Avaya Aura® Release Notes

Release 8.1.x.x

Issue 1.28

April 2021

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, https://support.avaya.com/LICENSEINFO, UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA

AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. 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 Designated Processor that hosts 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 on a number of Designated Processors up to the number indicated in the order. 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.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “**Unit**” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Named User License (NU). You 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. “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). You 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”).

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. Note that 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 G.729 CODEC, 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 G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. 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 15https://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).

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.

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.

Contents

Contents....6

Change history....17

Introduction....20

Documentation Catalog....20

Product Release Matrix....20

What’s new in Avaya Aura®....22

Future use fields visible in Avaya Aura® Release 8.1....22

Information about Meltdown and Spectre Vulnerabilities including Spectre/Meltdown and L1TF....22

Information about VMSA-2019-0020 - Hypervisor-Specific Mitigations for Speculative-Execution Vulnerabilities CVE-2018-12207....22

Security Service Packs....22

Compatibility....22

Contacting support....23

Contact support checklist....23

Contact support tasks....23

Avaya Aura® Communication Manager....24

What’s new in Communication Manager Release 8.1.x.x....24

What’s new in Communication Manager Release 8.1.3.1.0....24

What’s new in Communication Manager Release 8.1.3.0.1....24

What’s new in Communication Manager Release 8.1.3....24

What’s new in Communication Manager Release 8.1.2....25

What’s new in Communication Manager Release 8.1.1....25

What’s new in Communication Manager Release 8.1.0....25

Security Service Pack and Kernel Service Pack SSP08 & KSP08....26

Required artifacts for Communication Manager Release SSP/KSP-08....26

Security Service Pack and Kernel Service Pack SSP06 & KSP06....26

Required artifacts for Communication Manager Release SSP/KSP-06....26

Required artifacts for Avaya Aura® Communication Manager 8.1.x.x....26

Required artifacts for Communication Manager Release 8.1.3.1.0....26

Required artifacts for Communication Manager Release 8.1.3.0.1....27

Required artifacts for Communication Manager Release 8.1.3....27

Required artifacts for Communication Manager Release 8.1.2.1....27

Required artifacts for Communication Manager Release 8.1.2....27

Required artifacts for Communication Manager Release 8.1.1....28

Required artifacts for Communication Manager Release 8.1....28

Required patches for Avaya Aura® Communication Manager Release 8.1....29

Future use fields visible in Avaya Aura® Communication Manager Release 8.1.x.x....29

Future use fields visible in Avaya Aura® Communication Manager Release 8.1.3.1.0....29

Future use fields visible in Avaya Aura® Communication Manager Release 8.1.3....29

Future use fields visible in Avaya Aura® Communication Manager Release 8.1.2 29
Future use fields visible in Avaya Aura® Communication Manager Release 8.1 29
Installation for Avaya Aura® Communication Manager 8.1.x.x 30
Installation for Avaya Aura® Communication Manager Release 8.1.3.1.0 30
Installation for Avaya Aura® Communication Manager Release 8.1.3 30
Installation for Avaya Aura® Communication Manager Release 8.1.2 30
Installation for Avaya Aura® Communication Manager Release 8.1 30
Troubleshooting the installation 30
Enhanced Access Security Gateway (EASG) 31
Speculative Execution Vulnerabilities (includes Meltdown and Spectre and also L1TF Vulnerabilities) 31
Fixes in Communication Manager Release 8.1.x.x 32
Fixes in Communication Manager Release 8.1.3.1.0 32
Fixes in Communication Manager Release 8.1.3.0.1 37
Fixes in Communication Manager Release 8.1.3 38
Fixes in Communication Manager Release 8.1.2 48
Fixes in Communication Manager Release 8.1.1 53
Fixes in Communication Manager Release 8.1.0.2.0 60
Fixes in Communication Manager Release 8.1.0.1.1 61
Fixes in Communication Manager Release 8.1 62
Known issues and workarounds in Communication Manager Release 8.1.x.x 65
Known issues and workarounds in Communication Manager Release 8.1.3.1.0 65
Known issues and workarounds in Communication Manager Release 8.1.3.0.1 65
Known issues and workarounds in Communication Manager Release 8.1.3 65
Known issues and workarounds in Communication Manager Release 8.1.2 65
Known issues and workarounds in Communication Manager Release 8.1.1 65
Known issues and workarounds in Communication Manager Release 8.1 66
Avaya Aura® Session Manager 67
What’s new in Session Manager Release 8.1.x.x 67
What’s new in Session Manager Release 8.1.3.1 67
What’s new in Session Manager Release 8.1.3 67
What’s new in Session Manager Release 8.1.2 67
What’s new in Session Manager Release 8.1.1 67
Future use fields visible in Avaya Aura® Session Manager Release 8.1.x.x 67
Future use fields visible in Avaya Aura® Session Manager Release 8.1 67
Security Service Pack 68
Security Service Pack 68
Required artifacts for Session Manager Release 8.1.x.x 68
Required artifacts for Session Manager Release 8.1.3.1 68
Required artifacts for Session Manager Release 8.1.3 68
Required artifacts for Session Manager Release 8.1.2 68

Required artifacts for Session Manager Release 8.1.1 ... 69

Required artifacts for Session Manager Release 8.1 ... 69

Required patches for Session Manager Release 8.1 ... 69

Installation for Session Manager Release 8.1.x.x ... 70

Backing up the software ... 70

Installing the Session Manager software ... 70

Upgrading the Session Manager software ... 70

Special Case Upgrade Paths ... 70

Troubleshooting the installation ... 71

Restoring software to the previous version ... 71

Fixes in Session Manager Release 8.1.x.x ... 71

Fixes in Session Manager Release 8.1.3.1 ... 71

Fixes in Session Manager Release 8.1.3 ... 74

Fixes in Session Manager Release 8.1.2.1 ... 77

Fixes in Session Manager Release 8.1.2 ... 79

Fixes in Session Manager Release 8.1.1 ... 81

Fixes in Session Manager Release 8.1 ... 83

Known issues and workarounds in Session Manager 8.1.x.x ... 84

Known issues and workarounds in Session Manager Release 8.1.3.1 ... 84

Known issues and workarounds in Session Manager Release 8.1.3 ... 85

Known issues and workarounds in Session Manager Release 8.1.2.1 ... 85

Known issues and workarounds in Session Manager Release 8.1.2 ... 85

Known issues and workarounds in Session Manager Release 8.1.1 ... 86

Known issues and workarounds in Session Manager Release 8.1 ... 86

Avaya Aura® System Manager ... 87

What’s new in System Manager Release 8.1.3.x ... 87

Security Service Pack ... 87

Required artifacts for System Manager Release 8.1.3.x ... 87

Required artifacts for System Manager Release 8.1.3.1 ... 87

Required artifacts for System Manager Release 8.1.3 ... 88

Required artifacts for System Manager Release 8.1.2 ... 88

Required artifacts for System Manager Release 8.1.1 ... 89

Required artifacts for System Manager Release 8.1 ... 90

Required patches for System Manager Release 8.1.x ... 91

Software information: ... 92

How to find a License Activation Code (LAC) in PLDS for a product. ... 92

Installation for System Manager Release 8.1.x ... 93

Upgrading the System Manager software ... 93

System Manager upgrade path ... 93

Troubleshooting the installation ... 94

Speculative Execution Vulnerabilities (includes Meltdown and Spectre and also L1TF Vulnerabilities) 94
Fixes in System Manager 8.1.3.x 94
Fixes in System Manager 8.1.3.1....................94
Fixes in System Manager 8.1.3....................96
Fixes in System Manager 8.1.2....................105
Fixes in System Manager 8.1.1....................110
Fixes in System Manager 8.1....................115
Known issues and workarounds in System Manager in Release 8.1.3.x....................119
Known issues and workarounds in System Manager in Release 8.1.3.1 119
Known issues and workarounds in System Manager in Release 8.1.3 120
Known issues and workarounds in System Manager in Release 8.1.2 121
Known issues and workarounds in System Manager in Release 8.1.1 124
Known issues and workarounds in System Manager in Release 8.1 126
Solution Deployment Manager Adopter Matrix 129
Avaya Aura® Presence Services 134
What’s new in Presence Services Release 8.1.4 134
What’s new in Presence Services Release 8.1.3 134
What’s new in Presence Services Release 8.1.2 134
What’s new in Presence Services Release 8.1.1 134
Required artifacts for Presence Services Release 8.1.4 134
Required artifacts for Presence Services Release 8.1.3 134
Required artifacts for Presence Services Release 8.1.2 135
Required artifacts for Presence Services Release 8.1.1 135
Required artifacts for Presence Services Release 8.1 135
Required patches for Presence Services 8.1 135
Backing up the software....................136
Installing Presence Services Release 8.1.4 136
Installing Presence Services Release 8.1.3 136
Installing Presence Services Release 8.1.2 136
Installing Presence Services Release 8.1.1 136
Troubleshooting the installation 136
Restoring software to the previous version 136
Migrating to the PS 8.1.X release from a PS 6.2.X release 137
Changes Affecting Migrations to 8.1 137
Minimum required versions by Release 137
Upgrade References to Presence Services Release 8.1.4 138
Upgrade References to Presence Services Release 8.1.3 138
Upgrade References to Presence Services Release 8.1.2 138
Upgrade References to Presence Services Release 8.1.1 138
Interoperability and requirements/Applicability for Release 8.1.X 138

Software Development Kit........138
Functionality not supported in Presence Services 8.1.x.x........139
Functionality not supported in Presence Services 8.1.4........139
Functionality not supported in Presence Services 8.1.3........139
Functionality not supported in Presence Services 8.1.2........139
Functionality not supported in Presence Services 8.1.1........139
Fixes in Presence Services Release 8.1.4........139
Fixes in Presence Services Release 8.1.3........140
Fixes in Presence Services Release 8.1.2........140
Fixes in Presence Services Release 8.1.1........141
Fixes in Presence Services Release 8.1........141
Known issues and workarounds in Presence Services Release 8.1.4........141
Known issues and workarounds in Presence Services Release 8.1.3........142
Known issues and workarounds in Presence Services Release 8.1.2........143
Known issues and workarounds in Presence Services Release 8.1.1.0........144
Known issues and workarounds in Presence Services Release 8.1........145
Avaya Aura® Application Enablement Services........148
What’s new in Application Enablement Services 8.1.x.x........148
What’s new in Application Enablement Services Release 8.1.3.1........148
What’s new in Application Enablement Services Release 8.1.3........148
What’s new in Application Enablement Services Release 8.1.2.1 and 8.1.2.1.1........148
What’s new in Application Enablement Services Release 8.1.2........148
What’s new in Application Enablement Services Release 8.1.1........148
Security Service Packs........148
Security Service Packs (Linux Security Update – LSU)........148
Required artifacts for Application Enablement Services Release 8.1.x.x........149
Required artifacts for Application Enablement Services Release 8.1.3.1........149
Required artifacts for Application Enablement Services Release 8.1.3........149
Required artifacts for Application Enablement Services Release 8.1.2.1 and 8.1.2.1.1........149
Required artifacts for Application Enablement Services Release 8.1.2........150
Required artifacts for Application Enablement Services Release 8.1.1.0.2........151
Required artifacts for Application Enablement Services Release 8.1.1.0.1........151
Required artifacts for Application Enablement Services Release 8.1.1........152
Required artifacts for Application Enablement Services Release 8.1.0.0.1........152
Required artifacts for Application Enablement Services Release 8.1........153
Required patches for Application Enablement Services Release 8.1........153
Installation for Avaya Aura® Application Enablement Services Release 8.1.x.x........153
Installation for Avaya Aura® Application Enablement Services Release 8.1.x........153
Backing up the AE Services software........153
Interoperability and requirements........154

Installation for Avaya Aura® Application Enablement Services Release 8.1.x 154
Upgrading to AE Services 8.1.x....154
Upgrading to AE Services 8.1.3.1....154
Upgrading to AE Services 8.1.3....155
Upgrading to AE Services 8.1.2.1 and 8.1.2.1.1....155
Upgrading to AE Services 8.1.2....156
Upgrading to AE Services 8.1.1....156
AE Services Server Upgrade Instructions....156
Restoring AE Services software from the previous version....157
RHEL 7.6 Support for AE Services 8.1....157
Installation for Avaya Aura® Application Enablement Services Software Only 8.1.3.1....157
Installation for Avaya Aura® Application Enablement Services Software Only 8.1.3....158
Installation for Avaya Aura® Application Enablement Services Software Only 8.1.2.1....158
Installation for Avaya Aura® Application Enablement Services Software Only 8.1.2....158
Installation for Avaya Aura® Application Enablement Services Software Only 8.1.x....158
Installation steps for Avaya Aura® Application Enablement Services 8.1.1 and 8.1.2 Aura® OVA Media....158
Installation steps for Avaya Aura® Application Enablement Services 8.1.2 Aura® KVM Support....158
Installation steps for Avaya Aura® Application Enablement Services 8.1.x Aura® KVM Support....159
Functionality not supported....159
Functionality not supported for Release 8.1.3.1....159
Functionality not supported for Release 8.1.3....159
Functionality not supported for Release 8.1.2.1....159
Functionality not supported for Release 8.1.2....159
Functionality not supported for Release 8.1.1....159
Changes and Issues....160
WebLM server compatibility....160
Issues related to Enterprise Directory....160
Issues related to SNMP....160
Interaction between McAfee Antivirus and Executables....160
Speculative Execution Vulnerabilities (includes Meltdown and Spectre and also L1TF Vulnerabilities)....160
VM Foot Print Size and capacity....161
Fixes in Application Enablement Services in Release 8.1.x.x....161
Fixes in Application Enablement Services in Release 8.1.3.1....161
Fixes in Application Enablement Services in Release 8.1.3....163
Fixes in Application Enablement Services in Release 8.1.2.1.1....167
Fixes in Application Enablement Services in Release 8.1.2.1....167
Fixes in Application Enablement Services in Release 8.1.2....168
Fixes in Application Enablement Services in Release 8.1.1.0.2....170
Fixes in Application Enablement Services in Release 8.1.1.0.1....171
Fixes in Application Enablement Services in Release 8.1.1....171

Fixes in Application Enablement Services in Release 8.1.0.0.1 175
Fixes in Application Enablement Services in Release 8.1 176
Known issues and workarounds in Application Enablement Services 8.1.x.x 178
Known issues and workarounds Application Enablement Services in Release 8.1.3.1 178
Known issues and workarounds Application Enablement Services in Release 8.1.3 180
Known issues and workarounds Application Enablement Services in Release 8.1.2.1 and 8.1.2.1.1 184
Known issues and workarounds Application Enablement Services in Release 8.1.2 187
Known issues and workarounds Application Enablement Services in Release 8.1.1.0.2 189
Known issues and workarounds Application Enablement Services in Release 8.1.1.0.1 189
Known issues and workarounds Application Enablement Services in Release 8.1.1 191
Known issues and workarounds Application Enablement Services in Release 8.1.0.0.1 193
Known issues and workarounds Application Enablement Services in Release 8.1 194
Avaya Aura® AVP Utilities 195
What's new in AVP Utilities Release 8.1.3.1 195
What's new in AVP Utilities Release 8.1.3 195
What's new in AVP Utilities Release 8.1.2.1 195
What's new in AVP Utilities Release 8.1.2 195
What's new in AVP Utilities Release 8.1 195
Security Service Packs 195
Installation for Avaya Aura® AVP Utilities Release 8.1.x.x 196
Installation for Avaya Aura® AVP Utilities Release 8.1.3 196
Installation for Avaya Aura® AVP Utilities Release 8.1.2 196
Installation for Avaya Aura® AVP Utilities Release 8.1 196
Required artifacts for AVP Utilities Release 8.1.x.x 196
Required artifacts for AVP Utilities Release 8.1.3 197
Required artifacts for AVP Utilities Release 8.1.2.1 197
Required artifacts for AVP Utilities Release 8.1.2 197
Required artifacts for AVP Utilities Release 8.1.1 198
Required artifacts for AVP Utilities Release 8.1 198
Enhanced Access Security Gateway (EASG) 198
Speculative Execution Vulnerabilities (includes Meltdown and Spectre and L1TF Vulnerabilities) 198
Fixes in AVP Utilities Release 8.1.3.1 199
Fixes in AVP Utilities 8.1 SSP#3 199
Fixes in AVP Utilities Release 8.1.3 200
Fixes in AVP Utilities Release 8.1.2.1 200
Fixes in AVP Utilities Release 8.1.2 202
Fixes in AVP Utilities Release 8.1.1 202
Fixes in AVP Utilities Release 8.0.1.1 203
Known issues and workarounds in AVP Utilities Release 8.1.x.x 204
Known issues and workarounds in AVP Utilities Release 8.1.3 204

Known issues and workarounds in AVP Utilities Release 8.1.2 204
Known issues and workarounds in AVP Utilities Release 8.1.1 205
Known issues and workarounds in AVP Utilities Release 8.1 205
Avaya Aura® Communication Manager Messaging 206
Installation for Avaya Aura® Communication Manager Messaging 7.0.x.x 206
Backing up the software 206
Upgrade Paths (from/to System Platform) 206
File list 206
Installing the release 207
Troubleshooting the installation 207
Hardware compatibility 207
Interoperability and requirements 207
What’s new in Avaya Aura® Communication Manager Messaging Release 7.0.x.x 207
What’s new in Communication Manager Messaging 7.0.0.0 207
Fixes in Communication Manager Messaging Release 7.0.x.x 208
Fixes in Communication Manager Messaging 7.0.0.0 208
Fixes in Communication Manager Messaging 7.0.0.1 208
Known issues and workarounds in Communication Manager Messaging Release 7.0.x.x 210
Known issues and workarounds in Communication Manager Messaging Release 7.0.0.1 210
Avaya Aura® Appliance Virtualization Platform 211
What’s new in Avaya Aura® Appliance Virtualization Platform Release 8.1.3.x 211
What’s new in Avaya Aura® Appliance Virtualization Platform Release 8.1.3.1 211
What’s new in Avaya Aura® Appliance Virtualization Platform Release 8.1.3 211
What’s new in Avaya Aura® Appliance Virtualization Platform Release 8.1.2.1 211
What’s new in Avaya Aura® Appliance Virtualization Platform Release 8.1.2 211
What’s new in Avaya Aura® Appliance Virtualization Platform Release 8.1.1 211
Security Service Packs 211
Required artifacts for Avaya Aura® Appliance Virtualization Platform Release 8.1.3.1 212
Required artifacts for Avaya Aura® Appliance Virtualization Platform Release 8.1.3 212
Required artifacts for Avaya Aura® Appliance Virtualization Platform Release 8.1.2.1 212
Required artifacts for Avaya Aura® Appliance Virtualization Platform Release 8.1.2 213
Required artifacts for Avaya Aura® Appliance Virtualization Platform Release 8.1.1 213
Required artifacts for Avaya Aura® Appliance Virtualization Platform Release 8.1 213
Enhanced Access Security Gateway (EASG) 214
Speculative Execution Vulnerabilities (includes Meltdown and Spectre and also L1TF Vulnerabilities) 214
Installation for Avaya Aura® Appliance Virtualization Platform Release 8.1.x.x 214
Installation for Avaya Aura® Appliance Virtualization Platform Release 8.1.3 214
Installation for Avaya Aura® Appliance Virtualization Platform Release 8.1.2 214
Installation for Avaya Aura® Appliance Virtualization Platform Release 8.1.1 214
Installation of Avaya Aura® Appliance Virtualization Platform Release 8.1 215

Fixes in Avaya Aura® Appliance Virtualization Platform Release 8.1.3.1 ... 219
Fixes in Avaya Aura® Appliance Virtualization Platform 8.1.3 ... 219
Fixes in Avaya Aura® Appliance Virtualization Platform 8.1.2.1 ... 220
Fixes in Avaya Aura® Appliance Virtualization Platform 8.1.2 ... 220
Fixes in Avaya Aura®Appliance Virtualization Platform 8.1.1 ... 221
Fixes in Avaya Aura® Appliance Virtualization Platform 8.1 ... 221
Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform Release 8.1.x.x ... 222
Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform Release 8.1.3 ... 222
Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform Release 8.1.2 ... 222
Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform Release 8.1.2 ... 222
Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform Release 8.1.1 ... 223
Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform Release 8.1 ... 223
Languages supported ... 224
Avaya Aura® G430 and G450 Media Gateways ... 225
What’s new in Avaya Aura® G430 and G450 Media Gateways Release 8.1.x.x ... 225
What’s new in G430 and G450 Media Gateways Release 8.1.3 ... 225
What’s new in G430 and G450 Media Gateways Release 8.1.2 ... 225
What’s new in G430 and G450 Media Gateways Release 8.1.1 ... 225
Installation for Avaya Aura® G430 and G450 Media Gateways Release 8.1.x.x ... 226
Required patches ... 226
Pre-Install Instructions ... 227
File Download Instructions ... 227
Backing up the software ... 228
Installing the release ... 228
Troubleshooting the installation ... 229
Restoring software to the previous version ... 229
Fixes in G430 and G450 Media Gateways Release 8.1.x.x ... 229
Fixes in G430 and G450 Media Gateways Release 8.1.3 (Builds 41.34.01 and 41.34.31) ... 229
Fixes in G430 and G450 Media Gateways Release 8.1.3 (Builds 41.34.00 and 41.34.30) ... 229
Fixes in G430 and G450 Media Gateways Release 8.1.2 (Builds 41.24.00 and 41.24.30) ... 230
Fixes in G430 and G450 Media Gateways Release 8.1.1 (Builds 41.16.00 and 41.16.30) ... 230
Fixes in G430 and G450 Media Gateways Release 8.1.0.1 (Builds 41.10.00 and 41.10.30) ... 231
Fixes in G430 and G450 Media Gateways Release 8.1 (Builds 41.09.00 and 41.09.30) ... 231
Known issues and workarounds in G430 and G450 Media Gateways Release 8.1.x.x ... 231
Known issues and workarounds in G430 and G450 Media Gateways Release 8.1.3, 8.1.2, and 8.1.1 ... 231
Languages supported ... 231
Documentation errata ... 231
Avaya Aura® Media Server ... 232
Avaya WebLM ... 233
What’s new in Avaya WebLM for 8.1.x.x ... 233

What’s new in Avaya WebLM for 8.1.3 233
Security Service Pack 233
What’s new in Avaya WebLM for 8.1.2 233
What’s new in Avaya WebLM for 8.1.1 233
Required artifacts for Avaya WebLM Release 8.1.x.x 233
Required artifacts for Avaya WebLM Release 8.1.3.1 233
Required artifacts for Avaya WebLM Release 8.1.3 233
Required artifacts for Avaya WebLM Release 8.1.2 234
Required artifacts for Avaya WebLM Release 8.1.1 234
Required artifacts for Avaya WebLM Release 8.1 234
Installation for Avaya WebLM Release 8.1.x.x 235
Installation for Avaya WebLM Release 8.1.3 235
Installation for Avaya WebLM Release 8.1.2 235
Installing the release 8.1.1 235
Resource allocation and reservation for standalone WebLM on VMware 235
Software information 236
Troubleshooting the installation 236
Speculative Execution Vulnerabilities (includes Meltdown and Spectre and also L1TF Vulnerabilities) 236
Contacting support 237
Contact support checklist 237
Fixes in Avaya WebLM on VMware for 8.1.x.x 237
Fixes in Avaya WebLM on VMware for 8.1.3.1 237
Fixes in Avaya WebLM on VMware for 8.1.3 238
Fixes in Avaya WebLM on VMware for 8.1.2 238
Fixes in Avaya WebLM on VMware for 8.1.1 238
Fixes in Avaya WebLM on VMware for 8.1 239
Known issues and workarounds in Avaya WebLM for 8.1.x.x 239
Known issues and workarounds in Avaya WebLM for 8.1.3.1 239
Known issues and workarounds in Avaya WebLM for 8.1.3 239
Known issues and workarounds in Avaya WebLM for 8.1.2 239
Known issues and workarounds in Avaya WebLM for 8.1.1 239
Known issues and workarounds in Avaya WebLM for 8.1 239
Avaya Device Adapter Snap-in 240
What’s new in Avaya Device Adapter Snap-in Release 8.1.x.x 240
What’s new in Avaya Device Adapter Snap-in for 8.1.3 240
What’s new in Avaya Device Adapter Snap-in for 8.1.2 240
What’s new in Avaya Device Adapter Snap-in for 8.1 240
Required artifacts for Avaya Device Adapter Release 8.1.3.1 240
Required artifacts for Avaya Device Adapter Release 8.1.3 240
Required artifacts for Avaya Device Adapter Release 8.1.2.1 240

Required artifacts for Avaya Device Adapter Release 8.1.2 240
Required artifacts for Avaya Device Adapter Release 8.1.1 241
Required artifacts for Avaya Device Adapter Release 8.1 241
Installation for Avaya Device Adapter Snap-in for 8.1.x.x 241
Installation for Avaya Device Adapter Snap-in for 8.1.3 241
Installation for Avaya Device Adapter Snap-in for 8.1.2 241
Installation for Avaya Device Adapter Snap-in for 8.1 241
Fixes in Avaya Device Adapter Snap-in for 8.1.3.1 241
Fixes in Avaya Device Adapter Snap-in for 8.1.3 242
Fixes in Avaya Device Adapter Snap-in for 8.1.2.1 243
Fixes in Avaya Device Adapter Snap-in for 8.1.2 244
Fixes in Avaya Device Adapter Snap-in for 8.1.1 245
Fixes in Avaya Device Adapter Snap-in for 8.1 246
Known issues and workarounds for Avaya Device Adapter Snap-in for 8.1.x.x 248
Known issues and workarounds for Avaya Device Adapter Snap-in for 8.1.3.1 248
Known issues and workarounds for Avaya Device Adapter Snap-in for 8.1.3 248
Known issues and workarounds for Avaya Device Adapter Snap-in for 8.1.2.1 249
Known issues and workarounds for Avaya Device Adapter Snap-in for 8.1.2 249
Known issues and workarounds for Avaya Device Adapter Snap-in for 8.1.1 250
Known issues and workarounds for Avaya Device Adapter Snap-in for 8.1 251
Avaya Device Adapter General Limitations 252
Avaya Device Adapter General Limitations for 8.1.3 252
Avaya Device Adapter General Limitations for 8.1.2 252
Contacts handling logic limitation 253
Avaya Device Adapter General Limitations for 8.1.x 253
Device Adapter Limitations 258
Avaya Device Adapter Feature Interaction Limitations for 8.1.3 258
Avaya Device Adapter Feature Interaction Limitations for 8.1.2 258
Avaya Device Adapter Feature Interaction Limitations for 8.1.1 258
Avaya Device Adapter Product Interoperability for 8.1.3 259
Avaya Aura® Device Services 260

Change history

Issue	Date	Description
1	10-June-2019	GA Release of Avaya Aura® Release 8.1
1.1	14-June-2019	Updated information in the following product sections: CM, AES, and ADA. Added PCN details for CM, AVP, AVPU, SM, SMGR, WebLM, AES, and PS.
1.2	24-June-2019	Additional statement added for Session Manager upgrades.
1.3	09-July-2019	Updated information related to Avaya Aura® Release 8.1.0.1.1.
1.4	09-Sept-2019	Updates to Installation and Fixes for G430 and G450 Media Gateways Release 8.1.0.1 Builds 41.10.00 and 41.10.30. Updates for AES 8.1.0.0.1.
1.5	28-Oct-2019	GA Release of Avaya Aura® Release 8.1.1
1.6	19-November-2019	Added Information on AES 8.1.1 SP 1
1.7	20-January-2020	Updated System Manager 8.1.1 Fixed Issues list
1.8	07-February-2020	Updates for AES 8.1.1.0.2
1.9	02-Mar-2020	GA Release of Avaya Aura® Release 8.1.2.
1.10	09-April-2020	Updated the list of Fixes in Avaya WebLM on Vmware for 8.1.2
1.11	13-April-2020	Updated the Fixes list of System Manager and WebLM for 8.1.2
1.12	24-April-2020	Updates to the document references on Avaya Support website.
1.13	15-May-2020	Updated the Presence section to remove the Interop table from 8.1.2 and 8.1.1 sections and added the link for the information. Updated the Presence 8.1.1 and 8.1.2 Latest patch load details.
1.14	08-June-2020	GA Release of Avaya Aura® Release 8.1.2.1.
1.15	13-July-2020	GA Release of Avaya Device Adapter Snap-in Release 8.1.2.1. Updates to the list of Fixes in Session Manager Release 8.1.2.
1.16	28-July-2020	GA Release of Application Enablement Services Release 8.1.2.1.1.
1.17	26-Aug-2020	Added the System Manager upgrade path section. Updated the Download Data Migration Utility section.
1.18	18-Sep-2020	Added the Communication Manager new ISO in the Required artifacts for Communication Manager Release 8.1 section.
1.19	12-Oct-2020	GA Release of Avaya Aura® Release 8.1.3.
1.20	26-Oct-2020	Updated the Avaya Aura® Media Server section for the Media Server 8.0.2 SP5 Release Note reference.
1.21	05-Nov-2020	Updated the Required artifacts for Application Enablement Services Release 8.1.3 section.
1.22	09-Nov-2020	Added the Fixes in G430 and G450 Media Gateways Release 8.1.3 (Builds 41.34.01 and 41.34.31) section.
1.23	14-Dec-2020	GA Release of Avaya Aura® Release 8.1.3 SSP.
1.24	21-Dec-2020	GA Release of Avaya Aura® Communication Manager 8.1.3.0.1 SP.
1.25	08-Feb-2021	GA Release of Avaya Aura® Release 8.1.3.1.
1.26	17-Feb-2021	Updated the Fixes in Avaya Aura® Appliance Virtualization Platform Release 8.1.3.1 section.
1.27	5-Mar-2021	Updated the information about the Avaya Aura® Communication Manager 8.1E OVA.

1.28	12-Apr-2021	GA Release of Presence Services Snap-in Release 8.1.4.

Introduction

This document provides late-breaking information to supplement Avaya Aura® 8.1.x release software and documentation. For updated documentation, product support notices, and service pack information, go to the Avaya Support site at https://support.avaya.com.

Note: The Avaya Aura® System Manager release/version must always be greater than or equal to the release/version of the components of the solution (Session Manager, Communication Manager, Application Enablement Services).

Documentation Catalog

The Documentation Catalog document lists down the various guides that are available for the Avaya Aura® solution. For details see https://downloads.avaya.com/css/P8/documents/101057969

Product Release Matrix

The following table lists the chronological release numbers of Avaya Aura® applications by product.

Legend: NA denotes that no version was released for that cycle, and the last released version is compatible with all Avaya Aura® versions.

Product Name	8.1.3.1	8.1.3	8.1.2.1	8.1.2	8.1.1	8.1
Avaya Aura® Communication Manager	X	X	NA	X	X	X
Avaya Aura® Communication Manager SSP*	X	X	X			
Avaya Aura® Communication Manager KSP*	X	X	X			
Avaya Aura® Session Manager	X	X	X	X	X	X
Avaya Aura® Session Manager SSP*	X	X	X			
Avaya Aura® System Manager	X	X	NA	X	X	X
Avaya Aura® System Manager SSP*	X	X	X	X	X	
Avaya Aura® Presence Services	NA	X	NA	X	X	X
Avaya Aura® Application Enablement Services	X	X	X	X	X	X
*Avaya Aura® Application Enablement Services LSU**	X	X	X			
Avaya Aura® AVP Utilities	X	X	X	X	X	X
Avaya Aura® AVP Utilities SSP*	X	X	X	NA	NA	NA
Avaya Aura® Appliance Virtualization Platform	X	X	X	X	X	X
Avaya Aura® Appliance Virtualization Platform SSP*	X	X	X	NA	NA	NA
Avaya Aura® G430 and G450 Media Gateways	NA	X	NA	X	X	X
Avaya WebLM	X	X	NA	X	X	X
*Avaya WebLM SSP**	NA	NA	X			
Avaya Device Adapter Snap-in	X	X	X	X	X	X
Avaya Aura® Media Server Reléase 8.0.x	X	X	NA	X	X	X
Avaya Aura® Device Services	NA	NA	NA	NA	NA	NA
Avaya Aura® Communication Manager Messaging (supported through 7.0.x)	NA	NA	NA	NA	NA	NA

Note:

- The addition of the KSP/SSP/LSU indicates a new version of that file will be released at or around the same time as the Feature Pack and / or Service Pack.
    - Please read the PSN/PCN for the appropriate KSP/SSP/LSU. The files integrate and are installed uniquely per application.
- Customers can install CMM 7.0.0.1 on a new Appliance Virtualization Platform 8.0 Host. The same applies to upgrades of other Avaya Aura® VMs on a shared Appliance Virtualization Platform host with CMM 7.0.0.1; you can also upgrade to 8.0.
- Customers may use AADS 8.0 with the Aura 8.0 release line up.
- The Avaya Aura® System Manager release/version must always be greater than or equal to the release/version of the components of the solution (Session Manager, Communication Manager, Application Enablement Services).

  Note: Session Manager 8.1.2.1 is compatible with System Manager 8.1.2.0.

What’s new in Avaya Aura®

For more information, see ***What’s New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site.

https://downloads.avaya.com/css/P8/documents/101057859

Future use fields visible in Avaya Aura® Release 8.1

The underlying framework for an upcoming new Avaya Aura® Platform enhancement “Avaya Aura Distributed Architecture” will be seen in some Release 8.1 administration screens and deployment options. This applies to Communication Manager, System Manager, and Session Manager. These fields are for future use only. Reference the Communication Manager, System Manager and Session Manager “What’s New” sections in this document for details on the new fields and deployment options that will be visible in 8.1, but not currently recommended for use.

Information about Meltdown and Spectre Vulnerabilities including Spectre/Meltdown and L1TF

For more information about Speculative Execution Vulnerabilities fixes included in Avaya Aura® Release 8.x, see the following PSNs on the Avaya Support Site:

- PSN020346u - Avaya Aura® Meltdown and Spectre vulnerabilities
- PSN020369u - Avaya Aura® L1TF vulnerabilities

Information about VMSA-2019-0020 - Hypervisor-Specific Mitigations for Speculative-Execution Vulnerabilities CVE-2018-12207

For more information about Speculative Execution Vulnerabilities fixes included in Avaya Aura® Release 8.x, see the following PSNs on the Avaya Support Site:

- PSN020498u - Avaya Aura® Communication Manager performance impact with CVE-2018-12207 mitigation

Security Service Packs

Several of the Avaya Aura® applications are now publishing Security Service Packs (SSP) aligned with their application release cycle. This SSP will include all available, and applicable, updates for Red Hat Security Advisories (RHSA) published prior to the time of the building of the related software release. This SSP will be available for download via PLDS per normal procedures. The details of the SSP are published in a PSN or PCN specific to each product. Please refer to the product specific installation sections of this document for further details regarding SSPs being published for 8.1.x.

Beginning December 2020, SSPs will also be released on a more frequent cadence. This means that SSPs may also be available between application Service Packs/Feature Packs. These SSPs will also be available on PLDS and documented in the appropriate application PCN or PSN. SSP required artifacts and fix IDs will no longer be tracked in the Release Notes. Historical information on SSP artifacts and fix IDs already in the Release Notes will be maintained for reference. Fix ids related to security issues will continue to be listed when included in an application release Feature Pack or Service Pack.

Compatibility

For the latest and most accurate compatibility information, go to https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Contacting support

Contact support checklist

If you are having trouble with an Avaya product, you should:

1. Retry the action. Carefully follow the instructions in written or online documentation.
2. Check the documentation that came with your hardware for maintenance or hardware-related problems.
3. Note the sequence of events that led to the problem and the exact messages displayed. Have the Avaya documentation available.

   If you continue to have a problem, contact Avaya Technical Support:
4. Log in to the Avaya Technical Support Web site https://support.avaya.com.
5. Contact Avaya Technical Support at one of the telephone numbers in the Support Directory listings on the Avaya support Web site.

Avaya Global Services Escalation Management provides the means to escalate urgent service issues. For more information, see the Escalation Contacts listings on the Avaya Support site.

Contact support tasks

You may be asked to email one or more files to Technical Support for analysis of your application and its environment.

Avaya Aura® Communication Manager

What's new in Communication Manager Release 8.1.x.x

What's new in Communication Manager Release 8.1.3.1.0

For more information, see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site: https://downloads.avaya.com/css/P8/documents/101057859

What's new in Communication Manager Release 8.1.3.0.1

For more information, see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site: https://downloads.avaya.com/css/P8/documents/101057859

What's new in Communication Manager Release 8.1.3

For more information, see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site: https://downloads.avaya.com/css/P8/documents/101057859

The following table lists enhancements in this release.

Enhancement	Description
CM-19748	Interaction with Digital X-ported stations and H.323 un-named registration. Introducing the new field "Do not Share Port with Unnamed Registration?" on station form. When H.323 un-named endpoints registers digital x-ported stations will not be shared if the field "Do not Share Port with Unnamed Registration?" on station form with default value set to 'y'.
CM-28192	Displaying hunt-group name on SIP endpoint if the incoming call is via hunt-group and SA9142 is enabled.
CM-28991	Audit triggered every 15 mins and the threshold level is set to 90% default in ecs.conf file Audit verifies the virtual heap memory allocated. If the memory allocated crosses the threshold configured in ecs.conf, then the major alarm is raised
CM-30764	When the race condition of SIP UPDATE and INVITE method in dialog was encountered, the display was not updated correctly. With the new field "Resend Display UPDATE once on Receipt of 481 Response?" on trunk-group is set to 'Y' then, CM will send a SIP UPDATE message for 481 response received from far end.
CM-31872	"SA9143 - Hold/Unhold Notifications for SIP Trunks", Hold/Unhold Notification on trunk-group will be available via SA9143 special-applications only.
CM-31961	Tandem the unknown headers to farend when the call was playing announcement by vector step.
CM-33014	When SA9095 is enabled and the hunt-group algorithm is set to "circ" and there are no members in the hunt group, "Re-hunt on no answer" is configured and no coverage path assigned to hunt, then, the caller should hear a busy tone
CM-33659	This enhancement enabled the SIP attendant with transfer/hold recall feature.
CM-32942	"Allow SIP Agents to Use Multiple Devices" is provided with the specific purpose of allowing Emergency Services agents to have a backup device in cases where the primary device may fail. Specifically, SIP Call Center agents are expected to use a soft client as the primary device for handling emergency calls, and a physical phone as the backup device. Allows a SIP Contact Center (SIPCC) Agent to be logged in on more than one device using the Multiple Device Access (MDA) feature on Session Manager (SM). Any ACD

Enhancement	Description
	call delivered to a skill in which the agent is logged into or a Direct Agent Call will be delivered to all devices on which the agent is logged in. In addition, the ACD call will appear on a bridged call appearance on the physical phone. The agent can answer the call on one device and, if needed, talk to the caller from another device by pression the bridge call appearance.

