, click **Session Manager** > **System Tools** > **Maintenance Tests**.
2. In the **System Manager or a Session Manager to test** field, select **System Manager**, a Session Manager instance, or a Branch Session Manager instance from the drop-down menu.
3. Do one of the following:
   - To run all the tests, select **Execute All Tests**.
   - To run only certain tests, select the tests you want to run and click **Execute Selected Tests**.
4. Verify the tests pass.

Maintenance Test descriptions

Test Call Processing status

This test checks the call processing functionality for a particular Session Manager instance. If call processing is working correctly, the test passes. If the test fails, contact Avaya Technical Support.

Test data distribution and redundancy link

This test only runs on Session Manager. This test verifies the Session Manager data share mechanism is functioning properly by sending a test string to each configured Session Manager. Each Session Manager saves the test string Session Manager within its respective database. After a short wait, the system queries each Session Manager for the test string value.

The test passes if each Session Manager returns the correct value.

A test failure indicates a potential failure of link redundancy and Session Manager pass-through capabilities that could impact call processing and Call Admission Control.

Test host name resolution of each Session Manager

This test only runs on System Manager. The test verifies that the DNS server can resolve the host name of each configured Session Manager.

If the DNS server can resolve the host name for each Session Manager, the test passes. Otherwise, the test fails. Check for the following possible causes:

- The Session Manager host name is incorrect on the DNS server.
- The Session Manager host name is missing on the DNS server.

Test management link functionality

This test checks the administrative link to the Session Manager. If the test fails, administrative changes cannot take effect on Session Manager.

Test Postgres database sanity

This test runs on either System Manager or a Session Manager.

System Manager tests the functionality of the master database.

The Session Manager tests the functionality of the local instance database.

If the test fails, contact Avaya Technical Support.

Test sanity of Secure Access Link (SAL) agent

This test can run on either System Manager or Session Manager. The test checks if the Security Access Link agent is running on the server. If the link is up and running, the test passes.

If the test fails, see the troubleshooting procedure for this test in *Troubleshooting Avaya Aura® Session Manager*.

Test Security Module Status

This test queries the status of the Security Module on a specified Session Manager. If the query is successful, the test passes. Otherwise, the test fails.

Test network connections to each Session Manager

The Network Connections test runs only on System Manager. This test verifies the connectivity to each administered Session Manager.

If connectivity is up for each Session Manager, the test passes. If connectivity is down, the test fails. The following are possible causes of test failure:

1. An upgrade or install is in progress.
2. The server might be out of service. Check the log for an event code. If an event code exists, check the Log Event Codes in *Troubleshooting Avaya Aura® Session Manager* for the appropriate troubleshooting action.
3. The network might be out of service. Run a ping test between System Manager and the failing Session Manager to verify network connectivity.

Test User Data Storage sanity

Note:

This test is not available for:

- Branch Session Manager instances
- Session Manager instances that are running a release earlier than 6.3.8.

This test checks the status of the **Cassandra** application and the connectivity to the **Cassandra** database. The test passes if the application and the connectivity are operating correctly. The test fails otherwise.

Tracer Configuration

Use the Tracer Configuration page to configure the tracing of:

- incoming SIP messages through the security module.
- SIP messages outgoing from the security module.
- messages dropped by ASSET proxy or by the SIP firewall.

You can also filter these messages based on the user or the call. Session Manager logs all the traced messages to a file based on the configuration.

Tracer Configuration page field descriptions

Tracer Configuration

Name	Description
Tracer Enabled	Enable or disable SIP message tracing. The default is enabled.
Trace All Messages	Enable or disable SIP message tracing for all SIP messages.
From Network to Security Module	Enable or disable SIP message tracing for ingress calls sent to the Session Manager instance from the network.
From Security Module to Network	Enable or disable SIP message tracing for egress calls originating from the Session Manager instance and sent to the network.
From Server to Security Module	Enable or disable tracing of local SIP messages originating from the Session Manager instance.

Table continues…

Name	Description
From Security Module to Server	Enable or disable tracing of local SIP messages originating from the security module.
Trace Dropped Messages	Enable or disable tracing of messages from calls dropped by the SIP firewall as well as the SM100 proxy.
Max Dropped Message Count	If **Trace Dropped Messages** is enabled, this field displays the value of the maximum number of traced dropped messages.
Send Trace to a Remote Server	Enable or disable SIP Tracing to an external host. When enabled, Session Manager sends all the (decrypted) SIP traffic to an external host. Session Manager uses the Syslog protocol for sending the SIP traffic (as used currently for SIP Tracing).
Remote Server FQDN or IP Address	FQDN or IP address of the remote syslog server.
Send Trace Method	Method to transfer syslogs: • Syslog (unsecured UDP) : Traffic is sent without being encrypted to a remote server as specified in the **Remote Server FQDN or IP Address** field using the default syslog port. • Stunnel (encrypted TCP) : Traffic is sent as encrypted to a remote server that is specified in the to **Remote Server FQDN or IP Address** field using the port specified in **Stunnel Port**.
Stunnel Port	Port number on which the stunnel of the remote server is listening. Stunnel provides several modes for far-end certificate validation.

User Filter

Button	Description
New	Create a new filter for filtering SIP messages based on the users. You can define a maximum of three user filters.
Delete	Delete a selected user filter or filters.

Name	Description
From	Filter SIP messages based on the user from whom the message is sent. Type the user string. For example, a rule to trace all messages from user “pqr”: to=”” from=”pqr” stop-count=50

Table continues…

Name	Description
To	Filter SIP messages based on the user to whom the message is sent. For example, to create a rule to trace all messages to user “xyz”: to=”xyz” from=”” stop-count=50
Source	Filter SIP messages based on the source address.
Destination	Filter SIP messages based on the destination address.
Max Message Count	Value for the maximum number of messages matching the filter that the Session Manager should trace. The default is 25 messages.

Call Filter

Button	Description
New	Create a new filter for filtering all SIP messages that start a new call. You can define a maximum of three call filters.
Delete	Delete a selected call filter or filters.

Name	Description
From	Filter SIP messages from a specific user. Call tracing identifies a call by capturing the Call ID from the first message that matches the **From** filter, thereafter tracing all the messages that have the matching call ID. For example, to create a rule to trace all messages related to a CALL from user “pqr”: to=”” from=”pqr” request-uri=”” stop-count=50
To	Filter SIP messages based on the user to whom the message is sent. Call tracing identifies a call by capturing the Call ID from the first message that matches the To filter, thereafter tracing all the messages that have the matching call ID. For example, a rule to trace all messages related to a CALL to user “xyz”: to=”xyz” from=”” request-uri=”” stop-count=50
Source	Filter SIP messages based on the source address.
Destination	Filter SIP messages based on the destination address.

Table continues…

Name	Description
Max Call Count	Value for maximum number of messages matching the filter that the Session Manager should trace. The default is 25 messages.
Request URI	Filter calls based on the called party (URI address). A valid Request URI format, for example, is .@192.111.11.

Session Manager Instances

Name	Description
Name	Select one or more configured Session Manager instances for which the specific filters should be used. **Note:** If you select only one Session Manager from this list, the **Read** button is activated. You can click this button to retrieve the current Trace Configuration information for the selected Session Manager. A warning symbol indicates the Session Manager instance is in the **Maintenance Mode** service state.

Button	Description
Commit	Save the configuration changes.
Read	Retrieves the current Trace Configuration details for the selected Session Manager and display that within the Trace Configuration page.

SIP Tracing

Use the SIP tracer to trace SIP messages exchanged between the Session Manager server and remote SIP entities. SIP messages that are dropped by any of the components such as SIP Firewall are also logged by the SIP tracer. You can trace all the messages belonging to a user, for a call, or for a selected Session Manager instance.

The SIP tracer user interface has the following components:

- **Tracer Configuration** defines the characteristics of messages to be traced for the capturing engine in the security module.
- **Trace Viewer** displays the captured SIP messages.

Trace Viewer page field descriptions

Filter

Name	Description
From: Date	Date from which you want to filter the trace logs.
From: Time	Time from which you want to filter the trace logs.
From: Time Zone	Time Zone for the From date that you want to use for filtering trace logs.
To: Date	Date up to which you want to filter the trace logs.
To: Time	Time up to which you want to filter the trace logs.
To: Time Zone	Time Zone for the To date that you want to use for filtering trace logs.
Name	Name of the Session Manager instance.

Trace Viewer

Button	Description
Dialog Filter	Filter trace log entries. This option filters trace log entries and displays entries for the same Call ID, From, and To fields as the trace log that you select. **Note:** You can also click Filter: **Enable** to filter log entries based on a value or to sort them based on selected columns.
Clear Dialog Filter	Clear the filtering of the trace using Dialog Filter and displays all trace log entries.
Hide dropped messages	Hide dropped messages from the trace log entries.
More Actions > Export Trace Viewer Overview	Create a tabulator-separated plain text file with all of the overview columns of the Trace Viewer page. You can open this file with editors such as Wordpad and Excel. The **More Actions** button is active only if trace records are listed. The retrieved Trace Viewer list can be saved into a file at the client side.
More Actions > Export Trace Viewer Details	Create a plain text file with the details of the Trace View records. The **More Actions** button is active only if trace records are listed. The retrieved Trace Viewer list can be saved into a file at the client side.

Name	Description
Details	Display the complete message. Clicking the Show arrow displays the message.

Table continues…

Name	Description
Time	Timestamp when the trace record was written. The timestamp entry displays the date and time zone.
Tracing Entity	Host name of the system from where the Security Module logged the trace.
From	URI from where the traced SIP message originated.
Action	Action of the traced SIP message such as INVITE, ACK, or BYE. The SIP message action is surrounded by an arrow to indicate the direction of the action. For example, -- INVITE -> or <- BYE --. Dropped messages have a leading DROPPED, for example, -- DROPPED ACK ->
To	URI to which the traced SIP message was sent.
Protocol	Protocol used by the traced SIP message such as TCP, UDP, or TLS.
Call ID	Call ID of the traced SIP message.

Button	Description
View	Generate the trace log output for the selected Session Manager instances for the selected date range. **Note:** The number of retrieved records displays the number of records that matched the filter criteria. If Session Manager displays fewer records than this number, not all the matching records are being displayed to avoid problems caused by running out of memory. In these cases, you can further configure or refine the filter criteria in such a way that all the log entries are displayed.
Clear	Clear all the selections made on the Trace Viewer page.

Call Routing Test

The Call Routing Test tests the routing of a SIP INVITE based on the current Session Manager administration options. You can use the test to:

- Verify the Session Manager administration is correct before placing the Session Manager into service.
- Troubleshoot why a certain type of call is not being routed as expected.

The Call Routing Test does not send SIP messages. The test invokes call processing using the debugging mode to test routing.

Related links

Call Routing Test page field descriptions on page 602

Call Routing Test page field descriptions

Name	Description
Calling Party URI	SIP URI of the calling party. You must specify a handle and a domain, for example, 5552000@domain.com. You can also specify a full URI such as sip:5555555@domain.com:5060;sometag=3;otherta g=4. You can also copy a URI recorded in a SIP trace and use it. The **Calling Party URI** field accepts: • IPv4 address • FQDN or Hostname • IPv6 address enclosed in square brackets ([]) You can enter IPv6 addresses only if the **Enable IPv6** field on the Session Manager Administration screen is selected. • String and @ followed by a valid IPv6 address enclosed in [] For example, 5552000@[2001:cdba::3257:9652].
Calling Party Address	IP address from which the INVITE is received. The **Calling Party Address** field accepts: • IPv4 address • IPv6 address **Note:** You can enter IPv6 addresses only if the **Enable IPv6** field on the Session Manager Administration screen is selected.

Table continues…

Name	Description
Called Party URI	SIP URI of the called party. You must specify a handle and a domain, for example, sip:5551000@companydomain.com. You can also specify a full URI such as sip:5555555@domain.com:5060;sometag=3;otherta g=4. You can also copy a URI recorded in a SIP trace and use it. The **Called Party URI** field accepts: • IPv4 address • FQDN or Hostname • IPv6 address enclosed in square brackets ([]) You can enter IPv6 addresses only if the **Enable IPv6** field on the Session Manager Administration screen is selected. • String and @ followed by a valid IPv6 address enclosed in [] For example, 5552000@[2001:cdba::3257:9652].
Session Manager Listen Port	Port on which the called Session Manager instance receives the INVITE.
Day of Week	Day of the week. Call times can influence routing policies.
Time (UTC)	Time. Call times can influence routing policies.
Transport Protocol	The transport protocol used by the calling party, which may impact routing options. This field is used for testing the routing based on entity links.
Called Session Manager Instance	The Session Manager instance that receives the initial INVITE from the calling party. **Note:** These are only core Session Manager instances. A Session Manager name in light gray text indicates the Session Manager instance is in the **Maintenance Mode** service state. You cannot run the Call Routing Test on Session Manager instances that are in **Maintenance Mode**.

Button	Description
Execute Test	Carries out the routing test based on the parameters that you provide. The **Routing Decisions** field displays the result of the routing test. The result displays one line per destination choice. For a destination that has alternate routing choices available, the result displays one line per alternate routing choice, and the lines are displayed in the same order that the test attempted to test the destinations. Each line displays not only where the INVITE would be routed, but also what the adapted digits and domain would be. The **Routing Decision Process** field contains information about how the Session Manager made the routing decisions. This tool allows you to test your routing administration.

Related links

Call Routing Test on page 601

SNMP Management Information Base

SNMP MIB Download

Administrators can download a zip archive file containing the definitions of SNMP MIBs, alarm traps, and informs that are supported by Session Manager. SNMP MIBs can be used by Network Management Systems (NMS) supporting any version of Session Manager. For example, MIBs downloaded from a Session Manager 6.3.2 Element Manager can be used by an NMS supporting Session Manager 6.2.

Important:

The System Manager software version must always be the same or greater than the software version of each of the Session Manager instances in the system.

The downloaded Session Manager SNMP MIBs zip archive file contains the current versions of the following MIB files:

- Standard MIBs
  - HOST-RESOURCES-MIB.my
  - If-mib.my

- INADS-MIB.my
- SNMPv2-MIB.my
- Tcp-mib.my
- Udp-mib.my

• Session Manager enterprise specific MIBs

- SM-CommonAlarmDef-Data.my
- SmSecMod-CommonAlarmDef-Data.my
- SmSIPAS-CommonAlarmDef-Data.my
- SmThirdPrty-CommonAlarmDef-Data.my
- SMELEM-CommonAlarmDef-Data.my

For information about SNMP support for Session Manager, see *Maintaining Avaya Aura® Session Manager*.

Downloading SNMP MIBs

Download a zipped copy of the SNMP MIBs related to Session Manager that the system currently supports.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager** > **System Tools** > **SNMP MIB**.
2. Click **Download**.
3. In the **Save As** dialog box, specify the file name and the location for saving the MIB zip archive file.

   The system displays the message that the MIB file was successfully saved in the specified location. If an error occurs, the system displays the reason for the unsuccessful download attempt.

SNMP MIB Download page field descriptions

Name	Description
File Name	Name of the Download file.
Description	Information regarding the file.
Action	Download the file.

Chapter 11: Performance

Call Counts

Use the call count data of a selected SIP entity to:

- Generate graphs of the analyzed data.
- Export the analyzed data as a report in CSV (comma separated value) or XML format.

Related links

Call Counts Report Types on page 607

Viewing call counts data

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager** > **Performance** > **Call Counts**.
2. Select the required SIP entity.

   Session Manager is not supported as the SIP entity.
3. Specify the date and time for the required period of the call counts data.
4. Select the appropriate tab and click **Generate Graphs** to view the data in graphical format.

Related links

Call Counts field descriptions on page 607

Exporting analyzed call counts data

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager** > **Performance** > **Call Counts**.
2. Select the required SIP entity.

   Session Manager is not supported as the SIP entity.
3. Specify the date and time for the required period of the call counts data.

4. Select the required tab and specify the **Export Data Range** and **Export Data Format**.
5. Click **Download Data** to save a copy of the generated report.

Related links

Call Counts field descriptions on page 607

Call Counts Report Types

Report Name	Report Details
SIP call count	• Active “other” SIP calls per SIP entity. • Active fax SIP calls per SIP entity. • Active text SIP calls per SIP entity. • Active video SIP calls per SIP entity. • Active audio SIP calls per SIP entity. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.

Related links

Call Counts on page 606

Call Counts field descriptions

Name	Description
SIP Entity	SIP Entity for which call counts data is desired. Session Manager is not supported as the SIP entity.
Data Available	Period for which performance data is available.

Table continues…

Name	Description
Date and Time	Period for which call counts data should be retrieved: • Predefined Values: - all dates and times - last month - last week - today - yesterday • Last: 1-99 Days or Hours • Between: Specified Date Range
Generate Graphs	Generate call counts graphs based on specified parameters.
Export Data Range	Period for which call counts data should be exported: • **All :** Retrieve all data for specified SIP entity. • **Selected Range:** Retrieve data based on the **Date and Time** field selection.
Export Data Format	Format of downloaded call counts data: CSV or XML.
Download Data	Export call counts data based on specified parameters.

Related links

Viewing call counts data on page 606
Exporting analyzed call counts data on page 606

Location Performance

Use the bandwidth usage information for the selected location to:

- Generate graphs of the analyzed data.
- Export the analyzed data as a report in CSV (comma separated value) or XML format.

Related links

Location Performance Report Types on page 610

Viewing location performance data

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Performance** > **Location Performance**.
2. Select the appropriate location.
3. Specify the date and time for the required period of the bandwidth usage data for the selected location.
4. Select the appropriate tab.
5. Click **Generate Graphs** to view the data in graphical format.

Related links

Location Performance field descriptions on page 610

Exporting analyzed location performance data

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager** > **Performance** > **Location Performance**.
2. Select the required location.
3. Specify the date and time for the required period of the location performance data.
4. Select the required tab and specify the **Export Data Range** and **Export Data Format**.
5. Click **Download Data** to save a copy of the generated report.

Related links

Location Performance field descriptions on page 610

Location Performance Report Types

Report Name	Report Details
Bandwidth Usage	• Multimedia bandwidth allocated per location. • Audio bandwidth allocated per location. • Total bandwidth available per location. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.
Bandwidth Available	• Total bandwidth available per location. • Multimedia bandwidth available per location. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.
Call Counts	• Count of calls totally rejected or denied due to insufficient bandwidth per location. • Count of downgraded calls where quality was reduced due to insufficient bandwidth per location. • Count of completed calls per location. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.

Related links

Location Performance on page 608

Location Performance field descriptions

Name	Description
Location	Generate a graph or export bandwidth usage information for the selected location.
Data Available	Period for which performance data is available.

Table continues…

Name	Description
Date and Time	Period for which bandwidth usage data can be retrieved: • Predefined Values: - All dates and times - Last month - Last week - Today - Yesterday • Last: 1-99 Days or Hours • Between: Specified Date Range
Generate Graphs	Generate bandwidth usage graphs based on specified parameters.
Export Data Range	Period for which bandwidth usage data should be exported: • All : Retrieve all data for specified location. • Selected Range : Retrieve data based on the **Date and Time** field selection.
Export Data Format	Format of downloaded bandwidth usage data: CSV or XML.
Download Data	Export bandwidth usage data based on specified parameters.

Related links

Viewing location performance data on page 609
Exporting analyzed location performance data on page 609

SIP Performance

Use the Session Manager SIP performance data to:

- Generate graphs of the analyzed data
- Export the analyzed data as a report in CSV (comma separated value) or XML format.

You can use the generated reports for capacity planning, system diagnostics, and so on.

Note:

- Performance data can be collected for Session Manager 6.1 and later releases.

- The system collects performance data based on a sample frequency of 5 minutes for the displayed parameters.

Performance report acronym definitions

The SIP performance reports use the following acronyms:

- Mps – Messages per second
- GMps – giga Messages per second (10^9)
- MMps – mega Messages per second (10^6)
- kMps – kilo Messages per second (10^3)
- mMps – milli Messages per second (10^-3)
- uMPS – micro Messages per second (10^-6)
- nMps – nano Messages per second (10^-9)

Related links

SIP Performance Report Types on page 613

Viewing SIP performance data

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager** > **Performance** > **SIP Performance**.
2. Select the Session Manager instance you want to view.
3. Specify the date and time for the required period of the SIP performance data.
4. Select the appropriate tab and click **Generate Graphs** to view the data in graphical format.

Related links

SIP Performance field descriptions on page 616

Exporting analyzed SIP performance data

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Session Manager** > **Performance** > **SIP Performance**.
2. Select a Session Manager instance.
3. Specify the date and time for the required period of the SIP performance data.
4. Select the required tab and specify the **Export Data Range** and **Export Data Format**.
5. Click **Download Data** to save a copy of the generated report.

Related links

SIP Performance field descriptions on page 616

SIP Performance Report Types

Total Tab

Report Name	Report Details
Trusted SIP Entities – SIP traffic	• Total SIP messages transmitted from a trusted SIP entity per Session Manager. • Total SIP messages received by a trusted SIP entity per Session Manager The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.
Trusted SIP Entities – SIP requests and responses	• Total SIP requests transmitted from a trusted SIP entity per Session Manager. • Total SIP requests received by a trusted SIP entity per Session Manager. • Total SIP responses transmitted from trusted SIP entity per Session Manager. • Total SIP Responses received by trusted SIP entity per Session Manager. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.
Trusted SIP Entities – SIP errors	• Total Security Module drops on trusted SIP entity per Session Manager. • Total Transmission Errors on trusted SIP entity per Session Manager. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.
Default Policy SIP devices – SIP traffic	• Total SIP messages transmitted from an untrusted SIP entity per Session Manager. • Total SIP messages received by an untrusted SIP entity per Session Manager. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.