What's new in Communication Manager Release 8.1.2

For more information see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

As of 8.1.2, customers utilizing AVP or VMware based systems are able to activate disk encryption during OVA installation. To support ongoing maintenance of this feature, the following commands have been added in the 8.1.2 release: ***encryptionStatus, encryptionRemoteKey, encryptionPassphrase,*** and ***encryptionLocalKey***. Note that these commands are only applicable if disk encryption is enabled using the Avaya OVA methods. These commands are not to be used if the customer has provided their own disk encryption using other methods.

The following table lists enhancements in this release.

Enhancement	Description
CM-29434	Programmable time to play a Busy-Tone, Intercept-Tone and Re-Order Tone. Prior to this field Busy-Tone, Intercept-Tone and Re-Oder Tones were default playing 45 seconds for Analog/Digital/H.323 stations.

What's new in Communication Manager Release 8.1.1

For more information see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

The following table lists enhancements in this release.

Enhancement	Description
CM-27781	The Coach on SSC configuration option allows supervisors to coach their agents using the Service Observing Coach functionality even while the call is being recorded by recording applications that use the SSC invisible option to record calls. Prior to this option being available, supervisors could not coach their agents on any call that was being recorded. Agent coaching continues to be blocked on any other conference call.

What's new in Communication Manager Release 8.1.0

The following table lists enhancements in this release.

Enhancement	Description
CM-15641	CM generates a UCID with UTC timestamp and UUI data is preserved for Single Step or Consult Transfer.

Security Service Pack and Kernel Service Pack SSP08 & KSP08

Communication Manager releases Security Service Packs (SSPs) and Kernel Service Packs (KSPs) aligned with the application release cycle. Beginning December 2020, SSPs & KSPs will also be released on a more frequent cadence. Communication Manager SSPs and KSPs These are not intended for use by "software-only" customers

SSP & KSP required artifacts and fix IDs will no longer be tracked in the Release Notes. Historical information on SSP & KSP artifacts and fix IDs already in the Release Notes will be maintained for reference.

For further information on SSP & KSP contents and installation procedures for CM 8.1.x, please see **PCN2095S**.

Required artifacts for Communication Manager Release SSP/KSP-08

The following section provides Communication Manager downloading information. For deployment and upgrade procedure, see product-specific deployment and upgrade documents on the Avaya Support website.

Download ID	Artifact	Notes
CM000001558	PLAT-rhel7.6-0080.tar	Security Service Pack #8
CM000001559	KERNEL-3.10.0-1160.15.2.el7.tar	Kernel Service Pack #8

Security Service Pack and Kernel Service Pack SSP06 & KSP06

Communication Manager releases Security Service Packs (SSPs) and Kernel Service Packs (KSPs) aligned with the application release cycle. Beginning December 2020, SSPs & KSPs will also be released on a more frequent cadence. Communication Manager SSPs and KSPs These are not intended for use by "software-only" customers

SSP & KSP required artifacts and fix IDs will no longer be tracked in the Release Notes. Historical information on SSP & KSP artifacts and fix IDs already in the Release Notes will be maintained for reference.

For further information on SSP & KSP contents and installation procedures for CM 8.1.x, please see **PCN2095S**.

Required artifacts for Communication Manager Release SSP/KSP-06

The following section provides Communication Manager downloading information. For deployment and upgrade procedure, see product-specific deployment and upgrade documents on the Avaya Support website.

Download ID	Artifact	Notes
CM000001548	PLAT-rhel7.6-0060.tar	Security Service Pack #6
CM000001549	KERNEL-3.10.0-1160.6.1.el7.tar	Kernel Service Pack #6

Required artifacts for Avaya Aura® Communication Manager 8.1.x.x

Required artifacts for Communication Manager Release 8.1.3.1.0

The following section provides Communication Manager downloading information. For deployment and upgrade procedure, see product-specific deployment and upgrade documents on the Avaya Support website.

Download ID	Artifact	Notes
CM000001553	01.0.890.0-26766.tar	CM 8.1.3.1.0 Service Pack
CM000001554	PLAT-rhel7.6-0070.tar	Security Service Pack #7

CM000001555	KERNEL-3.10.0-1160.11.1.el7.tar	Kernel Service Pack #7

Required artifacts for Communication Manager Release 8.1.3.0.1

The following section provides Communication Manager downloading information. For deployment and upgrade procedure, see product-specific deployment and upgrade documents on the Avaya Support website.

Download ID	Artifact	Notes
CM000001550	01.0.890.0-26685.tar	CM 8.1.3.0.1 Feature Pack with Hot Fix

Note: With the introduction of CM 8.1.3.0.1 Feature Pack with Hot Fix, the 8.1.3.0.0 Feature pack 01.0.890.0-26568.tar is now obsolete. It is highly recommended that customers on 8.1.3.0.0 apply the 8.1.3.0.1 Feature Pack with Hot Fix (01.0.890.0-26685.tar). This feature pack hot fix follows the same installation/update rules as a Service Pack or Feature Pack and has the same service impacts as application of a Service Pack or Feature Pack.

Required artifacts for Communication Manager Release 8.1.3

The following section provides Communication Manager downloading information. For deployment and upgrade procedure, see product-specific deployment and upgrade documents on the Avaya Support website.

Download ID	Artifact	Notes
~~CM000001545~~	~~01.0.890.0-26568.tar~~	~~CM 8.1.3.0.0 Feature Pack~~ Use 8.1.3.0.1 Feature Pack with Hot Fix
CM000001546	PLAT-rhel7.6-0050.tar	Security Service Pack #5
CM000001547	KERNEL-3.10.0-1127.19.1.el7.tar	Kernel Service Pack #5

Required artifacts for Communication Manager Release 8.1.2.1

The following section provides Communication Manager downloading information. For deployment and upgrade procedure, see product-specific deployment and upgrade documents on the Avaya Support website.

Download ID	Artifact	Notes
CM000001540	PLAT-rhel7.6-0040.tar	Security Service Pack #4
CM000001541	KERNEL-3.10.0-1127.el7.tar	Kernel Service Pack #4

Required artifacts for Communication Manager Release 8.1.2

The following section provides Communication Manager downloading information. For deployment and upgrade procedure, see product-specific deployment and upgrade documents on the Avaya Support website.

Download ID	Artifact	Notes
CM000001529	01.0.890.0-26095.tar	CM 8.1.2.0.0 Feature Pack
~~CM000001530**~~	~~CM-Simplex-08.1.0.0.890-e67-0E.ova~~	~~CM 8.1.0.0.890.0 Simplex vAppliance for Encryption~~
~~CM000001531**~~	~~CM-Duplex-08.1.0.0.890-e67-0E.ova~~	~~CM 8.1.0.0.890.0 Duplex vAppliance for Encryption~~
CM000001538**	CM-Simplex-08.1.0.0.890-e67-2E.ova	CM 8.1.0.0.890.0 Simplex vAppliance for Encryption
CM000001539**	CM-Duplex-08.1.0.0.890-e67-2E.ova	CM 8.1.0.0.890.0 Duplex vAppliance for Encryption
CM000001532	PLAT-rhel7.6-0030.tar	Security Service Pack #3
CM000001533	KERNEL-3.10.0-1062.9.1.el7.tar	Kernel Service Pack #3

Note:** The CM 8.1E OVAs have been updated to address the issue identified in PSN020515u – Deployment of Avaya Aura® Communication Manager (CM) 8.1E OVA via SDM fails on ESXi 7.0. The OVA file name has changed to reflect a new version number and the checksum is updated. Use the new updated 8.1E OVAs going forward. Existing customers on the previous 8.1E OVAs do not need to redeploy the new OVAs.

Required artifacts for Communication Manager Release 8.1.1

The following section provides Communication Manager downloading information. For deployment and upgrade procedure, see product-specific deployment and upgrade documents on the Avaya Support website.

Download ID	Artifact	Notes
CM000001523	PLAT-rhel7.6-0020.tar	Security Service Pack #2
CM000001524	KERNEL-3.10.0-1062.1.2.el7.tar	Kernel Service Pack #2
CM000001526	01.0.890.0-25763.tar	CM 8.1.1 Feature Pack

Required artifacts for Communication Manager Release 8.1

The following section provides Communication Manager downloading information. For deployment and upgrade procedure, see product-specific deployment and upgrade documents on the Avaya Support website.

Download ID	Artifact	Notes
CM000001510	CM-Simplex-08.1.0.0.890-e67-0.ova	CM 8.1.0.0.890.0 Simplex vAppliance
CM000001511	CM-Duplex-08.1.0.0.890-e67-0.ova	CM 8.1.0.0.890.0 Duplex vAppliance
CM000001512	CM-Simplex-08.1.0.0.890-aws-0.ova	CM 8.1.0.0.890.0 Simplex AWS OVA
CM000001513	CM-Duplex-08.1.0.0.890-aws-0.ova	CM 8.1.0.0.890.0 Duplex AWS OVA
CM000001514	CM-Simplex-08.1.0.0.890-kvm-0.ova	CM 8.1.0.0.890.0 Simplex KVM OVA
CM000001515	CM-Duplex-08.1.0.0.890-kvm-0.ova	CM 8.1.0.0.890.0 Duplex KVM OVA
CM000001516	01.0.890.0-25393.tar	CM 8.1.0.1.0 Service Pack
~~CM000001517**~~	~~CM-08.1.0.0.890-e67-0.iso~~	~~CM 8.1.0.0.890.0 ISO Software Only~~
CM000001544**	CM-08.1.0.0.890-e67-1.iso	CM 8.1.0.0.890.0 ISO Software Only
CM000001518	01.0.890.0-25442.tar	CM 8.1.0.1.1 Service Pack
CM000001522	01.0.890.0-25578.tar	CM 8.1.0.2.0 Service Pack

** Communication Manager 8.1 ISO image has been updated on September 18, 2020 to address issues with differences in RHEL repositories that have changed since the CM 8.1 ISO image was originally released in 2019. These repository changes can result in the installer failing to install the CM 8.1 ISO. Reference PCN2095S for additional details.

Required patches for Avaya Aura® Communication Manager Release 8.1

For information about patches and product updates, see the Avaya Technical Support Web site https://support.avaya.com. For more details, see PCN2095S on the Avaya Technical Support site.

Future use fields visible in Avaya Aura® Communication Manager Release 8.1.x.x

Future use fields visible in Avaya Aura® Communication Manager Release 8.1.3.1.0

Future use fields visible in Avaya Aura® Communication Manager Release 8.1.3

Future use fields visible in Avaya Aura® Communication Manager Release 8.1.2

Future use fields visible in Avaya Aura® Communication Manager Release 8.1

The underlying framework for an upcoming new Avaya Aura® Platform enhancement “Avaya Aura Distributed Architecture” will be seen in some Release 8.1 administration screens and deployment options. This is applicable to Communication Manager, System Manager, and Session Manager. These fields are for future use only. Reference the Communication Manager, System Manager and Session Manager “What’s New” sections in this document for details on the new fields and deployment options that will be visible in 8.1, but not active/usable

1. Avaya Aura Communication Manager Release 8.1 OVA will have the following deployment options visible but are for future use.
   i. CM Standard Duplex Array Max Users 300000
   ii. CM High Duplex Array Max Users 300000
   iii. CM Array Max users 300000
2. Avaya Aura Communication Manager Release 8.1 SMI page will have the following options but are for future use
   i. Administration → Licensing → Feature Administration → Current Settings → Display → Optional Features → Clustering

ii. Administration → Server Administration → Server Role → Configure Memory → This Server's Memory Setting → X-Large/Array

iii. Administration → Server Administration → Network Configuration → docker0:

iv. Avaya Aura Communication Manager Release 8.1 SAT terminal will have the following fields and are for future use.

    i. System-parameter customer-option → CM Server Array

    ii. System-parameter customer-option → Number of Nodes

v. change cor n → page-3

    i. Homing Policy for Floating Users

    ii. Preferred CM

vi. change system-parameters homing-policy

vii. change ip-network-region n → page-3

    i. Type (SIM-ESS DUP-ESS LSP array)

viii. display array communication manager

ix. list homed-user

x. change system-parameters array-options

xi. list array homed-user

xii. list array communication-manager

Installation for Avaya Aura® Communication Manager 8.1.x.x

Installation for Avaya Aura® Communication Manager Release 8.1.3.1.0

Installation for Avaya Aura® Communication Manager Release 8.1.3

Installation for Avaya Aura® Communication Manager Release 8.1.2

Installation for Avaya Aura® Communication Manager Release 8.1

For information on the installation of Release 8.1, see **Upgrading Avaya Aura® Communication Manager.**

Communication Manager 8.1 software includes certain third-party components, including Open Source Software. Open Source Software licenses are included in the Avaya Aura® 8.1.

Communication Manager Solution Templates DVD. To view the licenses:

1. Insert the Avaya Aura® 8.1 Communication Manager Solution Templates DVD into the CD/DVD drive of a personal computer.
2. Browse the DVD content to find and open the folder D:\Licenses.
3. Within this folder are subfolders for Branch Gateway, Communication Manager, Installation Wizard, Session Manager, and Utility Services that contain the license text files for each application.
4. Right-click the license text file of interest and select Open With -> WordPad. This information is only accessible on the Communication Manager software DVD and is not installed or viewable on the Communication Manager Server.

Troubleshooting the installation

Support for Communication Manager is available through Avaya Technical Support.

If you encounter trouble with Communication Manager:

1. Retry the action. Follow the instructions in written or online documentation carefully.
2. Check the documentation that came with your hardware for maintenance or hardware-related problems.

3. Note the sequence of events that led to the problem and the exact messages displayed. Have the Avaya documentation available.

4. If you continue to have a problem, contact Avaya Technical Support by:

   a. Logging on to the Avaya Technical Support Web site http://www.avaya.com/support

   b. Calling or faxing Avaya Technical Support at one of the telephone numbers in the Support Directory

      listings on the Avaya support Web site.

You may be asked to email one or more files to Technical Support for analysis of your application and its environment.

Note: If you have difficulty reaching Avaya Technical Support through the above URL or email address, go to http://www.avaya.com for further information.

When you request technical support, provide the following information:

- Configuration settings, including Communication Manager configuration and browser settings.

- Usage scenario, including all steps required to reproduce the issue.

- Screenshots, if the issue occurs in the Administration Application, one-X Portal, or one-X Portal Extensions.

- Copies of all logs related to the issue.

- All other information that you gathered when you attempted to resolve the issue.

Tip: Avaya Global Services Escalation Management provides the means to escalate urgent service issues. For more information, see the Escalation Contacts listings on the Avaya Web site.

For information about patches and product updates, see the Avaya Technical Support Web site https://support.avaya.com.

Enhanced Access Security Gateway (EASG)

EASG provides a secure method for Avaya services personnel to access the Avaya Aura® applications remotely and onsite. Access is under the control of the customer and can be enabled or disabled at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck.

Speculative Execution Vulnerabilities (includes Meltdown and Spectre and also L1TF Vulnerabilities)

In order to help mitigate the Speculative Execution Vulnerabilities, the processor manufacturers and operating system developers provide software patches to their products. These are patches to the processors, hypervisors, and operating systems that the Avaya solutions utilize (they are not patches applied to the Avaya developed components of the solutions).

Once these patches are received by Avaya, they are tested with the applicable Avaya solutions to characterize any impact on the performance of the Avaya solutions. The objective of the testing is to reaffirm product/solution functionality and to observe the performance of the Avaya solutions in conjunction with the patches using typical operating parameters.

Avaya is reliant on our suppliers to validate the effectiveness of their respective Speculative Execution Vulnerability patches.

The customer should be aware that implementing these patches may result in performance degradation and that results may vary to some degree for each deployment. The customer is responsible for implementing the patches, and for the results obtained from such patches.

For more information about Speculative Execution Vulnerabilities fixes included in Avaya Aura® Release 8.x, see the following PSNs on the Avaya Support Site:

- PSN020346u - Avaya Aura® Meltdown and Spectre vulnerabilities
- PSN020369u - Avaya Aura® L1TF vulnerabilities

Fixes in Communication Manager Release 8.1.x.x

Fixes in Communication Manager Release 8.1.3.1.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-17731	H.323, Network Address Translations(NAT)	The H323 station behind the Network Translated Device (NAT) couldn't get dial tone if the user tried to go offhook the first time after registration.	6.3.8.0
CM-24845	Busy Indicator, SA9106, EC500	After placing a call to the principal station which then rings on the EC500 station, and answering the call on the EC500 station, Busy Indicator would be on. Now drop the call and the Busy Indicator is not turned off.	7.0.1.3.0
CM-30895	Contact Center with Proactive Outreach Manager (POM) transferring to a Vector Directory Number (VDN) before the call became stable.	Unstable Proactive Outreach Manager (POM) transfer to agent does not display customer's phone number.	8.0.1.2.0
CM-33514	SIPCC station with agent logged in, agent in AuxWrk state i.e not available	The call diversion information is not displayed correctly when the call lands on an available agent after being queued for a while listening to announcement.	7.1.3.5.0
CM-33653	telecommuter Agent	Sometimes NICE recorder is not able to record Telecommuter agent's calls.	7.1.3.3.0
CM-33804	Non-shuffable endpoints, service links	When 1X agent with service link transfers a call to another agent they hear a loud click.	8.1.1.0.0
CM-34456	Call Center with work-code buttons	Call Center work-code button fails to work in some scenarios while agent was in after-call-work.	8.1.2.0.0
CM-35099	Bridge station, transfer, Voice Mail, calling number	Call to a station that is answered by a bridged station and then transferred to a station that covers to Voice Mail is getting incorrect greeting	7.1.3.5.0
CM-35279	Encryption	Call to Service Link drops when agent holds the call.	8.0.1.1.0
CM-35395	Call routing through a Vector Directory Number (VDN) to Experience Portal, then back to Communication Manager (CM) and delivered to agent	User Information (UUI) information is missing in the Adjunct Switch Application Interface(ASAI) message after the call is transferred from Experience Portal to CM, and SIP trunking refer messages updated	7.1.3.5.0

CM-35547	Call Center with Special Application SA8702 with 'Copy UCID for Station Transfer/Conference" enabled.	SIP agent transferring calls with 'Transfer Now' produced two separate UCIDs despite enabling Special Application SA8702 with 'Copy UCID for Station Transfer/Conference".	8.1.2.0.0
CM-35589	2 SIP Signaling groups with different far-end ip and same far-end-port, near-end-ip, near-end-port.	Message Sequence Tracer(MST) traces on specific SIP signaling groups also trace other SIP traffic.	8.1.2.0.0
CM-35778	Resource Inter Gateway Connectivity, Computer Telephony Interface(CTI)	Announcements gets delayed by 6 seconds for the 3rd party CTI merge calls.	8.1.2.0.0
CM-35810	unlock_time is set to 0	System will report that the login was not locked (even though it is) when the unlock_time is set to 0.	7.1.2.0.0
CM-35848	SIP stations routing over SIP trunks.	SIP stations sometimes cannot receive inbound calls, all SIP trunks are stuck in busy state.	8.1.1.0.0
CM-35877	Calling-party number conversion, tandem calls	CM sat "CALLING PARTY NUMBER CONVERSION FOR TANDEM CALLS" form lost entries when "all" used in "delete" field sometimes.	8.1.1.0.0
CM-35910	Abbreviated-dial personal list, commandhistory log	The commandhistory log entry for "abbreviated-dialing personal" omits 'personal' from the entry.	8.1.2.0.0
CM-35979	Elite with CMS release 18 or higher connected.	Elite with CMS release 18 or higher connected.	7.1.3.0.0
CM-35991	High volume of DSP resources in a network region.	CM SAT 'list measurements ip dsp-resource hourly' command displayed incorrect data that overflows the 'DSP Usage' field when high volume of DSP resources were used for an IP network region.	7.1.3.5.0
CM-36008	Aura Media Server(AMS), Secure Real-Time Transport Protocol (SRTP) enabled codec set and endpoints	No talk path issues seen when using Secure Real-time Transport Protocol (SRTP) with Aura Media Server (AMS)	8.1.1.0.0
CM-36009	CC Elite with special application SA9137 activated for Externally controlled distribution	False agent available messages were being sent to the Afiniti EBP product. This fix only applies to customers with SA9137 and Afinti EBP deployed.	7.1.3.6.0
CM-36030	Adjunct route, vector collect step	Adjunct route failed while processing the vector collect steps.	8.1.2.0.0
CM-36086	CM active agent telecommuter service links	Increase max telecommuter service links from 3500 to 5000, thus allowing higher capacity.	7.1.3.1.0
CM-36126	Domain controlled SIP endpoint, Enhanced Call Forward	No CTI notification was sent for ECF (Enhanced Call Forward) invocation via button by SIP endpoints	7.1.3.4.0

CM-36155	SIP calls	Memory leak in transactionMap due to SIP INFOrmation method processing	8.0.1.2.0
CM-36195	J169 station, call-appr buttons, 6 buttons after autodial button	On J169 or J179 station types and others, autodial buttons can sometimes be corrupt if 6 call-appr buttons are administered after the autodial buttons.	8.0.1.2.0
CM-36199	Call appearance, EC500, IX workplace	Sometimes call appearance hangs after making EC500 call with IX Workplace	7.1.3.5.0
CM-36231	Unregistered SIP hunt-group user, EC500 enabled.	Unregistered SIP hunt-group user did not ring with EC500 enabled	7.1.3.0.0
CM-36235	Enterprise Survivable Server(ESS), recorded announcements on Aura Media Server(AMS)	Customer is not able to listen to Aura Media Server (AMS) announcements	7.1.3.5.0
CM-36280	One X Agents that are not ASAI controlled.	In using One X Agent, Service Link (S/L) is set for as-needed but is acting as if permanent and back to back calls are not ringing the cell phone for each new call, callers are immediately link to the cell on the same S/L.	8.1.2.0.0
CM-36281	Original CM8.1 OVA that does not support disk encryption,	Log entry is expected every 15 minutes on systems running the original cm8.1 OVA that does not support disk encryption. Log entry does not occur on all systems.	8.1.2.0.0
CM-36298	system-parameters features form, release field.	After activating 8.1.2.0.0 feature pack, the "CMS (appl mis)" release field on page 12 of the SAT "system-parameters features" form is missing previously administered release value and is set to blank.	8.1.2.0.0
CM-36358	Make 7 calls to a meet-me conference bridge	Meet-me conference feature allows more than six parties to be in a call and logs multiple proc errors after that.	8.1.2.0.0
CM-36359	Call redirection, Vector Directory Number(VDN), Interactive Voice Response(IVR), transfer.	Counted-call doesn't work if call is redirected to another Vector Directory Number (VDN) via SIP Interactive Voice Response (IVR) transfer	8.0.1.1.0
CM-36403	Incoming H323 trunk call to H323 station, which is being monitored by ASAI, and this call dropped due to NATO time expires.	No ASAI drop event when call dropped due to no answer time out expires.	8.0.1.1.0
CM-36404	Unregistered J169 and J179 phones, per-COline	J169 and J179 phones stay in incorrect internal ring state after release of the call causing incorrect ring for subsequent calls	8.1.0.2.0
CM-36420	SA8887, abbreviated list	Testing the "Hotline for IP telephones" (SA8887) feature and observed that this is working fine as long the DC for abbreviated list is lower or equal to 89.	8.1.2.0.0

CM-36421	Transport Layer Security (TLS), CLAN, large certificates	Transport Layer Security (TLS) handshake fails on CLANs with large certificates	8.1.2.0.0
CM-36474	Avaya Agent for Desktop (AAFD)	User having intermittent Avaya Agent for Desktop (AAFD) login issues.	7.0.1.3.0
CM-36495	Call Center with Externally Controlled Distribution (ECD) through an AES application.	CC Elite occasionally delivered a call to an agent without informing the ECD controller that the agent was available.	7.1.3.1.0
CM-36510	Call Centers without EAS and CMS connected	Call Centers with traditional ACD (not EAS) may encounter reset of the link to CMS after adding or removing an even-digit extension from an ACD hunt group.	7.0.0.0
CM-36574	Call Centers and Oceana customers with SIP agents.	SIP Agents were not moved to AUX after several failed attempts to route multiple Oceana DAC calls to the agent.	8.1.2.0.0
CM-36666	Principal station, call forward, and bridged station is unregistered.	Phones with bridge-appearance keep ringing and customer has to unplug the phone (9608G) to stop the issue	8.1.0.2.0
CM-36676	Extension to Cellular (EC500), Aura Media Server (AMS) and Secure Real-time Transport Protocol (SRTP)	If EC500 answers too soon, and SIP Direct Media is on, Secure Real-time Transport Protocol (SRTP) key from EC500 leg gets sent with AMS's answer and the caller does not hear ringback	7.1.3.4.0
CM-36713	SA9050	Executing command "list ars route-chosen 1xxxxxxxxx (where x is any digit) loc 3 par 3y (0-2)" results in to segmentation fault that can lead to restart of Communication Manager application.	8.1.1.0.0
CM-36726	Repeatedly pickup buttons get "stuck" and have to be cleared by Corruption team.	Occasionally, pickup buttons get "stuck" and have to be cleared by Corruption team.	7.1.3.6.0
CM-36747	Faulty recovery, process trap	Recovery from a process trap is not handled correctly which results in delayed recovery and an unnecessary system restart.	8.0.1.2.0
CM-36749	Call Center with Externally Controlled Distributor and SIP agents.	An Externally Controlled Distributor sometimes received 'resource busy' upon attempt to route a call, only to find that CC Elite later sent a call to the agent.	7.1.3.6.0
CM-36750	All Communication Managers (CMs) that are not configured as cluster or array CMs.	Depending on the configuration of Communication Manager (CM), a warning is displayed for missing files that are not backed up. This is not an error, but the backup reports it as a warning which is concerning to some customers.	8.1.2.0.0

CM-36774	Video call, Session Initiation Protocol (SIP) and H.323 station	Sometimes video calls between sip and H.323 stations result in a segmentation fault	8.0.1.2.0
CM-36849	Media Processor (MEDPRO), Voice over the LAN (VAL) ip-interface form that is enabled.	Cannot change or remove an enabled MEDPRO or VAL type ip-interface.	8.1.3.0.0
CM-36856	SIP agent, Look Ahead Routing (LAR)	SIP agent cannot be put into AUX mode after direct SIP agent call gets multiple 500 error responses if the last preference of LAR (Look Ahead Routing) route pattern had "next" or "rehu" configured.	8.1.2.0.0
CM-36886	Trunk call, Vector Directory Number (VDN), hunt group, Single Step Conferencing (SSC)	Automatic Call Distributor (ACD) auto answering agent is not able to auto answer the call after transfer.	8.1.2.0.0
CM-36994	Aura Media Server (AMS), Music on Hold (MOH) source	Music on Hold (MOH) terminates from Avaya Aura Media Server (AAMS) while listeners are connected.	8.1.2.0.0
CM-37018	Incoming trunk call	Incoming trunk call with leading destination digits similar to AUTO-IN Feature Access Code (FAC) code results in segmentation fault	8.1.1.0.0
CM-37019	Vector with wait step hearing ringback followed by queue-to skill step	Communication Manager (CM) reset as a result of an Intelligent Services Gateway (ISG) crash which is caused by an incoming call over QSIG trunk to a vector with a wait step providing ringback which is then queued to a skill with no available agents.	8.1.2.0.0
CM-37076	A small memory config Main CM with a survivable server registering to it.	A small main system experienced rolling reboot when Local Survivable Processor (LSP) registers to it.	8.1.3.0.0
CM-37139	Session Initiation Protocol (SIP) Direct Media (DM), media encryption	Call dropped when Avaya Agent for Desktop (AAfD) holds and unholds the Secure Real-Time Transport Protocol (SRTP) call on telecommuter	8.1.3.0.0
CM-37160	Call-Fwd Feature Access Code (FAC), Session Initiation Protocol (SIP)	Dialing Call-Fwd Feature Access Code (FAC) from SIP phone (9608) on dialpad results in denial event 1601.	8.1.3.0.0
CM-37254	Communication Manager (CM) 8.1.3, Amazon Web Services (AWS)	Communication Manager (CM) 81.3 running on Amazon Web Services (AWS), interchange sometimes	8.1.3.0.0
CM-37270	Incoming ISDN-PRI trunk call, consultative transfer	Call Detail Recording (CDR) report was not generated for 2nd leg in case of warm/consultative call transfer.	7.1.3.7.0
CM-37558	IX workplace (IXW), call park, call unpark	"Conference 2" appears on the endpoint display when a call parked by IX Workplace is un-parked. This results in no "Transfer" feature on the un-parked endpoint.	8.1.2.0.0

CM-37560	Port Networks (PNs) with a lot of announcements	Potential cross talk when the system has many announcements and agents across Port Networks (PNs) and announcements are configured only on 1 Port Network (PN)	7.1.3.3.0
CM-37623	Large number of trunks	Internal trunk translation corruption	8.1.2.0.0
CM-38256	Vector Directory Number (VDN), VDN of Origin Announcements (VOA), "Answer" button	We can't skip the VDN of Origin Announcements (VOA) by pressing "Answer" button twice on StationLink	8.0.1.1.0

Fixes in Communication Manager Release 8.1.3.0.1

ID	Minimum Conditions	Visible symptoms	Release found in
CM-36597	Group-page containing single SIP user	Group-page with single member would not work	7.1.3.7.0
CM-37076	A small memory config Main CM (1000 users) has a survivable server registering to it.	A small main system will go for a rolling reboot when a LSP registers to it.	8.1.3.0.0
CM-37180	Field 'EC500Delay Deactivation State?' in form 'change off-pbx-telephone configuration-set' is 'y’	When that field is set to “y”, connected IX Clients with versions 3.9(or lower than 3.9) will crash. Attempts to register will fail. **Note:** This will still cause a crash/not able to register in 8.1.3.0.1 when that field is set to “y” – it is simply the default will be changed from “y” to “n” in 8.1.3.0.1.	8.1.3.0.0

Fixes in Communication Manager Release 8.1.3

ID	Minimum Conditions	Visible symptoms	Release found in
CM-9508	QSIG, Communication Manager (CM), Look Ahead Routing (LAR)	History Info was lost in QSIG to SIP interworking calls involving LAR	6.3.12.0
CM-18825	Redirect On No Answer (RONA)/X-port station/SIP trunk	RONA (Redirect On No Answer) call that covered through a x-ported station to a remote coverage path got no History-Info header in the outgoing invite on the SIP trunk. As a result, the call couldn't cover to the right voice mail box	6.3.16.0
CM-24390	SIP, hold	The first call which was held by far-end gets dropped after SM connection was restored	7.1.3.2.0
CM-26003	SIP, Proxy Authentication	SIP call failed with 407 "Proxy Authentication Required" from SM for INVITE from CM	7.1.1.0.0
CM-28731	Any servers 7.1.3.4.0 and later in the 7.1.x load line or 8.1.0.1.1 and later in the 8.1.x load line	In certain conditions, installing a patch could cause the system to issue a crit_os warning while restarting the logging service.	7.1.3.4.0
CM-28929	Enhanced call forward, Application Enablement Service (AES)	Enhanced call forward notification was not sent to AES (Application Enablement Services) /AES clients (in turn)	7.1.3.2.0
CM-29230	Call Center, SIP trunks.	While processing a SIP REFER without Replaces, in some cases CM incorrectly sends a trunk IDLE to CMS, resulting in CMS ignoring a call.	7.1.3.1.0
CM-29382	Tandem calling party number form, modification of existing entries	The tandem calling number form, when they have a particular combination of entries including some with the "any" choice in the CPN Prefix column, could not be changed	7.1.3.3.0
CM-29596	SIP stations, forking	SIP calls drop after 30 seconds if PRACK was received after 200 OK	8.1.0.1.0
CM-29808	Personal Station Access (PSA) and unmerge	CM was in a hung state after PSA unmerge operation was attempted.	8.1.0.1.1
CM-29859	Adjunct/Switch Application Interface (ASAI), Device Media and Call Control (DMCC) recording, Single Step Conferencing (SSC)	ACR failed to record a call because DMCC station was reported busy after a CM system warm start.	8.0.1.1.0
CM-30031	Call Center, SIP Trunks, lookahead-routing (LAR), SIP blind REFER.	Call Center with SIP Trunks using lookahead-routing (LAR) and SIP blind REFER.	7.1.3.3.0

CM-30883	Adjunct/Switch Application Interface (ASAI), Computer Telephony Integration (CTI) link administration, negotiated ASAI link version	Sometimes ACR fails to record a call in spite of recording being enabled	7.1.3.4.0
CM-30919	NetSNMP with trunks.	If snmpwalk is used on avCmStatusTrunkRangeTable, due to an internal memory leak, SNMP traps/alarming were not performing as expected	8.0.1.1.0
CM-31121	SIP Hold/Unhold Notification, Network Call Redirection	Customer may experience call drop issue during transfer of a SIP call	8.1.0.1.1
CM-31124	Customer Root Account enabled during OVA deployment	System reports "Customer Root Account is NOT active (inconsistent state detected)" on first login after OVA deployment	8.1.0.0.0
CM-31334	SIP, transfer, conference	Failed transfer and stuck call record when a conference involving SIP phones, conf target initiates blind transfer and before 180 was received from the transferee, conf host completed conference.	7.1.1.0.0
CM-31371	Call Center, non-optim stations	Call work codes may not operate properly with non-optim sets on-hook	8.1.1.0.0
CM-31376	ip-codec-set - On page 1, media-encryption is set. For FAX, t.38-G711-fallback is set.	T38 Fax fallback to G711 with encryption failed	7.0.1.3.0
CM-31390	SIP Vector Directory number (VDN) call	SIP call could be stuck after the originator dropped the call if the originator of the call to vector SIP agent did not get 18x response before 200OK.	7.1.3.3.0
CM-31392	Communication Manager (CM), Avaya Aura Media Server (AMS)	Calls failed due to exhaustion of AMS licenses	7.1.3.3.0
CM-31460	H.323 station, team button	The call did not go to the main screen when it was answered using the team button for H.323 stations.	8.0.0.0.0
CM-31472	Agent, Consultative transfer	Call dropped by CM when agent did a consultative transfer.	8.0.1.2.0
CM-31476	SIP trunk call, transfer, unstaffed agent, coverage, Single Step Conference	Call dropped when recorded agent transferred the call to an unstaffed agent	8.0.1.1.0
CM-31677	Communication Manager (CM), hunt group traffic	The SAT command "list measurements hunt-group" sometimes displayed incorrect hunt-group number if the "Total Usage" data for that group exceeded 10,000.	7.1.3.3.0
CM-31699	Multi-tenant system, incoming trunk call, Listed Directory Number (LDN), SIP attendant	Incoming trunk call to a LDN (Listed Directory Number), did not route to an attendant, if it was Equinox Based Attendant group	7.1.3.5.0

CM-31840	Multi Device Access (MDA)	Segmentation fault encountered during certain off-PBX call scenarios,	7.1.3.4.0
CM-31853	Outbound call, Communication Manager (CM), Adjunct/Switch Application Interface (ASAI)	When 3rd party application requested a snapshot of the outbound call, CM 8.x did not send trunk as second leg.	8.0.1.2.0
CM-31857	SA9095	Hunt group using SA9095 queuing did not work as expected	8.0.1.2.0
CM-31863	SA9124	In ASAI transferred event, both calling and connected number were similar when SA9124 was enabled	7.1.3.3.0
CM-31864	Communication Manager (CM), Avaya Aura Media Server (AMS)	Calls got stuck in vector queues after interchange	7.1.3.5.0
CM-31877	SIP, call drop	In rare circumstances a SIP call may be dropped.	7.0.1.3.0
CM-31878	Communication Manager (CM), G450 connected	G450 faults not alarmed on CM server	7.1.3.4.0
CM-31902	SIP INVITE, Av-Global-Session-ID header	Customer may experience system reset if incoming SIP call is received with an empty Av-Global-Session-ID header	8.0.1.1.0
CM-31911	Monitor SIP station	End user received receive in-correct state of station in response to ASAI status station query.	7.0.0.0
CM-31930	Call pickup, H.323 station	Call continues ringing on H323 station on answering of call by another station using call pickup button	7.1.3.4.0
CM-32137	SIP, transfer, SIPS Uniform Resource Indicator (URI), Transmission Control Protocol (TCP)	Blind transfer failed when CM sends request uri with sips and the far end response with “503 Service Unavailable”, with mixed use of TLS and TCP across the solution.	7.1.1.0.0
CM-32139	Tandem call, Vector Directory Number (VDN), Adjunct/Switch Application Interface (ASAI)	In ASAI ALERT message, VDN number was seen instead of actual called party number.	7.1.3.4.0
CM-32812	Vector Directory Number (VDN) of origin announcement (VOA), auto-answer, call is transferred from another agent to VDN.	VOA playback aborted and auto-answer fails when call is transferred from another agent to VDN	7.1.3.5.0
CM-32836	9650 set, shared control	Segmentation fault was observed in calls when phone was in shared controlled mode	7.0.1.3.0
CM-32837	Avaya Aura® Media Server (AMS) recording	Callers hear incorrect ringback tone if the caller and AMS were in different locations	8.1.1.0.0
CM-32869	Tandem Calling Party Number form entries on page 16 and 33.	User couldn't administer entries on pages 16 or 33 of the SAT "TANDEM CPN" form.	8.1.0.0.0

CM-32951	Incoming SIP trunk call	One way talkpath if SIP trunk sends initial INVITE with sendonly followed by sendrecv REINV and call is termed to a H.323 station.	6.0.0.0
CM-32956	aut-msg-wt buttons assigned to stations	Sometimes save translation failed to complete and eventually errors out.	8.1.0.2.0
CM-32993	SIP, transfer, hunt group	When a SIP phone attempted to transfer a hunt group call, transfer failed	7.1.3.5.0
CM-32997	Local Survivable Processor (LSP), server ID	Customer could not add a lsp "survivable-processor" using "Server ID" set to 1 from the SAT.	7.1.3.4.0
CM-33015	Drop button, ACR extension, recording	Drop button on phone did not work when ACR extension was added for recording.	7.0.1.3.0
CM-33020	SIP session interval timer	For cancelled SIP-A to SIP-B call, CM sent 422 instead of 487 if SIP-B responded with 422 to the INVITE.	6.2.0.0
CM-33023	3rd Party SIP Endpoint, Communication Manager (CM), Session Manager (SM)	3rd Party SIP end point was crashing on receiving 422 instead of 487 for canceled call	7.1.3.5.0
CM-33039	H323 1xagent	1X Agent on Citrix Server could be stuck and consistently sent KARRQ (keep alive registration request) with obsolete endpointID without stop, that would cause CM (Communication Manager) overload.	7.1.3.0.0
CM-33062	h323 sig group	CM could experience a segmentation fault and a server interchange when an H323 sig group with "RRQ Required" set to "y".	8.0.1.1.0
CM-33065	Adjunct/Switch Application Interface (ASAI), alerting and connected event, bridge-appearance	Alert and connected events were missing when transfer is completed using the bridge-appearance	8.0.1.1.0
CM-33095	SIP transfer	SIP transfer could fail if the refer-to URI has no user portion in the refer header when the SEMT (SIP Endpoint Managed Transfer) was turned on.	8.0.1.2.0
CM-33185	predictive calling/Dialer	When Predictive call was made via AES to CM and customer, Customer was not connecting to Agent	8.1.0.2.0
CM-33205	Server duplication	System may crash after the interchange after an upgrade.	8.1.2.0.0
CM-33210	CAG(coverage answer group), pickup group, call coverage	No ASAI Redirected event was sent when call is answered by pickup feature of coverage answer group call	8.1.1.0.0

CM-33214	Coverage path, Single Step Conference (SSC), out of service stations	Single Step Conference (SSC) can incorrectly fail when coverage path includes stations which are not in-service before an in-service coverage point station answers the call. This can lead to CTI call recording failures after failed routing to coverage points.	7.1.3.5.0
CM-33251	Look Ahead Inter flow between 2 CMs	CTI-Applications was not receiving the delivered/Alert event for a customer call was queued to trunk and vector steps having multiple LAI(Look Ahead Inter flow) failed and connected to final Agent.	7.1.3.2.0
CM-33316	Any system running CM8.1	A listen socket was opened on port 111 for CM and reported as a vulnerability by a security scanner.	8.1.1.0.0
CM-33331	voice mail	When call goes to voice mail, CM (Communication Manager) could experience a segmentation fault.	7.1.3.4.0
CM-33345	H.323 trunks, 2 CMs	call drop during a H245 messaging race condition	7.1.3.2.0
CM-33357	Call Detail Recording (CDR), trunk member information	Incorrect trunk member information was captured in fixed format CDR report.	8.1.0.2.0
CM-33364	EC500	When a call was termed to an EC500 trunk, the media resource region was chosen from the principal instead of the EC500 trunk. As a result of this. wrong media codec was chosen for the call.	7.1.3.0.0
CM-33371	Communication Manager (CM), Avaya Aura Media server (AMS), interchange	There was a segmentation fault observed during CM interchange with active AMS SIP sessions	7.1.0.0.0
CM-33386	Endpoint that was both part of a hunt group and part of a multimedia complex.	CM (Communication Manager) could experience a segmentation fault when a call termed to an endpoint that was both part of a hunt group and part of a multimedia complex.	8.0.1.1.0
CM-33397	Avaya Media Server	Avaya Media Server connected to duplicated CM and when the interchange happens, CM was generating core-dump	8.1.3.0.0
CM-33398	Alternate Network Address Types (ANAT) configuration	MCD on interchange when exactly at same time, 420 with sdp-anat not supported is received for a ANAT INV Offer and CM attempts to resend non-ANAT offer.	8.1.3.0.0
CM-33414	3rd party SIP endpoint	Call is dropped.	7.1.3.4.0
CM-33415	Hunt Group, hunt coverage	Hunt coverage call did not follow to Message Adjunct Hunt group.	7.1.3.5.0

CM-33419	Long hold recall timer, Vector Directory Number (VDN), display	A two-party redirected display (e.g., for bridging or a VDN) reverted to a single-party display if the call was held and then returned due to the hold recall timeout.	8.0.0.0.0
CM-33433	SIP, blind transfer, drop event	Missing drop event for the agent on the held leg of the call for an IVR SIP blind transfer to an incorrect / intercepted number	8.1.1.0.0
CM-33514	SIPCC, agent, AuxWrk state	The call diversion information was not displayed correctly when the call landed on an available agent after being queued for a while listening to announcement.	7.1.3.5.0
CM-33529	EC500	It was required to have an extend button for the EC500 delayed call to be launched successfully.	7.1.3.5.0
CM-33530	OneX Station	Non-OneX stations show one-X Server Status as trigger or normal, causing misbehavior of calls termed to that station.	7.1.3.3.0
CM-33587	Avaya Aura Media Server (AMS), announcement/music	Occasionally an inter Gateway connection can lead to a segmentation fault	7.1.3.3.0
CM-33599	SIP station	When a Non-SIP administered set type was put in the off-pbx station form for OPS SIP station registration, proc error 7171 8936 could be seen in /var/log/ecs log file and the call-appr in the expansion module wouldn't function well on the SIP station.	7.1.3.4.0
CM-33606	Mempool Error	Internal software memory error did not capture the corrupted memory	7.1.3.4.0
CM-33609	SIP trunk, Avaya Aura Media Server (AMS), ringback	Double ring back tone was being heard in SIP outgoing trunk calls when far-end connected ring back tone.	8.0.1.2.0
CM-33734	sip	Double deletion MEMPOOL error for Class Bytes_32 was seen in /var/log/ecs.	7.1.3.4.0
CM-33744	Avaya Aura Media Server (AMS), interchange, Call stuck in the Skill queue with agents available (CIQAA)	After an AMS interchange, CIQAA happened due to corruption of service link	7.1.3.4.0
CM-33749	Message Waiting Indicator (MWI)	If station A has it's 'Message Lamp Ext:' assigned to station B and an upgrade is performed to 8.1.x this resulted in translation corruption causing no MWI updates	8.1.1.0.0
CM-33752	SIP agent	CM (Communication Manager) would drop the queued hunt call if the sip agent returned 500 error response.	7.1.3.2.0

CM-33766	Place a call to Vector Directory Number (VDN)/Vector with adjunct route step and any of the following BITs set: + FLEXBILL_BIT + VDN_OVERRIDE_ADJRTE_BIT + DONT_QUERY_IAP_ADJRTE_BIT For instance, if VDN override is enabled on the VDN, this will cause the problem.	Calling Number is set to '*****' in Adjunct Route Request.	8.1.2.0.0
CM-33777	Simple Network Management Protocol (SNMP), Federal Information Processing Standards (FIPS)	Cannot remove V3 SNMP users from polling, incoming traps and traps when FIPS enabled.	7.1.3.5.0
CM-33817	Native H.323 phone	CM (Communication Manager) could experience a system restart when the native h.323 station's MWL (message waiting lamp) button was audited through maintenance.	8.0.1.1.0
CM-33833	EC500, Feature Access Code (FAC), transfer	FAC for transfer from EC500 failed for transfer complete	7.1.3.6.0
CM-33850	one-x server	One-X server call back call could be dropped occasionally.	8.0.1.2.0
CM-33852	SIP Direct Media off	For initial INVITE with hold audio SDP, CM sent 200 with audio port 0 in 200 OK, causing call drop	7.1.3.5.0
CM-33853	Circular hunt group	The first call to a circular hunt group will fail after the system starts up.	7.1.3.2.0
CM-33873	dual reg	For a DUAL registration configured extension, if the administered set type was H323 station type and the h323 station was registered and SIP station not registered, a call to this extension would follow the Coverage Path Point "Logged off/PSA/TTI" rule for coverage.	7.1.3.6.0
CM-33927	SIP, SRTP	Unattended transfer fails for SIP calls with encryption	7.1.3.3.0
CM-33940	Duplicate a DS1FD station type.	The SAT "duplicate station" command hangs and causes system reset when duplicating a DS1FD set type.	7.1.3.0.0
CM-33941	Personal CO Line (PCOL), incoming call, transfer	Incoming call to a PCOL group that is transferred to a station that covers to VM got a generic greeting.	8.1.1.0.0
CM-33943	SIP call	SIP station call failed with 400 Bad Request since CM (Communication Manager) put invalid (0xff) in the "From" header of the outgoing Invite message to the SIP station intermittently.	8.1.0.1.1

CM-33949	Clustered Signaling-group.	Question marks displayed in "Primary SM" and "Secondary SM" fields on SAT ROUTE PATTERN form when SIP Signaling-Group "Clustered" field is enabled.	8.0.1.2.0
CM-34056	Cisco security manager (CSM), Communication Manager (CM), Application Enablement Services (AES), Interactive Voice Response (IVR), DS1FD	Cisco's CSM restarted when the call scenario to CM involved multiple transfers and conferences.	7.1.3.0.0
CM-34079	EC500, Automatic Call Distributor (ACD), hunt group	IP station port was corrupted after failed EC500 call on ACD hunt group agent. IP phone becomes unusable and the agent stops getting calls. It requires a CM reboot to fix this.	7.1.3.2.0
CM-34104	AEP call to station, that is transferred (via REFER) to an outgoing trunk	Incoming AEP call to station that is transferred (via REFER) to an outgoing trunk results in the caller getting the generic greeting when the call covers to VM.	7.1.3.5.0
CM-34105	System Manager	International characters can be truncated when using System Manager Native Names feature..	8.1.2.0.0
CM-34131	bridge-appearance, transfer	When transfer to a VDN is attempted from bridge appearance then EVNT_ALERT was not sent when agent logged in	7.1.3.7.0
CM-34135	Avaya Aura Media Server (AMS), announcement	Delay in playing an announcement from AMS	8.1.2.0.0
CM-34144	SA9114, Computer Telephony Integration (CTI) app, monitoring	CTI-application was not receiving the country code for an out dialed call with SA9114 enabled	7.0.0.1.0
CM-34177	iOS app, SIP direct media, EC500	When iOS app which is in background, answers incoming call using INVITE replaces, sometimes it resulted in no audio	8.0.0.1.2
CM-34205	SIPCC agent, Busy/ Release	Busy/Release a SIPCC phone could potentially drop a SIP trunk call owned by other SIP station	7.1.3.5.0
CM-34236	pick up group	CM (Communication Manager) could experience a segmentation fault after a warm restart due to an internal pick up group audit.	7.1.3.0.0
CM-34237	H323 station	CM (Communication Manager) could experience a server interchange due to message buffer exhaustion caused by the H323 IP station's TCP socket congestion	8.1.2.0.0
CM-34296	SIP, multiple inter CM calls	Sometimes CM denied conference involving two SIP stations and a SIP trunk.	8.1.3.0.0

CM-34406	H.323 endpoint, TTI	"disable ip-reg-tti old xxxx" did not work for H323 physical/hard phone	8.1.2.0.0
CM-34425	Station Service State query	Response to "Station status query" had service state as unknown	7.1.3.5.0
CM-34436	Voicemail, inter PBX call, X port	Call routing did not cover to voicemail when call originated on different PBX	7.1.3.2.0
CM-34437	Avaya Aura Messaging (AAM), Simple Network Management Protocol (SNMP).	The snmpinctrapconfig command fails in Voice Messaging Stand Alone mode.	7.1.3.3.0
CM-34440	J179 SIP station, pickup, hunt group	J179 SIP popup did not work when call routed through hunt group to pickup group.	7.1.3.2.0
CM-34467	Music On Hold (MOH), SIP direct media, incoming trunk call	ISG unhold event was not received when incoming trunk call to hunt and hold/resume from agent	8.1.2.0.0
CM-34504	8.1.2.0.0 service pack installed on CM 8.1	The CM SMI Web help pages were seen as blank pages	8.1.2.0.0
CM-34505	Contact Center, Circular hunt group	Sometimes circular hunt group calls resulted in an internal software loop leading to reset of CM.	7.1.3.6.0
CM-34522	Communication Manager (CM), station service state, SIP reach-ability	When a device force re-registers and if NOTIFY with terminated state comes later, CM sets the registered state as unregistered	8.1.1.0.0
CM-34523	H323 phone	An H323 phone's TCP socket could be stuck after a Duplicate CM (Communication Manager) server interchange.	7.1.3.4.0
CM-34646	SIP, H.323 trunks	Sometimes SIP/H.323 calls resulted in CM interchange	7.1.3.2.0
CM-34653	sip agent	The call was returned to the skill after AAFD (Avaya Agent For Desktop) responded 380 with "Line Appearance In Use" to the incoming Invite. The direct agent call that got 380 response with "Line Appearance In use" should be redirected to the agent's coverage path or "Redirect on IP/OPTIM Failure" VDN if agent coverage path is not configured.	7.1.3.3.0
CM-34676	R2MFC, call coverage	Call from a R2MFC trunk on a Port Network to a station which then cover-all to another R2MFC trunk did not have a Talk Path after answer.	8.1.1.0.0
CM-34697	Announcement, recording	When customer tried to change the source location for announcement, object already in use was displayed and when trying to rerecord the announcement, denial event 1052 was generated	7.1.3.6.0

CM-34732	SIP header "User-Agent" containing empty	When CM receiving SIP header "User-Agent" with Empty then CM was generating core dump	8.1.2.0.0
CM-34737	h323 phone	If H323 bridge phone was configured in telecommuter mode and with NICE recorder attached, when bridge button was pressed to answer the incoming call to principal, the call couldn't be answered.	8.1.2.0.0
CM-34993	2 Vector Directory Numbers (VDNs), Coverage Answer Group (CAG), CAG member Monitored by Computer Telephony Integration (CTI)	ASAI alert even contains the VDN number in CALLED PARTY information instead of hunt group extension.	8.1.2.0.0
CM-35017	Multiple Avaya Aura Media Servers, announcement on only one AMS	Announcement heard from AMS after a delayed time.	8.1.2.0.0
CM-35035	Vector Directory Number (VDN), Vector, Redirection On No Answer (RONA), Off-net number	A RONA call that routes to the RONA VDN that does a route-to an external number fails to go out the trunks assigned to route-pattern. CM returns denial event 1311 and the caller is connected to intercept tone.	7.1.3.4.0
CM-35040	Call Center, SIP agents, Blind Transfer, Call Management System (CMS)	Call Centers with SIP agents on stations that perform blind REFER may notice some calls transferred by those agents are not correctly tracked on CMS. The original SIP agent stations did not support a blind (plain) REFER.	7.1.3.2.0
CM-35055	Capability Negotiation (Capneg)	CM didn't send 200 OK to in dialog OPTIONS when the negotiated SDP is encrypted causing call failures	8.1.2.0.0
CM-35075	Multiple ISDN trunks with Path replacement enabled	When the path replacement triggered CM was not sending the disconnect event to CTI-Application	7.1.3.5.0
CM-35100	SIP station, coverage	Principal SIP station gave audible ring even when call was ringing on the coverage point.	6.3.118.0
CM-35129	One X Agent, service link	In using One X Agent, Service Link (S/L) is set for as-needed but was acting as if permanent, and back to back calls were not ringing cell phone for each new call, and callers were immediately linked to the cell on the same S/L.	7.1.3.3.0
CM-35166	Avaya Aura® Experience Portal (AAEP), blind transfer	Intermittently, blind transfer from AAEP to agent caused no talkpath	8.1.0.1.1
CM-35275	Computer Telephony Integration (CTI), recording	One of the call was not recorded when an internal software data structure array boundary condition was met	8.0.1.2.0

CM-35366	Communication Manager (CM) interchange, warm restart, H.323 stations/trunks	Sometimes H.323 calls resulted in CM interchange	7.1.3.4.0
CM-35431	Adjunct/Switch Application Interface (ASAI), bridge appearance	Drop/disconnect event was not received when bridge-appearance dropped	7.1.3.6.0
CM-35557	SIP station, Logged off/PSA/TTI, coverage path	Logged off SIP station with Logged off/PSA/TTI? was disabled for coverage path, and caller received ring back instead of busy tone.	7.1.3.6.0
CM-35621	Announcement, re-recording	When trying to rerecord the announcement, denial event 1052 was generated	7.1.3.6.0
CM-35687	Primary Rate Interface (PRI) trunks	Sometimes CM reported a segmentation fault when processing calls over PRI trunks	7.1.3.6.0
CM-35688	Automated Call Distribution (ACD), hunt group	A call made to an ACD (automated call distribution) hunt group consistently requeued to the Hunt group and that drove CM (Communication Manager) towards CPU overload	7.1.3.6.0

Fixes in Communication Manager Release 8.1.2

ID	Minimum Conditions	Visible symptoms	Release found in
CM-15861	AAM 7.0	Restore backup from Server (Maintenance)>Data Backup/Restore screen did not result in a prompt to stop messaging before restore, causing restore to fail	7.0.1.2.0
CM-16543	server config, SMI, footprint	AES licensing for MEDIUM ADVANCED TSAPI was not functioning correctly	7.0.1.1.0
CM-21971	In dialog OPTIONS request	Incorrect media attributes in 200 OK to OPTIONS leading to no talkpath	7.1.2.0.0
CM-22946	Communication Manager with small memory config, trunk call to vector with collect step	Segmentation fault observed when an incoming call was routed to a VDN with collect steps in the vector.	7.0.1.3.0
CM-24018	SIP trunk, vectors, announcement	Some incoming SIP trunk calls routed over vectors were dropped due to error response to SIP request	7.1.3.0.0
CM-25454	AMS, SIP endpoint, Announcement	User was not able to stop announcement recording if announcement length was 10 secs or more	7.1.3.1.0
CM-27395	SIP station	When the field "Criteria for Logged Off/PSA/TTI Stations?" was off, the 302 redirected call to the logged off SIP station will not go to the coverage path even if the "Coverage After Forwarding?" was turned on. "chained call-forwarding" had to be	7.1.3.1.0

ID	Minimum Conditions	Visible symptoms	Release found in
		turned on to make the call to cover to the coverage point.	
CM-28203	SIP traffic	Communication Manager could experience a segmentation fault during SIP traffic.	8.0.1.1.0
CM-28278	Coverage of Calls Redirected Off Net (CCRON), SIP Direct Media, call forward	Call forward off net failed in certain scenarios, if CCRON was enabled	6.3.0.0
CM-28431	Equinox SIP endpoint	Equinox transferred call could fail if the transfer target phone had LNCC (limited number of concurrent calls) feature was turned on.	7.1.3.3.0
CM-28794	Non-privileged administrator	When a non-privileged admin user logs in, they are prompted for their password a second time, then receive and error indicating that they are not allowed to run the 'customer_root_account' command.	7.1.3.3.0
CM-28987	CC Elite SIPCC 9611G agents using Service Observing.	When activating service observing on a SIPCC phone, the COR of the station is checked, not the COR of the agent.	7.1.3.1.0
CM-28992	one-x H.323 agent	If the user switched PC (Personal Computer) login account where one-x agent was running and registered the one-x agent to the same CM (Communication Manager) from the new account, CM treated it as recovery phone, CM would only have one instance of the registration record, but PC has two instances of one-x agent running. That could cause unexpected flooding KARRQ msg from the obsolete registration object on PC which drove CM overload.	8.0.1.1.0
CM-29300	Single step conference	SIP station couldn't finish the transfer if the SSC (single step conference) was involved in the transferred call.	8.0.0.1.1
CM-29319	SIDs exhausted	CM undergoes a warm restart when an internal data structure was exhausted	7.1.2.0.0
CM-29340	SEMT	SEMT (SIP Endpoint Managed Transfer) could fail if the transferred SIP station had preferred handle configured differently from the CM (Communication Manager) administered extension.	7.1.3.4.0
CM-29760	Bulk registration, IP phones, PSA un-merge	Sometimes PSA un-merge could lead to a warm reset	8.1.0.1.1
CM-29952	Multiple duplicated CMs sharing a common AAMS	Music on hold may be prematurely terminated	7.1.3.4.0
CM-29984	An unprivileged administrator using SMI	Unprivileged users were asked to change the password every time they logged in to the SMI	7.1.3.4.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-29993	Avaya Aura Conferencing	The SIP call to AAC (Avaya Aura Conference) could be dropped if the AAC long duration audit feature was used.	8.0.1.1.0
CM-30024	Agent, call coverage, un-registered state	A direct agent call to a logged-off agent with coverage path administered didn't get cover. Instead the caller heard busy tone.	8.0.1.1.0
CM-30027	AAMS, multiple agents, multiple recorders	Bad voice quality on a multi-party conference call with recorders.	8.0.1.1.0
CM-30028	AMS media server, IP trunk, H323 station	Noise on call	7.1.3.1.0
CM-30030	EC500, DTMF	When blind transfer was done from SIP station, no XFER event was sent to CMS for measured trunks if Fast connect on orig was set to true.	8.0.1.1.0
CM-30047	SIP Station, TSAPI, SM cluster	CM ecs logs were getting filled up with proc errors	8.0.1.1.0
CM-30055	1. EC500 call over SIP/H.323/PRI trunk. 2. CDR configured	Call Detail Recording was not being generated for EC500 leg after the call was dropped.	8.0.1.0.0
CM-30069	Bridge appearance, analog/ X-ported endpoints	XMOBILE/IP DECT user cannot transfer on bridged appearance	8.1.0.1.1
CM-30085	CDR, call transfer	CDR report is not getting generated for 2nd leg in case of call transfer	7.1.3.4.0
CM-30100	More than 1024 files for backup	Backup failed if security set files exceeded count of 1024	7.1.3.2.0
CM-30216	SIP station, call forward	On a SIP station, already set Call-Forward button does not get updated when new call forward is set using FAC	7.1.3.4.0
CM-30228	CM and AAM	CM was not sending correct number to AAM after "clear amw all" command	8.0.1.1.0
CM-30231	Full backup restore from 6.x/ 7.x to 8.x	License service failed to start	8.1.0.0.0
CM-30234	ISDN or H.323 trunks, SIP trunk, TCPN (tandem calling party number) form entry	An external international ISDN calling number was not sent with a leading + digit if the call routed over a SIP trunk	8.1.0.1.1
CM-30237	Upgrade translations to 8.1 that have user-profile 21 and try to log into sat.	Could not log into the SAT using user-profile 21	8.1.0.1.1
CM-30263	Auto-icom button	Pressing the Auto-ICOM button on a phone gives a busy tone	7.0.1.3.0
CM-30265	SW-only and manual configuration of umask to 077	A manual configuration of the umask to 077 caused patching and file-sync to fail.	8.1.0.1.1
CM-30352	Station with active 'ringer-off' button. Try removing from SAT	A station with a lit 'ringer-off' button could not be removed by an administrator using the 'remove station' command. Error "Object in use, try again later' would be displayed.	8.0.1.1.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-30353	Call Center, Vectoring, Music, Tenant Partitioning.	wrong announcement was played on vector step "wait hearing music" when Vector Directory Number (VDN)call was redirected another VDN.	8.1.0.1.1
CM-30369	SIP transfer from Experience Portal with Interactive Voice Response.	When Experience Portal IVR (Interactive Voice Response) tried to transfer a call to an extension using '#' + digits, it could fail if the SEMT (SIP Endpoint Managed Transfer) was turned on.	7.1.3.4.0
CM-30398	Survivable server, foot print	LSP in license error mode	8.1.0.2.0
CM-30403	SA8475 enabled	CM interchange if SA8475 was enabled and calls were passive monitored	8.1.1.0.0
CM-30428	SIP, 480 response with corrupt warning header	CM may experience reset	8.1.0.2.0
CM-30430	Multiple CM connected by SIP trunks Prefer G711 MOH enabled Hold/Unhold Notifications enabled	No Music on HOLD and 1 way talkpath	7.1.3.4.0
CM-30462	BRI board TN2185, Port network	BRI trunks and stations were OOS	8.1.0.1.1
CM-30478	SIP call with no tag in the From header	Communication Manager (CM) could experience a server interchange due to a memory issue caused by an invite SIP message that had no tag in the from header.	8.0.1.1.0
CM-30580	ASAI, monitoring, VDN	Incorrect VDN information in ASAI messages and CDR for incoming calls to an agent	8.0.1.2.0
CM-30581	Best service routing.	Best Service Routing over QSIG did not work properly after upgrade.	8.1.1.0.0
CM-30643	SIP trunk with LAR	Equinox conference call would fail if the LAR (Look Ahead Routing) was configured	7.0.1.0.0
CM-30652	SIP INVITE, From URI having port number	Incoming SIP call was dropped by the far end if CM did not respond with port number in 180 Ringing and incoming SIP INVITE had the port number in From URI	7.1.3.2.0
CM-30653	Automatic wakeup, check out	Automatic wakeup was still active after room was checked out.	7.1.3.1.0
CM-30775	ASAI client, SIP station, blind transfer	Blind transfer failed if transfer was completed even before target party started ringing	7.1.0.0.0
CM-30812	SIP trunks using the "Auto Assign" option. change trunk-group" form	In some rare cases can see following error message when reducing the number of members in a SIP trunk with more than 255 members using the "change trunk-group" form.. Error encountered, can't complete request; check errors before retrying	8.0.1.2.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-30857	ARS, ASAI	"Simultaneous Active Adjunct Controlled Calls" counter appeared to be increasing slowly	8.1.1.0.0
CM-30920	Call center, Media resources, Afiniti	Calls queued while agents were available	6.3.119.0
CM-30936	SIP endpoint	The SIP endpoint's transfer button would no longer work if the SIP end point cancelled the 1st transfer attempt in the case that the field "Restrict Second Call Consult?" on the COR form was set.	8.0.1.2.0
CM-30938	CM with media-gateways.	The SAT "display capacity" form page 6 "Media Gateway vVAL Sources" field displays incorrect data.	8.1.1.0.0
CM-30983	Audix step recording	Audix-rec delayed recording by 2 seconds.	8.0.1.0.0
CM-30984	Several Media Servers with "Dedicated Voip Channel Licenses" set to 9999.	SAT user cannot submit the media-server form. User sees Exceed error for licensed resources that aren't visible.	8.1.0.0.0
CM-31016	CM, ASAI monitored station	Under some conditions involving ASAI messaging, CM did a restart	7.0.0.0
CM-31125	MGs, NRs, IP trunk, ISDN trunk, inter gateway connections	One way talkpath was observed in IP trunk to ISDN trunk interworking scenario specific to internal network region connectivity values	8.1.0.2.0
CM-31131	AMS	AMS does not work after upgrade from CM7.0.	8.1.0.2.0
CM-31134	TCP sig group, SRTP attributes in unhold INVITE	Unhold failed if unhold INVITE contained crypto attributes and insecure transport	7.1.3.2.0
CM-31135	AAR, ARS, locations	CM uses per-location ARS or AAR entry to route a call to a voice mail system, even though the all-location ARS or AAR entry was a better match	7.1.3.3.0
CM-31303	AMS	In rare circumstances the user hears no ringback on call and CPU occupancy spikes	7.1.2.0.0
CM-31326	Agents with messages.	Message Waiting Indicator audit does not audit ACD logical-agent extensions and MWI lights on agent phones may not light after reboot or upgrade.	7.1.3.2.0
CM-31392	CM, AMS	Calls failed due to exhaustion of AMS licenses	7.1.3.3.0
CM-31409	Blast conference	CM reset sometimes during blast conference	8.1.1.0.0
CM-31472	Agent, Consultative transfer	Call dropped by CM when agent does a consultative transfer.	8.0.1.2.0
CM-31619	Call pickup, TSAPI user on a call	Not able to pickup the call from pick-group using 3PCC if user was already on another call	7.0.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-31651	Hunt group, removal of member	change hunt group command executed from SAT sometimes resulted in in CM reload	8.1.0.1.1
CM-31689	CTI in use with SIP trunk with UUI Treatment set to 'service-provider'.	ASAI does not send UUI when received over a trunk with UUI Treatment set to 'service-provider'.	7.1.3.5.0
CM-31726	SIP agent, ASAI	SIP agent can't cancel a call in progress via ASAI third party selective drop	7.1.3.5.0
CM-31840	SIP stations configured with Multiple Device Access	System reset occurs when two SIP MDA devices joins and ends the call.	7.1.3.4.0
CM-31895	SIP reachability feature	system reset after running traffic for the long time.	7.0.0.0.0
CM-31902	SIP	CM resets sometimes when INVITE has empty Av-Global-Session-ID header	8.0.1.2.0
CM-31974	shared control registered for an H.323 station of 96x1 type	Customer might see a segmentation fault or mempool errors when trying to delete an H.323 station which has a corresponding shared control station registered.	8.1.0.0.0

Fixes in Communication Manager Release 8.1.1

ID	Minimum Conditions	Visible symptoms	Release found in
CM-10028	Telecommuter call	CM did a software reset	6.3.9.1
CM-12585	Incoming call over FIPN trunk (SA8506 enabled) The calling party number must be mapped to a station in the off-pbx station-mapping form.	A call forwarded from Altura through FIPN trunk to a message center switch would get generic greeting if calling party is mapped in EC500	7.0.0.2.0
CM-18330	CM SMI pages	Missing HTTP Strict-Transport-Security-Header on Webhelp pages	7.1.0.0.0
CM-21102	SIP station, with IP version pref=IPv4 H323 station, with IP version pref=IPv4, Per Service Link with Attd-1 ATTD-1 [Attd station], IP version pref=IPv4, Mode=telecommuter CM with IP version pref=V4, DM=Y	SIP station direct media call to H323 telecommuter attendant fails	7.0.1.1.1
CM-21403	Call classification with TN744 HW11	Denial event 2399 seen when ofcom call classification is attempted on a TN744 HW11 board	7.1.1.0.0
CM-21432	Call center with SIP agents	RONAs are appearing on CMS report more than normal since SIP phones have been installed	6.3.117.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-21550	Two SIP trunk groups.	A customer could see corruption if administering 2 SIP trunks in close proximity time-wise when changing the "Measured" field to the 'both' value and changing the number of members for another measured=both SIP trunk group within a few seconds after the first transaction completed	8.0.0.0.0
CM-21799	WebLM server	CM did not come up since License Server took up 100% CPU when WebLM server was partially reachable	8.0.0.0.0
CM-22985	System Management Interface (SMI) and user operations	The secure log showed password in clear text when a new user was added, or an existing user password was changed using System Management Interface	7.1.3.1.0
CM-23053	Outgoing call via an analog (e.g., CO) trunk group and insert a pause character via the route pattern (e.g., to wait for far-end dial tone)	Call dropped when a call was made over an analog (e.g., CO) trunk group, with pause character added in the route pattern	7.1.2.0.0
CM-23510	Media Gateways in same NR having VOA announcement configured, VDN and pickup group	VOA was not played to the user when a call was picked up by pickup member and also resulting in no talkpath	7.1.2.0.0
CM-24016	SIP trunk to a H.323 station, hair-pinning enabled DTMF mode set to rtp-payload or in-band	Dual-Tone Multi-Frequency (DTMF) did not work with in-band or Real Time Protocol RTP-payload DTMF mode on hair-pinned calls	7.1.3.0.0
CM-24017	Make a video call via VDN and vectors	Customer may observe a problem with the video	7.1.3.0.0
CM-24562	One-X agent, SIP service link. An agent without a password administered. Direct media enabled	One-X agent heard DTMF tones if they use password while logging in	7.1.1.0.0
CM-24766	Three CMs with QSIG H323 trunks	50% of times, QSIG path replacement failed when multiple transfers to the trunk, no impact to the call	7.1.2.0.0
CM-24845	Principal with Busy Indicator button. EC500 enabled on principal. SA9106 enabled	Busy Indicator did not turn off on SIP phones, if EC500 mapped station answered the call and SA9106 was enabled	7.0.1.3.0
CM-25117	AMS announcement and SIP trunk	Under certain circumstances involving far end audio connections, AMS announcements would restart and play over from the beginning	7.1.3.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-25181	J169 set type SIP station, with ANAT=N, IP version pref=IPv4 B179 set type SIP station, with ANAT=N, IP version pref=IPv4 CM configured with ANAT=N, IP version pref=V4, DM=N	Hold failed when attempted from the B179 phone.	7.1.1.0.0
CM-25387	E-911 call and SIP station	Wrong ELIN for E-911 call if ELIN is part of P-Location header.	7.0.1.3.0
CM-25410	Privileged administrator command line access	Unauthorized root privileges could be obtained using sudo as privileged administrator	7.1.3.2.0
CM-25441	Modifications to web access mask, SMI	If Web Access Mask is changed, and then the system is upgraded, or backup/restore operation is performed, the user is unable to access SMI pages after restore	7.1.3.2.0
CM-25597	G650 gateways connected to a flaky network.	False alarms raised against the IPSI maintenance board during network instability	7.1.1.0.0
CM-26032	Deep Secure	The customer used Deep Secure to filter web traffic and found that the SMI has incorrect syntax with the line below.	7.1.3.1.0
CM-27056	ASAI	In rare instances, CM did a software reset	7.1.3.2.0
CM-27266	Coverage Answer Group members part of the Pickup Group. Call termed on CAG group	Members of the pickup group will not get Enhanced Call Pickup alert if CAG members are part of the Pickup group and call Termed on CAG group.	7.1.0.0.0
CM-27320	SIP trunk call, SAC enabled, Voice Mail, DM enabled	A covered call was not being forwarded if SIP Direct Media was enabled	7.0.1.2.0
CM-27445	CM, AMS with announcements	The data collected by "list directory so media-server" could potentially be incomplete	7.1.3.2.0
CM-27466	Multiple pickup groups	Intermittently other pickup group members were getting pickup group notifications for the group to which they did not belong	7.1.2.0.0
CM-27469	A SIP trunk, SIP station, call transfer, AES	AES restarted when it received a hold event from CM for SIP transfer scenario where the SIP REFER method was used for transferring the call	8.0.1.1.0
CM-27495	Call Centers with VuStats buttons of type "agent-extension".	VuStats button formats of type "agent-extension" always showed the agent as "NOT MEASURED".	8.0.0.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-27516	16xx set type	"disable ip-reg-tti old xxxx" command did not work for 16xx set type although 16xx set type is TTI un-named	7.1.3.0.0
CM-27648	NA	UDP sockets can be closed by sending zero-length packets.	7.1.2.0.0
CM-27673	Enable caller disconnect tone	Sometimes CMS_IDLE event is not sent in an SIP-agent call to CMS.	7.1.2.0.0
CM-27678	MCA bridge call	Possible system restart when processing an MCA bridge call	8.0.1.0.0
CM-27689	Unregistered SIP Stations as members in a hunt group	SIP Phones which are unregistered were not deactivated at hunt groups	7.1.3.2.0
CM-27695	SIP station with coverage path and SIP MM	Voicemail played a generic greeting instead of the prompt to leave a message for the called extension if "Coverage Answer Group" was the first coverage point followed by SIP MM as the second point in the coverage path	7.1.3.3.0
CM-27697	H323 station	Denial event 1941 always had ip address 0 in Data 2is	8.0.1.1.0
CM-27726	Administer AFR trunk with 256 members and then reduce it 1	Can't remove AFR trunk members	8.0.1.1.0
CM-27751	CM with AMS	AMS remained stuck in pending-lock state and became unusable	7.0.1.2.0
CM-27752	AMS link down	Customer does not see CM alarm when AMS link was down, and the only warning was seen which did not alarm out	7.1.3.3.0
CM-27845	TTI enabled	Multiple ports are unable to be assigned to stations. Data conflict detected, please cancel and try again error seen on SAT. Softphones could not login.	7.1.3.2.0
CM-28028	Signaling group, DPT not enabled, typical ip-network-map configuration	DPT was not triggered from SIP station in a survivable mode	7.0.1.3.0
CM-28074	Incoming INVITE with "History-Info" headers but no "histinfo" tag in "Supported:" header.	The "History-Info" headers were not tandem'ed in the outgoing INVITE from the incoming INVITE if "Supported:" header did not have "histinfo" tag.	7.1.3.3.0
CM-28107	Auto callback, SIP	Auto-cback showed up in phone display as a national call only. The phone display only displayed the national phone number as like 0069910xxxxx instead of the full international number	6.3.118.0

ID	Minimum Conditions	Visible symptoms	Release found in
		0004969910xxxxx even if the number is available in the sip methods	
CM-28119	Call Center	During vector processing, if DTMF tones were received, it caused no talk path on the call.	7.1.1.0.0
CM-28138	Logging Levels field logging enabled	The commandhistory file can have entries for vdn form field changes that did not occur.	7.1.3.2.0
CM-28178	Survivability servers and Avaya Aura Media Servers	In an installation with the Main server and one or more survivable servers served by Avaya Aura Media Servers (AAMS), the Main may go out of service (i.e., refuse registrations and service to endpoints) if certain AAMS are out of service and others go out of service temporarily and come back into service.	7.1.3.3.0
CM-28183	CM8.0 and new loads, System Manager cut through mode do not handle "brg-appr" buttons on the Station form properly when the "Per Button Ring Control" feature is enabled. The "R:" field is not drawn properly	System Manager cut through mode does not handle "brg-appr" buttons on the Station form properly when the "Per Button Ring Control" feature is enabled. The "R:" field is not drawn properly and display of page is incorrect	8.0.1.0.0
CM-28207	Avaya Experience Portal softphone ept registered to CM and SIP RFC2833 trunks	Avaya Experience portal stations configured on CM cannot detect DTMF input from SIP trunks using RFC2833	7.1.3.3.0
CM-28246	Incoming SIP trunk call to an agent	Incorrect CDR value for disconnect information field for incoming SIP trunk call to an agent	7.1.3.2.0
CM-28255	Large CM configuration with more than 50 audio group entries	The customer could not access all 378 entries on the AUDIO GROUP form	8.0.1.1.0
CM-28276	SA9095 enabled and 1 or 2 members available to take calls	SIP Phones which are unregistered are not deactivated at hunt groups. With SA9095 enabled and low number (<3) of available members to take calls, a call can experience long delays where no member is being alerted	7.1.2.0.0
CM-28283	CM and hunt group	Calls were not routed to agent or hunt group members when a stale entry existed in off-pbx-station records, i.e. no call appearance	8.0.1.1.0