Table continues…

Report Name	Report Details
Default Policy SIP devices – SIP requests and responses	• Total SIP requests transmitted from an untrusted SIP entity per Session Manager • Total SIP requests received by an untrusted SIP entity per Session Manager. • Total SIP responses transmitted from an untrusted SIP entity per Session Manager. • Total SIP Responses received by an untrusted SIP entity per Session Manager. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.
Default Policy SIP devices – SIP errors	• Total Security Module drops on an untrusted SIP entity per Session Manager. • Total Transmission Errors on an untrusted SIP entity per Session Manager. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.
SIP call count	• Active “other” SIP calls per Session Manager. • Active fax SIP calls per Session Manager. • Active text SIP calls per Session Manager. • Active video SIP calls per Session Manager. • Active audio SIP calls per Session Manager. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.

SIP Entity Tab

Report Name	Report Details
SIP traffic	• Total SIP messages transmitted per SIP Entity. • Total SIP messages received per SIP Entity. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.

Table continues…

Report Name	Report Details
SIP requests and responses	• Total SIP Requests transmitted per SIP Entity. • Total SIP Requests received per SIP Entity. • Total SIP Responses transmitted per SIP Entity. • Total SIP Responses received per SIP Entity. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.
SIP errors	• Total Security Module drops per SIP Entity. • Total Transmission Errors per SIP Entity. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.

SIP Per IP Tab

Report Name	Report Details
SIP traffic	• Total SIP messages transmitted per SIP IP Address. • Total SIP messages received per SIP IP Address. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.
SIP requests and responses	• Total SIP Requests transmitted per SIP IP Address. • Total SIP Requests received per SIP IP Address. • Total SIP Responses transmitted per SIP IP Address. • Total SIP Responses received per SIP IP Address. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.

Table continues…

Report Name	Report Details
SIP errors	• Total Security Module drops per SIP IP Address. • Total Transmission Errors per SIP IP Address. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.

Related links

SIP Performance on page 611

SIP Performance field descriptions

Name	Description
Session Manager	The name of the Session Manager for which you want the system to display the SIP performance data. The system prevents you from entering the name of a Session Manager instance that is the **Maintenance Mode** service state.
Data Available	Period for which performance data is available.
Date and Time	Period for which SIP performance data should be retrieved: 1. Predefined Values: • all dates and times • last month • last week • today • yesterday 2. Last: 1-99 Days or Hours 3. Between: Specified Date Range
Generate Graphs	Generate SIP performance graphs based on specified parameters.
Export Data Range	Period for which SIP performance data should be exported: • All : Retrieve all data for specified Session Manager. • Selected Range : Retrieve data based on the **Date and Time** field selection.

Table continues…

Name	Description
Export Data Format	Format of the downloaded SIP performance data: CSV or XML.
Download Data	Export SIP performance data based on the specified parameters.
SIP Entity	The specific SIP entity for which you want to see the performance data.
Total	All the SIP entities for which you want to see the performance data.
SIP Per IP	The SIP entities per IP address.
IP Address	The IP Address of the entity.
Protocol	The administered protocol.
Port	The port detail.

Related links

Viewing SIP performance data on page 612
Exporting analyzed SIP performance data on page 612

System Performance

Use Session Manager platform performance data to:

- Generate graphs of the analyzed data
- Export the analyzed data as a report in CSV (comma separated value) or XML format.

Note:

- Performance data can be collected for Session Manager 6.1 and later releases.
- The system collects performance data based on a sample frequency of 5 minutes for the displayed parameters.

Related links

System Performance Report Types on page 619

Viewing System Performance data

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Performance** > **System Performance**.
2. Enter or select the name of the **Session Manager** you want to view.

3. Specify the date and time for the period of the system performance data you want to view.
4. Select the tab of the type of data you want to view.
5. Click **Generate Graphs**. You only need to do this step once.
6. To view other data types in the graphical format, click the appropriate tab.

Related links

System Performance field descriptions on page 620

Exporting analyzed System Performance data

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Performance** > **System Performance**.
2. Enter or select the name of the **Session Manager**.
3. Specify the date and time for the period of the System Performance data you want to view.
4. Select the tab of the data type you want to export.
5. In the **Export Data Range** and **Export Data Format** fields, select the appropriate values from the drop-down menus.
6. Click **Download Data**.
7. Select if you want to open or save the file.

Related links

System Performance field descriptions on page 620

System Performance Report Types

CPU Tab

Report Name	Report Details
CPU Usage	• **User:** CPU occupancy for normal processes executing in user mode. • **System:** CPU occupancy for processes executing in kernel mode. • **Idle:** CPU occupancy when system is idle. • **IO Wait:** CPU occupancy of waiting for I/O to complete. The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.

Memory Tab

Report Name	Report Details
Physical Memory	• **Total:** Total usable RAM (physical ram minus a few reserved bits and the kernel binary code). • **Free :** Sum of LowFree + HighFree (overall stat). • **Used :** RAM used by the system. • **Cached :** Memory in the pagecache (diskcache) — SwapCache. The report shows the maximum, minimum, and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.
Swap Memory	• **Swap Total :** Total amount of physical swap memory. • **Swap Free :** Total amount of swap memory free. • **Swap Used :** Total amount of swap memory used. • **Swap In :** Total amount of swap memory swapped in. The report shows the maximum, minimum, and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.

Disk Tab

Report Name	Report Details
Disk Usage	Total Session Manager disk space used.

Management Network and SIP/HTTP Network tabs

Report Name	Report Details
Network Bytes	• **rxbytes:** Total Network bytes received • **txbytes:** Total Network bytes transmitted The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.
Network Packets	• **rxpackets:** Total Network packets received • **txpackets:** Total Network packets transmitted The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.
Network Errors	• **rxerr:** Total received network errors • **rxdrop:** Total received network drops • **txerr:** Total transmitted network errors • **txdrop:** Total transmitted network drops The report shows the maximum, minimum and average values in the selected time period for each of the displayed parameters at the bottom of graphs as part of the graph legend.

Related links

System Performance on page 617

System Performance field descriptions

Name	Description
Session Manager	The name of the Session Manager for which you want the system to display the System Performance data. The page displays `No data available` for a Session Manager that is in the **Maintenance Mode** service state.
Data Available	Period for which performance data is available.

Table continues…

Name	Description
Date and Time	Period for which System Performance data should be retrieved: • Predefined Values: - all dates and times - last month - last week - today - yesterday • Last: 1-99 Days or Hours • Between: Specified Date Range
Generate Graphs	Generate System Performance graphs based on the specified parameters.
Export Data Range	Period for which System Performance data should be exported: • **All** – Retrieve all data for the specified Session Manager. • **Selected Range** – Retrieve data based on the **Date and Time** field selection.
Export Data Format	Format to export the downloaded System Performance data: CSV or XML.
Download Data	Export the System Performance data based on the specified parameters.

Related links

Viewing System Performance data on page 617
Exporting analyzed System Performance data on page 618

Performance Data Collection

Use the Performance Data Collection page to monitor and collect performance measurement data from Session Manager instances.

Note:

The performance data is collected on a time sampled basis which is useful for time average analysis. This data may not provide accurate information about events and spikes.

The Performance Data Collection page:

- Displays the list of Session Manager instances for which the system can collect data.

- Displays general status information for performance processing and disk usage.
- Provides the ability to disable or enable data collection from all Session Manager instances or only selected Session Manager instances.
- Specifies a performance data storage location. The location can be either the existing performance data disk partition that resides on System Manager or an external Network File System (NFS) disk partition. By default, the data storage location is set to **Local**, the partition on System Manager.

Using NFS disk space for performance data storage

Use Remote NFS storage for large capacity configurations to ensure adequate space is available for performance data storage. The NFS partition should be 30 GB or more. The recommended size is 80 GB.

The system indicates successful completion of the data move by returning to the command prompt without displaying an error message. After the move completes, the performance data can no longer be accessed in the old storage location.

Before changing the storage location, the system verifies the NFS is properly mounted on the local mount point and the NFS server is accessible.

Before you begin

- On the NFS server, administer a user as `admin` and a group as `admin` and ensure that their UID and GID matches with the user `admin` and group `admin` of System Manager.
- Set permissions on the NFS partition to be exported to 775 and assign the ownership of the NFS partition to the user `admin` and group `admin`.
- If you have set up the NFS partition prior to Release 7.0, then change the ownership of all the files and directories to user `admin` and group `admin`.

Procedure

1. Using SSH, log in to System Manager as a non-root user.
2. Mount the NFS share. Run the command **`mountNFS_PerfData.sh server:directory`**, where
   - server is the Hostname, IP address, or fully qualified domain name of the NFS server.
   - directory is the path to the shared directory on the NFS server.
3. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Performance** > **Data Collection**.
4. Click **Disable All**.
5. On the SSH session, run the command **`move_to_perfdata-remote.sh`** to move existing performance data to the remote storage location.
6. On System Manager, on the Performance Data Collection page, click **Change Data Storage**.

7. Click **OK** and acknowledge the warning message.
8. Select **Remote (NFS) storage** and click **Commit**.

   The system updates the Performance Data Collection page with the new storage location.
9. Click **Enable All** to enable data collection for all Session Manager instances.

Reverting to local storage after using remote storage

This procedure is applicable if a customer wants to revert back to local storage after using a remote NFS storage location.

Caution:

If the size of the NFS performance data partition exceeds 30 GB, the data cannot be moved back to the local disk because the local disk partition is limited to a maximum of 30 GB.

The system indicates a successful completion of the data move by returning to the command prompt without displaying an error message. After the move completes, you can no longer access the performance data in the old storage location.

Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Performance** > **Data Collection**.
2. Click **Disable All**.
3. Using SSH, log in to System Manager as a non-root user.
4. In the SSH session, run the command `move_to_perfdata.sh`.
5. On System Manager, on the Performance Data Collection page, click **Change Data Storage**.
6. Click **OK** and acknowledge the warning message.
7. Select **Local** and click **Commit**.

   The system updates the Performance Data Collection page with the new storage location.
8. Click **Enable All** to enable data collection for all Session Manager instances.
9. In the SSH session, run the command **`unmountNFS_PerfData.sh`** to unmount the NFS share.

Performance Data Collection field descriptions

Button	Description
Refresh	Refresh the performance data collection status information.
Collect Now	Immediately start data collection from the enabled core Session Manager instances.
Reinitialize	Reinitialize the entire performance data collection system. Force re-retrieval of all data stored on the Session Manager instances. **Warning:** This operation forces a complete re-load from all Session Manager servers and is very resource intensive. Do not use this feature unless absolutely necessary.
Change Data Storage	Change the data storage location.

Name	Description
Data collection status	Display the state of the data collection process. The possible states are: • **IDLE:** The collection process is currently not running. • **COLLECTING:** The system is currently downloading measurement CSV files and converting to RRD files. • **ERROR: disk area problem:** The system detects a disk area problem that could be serious.. • **ERROR: disabled, disk full:** The performance partition is full and an alarm has been generated. • **COLLECTING: disk use warning:** The system threshold is above the warning alarm level.
Last Collection	Date and time of the last completed collection cycle for all enabled Session Manager servers.
Collection interval minutes	Interval between collection from the enabled Session Manager servers. Collection begins at the top of the hour.
5 Min sample retention days	Retention period for 5 minute sample data.
60 Min sample retention days	Retention period for Hourly roll up sample data.

Table continues…

Name	Description
CSV file retention days	Retention period for raw CSV files on System Manager.
Performance data storage location	Display the storage location of the performance data. Choices are: • Local • Remote (NFS)

Per Session Manager Collection

Button	Description
Disable	Turn off data collection for the selected Session Manager instances. This option does not stop measurement sampling.
Enable	Turn on data collection for the selected Session Manager instances.
Disable All	Disable data collection from all Session Manager instances. This option does not stop measurement sampling.
Enable All	Enable data collection from all Session Manager instances.
Reset	Discard changes and restore the original values.
Apply	Apply the changes and remain on this page.

Name	Description
Session Manager	Name of the administered Session Manager instance.
Release	Session Manager release version number.
Data Collection	Indicates whether data collection is enabled or disabled.
Last Collection	Date and time of the last successful collection from this Session Manager instance.
First Sample	Date and time of the first collected measurement sample.
Last Sample	Date and time of the last collected measurement sample.

Chapter 12: Managing system events

Managing alarms

Alarming

The System Manager web interface provides the following operations for alarms:

- Viewing alarms

  Note:

  Session Manager clears alarms automatically when the alarm condition has been resolved or not seen for a certain time.

- Changing alarm status
- Exporting alarms to a comma separated values (csv) file
- Configuring alarm throttling

Alarms are classified by their effect on system operation and identify the system component that generates the alarm.

Session Manager and Branch Session Manager send alarms through SNMP traps directly to the Secure Access Link (SAL) gateway. The SAL gateway then forwards the alarms to the Avaya Data Center (ADC) for processing and resolution. Session Manager can send alarms to up to ten (10) Network Management System (NMS) destinations. One of the destinations must be the SAL gateway.

The condition that one of the destinations must be the SAL gateway does not apply to Session Manager systems supported by others instead of Avaya Services.

Alarm throttling is a mechanism to reduce the frequency of alarm generation for the same events in a specified interval of time. You can configure alarm throttling and reduce the occurrence of alarm flooding events.

For information about the SNMP capabilities of the Session Manager server, see *Avaya Aura™ Session Manager R6.1 – SNMP Agent Whitepaper* on the Avaya support website.

For information about SNMP support for Session Manager, see SNMP support for Session Manager on page 717.

Viewing alarms

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Events** > **Alarms**.
3. On the Alarming page, select an alarm from the Alarm List. You can select multiple alarms.
4. Click **View**.

   The system displays the alarm details on the Alarm - View Alarm Detail page.

Changing the alarm status

The status of an alarm can be:

- **Acknowledged**: Maintenance support must manually set the alarm to this state. Indicates the alarm is under investigation.
- **Cleared**: Maintenance support must manually set the alarm to this state. Indicates the error condition has been resolved. The auto alarm clear event might result in the Cleared status.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Events** > **Alarms**.
3. On the Alarming page, select an alarm and click **Change Status**.

   You can select multiple alarms.
4. Click the status that you want to apply to the selected alarms.

Exporting alarms

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**.
2. In the left navigation pane, click **Events** > **Alarms**.
3. On the Alarming page, perform one of the following actions:
   - 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.

4. Click **Save** to save the exported file to the local disk.

Filtering alarms

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 criterion on the selected alarms.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left 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 records are found that match the specified filter criteria.

Result

The system displays the alarms that match the filter criteria.

Searching for alarms

Use the Advanced Search function to find alarms based on certain specified conditions. The system displays only 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 left 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 perform the following:
   a. Select the AND or OR operator from the drop-down field.
   b. Repeat Step 4 and Step 5.

   To delete a search condition, click **-**. You can delete a search condition only if you added more than one search condition.
7. To find alarms for the given search conditions, click **Search**.

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 entries for the primary and secondary System Manager.
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 alarms for the secondary System Manager that is in the 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 that matches the option that you must select from the following options:
   - (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)

The system displays the alarms according to the option that you selected.

Alarming 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.

Field	Description
Time Stamp	The date and time when the alarm is generated.
Severity	The severity of the alarm.
Status	The current status of the alarms.
Host Name/SysName	The name of the host computer that generated the alarm.
Source IP address	The IP address of the system from that generated the alarm.
Description	The detailed description of the problem that generated the alarm.
Identifier	The unique identifier for an alarm.
Event ID	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.
NotificationOID	The SNMP OID of the alarm.
M/E Ref Number/SysOID	The unique identification number assigned to the product, also called the product ID. This number helps in identifying the component that generated the alarm. For alarms that are generated from trap listener, the system displays the System OID.

Button	Description
Alarm landing Page	Changes the mode from **Auto-Refresh** to Manual refresh and displays the Alarming home page. This is a toggle button.

Alarming field descriptions

Field	Description
Time Stamp	The date and time when the alarm is generated.
Severity	The severity of the alarm.
Status	The current status of the alarms.
Host Name / SysName	The name of the host server that generated the alarm. In case of the trap listener service, this column displays the system name.
Source IP Address	The IP address of the system that generated the alarm.
Description	The detailed description of the problem that generated the alarm.
M/E Ref Number / SysOID	The unique identification number assigned to the product, also called the product ID. This number helps in identifying the component that generated the alarm. For alarms that are generated from trap listener, the system displays the System OID.
Identifier	The unique identifier for an alarm.
Event ID	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.
NotificationOID	The SNMP OID of the alarm.

Button	Description
View	Displays the details of the selected alarms.
Change Status	Changes the status of the selected alarm. The options are: • **Acknowledged** • **Cleared**
Auto-Refresh Mode	Changes over to the **Auto-Refresh** mode. When the Alarming page is set in this mode, it automatically updates the alarms in the table. This is a toggle button.
More Actions > **Export Selected**	Exports the selected alarms to a CSV file. You can view the logs using the Wordpad or Excel application.

Table continues…

Button	Description
More Actions > **Export All**	Exports all the alarms to a CSV file. You can view the logs using the Wordpad or Excel application. **Note:** When you use **Advanced Search** or **Filter** option to filter alarms based on some criteria, **Export All** exports all the filtered data.
More Actions > **Delete Selected**	Deletes the alarms that you select from the list.
More Actions > **Delete ALL**	Deletes all alarms that the system displays on the page.
Advanced Search	Displays fields that you can use to specify the search criteria for searching an alarm.
Refresh	Refreshes the log information in the table.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. A toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Clear	Clears the filter criteria.
Filter: Apply	Filters alarms based on the filter criteria.
All	Selects all the alarms in the table.
None	Clears the check box selections.
Previous	Displays the logs in the previous page. This button is not available if you are on the first page.
Next	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 upper-right corner of page.

Name	Description
Criteria	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. Select following search criteria from the first drop-down list: • 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. • Severity: Searches all the alarms that match the specified severity level. • Status: Searches all the alarms that match the specified status. • Host Name: Searches all alarms that are generated from the specified host. • M/E Ref Number: Searches all the alarms that match the specified M/E Ref Number. • Event ID: Searches all the alarms that match the specified Event ID. • Source IP address: Searches all alarms that are generated from the specified source IP address. • NotificationID: Searches all the alarms that match the specified NotificationID. • Identifier: Searches all the alarms that match the specified identifier. • Description: Searches all the alarms that match the specified description. The operators available are based on the search criterion that you select in the first drop-down field. The operators available for search criteria are as follows: • Time Stamp: =, >, <, >=, <=, >=, != • Severity: Equals, Not Equals • Status: Equals, Not Equals • Host Name: Equals, Not Equals, Starts With, Ends With, and Contains • Identifier: =, >, <, >=, <=, >=, != • Source IP address: Equals, Not Equals, Starts With, Ends With, and Contains

Name	Description
	• Event ID: Equals, Not Equals, Starts With, Ends With, and Contains • Description: Equals, Not Equals, Starts With, Ends With, and Contains • M/E Ref Number: Equals, Not Equals, Starts With, Ends With, and Contains When you select **Begin Date** and **End Date** from the first drop-down list, you are prompted to enter the date in the third field.

Button	Description
Clear	Clears the entered search criteria and sets the default search criteria.
Search	Searches the alarms based on the search conditions.
Close/Advanced Search	Hides the search fields.
+	Adds a search condition.
-	Deletes a search condition.

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 which generated 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. Log viewer displays only logs that are of type Audit.

Viewing log details

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left 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 left 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 a 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 left 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 left 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 the steps 4 through 6.

   Click **-** to delete a search condition. You can delete a search condition only if you have more than one search condition.
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 details of the selected logs, 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 title of the column to sort the data of the column in ascending or descending order.

Name	Description
Select check box	The option to select a log.
Log ID	The unique identification number that identifies the log.
Time Stamp	The date and time of the log generation.
Host Name	The name of the system from which the log is generated.
Product Type	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.

Table continues…

Name	Description
Severity	The severity level of the log. The following are the type of severities: • **Emergency**: System is unusable. • **Alert**: Action must be taken immediately. • **Critical**: Critical conditions. • **Error**: Error conditions. • **Warning**: Warning conditions. • **Notice**: Normal but significant condition. • **Informational**: Informational messages. • **Debug**: Debug-level messages. **Note:** The colors of severities do not indicate logging severities
Event ID	The unique identification number assigned to the event that generated the log.
Message	A brief description about 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.
Process Name	The process on the device that has generated the message, usually the process name and process ID.
Facility	The operating system, processes, and applications quantify messages into one of the several categories. These categories generally consist of the facility that generated them, along with the severity of the message. The following are the types of supported facilities: • User-Level Messages • Security/authorization • Log Audit

Button	Description
View	Opens the Log - View Log Detail page. Use this page to view the details of the selected log.
Auto-Refresh Mode	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.

Table continues…

Button	Description
More Actions > **Export Selected**	Exports the selected logs to a CSV file. You can view the logs using the Wordpad or Excel application.
More Actions > **Export All**	Exports all the logs to a CSV file. You can view the logs using the Wordpad or Excel application. **Note:** When you use **Advanced Search** or **Filter** option to filter logs based on some criteria, **Export All** exports all the filtered data.
Advanced Search	The fields that you can use to specify the search criteria for searching a log.
Refresh	Refreshes the log information in the table.
Filter: Enable	The fields under select columns that you can use to set filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Clear	Clears the filter criteria.
Filter: Apply	Filters logs based on the filter criteria.
Select: All	Selects all the logs in the table.
Select: None	Clears the selections.
Previous	Displays the logs in the previous page. This button is not available if you are on the first page.
Next	Displays the logs in 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
Criteria	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. Select following search criteria from the first drop-down list: • Log ID: The unique identification number assigned to the log. • Host Name: Name of the system for which log is generated. • Product type: A code which uniquely identifies the component which generated the log. For example, product, device, application, service, and so on. • Severity: Severity level of the log. • Message: Brief description about the log. • Event ID: Unique identification number assigned to the event. • Process Name: Process on the device that has generated the message. • Time Stamp: Date and time of the log generation. • Facility: The operating systems, processes, and applications quantify messages into one of several categories. These categories generally consist of the facility that generated them, along with the severity of the message. The second drop-down list displays operators. Based on the search criterion that 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 list. The following are the list of operators: • Equals • Not Equals • Starts With • Ends With • Contains The operators for Time Stamp are: =, >, <, >=, <=, and !=. 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.

Name	Description
	Enter the date in MM/DD/YYYY format. You can select the date from the calender. You need to enter the time in one of the following formats: • 24Hr • AM • PM

Button	Description
Clear	Clears the search criterion and sets the criterion to the default search criteria.
Search	Searches the logs based on the search conditions.
Close/Advanced Search	Hides the search fields.
+	Adds a search condition.
-	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
Log ID	The unique identification number that identifies the log.
Time Stamp	The date and time of the log generation.
Host Name	The name of the system from which the log is generated.
Product Type	The code which uniquely identifies the component which generated the log. For example, product, device, application, service and so on. GW600, which is a product type code identifier is an example of the log product type.

Table continues…

Name	Description
Severity	The severity level of the log. The following are the type of severities: • **Emergency**: System is unusable • **Alert**: Action must be taken immediately • **Critical**: Critical conditions • **Error**: Error conditions • **Warning**: Warning conditions • **Notice**: Normal but significant condition • **Informational**: Informational messages • **Debug**: Debug-level messages **Note:** The colors of severities do not indicate logging severities.
Event ID	The unique identification number assigned to the event that has generated the log.
Message	Brief description about 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.
Process Name	The process on the device that has generated the message. This is usually the process name and process ID.
Facility	The operating system, processes, and applications quantify messages into one of the several categories. These categories generally consist of the facility that generated them, along with the severity of the message. The following are the types of supported facilities: • User-Level Messages • Security/authorization • Log Audit

Button	Description
Logging Landing Page	Switches the mode from Auto-Refresh to manual refresh and displays the Logging Home page. 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 left navigation pane, click **Logs** > **Log Settings**.

Result

The system 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 left navigation pane, click **Logs** > **Log Settings**.
3. On the Log Settings page, click a log file from the **Select Log File** field.

Related links

Logging Settings field descriptions on page 642

Logging Settings field descriptions

Use this page to view and edit loggers defined in a log file.

Log Settings

Name	Description
Select Log File	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 log level indicating the level of logging set for the corresponding logger.
Attached Appenders > Name	The name of the appender.
Attached Appenders > File Path	The path of the file to which the appender logs the information.
Attached Appenders >Facility	The process running on the machine that created the log message.
Attached Appenders > host	The name of the syslog host where the log output is stored.
Show All	An option to select the maximum number of logger records that you can view at a time.

Button	Description
Edit	Opens the Edit Logger page that you can use to edit loggers.

Related links

Viewing loggers for a log file on page 642

Editing a logger in a log file

About this task

You can set log levels for loggers which defines the level of logging the logger logs.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Settings**.
3. On the Log Settings page, click a log file from the **Select Log File** field.
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, in the **Log Level** of the specified log, click **Info**.

   For example, as a user of System Manager Communication Manager capabilities, if you set the **Log Level** to **Info** in `com.avaya.iptcm.eps.logging.audit` and `com.avaya.iptcm.eps.logging.operation`, the system captures the successful events in the audit log and the operational log present at `/var/log/Avaya/mgmt/iptcm/audit.log` and `/var/log/Avaya/mgmt/iptcm/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 646

Forwarding System Manager syslog messages to remote server

Procedure

1. On 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 **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 log messages.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Settings**.
3. On the Log Settings page, click a log file from the **Select Log File** field.
4. In the **Logger List** section, select a logger and click **Edit**.
5. On the Edit logger page, click **Attach** in the Attached Appenders 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 647

Modifying an appender

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Settings**.
3. On the Log Settings page, click a log file from the **Select Log File** field.
4. In the **Logger List** section, select a logger and click **Edit**.
5. On the Edit logger page, select an appender in the **Attached Appenders** section.
6. Click **Edit**.
7. On the Edit Appender page, modify the appender information.

   You can modify information in the **Threshold Log Level**, **Max File Size**, **File Path**, and **Number Of Backup Files** fields
8. Click **Commit**.

Related links

Edit Appender field descriptions on page 647

Removing an appender from a logger

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Settings**.
3. On the Log Settings page, click a log file from the **Select Log File** field.
4. In the **Logger List** section, select a logger and click **Edit**.
5. On the Edit logger page, select an appender in the **Attached Appenders** 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
Logger	The name of the logger.
Log level	The level of logging for which the logger logs the information.

Attached Appender

Name	Description
Appender	The name of the appender.
Threshold Log Level	The threshold log level set for the appender. Appender logs only information of log type that is set in the threshold log level.
File Path	The path of the file where the appender logs the information.
Max File Size	The maximum size in KB, MB, and GB reserved for the appender file.
# Backup Files	The number of log files that an appender can use to store log information if one log file becomes full. If all the backup files are full, the appender overwrites the previous backup files in the order the files are created.
Facility	The process running on the machine for which log messages are created.
Host	The name of the syslog host that stores the log output.
Header	The header part of the syslog packet. The header part contains timestamp and host name information.
Facility Printing	The printed message includes the facility name of the application.

Button	Description
Edit	Opens the Edit Appender page. Use this page to modify the appender information.
Attach	Opens the Attach Appender page. Use this page to add an appender to the logger.
Detach	Removes the selected appender from the logger.

Table continues…

Button	Description
Commit	Saves the changes in the logger information to the database.
Cancel	Closes the Edit Logger page and takes you back to the Logging Configuration page.

Edit Appender field descriptions

Use this page to edit the information of an appender.

Name	Description
Logger	The name of the logger. **Note:** You can only view this information.
Appender	The name of the appender. **Note:** You can only view this information.
Threshold Log Level	The threshold log level set for the appender. Appender logs only information of log type that is set in the threshold log level.
File Path	The path of the file where the appender logs the information.
Max File Size	The maximum KB, MB, and GB reserved for the appender file.
# Backup Files	The number of log files that an appender can use to store log information if one log file becomes full. If all the backup files are full, the appender overwrites the previous backup files in the order the files are created.

Button	Description
Commit	Saves the changes to the database.
Cancel	Closes Edit Appender page and takes you back to the Edit Logger page.

Attach Appender field descriptions

Use this page to assign an appender to the logger.

Name	Description
Logger	The name of the logger.
Log Level	The level of logging for which the logger logs the information.

Table continues…

Name	Description
Select Appender	The list of appenders that you can assign to the logger.

Button	Description
Commit	Assigns the appender to the logger.
Cancel	Closes the **Attach Appender** page and takes you back to the Edit Logger page.

Managing log harvester

Log harvester

The log harvesting service manages the retrieval, archival, and analysis of 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 computer or on 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

1. On the System Manager web console, click **Services** > **Events**.

2. In the left navigation pane, click **Logs** > **Log Harvester**.

Result

The system displays the **Log Harvester** page.

Creating a new log harvesting profile

About this task

To create a new log harvesting profile, you must specify:

- The host name of the server on which the product is running

  If you do not see the host name 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

To harvest log files for products running on different servers, you must specify multiple filter criteria.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, click **New**.
4. On the Create New Profile page, enter the appropriate information in the **Profile Name** and **Profile Description** fields.
5. Select 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 for another instance of the same product running on the same server or on a different server, click plus (**+**).
6. If you select one or more directories, in the **File Name Filter** field, enter a text pattern as the filter criteria.

   During the harvesting operation, the system harvests only those files that match the filter criteria.

7. To save the profile and the log harvesting requests in the profile, click **Save Profile**.

Related links

Create New Profile field descriptions on page 657

Editing a log harvesting profile

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a profile and click **Edit**.
4. On the Harvest Criteria Edit page, modify the information in the **Profile Name** and **Profile Description** fields.
5. Modify 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 the `CTRL` and click the item you select.
   - To add another log harvesting request for another product or for another instance of the same product running on the same server or on a different server, click **+**.
6. If you select one or more directories, you can enter a new filter criteria in the text box below the **Directories / Filter Text** field and click **Commit**.

   During the harvesting operation, the system harvests only those files that match the filter text.
7. Click **Save Profile** to save the changes you made to the log harvesting profile.

Related links

Harvest Criteria Edit field descriptions on page 658

Viewing the harvested log files in an archive

You can view the harvested log files of a product stored in an archive file.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left 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 a request in the table in the Harvest Request Details section.

5. Click **Show files**.

   On the Search Archives page, navigate through the folders in the archive to view the harvested log files.

Deleting a profile

About this task

You cannot delete a profile that is in use by the Log Harvester service. If you attempt to delete a profile that is in use, the system displays an error message.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a profile and click **Delete**.
4. On the Profile Delete Confirmation page, click **Delete**.

   Note:

   When you delete a profile, the system deletes all requests and all 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 that are 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**.
2. In the left 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, enter the relevant information in the **Archive Name** and **Archive Description** fields.

   The system saves the harvested log files in the specified archive file.
5. Click **Run Profile** to send a request.

The table in the Harvest Criteria View section provides you the status of the log harvesting request. If the execution status of the request is successful, then 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 659

Viewing details of a log harvesting request

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left 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 a request in the table in the Harvest Request Details section.
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 662

Searching for text in a log file

Use this feature to search for matching text in the log file of a product.

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 left 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 a request in the table in the Harvest Request Details section.
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 661

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 left 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 a request in the table in the Harvest Request Details section.
5. If the system does not display any requests, submit a new request.
6. Click **Show Files**.

   The system lists the log files that are harvested.
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 661

Downloading the harvested log files

About this task

You can download the harvested log files of one or more products that you stored in a zip file on your local server.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left 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 a request in the table in the Harvest Request Details section.
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 on different servers.
   - If you select a host name of a server under a product, the system creates a zip file that contains the harvested log files for the products running on the server that you selected.
   - 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 661

Filtering log harvesting profiles

Use this feature to set filter criteria to view only those log harvesting profiles that meet the set filter criteria. The titles of the columns of the table that displays the log harvesting profiles are the filter criteria.

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left 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 matches the specified filter criteria.

Filtering log harvesting requests

Use this feature to set filter criteria to view only those log harvesting requests that meet the set filter 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 left 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 only those log harvesting requests that match the specified filter criteria.

Viewing details of a log harvesting profile

Procedure

1. On the System Manager web console, click **Services** > **Events**.
2. In the left navigation pane, click **Logs** > **Log Harvester**.
3. On the Log Harvester page, select a profile and click **View**.

   The Profile Criteria View page contains the details of the log harvesting profile you selected.

Related links

Profile Criteria View field descriptions on page 659

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
Profile Name	The name of the log harvesting profile.
Description	A brief description of the profile.
Created By	The name of the creator of the profile.
Created Time Stamp	The date and time when the profile was created.

Button	Description
View	Opens the Harvest Archives page. You can use this page to view the details of a selected log harvest profile.
New	Opens the Create New Profile page. You can use this page to create a new log harvesting profile.
Edit	Opens the Edit Profile page. You can use this page to edit a log harvesting profile.
Delete	Deletes the selected profile. You cannot delete a profile if the profile is in use by the Log Harvester service.

Table continues…

Button	Description
Requests	Opens the Harvest Archives page. You can use this page to run the log harvesting requests in a selected profile.
Filter: Disable	Hides the fields displayed under the columns on which you can apply the filters without resetting the filter criteria. This is a toggle button.
Filter: Enable	The fields under the columns in the table where you can enter the filter criteria. Only columns on which you can apply filter display the fields in which you can enter the filter criteria. This is a toggle button.
Filter: Apply	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
Profile Name	The name of the log harvesting profile.
Profile Description	A brief description of the profile. This is an optional field.

Host Name	The host name of the servers on which products are installed.
	If you do not see the host name 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>`

Product	The products for which you can harvest logs.
Directories / Filter Text	A list of directories that contains the log files for the selected product.
Files	The log files that you can harvest for the selected product.
Filter Text	The text based on which the system filters the log files present in the selected directory for harvesting. When you select the `/a/b/c`directory and enter `com` in this field, the harvest operation for this profile harvests the log files that are in the directory `/a/b/c`. The log files contain com in the file name. The field does not support wild cards.

Button	Description
+	Specifies another log harvesting request for a product.
-	Deletes the log harvesting request for the product.
Commit	Commits the filter criteria for the selected directories.
Save Profile	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
Profile Name	Displays the name of the log harvesting profile
Profile Description	Displays a brief description of the profile.
Host Name	Displays the hostname of the servers on which you installed the products.
Product	Displays the products for which you can harvest logs.
Directories / Filter Text	Lists the directories that contains the log files for the selected product.
Files	Displays the log files that you can harvest for the selected product
Filter Text	Displays the text based on which the log files present under a selected directory gets filtered for harvesting. If you select the directory `/a/b/c` and enter `com` in the **Filter Text** field, the harvest operation for this profile harvests the log files that contain *com* in the file name. The field does not support wildcards.

Button	Description
+	Allows you to specify another log harvesting request for a product.
-	Deletes the log harvesting request for the product.
Commit	Commits the filter criteria for the selected directories.
Save Profile	Saves the new profile and settings for log harvesting requests in the database.

Table continues…

Button	Description
Cancel	Ignores the changes you make to the Harvest Criteria Edit page and takes you back 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
Profile Name	Displays the name of the log harvesting profile.
Profile Description	A brief description of the profile.
Product	Displays the name of the product for which logs are harvested.
Hosts	Displays the hostname of the server on which the product resides.
Files	Displays the names of the log files for which you can harvest log messages.
Directory	Displays the directory that contains the log files.
Filter Text	The text based on which the log files present under a selected directory are filtered for harvesting. For example, if you select the directory `/a/b/c` and enter the text `com` in this field, the harvest operation for this profile harvests the log files that contain *com* in the file name. This field does not support wild characters.

Button	Description
Done	Closes this page and takes you back 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 zip file.

Name	Description
Archive Name	The name of the archive file that you want to create for storing the 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 that you create for storing the harvested log files.
Request Time Stamp	The date and time when the log harvesting request is submitted.
Request Description	A brief description of the log harvesting request.
Status	The status of the log harvesting request. The options are: • SUCCESS: The status is SUCCESS if System Manager successfully harvests the log messages. • FAILURE: The status is FAILURE if System Manager failed to harvest the log messages for the product. • PARTIAL SUCCESS: The status is PARTIAL SUCCESS if System Manager partially harvests the log messages.
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 provides you the 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 the log harvesting requests for the selected profile.
View	Opens the View Harvest detail page. You can use this page to view the details of a selected log harvesting request.
Show Files	Opens the Search Archives page. You can use this page to search for text contained in the harvested log files, download log files of one or more products running on a same or different servers, view the contents of a log file.
Filter: Disable	Hides the fields displayed under the column filter fields without resetting the filter criteria. This is a toggle button.

Table continues…

Button	Description
Filter: Enable	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 in which you can enter the filter criteria. This is a toggle button.
Filter: Apply	Filters the log harvest profiles present 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
Enter search text	The text that you want search for in the harvested log files.
List box	Displays the hierarchy of the harvested log files in an archive. The files are organized in a tree view.
Log Browser Panel	Displays the contents of the selected log files.
Search Results Panel	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 **Log Browser Panel** field.

Button	Description
Previous	Displays the log file contents on the previous page. This button is available only if the contents of a log files span across multiple pages.
Next	Displays the log file contents on the next page. This button is available only if the contents of a log files span across multiple pages.
Search	Searches for the occurrences of the text specified in the **Enter search text** field in the selected log files.
View	Displays the contents of the selected log files in the **Log Browser Panel** field.
Download	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
Request Id	Displays the unique identification number assigned to a log harvesting request.
Archive Name	Displays the name of the archive file that stores the harvested log files containing the log messages.
Status	Displays the status of log harvesting requests. The options are: • SUCCESS: The status is SUCCESS if System Manager successfully harvests the log messages. • FAILURE: The status is FAILURE if System Manager fails to harvest the log messages for the product.
Request Description	A brief description of the log harvesting request.

Child Request Details

Name	Description
Product	Displays the unique identification number assigned to a log harvesting request.
Status	Displays the status of the log harvesting request. The options are: • **SUCCESS**: The status is SUCCESS if System Manager successfully harvests the log messages. • **FAILURE**: The status is FAILURE if System Manager fails to harvest the log messages for the product.
Host Name	Displays the hostname of the server on which the product resides.
Status Description	A brief description about the execution status of the request.
Status Time Stamp	Displays the date and time when the system generates the status of the log harvesting request.

Button	Description
Done	Closes this page and takes you back to the Harvest Archives page.

Table continues…

Button	Description
Refresh	Refreshes the records in the table.
Filter: Enable	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 in which you can enter the filter criteria. This is a toggle button.
Filter: Apply	Filters the log harvesting requests based on the filter criteria.
Filter: Disable	Hides the fields displayed under the columns on which you can apply the filters without resetting the filter criteria. This is a toggle button.

Chapter 13: Managing system data

Backup and Restore

The backup and restore functions run on System Manager.

System Manager creates one backup file that contains all the data for the entire system. You do not need to create individual backup files of all the Session Manager instances. The data and configuration files for the entire system are stored centrally on System Manager.

System Manager supports local backup and remote backup. You can transfer backup files by using the sftp or scp protocol.

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 ignores all backup jobs that are scheduled at that time. System Manager displays a warning if you attempt to restore a corrupted or tampered backup file.

Note:

You can only restore a data file on the same software version on which the backup was taken. However, when you upgrade to a newer release of System Manager, the system preservers the data. If an upgrade failure occurs, System Manager rolls back the previous configuration.

Disk space required for backup

Table 6: 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

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.

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.

Creating 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 backup file that you want to create.
5. 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!!`

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. For more information, see Supported ciphers, key exchange algorithms, and mac algorithms.

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. 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!!`

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**.

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.

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.

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 694.
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**.

Restoring data backup from a local 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.

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. 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.
   ```

6. 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.

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 xyz with 1234 software patch installed, System Manager on which you restore the backup must run xyz that has 1234 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. 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**.
5. 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.
```

6. 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.

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 `$MGMT_HOME/pem/fileRestoreCLIUtility`.
3. In the `restorecli.properties` file, enter the build number of the machine in the **version** field.
4. In the properties file, ensure that `fq_backup_file_name` displays the complete path of the backup zip file.
5. In the `fileRestoreCLIUtility.properties` file, ensure that `backup_name` points to the backup zip file.
6. 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.

7. Complete the steps on the screen to perform the restore operation successfully.

Backup and Restore field descriptions

Name	Description
Operation	The type of operation. The values are: • Backup • Restore
File Name	• For the backup operation, the name of the backup file. • For the restore operation, the name of the backup file that was used for the restore.
Path	• For the backup operation, the path of the backup file. • For the restore operation, the path of the backup file that was used for the restore.
Status	The status of the backup or restore operation. The values are: • SUCCESS • FAILED • PLANNED • RUNNING
Status Description	The error details of the backup or restore operation that has failed.
Operation Time	The time of the backup or restore operation.
Operation Type	Defines whether the backup or restore operation is local or remote.
User	The user who performed the operation.

Button	Description
Backup	Opens the Backup page from where you can backup the System Manager data.
Restore	Opens the Restore page from where you can restore the data to System Manager.

Backup field descriptions

Name	Description
Type	The type of computer on which you can back up the application data. The options are: • **Local**: The system backs up the data on a local computer. • **Remote**: The system backs up the data on a remote computer.

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
File Name	The file name that identifies the backup. System Manager creates a backup file in the home directory of the specified user.

The page displays the following fields when you choose to create a backup of the System Manager data on a remote server.

Name	Description
Use Default	The option to use the default configured values. 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**.
File transfer protocol	The protocol that you can use to create the backup. The values are SCP and SFTP.
Remote Server IP	The IP address of the remote server.
Remote Server Port	The SSH port of the remote server.
User Name	The user name for logging into the remote server.
Password	The password for logging on to the remote server.
Test Credentials	Validates the login credential. The validation gives the connection result with the remote backup server.

Table continues…

Name	Description
File Name	The absolute path to the backup file and the file name. For example, `home/admin/smgr_backup_filename`. You can specify a different path for the backup file on the SMGR Element Manager Container page. To open the SMGR Element Manager Container page, click **Services** > **Configurations** and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.

Button	Description
Now	Creates a backs up of the data in the specified location immediately.
Schedule	Displays the Schedule Backup page where you can enter the details to schedule a backup.
Cancel	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
Job Name	The name of the job.

Job Frequency

Name	Description
Task Time	The date and time of running the job.
Recurrence	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: • Execute task one time only. • Tasks are repeated. The system generates an alarm if you do not schedule a System Manager backup every 7 days.

Table continues…

Name	Description
Range	The settings define the number of recurrences or date after which the job stops to recur. The options are: • No End Date • End After occurrences • End By Date

Button	Description
Commit	Schedules the backup job.
Cancel	Closes the Schedule Backup page and takes you back to the Backup Restore page.

Restore field descriptions

Use this page to restore the application data from a local or a remote location.