ID	Minimum Conditions	Visible symptoms	Release found in
		was used, but still, an entry existed in change off pbx station	
CM-28287	Coverage answer group, TEAM buttons monitoring the CAG SIP station members.	CM was getting strange resets, system message buffer exhaustion messages	7.1.3.1.0
CM-28429	A SIP trunk, transfer and across GW connections	Inter Gateway Connection was held by the call even after shuffling	7.1.3.1.0
CM-28544	Hold on the SBCE is set to RFC2543. MOH disabled	No talk path in remote worker case when a bridge appearance bridged on after principal held the call and resumed after a bridge on	7.1.3.2.0
CM-28596	H.323 agent	One-x H.323 agent was not put on-hook after the caller dropped the call before the announcement finished to play to the agent	7.1.3.1.0
CM-28604	Walk avCmStatusTrunkRange SNMP MIB on a system with over 1000 sip trunk members	The customer sees segmentation faults and failure to complete a MIB walk of avCmStatusTrunkRange MIB.	8.0.1.1.0
CM-28627	Busy out of SIP signaling group with 1500 trunk members	Unexpected internal buffer allocation resulted in CM restart & interchange	8.0.1.1.0
CM-28700	SIP station, Send All Calls button configured for the SIP station	Third-party feature activation failed on SIP station if the preferred handle configured for the third-party extension on SMGR had a different extension than the extension configured on CM.	7.1.3.1.0
CM-28792	SIP trunk call	SIP trunk member was active on a call with call record forever if the far end sent a BYE instead of a final response to CM's outgoing INVITE	7.1.3.2.0
CM-28795	Shared station, DMCC IP softphone registration	SAT showed station corruption	8.0.1.0.0
CM-28811	SIP trunk call, VDN and vector having typical steps, G729 codec, "Prefer G711 for announcement" flag on change system-parameters ip-options	Announcement on AMS did not get played when "prefer G711 for an announcement" was enabled	8.0.1.0.0
CM-28812	Auto callback	Canceling auto-callback failed when call routed from CM to SM to CM	6.3.118.0
CM-28813	IP trunks, AEP 7434ND administered stations, TN2602 media processor	Avaya Experience Portal IVR function may fail to detect customer entered digits	7.1.3.2.0
CM-28822	6.3 CM system, with non-EAS measured agents.	CM went into rolling reboots, after upgrade from CM6.3 to CM8.1	8.1.0.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-28837	SIP DM enabled	Occasionally no talk path on Service observed calls	7.1.3.1.0
CM-28840	QSIG CAS (centralized attendant group)	Occasionally QSIG CAS calls dropped when seg fault happens	8.0.1.1.0
CM-28841	SIP phone, non AST-2 phone, equinox and call recorded	When an equinox client has recorder ports, and it merged the call in adhoc conference way, then the recorder stopped getting RTP stream	7.1.3.2.0
CM-28849	Intervening Region field on the ip-network-regions form	The "Intervening Regions" field on the ip-network-regions form overlapped causing the data to be truncated	8.1.0.1.0
CM-28867	CM, call transfer to agent, ringing call	CTI-application did not receive the connect event when the transferred call was answered	7.1.3.3.0
CM-28983	Upgrade from 7.0 or earlier release	The "Cluster" field on the SAT Signaling Group form displayed a "?" after an upgrade from an earlier release	8.0.1.1.0
CM-29001	Softphone Agents in telecommuter mode, non-shuffable SIP trunk, permanent mode service links, NCR (Network Call Redirection) enabled	Agents in telecommuter mode, using non-shuffable SIP trunk, permanent mode service links, with NCR (Network Call Redirection) enabled experienced no talk-path during calls	7.1.3.2.0
CM-29029	ISDN-PRI trunk	Remote Automatic Callback activation occasionally failed	7.1.3.3.0
CM-29180	Disable EC500 from station form	EC500 destination of principal was alerted, even though EC500 state for the principal was disabled on station form	8.1.0.1.0
CM-29228	List trace command	Unassigned numbers looping between ASM and CM, and list trace command did not capture the appropriate information needed to troubleshoot the root cause quickly	7.1.3.3.0
CM-29253	ECD enabled in system, issue skill threshold status query.	ACR completely stops recording when CTI link is version 7	7.1.3.4.0
CM-29296	Call-pickup group	Call answered by call-pickup button was not getting recorded via DMCC	7.1.3.2.0
CM-29307	SIP, NCR	CM did reset/interchange due to NCR REFER-491 loop	7.1.2.0.0
CM-29319	BRI stations and trunks	CM did a warm restart when an internal data structure was exhausted	7.1.2.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-29321	SA9095 enabled and SIP stations in the hunt group	Coverage to hunt group caused an internal call to remain stuck	7.1.2.0.0
CM-29340	SEMT, SIP stations	SEMT (SIP Endpoint Managed Transfer) could fail if the transferred SIP station had preferred handle configured differently from the CM (Communication Manager) administered extension	7.1.3.4.0
CM-29538	Analog phone with bridge appearance on another analog phone	CM did a segmentation fault when a call is made to an analog station with the bridge to another analog station	8.1.0.1.1
CM-29745	SIP call	In a SIP-SIP call, if 183 was received with PAI header having an extension longer than 22 characters, CM sometimes did a software restart	8.1.0.1.1
CM-29760	On a CM8.1 system try and register a lot of IP stations at one time	CM becomes unresponsive	8.1.0.1.1
CM-29800	The customer uses analog bridging	The system reset in function when the station is alerting.	8.1.0.1.1
CM-29860	DCS config on trunk-group	Calls over DCS trunk, CM restarts	8.1.0.1.1
CM-29892	Trunk-member with > 32767	Incoming call with trunk member more than 32767 then the call was dropped after digits collected call routed to collected digits	8.1.0.1.1
CM-29974	AES with a version less than 8.1 SP1 (AES 8.1.1) in use. CTI adjunct issues agent login audit query	An Agent Login Audit query issued by a CTI application failed and received an abort generated by AES with a cause value of CS0/100 (Invalid IE)	7.1.3.4.0
CM-29984	An unprivileged administrator using SMI	Unprivileged users were asked to change the password every time they logged in to the SMI	7.1.3.4.0
CM-30007	More than 4 shared station through DMCC	When more than 4 shared stations were registered then, DMCC failed to display registration information for the registered stations on executing Endpoint reg info query	8.0.1.0.0

Fixes in Communication Manager Release 8.1.0.2.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-29180	EC500	EC500 status on the station is ignored whenever call follows a coverage-answer-group. EC500 call	8.1.0.1.0

ID	Minimum Conditions	Visible symptoms	Release found in
		invoked even when EC500 status is disabled for the station(s) in the group	
CM-29286	Call Center, CMS R19.0	In SAT system-parameters feature-related field "CMS (appl mis):" did not include an option for CMS R19.0	8.1.0.0.0
CM-28544	Music-On-Hold disabled on CM, hold on the SBCE is set to RFC2543	Inbound SIP call from OPTIM-mapped cell/mobile has no audio after transfer	7.1.3.2.0
CM-28795	Shared station/DMCC IP softphone unregisters and a new IP station is added	System Administration Tool (SAT) shows station corruption	8.0.1.0.0
CM-28822	Non-EAS measured Agents	CM went into rolling reboots, after upgrade from CM 6.3 to CM 8.1	8.1.0.0.0
CM-29093	Telecommuter Mode	Telecommuter stopped working after some time when the audit is triggered	8.1.0.0.0
CM-28405	No Hold Conference, Agent	No Hold Conference call kept on ringing even if parent call is disconnected when initiated from agent and agent disconnects	8.1.0.0.0
CM-28199	Register more than 1000 DMCC stations, Failover or network outage situation	With more than 1000 DMCC stations registered, CM resets if AES fails over and standby did not become active for more than 15 mins	8.1.0.1.0
CM-28972	Removing Extension	“Error Encountered” while removing 16-digit extensions (hunt-group, bridged appearance, team button, virtual map-to station)	8.1.0.0.0

Fixes in Communication Manager Release 8.1.0.1.1

ID	Minimum Conditions	Visible symptoms	Release found in
CM-28598	IP Dect station configured	Call to IP Dect station fails and CM was reset	8.1.0.0.0
CM-28277	SNMP trap configured	No SNMP Traps were sent.	8.1.0.0.0
CM-28023	SIP Service Observing	Coaching from a SIP service observer was denied.	8.1.0.0.0
CM-28434	Configure users more than 66K and try to monitor the users using TSAP exerciser	The user could not be domain controlled in 300k user base, when they were beyond the range of 65K	8.1.0.0.0
CM-28582	Have measured VDN, trunk or hunt on CM6.3	The system goes into rolling reboots, after upgrade from CM6.3 to CM8.1	8.1.0.0.0

Fixes in Communication Manager Release 8.1

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
CM-14982	Media Gateway configured for Clock Synchronization Over IP (CSoIP) with no external TDM clock source	"Status ip-synchronization oos-members" screen incorrectly shows a slave member is out of service.	7.0.1.2.0
CM-20978	Call Recording, send-nn	When send-nn is activated on the station, ACR could not record the call	7.0.0.0
CM-21140	Incoming call CPN contains '+'	Call failed to tandem if the incoming CPN contains '+' from ISDN/H.323 trunk	6.3.9.0
CM-21364	H.248 Media Gateway	CM did restart after many proc errors	7.1.1.0.0
CM-21387	Communication Manager 7.1.x or 8.0.x.	Under rare conditions, if a new user was added from the SMI and the "Force password change on next login" option was selected, the password change at first login fails with the message "Authentication token manipulation error, old password is not correct".	7.1.2.0.0
CM-21434	ESS, System Platform	Server interchanged (if duplicated) or loss of service (if not).	6.3.15.1
CM-21451	CM, Port Network with medpro, multiple network regions	CM may not be able to connect to an announcement from a remote PN	6.3.13.0
CM-21530	CM Paging Feature	CM Paging feature functioned differently, all analog lines on phones reflected to be domain controlled.	7.0.1.3.0
CM-21628	SIP Traffic	The call established successfully but retry-after: Header not parsed correctly, a parse error seen in the logs	6.3.15.1
CM-21733	SIP Traffic	SIP call dropped after receiving unexpected SDP MID attribute	7.1.2.0.0
CM-21899	Incoming SIP Call	Segmentation Fault was observed when an incoming INVITE to Avaya Aura Communication Manager has malformed reason code, or Unicode supported SDP	7.1.1.0.0
CM-22058	All trunk members in a SIP trunk group are in use. Call recording is active, and VOA is administered	CM sent BYE to SIP station erroneously when unrelated call drops	7.0.1.3.0
CM-22061	SIP Traffic	CM did restart	8.0.0.0.0, 7.1.0.0.0
CM-22081	SIP Traffic	CM did interchange	8.0.0.0.0
CM-22558	CM, AMS and filename with '&', i.e. AT&T_Greeting2	CM cannot request play AMS sourced announcement if the filename contains an '&' (ampersand)	7.1.1.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-22569	Configure per-co line group button on two stations	Softkeys on a station did not appear when taking a per-COline off hold from another station where it was answered	6.3.18.0
CM-22721	H.323 station with personalized buttons configured	When any personalized button label on CM H.323 endpoint was changed to blank, the button was removed from the phone display.	8.1.0.0.0, 8.0.0.0.0, 7.1.3.0.0
CM-22774	Incoming and outgoing numbering format were international and 'tandem calling party number' conversion table did not have an entry for 'insert'	Tandem Calling Party Number table entry was not prefixing outgoing digits with '+', if incoming and outgoing numbering format were of type 'international'.	6.3.12.0
CM-22979	SIP station	Barge tone was played continuously if the SIP station bridged in an EC500 call.	7.1.3.0.0
CM-23016	Attendant Group	The call-in attendant group queue is dropped when attendants became idle, denial event 1536 generated	7.1.3.1.0
CM-23083	CM, SMGR WebLM	"Call Center Release:" field value was not modified in 8.0 and 8.1 releases	8.0.0.0.0
CM-23134	Monitor VDN and predictive call	ASAI message for an incoming call, contained default trunk number (#####) and the called number as the VDN instead of correct calling party number in case of predictive calling.	7.1.3.0.0
CM-23166	calltype analysis configured	User dialed from call log containing ARS/AAR code was shown in ASAI called Device IE on event orig went to cti-applications	7.1.3.0.0, 6.3.113.0
CM-23188	Attendant, Transfer Call	When Attendant transfers a call while hearing the zip tone, covers to voicemail but the call is dropped	7.1.3.0.0
CM-23363	Team Button configured Station had COR enabled	Team Button monitoring station was not able to pick up the incoming call at the monitored station, by going off-hook	7.1.3.1.0
CM-23579	Call Parking	Digital stations that are logged in with Agent ID, which are recorded by Verint (SSC) are unable to park a call successfully	7.0.1.3.0
CM-23609	VDN, IP (H.323) Stations	The call dropped from AAEP due to missing UUI information. The UUI information did not get a pass to AES and AAEP as CM fails to build and send the ALERT and CONNECTED event to AES putting UUI information.	7.1.3.1.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-23678	Signal Button	Signal button gets denial treatment when signaling an analog station	7.1.3.0.0
CM-23742	Tenant form page 4, entry for 230.	At the SAT, the title of the field for tenant 230 on the Tenant form page 4 is incorrectly displayed as 220.	7.1.3.1.0
CM-23754	GA or prior kernel update is on system.	Communication Manager had certain vulnerabilities described in Avaya Security Advisory ASA-2018-284. To see this document, go to http://support.avaya.com and search for that number	8.0.0.0.0
CM-23851	SIPCC Agent, AAAD desktop	CMS Reports ignored the conference call involving SIPCC agent using AAAD as a moderator	7.1.3.0.0
CM-23903	SIP station	Communication Manager (CM) could experience a system segmentation fault if the termination to a SIP station returned BUSY.	7.1.3.0.0
CM-23947	Attendant, Transfer Call	Attendant extended call to a virtual station that covers to remote VM sometimes fails to complete	7.1.2.0.0
CM-24032	Hunt group with one member. The agent must be video-enabled RONA	Video enabled softphone agent cannot handle the same call coming out of the queue if the same agent did not answer the 1st time	7.1.3.0.0
CM-24153	Telecommuter mode, Permanent SIP Service Links, Incompatible Codec in between	Agents using telecommuter permanent SIP service link failed to get audio	7.1.3.0.0
CM-24168	SIPCC agent, COR not enabled for DAC call	While a SIPCC agent is on an outbound call, an incoming call is delivered to the agent by Experience Portal as a DAC when the agent COR does not allow DAC. CMS ignored the call.	7.1.3.1.0
CM-24310	IPV6 procr ip-interface	An error message was seen instead of data at the SAT interface when executing a "list ip-interface all" command	7.1.3.1.0
CM-24510	CM License, SMGR WebLM	SMGR 8.0 WebLM did not show license status for CM	7.1.2.0.0
CM-24669	CDR	CM SMDR process did cause it to interchange	7.1.3.2.0
CM-24975	Direct Agent Call	CM did not send Call handing preference, Service objective information to CMS for DAC calls sent to an agent	8.0.0.1.2, 7.1.2.0.0
CM-27056	Query to Agent status via TSAPI	Occasionally ASAI link did restart	7.1.3.2.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-27645	Analog Station	Analog station when it goes off-hook, no dial-tone	8.1.0.0.0

Known issues and workarounds in Communication Manager Release 8.1.x.x

Known issues and workarounds in Communication Manager Release 8.1.3.1.0

None

Known issues and workarounds in Communication Manager Release 8.1.3.0.1

None

Known issues and workarounds in Communication Manager Release 8.1.3

None

Known issues and workarounds in Communication Manager Release 8.1.2

ID	Minimum conditions	Visible symptoms	Workaround
CM-31721	Use SDM to upgrade and set “require passphrase at boot time” to ‘y’	CM upgrade fails	Set “require passphrase at boot time” to ‘n’
CM-31720	Enable encryption during installation Remote key server is not reachable	If a remote key server is down, then encryption Status command takes around 2 minutes 10 secs to execute. The time taken for command to execute increases exponentially based on number of remote key servers in disconnected state	NA
CM-31685	Enable encryption during installation. Remote key server configured	User is able to enable Local Key even after adding Remote Key server in encrypted CM	NA
CM-31119	SSP update	Host Name in CM SMI disappears when we deactivate old and activate new SSP (occurrence is Intermittent)	Reconfigure hostname on SMI in case it disappears.
CM-21851	VE based upgrade from 6.3 to 8.1 using SMGR SDM	Restore fails, upgrade fails	Upgrade manually without using SMGR SDM

Known issues and workarounds in Communication Manager Release 8.1.1

ID	Minimum conditions	Visible symptoms	Workaround
CM-29546	Trunk group members being modified which are greater than or equal to 255 from multiple sat sessions at any given time	Corruption of trunk group members impacting trunk calls	To address the issue, please look at PSN: PSN020424u

Known issues and workarounds in Communication Manager Release 8.1

ID	Minimum conditions	Visible symptoms	Workaround
AURABUILD-521	CM installation via the command line (AWS/KVM/ISO)	The first "(<U+FEEF>)" Special character appears before the End User License Agreement (EULA) text	None
CM-27645	Analog/CO Trunk	An outgoing call via Analog trunk could not be placed	Please execute below SAT commands • *busy-out board <board number # inserted in the gateway>* • *reset board <board number # inserted in the gateway>* • *release board <board number # inserted in the gateway>*
CM-28170	No Hold Conference button feature on the SIP endpoint	All other features are blocked when NHC call is initiated from the SIP endpoint	Wait for NHC time out, that can be configured on "No Hold Conference Timeout" field on system-parameters features page 7
CM-28023	SIP endpoint	SIP supervisor cannot initiate a coaching session to agents	None
CM-28822	The problem will happen if the 6.3 system, had non EAS measured agents	System goes into rolling reboots, after upgrade from CM6.3 to CM8.1	None

Avaya Aura® Session Manager

What's new in Session Manager Release 8.1.x.x

What's new in Session Manager Release 8.1.3.1

For more information see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

What's new in Session Manager Release 8.1.3

For more information see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

Note: Use of Session manager for Apple Push Notification requires IX Workplace for IOS version 3.14 or later, and Avaya SBC 8.1.2 or later. For more details see PSN020507u.

What's new in Session Manager Release 8.1.2

For more information see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

As of 8.1.2, customers utilizing AVP or VMware based systems are able to activate disk encryption during OVA installation. To support ongoing maintenance of this feature, the following commands have been added in the 8.1.2 release: ***encryptionStatus, encryptionRemoteKey, encryptionPassphrase,*** and ***encryptionLocalKey***. Note that these commands are only applicable if disk encryption is enabled using the Avaya OVA methods. These commands are not to be used if the customer has provided their own disk encryption using other methods.

What's new in Session Manager Release 8.1.1

For more information see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

Future use fields visible in Avaya Aura® Session Manager Release 8.1.x.x

Future use fields visible in Avaya Aura® Session Manager Release 8.1

The underlying framework for an upcoming new Avaya Aura® Platform enhancement "Avaya Aura Distributed Architecture" will be seen in some Release 8.1 administration screens and deployment options. The following fields seen on System Manager screens for Session manager are intended for future use:

- Session Manager → Global Settings → Enable Load Balancer

The SIP Resiliency Feature was introduced for Aura core components in 8.0 release. However, this feature is not useful until a future time when Avaya SIP clients also support SIP Resiliency. As a result, it is highly recommended that this feature NOT be enabled on Session Manager 8.0 (or later) until such time. The following field seen on System Manager screens for Session manager are intended for future use:

- Session Manager → Global Settings → Enable SIP Resiliency

Security Service Pack

Security Service Pack

Beginning with 8.1.1, Session Manager is releasing an 8.1 Security Service Pack (SSP). This SSP can be applied to any version of 8.1 and only includes Red Hat security updates. It is not necessary to apply the SSP on top of 8.1.1 itself because 8.1.1 includes all the same updates. The SSP is not intended for use by "software-only" customers.

Beginning December 2020, SSPs will also be released on a more frequent cadence. This means that SSPs may also be available between application Service Packs/Feature Packs. SSP required artifacts and fix IDs will no longer be tracked in the Release Notes. For further information on contents and installation procedures, please see PCN**2112S.**

Required artifacts for Session Manager Release 8.1.x.x

Required artifacts for Session Manager Release 8.1.3.1

The following section provides Session Manager downloading information. For deployment and upgrade procedure, see product-specific deployment and upgrade documents on the Avaya Support website.

Filename	PLDS ID	File size	Version number	Comments
Session_Manager_8.1.3.1.813113.bin	SM000000194	662 MB	8.1.3.1.813113	
Session_Manager_8.1-SSP-06002.bin	SM000000195	264 MB	8.1-SSP-06002	

Required artifacts for Session Manager Release 8.1.3

The following section provides Session Manager downloading information. For deployment and upgrade procedure, see product-specific deployment and upgrade documents on the Avaya Support website.

Filename	PLDS ID	File size	Version number	Comments
Session_Manager_8.1.3.0.813014.bin	SM000000187	528 MB	8.1.3.0.813014	
Session_Manager_8.1-SSP-04004.bin	SM000000188	252 MB	8.1-SSP-04004	
SM-8.1.0.0.810007-e70-1E	SM000000176	2126 MB	8.1.0.0.810007-e70-1E	Updated 8.1 Encrypted OVA

Required artifacts for Session Manager Release 8.1.2

The following section provides Session Manager downloading information. For deployment and upgrade procedure, see product-specific deployment and upgrade documents on the Avaya Support website.

Filename	PLDS ID	File size	Version number	Comments
Session_Manager_8.1.2.0.812033.bin	SM000000173	482 MB	8.1.2.0.812033	
Session_Manager_8.1-SSP-008.bin	SM000000174	227 MB	8.1-SSP-008	

Filename	PLDS ID	File size	Version number	Comments
dmutility-8.1.2.0.812002.bin	SM000000175	1.14 MB	8.1.2.0.812002	
SM-8.1.0.0.810007-e67-0E.ova	SM000000176	2126 MB	8.1.0.0.810007-e67-0E	Updated 8.1 OVA including encryption
BSM-8.1.0.0.810007-e67-0E.ova	SM000000177	1981 MB	8.1.0.0.810007-e67-0E	Updated 8.1 OVA including encryption

Required artifacts for Session Manager Release 8.1.1

The following section provides Session Manager downloading information. For deployment and upgrade procedure, see product-specific deployment and upgrade documents on the Avaya Support website.

Filename	PLDS ID	File size	Version number	Comments
Session_Manager_8.1.1.0.811021.bin	SM000000167	472 MB	8.1.1.0.811021	
Session_Manager_8.1-SSP-005.bin	SM000000168	218.7 MB	8.1-SSP-005	

Required artifacts for Session Manager Release 8.1

The following section provides Session Manager downloading information. For deployment and upgrade procedure, see product-specific deployment and upgrade documents on the Avaya Support website.

Filename	PLDS ID	File size	Version number	Comments
SM-8.1.0.0.810007-e67-01.ova	SM000000152	2105.6 MB	8.1.0.0.810007	
BSM-8.1.0.0.810007-e67-01.ova	SM000000153	1948.9 MB	8.1.0.0.810007	
SM-8.1.0.0.810007-kvm-01.ova	SM000000154	2090.8 MB	8.1.0.0.810007	
BSM-8.1.0.0.810007-kvm-01.ova	SM000000155	1943.9 MB	8.1.0.0.810007	
SM-8.1.0.0.810007-aws-01.ova	SM000000156	2136.2 MB	8.1.0.0.810007	
Session_Manager_8.1.0.0.810007.iso	SM000000157	2016.1 MB	8.1.0.0.810007	
dmutility-8.1.0.0.810007.bin	SM000000158	1.14 MB	8.1.0.0.810007	

Note: To determine the OVA version running on Session Manager, use the following command:

- ***grep "FullVersion" /opt/Avaya/common_services/ovf_file***

Required patches for Session Manager Release 8.1

For information about patches and product updates, see the Avaya Technical Support Web site https://support.avaya.com. For more details, see PCN2099S on the Avaya Technical Support site.

Installation for Session Manager Release 8.1.x.x

Backing up the software

Refer to the Session Manager Backup and Restore section of the Administering Avaya Aura® Session Manager guide.

Installing the Session Manager software

For more detailed information about installing your Session Manager, see Avaya Aura® Session Manager deployment documents on the Avaya Support website.

Upgrading the Session Manager software

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

Special Case Upgrade Paths

1. From bare metal Session Managers

   The supported upgrade paths to Session Manager 8.1.x are from:

   - SM 8.0 and subsequent feature or service packs
   - SM 7.1 and subsequent feature or service packs
   - SM 7.0 and subsequent feature or service packs
   - SM 6.3 and subsequent feature or service packs

   Note: Systems running any earlier SM release must be upgraded to one of the above releases before it can be upgraded to Session Manager 8.1.

2. Security Hardened Mode

   When upgrading from a Session Manager Release 8.0 that is configured in Security Hardened mode to Release 8.1, the Cassandra DB will also be upgraded. Session Managers that are on Release 8.1 will not synchronize Cassandra data with Session Managers that remain on Release 8.0. Also, Cassandra repair operations will fail. These issues will clear up once all Session Managers are updated to Release 8.1.

3. VMware-based Session Manager

   The supported upgrade paths to Session Manager 8.1.x are:

   - SM 6.3 and subsequent feature or service packs
   - SM 7.0 and subsequent feature or service packs
   - SM 7.1 and subsequent feature or service packs
   - SM 8.0 and subsequent feature or service packs

4. KVM-based Session Manager

   The supported upgrade paths to Session Manager 8.1.x are:

   - SM 7.1.1 and subsequent feature or service packs
   - SM 8.0 and subsequent feature or service packs

5. AWS-based Session Manager
   - SM 7.0.1 and subsequent service packs
   - SM 7.1 and subsequent feature or service packs

- SM 8.0 and subsequent feature or service packs

  Note: These upgrades are not supported by System Manager - Solution Deployment Manager (SDM), so to upgrade, it is necessary to use the data migration utility as described in the *Session Manager Upgrade* guide.

6. Upgrading SMGR and SM from R6 to R8

   Prior to upgrading the SMGR to R8, the SM R6 should be upgraded to SM 6.3.22 or above. See PSN: https://downloads.avaya.com/css/P8/documents/100171014 for details.

7. Upgrading Session Manager from 6.x or 7.x to 8.x

   SIP Endpoint device data is not shared between 8.x and prior release realms. Therefore, changes made to an endpoint registered to an 8.x Session Manager will not be reflected on endpoints registered to a prior release Session Manager. This issue will be resolved when all SM nodes are updated to 8.x.

8. System Manager Compatibility
   Session Manager 8.1.2.1 is compatible with System Manager 8.1.2.0.

Troubleshooting the installation

Refer to Troubleshooting Avaya Aura® Session Manager.

Restoring software to the previous version

Refer to the product documentation.

Fixes in Session Manager Release 8.1.x.x

Fixes in Session Manager Release 8.1.3.1

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-83224	Log harvester use on SM 7.1 or later	Log Harvester fails to collect logs from Session Managers.	7.1.3.6
ASM-83220	Remove diffie-hellman-group1-sha1 cipher support	N/A	8.1.3.0
ASM-83819	Jgroup failure	Session Manager Dashboard shows incorrect data	8.1.3.0
ASM-82975	Remove static key cipher support	N/A	8.1.3.0
ASM-82989	Session manager upgrade from 8.1.1 to 8.1.3	Cassandra DB is out of service	8.1.3.0
ASM-83882	User has multiple SIP devices and has device adaptation configured.	Adaptation is invoked for first device only when user is called.	8.1.3.0
ASM-83233	CS1K adapter configured for an entity that sends History-Info header with dotted values in index or rc parameter(s).	CS1K adapter encounters an exception which may affect processing of the message and cause problems with other features (e.g. CDR).	8.1.3.0
ASM-83068	Upgrade Session Manger to 8.1.3 after removing some nodes from Cassandra cluster	Session Manager dashboard shows User Data Storage status failed	8.1.3.0
ASM-83989	Performing a reboot of SM after at least 24 hours of running	The generateTestAlarm.sh script fails to generate an alarm.	8.1.3.0
ASM-82912	Administrator changes to the extension number of a user that has an associated Branch Session Manager	The user edit operation times out after 7 minutes and displays a message of an internal error	7.1.3.6
ASM-82906	Attempted CODEC change in SIP INVITE exchange	traceSM incorrectly showing CODEC change in RTP view	8.1.0.0
ASM-80502	Remote Worker	Incorrect VMON server information is sent to Avaya Remote Worker devices	7.0.1.0
ASM-83193	[RHSA-2020:5002] Moderate: curl	N/A	8.1.3
ASM-83194	[RHSA-2020:5009] Moderate: python	N/A	8.1.3
ASM-83195	[RHSA-2020:5011] Moderate: bind	N/A	8.1.3
ASM-83655	[RHSA-2020:5566] Important: openssl	N/A	8.1.3
ASM-82609	[RHSA-2020:3901] Low: libpng security update	N/A	8.1.3
ASM-76337	[RHSA-2019:1619] Important: vim security update	N/A	8.1.3
ASM-82614	[RHSA-2020:4005] Moderate: libxslt security update	N/A	8.1.3
ASM-82598	[RHSA-2020:4041] Moderate: openldap security update	N/A	8.1.3
ASM-82604	[RHSA-2020:4072] Moderate: libcroco security update	N/A	8.1.3

ASM-82599	[RHSA-2020:3908] Moderate: cpio security update	N/A	8.1.3
ASM-83196	[RHSA-2020:5083] Moderate: microcode_ctl	N/A	8.1.3
ASM-82584	[RHSA-2020:3952] Moderate: expat security update	N/A	8.1.3
ASM-82919	[RHSA-2020:4276] Important: kernel security update	N/A	8.1.3
ASM-82612	[RHSA-2020:4032] Moderate: dbus security update	N/A	8.1.3
ASM-82613	[RHSA-2020:3848] Low: libmspack security update	N/A	8.1.3
ASM-83190	[RHSA-2020:4907] Important: freetype security update	N/A	8.1.3
ASM-82611	[RHSA-2020:3915] Moderate: libssh2 security update	N/A	8.1.3
ASM-82610	[RHSA-2020:3911] Moderate: python security update	N/A	8.1.3
ASM-82602	[RHSA-2020:3916] Moderate: curl security update	N/A	8.1.3
ASM-82608	[RHSA-2020:3864] Moderate: cups security and bug fix update	N/A	8.1.3
ASM-82615	[RHSA-2020:4060] Important: kernel security, bug fix, and enhancement update	N/A	8.1.3
ASM-82603	[RHSA-2020:4011] Moderate: e2fsprogs security and bug fix update	N/A	8.1.3
ASM-82605	[RHSA-2020:3861] Low: glibc security, bug fix, and enhancement update	N/A	8.1.3
ASM-82607	[RHSA-2020:4007] Low: systemd security and bug fix update	N/A	8.1.3
ASM-82606	[RHSA-2020:3978] Moderate: glib2 and ibus security and bug fix update	N/A	8.1.3
ASM-82597	[RHSA-2020:3996] Moderate: libxml2 security and bug fix update	N/A	8.1.3
ASM-82585	[RHSA-2020:4026] Moderate: mariadb security and bug fix update	N/A	8.1.3
ASM-83189	[RHSA-2020:5023] Moderate: kernel security and bug fix update	N/A	8.1.3
ASM-82951	[RHSA-2020:4350] Moderate: java-1.8.0-openjdk security and bug fix update	N/A	8.1.3
ASM-83652	[RHSA-2020:5437] Important: kernel security and bug fix update	N/A	8.1.3
ASM-82600	[RHSA-2020:4076] Moderate: nss and nspr security, bug fix, and enhancement update	N/A	8.1.3

Fixes in Session Manager Release 8.1.3

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-79440	Attempt to add dial pattern in routing policies using filter	Operation fails with error message	7.1.3.3
ASM-81552	An egress adaptation is configured to adapt To/From headers. The far end entity responds with a 200 OK to the INVITE request without sending any provisional response(s).	The To/From headers in 200 OK are not restored to pre-adapted values when the response is sent to the originating entity.	8.1.2.1
ASM-81214	Cannot add both Crisis alert and No hold conference buttons as favorites in endpoint editor	Operation fails	8.1.0.0
ASM-80437	Mixture of UDP and TCP entity links.	SIP reINVITE is not retransmitted as mandated by RFC 3261.	7.1.0.0
ASM-80701	Setting CDR record format to XML and having calls active longer than the CDR Service interval	CDR records will have the port number rather than the dialed number.	7.1.3.3
ASM-79245	An egress adaptation is configured to adapt To/From headers. The far end entity modifies only the display name portion of the header values when it responds to the INVITE or sends a new request on the session towards the Session Manager.	The To/From headers in the 200 OK response and in subsequent requests on the session from the far end entity are not restored back to original values when sending the message back to the originating entity.	8.0.1.0
ASM-78341	Adding a contact from Active Directory on One-X Communicator	Calling the contact may fail because the endpoint will make the call using the contact’s email handle.	7.1.3.3
ASM-80490	Unable to modify Profile Settings via the endpoint editor for a newly added SIP user.	Settings fail to appear on user’s SIP endpoint	8.1.2.0
ASM-80733	Device adaptation is configured to modify NOTIFY requests sent by SM.	NOTIFY requests sent by SM are not modified.	8.1.2.0
ASM-79820	Unable to apply language setting to SIP endpoints served by Avaya Device Adapter.	Settings fail to appear on user’s SIP endpoint	8.1.2.0
ASM-78557	High usage of the Cassandra database on Session Manager.	Stale endpoint data on the SMGR SIP Registration page.	8.0.1.0
ASM-80636	Have the user registrations page up and leave it up in System Manager.	Registration details will indicated no registration even for devices that are actively registered.	7.1.3.3
ASM-79738	Branch Session Manager with links to the main Communication Manager.	When links to the main Communication Manager are updated or removed on the Branch Session Manager, the changes do not get translated to the links to LSP.	7.1.3.2
ASM-81488	SIP request arrives at Session Manager with Max-Forwards set to 6.	SIP request receives 500 response rather than 483 response.	7.1.3.0

ASM-81264	Alarm conditions met	Alarms with Event IDs that start with “OP_C” are not raised.	8.1.2.0
ASM-80115	An adaptation is configured on the Session Manager to adapt the Refer-To header.	The adaptation fails to take place because the authoritative domains list is not properly updated in memory after the initial load completes.	8.1.2.0
ASM-79973	From System Manager, add an adaptation for a trunk gateway to a Branch Session Manager.	This and future replication events fail to all Branch Session Mangers.	8.1.2.0
ASM-78383	Out-of-dialog REFER gets NOTIFY before 202 response.	Session Manager memory leak	8.0.1.2
ASM-80432	An egress adaptation is configured to remove specific headers in requests sent to a destination SIP entity. The requests must be routed through a second Session Manger in order to reach the destination entity.	The headers are removed when adaptation is applied on the first Session Manager, but the second Session Manager in the route-thru scenario adds these headers back and does not remove them.	8.0.1.2
ASM-79378	[RHSA-2020:0196] Important: java	N/A	8.1.2.1
ASM-79379	[RHSA-2020:0227] Important: sqlite	N/A	8.1.2.1
ASM-79376	[RHSA-2020:0374] Important: kernel	N/A	8.1.2.1
ASM-79605	[RHSA-2020:0540] Important: sudo security update	N/A	8.1.2.1
ASM-80056	[RHSA-2020:0834] Important: kernel	N/A	8.1.2.1
ASM-80051	[RHSA-2020:0897] Important: icu security update	N/A	8.1.2.1
ASM-80096	[RHSA-2020:1000] Moderate: rsyslog security, bug fix, and enhancement update	N/A	8.1.2.1
ASM-80089	[RHSA-2020:1011] Moderate: expat security update	N/A	8.1.2.1
ASM-80090	[RHSA-2020:1016] Moderate: kernel security, bug fix, and enhancement update	N/A	8.1.2.1
ASM-80087	[RHSA-2020:1020] Low: curl security and bug fix update	N/A	8.1.2.1
ASM-80084	[RHSA-2020:1021] Moderate: GNOME security, bug fix, and enhancement update	N/A	8.1.2.1
ASM-80102	[RHSA-2020:1022] Low: file	N/A	8.1.2.1
ASM-80097	[RHSA-2020:1047] Moderate: wireshark	N/A	8.1.2.1
ASM-80103	[RHSA-2020:1050] Moderate: cups	N/A	8.1.2.1
ASM-80105	[RHSA-2020:1061] Moderate: bind	N/A	8.1.2.1
ASM-80085	[RHSA-2020:1100] Moderate: mariadb security and bug fix update	N/A	8.1.2.1
ASM-80106	[RHSA-2020:1113] Moderate: bash	N/A	8.1.2.1