Field	Description
Type	The type of computer from where you restore the application data. The options are: • **Local**. The data is restored from a local machine. • **Remote**. The data is restored from a remote machine.

The page displays the following fields, when you select **Local** as **Type**.

Field	Description
Select File Name	The list of files from where you select the backup file that you must restore.
File Name	The name of the backup file that you must restore. If the system does not display the file that you must restore, specify the complete path of the backup file. **Note:** System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.

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**.

Field	Description
File Name	The name and complete path of the backup file that you want to restore.
File transfer protocol	The protocol that you can use to restore the backup. The values are SCP and SFTP.
Remote Server IP	The IP address of the SFTP or SCP server.
Remote Server Port	The SSH port of the SFTP or SCP server.
User Name	The user name for logging in to the SFTP or SCP server.
Password	Password for logging in to the SFTP or SCP server.
Use Default	Select this check box to use the default configured values. 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**.

Button	Description
Restore	Restores the data from the specified backup file.
Cancel	Cancels any operation in progress, closes the Restore page, and opens the Backup and Restore page.

Managing data retention rules

Accessing the Data Retention Rules service

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.

2. In the left navigation pane, click **Data Retention**.

   The system displays the Data Retention page with the Rule list.

Result

The system displays the Data Retention page.

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
- Backup files
- Cleared alarms
- Aged alarms

Viewing data retention rules

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.
2. In the left navigation pane, click **Data Retention**.

   The system displays the Data Retention page with the Rule list.

Related links

Data Retention field descriptions on page 679

Modifying data retention rules

Procedure

1. On the System Manager web console, click **Services** > **Configurations**.
2. In the left navigation pane, click **Data Retention**.

   The system displays the Data Retention page with the Rule list.
3. Select a rule from the Rule list.
4. Click **Edit**.
5. Modify the value in the **Retention Interval (Days)** field.
6. Click **Update** to save the value.

Related links

Data Retention field descriptions on page 679

Data Retention field descriptions

Use this page to view and edit data retention rules.

Name	Description
Option button	The option to select a data retention rule.
Rule Name	The name of the rule.
Rule Description	A brief description about the data retention rule.
Retention Interval (Days)	The number of days the data is retained.

Button	Description
Edit	Modifies the selected rule.
Update	Updates the rule with changes made to the rule.
Cancel	Cancels the editing operation.
Apply	Applies the selected rule.

Data Replication Service

The Data Replication Service (DRS) replicates data from the master database on the System Manager server to databases on Session Manager client servers.

DRS supports the following modes of replication:

- Replication in Repair mode: DRS replicates the requested data from the master database to the database of the replica node. Repair is only necessary if an installation of DRS fails.
- Automatic synchronization mode: After the database of the replica node is updated with the requested data, subsequent synchronizations occur automatically. DRS replicates only the data that has been updated since the last replication. Automatic synchronization is a scheduled activity and occurs after a fixed interval of time as set in the configuration files.

DRS sends the data in batches from the master database to the replica node. DRS creates replication batches when the data in the master database is added, modified, and deleted.

On the DRS Replication page, you can:

- View replica nodes in a replica group.
- Replicate requested data from the System Manager master database to the database of the replica nodes if the databases are not synchronized.

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.

Viewing replica nodes in a replica group

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.

Repairing a replica node

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.

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 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 a replica node and click **Repair**.

   The **Synchronization Status** column displays the data replication status for the repairing replica node.

Related links

Replica Nodes field descriptions on page 683

Repairing all replica nodes in a replica group

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.

Removing a replica node

About this task

Warning:

Removing replica nodes or groups can cause problems with systems that use the configuration data for active call processing. These operations should be done with care to avoid unwanted service disruptions.

Procedure

1. On the System Manager web console, click **Services** > **Replication**.
2. On the **Replica Groups** page, select the replica group in which you want to remove a node.
3. Select **View Replica Nodes**.
4. Select the **Replica Node Host Name** you want to remove.
5. Select **Remove**.

Removing a replica node from queue

About this task

Warning:

Removing replica nodes or groups can cause problems with systems that use the configuration data for active call processing. These operations should be done with care to avoid unwanted service disruptions.

Procedure

1. On the System Manager web console, click **Services** > **Replication**.
2. On the **Replica Groups** page, select the replica group you want to remove the node from queue.
3. Select **View Replica Nodes**.
4. Select the **Replica Node Host Name** you want to remove.
5. Select **Remove from Queue**.

Troubleshooting Replica Nodes

About this task

Perform the following troubleshooting steps if the replica group state is not **Synchronized**, **Queued for Repair**, or **Repairing**, or if the replica group is stuck in the **Starting** state.

Procedure

1. On the home page of the System Manager Web Console, under **Services**, select **Replication**.
2. Select the appropriate **Replica Group** for the Session Manager server.
3. Click **View Replica Nodes**.
4. Verify that the Enrollment password has not expired.
5. Enter **`initTM`**. The command should complete within 5 minutes. If it does not complete within that time, continue with the next step.
6. Verify that the system date and time on the Session Manager server is in sync with the system date and time on the System Manager virtual machine. Trust certificate initialization can fail if the clocks differ by more than a few seconds.
7. Enter **`SMnetSetup`**.
    a. Verify that all information is correct.
    b. Verify the Enrollment password is correct on the System Manager Security screen.
    c. Re-enter the Enrollment password.

8. On System Manager, verify the Session Manager is now synchronized.

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
Select check box	An option to select a replica group.
Replica Group	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.
Synchronization Status	For each replica group, displays the combined synchronization status of all replica nodes under the group
Group Description	A brief description of the replica group.

Button	Description
View Replica Nodes	Displays the Replica Nodes page. Use this page to view replica nodes for a group that you select.
Repair	Initiates full-sync for the selected groups and effectively for all the replica nodes that belong to the selected groups.
Filter: Enable	Displays fields under **Replica Group** and **Synchronization Status** columns where you can set the filter criteria. **Filter: Enable** is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.
Filter: Apply	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. 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
Synchronization Status	Displays the synchronization status of the replica node. When you install a node, the node goes from a **Ready for Repair** state to the **Queued for Repair** to **Repairing**, and finally to the **Synchronized** 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. A replica node can be in any one of the following states during the lifecycle: • **Ready for Repair**. The database of the replica node is not synchronized with the master database. • **Queued for Repair**. The replication request of the replica server is in queue with other data replication requests. The color code of the status is yellow. • **Repairing**. The data replication process is in progress. The color code of the status is yellow. • **Synchronized**. 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. **Note:** If you encounter the following, contact the administrator who can manually intervene to resolve the problem: • `Not Reachable`. 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. • `Synchronization Failure`. Data replication is broken between System Manager and the replica node. This status generally indicates a catastrophic failure.

Table continues…

Name	Description
	During the automatic replication of data from the master to the replica node, the system displays the following status: • **Synchronizing**. The data replication is in progress for the replica node. The color code of the status is yellow. • **Synchronized**. 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. • **Pending Audit**. 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 displays any of the other states as applicable. The color code of the status is yellow.
Last Synchronization Time	Displays the last time when the system performed the data synchronization or replication for the replica node.
GR Enabled	Displays whether the replica node is GR-enabled or not.
Last Replication Request Time	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
View Details	Opens the Data Replication page. Use this page to view the synchronization details for a replica node.
Repair	Replicates or resynchronizes data from the master node to a selected replica node.
Remove	Removes the nodes you select from the replica group.
Remove From Queue	Removes the replica node you select from the queue.
Show All Replica Groups	Takes you back to the Replica Groups page.

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
Replica Node Group	Displays the name of the group that the replica node belongs to. A node-group is a logical grouping of similar nodes.
Replica Node Host Name	Displays the full hostname of the replica node. 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.
Last Down Time	Displays the last time and date when the replica node could not be reached. System Manager periodically checks whether a replica node is reachable.
Last Repair Start Time	Displays the last time and date when a full-sync was started for the node.
Last Repair End Time	Displays the last time and date when a full-sync was completed for the node.
Last Pull Time	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.
Build Version	Displays the version of the element configuration.
GR Enabled	Displays whether the replica node is GR-enabled or not.

Synchronization Statistics

Name	Description
Pending Batches	Lists the batches that are yet to be replicated to the replica node. 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.
Pending Unbatched Events	Lists the change events that are yet to be formed into batches. 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.
Synchronization Status	Displays the synchronization status of the replica node. For details, see Replica Nodes field descriptions.
Last Synchronization Time	Displays the last time when the system performed the data synchronization or replication for the replica node.
Last Batch Acknowledged	Displays the last batch that an element acknowledged as successfully processed on the element side. 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
Marked For Audit	Marks all replica nodes that are GR-enabled for audit: The status can be: • ✔: Indicates that the node is marked for audit. • ✘: Indicates that the node is not marked for audit. When the node is marked for audit, the replica status changes to **Pending Audit**, and the color changes to yellow. • When you activate the secondary System Manager or when you enable GR after the primary System Manager restores • When the primary System Manager restores and you choose the database of the primary System Manager • When the primary System Manager restores and you choose the database of the secondary System Manager DRS denies any request from the replica node that is marked for audit until the audit is complete for the replica node.
Last Audit Time	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
Cause of Error	Describes why the system failed to replicate or synchronize data.
Time of Error	Displays the time when the error occurred.

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.

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 left 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 **scheduleroperation**.
9. In **Element or Resource Instance**, select **adminSched**, **onDemand**, **sysSched**, or **All**.
10. Click **Next**.
11. 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 left 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 696

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 698

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 competed 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 competed 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

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. Perform one of the following steps:
   - To remove 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.

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**.

Note:

If the job that you want to delete is in the enabled state, disable the job. See Disabling a job on page 694 on how to disable a job.

c. Click **Delete**.

- To remove a competed job, perform the following steps:

a. Click **Completed Jobs** in the left navigation pane.

b. On the Completed Jobs page, select a completed job.

Note:

If the job that you want to delete is in the enabled state, disable the job.

c. Click **Delete**.

3. On the Delete Confirmation page, click **OK**.

System Manager deletes the job you select 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. Perform one of the following steps:

- To disable 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** > **Disable**.

- To disable a competed 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** > **Disable**.

3. On the Disable Confirmation page, click **Continue**.

The **State** of the job you selected 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. Perform one of the following steps:
   - 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**.
   - To enable a competed 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 left 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
Job Type	The type of job, represented by a job type icon. The types of job with icons are: 1. System scheduled job. 2. Admin scheduled job. 3. On-demand job.
Job Name	The name of the scheduled job.
Job Status	The current status of the pending job. The types of status are: 1. Pending Execution 2. Running
State	The state of a job whether the job is active or inactive. The types of state are: • Enabled: An active job. • Disabled: An inactive job.
Frequency	The time interval between two consecutive executions of the job.
Scheduled By	The person who scheduled the job.

Button	Description
View	Displays the Job Scheduling-View Job page that displays the details of the selected pending job.
Edit	Displays the Job Scheduling-Edit Job page that you can use to modify the information of a selected pending job.
Delete	Displays the Delete Confirmation page that prompts you to confirm the deletion of the selected jobs.
More Actions > **View Log**	Displays the Logging page that displays the logs for the selected pending jobs.
More Actions > **Stop**	Stops the selected job that is currently running.
More Actions > **Enable**	Changes the state of the selected pending job from inactive to active.
More Actions > **Disable**	Displays the Disable Confirmation page that prompts you to confirm the disabling of the selected pending job.

Table continues…

Button	Description
More Actions > **Schedule On Demand Job**	Displays the Job Scheduling-On Demand Job page that you can use to schedule the selected pending job of type On Demand.
Advanced Search	Displays fields that you can use to specify the search criteria for searching a pending job.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. **Filter: Enable** is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. **Filter: Disable** is a toggle button.
Filter: Apply	Filters pending jobs based on the filter criteria.
Select: All	Selects all the pending jobs in the table displayed in the **Job List** section.
Select: None	Clears the selection for the pending jobs that you have selected.
Refresh	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
Criteria	The following three fields: • Field 1– The list of criteria that you can use to search the pending jobs. • Field 2 – The operators for evaluating the expression. The operators displayed depends on the type of criterion that you selected in the first field. • Field 3 – The value corresponding to the search criteria.

Button	Description
Clear	Clears the search value that you entered in the third field.
Search	Searches the pending jobs based on the specified search conditions and displays the search results in the **Groups** section.
Close	Cancels the search operation and hides the **Criteria** section.

Related links

Viewing pending jobs on page 691
Scheduler on page 689

Completed Jobs field descriptions

Name	Description
Job Type	The type of job, represented by a job type icon. The types of job with icons are: 1. System scheduled job. 2. Admin scheduled job. 3. On-demand job.
Job Name	The name of the scheduled job.
Job Status	The current status of the pending job. The types of status are: 1. Status Unknown 2. Interrupted 3. Failed 4. Successful 5. Not Authorized
Last Run	The date and time when the job was last run.
State	The state of a job, whether the job is active or inactive. The types of state are: • Enabled: An active job. • Disabled: An inactive job.
Frequency	The time interval between two consecutive executions of the job.
Scheduled By	The person who scheduled the job.

Button	Description
View	Displays the Job Scheduling-View Job page that displays the details and of the selected completed job.
Edit	Displays the Job Scheduling-Edit Job page that you can use to modify the information of a selected completed job.

Table continues…

Button	Description
Delete	Displays the Delete Confirmation page that prompts you to confirm the deletion of the selected Jobs.
More Actions > **View Log**	Displays the Logging page that displays the logs for the selected completed jobs.
More Actions > **Enable**	Changes the state of the selected completed job from inactive to active.
More Actions > **Disable**	Displays the Disable Confirmation page that prompts you to confirm the disabling of the selected completed job.
More Actions > **Schedule On Demand Job**	Displays the Job Scheduling-On Demand Job page that you can use to schedule an On Demand job.
Advanced Search	Displays fields that you can use to specify the search criteria for searching a completed job.
Filter: Enable	Displays fields under select columns that you can use to set filter criteria. This is a toggle button.
Filter: Disable	Hides the column filter fields without resetting the filter criteria. This is a toggle button.
Filter: Apply	Filters pending jobs based on the filter criteria.
Select: All	Selects all the completed jobs in the table displayed in the Job List section.
Select: None	Clears the selection for the completed jobs that you have selected.
Refresh	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
Criteria	Displays the following three fields: • Field 1 - The list of criteria that you can use to search the completed jobs. • 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. • Field 3 – The value corresponding to the search criteria.

Button	Description
Clear	Clears the search value that you entered in the third field.
Search	Searches the completed jobs based on the specified search conditions and displays the search results in the **Groups** section.
Close	Cancels the search operation and hides the **Criteria** section.

Related links

Viewing completed jobs on page 691
Scheduler on page 689

Job Scheduling-View Job field descriptions

Use this page to view the details and frequency of a job.

Job Details

Name	Description
Job Name	The name of the job.
Job Type	The type of job, represented by a job type icon. The types of job with icons are: 1. System scheduled job. 2. Admin scheduled job. 3. On-demand job.
Job Status	The current status of the job. The types of status are: 1. Running 2. Pending 3. Status Unknown 4. Interrupted 5. Failed 6. Successful 7. Not Authorized
Job State	The state of a job whether the job is active or inactive. The types of state are: • **Enabled**: An active job. • **Disabled**: An inactive job.

Job Frequency

Name	Description
Task Time	The date and time of running the job.
Recurrence	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.
Range	The number of recurrences or a date after which the job stops to recur.

Button	Description
View Log	Opens the Logging page that you can use to view the logs for the selected job.
Edit	Opens the Job Scheduling-Edit Job page that you can use to edit the pending job information.
Cancel	Closes the Job Scheduling-View Job page and returns to the Pending Jobs or Completed Jobs page.

Related links

Scheduler on page 689

Job Scheduling-Edit Job field descriptions

Job Details

Name	Description
Job Name	The name of the job.
Job Type	The type of job, represented by a job type icon. The types of job with icons are: 1. System scheduled job. 2. Admin scheduled job. 3. On-demand job. **Note:** You can only view the information in this field.

Table continues…

Name	Description
Job Status	The current status of the job. The types of status are: 1. Running 2. Pending 3. Status Unknown 4. Interrupted 5. Failed 6. Successful 7. Not Authorized **Note:** You can only view the information in this field.
Job State	The state of a job whether the job is active or inactive. The types of state are: • Enabled: An active job. • Disabled: An inactive job.
Scheduled By	The scheduler of the job. **Note:** You can only view the information in this field.

Job Frequency

Name	Description
Task Time	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.
Recurrence	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.
Range	The number of recurrences or the date after which the job stops to recur.

Button	Description
Commit	Saves the changes to the database.
Cancel	Closes the Job Scheduling-View Job page and returns to the Pending Jobs or Completed Jobs page.

Related links

Scheduler on page 689

Job Scheduling-On Demand Job field descriptions

Use this page to schedule an on-demand job.

Job Details

Name	Description
Job Name	The name of the job.

Job Frequency

Name	Description
Task Time	The date and time of running the job.
Recurrence	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: • Execute task one time only. • Task are repeated: - Minutes - Hourly - Daily - Weekly - Yearly
Range	The settings that define the number of recurrences or date after which the job stops recurring. The options are: • No End Date • End After occurrences • End By Date

Button	Description
Commit	Schedules an On-Demand job.
Cancel	Cancels the scheduling of an On Demand job operation and takes you back to the Pending Jobs or Completed Jobs page.

Disable Confirmation field descriptions

Use this page to disable selected jobs.

Name	Description
Job Type	The type of job, represented by a job type icon. The types of job with icons are: 1. System scheduled job. 2. Admin scheduled job. 3. On-demand job.
Job Name	The name of the scheduled job.
Job Status	The current status of the pending job. The types of status are: 1. Running 2. Pending 3. Status Unknown 4. Interrupted 5. Failed 6. Successful 7. Not Authorized
State	The state of a job whether the job is active or inactive. The types of state are: • **Enabled**: An active job. • **Disabled**: An inactive job.
Last Run	The date and time when the job was last run successfully. **Note:** The last run is applicable only for completed jobs.
Frequency	The time interval between two consecutive executions of the job.
Scheduled By	The scheduler of the job.

Button	Description
Continue	Disables the job and cancels the next executions that are scheduled for the job.
Cancel	Cancels the operation of disabling a job and takes you back to the Pending or completed Jobs page.

Related links

Scheduler on page 689

Stop Confirmation field descriptions

Use this page to stop a running job.

Name	Description
Job Type	The type of job, represented by a job type icon. The types of job with icons are: 1. System scheduled job. 2. Admin scheduled job. 3. On-demand job.
Job Name	The name of the scheduled job.
Job Status	The current status of the pending job. The jobs on this page have status Running.
State	The state of a job whether the job is active or inactive. The types of state are: • **Enabled**: An active job. • **Disabled**: An inactive job. All the jobs on this page are in the **Enabled** state.
Last Run	The date and time when the job was last run successfully. **Note:** The last run is applicable only for completed jobs.
Frequency	The time interval between two consecutive executions of the job.
Scheduled By	The scheduler of the job.

Button	Description
Continue	Stops the job.
Cancel	Cancels the operation of stopping a job and takes you back to the Pending Jobs page.

Related links

Scheduler on page 689

Delete Confirmation field descriptions

Name	Description
Job Type	The type of job, represented by a job type icon. The types of job with icons are: 1. System scheduled job. 2. Admin scheduled job. 3. On-demand job.
Job Name	The name of the scheduled job.
Job Status	The current status of the job.
State	The state of a job whether the job is active or inactive. The types of state are: • **Enabled**: An active job. • **Disabled**: An inactive job. The jobs on this page are in the **Disabled** state.
Last Run	The date and time when the job was last run. **Note:** The last run is applicable only for completed jobs.
Frequency	The time interval between two consecutive executions of the job.
Scheduled By	The scheduler of the job.

Button	Description
Continue	Deletes the selected job.
Cancel	Cancels the operation of deleting a job and takes you back to the Pending or completed Jobs page.

Related links

Scheduler on page 689

Chapter 14: SIP phone pre-configuration template

In Session Manager, Avaya provides support for pre-configuring endpoint-specific settings such as button assignments, Language and Region settings, and whether button clicks are enabled. Customers use administration screens on System Manager to centrally administer SIP phone settings that were previously only accessible from the SIP phone device itself.

When the user first logs in, the endpoint downloads the endpoint settings from the PPM and applies the values.

As an administrator you can configure the SIP phones from System Manager Web Console to provide a consistent appearance and user experience on the phones. This setting was previously available from the SIP phone.

On the System Manager Web Console, as an end user you can assign favorites, button labels and other settings for 96x1 SIP phones.

On the 96x1 SIP phones you can configure the following:

- Favorites: For quick access, you can set up to nine favorite items, such as contacts or features.
- Labels: You can change the labels for the extensions, features, the system numbers, and speed dial buttons. Labels are up to 15 characters in length.
- Auto-dial numbers: Auto-dial numbers are the frequently called numbers. The system administrator sets up auto-dial numbers, you can assign and edit their labels.
- Phone settings: You can set additional customized phone settings.

You can configure the settings mentioned here in a Communication Manager Endpoint template. The template, then, can be reused through System Manager by specifying the template in the Communication Manager Endpoint profile.

For the existing users, the administrator can edit the user details in the Endpoint Editor. To edit details of multiple users, the administrator can use Global Endpoint Change.

After the configuration using the System Manager Web Console, all endpoint settings data is stored in the System Manager database. The system replicates the settings changes to the Session Manager and Branch Session Manager databases. The Personal Profile Manager (PPM) makes these settings available to the user’s endpoints for reading and updating.

Note:

When the user logs in to the user's Endpoint for the first time, the administered template may not match the specific endpoint type of that Endpoint. For example, the administrator assigns a 9641 template to the user and the user logs in with a 9611 Endpoint. If the 9611 Endpoint does not support a specific 9641 setting, such as full screen mode, the 9611 Endpoint removes that setting since the setting does not apply to the 9611. The net effect is that the 9641 parameter is never administered. If that same user later logs in with a 9641 Endpoint, the removed 9641 setting is no longer present and the 9641 Endpoint does not reflect that setting.

Users can override template settings by changing the settings on the endpoint. The changes take effect immediately, assuming the changes are valid.

The system supports the SIP phone pre-configuration template for the following set types:

- 96x1SIP
- 96x1SIPCC

The following use cases are not supported:

- Applying a template to a group of existing users. Due to existing limitations, you can only apply a template to individual users, one at a time.
- Updating a template and propagating endpoint setting changes to all users and devices assigned to that template.

Software requirements for the SIP phone pre-configuration template

The software requirements for the SIP phone pre-configuration template are:

- Communication Manager 6.2 or 6.3.x and later
- System Manager 6.3.8 and later
- Session Manager 6.3.8 and later

Creating a new customized SIP phone template

Create a new customized SIP phone template. The administrator can change any of the parameter values in the new custom template.

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Templates** > **CM Endpoint**.

2. In the **Supported Feature Server Versions** table, select the appropriate software version for the **CM** System Type.
3. Click **Show List**.
4. Click the **Custom templates** tab.
5. Click **New** to create a new template.
6. On the **New Endpoint Template** screen, select the appropriate **Set Type** from the drop-down menu. The screen refreshes after you make a selection.
7. Enter a **Template Name**.
8. Under the **General Options** tab, enter the required information.
9. Click on the tabs and specify the endpoint settings for the new template.
10. Click **Commit**.

Creating a SIP phone template from a default template

Administrators can create a new customized template using a copy of a default template. The administrator can change any of the parameter values in the new template.

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Templates** > **CM Endpoint**.
2. In the **Supported Feature Server Versions** table, select the appropriate software version for the **CM**.
3. Click **Show List**.
4. Click the **Default templates** tab.
5. Select the appropriate template from the **Default Templates List**.
6. Click **Duplicate**.
7. On the **Duplicate Endpoint Template** screen, select the **Set Type** from the drop-down menu. The screen refreshes after you make a selection.
8. Enter the **New Template Name**.
9. On the **General Options** screen, enter the required information.
10. Click on the tabs and specify the endpoint settings as needed.
11. Click **Commit**.

Applying a SIP phone template to an existing user

You can also make changes by navigating to **Home** > **Users** > **User Management** > **Manage Users** and selecting and editing the user information.

Important:

When you apply a template to an existing user, the values in the template override all existing settings that are configurable using the System Manager Endpoint Editor. If a value is currently set on the endpoint and not set in the template, applying the template causes the setting on the endpoint to become unassigned.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Communication Manager** > **Endpoints** > **Manage Endpoints**.
2. Select the endpoint to which you want to apply the template.
3. Click **Edit**.
4. In the **Template** field, select the template you want to apply from the drop-down menu.
5. To customize other endpoint settings, make changes to any of the parameters on any of the tabs.
6. Click **Commit**.

Modifying endpoint settings for an existing user

This procedure describes how to modify the endpoint settings for an existing user.

Using the **Job Scheduler** screen, you can schedule endpoint setting changes to occur at a later time that might be less disruptive to the user, for example, midnight local time.

Important:

When the administrator commits the changes, the system sends the changes to the endpoint. Certain changes can be disruptive. Use caution when making changes and be aware of the impact of a change on a user.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Elements** > **Communication Manager** > **Endpoints** > **Manage Endpoints**.
2. Click **Show List**.
3. Select the **Name** of the endpoint you want to modify.
4. Click **Edit**.
5. Make the necessary changes.

6. When you finish modifying the settings do one of the following:
   - Click **Commit** to commit the changes, or
   - Click **Schedule**, specify the date and time to change the endpoint settings, and click **Schedule**.

Modifying endpoint settings for a group of existing users

This procedure describes how to modify the endpoint settings for a group of existing users using the Global Endpoint Change capability, also known as Global Search & Replace.

Using the **Job Scheduler** screen, you can schedule endpoint setting changes to occur at a later time that might be less disruptive to the user, for example, midnight local time.

Important:

When the administrator submits the changes, the system sends the changes to the endpoint. Certain changes can be disruptive. Use caution when making changes and be aware of the impact of a change on a user.

Before you begin

Perform a bulk import of a group of users to apply an initial set of endpoint settings. For example, LDAP import.

When using bulk import to define a group of users, import the users in such a way to easily identify those users with the Global Search & Replace criteria, for example, a sequential set of extensions.

If the Global Search & Replace criteria match multiple endpoint types, for example 9641 and 9611, you can change parameters that are applicable to one endpoint type but not the other.

Procedure

1. On the home page of the System Manager Web Console, under **Elements**, click **Elements** > **Communication Manager** > **Endpoints** > **Manage Endpoints**.
2. In the upper right corner of the **Endpoint List** table, click **Advanced Search**.
3. Enter the search criteria to obtain the list of endpoints you want to change.
4. Select the endpoints from the resulting list.
5. Click **More Actions** > **Global Endpoint Change**.
6. Change the settings under the appropriate tabs.
7. When you finish modifying the settings, do one of the following:
   - Click **Commit** to commit the changes, or
   - Click **Schedule**, specify the date and time to change the endpoint settings, and click **Schedule**.

Removing a SIP phone template

Delete a previously defined SIP phone template. Deleting a template makes it unavailable for future use. Removing a template does not directly affect endpoint settings.

Note:

You can only remove custom templates. You cannot remove default templates.

Procedure

1. On the home page of the System Manager Web Console, under **Services**, click **Templates** > **CM Endpoint**.
2. Select the template you want to delete.
3. Click **Delete**.

Chapter 15: SIP Team button

A SIP Team button has two functions: a display function and an execution function.

With the display function a member of the team (monitoring station) can observe the station state of another team member (monitored station). The station state of the monitored station is a combination of active calls and ringing calls on the station.

With the execution function, a member of the team can:

- Establish a call directly to the monitored station.
- Pick up a ringing call from the monitored station.
- Transfer an active call.
- Complete a transfer operation.
- Override the redirection of the monitored stations.

Feature operation and control are the same for H.323 and SIP.

The SIP Team button is supported on 1XC 6.2 and 96X1 SIP 6.2.4.

SIP Team button features

Features of the SIP Team button include:

- **Direct Transfer:** Transfer an active call. The call automatically is put on hold and the transfer-destination (monitored station) is called. The user does not need to press the transfer button.
- **Transfer Upon Hangup:** Complete a transfer operation when the user hangs up the phone. The user does not need to press the **Transfer Complete** button.
- **Override the Monitored Station's Forwarding:** The monitoring station overrides the redirection of the monitored station if the monitored station does not answer a call within a certain time. The system redirects the call according to the redirection policy of the monitoring station.

Administering the SIP Team button

The system takes about 3 minutes for the changes to download to the SIP phones after you make the changes.

Procedure

1. Administer the **Transfer Upon Hang-up** value, configured per Communication Manager.
2. Administer the COR values, configured per Communication Manager and per station.
3. Configure the Monitoring Station:
    a. On the home page of the System Manager Web Console, under **Users**, select **User Management** > **Manage Users**.
    b. Select the user to configure. This user is the **Monitoring Station**.
    c. Click **Edit**.
    d. On the **Communication Profile** page, select **CM Endpoint Profile**.
    e. Click **Endpoint Editor**, located next to the **Extension** field.
    f. On the **Edit Endpoint** page, select the **Button Assignment** tab.
    g. Select a button to be the Team button, and select **Team** from the drop-down menu.
    h. Enter the extension of the Monitored station/team member.
    i. Enter **y** or **n** to enable/disable ringing for the monitoring station.
    j. Select the **Enhanced Call Fwd** tab.
    k. In the **SAC/CF Override** field, select the appropriate value from the drop-down menu.
    l. Select the **General Options** tab and note the **Class of Restriction** for the Monitoring station.
    m. Click **Done**.
    n. Click **Commit**.
4. Determine the COR for the Monitored Station:
    a. Select the user to configure. This is the **Monitored Station**.
    b. Click **View**.
    c. On the **Communication Profile** page, select **CM Endpoint Profile**.
    d. Click **Endpoint Editor**, located next to the **Extension** field.
    e. Select the **General Options** tab and note the **Class of Restriction** for the Monitored station.
    f. Click **Cancel**, then click **Cancel** again.
5. Configure the **Transfer Upon Hang-up** value:
    a. On the home page of the System Manager Web Console, under **Elements**, select **Communication Manager** > **Parameters** > **System Parameters** > **Features**.
    b. Select the Communication Manager you want to change.
    c. Click **Edit**.

d. Click **Next Page** until you get to Page 7.
e. Under **Conference/Transfer**, set the **Transfer Upon Hang-Up?** value to **y** or **n**.
f. Click **Enter** to save the changes.

6. Configure the COR of the Monitoring station:
   a. On the home page of the System Manager Web Console, under **Elements**, select **Communication Manager** > **System** > **Class Of Restriction**.
   b. Select the COR of the Monitoring station for the correct Communication Manager.
   c. Click **Edit**.
   d. Go to Page 3.
   e. Set the value for **SAC/CF Override by Team Btn** to **y**.
   f. Click **Enter** to save the changes.
7. Configure the COR of the Monitored station:
   a. Select the COR of the Monitored station for the correct Communication Manager.
   b. Click **Edit**.
   c. Go to Page 3.
   d. Set the value for **SAC/CF Override Protection for Team Btn** to **n**.
   e. Click **Enter** to save the changes.

Chapter 16: Service Observing from SIP Phone

Using the Service Observing feature, a supervisor or authorized user can use a telephone to activate an observing session towards a station, an agent LoginID, or VDN to listen in and possibly talk on calls received by the station/agent or VDN for quality control and training purposes. The audio from the observed connection is switched in to the first idle appearance on the phone being used for the Service Observing feature. The observer remains off-hook or idle during the call.

The **sip-sobsrv** button appears on the station form for the 96x1 SIPCC and an Avaya one-X® Agent defined as a SIPCC station type only if the **Call Center Release** field is set to 7.0 or later. This button is not available for assignment to any other station type and limited to one per endpoint.

When the user assigns this button to a 96x1SIPCC station type, the following two options appear:

- **listen-only? :** The default is **n**. The service observing activation is in listen-only mode and cannot be changed to the **listen-talk** mode. An observer can change the talk mode from **listen-only** to **listen-talk**, and vice-versa, *only* while the observer is actively observing a call. The talk mode cannot be changed while the observer is in the wait state. If the observer changes the talk mode during a call, that specific talk mode stays active after the observed call is cleared, unless the user changes the talk mode prior to the clearing of the call.
- **coach?:** The default is **n**. The observer can activate coaching while observing a call that is connected to a local station or agent if the observer is in either listen-only or listen-talk mode.

The text string presented on the display of the endpoint depends on the observed entity's type (Station, AgentID, or VDN) and on the type of called number (Station, AgentID (DAC), or VDN).

For more information about this feature, see the following documentation on the Avaya Support website:

- *Avaya Aura® Call Center Elite Feature Reference*
- *Avaya Aura® Call Center Elite Overview and Specification*
- *Administering Avaya Aura® System Manager*
- *Administering Avaya Aura® Communication Manager*

Chapter 17: SNMP support for Session Manager

This section describes the procedures to create SNMP User and Target profiles and how to attach the profiles to Serviceability Agents.

The Session Manager SNMP master agent is installed as part of a factory installation. This agent provides basic IP discovery, inventory, and status capabilities through the MIB II and Host Resources MIBs for the server and Linux operating system. You configure the Session Manager agent using System Manager to assign an SNMP V3 user. The agent:

- Provides read-only access to the SNMP agent on the Session Manager server.
- Does not provide any SNMP Set capability to the Session Manager.
- Does not restrict the IP addresses to query the MIBs.
- Provides access control only using SNMP V3.

The System Manager server also provides a basic SNMP V3 agent.

For more information on fault management using SNMP, see *Avaya Aura® System Manager Fault Management and monitoring using SNMP* on the Avaya support web site.

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 SNMP and SNMP V3 traps/informs to the configured NMS destinations. Two of the mandatory destinations are System Manager and the SAL Gateway.

Using the Serviceability Agent user interface on System Manager, you can:

- Remotely manage and configure SNMP V3 users.
- Remotely manage and configure SNMP trap destinations.
- Create, edit, view, and delete user and target profiles, and attach or detach the profiles from agents.

The **Manage Serviceability Agents** interface has the following pages:

- **SNMPv3 User Profiles:** Create, view, edit, and delete SNMP V3 user accounts. The system uses these accounts for SNMP V3 traps/informs and for SNMP V3 queries of the SNMP master agent.
- **SNMP Target Profiles:** Create, view, edit, and delete SNMP trap/inform destinations for System Manager, SAL Gateway, and customer NMS. The profile setup interface supports both SNMP V2 and SNMP V3 with either a trap or inform type for notifications.
- **Notification Filter Profile:** Create, view, edit, and delete alarm notification profiles, and attach the profiles to serviceability agents.
- **Serviceability Agents:** Activate Serviceability agents. Send SNMP V3 user profiles and SNMP target profiles to the selected Serviceability Agents. The System Manager host name is automatically included in the list of agents.

Configuring the Session Manager Serviceability Agent

Configure the Session Manager serviceability agent to send alarm traps.

#	Action	Link/Notes	✔
1	View and note the System Manager TrapListener settings.	Viewing the SMGR TrapListener settings on page 733.	
2	Create an SNMP V3 user profile using the same settings as the System Manager TrapListener settings.	Creating an SNMPv3 user profile on page 722.	
3	Create an SNMP user profile and assign the System Manager user profile.	Creating an SNMP target profile on page 725. Use the following values: • **Port** 10162 • **Domain Type** UDP • **Protocol** V3	
4	Verify the Session Manager serviceability agent can register with System Manager.	Verifying the Session Manager serviceability agent registration on page 719.	
5	Assign the System Manager target profile.	Managing target profiles for the selected serviceability agents on page 720.	
6	Attach the user profile to the Session Manager serviceability agent.	Managing SNMPv3 user profiles for the selected serviceability agents on page 719.	
7	Verify the Session Manager serviceability agent can forward alarms to the System Manager.	Generating test alarms on page 720.	

Verifying the Session Manager serviceability agent registration

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Serviceability Agents** > **Serviceability Agents**.
2. Verify the Session Manager **Hostname** and **IP address** appear in the Agents List.
3. Verify the status of the Session Manager serviceability agent is **active**.
4. If the status of the Session Manager serviceability agent is not **active**, select the serviceability agent and click **Activate**.

Activating a serviceability agent

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left 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.

Managing SNMPv3 user profiles for the selected serviceability agents

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left 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.

Managing target profiles for the selected serviceability agents

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left 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.

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 that are 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 left 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 the alarm.

5. To view the alarm, click **Events** > **Alarms**.

   To view the details of the alarm, wait until the system displays the alarms on the Alarming page.

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 left 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 `restart sal-agent`.

   You can perform this step if you do not want to wait for the next heartbeat of the agent.

Serviceability Agents list

Name	Description
Hostname	The host name of the server on which the serviceability agent runs.
IP Address	The IP address of the server on which the serviceability agent runs.
System Name	The system name of the server on which the serviceability agent runs.
System OID	The system OID of the server on which the serviceability agent runs.

Table continues…

Name	Description
Status	The enabled or disabled status of the serviceability agent. The system disables SNMPv3 and displays **Inactive** as the default status.

Managing SNMPv3 user profiles

Creating an SNMPv3 user profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left 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**.

Editing an SNMPv3 user profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left 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**.

Viewing an SNMPv3 user profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.

2. In the left 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.

Deleting an SNMPv3 user profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left 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 left 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
User Name	The SNMPv3 user name. **Note:** The user name can contain the following characters: alphanumeric, period, underscore, white space, single quote, and hyphen. The user name cannot be blank.
Authentication Protocol	The authentication protocol used to authenticate the source of traffic from SNMP V3 users. The possible values are: • MD5 • SHA The default is MD5.
Authentication Password	The password used to authenticate the user. **Note:** 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.
Confirm Authentication Password	The authentication password that you re-enter for confirmation.
Privacy Protocol	The encryption policy for an SNMP V3 user. The possible values are: • DES: Use DES encryption for SNMP-based communication. • AES: Use AES encryption for SNMP-based communication. • None The default value is AES.
Privacy Password	The pass phrase used to encrypt the SNMP data.
Confirm Privacy Password	Retype the privacy password in this field for confirmation.

Table continues…

Name	Description
Privileges	The privileges that determines the operations that you can perform on MIBs. • Read/Write: Use to perform GET and SET operations. • Read: Use to perform only GET operation. • None. The default is None.

Button	Description
Commit	Use to create a new SNMPv3 user profile. Saves the changes after an edit operation.
Back	Cancels the action and takes you to the previous page.
Delete	Use to delete the user profiles you select.
Edit	Use to edit the user profile you select.

Managing SNMP target profiles

Creating an SNMP target profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left 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**.

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 left 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**.

Viewing an SNMP target profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left 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.

Deleting an SNMP target profile

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left 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.

Filtering target profiles

Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left 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.

SNMP Target profile list

Name	Description
Name	The name of the SNMP target profile. This name should be a unique value.
Domain Type	The type of transport for the flow of messages. The default value is UDP.
IP Address	The IP address of the SNMP target profile.
Port	The port of the SNMP target profile.
SNMP Version	The version of the SNMP protocol.

Button	Description
New	To go to the New Target Details page where you can add a new SNMP target profile.
View	To go to the View Target Details page where you can view an existing SNMP target profile.
Edit	To go to the Edit Target Details page where you can edit an existing SNMP target profile.
Delete	To delete the existing SNMP target profiles that you select.
Filter: Enable	To filter the SNMP target profiles list by one or multiple criteria.

SNMP target profiles field descriptions

Name	Description
Name	The name of the SNMP target profile.
Description	The description of the SNMP target profile.
IP Address	The IP address of the target.
Port	The port number of the target.
Domain Type	The type of the message flow. The default is UDP.
Notification Type	The type of notification. The options are: • Trap • Inform
Protocol	The type of the SNMP protocol.

Button	Description
Commit	Creates the target profile in the New Target Profile page or saves the changes in the Edit Target Profile page.
Back	Cancels your action and takes you to the previous page.

Notification Filter Profile

System Manager supports alarm filtering capability. You can select a product that System Manager supports and send filtered alarms only to specific targets.

When you send notifications to System Manager, a SAL Gateway, or a Network Management System (NMS), you can exclude or include notifications from certain elements. Using the Notification Filter Profile pages, you can:

- create filter profiles and assign the profiles to the target and serviceability agent pair.
- remove the filter profiles from the target and serviceability agent pair.
- select alarms that you want to receive from a product on an NMS.

An NMS can be a System Manager or a third-party system.

For a product, you can define the filter criteria to receive or block notifications on the target serviceability agent from specific Object Identifiers (OID)s.

Creating a Notification Filter Profile

Create a Notification Filter Profile to include or exclude alarms from the notification IDs that you select.

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Serviceability Agents** > **Notification Filter Profile**.
2. Click **New**.
3. Click the Filter Profile Details tab and enter the required information.
4. Select one of the following:
   - Select **Include** to include the notification OIDs.
   - Select **Exclude** to exclude the notification OIDs.
5. Click the Attach/Detach Notification Oids tab and do one of the following:
   - In the **Notification Subtree** field, enter a value that ends with dot star (.*) and click **Add**. For example: 6889.2.35.*
   - Do the following:
     a. Open the Select Notifications section.
     b. In the **Products** field, select a product from the drop-down menu.
     c. In the **NotificationOID** list, select one or more notification IDs.
6. Click **Commit**.

Viewing a Notification Filter Profile

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Serviceability Agents** > **Notification Filter Profile**.
2. Select a filter profile.
3. Click **View**.

Editing a Notification Filter Profile

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Serviceability Agents** > **Notification Filter Profile**.

2. Select a filter profile.
3. Click **Edit**.
4. Change the information as needed.
5. Click **Commit**.

Deleting a Notification Filter Profile

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Serviceability Agents** > **Notification Filter Profile**.
2. Select the filter profile or profiles you wish to delete.
3. Click **Delete**.
4. Click **Delete** on the confirmation page.

Assigning a Notification Filter Profile to a serviceability agent

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, you can add only one filter profile to the System Manager target for the same Session Manager system.

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Serviceability Agents** > **Serviceability Agents**.
2. Select the serviceability agent server from the **Serviceability Agents** list.
3. Click **Manage Profiles**.
4. Click the SNMP Target Profiles tab.
5. Select System Manager or the third-party NMS target agent, and click **Assign**.
6. To assign the filter profile from the serviceability agent:
   a. In the Removable Profiles section, select the target.
   b. After the **Assign/Remove Filter Profile** link becomes active, click the link.
   c. In the Profile List section, click the plus sign (+).

      The system displays the filter profile that you selected in the Assigned Filter Profiles section.
7. Click **Commit**.

Unassigning a Notification Filter Profile from a serviceability agent

Procedure

1. On the home page of the System Manager Web Console, in **Services**, click **Inventory** > **Manage Serviceability Agents** > **Serviceability Agents**.
2. Select the serviceability agent server from the **Serviceability Agents** list.
3. Click **Manage Profiles**.
4. Click the SNMP Target Profiles tab.
5. In the Removable Profiles section, select the target.
6. After the **Assign/Remove Filter Profile** link becomes active, click the link.
7. In the Profile List section, click the minus sign (-).