ASM-80088	[RHSA-2020:1131] Moderate: python security update	N/A	8.1.2.1
ASM-80099	[RHSA-2020:1135] Low: polkit	N/A	8.1.2.1
ASM-80101	[RHSA-2020:1138] Low: gettext	N/A	8.1.2.1
ASM-80107	[RHSA-2020:1176] Low: avahi	N/A	8.1.2.1
ASM-80098	[RHSA-2020:1181] Low: unzip	N/A	8.1.2.1
ASM-80100	[RHSA-2020:1190] Moderate: libxml2	N/A	8.1.2.1
ASM-80500	[RHSA-2020:1512] Important: java-1.8.0-openjdk security update	N/A	8.1.2.1
ASM-80641	[RHSA-2020:2082] Important: kernel	N/A	8.1.2.1
ASM-80975	[RHSA-2020:2344] Important: bind security update	N/A	8.1.2.1
ASM-81087	[RHSA-2020:2432] Moderate: microcode_ctl security, bug fix and enhancement update	N/A	8.1.2.1
ASM-81317	[RHSA-2020:2663] Moderate: ntp security update	N/A	8.1.2.1
ASM-81318	[RHSA-2020:2664] Important: kernel	N/A	8.1.2.1
ASM-81503	[RHSA-2020:2894] Important: dbus security update	N/A	8.1.2.1
ASM-81557	[RHSA-2020:2968] Important: java-1.8.0-openjdk security update	N/A	8.1.2.1
ASM-81862	[RHSA-2020:3217] Moderate: grub2 security and bug fix update	N/A	8.1.2.1
ASM-81868	[RHSA-2020:3220] Important: kernel security and bug fix update	N/A	8.1.2.1

Fixes in Session Manager Release 8.1.2.1

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-79820	Use of Avaya Device Adapter	Language setting administered via endpoint template is not received by endpoints.	8.1.2.0
ASM-78383	Use of SIP Out of dialogue Refer message, followed by SIP messages in reverse order	Out of memory condition due to memory leak	8.1.0.0
ASM-80490	Add user with customized values in the profile settings tab of the endpoint editor	Customized values not received by endpoint.	8.1.2.0
ASM-80502	Remote users with voice monitoring (VMON)	VMON server address is not provide to remote endpoint	7.1.3.0
ASM-80605	N/A	Some alarms including test alarms not being sent to configured serviceability agents	8.1.2.0
ASM-80056	[RHSA-2020:0834] Important: kernel	N/A	8.1.2.0
ASM-80101	[RHSA-2020:1138] Low: gettext	N/A	8.1.2.0
ASM-80100	[RHSA-2020:1190] Moderate: libxml2	N/A	8.1.2.0
ASM-80103	[RHSA-2020:1050] Moderate: cups	N/A	8.1.2.0
ASM-80107	[RHSA-2020:1176] Low: avahi	N/A	8.1.2.0
ASM-80102	[RHSA-2020:1022] Low: file	N/A	8.1.2.0
ASM-80098	[RHSA-2020:1181] Low: unzip	N/A	8.1.2.0
ASM-80105	[RHSA-2020:1061] Moderate: bind	N/A	8.1.2.0
ASM-80097	[RHSA-2020:1047] Moderate: wireshark	N/A	8.1.2.0
ASM-80099	[RHSA-2020:1135] Low: polkit	N/A	8.1.2.0
ASM-80106	[RHSA-2020:1113] Moderate: bash	N/A	8.1.2.0
ASM-80641	[RHSA-2020:2082] Important: kernel	N/A	8.1.2.0
ASM-80088	[RHSA-2020:1131] Moderate: python security update	N/A	8.1.2.0
ASM-80089	[RHSA-2020:1011] Moderate: expat security update	N/A	8.1.2.0
ASM-80051	[RHSA-2020:0897] Important: icu security update	N/A	8.1.2.0
ASM-79605	[RHSA-2020:0540] Important: sudo security update	N/A	8.1.2.0
ASM-80500	[RHSA-2020:1512] Important: java-1.8.0-openjdk security update	N/A	8.1.2.0
ASM-80096	[RHSA-2020:1000] Moderate: rsyslog security, bug fix, and enhancement update	N/A	8.1.2.0
ASM-80090	[RHSA-2020:1016] Moderate: kernel security, bug fix, and enhancement update	N/A	8.1.2.0

ASM-80085	[RHSA-2020:1100] Moderate: mariadb security and bug fix update	N/A	8.1.2.0
ASM-80087	[RHSA-2020:1020] Low: curl security and bug fix update	N/A	8.1.2.0
ASM-80084	[RHSA-2020:1021] Moderate: GNOME security, bug fix, and enhancement update	N/A	8.1.2.0

Fixes in Session Manager Release 8.1.2

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-77359	Incorrect UCID format received from SIP entity	CDR records may be missing information or in certain cases, calls may fail.	7.1.3.1
ASM-77121	Use of RTCP server	Session Manager doesn't send RTCP details configured under "device settings group – Voip monitoring manager" to SIP endpoints	8.1.1.0
ASM-77363	Session Manager Communication Profile editing	On the Session Manager Communication Profile editor page, the list of SMs does not show up after clicking on the Primary Session Manager drop-down list.	8.1.1.0
ASM-77666	Regular on demand execution of maintenance tests on the Session Manager -> System Tools -> Maintenance Tests GUI	System Manager memory use increases and becomes sluggish over a large period of time, typically a couple of months.	7.1.3.4
ASM-78115	When administering Entity Links on the Routing -> SIP Entity GUI the user adds more than 5 Entity Links or adds Entity Links while the table is being filtered	Error message on Commit for values do match Entity Link values entered on form. Error message for what appear to be valid values.	8.1.0.0
ASM-77121	The administrator adds a new device group with an RTCP server address.	Any endpoint that receives device parameters from that new device group does not see the RTCP server address.	7.1.3.3
ASM-78308	Ingress adaptation for the destination address has been administered for the entity and request contains an SM IP address in the host field of the request-URI. The "adaptForeignURI" parameter is not set to true for the adaptation.	Ingress adaptation of the request-URI fails to take place. The request/call may fail or be routed incorrectly.	8.1.1.0

ASM-73880	Network misconfiguration	Jgroups message queue backs up trying to send messages. System runs out of memory and gets restarted causing a service outage.	8.0.0.0
ASM-78544	SMnetSetup must be used to add a network domain to a Session Manager that previously did not have a network domain administered.	Alarms are not generated by Session Manager.	8.1.0.0
ASM-78037	A call routed by Session Manager is unanswered for 3 hours.	Session Manager drops the unanswered call after three hours.	7.1.3.1
ASM-79376	[RHSA-2020:0374] Important: kernel	N/A	8.1.1.0
ASM-79378	[RHSA-2020:0196] Important: java	N/A	8.1.1.0
ASM-79379	[RHSA-2020:0227] Important: sqlite	N/A	8.1.1.0
ASM-77861	[RHSA-2019:3834] Important: kernel security update	N/A	8.1.1.0
ASM-77693	[RHSA-2019:3128] Important: java-1.8.0-openjdk security update	N/A	8.1.1.0
ASM-77688	[RHSA-2019:3197] Important: sudo security update	N/A	8.1.1.0
ASM-77872	[RHSA-2019:3872] Important: kernel security update	N/A	8.1.1.0
ASM-77352	[RHSA-2019:2829] Important: kernel security update	N/A	8.1.1.0
ASM-77396	[RHSA-2019:2964] Important: patch security update	N/A	8.1.1.0
ASM-78323	[RHSA-2019:3979] Important: kernel security and bug fix update	N/A	8.1.1.0
ASM-77593	[RHSA-2019:3055] Important: kernel security and bug fix update	N/A	8.1.1.0
ASM-76434	[RHBA-2019:1703] tzdata enhancement update	N/A	8.1.1.0
ASM-78322	[RHSA-2019:4190] Important: nss, nss-softokn, nss-util security update	N/A	8.1.1.0

Fixes in Session Manager Release 8.1.1

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-76174	Mutual authentication set as “optional” and the occurrence of certificate errors on TLS links.	Spontaneous TLS connection failures	8.0.0.0
ASM-75853	A large number of Session Manager instances	When assigning a user to a Session Manager, typeahead function failed to filter the list of possible Session Managers	8.0.0.0
ASM-76599	Session Manager deployed on AWS	SMnetSetup commands may fail	8.1.0.0
ASM-76601	Insufficient bandwidth for voice media	The alarm was not reported to System Manager	8.0.0.0
ASM-75825	High alarming rates	Alarm failures and Serviceability Agent stops responding	7.1.3.0
ASM-75851	A large amount of log files and CDR files.	High CPU usage and multiple instances of the process log_file_permissions.sh.	7.1.3.2
ASM-74370	SIP Device registered, which is non-AST and dual registered. An ELIN server configured for primary and secondary SMs.	Neither ELIN nor ELIN Last Updated fields in the User Registration Status Detail are displayed	7.1.3.0
ASM-75856	Use of maximum Session Manager profile 6 on the AWS platform	Installation fails.	8.1.0.0
ASM-75873	Installing Software Only offer to Branch Session Manager using SDM	Installation fails.	8.1.0.0
ASM-75805	Upgrading Session Manager from 6.3.x to SM 8.1 while offline call logs are in use.	Call logs are not restored after the upgrade. End-users may see call logs missing from the phone after logout/login.	8.1.0.0
ASM-75818	[RHSA-2019:1168] (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout) kernel	N/A	8.1.0.0
ASM-75817	[RHSA-2019:1228] wget	N/A	8.1.0.0
ASM-76126	[RHSA-2019:1294] Important: bind security update	N/A	8.1.0.0
ASM-76150	[RHSA-2019:1481] Important: kernel security update	N/A	8.1.0.0
ASM-76225	[RHSA-2019:1587] python	N/A	8.1.0.0
ASM-76337	[RHSA-2019:1619] Important: vim security update	N/A	8.1.0.0
ASM-76606	[RHSA-2019:1815] java-1.8.0-openjdk	N/A	8.1.0.0
ASM-76920	[RHSA-2019:1873] Important: kernel	N/A	8.1.0.0
ASM-76795	[RHSA-2019:1880] Low: curl security and bug fix update	N/A	8.1.0.0
ASM-76598	[RHSA-2019:1884] Moderate: libssh2 security update	N/A	8.1.0.0
ASM-76921	[RHSA-2019:2029] Important: kernel	N/A	8.1.0.0
ASM-76934	[RHSA-2019:2030] Moderate: python	N/A	8.1.0.0

ASM-76922	[RHSA-2019:2033] Low: patch	N/A	8.1.0.0
ASM-76740	[RHSA-2019:2046] Moderate: polkit security and bug fix update	N/A	8.1.0.0
ASM-76923	[RHSA-2019:2047] Moderate: libcgroup	N/A	8.1.0.0
ASM-76735	[RHSA-2019:2049] Moderate: libmspack security update	N/A	8.1.0.0
ASM-76924	[RHSA-2019:2052] Moderate: libjpeg	N/A	8.1.0.0
ASM-76925	[RHSA-2019:2057] Moderate: bind	N/A	8.1.0.0
ASM-76926	[RHSA-2019:2060] Moderate: dhclient	N/A	8.1.0.0
ASM-76927	[RHSA-2019:2091] Moderate: systemd	N/A	8.1.0.0
ASM-76928	[RHSA-2019:2110] Moderate: rsyslog	N/A	8.1.0.0
ASM-76929	[RHSA-2019:2118] Moderate: glibc	N/A	8.1.0.0
ASM-76885	[RHSA-2019:2136] Moderate: libssh2 security, bug fix, and enhancement update	N/A	8.1.0.0
ASM-76930	[RHSA-2019:2143] Low: openssh	N/A	8.1.0.0
ASM-76931	[RHSA-2019:2159] Low: unzip	N/A	8.1.0.0
ASM-76741	[RHSA-2019:2169] Important: linux-firmware security, bug fix, and enhancement update	N/A	8.1.0.0
ASM-76886	[RHSA-2019:2181] Low: curl security and bug fix update	N/A	8.1.0.0
ASM-76737	[RHSA-2019:2189] Moderate: procps-ng security and bug fix update	N/A	8.1.0.0
ASM-76739	[RHSA-2019:2197] Low: elfutils security, bug fix, and enhancement update	N/A	8.1.0.0
ASM-76932	[RHSA-2019:2237] Moderate: nspr	N/A	8.1.0.0
ASM-76933	[RHSA-2019:2304] Moderate: openssl	N/A	8.1.0.0
ASM-76738	[RHSA-2019:2327] Moderate: mariadb security and bug fix update	N/A	8.1.0.0
ASM-77124	[RHSA-2019:2600] Important: kernel security and bug fix update	N/A	8.1.0.0
ASM-77352	[RHSA-2019:2829] Important: kernel security update	N/A	8.1.0.0
ASM-76915	[RHSA-2019-2075] Moderate: binutils security and bug fix update	N/A	8.1.0.0
ASM-76914	[RHSA-2019-2077] Low: ntp security, bug fix, and enhancement update	N/A	8.1.0.0

Fixes in Session Manager Release 8.1

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-70682	Malformed SIP messages from 3rd-party SIP equipment	Elevated CPU utilization on Session Manager	7.1.2
ASM-72091	TLS with Mutual Authentication enabled.	CA certificates with neither SAN nor CN are invalidated when mutual authentication is enabled, and thus such TLS connections won't be allowed.	7.1.3
ASM-73971	E129 phone registered to SM.	Incoming call to E129 phone may appear simultaneously on two-line appearances and cannot be answered.	7.1.3
ASM-69956	Create a sub role and then "Copy All From...." of "All elements..." will then provide all the distinct roles permissions to modify	Distinct role access permissions don’t appear for a custom role created based on the Session Manager and Routing role.	7.1.0
ASM-72789	Java Security Update (RHSA-2018:2942)	N/A	8.0.1
ASM-72398	[RHSA-2018:2768-01] Moderate: nss security update	N/A	8.0.1
ASM-74160	[RHSA-2019:0109] Perl Security Update	N/A	8.0.1
ASM-71635	[RHSA-2018:2570-01] Important: bind security update	N/A	8.0.1
ASM-74078	[RHSA-2019:0049] Important: systemd update	N/A	8.0.1
ASM-75288	[RHSA-2019:0679-01] Important: libssh2 security update	N/A	8.0.1
ASM-75310	[RHSA-2019:0710] Important python security update	N/A	8.0.1
ASM-75386	[RHSA-2019:0775] Important: java security update	N/A	8.0.1
ASM-73669	[RHSA-2018:3651-01] Low: kernel security and bug fix update	N/A	8.0.1
ASM-72360	[RHSA-2018:2748-01] Important: kernel security and bug fix update	N/A	8.0.1
ASM-74970	[RHSA-2019:0483-01] Moderate: openssl security and bug fix update	N/A	8.0.1
ASM-74971	[RHSA-2019:0512-01] Important: kernel security, bug fix, and enhancement update	N/A	8.0.1
ASM-75626	[RHSA-2019:0818-01] Important: kernel security and bug fix update	N/A	8.0.1

Known issues and workarounds in Session Manager 8.1.x.x

Known issues and workarounds in Session Manager Release 8.1.3.1

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Minimum conditions	Visible symptoms	Workaround
ASM-82331	Upgrade of Session Manager to 8.1.3 when Cassandra schema change is involved.	30 minutes or longer after upgrading, User Data Storage status on dashboard shows failed status.	Reboot the newly upgraded SM.
ASM-82448	Regular-expression adaptation global setting changes from disabled to enabled	Existing adaptations are no longer applied to SIP messages	Restart the Session Managers involved in adaptation
ASM-83611	FIPS mode operation	Cassandra DB not in FIPS compliance until all Session Managers are updated to 8.1.3.1.	None
ASM-84074	Session manager 8.0.0.0 upgrade to 8.1.3.1	Cassandra DB will be unavailable until all Session Managers are updated to 8.1.3.1.	Upgrades from any release later than 8.0.0.0 will not experience the issue

Known issues and workarounds in Session Manager Release 8.1.3

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Minimum conditions	Visible symptoms	Workaround
ASM-82331	Upgrade of Session Manager to 8.1.3 when Cassandra schema change is involved.	30 minutes or longer after upgrading, User Data Storage status on dashboard shows failed status.	Reboot the newly upgraded SM.
ASM-82448	Regular-expression adaptation global setting changes from disabled to enabled	Existing adaptations are no longer applied to SIP messages	Restart the Session Managers involved in adaptation

Known issues and workarounds in Session Manager Release 8.1.2.1

The following table lists the known issues, symptoms, and workarounds in this release

ID	Minimum conditions	Visible symptoms	Workaround
None			

Known issues and workarounds in Session Manager Release 8.1.2

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Minimum conditions	Visible symptoms	Workaround
None			

Known issues and workarounds in Session Manager Release 8.1.1

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Minimum conditions	Visible symptoms	Workaround
ASM-77121	Use of RTCP server	Session Manager doesn’t send RTCP details configured under “device settings group – Voip monitoring manager” to SIP endpoints	Edit the device settings group information and commit a 2nd time
ASM-77363	Session Manager Communication Profile editing	On the Session Manager Communication Profile editor page, the list of SMs does not show up after clicking on the Primary Session Manager drop-down list.	Install System Manager Hotfix described in PSN005280u.

Known issues and workarounds in Session Manager Release 8.1

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Minimum conditions	Visible symptoms	Workaround
ASM-75856	Use of maximum Session Manager profile 6 on the AWS platform	Installation fails.	None. Fix in 8.1.1.
ASM-75873	Installing Software Only offer to Branch Session Manager using SDM	Installation fails.	Install using manual methods instead of SDM
ASM-75805	Upgrading Session Manager from 6.3.x to SM 8.1 while offline call logs are in use.	Call logs are not restored after an upgrade. End-users may see call logs missing from the phone after logout/login.	None

Avaya Aura® System Manager

What's new in System Manager Release 8.1.3.x

For more information see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

As of 8.1.3, customers utilizing AVP or VMware based systems are able to activate disk encryption during OVA installation. To support ongoing maintenance of this feature, the following commands have been added in the 8.1.3 release: ***encryptionStatus, encryptionRemoteKey, encryptionPassphrase,*** and ***encryptionLocalKey***. Note that these commands are only applicable if disk encryption is enabled using the Avaya OVA methods. These commands are not to be used if the customer has provided their own disk encryption using other methods.

Security Service Pack

Beginning with 8.1, System Manager is releasing an 8.1 Security Service Pack (SSP). This SSP can be applied to any version of 8.1 and only includes Red Hat security updates.

Installing System Manager Security Service Pack through Solution Deployment Manager (SDM) is not supported.

This patch does not apply to System Manager 8.1.x Software Only deployments. This patch should NOT be installed on System Manager 8.1.x Software Only deployments.

Beginning December 2020, SSPs will also be released on a more frequent cadence. This means that SSPs may also be available between application Service Packs/Feature Packs. SSP required artifacts and fix IDs will no longer be tracked in the Release Notes. For further information on contents and installation procedures, please see PCN2105S for more details.

Required artifacts for System Manager Release 8.1.3.x

Required artifacts for System Manager Release 8.1.3.1

The following section provides the System Manager downloading information. For deployment and upgrade procedure, see product-specific deployment and upgrade documents on the Avaya Support website.

Filename	PLDS ID	File size (KB)	File size (MB)	Comments
System_Manager_8.1.3.1_r813112244.bin	SMGR8131GA1	System Manager 8.1.3.1 Release	1,919 MB	eb87510926aca10a45b8d1f27c453e96
Avaya_SDMClient_win64_8.1.3.1.0035973_5.zip	SMGR8131GA2	SDM Client for System Manager 8.1.3.1	224 MB	0c289f4afe3a03ddb28cb7eac95bc805

Required artifacts for System Manager Release 8.1.3

The following section provides the System Manager downloading information. For deployment and upgrade procedure, see product-specific deployment and upgrade documents on the Avaya Support website.

Filename	PLDS ID	File size (KB)	File size (MB)	Comments
System_Manager_8.1.3.0_r813011784.bin	SMGR8130GA1	System Manager 8.1.3.0 Release	1888	46d8ea500a2ad0a1ed5e89aced444911
Avaya_SDMClient_win64_8.1.3.0.1035538_49.zip	SMGR8130GA2	SDM Client for System Manager 8.1.3.0	224	4d954e52385ebe82bdcae78bb3539e79
System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin	SMGR81SSP06	Avaya Aura® System Manager 8.1 SSP 5	376	f54d7522e70825b4e2983555d36b6031

Required artifacts for System Manager Release 8.1.2

The following section provides the System Manager downloading information. For deployment and upgrade procedure, see product-specific deployment and upgrade documents on the Avaya Support website.

Filename	PLDS ID	File size (KB)	File size (MB)	Comments
System_Manager_8.1.2.0_r812011097.bin	SMGR8120GA1	1640998	1603	System Manager 8.1.2.0 Release Md5sum: ed113f3a3f8a16534cb6de03152ed6a5
Avaya_SDMClient_win64_8.1.2.0.0734476_28.zip	SMGR8120GA2	228897	224	SDM Client for System Manager 8.1.2.0 Md5sum: 1d70feebde9f74a791820c0ab3663b00
WebLM_8.1.2.0_r81211102.bin	SMGR8120GA3	358001	350	e31442c909018bf7a5987325c370555a
System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin	SMGR81SSP03	338605	331	d01cb2b0af3d79d8e51aede2c93097f0
SMGR-8.1.0.0.733078-e67-34E.ova	SMGR8120GA5	4053170	3958	73c5dcb09099b0757b3a6347b609ed82
SMGR-PROFILE3-8.1.0.0.733078-e67-34E.ova	SMGR8120GA6	4045450	3951	cfecc55234f69a24f1005f6dfbb1709d
SMGR-PROFILE4-8.1.0.0.733078-e67-34E.ova	SMGR8120GA7	4051540	3957	4add3148a732290cceaa519e651f3d82

Required artifacts for System Manager Release 8.1.1

The following section provides the System Manager downloading information. For deployment and upgrade procedure, see product-specific deployment and upgrade documents on the Avaya Support website.

Filename	PLDS ID	File size (MB)	Comments
System_Manager_8.1.1.0_r811010503.bin	SMGR8110GA1	1222	System Manager 8.1.1.0 Release Md5sum: 9ff9dd881da5eb76839d7ec842ce305a
Avaya_SDMClient_win64_8.1.1.0.0333784_28.zip	SMGR8110GA2	223	SDM Client for System Manager 8.1.1.0 Md5sum: 51e79c96aa976ac622007ede28468b82
System_Manager_R8.1.1.0_HotFix1_r811010504.bin	SMGR8110GA4	143	5520625756b95a84f8dbad16749a688e
System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin	SMGR81SSP02	330	ce5a8c6eb39b1b02787bbbe416b6ffdb

Required artifacts for System Manager Release 8.1

The following section provides the System Manager downloading information. For deployment and upgrade procedure, see product-specific deployment and upgrade documents on the Avaya Support website.

Filename	PLDS ID	File size (MB)	Comments
SMGR-8.1.0.0.733078-e65-47.ova	SMGR81GA001	3906	Avaya Aura System Manager 8.1 OVA MD5 Checksum: 967c52f8290c0d06912ebeaf237aea97
SMGR-PROFILE3-8.1.0.0.733078-e65-47.ova	SMGR81GA002	3894	Avaya Aura System Manager 8.1 High Capacity (Profile 3) OVA MD5 Checksum: 3ce82c75c2e69a7005e2f6384a6b1036
SMGR-PROFILE4-8.1.0.0.733078-e65-47.ova	SMGR81GA003	3893	Avaya Aura System Manager 8.1 High Capacity (Profile 4) OVA MD5 Checksum: e42dfb0cd5bb4f502451f10a67440215
SMGR-8.1.0.0.733078-AWS-47.ova	SMGR81GA004	3906	Avaya Aura System Manager 8.1 AWS OVA MD5 Checksum: 91ffa8d10bdd71a93d083729fa7323fd
SMGR-PROFILE3-8.1.0.0.733078-AWS-47.ova	SMGR81GA005	3901	Avaya Aura System Manager 8.1 AWS Profile-3 (High Capacity) OVA MD5 Checksum: a283fb55cbd05f444b28a7f7048d874a
SMGR-PROFILE4-8.1.0.0.733078-AWS-47.ova	SMGR81GA006	3905	Avaya Aura System Manager 8.1 AWS Profile-4 (High Capacity) OVA MD5 Checksum: 9f6452f0b539d055ad5c4bfd3cf16079
SMGR-8.1.0.0.733078-KVM-47.ova	SMGR81GA007	6633	System Manager 8.1 KVM OVA MD5 Checksum: a8edaccc1325c816e23f325774522354
SMGR-PROFILE3-8.1.0.0.733078-KVM-47.ova	SMGR81GA008	6636	System Manager 8.1 KVM Profile-3 (High Capacity) OVA MD5 Checksum: 0f8ca8c8c339c9fa9ba29dc859738829
SMGR-PROFILE4-8.1.0.0.733078-KVM-47.ova	SMGR81GA009	12870	System Manager 8.1 KVM Profile-4 (High Capacity) OVA MD5 Checksum: d8f901dc7233986542a44bac75f3f46e
AvayaAuraSystemManager-8.1.0.0.733078_v47.iso	SMGR81GA010	3474	Avaya Aura System Manager 8.1 Software Only MD5 Checksum: fa1a15d64ad8792ff97f5e7108e012df
Avaya_SDMClient_win64_8.1.0.0.0733229_26.zip	SMGR81GA012	223	SDM Client for System Manager 8.1 MD5 Checksum: 2a99383a6e1a218f59b4bc57c1e50823
System_Manager_R8.1_Patch_r810009814.bin	SMGR81GA013	984	System Manager 8.1 GA Mandatory Patch bin file Post OVA deployment / Data Migration

Filename	PLDS ID	File size (MB)	Comments
			MD5 Checksum: 6f4e1eedf1a02ea70bb5973896da7ac1

Required patches for System Manager Release 8.1.x

For information about patches and product updates, see the Avaya Technical Support Web site https://support.avaya.com.

Download Data Migration Utility

This section gives the download information. For deployment and upgrade procedure, see product-specific deployment and upgrade documents on the Avaya Support website.

Note: The data migration utility is required only if you are upgrading from System Manager 6.0.x, 6.1.x, 6.2.x, 6.3.x, 7.0.x, 7.1.x and 8.0.x. Ensure that you run the data migration utility only on 8.1 release. For more information, see the Upgrading Avaya Aura® System Manager to Release 8.1.x document.

Filename	PLDS ID	File size (MB)	Comments
datamigration-8.1.0.0.7-36.bin	SMGR8120DM1	16	Data Migration utility for System Manager 8.1.3 MD5 Checksum: 472286df32d77050d2a56861e459cf37

Must read:

1. For Release 8.1 GA Installation:
   - Fresh: Deploy 8.1 GA OVA + Apply 8.1 GA Patch bin.
   - Upgrade: Deploy 8.1 GA OVA + 8.1 Data Migration Bin + 8.1 GA Patch bin.

2. To verify that the System Manager installation is ready for patch deployment, do one of the following:
   - On the web browser, type https://<Fully Qualified Domain Name>/SMGR and ensure that the system displays the System Manager login webpage.
     The system displays the message: Installation of the latest System Manager Patch is mandatory.
   - On the Command Line Interface, log on to the System Manager console, and verify that the system does 'not' display the message:
     `Maintenance: SMGR Post installation configuration is In-Progress.`

     It should only display the message: `Installation of latest System Manager Patch is mandatory.`

3. Perform the following steps to enable EASG on System Manager 8.1:
   - To enable EASG on System Manager via Command Line Interface via Cust user type the following command:
     `# EASGManage --enableEASG`
   - To disable the EASG on System Manager type the following command:
     `# EASGManage –disableEASG`

4. For VMware to VE System Manager Upgrade, remove all the snapshots from old VMware System Manager; otherwise, rollback operation will fail.

5. The versions*.xml is published on PLDS. To download the latest versions.xml file for SUM, search on PLDS using Download PUB ID “SMGRSUM0001” only. Do not use version or product on PLDS in the search criteria.
6. System Manager Login banner no longer supports HTML characters.
7. Breeze Element Manager in System Manager 8.1 is called Breeze 3.7.
8. System Manager no longer supports Profile 1 from Release 8 onwards. If you are upgrading from Profile 1 in Releases 6 or 7, you will have to select Profile 2 or higher while installing R8.x. Note that Profile 2 will require more VM resources compared to Profile 1.
9. If you need to configure IP Office branches beyond 2000 with a single System Manager, please contact Lisa Marinelli, lmarinelli@avaya.com before the design or deployment.

Software information:

Software	Version	Note
Database	Postgres 9.6.17	Used as a System Manager database. For more information, see: https://www.postgresql.org/docs/9.6/static/index.html
OS	RHEL 7.6 64 bit	Used as the operating system for the System Manager OVA. It is required in the case of Software Only deployment.
Open JDK	1.8 update 262 64 bit	For Solution Deployment Manager Client, Open JDK 1.8.0-java-1.8.0-openjdk-1.8.0.192 Not specific to 8.1.2, but OpenJDK will be updated to version 1.8 update 262 as part of SSP 8.1 Patch 5 installation.
Application Server	WildFly AS 10.1.0 Final	
Supported Browsers	Internet Explorer 11.x	Earlier versions of Internet Explorer are no longer supported.
	Firefox 65 and above	Earlier versions of Firefox are no longer supported.
VMware vCenter Server, ESXi Host, VMware Web Client	6.0,6.5,6.7,7.0	Earlier versions of VMware are no longer supported.
SDM Client Application Server	Tomcat 8.5.39	
SDM Client Supported OS	Windows 7, 8, 10 Windows Server 2016	

Adobe Flash EOL impact:

Starting System Manager release 7.1.1 Adobe Flash is not used in System Manager UI so there is no impact of Adobe Flash going End of Life.

How to find a License Activation Code (LAC) in PLDS for a product.

- Log in to the PLDS at https://plds.avaya.com.
- From the Assets menu, select View Entitlements.

- In the Application field, select System Manager.
- Do one of the following:
  - To search using group ID, in the Group ID field, enter the appropriate group ID.
    Note: All group IDs are numeric without any leading zeros.
  - To search using the SAP order number, click Advanced Search, and in the Sales/Contract # field, enter the SAP order number.
- Click Search Entitlements.
  The system displays the LAC(s) in the search results.

Installation for System Manager Release 8.1.x

Backing up the software

Refer to the System Manager Backup and Restore section of the Administering Avaya Aura® System Manager guide.

Installing the System Manager software

For detailed information about installing System Manager, see Avaya Aura® System Manager deployment documents on the Avaya Support website.

Upgrading the System Manager software

For detailed information about upgrading your System Manager, see Upgrading Avaya Aura® System Manager on the Avaya Support website.

System Manager upgrade path

Note: When a Service Pack on the “N-1” GA release is introduced AFTER a Feature Pack on the current GA release “N”, there will not be feature parity between the two and only tested upgrade paths are supported.

The following upgrade paths from 7.1.3.x to 8.x are currently supported.

System Manager running this version	Can upgrade to this version
7.1.3.0	8.1.x
7.1.3.1	8.1.x
7.1.3.2	8.1.x
7.1.3.3	8.1.x
7.1.3.4	8.1.x
7.1.3.5	8.1.2, 8.1.3
7.1.3.6 (feature parity will not match with 8.1.2) Reference PSN020490u – Avaya Aura® System Manager 8.1.2.x Upgrade Restrictions	8.1.2, 8.1.3
7.1.3.7	8.1.3

Troubleshooting the installation

Execute the following command from System Manager Command Line Interface with customer user credentials to collect logs and contact the Avaya Support team.

```
#collectLogs -Db-Cnd
```

This will create a file (LogsBackup_xx_xx_xx_xxxxxx.tar.gz) at /swlibrary location.

Speculative Execution Vulnerabilities (includes Meltdown and Spectre and also L1TF Vulnerabilities)

In order to help mitigate the Speculative Execution Vulnerabilities, the processor manufacturers and operating system developers provide software patches to their products. These are patches to the processors, hypervisors, and operating systems that the Avaya solutions utilize (they are not patches applied to the Avaya developed components of the solutions).

Once these patches are received by Avaya, they are tested with the applicable Avaya solutions to characterize any impact on the performance of the Avaya solutions. The objective of the testing is to reaffirm product/solution functionality and to observe the performance of the Avaya solutions in conjunction with the patches using typical operating parameters.

Avaya is reliant on our suppliers to validate the effectiveness of their respective Speculative Execution Vulnerability patches.

The customer should be aware that implementing these patches may result in performance degradation and that results may vary to some degree for each deployment. The customer is responsible for implementing the patches, and for the results obtained from such patches.

For more information about Speculative Execution Vulnerabilities fixes included in Avaya Aura® Release 8.x, see the following PSNs on the Avaya Support Site:

- PSN020346u - Avaya Aura® Meltdown and Spectre vulnerabilities
- PSN020369u - Avaya Aura® L1TF vulnerabilities

Fixes in System Manager 8.1.3.x

Fixes in System Manager 8.1.3.1

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible Symptoms
SMGR-58095	User Interface	Welcome alert popup not shown properly in Dashboard page.
SMGR-58250	User Interface	Shows the last login information in the Notification widget instead of a pop-up.
SMGR-57977	User Interface	After Upgrade from 7.0.x to 8.0.x external authentication and Policy links stop working
SMGR-58101	User Interface	SMGR dashboard redirects to old SMGR home pages present in 7.1 release instead 8.1 pages if user has Tenant Administrator Template and system has Tenant Management not enabled.
SMGR-57995	Fault Management	Unable to generate test alarms from the System Manager 8.1.x due to spiritAgent keeps loosing connection with snmpd.
SMGR-58493	Fault Management	Security Scan detected the TCP Ports 4xxxx opend by java process (spiritAgent).

SMGR-57988	User Management	Duplicate a user and after filling out the required information and then Commit, admin received error popup “Error on Commit. Communication Profile: CM endpoint Profile contains error,
SMGR-58386	User Management	Preferred handle doesn't get updated if user has two sip handles and admin tries to update it with second one.
SMGR-57775	User Management	Display information of user text gets overflowed on the search box in Manage Users.
SMGR-58216	User Management	Error when using "Use Existing Endpoints" option with selecting custom template and "Override Endpoint Name and Localized Name" is disabled.
SMGR-57767	User Management	Same CM extension can be assigned to multiple users through AD sync.
SMGR-57957	User Management	Getting Error GenericJDBCException in OfficelinxBulkImportDBUtils - While Export All Users.
SMGR-57763	User Management	Export All Users does not complete 100%.
SMGR-57928	User Management	Latin transcription of "First Name" and "Last Name" in the Identity Tab of User in SMGR are not happening properly for Russian name with the Cyrillic alphabet.
SMGR-56637	User Management	System Manager integrated with AD, phone numbers attributes values can be change but unable to remove.
SMGR-57864	User Management	All user information are blank when view/edit a user.
SMGR-53654	User Management	Non Admin User is able to assign System Admin Roles.
SMGR-54172	User Management	Communication profile password can be seen in plain text in browser development tools.
SMGR-58430	User Management	Issues when adding / removing Associated Contacts to a user.
SMGR-58539	User Management	Custom user with view only permission can edit the user.
SMGR-58464	User Management	Issues on Bulk Edit Feature User Interface in User Management.
SMGR-58977	User Management	Synchronization User Name and Domain Account Name didn't apply to IXM server when changed Login name of AD user on LDAP.
SMGR-58597	Directory Synchronisation	User shows as modified in AD sync summary when UPR name is blanked out on AD server.
SMGR-57954	Report Management	list registration report for station get have one entry for each station
SMGR-57840	Report Management	Unable to save the new report to the remote SFTP server.
SMGR-57780	Communication Manager Management	CSM_Iptcmobject_MAINTENANCE job not clearing "recoded-ann" entries in CM notification table.
SMGR-57777	Communication Manager Management	Adding a ip-network-map on CM, sets all parameters on correlated location form to default.
SMGR-57852	Communication Manager Management	sort by columns does not show correctly results for Set Type columns in Templates Services
SMGR-58186	Communication Manager Management	Display Errors, alarms, events report won’t be generated if we select All CMs in the list
SMGR-58259	Communication Manager Management	When user tries to associate existing H323 station with existing user and enables dual registration, then

		System tries to add incorrect station number to the off-pbx station-mapping form
SMGR-58364	Communication Manager Management	When CM station name is edited with umlaut characters, Notify sync removes umlaut characters from name and removes all buttons from button module along with labels.
SMGR-58360	Communication Manager Management	In Some scenario, editing the endpoint will cause endpoint to be part of coverage path twice and same can viewed in group membership tab.
SMGR-58480	Communication Manager Management	"duplicate agent" command using cut-through OR incremental sync doesn't update agent list on System Manager.
SMGR-58588	Communication Manager Management	Unable to export the hunt group with "First Announcement extension" field set.
SMGR-58255	Communication Manager Management	Importing multiple Service Hours Table into SMGR does not populate Start/End Time for week.
SMGR-58003	Communication Manager Management	Button parameters field doesn't appear while adding OR editing endpoints with few set types.
SMGR-57823	Communication Manager Management	Communication Manager Management pages of showing white pages.
SMGR-58432	Communication Manager Management	Shortcut keys present in UI is not working
SMGR-58301	Data Replication Management	Database partition grow FULL due to un-ending SMGR-Breeze sync caused by none-zero fail_count for symmetric node communication.
SMGR-58305	Data Replication Management	symmetric events not getting cleaned up quickly after bulk changes causing backlog which eventually causes disk full issues.
SMGR-58636	Infrastructure	Contents of significant log files getting cleared.
SMGR-58790	Infrastructure	JBoss service is not starting up in DoD mode after 8.1.3 HF installation.
SMGR-57894	Infrastructure	Secure flag missing in set-cookie
SMGR-58196	Software Deployment Manager	sdm.iso files space is not freed after it was deleted.
SMGR-58272	Software Deployment Manager	While performing Refresh Element operation on Gateway, SDM tries authentication on gateway using csadmin user.
SMGR-57795	License Management	System Manager with centralized CM license file denies licenses to Communication Manager.
SMGR-58643	License Management	License files went missing after activating secondary server.
SMGR-58083	License Management	License usage shows incorrect count for TSAPI feature of AES license
SMGR-49355	Messaging Element Management	Changing fields with Messaging Editor does not take effect on Subscriber profile.