   The system displays the filter profile in the Profile List section.
8. Click **Commit** to disassociate the filter profile from the serviceability agent.

Filter Profiles field descriptions

Name	Description
Name	The name of the notification filter profile.
Description	A description of the notification profile.

Button	Description
New	Displays the New Filter Profile page where you can create a notification filter profile.
View	Displays the View Filter Profile page where you can view a notification filter profile.
Edit	Displays the Edit Filter Profile page where you can view a notification filter profile.
Delete	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
Name	The name of the notification filter profile.
Description	A description of the notification filter profile.
Specify Include/Exclude criteria	An option to include or exclude the notification OIDs. • **Include** • **Exclude** The default is **Include**.

Attach/Detach Notification Oids Specify Notification Subtrees

Name	Description
Notification Subtree	The notification subtree that you want to add to the subtree list. 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.
Add	Adds the notification subtree to the list.

Specify Notifications

Name	Description
Product	The product for which you want to filter the notifications while sending notifications to System Manager, SAL Gateway or other NMS systems.

Button	Description
Commit	Saves the changes made to the page and returns to the Filter Profile page.
Back	Discards the changes and returns to the Filter Profile page.

System Manager TrapListener service

The TrapListener service receives traps and informs from different applications and displays the traps and alarms on the System Manager alarming page.

The TrapListener receives SNMP V2 and SNMP V3 traps and informs the applications that are defined in the common alarm definition file. The TrapListener also processes the Common Alarm Definition file for applications, where all the trap definitions are present.

You configure the TrapListener service using the Service Profile Management pages on System Manager.

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**.

Viewing the System Manager TrapListener Service settings

Procedure

1. On the home page of the System Manager web console, under **Services**, click **Configurations** > **Settings** > **SMGR**.
2. Click **TrapListener**.
3. Click **Done** when you are finished viewing the settings.

TrapListener service field descriptions

Name	Description
Authentication Password	The password used to authenticate the user. The default is avaya123.
Authentication Protocol	The authentication protocol used to authenticate the source of traffic from SNMP V3 users. The options are: • md5 • SHA The default is md5.

Table continues…

Name	Description
Community	The community for TrapListener.
Privacy Password	The password that you use to encrypt the SNMP data. The default is avaya123.
Privacy Protocol	The encryption policy for an SNMP V3 user. The options are: • **DES**: Use the DES encryption for the SNMP-based communication. • **AES**: Use the AES encryption for the SNMP-based communication. The default is AES.
TrapListener Port	The port on which TrapListener listens. The default is 10162. The field is read-only.
V3 UserName	The SNMP V3 user name. The default is initial. 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
Commit	Saves the changes you have made in the **TrapListener Configuration Parameters** section.
Cancel	Cancels the edit and returns to the previous page.

Session Manager SNMP MIB

This section lists the SNMP MIB tables and objects that can be queried on the Session Manager server by a network management system on the same network as the Session Manager management interface. The Security Module is not included in this MIB. The Security Module is a different network interface and does not support SNMP queries.

- HOST-RESOURCES-MIB::hrDeviceDescr
- HOST-RESOURCES-MIB::hrDeviceErrors
- HOST-RESOURCES-MIB::hrDeviceID
- HOST-RESOURCES-MIB::hrDeviceIndex
- HOST-RESOURCES-MIB::hrDeviceStatus

- HOST-RESOURCES-MIB::hrDeviceType
- HOST-RESOURCES-MIB::hrDiskStorageAccess
- HOST-RESOURCES-MIB::hrDiskStorageCapacity
- HOST-RESOURCES-MIB::hrDiskStorageMedia
- HOST-RESOURCES-MIB::hrDiskStorageRemoveble
- HOST-RESOURCES-MIB::hrFSAccess
- HOST-RESOURCES-MIB::hrFSBootable
- HOST-RESOURCES-MIB::hrFSIndex
- HOST-RESOURCES-MIB::hrFSLastFullBackupDate
- HOST-RESOURCES-MIB::hrFSLastPartialBackupDate
- HOST-RESOURCES-MIB::hrFSMountPoint
- HOST-RESOURCES-MIB::hrFSRemoteMountPoint
- HOST-RESOURCES-MIB::hrFSStorageIndex
- HOST-RESOURCES-MIB::hrFSType
- HOST-RESOURCES-MIB::hrMemorySize
- HOST-RESOURCES-MIB::hrNetworkIfIndex
- HOST-RESOURCES-MIB::hrPartitionFSIndex
- HOST-RESOURCES-MIB::hrPartitionID
- HOST-RESOURCES-MIB::hrPartitionIndex
- HOST-RESOURCES-MIB::hrPartitionLabel
- HOST-RESOURCES-MIB::hrPartitionSize
- HOST-RESOURCES-MIB::hrProcessorFrwID
- HOST-RESOURCES-MIB::hrProcessorLoad
- HOST-RESOURCES-MIB::hrSWRunPerfCPU
- HOST-RESOURCES-MIB::hrSWRunPerfMem
- HOST-RESOURCES-MIB::hrStorageAllocationUnits
- HOST-RESOURCES-MIB::hrStorageDescr
- HOST-RESOURCES-MIB::hrStorageIndex
- HOST-RESOURCES-MIB::hrStorageSize
- HOST-RESOURCES-MIB::hrStorageType
- HOST-RESOURCES-MIB::hrStorageUsed
- HOST-RESOURCES-MIB::hrSystemDate

- HOST-RESOURCES-MIB::hrSystemInitialLoadDevice
- HOST-RESOURCES-MIB::hrSystemInitialLoadParameters
- HOST-RESOURCES-MIB::hrSystemMaxProcesses
- HOST-RESOURCES-MIB::hrSystemNumUsers
- HOST-RESOURCES-MIB::hrSystemProcesses
- HOST-RESOURCES-MIB::hrSystemUptime
- IF-MIB::ifAdminStatus
- IF-MIB::ifDescr
- IF-MIB::ifInDiscards
- IF-MIB::ifInErrors
- IF-MIB::ifInNUcastPkts
- IF-MIB::ifInOctets
- IF-MIB::ifInUcastPkts
- IF-MIB::ifInUnknownProtos
- IF-MIB::ifIndex
- IF-MIB::ifLastChange
- IF-MIB::ifMtu
- IF-MIB::ifNumber
- IF-MIB::ifOperStatus
- IF-MIB::ifOutDiscards
- IF-MIB::ifOutErrors
- IF-MIB::ifOutNUcastPkts
- IF-MIB::ifOutOctets
- IF-MIB::ifOutQLen
- IF-MIB::ifOutUcastPkts
- IF-MIB::ifPhysAddress
- IF-MIB::ifSpecific
- IF-MIB::ifSpeed
- IF-MIB::ifType
- SNMPv2-MIB::snmpEnableAuthenTraps
- SNMPv2-MIB::snmpInASNParseErrs
- SNMPv2-MIB::snmpInBadCommunityNames

- SNMPv2-MIB::snmpInBadCommunityUses
- SNMPv2-MIB::snmpInBadValues
- SNMPv2-MIB::snmpInBadVersions
- SNMPv2-MIB::snmpInGenErrs
- SNMPv2-MIB::snmpInGetNexts
- SNMPv2-MIB::snmpInGetRequests
- SNMPv2-MIB::snmpInGetResponses
- SNMPv2-MIB::snmpInNoSuchNames
- SNMPv2-MIB::snmpInPkts
- SNMPv2-MIB::snmpInReadOnlys
- SNMPv2-MIB::snmpInSetRequests
- SNMPv2-MIB::snmpInTooBigs
- SNMPv2-MIB::snmpInTotalReqVars
- SNMPv2-MIB::snmpInTotalSetVars
- SNMPv2-MIB::snmpInTraps
- SNMPv2-MIB::snmpOutBadValues
- SNMPv2-MIB::snmpOutGenErrs
- SNMPv2-MIB::snmpOutGetNexts
- SNMPv2-MIB::snmpOutGetRequests
- SNMPv2-MIB::snmpOutGetResponses
- SNMPv2-MIB::snmpOutNoSuchNames
- SNMPv2-MIB::snmpOutPkts
- SNMPv2-MIB::snmpOutSetRequests
- SNMPv2-MIB::snmpOutTooBigs
- SNMPv2-MIB::snmpOutTraps
- SNMPv2-MIB::snmpProxyDrops
- SNMPv2-MIB::snmpSilentDrops
- SNMPv2-MIB::sysContact
- SNMPv2-MIB::sysDescr
- SNMPv2-MIB::sysLocation
- SNMPv2-MIB::sysName
- SNMPv2-MIB::sysORDescr

- SNMPv2-MIB::sysORID
- SNMPv2-MIB::sysORLastChange
- SNMPv2-MIB::sysORUpTime
- SNMPv2-MIB::sysObjectID
- TCP-MIB::tcpActiveOpens
- TCP-MIB::tcpAttemptFails
- TCP-MIB::tcpCurrEstab
- TCP-MIB::tcpEstabResets
- TCP-MIB::tcpInErrs
- TCP-MIB::tcpInSegs
- TCP-MIB::tcpMaxConn
- TCP-MIB::tcpOutRsts
- TCP-MIB::tcpOutSegs
- TCP-MIB::tcpPassiveOpens
- TCP-MIB::tcpRetransSegs
- TCP-MIB::tcpRtoAlgorithm
- TCP-MIB::tcpRtoMax
- TCP-MIB::tcpRtoMin
- UDP-MIB::udpInDatagrams
- UDP-MIB::udpInErrors
- UDP-MIB::udpNoPorts
- UDP-MIB::udpOutDatagrams

Chapter 18: Resources

Documentation

The following documents are available at http://support.avaya.com.

For the latest information, see the Session Manager Release Notes.

Title	Description	Audience
Overview		
Avaya Aura® Session Manager Overview and Specification	Describes the key features of Session Manager.	IT management System administrators
Avaya Aura® Virtualized Environment Solution Description	Describes the Avaya Virtualized Environment, design considerations, topology, and resources requirements.	Sales engineers Implementation engineers Support personnel
Avaya Aura® Session Manager Security Design	Describes the security considerations, features, and solutions for Session Manager.	Network administrators, services, and support personnel
Avaya Aura® Session Manager 7.1 Release Notes	Contains enhancements, fixes, and workarounds for the Session Manager 7.1 release.	System administrators Services and support personnel
Implementation		
Deploying Avaya Aura® applications from System Manager	Describes how to deploy the Avaya Aura® virtual applications using the System Manager Solution Deployment Manager.	Services and support personnel
Deploying Avaya Aura® Session Manager	Describes how to deploy the Session Manager virtual application in a virtualized environment.	Services and support personnel
Deploying Avaya Aura® Branch Session Manager	Describes how to install and configure Branch Session Manager in a virtualized environment.	Services and support personnel

Table continues…

Title	Description	Audience
Routing Web Service API Programming Reference	Describes how to use the System Manager Routing Web Service API for Session Manager.	Services and support personnel
Upgrading and Migrating Avaya Aura® applications from System Manager	Describes how to upgrade and migrate the Avaya Aura® virtual applications using System Manager Solution Deployment Manager.	Services and support personnel
Using		
Using the Solution Deployment Manager client	Deploy and install patches for Avaya Aura applications.	System administrators
Administration		
Administering Avaya Aura® Session Manager	Describes the procedures to administer Session Manager using System Manager.	System administrators
Administering Avaya Aura® Communication Manager Server Options	Describes the procedures to administer Communication Manager as a feature server or an evolution server. Provides information related to Session Manager administration.	System administrators
Avaya Aura® Session Manager Case Studies	Provides common administration scenarios.	System administrators
Installation and upgrades		
Installing the Dell™ PowerEdge™ R610 Server	Describes the installation procedures for the Dell™ PowerEdge™ R610 server.	Services and support personnel
Installing the Dell™ PowerEdge™ R620 Server	Describes the installation procedures for the Dell™ PowerEdge™ R620 server.	Services and support personnel
Installing the Dell™ PowerEdge™ R630 Server	Describes the installation procedures for the Dell™ PowerEdge™ R630 server.	Services and support personnel
Installing the HP ProLiant DL360 G7 Server	Describes the installation procedures for the HP ProLiant DL360 G7 server.	Services and support personnel
Installing the HP ProLiant DL380p G8 Server	Describes the installation procedures for the HP ProLiant DL380p G8 server.	Services and support personnel
Installing the HP ProLiant DL360 G9 Server	Describes the installation procedures for the HP ProLiant DL360 G9 server.	Services and support personnel
Upgrading Avaya Aura® Session Manager	Describes the procedures to upgrade Session Manager to the latest software release.	Services and support personnel
Migrating and Installing Avaya Aura® Appliance Virtualization Platform	Describes the migration and installation procedures for Appliance Virtualization Platform.	Services and support personnel
Using the Solution Deployment Manager client	Describes the patch deployment and installation procedure for Avaya Aura® applications.	Services and support personnel

Table continues…

Title	Description	Audience
Maintaining and Troubleshooting		
Maintaining Avaya Aura® Session Manager	Contains the procedures for maintaining Session Manager.	Services and support personnel
Troubleshooting Avaya Aura® Session Manager	Contains the procedures to troubleshoot Session Manager, resolve alarms, and replace hardware.	Services and support personnel

Finding documents on the Avaya Support website

Procedure

1. Navigate to http://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 an appropriate release number.
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 displays the documents only from 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 more of the following categories:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

   The list displays the product-specific Port Matrix document.

7. Click **Enter**.

Training

The following table contains courses that are available on https://www.avaya-learning.com. To search for the course, in the **Search** field, enter the course code and click **Go**.

New training courses are added periodically. Enter **Session Manager** in the **Search** field to display the inclusive list of courses related to Session Manager.

Course code	Course title
1A00236E	Knowledge Access: Avaya Aura® Session and System Manager Fundamentals
4U00040E	Knowledge Access: Avaya Aura® Session Manager and System Manager Implementation
5U00081V	Session Manager Administration
5U00082I	Session Manager and System Manager Administration
5U00082R	Session Manager and System Manager Administration
5U00050E	Knowledge Access: Avaya Aura® Session Manager and System Manager Support
5U00095V	System Manager Implementation, Administration, Maintenance and Troubleshooting
5U00096V	Avaya Aura® Session Manager Implementation, Administration, Maintenance and Troubleshooting
5U00097I	Avaya Aura® Session and System Manager Implementation, Administration, Maintenance and Troubleshooting
5U00105W	Avaya Aura® Session Manager Overview
ATC01840OEN	Survivable Remote Session Manager Administration
ATU00171OEN	Session Manager General Overview
ATC00175OEN	Session Manager Rack and Stack
ATU00170OEN	Session Manager Technical Overview
2011V	What is new in Avaya Aura® System Manager 7.0 and Avaya Aura® Session Manager 7.0

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 http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at http://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 743

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 743

Appendix A: Restricted commands for the Security Module

The Security Module is also known as SM100 and ASSET.

Caution:

Only use System Manager to manipulate the Security Module interface. *Do not use any Linux administration tools that involve the Security Module interface, other than status commands, on the Session Manager platform.*

The following Linux commands do not work correctly or persistently, and can cause Session Manager to enter an irrecoverable state. *Do not use the following commands*:

- **`systemctl start/stop/restart network`**
- **`ifup`**
- **`ifdown`**
- **`route`**
- **`ip`**
- **`ethtool`**
- **`iptables`**

Appendix B: Regular Expression constructs

For more information, see the information regarding patterns at http://download.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html.

Construct	Matches
Characters	
x	The character x
\\	The backslash character
Character classes	
[abc]	a, b, or c (simple class)
[^abc]	Any character except a, b, or c (negation)
[a-zA-Z]	a through z or A through Z, inclusive (range)
[a-d[m-p]]	a through d, or m through p: [a-dm-p] (union)
[a-z&&[def]]	d, e, or f (intersection)
[a-z&&[^bc]]	a through z, except for b and c: [ad-z] (subtraction)
[a-z&&[^m-p]]	a through z, and not m through p: [a-lq-z](subtraction)
Predefined character classes	
.	Any character (may or may not match line terminators)
\d	A digit: [0-9]
\D	A non-digit: [^0-9]
\s	A whitespace character: [\t\n\x0B\f\r]
\S	A non-whitespace character: [^\s]
\w	A word character: [a-zA-Z_0-9]
\W	A non-word character: [^\w]
java.lang.Character classes (simple java character type)	
\p{javaLowerCase}	Equivalent to java.lang.Character.isLowerCase()
\p{javaUpperCase}	Equivalent to java.lang.Character.isUpperCase()
\p{javaWhitespace}	Equivalent to java.lang.Character.isWhitespace()
\p{javaMirrored}	Equivalent to java.lang.Character.isMirrored()

Table continues…

Construct	Matches
Classes for Unicode blocks and categories	
\p{InGreek}	A character in the Greek block (simple block)
\p{Lu}	An uppercase letter (simple category)
\p{Sc}	A currency symbol
\P{InGreek}	Any character except one in the Greek block (negation)
[\p{L}&&[^\p{Lu}]]	Any letter except an uppercase letter (subtraction)
Boundary matchers	
^	The beginning of a line
$	The end of a line
Greedy quantifiers	
X?	X, once or not at all
X*	X, zero or more times
X+	X, one or more times
X{n}	X, exactly n times
X{n,}	X, at least n times
X{n,m}	X, at least n but not more than m times
Logical operators	
XY	X followed by Y
X|Y	Either X or Y

Appendix C: Product notifications

Avaya issues a product change notice (PCN) for a software update. A PCN accompanies a service pack or patch that must be applied universally.

Avaya issues a product support notice (PSN) when there is a change in a product. A PSN provides information such as a workaround for a known problem and steps to recover software.

Both of these types of notices alert you to important issues that directly impact Avaya products.

Viewing PCNs and PSNs

Procedure

1. Go to the Avaya Support website at http://support.avaya.com.
2. Enter your login credentials, if applicable.
3. On the top of the page, click **DOCUMENTS**.
4. In the **Enter your Product Here** field, enter the name of the product, then select the product from the drop-down menu.
5. In the **Choose Release** field, select the specific release from the drop-down menu.
6. In the list of filters, select the **Product Correction Notices** and/or **Product Support Notices** check box.

   Note:

   You can select multiple filters to search for different types of documents at one time.
7. Click **Enter**.

Registering for product notifications

Note:

This procedure applies only to registered Avaya customers and business partners with an SSO login.

Procedure

1. Go to the Avaya Support website at http://support.avaya.com.
2. Log in using your SSO credentials.
3. Click on the **MY PROFILE** link.
4. Click the highlighted **HI, <username>** tab.
5. Select **E Notifications** from the menu.
6. In the **Product Notifications** section:
   a. Click **Add More Products**.
   b. Select the appropriate product.
7. In the Product box that appears on your screen:
   a. Select the appropriate release or releases for which you want to receive notifications.
   b. Select which types of notifications you want to receive. For example, **Product Support Notices** and **Product Correction Notices (PCN)**.
   c. Click **Submit**.
8. If you want notifications for other products, select another product from the list and repeat the above step.
9. Log out.

Appendix D: 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, CallPilot profiles, IP Office profiles, agent profiles, Session Manager profiles, Presence profiles, Avaya Breeze™, Work Assignment, Conferencing, Officelinx, and Avaya Equinox 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 <
- Ampersand character (&) as &
- Greater-than character (>) as >
- Double-quote character (") as "
- Apostrophe or single-quote character (') as '

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: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:xmLocalizedNames" 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: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>
                        <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 = "!" / "$" / "&amp;" / "'" / "(" / ")" / "*" / "+" / "," / ";" / "="
     ---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 with 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 CSCommProfile
        uniqueness constraint include type, cs_commprofile_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 with 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 inlcude 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: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>
      <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 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/rts"
    xmlns="http://www.avaya.com/rts"
    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: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"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1" isTrusted="false"
name="Test5">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
```

```
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1" isTrusted="false"
name="Test6">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1" isTrusted="false"
name="Test7">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1" isTrusted="false"
name="Test8">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1" isTrusted="false"
name="Test9">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1" isTrusted="false"
name="Test10">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1" isTrusted="false"
name="Tes11t">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1" isTrusted="false"
name="Test12">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1" isTrusted="false"
name="Test13">
            <Host description="Host" ipaddress="localhost" ostype="Host"/>
            <ApplicationSystemType name="Other Applications" version="0"/>
        </ApplicationSystem>
        <ApplicationSystem description="Test" displaykey="NewGateway1" isTrusted="false"
name="Test14">
            <Host description="Host" ipaddress="localhost" ostype="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>

        <!--
        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 Mananger" instance ('Secondary SM')
            "Termination Sequence" ('Sequence to My CM'),
            "Origination Sequence" ('Sequence to My CM'),
```

```
            "Conference Factory Set" ('EngeeringDepartmentConferenceSet')
            "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>EngeeringDepartmentConferenceSet</
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: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 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.
                -->
                <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
                    is used by the PIM module of the 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. Available for all analog and IP
                    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 service
                    link provides the actual connection between the Avaya DEFINITY Server
                    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               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
                    trunks. Do not use 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. Please contact your Avaya representative if you have
                    questions about emergency calls from IP telephones. Available only if
                    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:
                                                If the administrator chooses to leave the
Emergency Location
                                                Extension fields (that correspond to this
station's IP address) on
                                                the IP Address Mapping screen blank, the
value as-on-local
                                                sends the extension entered in the Emergency
Location
                                                Extension field in the Station screen to the
Public Safety
                                                Answering Point (PSAP).
                                                If the administrator populates the IP Address
Mapping screen with
                                                emergency numbers, the value as-on-local
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 value as-on-
local 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 value as-on-
local sends the
                                                extension in the IP Address Mapping screen to
the Public Safety
                                                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
                                             the call is blocked, they can dial 911 from a
nearby circuit-switched
                                             telephone instead.

                    cesid                    Enter cesid to allow 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.
                                             Use this entry for IP Softphones with road
warrior service that are near
                                             enough to the Avaya S8XXX Server that an
emergency call routed over
                                             the it's trunk reaches the PSAP that covers
the server or switch.
                                             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                     Enter option to allow the user to select
the option (extension, block, or
                                             cesid) that the user selected during
registration and the IP Softphone
                                             reported. Use this entry for extensions that
can be swapped back and
                                             forth between IP Softphones and a telephone
with a fixed location.
                                             The user chooses between block and cesid on
the softphone. A DCP or
                                             IP telephone in the office automatically
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
                    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
                    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.
                -->
                            <xs:element name="autoSelectAnyIdleAppearance"
type="xs:boolean" maxOccurs="1" minOccurs="0" />

                <!--
                    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.
                -->

                <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™ 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™ 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>
        <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_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>
        <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>
        <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 Officelinx 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 Officelinx 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>
        <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 overrriding  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][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: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 and CallPilot Communication 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/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 and CallPilot 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:propert>Y
                        <ns3:property name="prefDn">8054</ns3:propert>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 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="DNDExceptions" 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: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="AnnexlSupport" 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="NSFOveride" 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: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="EUAEnable"/>
      <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: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="EUATwinnedMobileNumber"/>
      <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="EUAForwardNumber"/>
      <xs:element type="xs:string" name="EUAForwardBusyNumber"/>
      <xs:element type="xs:string" name="EUAForwardOnBusy"/>
      <xs:element type="xs:string" name="EUAForwardOnNoAnswer"/>
      <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: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:AnnexlSupport>false</csm:AnnexlSupport>
                  <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:EUAuth>
            <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:EUADNDExceptions>0</csm:EUADNDExceptions>
            <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:EUATwinnedMobileNumber>0</csm:EUATwinnedMobileNumber>
                    <csm:EUALoginCode>0</csm:EUALoginCode>
                    <csm:EUADenyAutoIntercomCalls>0</csm:EUADenyAutoIntercomCalls>
                    <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:EUADSSKeys>0</csm:EUADSSKeys>
                    <csm:EUAVoicemailRingback>0</csm:EUAVoicemailRingback>
                    <csm:EUAConferencePIN>0</csm:EUAConferencePIN>
                  </csm:EUAuth>
                  <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:Datab>=</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:PopupRinging>false</csm:PopupRinging>
                <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:StayInCompactModeOnIncommingCall>false</
csm:StayInCompactModeOnIncommingCall>
                <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:PAServicesEnabled>false</csm:PAServicesEnabled>
                <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:DNDExceptions />
                <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: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:PMType>0</csm:PMType>
                <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>
<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_0Decription_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">