Fixes in System Manager 8.1.3

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible Symptoms
SMGR-57547	User Management	In certain scenarios user update either via Web Console or Active Directory (AD) Sync fails with the error "GLS_RESOURCE_DOES_NOT_EXIST"

SMGR-57277	Officelinx Element Management	Updating a user that has a Officelinx Comm Profile associated with it causes the mailbox values on the Officelinx server to get reset with the default values. Note: you need a corresponding fix on OfficeLinx side as well for the issue to get resolved
SMGR-56966	Infrastructure	Jackson-databind-2.9.6.jar vulnerability (Third party vulnerability)
SMGR-56965	Infrastructure	Commons-fileupload-1.3.1.jar CVE-2016-1000031 vulnerability (Third party vulnerability)
SMGR-56964	Infrastructure	XStream CVE-2013-7285 vulnerability (Third party vulnerability)
SMGR-56859/SMGR-57328	Communication Manager Management	Unable to create a new user using the duplicate user functionality and by selecting a template in the CM comm profile
SMGR-56828	Communication Manager Management	Button Label Not added for any button administered on button no. 24
SMGR-56816	User Management	"Export selected users" exports fewer users than selected
SMGR-56814	Infrastructure	snmpd corruption after installing System Manager 8.1 Security Service Pack 1 causing Alarming to stop working on System Manager.
SMGR-56813	Fault Management	Repair Serviceability Agent cause snmpd.conf to default
SMGR-56796	Fault Management	SMs serviceability agents all in "inactive" state after deploy
SMGR-56789	Security Updates	(RHSA-2020:2894) Important: dbus security update
SMGR-56663	Communication Manager Management	"Allow H.323 and SIP Endpoint Dual Registration" field gets disabled if EC500 state for CM extension is changed
SMGR-56410	User Management	System Manager Active Directory User sync takes longer starting System Manager 8.1.2 Hot Fix #4
SMGR-56394	Communication Manager Management	Download report feature does not download all selected reports, shows inconsistency on different machines
SMGR-56366	Geographic Redundancy	System Monitor and Serviceability Agent processes do not come up automatically after the System Manager Virtual Machine is rebooted
SMGR-56321	User Management	"change station" command is triggered when editing a user even though nothing has changed in the CM Comm profile for the user
SMGR-56318	Communication Manager Management	Unable to search for Breeze Service Profiles using the Global Search option after 8.1.2 Hot Fix installation or after patching the Breeze Element Manager
SMGR-56264	Communication Manager Management	Patch install does not fail in certain cases if there is a failure during the patch execution
SMGR-56213	Communication Manager Management	Report for "List ip-network-map" asks for an inpit qualifier even when one has been provided
SMGR-56212	Role Management	Cannot edit custom roles in certain scenarios
SMGR-56203	Communication Manager Management	A CM Endpoint Template for an older version of CM that has been edited cannot be upgraded to a CM template for a higher version of CM

SMGR-56060	Communication Manager Management	Cannot update coverage point if it has remote coverage point configured
SMGR-55951	Software Upgrade Management	SDM upgraded job runs immediately although user selected schedule later
SMGR-55946	Infrastructure	Incorrect Patching of standalone.xml file while applying 8.1.2 GA Patch
SMGR-55945	User Management	Proper validations for mandatory fields on the User Management page
SMGR-55931	Communication Manager Management	Duplicate user fails if CM Comm Profile contains autodial button with blank DialNumber button and Favorite/button labels
SMGR-55919	Communication Manager Management	Unable to set "Crisis-Alert" or "no-hold-conf" button as favourites for J179 phones
SMGR-55889	Communication Manager Management	"save as template" option doesn't work for specific extensions
SMGR-55861	Communication Manager Management	No errors seen when upgrading a CM Endpoint Template for an older version of CM without providing the new CM version or Template name even though it does not work
SMGR-55857	Communication Manager Management	Endpoints with blank Location field cannot be searched through Advanced search option on Manage endpoint page
SMGR-55831	Import Export Management	User loses its group association when you change the loginname of the user using Bulk Import XML
SMGR-55764	Scheduler Management	Duplicate error messages are shown in the log viewer for failed discovery jobs
SMGR-55706	User Management	User Management page allows addition of private address with same name
SMGR-55705	User Management	Shared address is converted into private address if it is edited
SMGR-55704	Communication Manager Management	User deletion fails because SMGR doesn't run "clear amw" command
SMGR-55608	User Management	Administrative users can change the Communication Profile Password for a user via the Web UI without filling anything in the confirmed password field
SMGR-55593	Communication Manager Management	Destination of Enhanced Call Forward cannot be deleted in Endpoint Editor
SMGR-55591	Communication Manager Management	In certain scenarios User edit does not work if the CM station is edited using the Station Editor in the CM communication Profile section
SMGR-55587	Fault Management	System Manager Security fixes
SMGR-55555	User Management	Multiple issues when adding private contact to a user via the System Manager User Management Page
SMGR-55541	Data Replication Management	DRS replication for a Session Manager node may fail if the SM node is rebooted in the middle of a repair operation
SMGR-55508	Software Upgrade Management	System Manager SDM Pre-Upgrade check screen gets stuck if an existing Job name is used for a new Pre-upgrade job
SMGR-55502	Software Upgrade Management	Support for pre-upgrade patch for upgrading AVPU to 8.1.2.1

SMGR-55480	User Management	User can change last name and first name to blank on the field and save that changes without error/warning message
SMGR-55451	User Management	unable to edit / remove contacts for users from the User Management page
SMGR-55368	Software Upgrade Management	Add pre-upgrade check as part of CM via SDM ensure that the CM hostname does to not contain underscore
SMGR-55349	User Management	When a user with a role is edited from User Management page their password gets set to a default password
SMGR-55193	Communication Manager Management	On the CM sync job schedule page, the Label does not change then changing the repeat type interval from the dropdown
SMGR-55189	User Management	Discrepancy in password field validation between System Manager User Management Bulk Import and Web Service APIs
SMGR-55149	Scheduler Management	Scheduler and Backup/Restore page does not show the correct timezone as per the client browser
SMGR-55143	Communication Manager Management	Blank agent name when tilde is used in "Endpoint Display Name" while configuring user
SMGR-55142	Communication Manager Management	Incremental sync fails after duplicate station command run from CM
SMGR-55120	Communication Manager Management	Group number field of trunk group page is not throwing 'out of range' error the way CM does.
SMGR-55041	Geographic Redundancy	Enable Geo Replication may fail in certain scenarios due to transaction timeout
SMGR-55032	Communication Manager Management	"duplicate station" with SIP URI does not work from System Manager
SMGR-55021	Scheduler Management	Unable to schedule CM sync jobs for Saturday
SMGR-55016	Import Export Management	Unable to chance endpoint name using endpoint import if the endpoint has feature buttons associated with it
SMGR-54999	Backup and Restore Management	Logs for recurring backup job may go in the same log file in certain scenarios causing performance issues
SMGR-54841	Communication Manager Management	System Manager User Management Bulk Import does not work properly for Station button data when using the "merge" option
SMGR-54840	User Management	Error while updating SIP user with delta XML from User Management webservice
SMGR-54824	Infrastructure	OVA deployment from System Manager SDM / SDM Client using the URL option fails if the URL contains unwanted path parameters
SMGR-54821	Communication Manager Management	AD sync fails to remove user is the station is part of hunt group on a tenant management enabled system
SMGR-54789	User Management	Unable to Edit OR delete UPR on a system upgraded from 7.1-GA to 8.1.x
SMGR-54771	Trust Management	Fix authentication checks for System Manager EJBCA pages
SMGR-54769 SMGR-56634	User Management	Using "Select All" on the Manage Users page table which has results based on a search criteria , results in users that are not part of the results to get selected

SMGR-54738	Communication Manager Management	Call-appr button cannot be added to cs1k endpoints using "Global Endpoint Change" functionality
SMGR-54652	Software Upgrade Management	Errors seen when a user clicks on “Services - Solution Deployment Manager -> upgrade Jobs Status page” and selects a Job Type with no records in it
SMGR-54617	Communication Manager Management	Export Endpoint fails and results in an empty file if you have more than 30K endpoints and you try to export all of them into a single file
SMGR-54613	Infrastructure	"emdata" folder does not have appropriate permissions in a Software only deployment of System Manager.
SMGR-54587	Geographic Redundancy	Fix issues in the Geo Redundancy Disaster Recovery workflow
SMGR-54584	User Management	Changing loginname of a user that has a Officelinx Comm Profile associated with it does not propagate the updated loginname on to the Officelinx Server
SMGR-54571	User Interface Management	Unable to use passwords greater than 63 characters when scheduling System Manager backups on to a remote server
SMGR-54566	User Management	Unable to create users that have brackets in First name and/or last name
SMGR-54502	User Interface Management	Shortcuts in Home Dashboard widget gets overlapped
SMGR-54490	Infrastructure	Remove irrelevant log messages that are causing the postgres logs and /var/log/messages to fill up
SMGR-54473	Communication Manager Management	When Voicemail password is changed on OfficeLinx, SMGR Event/Log Viewer page shows activity done by "admin" user irrespective of the user configured on OfficeLinx
SMGR-54472	Communication Manager Management	When Voicemail password is changed on OfficeLinx, on SMGR it changes ButtonModulesButtonPerPage field from “ ” to “24”
SMGR-54456	Security Updates	Security Fixes related to Blind Out-Of-Band XML External Entity
SMGR-54417	Communication Manager Management	Memory Leak related to QueryPlanCache in certain System Manager workflows
SMGR-54402 SMGR-54401	Infrastructure	Implement log rotation based on file size for derby logs
SMGR-54394	Communication Manager Management	Voice Mail Number for station associated with a user in CM comm profile get cleared after changing Voicemail Password from OfficeLinx
SMGR-54389	User Management	Unassign for Messaging Communication Profile does not work properly in certain scenarios
SMGR-54381	User Management	Users can be created with first name / last name that have unsupported characters
SMGR-54353	Communication Manager Management	Notify sync and incremental sync fails after removing station from CM which is part of pickup group
SMGR-54277	Communication Manager Management	List trace station command not working in SMGR in 8.x

SMGR-54253	Geographic Redundancy	Geo configuration fails when Secondary System Manager FQDN is in upper / mixed case
SMGR-54245	Communication Manager Management	unable to manage custom endpoint templates having "abbr dial list type" is set as "personal"
SMGR-54226	Communication Manager Management	unable to edit endpoint when the value of COR is > 995
SMGR-54186	Geographic Redundancy	After Geo configuration /etc/hosts on secondary server is set with wrong permissions
SMGR-54182	Communication Manager Management	Long russian display name in AD sync scenario is causing issue
SMGR-54174	Communication Manager Management	Blank page is seen when trying to view an Agent that has just been edited without reloading the page
SMGR-54173	Infrastructure	Default Breeze Snap-ins are not loaded on fresh installs of System Manager 8.1 when using the 8.1 E template. See PSNxxxx for details
SMGR-54155	Software Upgrade Management	Added support for ESXi version 6.7.3 on VM Management and SDM Upgrade Management
SMGR-54079	Communication Manager Management	Unable to upgrade/convert CM templates associated with a lower release version of CM to a higher release version of CM
SMGR-54078	Software Upgrade Management	Unable to get upgrade option for non-encrypted 8.1 CM OVA
SMGR-54061	Tenant Management	Unable to add tenant administrator for a Tenant in System Manager when the Tenant Management feature is enabled
SMGR-54059	Infrastructure	Fixes to Common Console scripts
SMGR-54056	Software Upgrade Management	Database connection leak in System Manager when using SDM VM Management
SMGR-54048	User Management	Add contact tab when editing a user via the User Management page does not work correctly in some cases
SMGR-53976	Communication Manager Management	Unable to add more than 9 Favorite buttons on station configured with a J179 SIP Endpoint Template
SMGR-53966	User Interface Management	Help links are missing for Certain pages on the "Home / Services / Inventory" page
SMGR-53959	User Interface Management	Clicking on the Help link on the "Home / Services / Inventory" page results in an error
SMGR-53943	Infrastructure	run the changeVFQDN command in the background
SMGR-53888	User Management	User Export failures logs show wrong failures
SMGR-53878	Communication Manager Management	"Import Jobs List" table on the Import Holiday Tables page does not show the correct number of jobs causing all the jobs to not be shown properly
SMGR-53875	Communication Manager Management	Agent editor doesn't show all buttons for view and edit
SMGR-53832	Infrastructure	vi: /var/log partition is 100% full on SMGR
SMGR-53825	Communication Manager Management	Usability: After viewing a Station by searching for it via the Global Search Option, and then clicking on the Done button results in a blank pop-up

SMGR-53817	User Interface Management	Support for apostrophe in User Management Login Name field
SMGR-53815	Communication Manager Management	ADA device language setting cannot be configured in SMGR
SMGR-53806	User Management	User can inadvertently soft delete all users on the system even though they do not have access to all the users on the system
SMGR-53805	User Management	User update via Web Services does not work in certain scenarios
SMGR-53796	Communication Manager Management	Unable to broadcast announcements from System Manager Web UI
SMGR-53662	Communication Manager Management	User edit operation is wiping out Password field for Agent comm profile
SMGR-53655	Software Upgrade Management	Encryption fields are not present in Bulk upgrade excel sheet
SMGR-53653	User Management	Non Admin User is able to assign System Admin Roles
SMGR-53631	Infrastructure	SMGR AWS OVA is generating duplicate Spirit Agent UUIDs
SMGR-53628	Global Search Management	Global search for Presence handle doesn't show correct results for users that have been created via Active Directory Sync
SMGR-53626	Import Export Management	XML based bulk import not working on Systems upgraded from 8.1.x to 8.1.2
SMGR-53623	Software Upgrade Management	Upgrade status Icon is stuck after upgrading a Session Manager / AVP or AVP utilities VM via SDM
SMGR-53563	Infrastructure	When changing the security mode of System Manager from Standard / Military hardening to MUDG mode the passphrase screen at boot time still appears and requires manual input even though a remote key server was provided
SMGR-53562	Communication Manager Management	Unable to delete Coverage time of day via the System Manager Web UI
SMGR-53556	Infrastructure	CND related files on the file system should be owned by admin user
SMGR-53555	Software Upgrade Management	Data store values are not showing during Pre-upgrade Configuration page for IE Browser.
SMGR-53546	Infrastructure	System Manager logs getting rotated after jboss restart even when the size or retention criteria has not been met
SMGR-53543	Fault Management	Set proper log levels in the Spirit Appenders which are used by Serviceability Agent so that performance is no impacted
SMGR-53506	Import Export Management	Not able to export user after upgrading to 8.1.x from 7.1.x.x
SMGR-53500	Geographic Redundancy	Geo Configuration failing after Cold Standby procedure is performed on System Manager
SMGR-53499	User Management	Unable to assign Shared Address to user
SMGR-53497	User Management	DN is not getting updated in SMGR via LDAP sync if user is moved from one OU to another OU under same data store
SMGR-53476	Communication Manager Management	While adding an analog endpoint, the list of available ports is not displayed on SMGR

SMGR-53197	Software Upgrade Management	Status of IPO upgrade stuck in "Running" when the IPO is upgraded using System Manager
SMGR-53177	Infrastructure	User can enter number 0 days and the number is larger 180 days on retention Interval (Days) field at Data retention page.
SMGR-53172	Infrastructure	The information for audit logs for "Update", "Execute" action should be showed more appropriately
SMGR-53158	Communication Manager Management	Dual Registration is automatically unchecked when using Editor Extension button in CM Endpoint Profile
SMGR-53146	Software Upgrade Management	Upgrade Dependency check as part of Data Migration
SMGR-53128	License Management	Intermittent 307 temporary redirect when trying to register collector to WebLM
SMGR-53120	Communication Manager Management	Alias template of CS1k Settype is not created correctly
SMGR-53102	Communication Manager Management	Phone Screen option is missing on Endpoint editor for Alias set type
SMGR-52989	Software Upgrade Management	SDM will not allow addition of ESXi server with license w/valid expiration date
SMGR-52981	Software Upgrade Management	SDM upgrade job does data pool continuously causing performance issues in certain scenarios
SMGR-52969	User Management	Users unable to delete private contact on SMGR, random users are getting deleted from associated contacts
SMGR-52960	User Management	XMPPHandles_domain_change_util.sh script may not work on all Systems because of hardcoded values
SMGR-52921	Communication Manager Management	Support subset, terminal number, systemid, Feature1 and feature2 fields in endpoint export for CS1k endpoint
SMGR-52910	Report Management	Unable to generate new reports due to CM type is missing after the migration
SMGR-52907	Communication Manager Management	"MWI Served User Type" to be added to SMGR template for agents
SMGR-52868	Geographic Redundancy	Geo Redundancy configuration is failing over IPv6
SMGR-52704	User Management	Intermittently users are not updated via Active Directory sync
SMGR-52336	Geographic Redundancy	Unable to perform convert to standalone because of failures in restarting the HealthMonitor service
SMGR-52072	Software Upgrade Management	“Enable Customer Root Account for this Application” checkbox should be cleared when users click "X" to close the popup of ROOT ACCESS ACCEPTANCE STATEMENT, to be consistent with the result when users clicks on the Decline button
SMGR-51933	User Management	Export Users result contains users that were not selected for export
SMGR-51613	Communication Manager Management	XML Parsing Error when adding new element on Secondary System after activating it
SMGR-51593	Infrastructure	Put checks in the changeIPFQDN command to make sure it does not run on geo setups

SMGR-51311	User Interface Management	Improve logging in Geo-Redundancy workflows
SMGR-51286	Communication Manager Management	Adding CM using SDM doesn't populate cluster type
SMGR-51084	User Interface Management	Log Settings UI enhancement to support new Appenders
SMGR-51074	Infrastructure	Clean up unwanted files that remain in the /tmp folder post patch installation
SMGR-51069	Geographic Redundancy	Misleading alarms are raised from Secondary SMGR when it is in Standby Mode
SMGR-50997	User Management	Issues in updating Localized Display Name, Endpoint Display Name and Name on CM endpoint if First/Last Name of user is updated via UPM Web Services OR Bulk Import xml
SMGR-50920	User Management	Cannot add user to group using "More Actions -> Add to Group" link
SMGR-50872	Software Upgrade Management	Unable to deploy Software only SMGR 8.1 ISO via SDM Client
SMGR-50869	Communication Manager Management	User with custom role can perform operations on a CM even if they don't have permission for that CM
SMGR-50776	Communication Manager Management	IPTCM: SMGR shows BW Sharing enabled but no NRs on CM associated
SMGR-50626	User Interface Management	Display Issues with Managed Elements Page
SMGR-50481	Communication Manager Management	"Audio File Information" section should be disabled when adding an announcement for an audio-group
SMGR-50334	Fault Management	Default ASG Auth file found on System Manager alarm should not be raised on SMGR 8.1 release
SMGR-50245	Geographic Redundancy	Geo Redundancy configuration gets stuck at "Configuration Finalization" step
SMGR-49889	Infrastructure	Application vulnerabilities for certain cookies detected by Burp scanner.
SMGR-49793	User Management	Unable to remove information related to the "Feature" field associated with the station when editing user on System Manager
SMGR-49760	Infrastructure	Add loggers / appenders for Messaging Element Manager
SMGR-49620	Role Management	Unable to parse comma (" , ") in role description field, While creating new or updating the role
SMGR-49488	Global Search Management	Global search shows less results than filtered table search
SMGR-49268	User Management	When creating a new user if there are special characters in the login name it results in issues in the user creation workflow
SMGR-49196	User Management	Cannot view or edit a user after searching for the user via the Global Search if the user contains % in the login name
SMGR-49145	Coverity Management	Coverity Fixes
SMGR-48963	Software Upgrade Management	Unable to download files from plds if Authentication base proxy server is used under user setting

SMGR-48686	Communication Manager Management	Unable to change List Type on Abbreviated Call Dialing Option to None for a station from the CM comm profile editor page from User Management
SMGR-48618	Software Upgrade Management	The parent field for Media Modules shows up as empty in certain upgrade paths
SMGR-48454	Software Upgrade Management	On System Manager 8.x Local FTP Server cannot be enabled which is required for media module upgrade using SDM
SMGR-47466	Communication Manager Management	Unable to change H323 extension password using SMGR self-provisioning User interface
SMGR-47211	Communication Manager Management	Unable to remove feature buttons associated with a Station from the User Management page
SMGR-46587	Infrastructure	ChangeVFQDN command should acquire system maintenance lock during execution
SMGR-45843	User Interface Management	System Manager Web UI login/logout events are not captured in audit logs
SMGR-45693/SMGR-54183	User Management	Clicking on the Endpoint Editor a second time does not show the changes made in the previous attempt
SMGR-41503	Infrastructure	Provide System Manager VM restart option from the System Manager Web Interface
SMGR-26899	Infrastructure	OS related Security fixes
IPOFFICE-159759,IPOFFICE-159631,SMGR-54601	IPO Element Management	IP Office Element Manager Fixes (These fixes also include fixes for the issue where when someone uses IPO Element Manager it causes the DRS replication to fail)

Fixes in System Manager 8.1.2

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible Symptoms
SMGR-50410	Certificate Management	Set default certificate end entity template and EJBCA to certificate validity max 825 days
SMGR-50619	Certificate Management	Unable to access Secondary System Manager Certificates from Primary System Manager Web Console.
SMGR-49076	Fault Management	SMGR Geo is not working properly as Replication does not get disabled on Secondary After primary is made down
SMGR-49322	Fault Management	Add or remove operation failed for profile in Serviceability Agents
SMGR-50936	Fault Management	SPM properties missing for TrapListener from the TrapListener SPM pages on system that have been upgraded from 7.1 or older releases
SMGR-50386	Fault Management	Secondary server logs being sent to primary server once secondary server activated instead of secondary server
SMGR-50196	Fault Management	Secondary Server shows notification as “Primary Server status: Not Reachable.” due health monitor service state
SMGR-50937	Fault Management	Logs for SpiritAgent should be going under /var/log/ instead of /opt/ partition.

ID	Minimum Conditions	Visible Symptoms
SMGR-50242	Fault Management	Disk usage alarm is missing for disk partitions like /var/log/, /var/log/audit
SMGR-49042	Import Export Management	Not able to import users using excel sheet on a data migrated machine to 8.1 Sprint7
SMGR-50338	Import Export Management	Cannot add public contacts using the public contacts bulk import feature
SMGR-51404	Communication Manager Management	Import user with XML fails if security code is not given.
SMGR-51312	Communication Manager Management	Export user fails if speakerphone field is set as "grp-listen"
SMGR-51324	Communication Manager Management	Blank page when backup all announcement with repeated schedule that is invalid
SMGR-51054	Communication Manager Management	Communication Manager Agent Template Upgrade works only first time. Second time user sees blank screen.
SMGR-51008	Communication Manager Management	User with Communication profile creation does not display terminal number filed if user selects option 'use existing extension' and extension of CSK1 type
SMGR-50870	Communication Manager Management	Global search for the custom user doesn't work
SMGR-52914	Communication Manager Management	COR valued is not editable in Communication Manager Agent for values apart from 1
SMGR-52878	Communication Manager Management	Import of VDN fails
SMGR-52757	Communication Manager Management	Group membership incorrect behavior if endpoints are being edited from different laptops/sessions at the same time
SMGR-52714	Communication Manager Management	Adding Hunt group to user is not working.
SMGR-50908	Communication Manager Management	Cannot edit/view users/agents/announcements using Global search in Communication Manager section if using IE11
SMGR-47559	Communication Manager Management	User cannot press Edit button to edit the endpoint in SMGR
SMGR-50650	Communication Manager Management	Buttons on button module get wiped out if user is assigned to CM endpoint using "Use Existing Endpoints" option

ID	Minimum Conditions	Visible Symptoms
SMGR-50647	Communication Manager Management	Thread leak observed in Communication Manager Element Manager.
SMGR-50645	Communication Manager Management	Session Manager asset IP changed features not working if Session Manager is changed via session manager >Communication Profile Editor page.
SMGR-50617	Communication Manager Management	Non admin users having read/write access to the files in SearchConfig and REPORTS directory
SMGR-50579	Export and Import Management	Export user to excel sheet fails on 8.1 after upgrade from 7.x
SMGR-50406	Communication Manager Management	Mismatch Feature Button on phone 1220 between System Manager and Communication Manager.
SMGR-50405	Communication Manager Management	“Shift Key” does not work on 2002 type phones.
SMGR-51608	Communication Manager Management	Agent communication profile creation is failing from user management
SMGR-50396	Communication Manager Management	Import of users with Communication Manager and Session Manager communication profile is failing using excel option.
SMGR-52892	Communication Manager Management	Hunt group cannot be exported if hunt group members are not added in sequence.
SMGR-52898	Communication Manager Management	"Security Code:" field is not getting updated for import operation from Manage endpoint page.
SMGR-52891	Communication Manager Management	"SIP Trunk" field doesn't accept value in range rp6xx for SIP endpoint templates.
SMGR-51993	Communication Manager Management	Memory leak observed when running reports for Communication Manager.
SMGR-51012	Communication Manager Management	Upgraded System Manager from 8.0.1.2 to 8.1.1 shows successful but on upgraded some of database tables missing.
SMGR-50346	Communication Manager Management	Alias station Settype is not used if add user performed using the alias template without UPR from user management.
SMGR-50525	User Management	Failure observed in user commit when uncheck, check "Allow H.323 and SIP Endpoint Dual Registration" for a user with EC500
SMGR-52275	User Management	While Adding Contact to user, filter contacts using Last Name is not possible on 8.x release.
SMGR-50097	User Management	Failures are marked on "Export All Users", but no logging for which users are failed and why.

ID	Minimum Conditions	Visible Symptoms
SMGR-50670	Communication Manager Management	Status Message not displayed when CM Synchronization is from Services / Inventory / Synchronization / Communication System
SMGR-50888	Communication Manager Management	Abbr dialing configurations get wiped up and add/edit user fails with error "abbreviating dialing list not assigned" if existing endpoint OR template has abbr-dial button assigned
SMGR-50869	Communication Manager Management	Custom user can view/edit/delete CM data like endpoints, VDN from different CM for which custom user does not have permissions
SMGR-52334	Communication Manager Management	Holiday table import and export issues
SMGR-50295	Communication Manager Management	WCBRI Endpoint is throwing 3 unambiguous validation errors upon commit
SMGR-49204	Communication Manager Management	System manager blocks adding more than 9 favorites for set-type J100
SMGR-50672	User Management	System manager operation are very slow if we use the custom role
SMGR-50620	Communication Manager Management	Communication Manager Incremental sync failing intermittently.
SMGR-50337	User Management	Unable to remove users that are added to many hunt groups
SMGR-52955	Communication Manager Management	Add Coverage time-of-day table issue
SMGR-50871	User Interface Management	French Canadian Language Pack Installation Fails
SMGR-50524	Data Replication Management	Replication SSF for BSMs in 8.x is missing database triggers for new BSMs
SMGR-51038	Infrastructure	System Monitor Service causing System Manager Web UI to be inaccessible
SMGR-50685	Trust Management	Unable to access secondary System Manager certificates from primary System Manager Web UI.
SMGR-52755	Geographic Redundancy	GEO configuration failed because a number of system level commands were taking long time to respond, the response caused due to DNS server not responding correctly at customer system.
SMGR-50655	Geographic Redundancy	Corrected logic in validate geo script to avoid false errors
SMGR-49560	Geographic Redundancy	Secondary entry converted to UCMAPP on Secondary server causing GEO issues with error "SMGR missing Secondary element entries in RTS" after patch installation
SMGR-49967	Geographic Redundancy	GEO configuration fails if postgres(database) files in corrupted state.
SMGR-49480	Fault Management	Serviceability Agent for secondary server missing on Geo Redundancy enabled setup.

ID	Minimum Conditions	Visible Symptoms
SMGR-49254	Geographic Redundancy	GEO configuration fails due to EJB remote call failure
SMGR-51438	Geographic Redundancy	Primary SMGR Failed to remove Secondary Serviceability Agent Entry After converting it to Standalone
SMGR-50993	Geographic Redundancy	Unable to perform “convert to standalone” after FINALIZE configuration failure.
SMGR-51424	Infrastructure	File permission needs to be corrected at rpms level for rpms associated with Communication Manager, Messaging and SDM managements.
SMGR-50832	Infrastructure	Default ASG Auth file found on System Manager alarm should not be raised
SMGR-50944	Infrastructure	Need 'Reboot Required' message after executing configureTimeZone
SMGR-45610	Infrastructure	World writeable folders
SMGR-50243	Infrastructure	/var/log/Avaya/systemmonitor_service_affects.log and spiritagent_service_affects.log file not rotating and filling up disk space
SMGR-50348	Infrastructure	Session Manager Element Manager Component file permission issues on System Manager server.
SMGR-49877	Infrastructure	Security vulnerabilities on System manager where Non admin users having read/write access to the files
SMGR-50477	Infrastructure	No log rotation for /var/log/Avaya/getAuthorizedKey.log file
SMGR-50404	Infrastructure	In software only environment NTP service not starting automatically after system restart
SMGR-50402	Infrastructure	syslog used in System Manager has memory leak, can cause SWAP usage issue over time.
SMGR-51478	Infrastructure	After applying the kernel rpm during the Service patch installation, didn't get reboot Message on SMGR CLI
SMGR-51592	Infrastructure	All command line history is not logged
SMGR-51233	Software Upgrade Management	During the AVP update/Upgrade timeout happens and doesn't show proper message
SMGR-52922	Software Upgrade Management	S8300E heartbeat broken by SDM 8.1.1 kickstart file
SMGR-50891	Software Upgrade Management	AVP 7.1.3.5 patch installation failed via SDM client
SMGR-52976	Software Upgrade Management	[SPLIT:8.1.2.0] S8300E heartbeat broken by SDM 8.1.1 kickstart file
SMGR-50223	Software Upgrade Management	Refresh Families and Analyze operation fails due to change in PLDS certificate
SMGR-49764	Software Upgrade Management	SMGR SDM Pre-upgrade Check job never executes.
SMGR-50485	Software Upgrade Management	AVP SSH remains enabled after every SDM operation

ID	Minimum Conditions	Visible Symptoms
SMGR-46905	Software Upgrade Management	Trust establishment fails if VM associated with multiple datastores
SMGR-50700	Software Upgrade Management	After re-establish connection or VM refresh from VM manager page for CM, Current version is not proper in upgrade management page.
SMGR-50649	Trust management	SMGR is missing the cert used for SVAR signing
SMGR-45676	User Interface Management	SMGR UI not accessible by IP address after migration/patch installation/initialization.
SMGR-50801	User Management	E.164 cannot be updated though LDAP sync after editing E.164 manually from SMGR UI
SMGR-52805	User Management	System Manager automatically generate "amp;" in Lastname / FirstName (for Latin) and Localised/EndPoint Display Name when adding UPM have special characters "&"
SMGR-50935	User Management	CS1K-IP set type cannot be added on the User management with "Use Existing Endpoints" option
SMGR-50339	User Management	Cannot add public contacts to users via the SMGR Web UI
SMGR-50926	User Management	"Export selected user" is picking up only users which are selected on current page.
SMGR-52075	User Management	For custom users sorting of user doesn't happen correctly
SMGR-50799	License Management	WebLM audit log enhancement for more readability
SMGR-51479	License Management	Centralized License Installation failed when PPU is enabled
SMGR-50580	Security Updates	(RHSA-2019:3055) Important: kernel security and bug fix update
SMGR-52455	Security Updates	nss, nss-softokn, nss-util (RHSA-2019:4190) (tcp)
SMGR-51750	Security Updates	(RHSA-2019:4326) Important: fribidi security update
SMGR-50879	Security Updates	(RHSA-2019:3872) Important: kernel security update
SMGR-51333	Security Updates	(RHSA-2019:4190) Important: nss, nss-softokn, nss-util security update
SMGR-52459	Security Updates	(RHSA-2019:3979) Important: kernel security and bug fix update
SMGR-50704	Security Updates	(RHSA-2019:3128) Important: java-1.8.0-openjdk security update
SMGR-51339	Security Updates	(RHSA-2019:3976) Low: tcpdump security update
SMGR-50859	Security Updates	(RHSA-2019:3834) Important: kernel security update
SMGR-50350	Security Updates	(RHSA-2019:2169) Important: linux-firmware security, bug fix, and enhancement update
SMGR-50340	Security Updates	(RHSA-2019:2829) Important: kernel security update
SMGR-53774 (SMGR-53925)	Security Updates	(RHSA-2020:0374) Important: kernel security and bug fix update

Fixes in System Manager 8.1.1

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible Symptoms
SMGR-50282	Certificate Management	Unable to parse comma (“ , “) in role description field, while creating new or updating the role.
SMGR-47750	Certificate Management	System Manager UI (page) gets stuck once certificate export is done.
SMGR-47841	Certificate Management	Provide proper Audit logs for Security Configuration changes
SMGR-49944	Communication Manager Management	User cannot configure more than 256 SIP trunk group members (native mode)
SMGR-49843	Communication Manager Management	Reports - Graph is not showing the proper percentage
SMGR-49730	Communication Manager Management	Editing already run report and executing it causes all future reports to Fail
SMGR-49661	Communication Manager Management	Display issue on Service Hours Tables
SMGR-49639	Communication Manager Management	Extension cannot be added to CAG from User management -> CM endpoint comm profile -> endpoint editor -> group membership tab
SMGR-49192	Communication Manager Management	Report optimization for list reports.
SMGR-49134	Communication Manager Management	"list registered-ip-stations” and “list usage hunt-group” created by custom account does not populate data
SMGR-49119	Communication Manager Management	Data Module/Analog Adjunct (D)" not showing required (mandatory fields) for CM Endpoint template with "Data Module" enabled in Feature Options.
SMGR-49115	Communication Manager Management	Coverage time-of-day shows wrong values
SMGR-49117	Communication Manager Management	CM entries are not showing on sync page if we try to sort the table based on sync status
SMGR-49103	Communication Manager Management	Report generation fails for a custom role when report (such as display/status), which requires Qualifier Value.
SMGR-48675	Communication Manager Management	Downloading the Excel template from the manage endpoints page and using it to delete stations does not work
SMGR-48559	Communication Manager Management	"Bulk Delete Endpoint Confirmation" page shows duplicate buttons "Now", "Schedule", "Cancel"
SMGR-48329	Communication Manager Management	The incorrect report is generated when pagination/order settings are changed
SMGR-48328	Communication Manager Management	Group membership tab is blank if we try to view endpoint
SMGR-49792	Communication Manager Management	SMGR is returning unacceptable data in the XML when we do a GET User through the API

ID	Minimum Conditions	Visible Symptoms
SMGR-49931	Communication Manager Management	Group members tab (Hunt Group/Trunk group form) doesn't update properly if the user tried to navigate to page 2
SMGR-49696	Communication Manager Management	Session Manager Asset IP change feature is not working.
SMGR-49156	Communication Manager Management	Cannot add more ip-network-map entries if ip-network-map already has >=500 entries
SMGR-45854	Communication Manager Management	Cannot save as template
SMGR-49680	Communication Manager Management	"Identity for Calling Party Display" value on CM SIP trunk form is not saved properly in SMGR database
SMGR-47559	Communication Manager Management	User cannot press the Edit button to edit the endpoint in SMGR
SMGR-47952	Communication Manager Management	Export All Endpoints causes the system to go out of memory
SMGR-48129	Communication Manager Management	In System Manager 8.0.1, Cannot edit user with comm profile under user management to change the first name, last name, and login name
SMGR-50151	Communication Manager Management	Customer Enhancement (LBG/BT) - list usage service-hours-table option is not available in SMGR
SMGR-49709	Communication Manager Management	Duplicate station entries when paging on Manage Endpoints.
SMGR-49024	Communication Manager Management	Extension cannot be added to CAG from User management -> CM endpoint comm profile -> endpoint editor -> group membership tab
SMGR-48621	Communication Manager Management	AD sync OR user creation fails if endpoint template having favorite checkbox enabled for autodial button without Dial Number
SMGR-49057	Communication Manager Management	CM comm profile can't be unassigned from a user if CM extension is part of coverage answer group
SMGR-50238	Communication Manager Management	Duplicate station entries when paging on Manage Endpoints.
SMGR-50218	Communication Manager Management	Coverage Path does not display Coverage Remote configuration for value "r1"
SMGR-48676	Communication Manager Management	Remove options does not work when using the Excel template to remove stations
SMGR-49611	Communication Manager Management	Cannot permanently delete user if it's associated with CM extension which is part of pickup group
SMGR-50188	Communication Manager Management	Removed non supported language “Simplified Chinese" and added with supported language like (Chinese, Polish, Thai, Traditional Chinese and Turkish) in System Manager Web console – Communication Manager Endpoint editor.

ID	Minimum Conditions	Visible Symptoms
SMGR-49625	Global Search Management	Group membership data is not populated properly in Global search if multiple endpoints are viewed/edited one after another
SMGR-49316	Global Search Management	Global search feature does not show group membership
SMGR-49245	Global Search Management	Group membership data is not populated properly in Global search if multiple endpoints are viewed/edited one after another
SMGR-49149	Global Search Management	Global search for the custom user doesn't work in 8.x
SMGR-49903	Global Search Management	Global search feature does not show group membership
SMGR-50198	Inventory Management	Not able to edit the assignment name for the AES element from Manage element
SMGR-49029	Fault Management	HttpThread Usage Monitor is not calculating the http thread percentage properly
SMGR-49423	Geographical Redundancy	Geo config shows successful in Audit logs in spite GEO configuration failure
SMGR-49205	Geographical Redundancy	Geo backup files are stored in world readable folders
SMGR-47633	Geographical Redundancy	No logrotate for /var/log/Avaya/mgmt/geo/csync2.log
SMGR-49597	Geographical Redundancy	Cannot reconfigure GEO configuration on SMGR Secondary after Primary SMGR convert to standalone.
SMGR-50194	Geographical Redundancy	Geo aware Elements are not switching to Secondary SMGR automatically after activating secondary SMGR
SMGR-49750	Geographical Redundancy	SMGR GEO setup - Primary SMGR loses management status of breeze elements
SMGR-50190	Geographical Redundancy	Geo configuration is failing in when user try to configure it first time
SMGR-49130	Infrastructure	changePublicIPFQDN command is not working
SMGR-50116	Infrastructure	IPFQDN change corrupts network files causing postgres startup issue
SMGR-49748	Infrastructure	SMGR WebLM firewall is blocking SBCE as it is sending more than 100 requests within 60 seconds on port 52233
SMGR-49683	Infrastructure	In SMGR FIPS mode not able to enable EASG using 'EASGManage –enableEASG' command
SMGR-49607	Infrastructure	Vacuum cron job does not work properly
SMGR-49359	Infrastructure	No log rotate for jboss_service_affects.log
SMGR-48645	Infrastructure	Audit.log does not rotate in SMGR Military mode
SMGR-49840	Infrastructure	System Manager stops working properly if default outbound trust store contains more than 250 trusted CA certificates in it.
SMGR-49905	Infrastructure	Notify sync is not working due to firewall reject rule for 9000 port added

ID	Minimum Conditions	Visible Symptoms
SMGR-48282	Infrastructure	If changeIPFQDN script failed at certificate renewal, then SMGR may end up with two IP
SMGR-49072	Scheduler Management	Scheduler: End by Date fields are missing from job schedule page.
SMGR-49308	Security Updates	(RHSA-2019:1481) Important: kernel security update
SMGR-49269	Security Updates	(RHSA-2019:1235) Important: ruby security update
SMGR-49266	Security Updates	(RHSA-2019:1294) Important: bind security update
SMGR-49267	Security Updates	(RHSA-2019:1228) Important: wget security update
SMGR-49140	License Management	Enterprise System Manager WebLM shows negative value for Currently Available AES license count when AES is pointed directly to master WebLM and when clicked on Allocations link
SMGR-50237	License Management	special characters are showing when viewing allocations on WebLM 8.1
SMGR-49314	Security Updates	(RHSA-2019:1481) Important: kernel security update
SMGR-49299	Security Updates	(RHSA-2019:1235) Important: ruby security update
SMGR-49283	Security Updates	(RHSA-2019:1294) Important: bind security update
SMGR-49291	Security Updates	(RHSA-2019:1228) Important: wget security update
SMGR-50145	Software Upgrade Management	[customer issue]SDM vCenter 6.7 mapping failed with error getting SSO token
SMGR-50126	Software Upgrade Management	[SPLIT:8.1.1.0] Customer Issue [FRB] - Refresh Element shows successful even when it failed
SMGR-49735	Software Upgrade Management	[SPLIT:8.1.1.0] Customer Escalation: ON SMGR Local FTP Server cannot be enabled which is required for media module upgrade using SDM
SMGR-49315	Software Upgrade Management	[Customer Issue] File upload to external FTP server using alternate source or /swlibrary/staging/sync does not work
SMGR-47957	Software Upgrade Management	Customer Issue [FRB] - Refresh Element shows successful even when it failed
SMGR-48134	Software Upgrade Management	[Customer Issue - VODAFONE UK] In System Manager 8.0.1 cannot upload ASM 8.0 OVA to software library using My Computer option in the google Chrome browser
SMGR-50232	Software Upgrade Management	[SPLIT:8.1.1.0] [Customer Issue] In System Manager 8.0.1, Issue with Download the g450 fdl file using My Computer option
SMGR-48963	Software Upgrade Management	Customer issue: Not able downloaded files from plds if Authentication base proxy server is used under user setting

ID	Minimum Conditions	Visible Symptoms
SMGR-48287	Software Upgrade Management	Customer Issue - Migrating from CM 6.3.x on VSP to CM 7.1 on AVP does not work if remote software library used to provide the AVP ISO file
SMGR-50016	Software Upgrade Management	[SPLIT:8.1.1.0] Customer Escalation: For G450 MG, MP160 board subtype shows as 'other'
SMGR-48743	Software Upgrade Management	[Customer Issue] The Avaya Aura messaging element should not get added to System Manager inventory through SDM after trust re-establishment.
SMGR-48147	Software Upgrade Management	[Customer Issue - UNIVERSITY OF NEW HAMPSHIRE] Refresh Host gets stuck after changing host password through SDM
SMGR-49253	Software Upgrade Management	[Customer Issue -FOND DU LAC BAND OF LAKE SUPERIOR] Gateway discovery does not work with SNMPv3
SMGR-49628	User Management	Can't create Officelinx user using User Provisioning Rule in case "Application User Password" field set to "Use Mailbox" or "Reverse Mailbox"
SMGR-49073	Authentication Management	SAML Authentication in not working on 8.0.1.1
SMGR-48617	Role Management	RBAC users see Blank pages if mappings are created under group
SMGR-48181	User Management	While create/edit of user/role gets error "Invalid request received. Please contact your system administrator"
SMGR-49873	User Management	non admin user with administrator privilege cannot change Public Contact
SMGR-49815	User Management	Directory Sync fails where UPR has mapped officelinx mailbox field with active directory attribute like ipPhone
SMGR-49421	User Management	SMGR not able to roll back CM user if user creation fails due to messaging error
SMGR-49195	Global Search Management	Global Search with Russian Language doesn't work as expected
SMGR-49075	User Management	Not able to edit the user if "Other XMPP" type communication address is added.

Fixes in System Manager 8.1

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms
SMGR-39711	Backup and Restore Management	After Restore earlier scheduled backup job is getting disabled
SMGR-39209	Backup and Restore Management	PEM backup fails due to large Announcement files
SMGR-46745	Backup and Restore Management	Provide validation during restore to check system FQDN value vs value in backup.info file

ID	Minimum Conditions	Visible symptoms
SMGR-47750	Certificate Management	UI (page) gets stuck once certificate export is done
SMGR-48663	Certificate Management	Thread in SMGR cause up TM code because of incorrect usage of SPM
SMGR-46641	Certificate Management	CRLExpirationCheckerJob job execution is failing so alarm is getting generated
SMGR-48294	Communication Manager Management	Edit VDN operation by custom user (with extension range) fails on SMGR if VOA extension contains "-"
SMGR-48695	Communication Manager Management	Coverage path is removed from existing station on CM when same extension is used while adding "CM endpoint profile" on SMGR
SMGR-48160	Communication Manager Management	Issue while edit ars digit-conversion operation via "cut through" OR "ARS Digit Conversion" page
SMGR-47168	Communication Manager Management	Customer user (any user other than super user) cannot delete announcement backup manually
SMGR-48190	Communication Manager Management	User creation fails If UPR uses a template that has Voicemail Number entry set
SMGR-46896	Communication Manager Management	Preferred Handle attribute to "None" when name changes for user is performed
SMGR-47848	Communication Manager Management	Using UM edit option Coverage Path field is not getting set to blank once assigned a value
SMGR-48156	Communication Manager Management	Using Classic view, Agent skill changes are not getting updated OR saved
SMGR-48460	Communication Manager Management	Cannot modify an abbreviated dialing enhanced object on second (or next) page
SMGR-46782	Communication Manager Management	Failed to add hunt group, if RBAC user has all permissions and also it has Endpoint and hunt extension ranges defined
SMGR-47467	Communication Manager Management	Download announcement issues
SMGR-46723	Communication Manager Management	Custom users cannot use the Import/Export feature on VDN form
SMGR-46930	Communication Manager Management	Extension lookup very slow on VND and hunt group pages causing system slowness
SMGR-48033	Communication Manager Management	List extension-type report puts COR and COS field values in wrong place
SMGR-47826	Communication Manager Management	Cannot update preferred handle of CM comm profile using SMGR bulk edit option
SMGR-47620	Communication Manager Management	iptcm usage of cssecurestore filling up the cssecurestore table to the extent that it causes Geo workflow to fail
SMGR-48293	Communication Manager Management	Few specific feature-access-codes are not listed in the System Manager
SMGR-46515	Communication Manager Management	Backup All Announcement job shows success even though it is unable to download all announcement file.
SMGR-47807	Communication Manager Management	Selected endpoint records do not get clear after reload page or moved across table pages if records are more than 15

ID	Minimum Conditions	Visible symptoms
SMGR-47434	Communication Manager Management	Click Agent Skill tab freezes
SMGR-47849	Communication Manager Management	Report generation for "list monitored-station" is failing
SMGR-47845	Communication Manager Management	CM IP gets interchanged on System Manager -> Communication Manager pages causing interchanged CM to disappear for logged in user having custom role mapped with CM active IP address
SMGR-48084	Communication Manager Management	129 phone cannot create adhoc conference when using J129_DEFAULT_CM_8_0 template
SMGR-47133	Communication Manager Management	Filter enabled by one user is not cleared on Mange Endpoint page if another user logs in to SMGR UI
SMGR-47876	Communication Manager Management	"Global Endpoint Change" deletes station Name when "Endpoint Display Name:" contains "~" character.
SMGR-47156	Communication Manager Management	Delete station job gets stuck in running mode
SMGR-46163	Communication Manager Management	Unable to configure COR > 250 on CM 5.2.1 using Endpoint Editor
SMGR-47155	Communication Manager Management	After selecting VDN record buttons(view/edit/delete) are not getting enabled
SMGR-47453	Communication Manager Management	XML Parsing Error when using "Bulk Add Agents" and "Bulk Delete Agents" options
SMGR-47429	Communication Manager Management	Features on JEM24 are removed but LED still on after Feature are removed out of Favorite list
SMGR-46734	Communication Manager Management	SV-SP1: Breeze replication failed, SMGR runs out of space in /var/log
SMGR-44755	Geographical Redundancy	GEO-R Enable Replication resulted in full /var on both primary and secondary
SMGR-46433	Infrastructure	Customer Issue: Logout does not work on IE 11
SMGR-46815	Infrastructure	Display only shows 15 rows at a time even though the common console is configured to display more
SMGR-43365	Infrastructure	Issues with changeIPFQDN script
SMGR-46934	Infrastructure	Left menu of Routing shows blank after we drag (accidentally) Routing item in Elements list
SMGR-48266	Infrastructure	118555 - RHEL 7 : git (RHSA-2018:3408) (tcp)
SMGR-48267	Infrastructure	RHEL 7 : libmspack (RHSA-2018:3327) (tcp)
SMGR-48269	Infrastructure	RHEL 7 : java-1.8.0-openjdk (RHSA-2019:0435) (tcp)
SMGR-48271	Infrastructure	RHEL 7 : binutils (RHSA-2018:3032) (tcp)
SMGR-48273	Infrastructure	RHEL 7 : systemd (RHSA-2019:0201) (tcp)
SMGR-48274	Infrastructure	RHEL 7 : glibc (RHSA-2018:3092) (tcp)
SMGR-48277	Infrastructure	Red Hat Update Level (tcp)
SMGR-48965	Infrastructure	RHEL 7 : wget (RHSA-2019:1228) (tcp)

ID	Minimum Conditions	Visible symptoms
SMGR-48966	Infrastructure	RHEL 7 : kernel (RHSA-2019:1168) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout) (tcp)
SMGR-37985	License Management	WebLM email notifications doesn't have a valid from field
SMGR-47680	License Management	Provide a command line utility to add certificates to trust store of standalone WebLM OVA based deployment
SMGR-39633	License Management	SMGR WebLM home page goes blank screen after installing 3rd party certs
SMGR-47971	License Management	When attempting to install a valid license on System Manager, getting an error "Solution License can be installed through Collector only"
SMGR-48192	Report Management	Email not received when reports generated thru SMGR webpage
SMGR-46783	Report Management	"list measurements ip dsp-resource" report doesn't match column headings and values
SMGR-48340	Report Management	User cannot generate report when he has multiple ranges defined under endpoint, VDN, Vector etc.
SMGR-47887	Report Management	User cannot configure Task Time, Recurrence and Range values if he wants to schedule report generation job later
SMGR-48484	Report Management	Display vector report generation fails for PDF format
SMGR-48182	Report Management	Setdata report taken in SMGR has incorrect column alignments.
SMGR-48260	Report Management	"Creation Time" does not show date and time in AM/PM in report generation and history pages
SMGR-48545	Report Management	When multiple reports are run concurrently, some of the runs produce zero size (empty) reports
SMGR-47640	Report Management	"REPORTS_CleanUp_System_Job" is failing on SMGR 8.0
SMGR-46220	Software Upgrade Management	SDM shows incorrect Entitled Update Version
SMGR-48571	Software Upgrade Management	SMGR SDM ‘Analyze’ and ‘Refresh Elements’ not enabled for AVPU.
SMGR-46365	Software Upgrade Management	SMGR (military mode) is not able to establish “trust” with the servers deployed in the environment
SMGR-48717	User Management	Coverage path is set to blank even if it is configured in UPR with custom template
SMGR-47112	User Management	UPM Error code issue when webservice is used for user creation which is not administered in CM dialplan
SMGR-46642	User Management	UserMgmtJob job execution is failing so alarm is getting generated
SMGR-41634	User Management	Self-provisioning does not work after providing windows user id if external authentication is configured on SMGR
SMGR-45884	User Management	If the same attribute from AD is mapped to loginname and otherEmail and value of the attribute is in mixed case or upper case, then after each sync user shows as Modified on SMGR.

Known issues and workarounds in System Manager in Release 8.1.3.x

Known issues and workarounds in System Manager in Release 8.1.3.1

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Minimum Conditions	Visible Symptoms	Workaround
SMGR-57926	Software Upgrade Management	On using a build name containing '(', upgrade from 7.1.3.7 to 8.1.3 completes successfully, however status does not reflect on SDM client.	Use build name that does not contain '(' or ')' , for upgrade.
SMGR-57686	User Interface Management	SMGR 8.1.3: Supported Browsers warning message needs to be corrected for Firefox browser version on Login Page	Use Firefox 65 and above
SMGR-55937	Security Management	User being logged-out from UI randomly while accessing the UI	None
SMGR-54851	Authentication Management	SAML Authentication not working after upgrading 7.0.1.2 to 7.1.3	None
SMGR-54468	Trust Management	PEM Certificate Error seen while creating a PEM certificate on a FIPS enabled SMGR	Create a JKS format file and then convert it to PEM format(or any other desired format).
SMGR-53558	Client Management	Java core dumps seen on Breeze nodes because of the openSSO client with SMGR.	Restart the Service on System Manager
SMGR-50300	Communication Manager Management	Changes related to Per Button Ring Control feature for Call Appearance button of SIP station is not applied to the station when done via the Station Editor form in the CM communication Profile section	None
SMGR-49616	Software Upgrade Management	After Upgrade from 7.0.x to 8.0.x external authentication and Policy links stop working	None
SMGR-59032	Security Policies	Administrative users cannot change password when password policy is disabled for SMGR UI logins	Enable password policy and set the password.
SMGR-58988	External Authentication	External authentication fails once the password for AD server changes	Restart JBoss service
SMGR-58635	User Management	AD sync fails for users having CM comm profile if loginname is changed through AD sync.	None
SMGR-58339	Communication Password Management	"Automatic generation of communication profile password" fails in UPR after comm profile password policy is changed.	None
SMGR-43249	User Interface	Time zone not showing properly with certificate based login.	None

SMGR-58001	Global Search Component	Admin cannot search from Global Search if User with special characters like [,] , {, }	Remove special characters like [,] , {, } from user.
SMGR-59052	Fault Management	Editing log appender does not work in certain cases.	First change the Max retention file size and then come back and change the rotate file size.
SMGR-46088	User Interface Management	Cannot login to secondary SMGR UI using EASG after secondary SMGR is activated	Use other user credentials.
SMGR-59089	Reports Generation	The report cannot be generated on System Manager because of the error message in the completed job.	None
SMGR-59125	User Management	Cannot edit fields other than Address Name in the Address section of User Profile.	To change other fields in the Address section of User Profile, you must change the "Address Name" field as well.

Known issues and workarounds in System Manager in Release 8.1.3

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Minimum Conditions	Visible Symptoms	Workaround
SMGR-57926	Software Upgrade Management	On using a build name containing '(', upgrade from 7.1.3.7 to 8.1.3 completes successfully, however status does not reflect on SDM client.	Use build name that does not contain '(' or ')' , for upgrade.
SMGR-57686	User Interface Management	SMGR 8.1.3: Supported Browsers warning message needs to be corrected for Firefox browser version on Login Page	Use Firefox 65 and above
SMGR-57282	User Management	Export All Users does not export 100%	None
SMGR-55937	Security Management	User being logged-out from UI randomly while accessing the UI	None
SMGR-54851	Authentication Management	SAML Authentication not working after upgrading 7.0.1.2 to 7.1.3	None
SMGR-54606	Communication Manager Management	Associating existing H323 station with existing user on SMGR for dual registration, incorrect station number added to the off-pbx station-mapping form	Enable dual reg field in second Edit option

SMGR-54468	Trust Management	PEM Certificate Error seen while creating a PEM certificate on a FIPS enabled SMGR	Create a JKS format file and then convert it to PEM format(or any other desired format).
SMGR-53558	Client Management	Java core dumps seen on Breeze nodes because of the openSSO client with SMGR	Restart the Service on System Manager
SMGR-51282	Fault Management	Selecting ALL in the Alarm Table on a specific page, then de-selecting a single entry on another page results in incorrect selection.	None
SMGR-50300	Communication Manager Management	Changes related to Per Button Ring Control feature for Call Appearance button of SIP station is not applied to the station when done via the Station Editor form in the CM communication Profile section	None
SMGR-49616	Software Upgrade Management	After Upgrade from 7.0.x to 8.0.x external authentication and Policy links stop working	None
SMGR-49355	User Management	Changing fields with Messaging Editor does not take effect on Subscriber profile	None
SMGR-47622	Command Manager Management	Restricted RBAC users able to see other CMs even if they don't have permission.	None
SMGR-46088	User Interface Management	Cannot login to secondary SMGR UI using EASG after secondary SMGR is activated	User other user credentials.

Known issues and workarounds in System Manager in Release 8.1.2

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Minimum Conditions	Visible Symptoms	Workaround
SMGR-53102	Communication Manager Management	Phone Screen option is missing on Endpoint editor for Alias set type	None
SMGR-53020	Communication Manager Management	Announcement backups are going to directory with very limited space "/opt"	None
SMGR-52969	User Management	Users unable to delete private contact on SMGR, random users are getting deleted from associated contacts	None
SMGR-52910	Communication Manager Management	Unable to generate new reports due to CM type is missing after the migration	Contact Avaya Support Team.
SMGR-52849	Software Upgrade Management	NTP server details on AVP are not updated properly through SDM	None

SMGR-52744	User Interface Management	CS1000 Elements cannot be sorted in 8.1.1	None
SMGR-52704	User Management	Cannot update user via AD sync. Error shows "could not initialize proxy - no Session"	None
SMGR-51282	Fault Management	Selecting ALL in the Alarm Table on a specific page, then de-selecting a single entry on another page results in incorrect selection.	None
SMGR-51069	Geographic Redundancy	Irrelevant alarms are raised from Secondary SMGR when it is in Standby Mode	None
SMGR-50997	User Management	Issues in updating Localized Display Name, Endpoint Display Name and Name on CM endpoint if First/Last Name is updated through API OR Import xml functionality	None
SMGR-50333	Trust Management	After running change VFQDN, old vFQDN still appears in CRL Distribution Points & Authority Information Access	None
SMGR-50229	Communication Manager Management	SMGR Endpoint template is missing for 4624 set type	None
SMGR-49620	Role Management	Unable to parse comma (“ , “) in role description field, While creating new or updating the role.	Remove comma in role description field before role create/update operation.
SMGR-49488	Search Management	Global search shows less results than filtered table search	None
SMGR-49316	Communication Manager Management	Global search feature does not show group membership	None
SMGR-49264	User Interface Management	GEO configuration fails if port 8193 is blocked between both SMGR servers	Refer PSN005273u for more details.
SMGR-48200	Backup and Restore Management	Unable to take remote backup on HDI (Hitachi Data Ingestor) Linux appliance remote server	None
SMGR-47786	Communication Manager Management	Need to provide 'Attendant' field for J169 & J179 set types	None
SMGR-47622	Command Manager Management	Restricted RBAC users able to see other CMs even if they don't have permission.	None
SMGR-46872	User Interface Management	Issue noticed with Shutdown System Manager option in SMGR web console	None
SMGR-46552	User Interface Management	SMGR - jQuery 1.4.2 is out-of-date, current version is 1.11	None

SMGR-46363	Trust Management	Trying to replace a pem certificate using a third-party cert which is signed using Elliptical Curve signing algorithm results in the certificate to get corrupted and removed from the Manager Id cert UI	Use different algorithm to sign certificate.
SMGR-46088	User Interface Management	Cannot login to secondary SMGR UI using EASG after secondary SMGR is activated	User other user credentials.
SMGR-45913	User Interface Management	User gets system error while updating existing role having permissions for group once group is renamed	1. Select the custom role 2. Remove permissions associated with old group Ex. "group1"(All elements of type: users under group group1) and save role Add required permissions for new group Ex. “group2” in the custom role
SMGR-45856	User Management	Latin transcription of "First Name" and "Last Name" in the Identity Tab of User in SMGR are not happening properly for Russian name with the Cyrillic alphabet	Manually update Latin transcription value for the First Name" and "Last Name" in the Identity Tab of User and save user.
SMGR-45752	Communication Manager Management	Announcement backup works only for MD5 and DES combination	None
SMGR-45742	Communication Manager Management	UDP group ENP entry design issue if there are more than 3 CMs in the UDP group	None
SMGR-43445	User Interface Management	Shortcut keys present in UI is not working	None
SMGR-43249	User Interface Management	Time zone not showing properly with cert based login.	None
SMGR-41461	User Management	Not displaying description for error code during SMGR AD user update failed	None
SMGR-40715	Trust Management	SSL handshake fails on JMX port connection if revocation checking set to OCSP.	Revert to OCSP settings back to default settings in Home / Services / Security / Configuration / Security Configuration (Revocation

			Configuration section.)

Known issues and workarounds in System Manager in Release 8.1.1

The following table lists the known issues, symptoms, and workarounds in this release.

Key	Minimum Conditions	Summary	Workaround
SMGR-46363	Certificate Management	Trying to replace a pem certificate using a third-party cert which is signed using Elliptical Curve signing algorithm results in the certificate to get corrupted and removed from the Manager Id cert UI	None
SMGR-47167	Communication Manager Management	Enhancement request to add remote server settings for storing announcement backup	None
SMGR-49967	Geographical Redundancy	GEO configuration fails if postgres file pg_control is in corrupted state	On primary Server make sure swlibrary has more free space than actual space used by partition /var/lib/pgsql.
SMGR-47622	Geographical Redundancy	Restricted RBAC users able to see other CMs even if they don't have permission	None
SMGR-49615	Infrastructure	Software only installer corrupts the /etc/fstab file which caused the OS to not both up	None
SMGR-48582	License Management	IPO based WebLM fails to generate hosts ID when system language is set to local language like de_DE.UTF-8 i.e. Germany (other than English)	1. Change System language to English rather than other local language like de_DE (Germany) and reboot system. 2. If customer don't want to keep system language as English then: a. Follow step 1 b. After host ID generation, change the system language back to local language. Note: If you choose 2nd option, then need to follow this option on every reboot
SMGR-49488	Global Search Management	global search shows less results than filtered table search	None
SMGR-48408	Software Upgrade Management	For G450 MG, MP160 board subtype shows as 'other'	None
SMGR-48200	Software Upgrade Management	Unable to take remote backup on HDI (Hitachi Data Ingestor) Linux appliance remote server	None
SMGR-48090	Software Upgrade Management	TN board discovery for duplex CM does not work after CM interchange	None

Key	Minimum Conditions	Summary	Workaround
SMGR-46905	Software Upgrade Management	Trust establishment fails if VM associated with multiple datastores	None
SMGR-50485	Software Upgrade Management	AVP SSH remains enabled after every SDM operation	Manually disable SSH on AVP after utilizing SMGR SDM OR SDM Client
SMGR-50097	User Management	Failures are marked on "Export All Users", but no logging for which users are failed and why	None
SMGR-46088	User Management	Cannot login to secondary SMGR UI using EASG after secondary SMGR is activated	None
SMGR-45913	Role Management	User gets system error while updating existing role having permissions for group once group is renamed	1. Select the custom role 2. Remove permissions associated with old group Ex. "group1"(All elements of type: users under group group1) and save role Add required permissions for new group Ex. “group2” in the custom role
SMGR-43445	User Management	Shortcut keys present in UI is not working	None
SMGR-43249	User Management	Time zone not showing properly with cert-based login.	None
SMGR-50338	User Management	Cannot add public contacts using the public contacts bulk import feature	None
SMGR-50339	User Management	Cannot add public contacts to users via the SMGR Web UI	None
SMGR-50383	Communication Manager Management	Export user to Excel doesn't work on 8.0.1.2 for SIP endpoint with CM and SM comm profile	None
SMGR-50409	Infrastructure	Unable to see VM Console permission while creating custom role for resource type SDM	None
SMGR-50404	Infrastructure	In software only environment NTP service not starting automatically after system restart	Manually start NTP service
SMGR-50402	Infrastructure	rsyslog used in SMGR has memory leak can cause SWAP usage issue over time	restart ryslog service
SMGR-50386	Geographical Redundancy	Customer Issue (LBG) - Secondary server logs being sent to primary server once secondary server activated instead of secondary server	Rrestart spirit Agent service on Secondary once activated and deactivated.
SMGR-50348	EID	SMEM file permission issues per customer via APS	None
SMGR-50337	Communication Manager Management	Unable to remove users that are added to many hunt groups	None
SMGR-50334	Fault Management	Default ASG Auth file found on System Manager alarm should not be raised on SMGR 8.1 release	None
SMGR-50333	Infrastructure	After running changeVFQDN, old vFQDN still appears in CRL Distribution Points & Authority Information Access	None

Key	Minimum Conditions	Summary	Workaround
SMGR-50245	Geographical Redundancy	[Customer Issue - KIRKLAND AND ELLIS] Geo Redundancy configuration gets stuck at "Configuration Finalization" step	None
SMGR-50243	Infrastructure	/var/log/Avaya/systemmonitor_service_affects.log and spiritagent_service_affects.log file not rotating and filling up disk space	Manually truncate contents of the file /var/log/Avaya/systemmonitor_service_affects.log
SMGR-50524	Infrastructure	Replication SSF for BSMs in 8.x is missing database triggers for new BSMs	None
SMGR-50223	User Management	[Customer Issue] Refresh Families and Analyze operation fails due to change in PLDS certificate	Refer PSN005260u for details
SMGR-50341	Communication Manager Management	Cannot remove button labels using the CM Endpoint Editor	Workaround is to use manage endpoint page
SMGR-50579	User Management	Customer Issue (PIERCE COUNTY IT DEPT): Export user to excel sheet fails on 8.1 after upgrade from 7.x	Export users to xml

Known issues and workarounds in System Manager in Release 8.1

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-48200	Backup and Restore Management	Unable to take remote backup on HDI (Hitachi Data Ingestor) Linux appliance remote server	None
SMGR-48877	Communication Manager Management	"Allow H.323 and SIP Endpoint Dual Registration" is not grayed out for SIP CM endpoint Template	None
SMGR-48555	Communication Manager Management	Attendant header is missing in CM Endpoint Profile in Exported list of users	None
SMGR-47952	Communication Manager Management	Export All Endpoints causes system to go out of memory	None
SMGR-47622	Communication Manager Management	Restricted RBAC users able to see other CMs even if they don't have permission	None
SMGR-48329	Communication Manager Management	Incorrect report is generated when pagination/order settings are changed	None
SMGR-45752	Communication Manager Management	Announcement backup works only for MD5 and DES combination	None
SMGR-47633	Geographic Redundancy	No logrotate for /var/log/Avaya/mgmt/geo/csync2.log	In Geo Redundancy system, empty the log file - /var/log/Avaya/mgmt/geo/csync2.log
SMGR-48645	Infrastructure	Audit.log does not rotate in SMGR Military mode	Empty the log files, then Restart auditd service (service auditd restart) with root user.

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-48582	License Management	IPO based WebLM fails to generate hosts ID when system language is set to local language like de_DE.UTF-8 i.e. Germany (other than English)	1. Change System language to English rather than other local language like de_DE (Germany) and reboot system. 2. If customer don't want to keep system language as English then: a. Follow step 1 b. After host ID generation, change the system language back to local language. Note: If you choose 2nd option, then need to follow this option on every reboot
SMGR-48408	Software Upgrade Management	For G450 MG, MP160 board subtype shows as 'other'	None
SMGR-48289	Software Upgrade Management	AVP custom patches should not be displayed in download management as its not supported.	None
SMGR-48147	Software Upgrade Management	Refresh Host gets stuck after changing host password through SDM	None
SMGR-48090	Software Upgrade Management	TN board discovery for duplex CM does not work after CM interchange	None
SMGR-48086	Software Upgrade Management	In System Manager 8.0.1, Issue with Download the g450 fdl file using My Computer option	None
SMGR-46905	Software Upgrade Management	Trust establishment fails if VM associated with multiple datastores	None
SMGR-45036	Software Upgrade Management	When WebLM 7.1 OVA is deployed on AVP 7.1, AVP shows a warning that configured Guest OS and OS of running VM doesn't match	None
SMGR-46363	Trust management	Trying to replace a pem certificate using a third-party cert which is signed using Elliptical Curve signing algorithm results in the certificate getting corrupted and removed from the Manager Id cert UI	None
SMGR-48621	User Management	AD sync OR user creation fails if endpoint template having favorite checkbox enabled for autodial button without Dial Number	None
SMGR-48617	User Management	RBAC users see Blank pages if mappings are created under group	None

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-48181	User Management	During create/edit of user/role “Invalid request received. Please contact your system administrator" error is displayed	During create or update if user's id or full name or role name or description has a space at the beginning or at the end then remove space if present at end or beginning from value and then perform operation
SMGR-46088	User Management	Cannot login to secondary SMGR UI using EASG after secondary SMGR is activated	None
SMGR-45913	User Management	User gets system error while updating existing role having permissions for group once group is renamed	1. Select the custom role 2. Remove permissions associated with old group Ex. "group1"(All elements of type: users under group group1) and save role Add required permissions for new group Ex. “group2” in the custom role
SMGR-45856	User Management	Latin transcription of "First Name" and "Last Name" in the Identity Tab of User in SMGR are not happening properly for Russian name with the Cyrillic alphabet	None
SMGR-44830	User Management	GEO configuration will fail if we set Maximum Sessions Per User: 1	Set Maximum Sessions Per user defined as below on primary server: • Maximum Sessions Per User: 5 Perform Geo configuration from secondary server
SMGR-43249	User Management	Time zone not showing properly with cert-based login	None

Solution Deployment Manager Adopter Matrix

Solution Deployment Manager Adopter Matrix	Adopting Product (System Manager Release 8.1)													
System Manager Solution Deployment Manager - Centralized									Breeze				Avaya Aura®	
Functionality	Appliance Virtualization Platform	System Manager	Session Manager	Communication Manager	CM Adjuncts (MM, TN Boards, Gateways)	Branch Session Manager	AVP Utilities	CM Messaging	(w/ Presence Snap-in)	Secure Access Gateway	WebLM	Application Enablement Services	Media Server	Session Border Controller (SBCE 8.0.1)
OVA Deployment R 7.0.0/7.1/8.0/8.1 (Configuration and Footprint)	N	N	Y	Y	n/a	Y	Y	Y	Y	Y	Y	Y	Y	Y[2] [Supported from 8.1.1]
OVA Deployment R 7.1R (Configuration and Footprint)	n/a	N	Y	Y	n/a	Y	Y	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Encrypted OVA Deployment (Configuration and Footprint)	N	Y(only through SDM client)	Y	Y	n/a	Y	Y	n/a	n/a	n/a	N	n/a	n/a	N
Patching Deployment (hotfixes)	Y [Other than AVP hosting System Manager]	N	Y	Y	n/a	Y	Y	Y	N	N	N	Y	N	N

Solution Deployment Manager Adopter Matrix	Adopting Product (System Manager Release 8.1)													
System Manager Solution Deployment Manager - Centralized									Breeze				Avaya Aura®	
Functionality	Appliance Virtualization Platform	System Manager	Session Manager	Communication Manager	CM Adjuncts (MM, TN Boards, Gateways)	Branch Session Manager	AVP Utilities	CM Messaging	(w/ Presence Snap-in)	Secure Access Gateway	WebLM	Application Enablement Services	Media Server	Session Border Controller (SBCE 8.0.1)
Custom Patching Deployment	n/a	N	Y	Y	n/a	Y	Y	Y	N	N	Y [7.0.1 onwards]	Y	N	Y
Service/Feature Pack Deployment	Y [Other than AVP hosting System Manager]	N	Y	Y	n/a	Y	Y	Y	N	N	N	Y	N	N
Automated Migrations R7.x to R8.0/R8.1 (analysis and pre-upgrade checks) [Target Platform: AVP / customer VMware]	Y [Other than AVP hosting System Manager]	Y	Y	Y	n/a [Covered as Firmware Updates]	Y	Y	Y	N (Breeze Upgrade Supported from Breeze 3.3 Onwards)	N	Y	Y	N	N

Solution Deployment Manager Adopter Matrix	Adopting Product (System Manager Release 8.1)													
System Manager Solution Deployment Manager - Centralized									Breeze				Avaya Aura®	
Functionality	Appliance Virtualization Platform	System Manager	Session Manager	Communication Manager	CM Adjuncts (MM, TN Boards, Gateways)	Branch Session Manager	AVP Utilities	CM Messaging	(w/ Presence Snap-in)	Secure Access Gateway	WebLM	Application Enablement Services	Media Server	Session Border Controller (SBCE 8.0.1)
Automated Migrations R6.x to R7.x/8.0/R8.1 (analysis and pre-upgrade checks)	n/a	N	Y[1]	Y	n/a [Covered as Firmware Updates]	Y	Y	Y	N	N	N	N	N	N
Automated Migrations R6.x to 7.x/8.0/8.1 [Source Platform: System Platform] [Target Platform: AVP / customer VMware]	n/a	N [Only using SDM Client]	Y[1] [Bare Metal which is not on SP]	Y	n/a [Covered as Firmware Updates]	Y	Y	Y	N	N	N	N	N	N
Automated Migrations R6.x to 7.x/8.0/8.1 [Source Platform: System Platform] [Target Platform: AVP / customer VMware]	n/a	N	Y[1] [Bare Metal which is not on SP]	Y	n/a [Covered as Firmware Updates]	Y	Y	Y	N	N	N	N	N	N
Automated Migrations R 5.2.1 to 7.x/8.0/8.1	N	N	N	Y	N	N	N	Y	N	N	N	N	N	N

Solution Deployment Manager Adopter Matrix	**Adopting Product (System Manager Release 8.1)**													
System Manager Solution Deployment Manager - Centralized									Breeze				Avaya Aura®	
Functionality	Appliance Virtualization Platform	System Manager	Session Manager	Communication Manager	CM Adjuncts (MM, TN Boards, Gateways)	Branch Session Manager	AVP Utilities	CM Messaging	(w/ Presence Snap-in)	Secure Access Gateway	WebLM	Application Enablement Services	Media Server	Session Border Controller (SBCE 8.0.1)
Firmware Updates	n/a	n/a	n/a	n/a	Y	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Scheduler (upgrades and patching)	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N
Virtual Machine Management (start, stop, reset, status, dashboard)	Y	N	Y	Y	n/a	Y	Y	Y	Y	Y	Y	Y	Y	N
Solution Deployment Manager RBAC Available	n/a	Y	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Create Software Library	n/a	Y	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Support for changing VM Flexible Footprint	n/a	Y [Only using SDM Client]	Y	Y	n/a	Y	n/a	Y	Y	Y	Y	Y	Y	N
Change Network Parameters	Y	n/a	n/a	n/a	n/a	n/a	Y	n/a	n/a	n/a	n/a	n/a	n/a	n/a

n/a: Not Applicable Y: Yes N: No

Y[1]: Session Manager Bare Metal which is not on System Platform.

Y[2]: SBCE OVA Deployment supported only using the SDM Client and not SMGR SDM

AVP: Appliance Virtualization Platform

VMware: Virtualized Environment

Avaya Aura® Presence Services

What's new in Presence Services Release 8.1.4

For more information see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

What's new in Presence Services Release 8.1.3

For more information see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

What's new in Presence Services Release 8.1.2

For more information see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

What's new in Presence Services Release 8.1.1

For more information see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

Required artifacts for Presence Services Release 8.1.4

The following section provides Presence Services downloading information. For deployment and upgrade procedure, see product-specific deployment and upgrade documents on the Avaya Support website.

Filename	PLDS ID	File size	Version number	Comments
PresenceServices-Bundle-8.1.4.0.28.zip	PS080104000	170 MB	PresenceServices-8.1.4.0.69.svar	Requires the use of Breeze 3.7 as a platform (minimum release)

Required artifacts for Presence Services Release 8.1.3

The following section provides Presence Services downloading information. For deployment and upgrade procedure, see product-specific deployment and upgrade documents on the Avaya Support website.

Filename	PLDS ID	File size	Version number	Comments
PresenceServices-Bundle-8.1.3.0.88.zip	PS080103000	167 MB	PresenceServices-8.1.3.0.87.svar	Requires the use of Breeze 3.7 as a platform (minimum release)

Required artifacts for Presence Services Release 8.1.2

The following section provides Presence Services downloading information. For deployment and upgrade procedure, see product-specific deployment and upgrade documents on the Avaya Support website.

Filename	PLDS ID	File size	Version number	Comments
PresenceServices-Bundle-8.1.2.0.140.zip	PS080102000	163 MB	PresenceServices-8.1.2.0.27.svar	Requires the use of Breeze 3.6 as a platform (minimum release)

Required artifacts for Presence Services Release 8.1.1

The following section provides Presence Services downloading information. deployment and upgrade procedure, see product-specific deployment and upgrade documents on the Avaya Support website.

Filename	PLDS ID	File size	Version number	Comments
PresenceServices-Bundle-8.1.1.0.354.zip	PS080101000	164 MB	PresenceServices-8.1.1.0.35. svar	Requires the use of Breeze 3.6 as a platform (minimum release)

Required artifacts for Presence Services Release 8.1

The following section provides Presence Services downloading information. For deployment and upgrade procedure, see product-specific deployment and upgrade documents on the Avaya Support website.