<!--
    This is the XML schema for the Avaya Aura Conferencing 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="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="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: 5555555@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: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.
                    ---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 with 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 inlcude 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.
                </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>
                        <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 with 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 inlcude 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: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: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: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: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

```
&lt;?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: • BASIC • ENTERPRISE
description	A description of the user. A human readable description of this user instance.	Optional	
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	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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.
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.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
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	
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	The options are: • English (United States) - en_US • Chinese (Simplified) - zh_CN • Japanese (Japan) - ja_JP • Korean (Korea) - ko_KR • French (France) - fr_FR • German (Germany) - de_DE • Italian (Italy) - it_IT • Russian (Russia) - ru_RU • English (United Kingdom) - en_GB • Spanish (Mexico) - es_MX • Portugese (Brazil) - pt_BR • French (Canada) - fr_CA • English (Canada) - en_CA
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: AUTHPENDING; PENDINGAUTHZ; 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	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 TimeZone.getTimeZone("Europe/Moscow"); In the absence of a value, the system uses the local services timezone. **Note:** While using the suggested **timeZone** values, consider daylight saving time (DST) and summer time adjustments. Typically, you add 1 hour to the offset. **Note:** In the import xml files, make the following changes while using specific characters: • less-than character (<) as < < • ampersand character (&) as & • greater-than character (>) as > • double-quote character (") as " • apostrophe or single-quote character (') as '	Optional	(-12:0)International Date Line West (-11:0)Midway Island, Samoa (-10:0)Hawaii (-9:0)Alaska (-8:0)Pacific Time (US & Canada); Tijuana (-7:0)Mountain Time (US & Canada); Chihuahua, La Paz (-7:0)Arizona (-6:0)Central Time (US & Canada); Guadalajara, Mexico City (-6:0)Central America; Saskatchewan (-5:0)Indiana (East); Bogota, Lima, Quito (-5:0)Eastern Time (US & Canada) (-4:0)Caracas, La Paz (-4:0)Atlantic Time (Canada); Santiago, Manaus (-3:30)Newfoundland (-3:0)Georgetown (-3:0)Brasilia, Greenland, Buenos Aires, Montevideo (-2:0)Mid-Atlantic (-1:0)Azores (-1:0)Cape Verde Is. (0:0)Monrovia, Reykjavik

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			(0:0)GMT : Dublin, Edinburgh, Lisbon, London, Casablanca (+1:0)West Central Africa (+1:0)Amsterdam, Berlin, Rome, Belgrade, Prague, Brussels, Sarajevo (+2:0)Harare, Pretoria (+2:0)Amman, Athens, Minsk, Beirut, Cairo, Jerusalem, Helsinki, Windhoek (+3:0)Baghdad, Kuwait, Riyadh, Nairobi, Tbilisi (+3:0)Moscow, St. Petersburg, Volgograd (+3:30)Tehran (+4:0)Abu Dhabi, Muscat, Caucasus Standard Time (+4:0)Baku, Tbilisi, Yerevan (+4:30)Kabul (+5:0)Islamabad, Karachi, Tashkent, Ekaterinburg (+5:30)Chennai, Kolkata, Mumbai, New Delhi, Sri Jayawardenepura (+5:45)Kathmandu (+6:0)Astana, Dhaka, Almaty, Novosibirsk (+6:30)Rangoon (+7:0)Bangkok, Hanoi, Jakarta, Krasnoyarsk

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			(+8:0)Beijing, Hong Kong, Singapore; Taipei (+8:0)Perth; Irkutsk, Ulaan Bataar (+9:0)Seoul, Osaka, Sapporo, Tokyo (+9:0)Yakutsk (+9:30)Darwin, Adelaide (+10:0)Brisbane, Guam, Port Moresby (+10:0)Canberra, Melbourne, Sydney, Hobart, Vladivostok (+11:0)Magadan, Solomon Is., New Caledonia (+12:0)Auckland, Wellington (+12:0)Fiji, Kamchatka, Marshall Is. (+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	Defines the delete type of the user. If the user selects: • soft: The system does not delete the user record permanently. You can recover the user record. • permanent: The system permanently deletes all attributes associated with the user and the links to public contacts and shared addresses.	Mandatory	The options are: • soft • permanent
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 cmName	The name of the Communication Managersystem as it appears in the Applications/Application Management/Entities.	Mandatory	
Use Existing Extension useExistingExtension	Select **true** if you want to use an already created extension. Select **false** if you want to use an available extension.	Optional	
Template Name 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 setType	The set type of the endpoint.	Optional	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
Port port	The valid port value.	Optional	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. 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. 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.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
Delete endpoint is unassigned deleteOnUnassign	Specifies whether the endpoint must be deleted if it is unassigned from the user.	Optional	
Lock messages feature. lockMessages	Select to enable the lock messages feature.	Optional	Select true or false to enable or disable the lock messages feature respectvely.
Coverage Path 1 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 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 tn	Provides partitioning of attendant groups and endpoints and trunk groups. 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 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 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 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.). 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 personalizedRingingPattern	The personalized ringing pattern for the endpoint. Personalized Ringing allows the users of some telephones to have one of the eight ringing patterns for incoming calls. 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 Valid Entries Usage: 1. MMM (standard ringing) 2. HHH 3. LLL 4. LHH 5. HHL 6. HLL 7. HLH 8. LHL
Message Lamp Extension 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 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. 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. Blank: Leave this field blank for single-connect IP applications.
IP Softphone ipSoftphone	Specifies whether the endpoint is an IP soft phone.	Optional	

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
Servivable GK Node Name survivableGkNodeName	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 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 (46xxor 96xx set types).	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 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	Valid Entries: Usage emergency - This endpoint can only be used to place emergency calls. Internal - This endpoint can only make intra-switch calls. This is the default value. 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. 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. 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.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
Survivable Trunk Destination 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: 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. false - Prevents this endpoint from receiving incoming trunk calls when the endpoint in survivable mode.
Voice Mail Number voiceMailNumber	Enter the complete Voice Mail Dial Up number.	Optional	String
offPremisesStation	Analog telephones only.	Optional	Valid entries Usage: • 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. • 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 `analog`. Else, enter the data module if applicable, or enter `none`.	Optional	Valid entries: analog, none.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
Message Waiting Indicator 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 **true** to use this endpoint as an endpoint in a remote office configuration.	Optional	Valid entries: • 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.
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: • single • continuous • if-busy-single • silent

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 • continuous - Select continuous to cause all calls to this telephone to ring continuously. • 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. • silent-if-busy - Select silent-if-busy to cause calls to ring silently when this endpoint is busy. • single - Select single to cause calls to this telephone to receive one ring cycle and then ring silently.
switchhookFlash	Set this field to true when the **Type** 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	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: • 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	Optional	Valid entries: as-needed permenant

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
	to disconnect a multimedia call and then make another multimedia call without having to wait for the service link to disconnect and reestablish. • 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 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.		

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
multimediaMode	There are two multimedia modes, Basic and Enhanced.	Optional	Basic - A basic multimedia complex consists of a BRIconnected multimedia-equipped PC and a non-BRI-connected multifunction telephone set. Enhanced - An enhanced multimedia complex consists of a BRI-connected multimediaequipped PC and a non-BRIconnected multifunction telephone.
mwiServedUserType	Controls the auditing or interrogation of a served user's message waiting indicator (MWI).	Optional	Valid entries: 1. fp-mwi - Select this option if the endpoint is a served user of an fp-mwi message center. 2. qsig-mwi - Select this option if the endpoint is a served user of a qsig-mwi message center. 3. sip adjuncts - Select this option if the endpoint is a served user of a sip adjunct message center. 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.
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: 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. 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. 3. no - Enter no to require administration in order to move the DCP telephone. 4. done - Done is a display-only value. Communication Manager sets the field to done after the telephone is moved and routine maintenance runs

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			on the DCP telephone. 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.
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	Valid entries: 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) 2. Block - Block prevents the completion of emergency calls. 3. Cesid - Cesid allows Communication Manager to send the CESID information supplied by the IP Softphone to the PSAP. 4. Option - Option allows the user to select the option (extension, block, or cesid) that the user selected during registration.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
emergencyLocationExt	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. 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	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	Valid entries: 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. 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. 3. none: All calls ended to this endpoint receive an

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
			audible ringing treatment. 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. 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 attendantoriginated 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. Distinctive ringing might not work properly for off-premises telephones.	Optional	
restrictLastAppearance		Optional	Valid entries: 1. true: Restricts the last idle call appearance used for incoming priority calls and outgoing call originations only. 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: 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. 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.

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
perStationCpnSendCallingNumber	Send Calling Number	Optional	Valid entries: 1. y: All outgoing calls from the endpoint will deliver the Calling Party Number (CPN) information as Presentation Allowed. 2. n: No CPN information is sent for the call. 3. r: Outgoing non-DCS network calls from the endpoint will deliver the Calling Party Number information as Presentation Restricted.
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	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. 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.	Optional	Boolean

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
selectLastUsedAppearance		Optional	Valid entries: 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. 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.
coverageAfterForwarding	Specifies whether an unanswered forwarded call is provided coverage treatment.	Optional	
directIpIpAudioConnections	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: 1. restricted 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: 1. enhanced 2. group 3. personal 4. system
listId	This is a Station Data module field.	Optional	
specialDialingOption	This is a Station Data module field.	Optional	Valid values: 1. default 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	This is a Native Name Data field. **Note:** If the **displayName**, **givenName**, or **surname** contains characters of multiple scripts then the locale tag should be present. The locale for the multiscript languages are: • Japanese: **ja** • Simplified Chinese: **zh-cn** • Traditional Chinese: **zh-tw** • Korean: **ko-kr** • Vietnamese: **vi-vn** The locale tag is case sensitive. 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.	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
			If you select **Calculate Route Pattern** check box, the system: • Populates the **Sip Trunk** field • Makes **Sip Trunk** field read-only.
		Optional	

Attribute details defined in the Messaging communication profile XSD

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
Messaging System Name messagingName	The name of Messaging System	Mandatory	
Use Existing Mailbox number useExisting	true if already created mailbox number is to be used. false if available mailbox number is to be used.	Optional	
Messaging Template messagingTemplate	Specifies the messaging template of a subscriber.	Optional	
Password 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 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	Mandator y/Optional	Validation Constraints
Community ID 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 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 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 number values of length 10

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
Time Zone timezone	This is the time zone for Avaya Aura® Messaging time subscribers.	Optional	Time zone in the StandardizedName format. For example, America/Phoenix. The field applies to Avaya Aura® Messaging 6.3 and later only. **Note:** 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.
mmSpecific	This is complex type for Messaging Messaging specific fields data.	Optional	
numericAddress	This is field of Messaging specific data. 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.	Optional	
pbxExtension	This is field of Messaging specific data. The primary telephone extension of the subscriber.	Optional	
telephoneNumber	This is field of Messaging specific data. The telephone number of the subscriber as displayed in address book listings and client applications.	Optional	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 (]).

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
asciiVersionOfName	This is field of Messaging specific data. 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. Specifies whether your password expires or not.	Optional	You can choose one of the following: • yes: for password to expire • no: if you do not want your password to expire
mailBoxLocked	This is field of Messaging specific data. 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: • no: to unlock your mailbox • yes: to lock your mailbox and prevent access to it
personalOperatorMailbox	This is field of Messaging specific data. 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. 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	Mandator y/Optional	Validation Constraints
tuiMessageOrder	This is field of Messaging specific data. Specifies the order in which the subscriber hears the voice messages.	Optional	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.

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
intercomPaging	This is field of Messaging specific data. Specifies the intercom paging settings for a subscriber.	Optional	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.
voiceMailEnabled	This is field of Messaging specific data. 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.	Optional	

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
miscellaneous1	This is field of Messaging specific data. 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. 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. 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. 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	Mandator y/Optional	Validation Constraints
cmmSpecific	This is field of Messaging specific data. Specifies the number of the switch on which this subscriber's extension is administered.	Optional	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.
accountCode	This is field of Communication Manager Messaging data. 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.	Optional	
coveringExtension	This is field of Communication Manager Messaging data. Specifies the number to be used as the default destination for the Transfer Out of Messaging feature.	Optional	You can enter 3 to 10 digits in this field depending on the length of the system's extension, or leave this field blank.

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
miscellaneous1	This is field of Communication Manager Messaging data. Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.	Optional	Max length 11
Miscellaneous2	This is field of Communication Manager Messaging data. Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.	Optional	Max length 11
Miscellaneous2	This is field of Communication Manager Messaging data. Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.	Optional	Max length 11
Miscellaneous4	This is field of Communication Manager Messaging data. Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.	Optional	Max length 11

Attribute details defined in the Session Manager communication profile XSD

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
Primary Session Manager 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 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	Mandator y/Optional	Validation Constraints
Survivability Server survivabilityServer	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. 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. **Note:** 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	Optional	-

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
	Branch Session Manager.		
Max. Simultaneous Devices maxSimultaneousDevices	The maximum number of endpoints that you can register at a time using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.		
Block New Registration When Maximum Registrations Active blockNewRegistrationWhenMaxActive	Set the value to true or false. If you do not set the attribute, by default, the system sets the attribute to false. 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. 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.		

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
Origination Application Sequence originationAppSequence	An Application Sequence that is invoked when calls are routed from this user. **Note:** 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.	Optional	-
Termination Application Sequence terminationAppSequence	An Application Sequence that is invoked when calls are routed to this user. **Note:** 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.	Optional	-

Table continues…

Attribute	Attribute Description	Mandator y/Optional	Validation Constraints
Home Location homeLocation	The home location that you set from **Routing** > **Locations** 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**Routing** > **Dial Patterns** 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 confFactorySet	The conference factory set to enable media capability-based call routing to the Conferencing SIP entities. Use the **Session Manager** > **Application Configuration** > **Conference Factories** 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 template	Specify the name of the User Template. User Templates are created in Avaya Aura Conferencing Provisioning Client. The following default templates always exist: executive, desktop_user_with_video, desktop_user_no_video, desktop_user_low_priority, guest_user_no_video, event_1000, event_2000, event_3000.	Mandatory	-
Location location	Specify location for the user. Location is a mandatory field. However, Conferencing can get the value of location from the **Location** field in Conferencing Profile. Conferencing can also get the value of location from the **Home Location** field in Session Manager Profile if Session Manager profile is configured and the location in Conferencing Profile is not configured.	Mandatory	-
Participant Security Code securityCode	The participant code for the chairperson bridge.	Mandatory if the autoGeneratedCodeLength parameter is not set.	-

Table continues…

Attribute	Attribute Description	Mandatory/Optional	Validation Constraints
Moderator Security Code moderatorPin	The unique participant code that you use to login to a conference as a moderator.	Mandatory if the autoGeneratedCodeLength parameter is not set.	-
Auto Generated Participant and Moderator Security Codes Length 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 eventConfCode	Specify Presenter Security Code. 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.	-

Index

A

abort
  global user settings import job on first error 204
abort a user import job 196
abort global user settings import job on first error 204
accept new service
  for all links 345
accessing log harvest 648
accessing port matrix 741
accessing scheduler 690
accessing the Backup and Restore service 666
accessing the Data Retention Rules service 677
accessing the Log Settings service 642
access log harvesting 648
access permissions
  for System Manager web pages 172
access profile 60
activating
  new Identity Certificate 101
activating agent 719
activating serviceability agent 719
Adaptation Details
  adaptation module parameters 313
adaptation module
  Module Parameter Type 313
Adaptation Module Management 335
adaptations
  bulk import 335
  creating 321
add
  communication profile for user 119
Add Communication Manager field descriptions 52
adding
  Root CA to Session Manager trusted list 100
  System Manager root certificate to phones 74
  third party root certificate to phones 85
  trusted certificates 87, 90
  users 115
adding a CM Endpoint profile 123
adding a contact in contact list 141
adding a CS 1000 or CallPilot profile 130
adding a CS 1000 profile 131
adding a messaging profile 127
adding an IP Office endpoint profile 133
adding an SNMP target profile 725
adding communication profile for user 119
adding communication profiles
  IP Office endpoint 133
adding data center
  Session Manager 439
adding new instance of element 51
adding Root CA
adding Root CA *(continued)*
  to System Manager trusted list 100
adding System Manager CA
  to Communication Manager 73
adding third party CA
  to Communication Manager 84
Add service to user 152
Add Trusted Certificate page 91
administering
  Branch Session Manager 447
  initial setup of the Session Manager 291
  SIP Identity Certificate 101
  SIP Team button 713
  users 112
administration
  Branch SIP trunk 447
  Session Manager communication profile 118
advanced intrusion detection environment 71
advanced searching 568, 581
AIDE commands 71
Alarm List page 631
alarms
  forward from secondary to primary System Manager 629
  standby mode 629
alarms; export 627
alarms; search 628
appender; modify 645
application instance
  create 51
  new 51
application management page 57
applying SIP phone template
  to existing user 710
assigning
  data center 586
  notification filter profile to a serviceability agent 730
assigning an appender to a logger 644
assigning an RBAC role to a user 171
assign permissions in Scheduler 690
association between IP Office endpoint profile and user
  remove 136
Attach Appender page 647
attach contacts page 142
attribute details defined in Delete user XSD 875
attribute details defined in Import User XSD 865
attribute details defined in the CM Endpoint profile XSD 876
attribute details defined in the Conferencing communication profile XSD 919
attribute details defined in the Messaging communication profile XSD 905
attribute details defined in the Session Manager communication profile XSD 914
audit

audit *(continued)*
run on Backup Storage Location ... 591
automatic
call routing ... 125
AutoRefresh Alarm List page ... 630
auto-refresh log list page ... 640
Avaya Aura Device Services ... 437
Avaya SIP AST endpoints ... 149

B

backup ... 665
remote server ... 666
backup and restore ... 665
Backup and Restore page ... 673
backup and restore service; access ... 666
backup data ... 664
backup files; view ... 666
backup file size ... 664
Backup page ... 674
Backup Storage location
run audit ... 591
Branch
SIP trunk administration ... 447
branch session manager instances ... 449, 456
Bulk Communication Profile
edits ... 168
bulk export ... 175, 182
key features ... 182
bulk export of global user settings ... 201
bulk export of users ... 187
bulk export of users partially ... 191
bulk export users ... 186
bulk import ... 175, 182
domains ... 299
for adaptations ... 335
global settings options ... 200
key features ... 182
locations ... 310
sample XMLs ... 206
schema definitions ... 206
time ranges ... 382
Bulk Import
dial patterns ... 401
Regular Expressions ... 408
routing policies ... 391
bulk import and export ... 175, 182
bulk import and export of user by using Excel file ... 177
bulk import and export with Excel ... 175
BulkImportEncryptionUtil ... 192, 193
bulk import encryption utility ... 192
Bulk Import example for Entity Links ... 378
bulk import for SIP Entiies ... 368
bulk import of global user settings ... 200
bulk import of partial user attributes ... 190
bulk import users ... 182
bulk import XML for users with SIP phone ... 223
bundle identity certificate ... 106
bundle private key ... 106

C

Call Counts Report Types ... 607
CallPilot profile
modify ... 133
Call Routing Test ... 601
cancel
global user settings import job ... 205
cancel a global user settings import job ... 205
cancel a user import job ... 197
Cassandra admin user password
changing ... 437
Cassandra clustering
overview ... 435
topology ... 436
Centralized Call History administration ... 434
certificate management ... 71
certificates
revoking ... 78
unrevoking ... 78
viewing ... 76
Certificate signing request generation ... 102
certificate validation
SIP TLS connection ... 94
System Manager ... 94
certificate validation for SIP endpoints
enforcing ... 111
changing
Cassandra admin user password ... 437
changing alarm status ... 627
changing compatibility view setting ... 24
CM Endpoint profile
delete ... 126
CM station data
export ... 175
import ... 175
command
exportUpmGlobalsettings ... 201
command line restore ... 672
communication address
modify ... 121
Communication Manager
add ... 52
trusting system Manager CA ... 73
trusting third party CA ... 84
communication profile
add ... 119
Presence ... 122
Communication profile ... 227
Communication Profile Edit Confirmation page field descriptions ... 465
communication profile for user
delete ... 120
Communication profiles ... 119

communication profiles for a user 122
communication profile worksheets
communication profile hierarchy 179
hierarchy 179
parent-child communication profile 179
relationship 179
worksheets 179
compatibility mode 24
completed jobs 693
view 692
Completed Jobs Page 698
configuration 184, 189
configuration options for bulk import of users 189
configuration options for bulk import through Excel 184
configure permissions
to access System Manager web pages 172
configuring
CRL download 80
configuring trap listener 733
contact
add in default contact list 141
modify 141
contact list member
edit 144
contacts
attach 142
copying permission mapping for a role 173
create
log harvesting profile 649
user provisioning rule 152
create filter profiles 731, 732
create log harvesting profile 649
Create New Profile page 657
creating
domains 297
messaging instance 55
new CRL 79
new SIP phone template 708
notification filter profile 729
RBAC role with full permissions 170
routing policies 384
scheduler operation role 169
SIP Entities 342
SIP Entity 416
SIP phone template from default 709
time ranges 380
creating a new communication address for a profile 120
creating an SNMP target profile 725
creating an SNMPv3 user profile 722
creating data backup on remote server 666
creating duplicate user provisioning rule 154
creating duplicate users 140
creating new instance 51
creating system data backup on a local server 666
creating user provisioning rule 152
creation
new CRL 79
CRL
configuring download 80
configuring download job 80
creating new 79
deleting download job 81
download 80
scheduling download 80
scheduling download job 80
viewing download job 81
CRL download
configuring 80
scheduling 80
CRL download configuration
field descriptions 82
CRL download configuration field descriptions 82
CRL download job
deleting 81
viewing 81
CRL download job details
field descriptions 82
CRL download job details field descriptions 82
CS1000 Adapter 324
CS 1000 and CallPilot profile administration 129
CS1000 Presence users 133
CSR 102, 103
CSR generation checklist 102

D

dashboard
login 25
data backup
create 666
remote server 666
data backup; schedule 667, 668
data backup from local server 670
Database size 664
data center
adding 586
field descriptions 586
data center failure
case 2 42
case 6 44
case 8 46
data center failures 40
data collection 621
data distribution test 594
Data entry warning in Excel 181
Data entry warning in Microsoft Excel 181
Data link error in Excel 181
Data link error in Microsoft Excel 180
data replication 435
Data Retention page 679
data retention rules 678
data retention rules; edit 678
data retention rules; modify 678
data retention rules; view 678

data retention rules service; access 677
Data Server Status
field descriptions 584
data storage clustering 436
default contact
add contact list 141
delete
communication profile 120
global user settings import job on first error 205
user provisioning rule 154
delete a global user settings import Job 205
delete a user import job 198
Delete Confirmation Page 706
Deleted Trusted Certificate Confirmation page 93
deleted user
restore 139
delete filter profiles 731, 732
delete IP Office endpoint profile of a user 135
delete SNMPv3 user profiles 723
deleting
CRL download job 81
deleting a communication address 121
deleting a communication profile 120
deleting an CM Endpoint profile 126
deleting an SNMP target profile 726
deleting an SNMPv3 user profile 723
deleting a profile 651
deleting a station profile 128
deleting completed jobs 693
deleting contacts from the contact list 142
deleting jobs 693
deleting pending jobs 693
deleting scheduled backup job 669
deleting SNMP target profiles 726
deleting user provisioning rule 154
demo certificates 88
installing 88
deny new service
for entity links 340
dial patterns
bulk import 401
Disable Confirmation page 703
disabling
completed jobs 694
IPv6 426
pending jobs 694
document changes 20
domains
bulk import 299
creating 297
download
harvested log files 653
Downloading Excel template 185
downloading harvested log files 653
duplicate
UPR 154
user provisioning rule 154
Duplicate User Provisioning Rule
field descriptions 155

E

edit
scheduled job 701
Edit Appender page 647
edit contact in a contact list 141
edit contact list member page 144
Edit Element page 60
edit filter profiles 731, 732
Editing
completed jobs 669
pending jobs 669, 693
editing an IP Office endpoint profile 135
editing an SNMP target profile 726
editing an SNMPve user profile 722
editing SNMPv3 user profiles 722
edit IPOffice.properties file 136
edit logger 643
Edit Logger page 646
Edit User Profile 249
Edit User Provisioning Rule
field descriptions 155
element
add 51
create 51
new 51
Element Manager
redirect CallPilot user 129
redirect CS 1000 user 129
enabling
IPv6 425
Enabling
completed jobs 695
pending jobs 695
enabling security hardening 70
encrypt passwords 192, 193
endpoint settings
modifying for existing group 711
modifying for existing user 710
End-to-End Secure Call Indication
feature 432
enforcing
certificate validation for SIP endpoints 111
entity links
deny new service 340
Example
bulk import and export of user by using Excel file 177
Excel
bulk import 184
Data entry warning 181
Data link error 180, 181
export 175
import 175
Excel file

Excel file *(continued)*
bulk import and export of user ... 177
import users ... 206
Excel template
download ... 185
existing user
applying SIP phone template ... 710
export
communication profile ... 187
contacts ... 187
global user settings ... 201
user data ... 175, 182
user data to Excel ... 175
export alarms ... 627
export CM Agent profile ... 175
export CM station data ... 175
exporting
Session Manager Certificate ... 93
System Manager CA ... 73
System Manager root CA certificate ... 94
user registrations ... 578
export logs ... 635
exportUpmGlobalsettings command, ... 201
export users ... 186
System Manager web console ... 187
Export Users ... 212
extended security hardening ... 69

F

failback policy
SIP phones ... 433
Failover groups
best practices ... 474
field descriptions
Add Communication Manager ... 52
Add Trusted Certificate page ... 91
CRL download configuration ... 82
CRL download job details ... 82
Duplicate User Provisioning Rule ... 155
Edit User Provisioning Rule ... 155
Export Users ... 212
Filter Profiles ... 731
Import Global Settings page ... 219
manage certificate revocation ... 77
Manage Elements ... 57
New User Profile ... 227
New User Provisioning Rule ... 155
Notification Filter Profiles ... 732
replace identity certificates ... 98
revoke certificate ... 79
schedule CRL download ... 80
security configuration ... 83
Station Access Code Policy ... 522
TrapListener ... 733
User Provisioning Rules ... 155
view certificate detail ... 77
field descriptions *(continued)*
View Trust Certificate ... 89
View User Provisioning Rule ... 155
filtering alarms ... 628
filtering jobs ... 692
filtering log harvesting profiles ... 654
Filtering log harvesting requests ... 655
filtering logs ... 635
filtering SNMPv3 user profiles ... 723
filtering target profiles ... 727
Filter Profiles
field descriptions ... 731
filter users ... 148
finding port matrix ... 741
forwarding syslog messages to remote server ... 644
forward the secondary alarms to primary System Manager ... 629

G

general guidelines and capabilities
user provisioning rules ... 150
generating
CSR ... 103
generating test alarms ... 720
geographic redundancy
system verification tests ... 50
Geographic Redundancy
backup and restore ... 665
failure use cases and recovery ... 39
scenarios ... 28
Setting up a Geographic Redundancy enabled system ... 47
System Manager ... 27
Upgrading to a Geographic Redundancy-enabled system ... 48
global user settings import job
abort ... 204

H

Harvest Archives page ... 659, 662
Harvest Criteria Edit page ... 658
harvested log files; download ... 653
Hierarchy in communication profile worksheets ... 179
host name resolution test ... 594
HTTPS Identity Certificate
extensions and attributes ... 108

I

Identity Certificate
activating new ... 101
replacing ... 97
Identity Certificates ... 96
viewing ... 97

identity certificates attributes
management, postgres, SPIRIT 109
Identity CertificateslLifecycle 107
Identity Certificates page 96
import
user data 175, 182
user data from Excel 175
import CM station data 175
Import Global Settings page 219
import job on the Scheduler page
view 198
import of users 184, 189
import user considerations 194
import users 182
Import Users 206
initial setup of Session Manager 291
InSite Knowledge Base 743
installing
demo certificates 88
third party certificates 86
Internet Explorer
compatibility view setting 24
IP address family 345
IPOffice.properties file
remove association between IP Office endpoint profile and user 136
IP Office endpoint profile 133
delete 135
edit 135
view 134
IPv6
enabling 425

J

Job Details page 210, 218
Job Scheduling -Edit Job page 701
Job Scheduling -On Demand Job page 703
Job Scheduling -View Job page 700

K

key features
bulk export 182
bulk import 182

L

list of XML Schema Definitions and Sample XMLs for bulk import 750
local host name
resolution 475
local storage
NFS storage 623
remote storage 623
locations
locations *(continued)*
bulk import 310
Locations
creating 303
Log; log settings 642
log details; view 634
log file; search for text 652
logger
edit 643
Logging Configuration page 642
Logging page 636
log harvest; access 648
log harvester overview 648
Log Harvester page 656
log harvesting 648
log harvesting profile
create 649
log harvesting profile; view details 650, 656
log harvesting profiles; filter 654
log harvest requests; filter 655
log into System Manager 25
logs; export 635
logs; log viewer 634
logs; search 636
Log Settings 642
Logs Settings service; access 642
Log Viewer 634

M

maintenance tests
secure access link agent 595
manage certificate revocation field descriptions 77
Managed Bandwidth Usage 556
Managed Bandwidth Usage errors 558
Manage Elements
access permissions 172
Manage Elements field descriptions 57
managing
users 112
managing SNMPv3 user profiles 719, 721
managing target profiles 720
managing user profiles 719
map permission 173
messaging data
synchronize 57
messaging elements 55
messaging instance
creating 55
MIB 734
modify
communication address 121
user provisioning rule 153
modify appender 645
modifying
endpoint settings for existing group 711
endpoint settings for existing user 710

modifying a CallPilot profile 133
modifying a CM Endpoint profile 124
modifying a CS 1000 profile 132
modifying a messaging profile 127
modifying an appender 645
modifying an IP Office endpoint profile 135
modifying contact in a contact list 141
modifying data retention rules 678
modifying SNMPv3 user profiles 722
modifying the communication address 121
modifying user account 137
modifying user provisioning rule 153
Multi Device Access 118
multiple SIP endpoints
register 118
Multi Tenancy
Avaya SIP AST endpoints 149

N

network connections test 595
new CRL
creation 79
New Element page 60
new Identity Certificate
activating 101
New log harvesting profile 657
New SIP phone template
creating 708
New User Profile page 227
New User Provisioning Rule
field descriptions 155
NFS partition
NFS partition
permissions 622
performance data storage 622
nodes; remove 681
notification filter profile
assigning to serviceability agent 730
creating 729
unassigning from serviceability agent 731
Notification Filter Profiles
field descriptions 732
notification IDs 732
notifications 748

O

on-demand job 689

P

Pairing Session Manager
with an Avaya Aura Device Services 439
P-Charging-Vector, P-Location 317
PCNs
PCNs *(continued)*
viewing 748
PCN updates 748
peer certificate validation 94
pending jobs
view 692
pending jobs; stop 695
pending jobs; view 691
Pending Jobs page 696
permissions
Scheduler 690
PKCS #12 106
Port 60
port matrix 741
postgres database sanity test 595
pre-administration
for Session Manager profile 113
pre-configuration template
for SIP phones 707
Presence communication profile administration 122
private key 103
product notification enrollment 749
product notifications
e-notifications 749
profile
delete 651
Profile Criteria View page 659
provision
users 149
PSNs
viewing 748
PSN updates 748

Q

quick start to importing users 222

R

RBAC 165
RBAC permissions
Bulk Communication Profile edits 168
RBAC role
creating with full permissions 170
redirect
CallPilot user to Element Manager 129
CS 1000 user to Element Manager 129
redirecting CallPilot user to Element Manager 129
redirecting CS 1000 to Element Manager 129
redundancy link test 594
register
multiple SIP endpoints 118
Regular Expressions
bulk import 408
remote server
forward syslog messages 644
Remote Worker

Remote Worker *(continued)*
core redundancy 483
remove association between IP Office endpoint profile and user 136
remove user account 138
removing
SIP header 318
SIP phone template 712
trusted certificates 76, 93
removing access permissions
for Session Manager and Routing web pages 174
removing an appender from a logger 645
removing an association between a subscriber and a user 128
removing a node 681
removing association between an endpoint and a user 125
removing deleted users from database 139
removing replica node from queue 682
repairing a replica node 680
replace identity certificates
field descriptions 98
replacing
Identity Certificate 97
replica group; remove nodes 681
replica group; removing replica node from queue 682
replica groups; view 679
Replica Groups page 683
Replica Nodes page 683
Replication Node Details page 687
restore backup
remote server 671
restore backup from remote server 671
restore data 664
restore data backup 670
restore deleted user 139
restore on System Manager Geographic Redundancy 665
Restore page 676
restore system backup from local server 670
restoring
default SIP Identity Certificate 110
restoring the backup data through CLI 672
restoring through command line 672
retrieve harvested log file 648
revoke certificate field descriptions 79
revoking certificates 78
role
copy permission mapping 173
Role Based Access Control 165
root certificate
adding to phones 74
routing
of a call using routing policy data 290
Routing Policies
bulk import 391
rules 149

S

sample XML file for a user with SIP Communication Profile 226
sample XML files
for bulk import 177
sample XMLs
for bulk import 206
sample XML with a single user profile 222
schedule
on-demand job 689
schedule a user import job 195
Schedule Backup page 675
schedule CRL download
field descriptions 80
schedule CRL download field descriptions 80
schedule data backup; remote server 668
scheduled backup job
deleting 669
scheduled job
edit 701
scheduled jobs
completed 698
scheduler 689
Scheduler
permissions 690
scheduler; access 690
scheduler operation role
creating 169
scheduler service 689
scheduling
CRL download 80
scheduling a data backup on a local server 667
scheduling a data backup on a remote server 668
scheduling a global user settings import job 202
schema definitions
for bulk import 206
Search Archives page 661
searching contacts on Avaya SIP AST endpoints 149
searching for alarms 628
searching for a text in a log file 652
searching for logs 636
searching logs 636
search users 149
secondary alarms
forward to primary System Manager 629
secondary server alarms
view 629
security configuration
field descriptions 83
security configuration field descriptions 83
security management 71
selected element method 49
serviceability agent
activate 719
Serviceability agents
repair 721

serviceability agents list 721
Service Observing
SIP Phone 716
Session Manager
Geographic Redundancy 32
SIP Entity Monitoring 552
Session Manager Certificate
exporting 93
Session Manager communication profile administration 118
Session Manager Communication profile administration 118
Session Manager configuration sequence 117
session manager instance 425
Session Manager profile
pre-administration 113
Session Manager trusted list
adding Root CA 100
setting
Station Access Code Policy 521
simultaneous element method 48
SIP elements
authentication
of SIP Entities 339
TLS layer validation 339
SIP Entities
creating 342
SIP Entity
creating 416
SIP Entity Details
field descriptions for other SIP Entity types 358
SIP firewall configuration
field descriptions 503
SIP header
removing 318
SIP Header Removal 317
SIP Identity Certificate
administering 101
extensions and attributes table 107
restoring the default 110
SIP phone
pre-configuration template 707
SIP phone template
apply to existing user 710
creating from default 709
removing 712
SIP phone template software requirements 708
SIP Team button
administering 713
SNMP attributes 60
SNMP MIB 734
SNMP target profile
add 725
edit 726
SNMP target profile; view 726
SNMP target profile list 727
SNMP target profiles; delete 726
SNMP target profiles field descriptions 728
SNMP traps 732
SNMPv3 user profile; add 722
SNMPv3 user profile; create 722
SNMPv3 user profile; delete 723
SNMPv3 user profile; edit 722
SNMPv3 user profile; filter 723
SNMPv3 user profile; view 722
SNMPv3 user profiles
assign 719
manage 719
SNMPv3 user profiles field description 724
software requirements
SIP phone template 708
Station Access Code Policy
field descriptions 522
setting 521
Stop Confirmation page 705
stopping pending jobs 695
submitting a request for harvesting log files 651
support 743
Survivable Public Remote SIP Trunking
administration 447
synchronize
CM data 56
configuring options 56
synchronize CM data 56
synchronizing
Communication Manager and System Manager 51
synchronizing messaging data 57
synchronizing System Manager master database and replica
computer database 680
syslog messages
forwarding to remote server 644
system
scheduled job 689
system manager
adding 437
System Manager
adding CA to Communication Manager 73
Geographic Redundancy 27
overview 22
System Manager CA
exporting 73
using 72
System Manager dashboard 25
System Manager login 25
System Manager root CA certificate
exporting 94
System Manager trusted list
adding Root CA 100

T

target profile; manage 720
target profiles
edit 726
target profiles; delete 726
target profiles; filter 727

target profiles field descriptions 728
tenant partitioning
Avaya SIP AST endpoints 149
test alarms from web console
generate 720
third party CA
using 84
third party certificates
installing 86
third party root certificate
adding to phones 85
time ranges 379
bulk import 382
creating 380
TLS Endpoint Certificate Validation 111
TLS version
viewing 88
Tracer Configuration 596
TrapListener 732
field descriptions 733
Trap listener field description 733
TrapListener service 733
Traplistener service; alarming UI 733
TrapListener service; configure 733
trusted certificates
adding 87, 90
removing 76, 93
viewing 89
Trusted Certificates page 96
trust management 71
overview 109
turn off compatibility mode 24

U

unassigning
filter profile from serviceability agent 731
un-assigning
data center 587
unassigning the RBAC role from a user 174
unrevoking certificates 78
UPM 119
UPR
duplicate 154
user
restore 139
user account
remove 138
User Attribute Options 212
user data storage sanity test 596
User Delete Confirmation page 288
user details; view 136
user import job
cancel 197
delete 198
schedule 195
user management 112
User Profile Edit page 249
User Profile View page 271
user provisioning rule 149
add service to user 152
create 152
delete 154
duplicate 154
modify 153
view 153
User Provisioning Rule 227
User Provisioning Rules
field descriptions 155
user registration export, field descriptions 578
users
adding 115
bulk export 187
search 149
users; filter 148
using
System Manager CA 72
third party CA 84
using init -d 88
utility
bulk import encryption 192

V

validation 345
verifying Session Manager configuration sequence 117
Verizon ANI Feature 329
videos 742
view
global user settings import job details 203
import global user settings job 204
secondary server alarms 629
user import job details 199
user provisioning rule 153
view an import global user settings job 204
view an import global user settings job on the Scheduler page 204
view backup files 666
view certificate detail field descriptions 77
view completed jobs 691
view contact list member page 146
view contents; log harvested files 653
view details; log harvesting request 652
view details of a global user settings importing job 203
view details of import job 203
View Element page 60
view filter profiles 731, 732
viewing
certificates 76
CRL download job 81
Identity Certificates 97
PCNs 748
PSNs 748
TLS version 88

viewing *(continued)*
trusted certificates 89
viewing alarms 627
viewing a messaging profile of a user 128
viewing an SNMP target profile 726
viewing an SNMPv3 user profile 722
viewing a station profile of a user 124
viewing certificates 76
viewing data retention rules 678
viewing deleted users
view deleted users 139
viewing details of a log harvesting profile 650, 656
viewing details of a log harvesting request 652
viewing details of a user 136
viewing harvested log files in an archive 650
viewing IP Office endpoint profiles 134
viewing list of backup files 666
viewing log details 634
viewing loggers for a log file 642
viewing pending jobs 691
viewing replica groups 679
viewing replica node details 681
viewing replica nodes in a replica group 680
viewing replication details for a replica node 681
viewing the contents of harvested log files 653
viewing the details of a contact in the contact list 142
viewing user provisioning rule 153
view log details 634
view loggers 642
view log harvested files; archive 650
view logs
completed jobs 692
pending jobs 692
view replica groups 679
view secondary server alarms 629
view the details of a user import job 199
View Trust Certificate page 89
view user import job on the Scheduler page 198
View User Provisioning Rule
field descriptions 155

W

warning
data entry in Excel 181

X

XML file
import users 206
XML for user with core attributes 222
XML Schema definitions 177