Filename	PLDS ID	File size	Version number	Comments
PresenceServices-Bundle-8.1.0.0.399.zip	PS080100000	165 MB	PresenceServices-8.1.0.0.278.svar	Requires the use of Breeze 3.6 as a platform

Required patches for Presence Services 8.1

Patches in 8.1.x are cumulative. Only the latest supported cumulative update of a Generally Available release will be available for download from the Avaya Support/PLDS website.

Be sure to apply any applicable service packs and cumulative updates posted on support.avaya.com to the system. Check support.avaya.com frequently for important software updates as documented in Product Support Notices and Release Notes.

It is important that any GA patches available at a later date be applied as part of all 8.1.x deployments.

Be sure to apply any applicable service packs and patches posted on support.avaya.com to the system after applying this release. Check support.avaya.com frequently for important software updates, as documented in Product Support Notices.

Presence Services 8 and above uses the following version string syntax:

<major>.<minor>.<feature pack>.<service pack>.<cumulative update>

Cumulative updates only change the fifth digit in the version string. You should only apply cumulative updates that match the same four leading digits of the version currently deployed. There may be special upgrade paths required when deploying releases where any of the four leading digits are incremented. Refer to the release notes for that release for more information.

For more details see PCN2103S on the Avaya Technical Support site.

Backing up the software

Presence Services software is mastered on the SYSTEM MANAGER. If you wish to back-up presence services configuration data, refer to System Manager Documentation.

Installing Presence Services Release 8.1.4

See the Avaya Aura® Presence Services Snap-in Reference document for instructions related to the deployment of the PS Release 8.1.4.

Note: To install the PS 8.1.4 SVAR, all previous versions of the PS SVAR will need to be uninstalled and the SVAR file needs to be deleted from the SMGR. This procedure (deleting previous versions of the SVAR from the SMGR) only needs to be performed when upgrading from releases older than 8.0.1. This procedure is not required when upgrading from 8.0.1 or newer versions.

Installing Presence Services Release 8.1.3

See the Avaya Aura® Presence Services Snap-in Reference document for instructions related to the deployment of the PS Release 8.1.3.

Note: To install the PS 8.1.3 SVAR, all previous versions of the PS SVAR will need to be uninstalled and the SVAR file needs to be deleted from the SMGR. This procedure (deleting previous versions of the SVAR from the SMGR) only needs to be performed when upgrading from releases older than 8.0.1. This procedure is not required when upgrading from 8.0.1 or newer versions.

Note: It is recommended to set the property "HTTP or HTTPS limit on connections per client" in Breeze Cluster Attributes page to 15 in clustered environments

Installing Presence Services Release 8.1.2

See the Avaya Aura® Presence Services Snap-in Reference document for instructions related to the deployment of the PS Release 8.1.2.

Note: To install the PS 8.1.2 SVAR, all previous versions of the PS SVAR will need to be uninstalled and the SVAR file needs to be deleted from the SMGR. This procedure (deleting previous versions of the SVAR from the SMGR) only needs to be performed when upgrading from releases older than 8.0.1. This procedure is not required when upgrading from 8.0.1 or newer versions.

Installing Presence Services Release 8.1.1

See the Avaya Aura® Presence Services Snap-in Reference document for instructions related to the deployment of the PS Release 8.1.1.

Note: To install the PS 8.1.1 SVAR, all previous versions of the PS SVAR will need to be uninstalled and the SVAR file needs to be deleted from the SMGR. This procedure (deleting previous versions of the SVAR from the SMGR) only needs to be performed when upgrading from releases older than 8.0.1. This procedure is not required when upgrading from 8.0.1 or newer versions.

Troubleshooting the installation

See the Avaya Aura® Presence Services Snap-in Reference document on the Avaya Support website for troubleshooting instructions.

Restoring software to the previous version

To revert to the previous version of the PS Snap-in refer to the upgrade instructions in the Avaya Aura® Presence Services Snap-in Reference document. The procedure to install the older SNAP-IN software is the same as the procedure for installing the new SNAP-IN software.

Migrating to the PS 8.1.X release from a PS 6.2.X release

Changes Affecting Migrations to 8.1

Avaya Aura® Presence Services 6.X loads cannot be migrated directly to PS 8.1.x Customers wishing to migrate from PS 6.X loads must first migrate to the latest available PS 7.1.X release. Once a migration has been completed to PS 7.X it will then be possible to upgrade to PS 8.1.X

For instructions on how to perform the migration from PS 6.2.X to release 7.X, refer to the documentation bundled with the Migration tool found in PLDS and refer to the release notes for the PS 7.X release.

Note: At the time of general availability of Presence Services 8.1.1 was announced, no patches were available for download from support.avaya.com. It is important that any GA patches available at a later date be applied as part of all 8.1.x deployments.

Note: To install the PS 8.1.1 SVAR, all previous versions of the PS SVAR will need to be uninstalled, and the SVAR file needs to be deleted from the SMGR. This procedure (deleting previous versions of the SVAR from the SMGR) only needs to be performed when upgrading from releases older than 8.0.1. This procedure is not required when upgrading from 8.0.1 or newer releases.

Migrations to release 8.1.x are supported from the following releases only:

Minimum required versions by Release

Release	**Minimum Required Version**
Avaya Aura® Presence Services 7.0	PresenceServices-7.0.0.0.1395.svar + any additional patch(es)
Avaya Aura® Presence Services 7.0 Service Pack 1	PresenceServices-7.0.0.1.1528.svar + any additional patch(es)
Avaya Aura® Presence Services 7.0 Feature Pack 1	PresenceServices-7.0.1.0.872.svar + any additional patch(es)
Avaya Aura® Presence Services 7.1	PresenceServices-7.1.0.0.614.svar + any additional patch(es)
Avaya Aura® Presence Services 7.1 Feature Pack 2	PresenceServices-7.1.2.0.231.svar + any additional patch(es)
Avaya Aura® Presence Services 8.0	PresenceServices-8.0.0.0.294.svar + any additional patch(es)
Avaya Aura® Presence Services 8.0 Feature Pack 1	PresenceServices-8.0.1.0.301.svar + any additional patch(es)
Avaya Aura® Presence Services 8.0 Feature Pack 2	PresenceServices-8.0.2.0.253.svar + any additional patch(es)
Avaya Aura® Presence Services 8.1	PresenceServices-8.1.0.0.277.svar + any additional patch(es)
Avaya Aura® Presence Services 8.1.1	PresenceServices-8.1.1.0.26.svar + any additional patch(es)
Avaya Aura® Presence Services 8.1.2	PresenceServices-8.1.2.0.27.svar + any additional patch(es)
Avaya Aura® Presence Services 8.1.3	PresenceServices-8.1.3.0.87.svar + any additional patch(es)
Avaya Aura® Presence Services 8.1.4	PresenceServices-8.1.4.0.69. svar + any additional patch(es)

Upgrade References to Presence Services Release 8.1.4

Upgrade Quick Reference	Download	Prerequisite Downloads
Presence Services Customer Documentation	PresenceServices-Bundle-8.1.4.0.28.zip (PLDS ID: PS080104000)	Breeze 3.7 or higher Platform OVA – PS 8.1.4 is only compatible with Breeze 3.7 and newer platform loads.

Upgrade References to Presence Services Release 8.1.3

Upgrade Quick Reference	Download	Prerequisite Downloads
Presence Services Customer Documentation	PresenceServices-Bundle-8.1.3.0.88.zip (PLDS ID: PS080103000)	Breeze 3.7 or higher Platform OVA – PS 8.1.3 is only compatible with Breeze 3.7 and newer platform loads.

Upgrade References to Presence Services Release 8.1.2

Upgrade Quick Reference	Download	Prerequisite Downloads
Presence Services Customer Documentation	PresenceServices-Bundle-8.1.2.0.128.zip (PLDS ID: PS080102000)	Breeze 3.6 or higher Platform OVA – PS 8.1.2 is only compatible with Breeze 3.6 and newer platform loads.

Upgrade References to Presence Services Release 8.1.1

Upgrade Quick Reference	Download	Prerequisite Downloads
Presence Services Customer Documentation	PresenceServices-Bundle-8.1.1.0.163.zip (PLDS ID: PS080101000)	Breeze 3.6 or higher Platform OVA – PS 8.1.1 is only compatible with Breeze 3.6 and newer platform loads.

Interoperability and requirements/Applicability for Release 8.1.X

Note: See the Avaya Compatibility Matrix application for full Avaya product compatibility information.

Software Development Kit

In PS Release 8.1.0.0, the Local Presence Service (LPS) SDK (Software Development Kit) will no longer be supported, and an 8.1.0.0 version of the SDK will not be published. Existing applications using the older SDK will still be usable in 8.1.0.0, but users are encouraged to update their applications to use the REST interface or the JAVA API in the PS Connector.

The Local Presence Service (LPS) SDK (Software Development Kit) is available as follows:

SDK Filename	SDK Version	Presence Services Compatibility
PresenceServices-LPS-SDK-8.0.2.0.241.zip	8.0.2	PS 8.0.2
PresenceServices-LPS-SDK-8.0.1.0.767.zip	8.0.1	PS 8.0.1
PresenceServices-LPS-SDK-8.0.0.0.147.zip	8.0.0	PS 8.0.0, PS 7.1.2, PS 7.1.0 and PS 7.0.1
PresenceServices-LPS-SDK-7.1.2.0.182.zip	7.1.2	PS 7.1.2, PS 7.1.0 and PS 7.0.1
PresenceServices-LPS-SDK-7.1.0.0.556.zip	7.1.0	PS 7.1 and PS 7.0.1

For more information about the Presence Services SDKs and other Avaya SDKs, refer to Avaya DevConnect at http://devconnect.avaya.com.

Functionality not supported in Presence Services 8.1.x.x

Functionality not supported in Presence Services 8.1.4

Avaya Multimedia Messaging – federation with AMM (either via XMPP or REST) is no longer supported as of PS 8.0.1. It is still possible to deploy PS and AMM in the same solution, but the two applications cannot be federated. PS 8.1.3 supports all of the AMM feature set and in most cases, the AMM application can be eliminated

Functionality not supported in Presence Services 8.1.3

Avaya Multimedia Messaging – federation with AMM (either via XMPP or REST) is no longer supported as of PS 8.0.1. It is still possible to deploy PS and AMM in the same solution, but the two applications cannot be federated. PS 8.1.3 supports all of the AMM feature set and in most cases, the AMM application can be eliminated

Functionality not supported in Presence Services 8.1.2

Avaya Multimedia Messaging – federation with AMM (either via XMPP or REST) is no longer supported as of PS 8.0.1. It is still possible to deploy PS and AMM in the same solution, but the two applications cannot be federated. PS 8.1.2 supports all of the AMM feature set and in most cases, the AMM application can be eliminated.

Functionality not supported in Presence Services 8.1.1

Avaya Multimedia Messaging – federation with AMM (either via XMPP or REST) is no longer supported as of PS 8.0.1. It is still possible to deploy PS and AMM in the same solution, but the two applications cannot be federated. PS 8.1.1 supports all of the AMM feature set and in most cases, the AMM application can be eliminated.

Fixes in Presence Services Release 8.1.4

The following issues are resolved in cumulative updates to the 8.1.4 release:

ID	Minimum conditions	Visible symptoms	Release found in
PSNG-9492		Super-cluster: IM and presence does not work between users on different clusters	8.1.3.0
PSNG-10267		SFTP: Old messages are not uploaded to the SFTP server after SFTP server is up again	8.1.3.0
PSNG-10262		Super-cluster: Status of super cluster contact always displays Offline after watcher has logged in IX Workplace	8.1.3.0
PSNG-9382		DevConnectSupport Forum: EventDelivery url returning 400 Bad Request	8.1.2
PSNG-10809		Presence service failure when resuming cluster servers	8.1
PSNG-11093		Presence of favorite user's missing in 1XC clients and does not show After an upgrade to 8.1.3	8.1.3

PSNG-10348		Some users are unable to edit their presence and are showing in a "stuck" state	
Note		Various Performance fixes have been added to 8.1.4 release	8.1.2/8.1.3
Note	Existing AMM deployments	There is a Migration path from existing AMM deployments to use the PS 8.1.3/8.1.4 application. Existing AMM deployments that are to migrate to PS 8.1.4 should be treated as new installs.	

Fixes in Presence Services Release 8.1.3

The following issues are resolved in cumulative updates to the 8.1.3 release:

ID	Minimum conditions	Visible symptoms	Release found in
PSNG-9553		presHealthCheck for ID cert fails	8.1.2.0
PSNG-9092		IM's are not updating correctly	8.1.0.0
PSNG-8943		Unknown state in manual tuple is causing nullpointerexception on PS code	8.1.3.0
PSNG-8783		SFTP Message Archiving not working, issue with Remote Path	8.1.1.0
PSNG-9685		Deskphone’s showing question marks for Contact’s Presence	8.1.2.0
PSNG-9014		support multi-FE-pools deployments	8.0.1.0
PSNG-9347		Customer is losing Multimedia Messaging, the snap-in service must be restarted in order to have messaging enabled again.	8.1.1.0

Fixes in Presence Services Release 8.1.2

The following issues are resolved in cumulative updates to the 8.1.2 release:

ID	Minimum conditions	Visible symptoms	Release found in
PSNG-7897		[PS 8.1.1]: Away timer should be stopped when upon publishing the “In-a-Call” state or “DND” state or “Offline” state	8.1.1.0
PSNG-7869		Bug - TestApp doesn't receive htmlBody content when other user sent message using font formatted via PS.	8.1.1.0
PSNG-7514		Invalid bsid in MM rest client should be rejected with 403 forbidden	8.1.2.0
PSNG-7424		[PS 8.1.2]: Presence API should display a warning when sending message exceeding 2048 characters	8.1.2.0
PSNG-6474		[PS 8.1.2] Presence state is not changed after it has been expired in Service Profiles level	8.1.2.0
PSNG-6473		[PS 8.1.2] Failed to set manual presence state from client using REST API	8.1.2.0
PSNG-6222		Customer Escalation: Cannot add/edit presence services after SMGR upgrade from 6.3. to 8.1	8.1.0.0
PSNG-6220		Could not open attachment sent from PS to Skype for Business user	8.1.1.0

Fixes in Presence Services Release 8.1.1

The following issues are resolved in cumulative updates to the 8.1.1 release:

ID	Minimum conditions	Visible symptoms	Release found in
PSNG-6064		No contact presence for geographically redundant deployments	8.1.0.0

Fixes in Presence Services Release 8.1

The following issues are resolved in cumulative updates to the 8.1 release:

ID	Minimum conditions	Visible symptoms	Release found in
PSNG-6055		Presence SIP subscription retry-after time too long	7.1.2.0
PSNG-6040		Fix PS vulnerability PSC not closing collab bus on context destroy to XML External Entity (XXE) attack	8.1.0.0
PSNG-6030		PSC not closing collab bus on context destroy	7.1.2.0
PSNG-5948		AES Collector 940x digital set interaction with 1XC	7.1.2.0
PSNG-5940		AEM Metrics active subscriptions gauge is negative	8.0.2.0
PSNG-5929		AES Collector not publishing Available for 9408/9404 digital sets	7.1.2.0
PSNG-5863		Disabling AES Collector does not remove DND state if SAC was enabled	7.1.2.0

Known issues and workarounds in Presence Services Release 8.1.4

ID	Minimum conditions	Visible symptoms	Workaround
PSNG-11311		InterPS Federation - Could not play audio which was recorded and sent from InterPS federated user	Inter PS Federation issues would be addressed by a patch after 8.1.4
PSNG-11309		InterPS Federation - After a user has been re-added to a p2p conversation, it could not receive new messages in that conversation	Inter PS Federation issues would be addressed by a patch after 8.1.4
PSNG-10915		2 PSs on different SMGRs: Unable to receive message after re-joining conversation	NA
PSNG-9261		S4B with hybrid user: Skype does not change to On-a-call when PS make call.	NA

Known issues and workarounds in Presence Services Release 8.1.3

ID	Minimum conditions	Visible symptoms	Workaround
PSNG-10262		In Super Cluster deployments, initially he may not be able to see the correct status of his contacts	If the contact concerned changes his/her state manually/automatically, correct status will be shown
PSNG-10267		SFTP: Old messages are not uploaded to the SFTP server after SFTP server is up again	NA
PSNG-10244		The subject is not sent to recipient in first time starting a new conversation between 2 PSs on 2 SMGRs	NA
PSNG-9382		DevConnectSupport Forum: EventDelivery url returning 400 Bad Request	NA
PSNG-9085		PMM Amazon S3 bucket support as attachment storage	NA
Note		After an Avaya contact is removed from an XMPP federated client, presence does not render if the Avaya contact is re-added to the federated user.	Use either of the two solutions: 1. Toggle the favorite flag for the federated user in the Avaya client 2. Logout and log back into the Avaya client
Note	PS federation with Zang.	Federation between Avaya Aura Presence Services and Zang Cloud Services is supported only in geographical regions where Zang is fully operational	There is no work-around for this limitation. PS federation with Zang is only supported only in geographical regions where Zang is fully operational.
Note	PS Geo deployments	The AMM feature set (Equinox Multi Media messaging) which was added to the PS application in 8.0.1 is not compatible with Geo deployments.	The work-around is to deploy in a non-geo environment. The existing AMM application does not support geo-redundancy so no functionality is lost. Support for Equinox multimedia messaging in a geo deployment will be added in a future release.
Note	Federated deployments	The multimedia attachments associated with Equinox clients can't be exchanged with any federated clients such as Skype for business, or Jabber.	There is no work-around. This functionality may be delivered in a future release.
Note	PS deployments hosting Equinox Multimedia Messaging clients	It is mandatory that users' messaging addresses (as configured in SMGR) match the users' e-mail address as configured in the LDAP.	This is a mandatory configuration and is required for compatibility with the Equinox clients.
Note	PS deployments hosting Equinox Multimedia	Equinox clients must be configured via AADS.	This is a mandatory configuration and is required for compatibility with the Equinox clients.

ID	Minimum conditions	Visible symptoms	Workaround
	Messaging clients.		
Note	PS deployments hosting Equinox Multimedia Messaging clients using AADS 7.1.3.2	When AADS 7.1.3.2 is used only single node PS clusters are supported. Multi node PS clusters and HA deployments are not supported,	On AADS 7.1.3.2 set the ESM_MULTISITE_ENABLED attribute to 0 and manually set the ESMSRVR attribute to be the FQDN of the Breeze cluster. Or alternatively, use AADS 7.1.5 which will be released in January 2019.
Note	Existing AMM deployments	There is no direct upgrade path from existing AMM deployments to use the PS 8.1.2 application.	Existing AMM deployments that are to migrate to PS 8.1.2 should be treated as new installs.
Note	HA deployments	HA deployments are only supported when using Breeze profile 5. HA deployments are not supported with Breeze profiles 2, 3, and 4.	If HA is desired deploy the PS SNAP-IN on a Breeze profile 5 clusters with an appropriate number of VMs in the cluster.

Known issues and workarounds in Presence Services Release 8.1.2

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Minimum conditions	Visible symptoms	Workaround
Note		After an Avaya contact is removed from an XMPP federated client, presence does not render if the Avaya contact is re-added to the federated user.	Use either of the two solutions: 1. Toggle the favorite flag for the federated user in the Avaya client 2. Logout and log back into the Avaya client
Note	PS federation with Zang.	Federation between Avaya Aura Presence Services and Zang Cloud Services is supported only in geographical regions where Zang is fully operational	There is no work-around for this limitation. PS federation with Zang is only supported only in geographical regions where Zang is fully operational.
Note	PS Geo deployments	The AMM feature set (Equinox Multi Media messaging) which was added to the PS application in 8.0.1 is not compatible with Geo deployments.	The work-around is to deploy in a non-geo environment. The existing AMM application does not support geo-redundancy so no functionality is lost. Support for Equinox multimedia messaging in a geo deployment will be added in a future release.
Note	Federated deployments	The multimedia attachments associated with Equinox clients can’t be exchanged with any federated clients such as Skype for business, or Jabber.	There is no work-around. This functionality may be delivered in a future release.

ID	Minimum conditions	Visible symptoms	Workaround
Note	PS deployments hosting Equinox Multimedia Messaging clients	It is mandatory that users' messaging addresses (as configured in SMGR) match the users' e-mail address as configured in the LDAP.	This is a mandatory configuration and is required for compatibility with the Equinox clients.
Note	PS deployments hosting Equinox Multimedia Messaging clients.	Equinox clients must be configured via AADS.	This is a mandatory configuration and is required for compatibility with the Equinox clients.
Note	PS deployments hosting Equinox Multimedia Messaging clients using AADS 7.1.3.2	When AADS 7.1.3.2 is used only single node PS clusters are supported. Multi node PS clusters and HA deployments are not supported,	On AADS 7.1.3.2 set the ESM_MULTISITE_ENABLED attribute to 0 and manually set the ESMSRVR attribute to be the FQDN of the Breeze cluster. Or alternatively, use AADS 7.1.5 which will be released in January 2019.
Note	Existing AMM deployments	There is no direct upgrade path from existing AMM deployments to use the PS 8.1.2 application.	Existing AMM deployments that are to migrate to PS 8.1.2 should be treated as new installs.
Note	HA deployments	HA deployments are only supported when using Breeze profile 5. HA deployments are not supported with Breeze profiles 2, 3, and 4.	If HA is desired deploy the PS SNAP-IN on a Breeze profile 5 clusters with an appropriate number of VMs in the cluster.

Known issues and workarounds in Presence Services Release 8.1.1.0

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Minimum conditions	Visible symptoms	Workaround
PSNG-6220	Could not open attachment send from PS to Skype for Business user	Could not open an attachment sent from PS to Skype for Business user	Enable InterPS-Federation, reboot Skype for Business Server and Breeze
Note		After an Avaya contact is removed from an XMPP federated client, presence does not render if the Avaya contact is re-added to the federated user.	Use either of the two solutions: 1. Toggle the favorite flag for the federated user in the Avaya client 2. Logout and log back into the Avaya client
Note	PS federation with Zang.	Federation between Avaya Aura Presence Services and Zang Cloud Services is supported only in geographical regions where Zang is fully operational	There is no work-around for this limitation. PS federation with Zang is only supported only in geographical regions where Zang is fully operational.
Note	PS Geo deployments	The AMM feature set (Equinox Multi Media messaging) which was added to the PS application in	The work-around is to deploy in a non-geo environment. The existing AMM application does not support

ID	Minimum conditions	Visible symptoms	Workaround
		8.0.1 is not compatible with Geo deployments.	geo-redundancy so no functionality is lost. Support for Equinox multimedia messaging in a geo deployment will be added in a future release.
Note	Federated deployments	The multimedia attachments associated with Equinox clients can't be exchanged with any federated clients such as Skype for business, or Jabber.	There is no work-around. This functionality may be delivered in a future release.
Note	PS deployments hosting Equinox Multimedia Messaging clients	It is mandatory that users' messaging addresses (as configured in SMGR) match the users' e-mail address as configured in the LDAP.	This is a mandatory configuration and is required for compatibility with the Equinox clients.
Note	PS deployments hosting Equinox Multimedia Messaging clients.	Equinox clients must be configured via AADS.	This is a mandatory configuration and is required for compatibility with the Equinox clients.
Note	PS deployments hosting Equinox Multimedia Messaging clients using AADS 7.1.3.2	When AADS 7.1.3.2 is used only single node PS clusters are supported. Multi node PS clusters and HA deployments are not supported,	On AADS 7.1.3.2 set the ESM_MULTISITE_ENABLED attribute to 0 and manually set the ESMSRVR attribute to be the FQDN of the Breeze cluster. Or alternatively, use AADS 7.1.5 which will be released in January 2019.
Note	Existing AMM deployments	There is no direct upgrade path from existing AMM deployments to use the PS 8.0.1 application.	Existing AMM deployments that are to migrate to PS 8.0.1 should be treated as new installs.
Note	HA deployments	HA deployments are only supported when using Breeze profile 5. HA deployments are not supported with Breeze profiles 2, 3, and 4.	If HA is desired deploy the PS SNAP-IN on a Breeze profile 5 clusters with an appropriate number of VMs in the cluster.

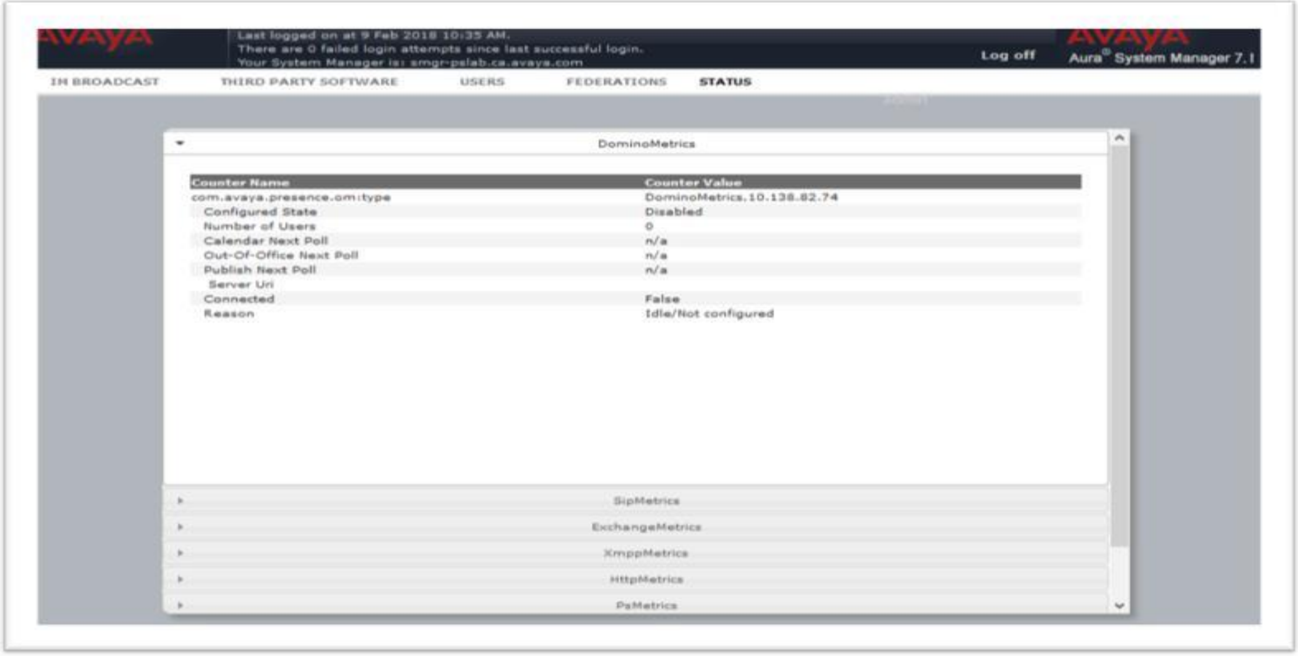
Known issues and workarounds in Presence Services Release 8.1

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Minimum conditions	Visible symptoms	Workaround
PSNG-2630	Avaya Aura is federated with Microsoft Lync	There is no message notification when Lync sends a chat message to 1XC in DND state,	There is no workaround for this issue.
PSNG-1379	Clear Logs in the EDP EM for Presence Services does not clear logs	The "Clear Logs" button on the EDP EM does not have any effect on the ps.log file.	There is no workaround for this issue.

ID	Minimum conditions	Visible symptoms	Workaround
Note	PS federation with Zang.	Federation between Avaya Aura Presence Services and Zang Cloud Services is supported only in geographical regions where Zang is fully operational	There is no work-around for this limitation. PS federation with Zang is only supported only in geographical regions where Zang is fully operational.
Note	PS Geo deployments	The AMM feature set (Equinox Multi Media messaging) which was added to the PS application in 8.0.1 is not compatible with Geo deployments.	The work-around is to deploy in a non-geo environment. The existing AMM application does not support geo-redundancy so no functionality is lost. Support for Equinox multimedia messaging in a geo deployment will be added in a future release.
Note	Federated deployments	The multimedia attachments associated with Equinox clients can't be exchanged with any federated clients such as Skype for business, or Jabber.	There is no work-around. This functionality may be delivered in a future release.
Note	PS deployments hosting Equinox Multimedia Messaging clients	It is mandatory that users' messaging addresses (as configured in SMGR) match the users' e-mail address as configured in the LDAP.	This is a mandatory configuration and is required for compatibility with the Equinox clients.
Note	PS deployments hosting Equinox Multimedia Messaging clients.	Equinox clients must be configured via AADS.	This is a mandatory configuration and is required for compatibility with the Equinox clients.
Note	PS deployments hosting Equinox Multimedia Messaging clients using AADS 7.1.3.2	When AADS 7.1.3.2 is used only single node PS clusters are supported. Multi node PS clusters and HA deployments are not supported,	On AADS 7.1.3.2 set the ESM_MULTISITE_ENABLED attribute to 0 and manually set the ESMSRVR attribute to be the FQDN of the Breeze cluster. Or alternatively, use AADS 7.1.5 which will be released in January 2019.
Note	Existing AMM deployments	There is no direct upgrade path from existing AMM deployments to use the PS 8.0.1 application.	Existing AMM deployments that are to migrate to PS 8.0.1 should be treated as new installs.
Note	HA deployments	HA deployments are only supported when using Breeze profile 5. HA deployments are not supported with Breeze profiles 2, 3 and 4.	If HA is desired deploy the PS SNAP-IN on a Breeze profile 5 clusters with an appropriate number of VMs in the cluster.

Note: The Presence Services Admin Web GUI, as shown below, is disabled by default in PS 8.1.1.0

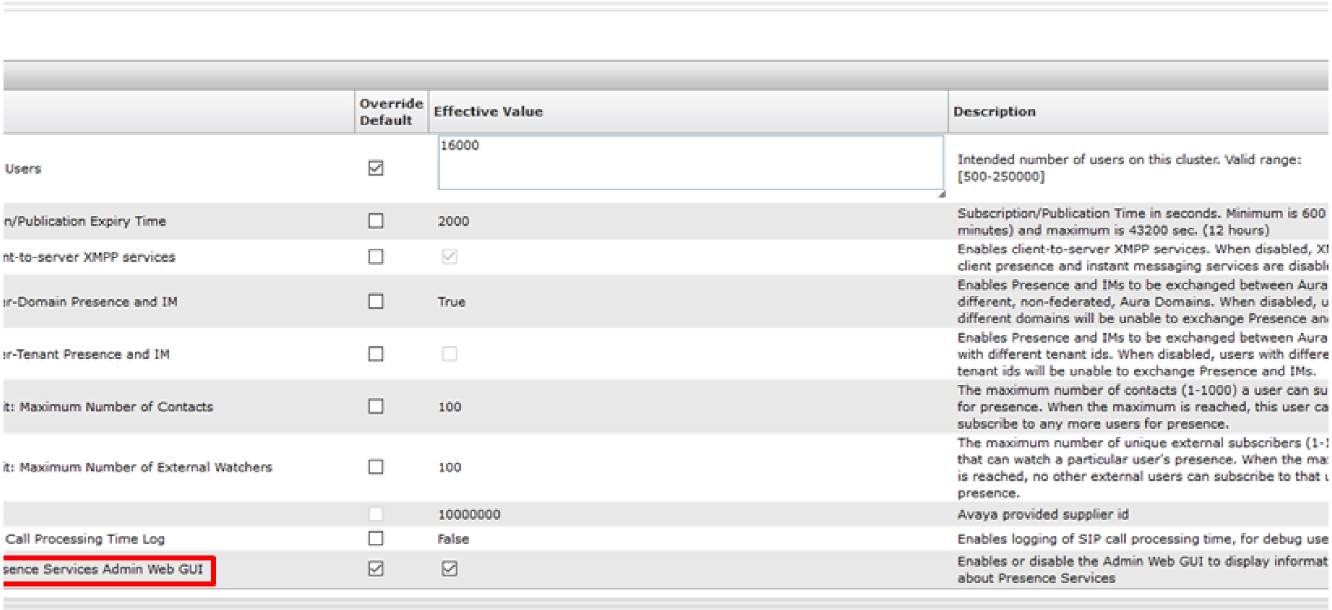


Last logged on at 9 Feb 2018 10:35 AM.
There are 0 failed login attempts since last successful login.
Your System Manager is: smgr-pslab.ca.avaya.com

DominoMetrics

Counter Name	Counter Value
com.avaya.presence.om:type	DominoMetrics.10.138.82.74
Configured State	Disabled
Number of Users	0
Calendar Next Poll	n/a
Out-Of-Office Next Poll	n/a
Publish Next Poll	n/a
Server Uri	
Connected	False
Reason	Idle/Not configured

To enable the Presence Services Admin Web GUI, override the “Enable Presence Services Admin Web GUI” service attribute as shown below:



	Override Default	Effective Value	Description
Users	☑	16000	Intended number of users on this cluster. Valid range: [500-250000]
n/Publication Expiry Time	☐	2000	Subscription/Publication Time in seconds. Minimum is 600 minutes) and maximum is 43200 sec. (12 hours)
nt-to-server XMPP services	☐	☑	Enables client-to-server XMPP services. When disabled, XI client presence and instant messaging services are disabl
r-Domain Presence and IM	☐	True	Enables Presence and IMs to be exchanged between Aura different, non-federated, Aura Domains. When disabled, u different domains will be unable to exchange Presence an
r-Tenant Presence and IM	☐	☐	Enables Presence and IMs to be exchanged between Aura with different tenant ids. When disabled, users with differe tenant ids will be unable to exchange Presence and IMs.
t: Maximum Number of Contacts	☐	100	The maximum number of contacts (1-1000) a user can su for presence. When the maximum is reached, this user ca subscribe to any more users for presence.
t: Maximum Number of External Watchers	☐	100	The maximum number of unique external subscribers (1-1 that can watch a particular user's presence. When the ma is reached, no other external users can subscribe to that u presence.
	☐	10000000	Avaya provided supplier id
Call Processing Time Log	☐	False	Enables logging of SIP call processing time, for debug use
sence Services Admin Web GUI	☑	☑	Enables or disable the Admin Web GUI to display informat about Presence Services

Avaya Aura® Application Enablement Services

What's new in Application Enablement Services 8.1.x.x

What's new in Application Enablement Services Release 8.1.3.1

For more information see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

What's new in Application Enablement Services Release 8.1.3

For more information see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

What's new in Application Enablement Services Release 8.1.2.1 and 8.1.2.1.1

For more information see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

What's new in Application Enablement Services Release 8.1.2

For more information see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

As of 8.1.2, customers utilizing AVP or VMware based systems are able to activate disk encryption during OVA installation. To support ongoing maintenance of this feature, the following commands have been added in the 8.1.2 release: ***encryptionStatus, encryptionRemoteKey, encryptionPassphrase,*** and ***encryptionLocalKey***. Note that these commands are only applicable if disk encryption is enabled using the Avaya OVA methods. These commands are not to be used if the customer has provided their own disk encryption using other methods.

What's new in Application Enablement Services Release 8.1.1

For more information see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

Security Service Packs

Security Service Packs (Linux Security Update – LSU)

AE Services releases Linux Security Updates (LSUs) aligned with the application release cycle. Beginning December 2020, LSU will also be released on a more frequent cadence. LSU required artifacts and fix IDs will no longer be tracked in the Release Notes. Historical information on LSU artifacts and fix IDs already in the Release Notes will be maintained for reference.

For further information on LSU contents and installation procedures for AE Services 8.1.x, please see its respective **PSN(s)**:

- **PSN020481u - Avaya Aura® Application Enablement (AE) Services 8.1.2 and greater Linux Security Updates**

- **PSN020452u - Avaya Aura® Application Enablement (AE) Services 8.1.1 Linux Security Updates**.
- **PSN020434u - Avaya Aura® Application Enablement (AE) Services 8.1 Linux Security Updates**.

It is not necessary to apply AES 8.1 LSU 1 on top of AES 8.1.1 itself because AES 8.1.1 includes all the same updates.

Refer to **Upgrading to AE Services 8.1.2** section for more details on mandatory installation of LSU patches.

LSUs are not intended for use by "software-only" customers

Required artifacts for Application Enablement Services Release 8.1.x.x

Required artifacts for Application Enablement Services Release 8.1.3.1

Filename	PLDS ID	File size	Version number	Comments
aesvcs-8.1.3.1.0.7-servicepack.bin	AES00000851	191 MB (195,402 KB)	AES-8.1.3.1.0.7-0	Avaya Aura® Application Enablement Services 8.1.3.1 Service Pack Installer MD5 Checksum: 4b768813faa9d9751ff0e2e85cfc9160 Please refer to PCN2102S for additional details

Required artifacts for Application Enablement Services Release 8.1.3

Filename	PLDS ID	File size	Version number	Comments
aesvcs-8.1.3.0.0.25-featurepack.bin	AES00000823	190.74 MB (195,317.38 KB)	AES-8.1.3.0.0.25-0	Avaya Aura® Application Enablement Services 8.1.3 Feature Pack Installer MD5 Checksum: 4326313f66dd69d5f4fc7fef7a59ed0c Please refer to PCN2102S for additional details
812Plus_LSUPatch2.bin	AES00000824	354.63 MB (363145.52 KB)	LSU-8.1.2Plus-2	Avaya Aura® AE Services 8.1.2_Plus Linux Security Update Patch 2 MD5 Checksum: 5114765dd28aacf6410bdfff92c4dc74 Please refer to PSN020481u for additional details

Required artifacts for Application Enablement Services Release 8.1.2.1 and 8.1.2.1.1

The following section provides Application Enablement Services downloading information.

Please refer to PSN020489 for additional details.

Filename	PLDS ID	File size	Version number	Comments
aesvcs-8.1.2.1.0.6-servicepack.bin	AES00000820	159.42 MB (163, 255.1KB)	AES-8.1.2.1.0.6-0	Avaya Aura® Application Enablement Services 8.1.2.1 Service Pack MD5 Checksum: 1ab63845fd028e2d3373479162358e1c Please refer to PCN2102S for additional details
812Plus_LSUPatch1.bin	AES00000819	134.15MB (137,372 KB)	LSU-8.1.2Plus-1	Avaya Aura® AE Services 8.1.2_Plus Linux Security Update Patch 1 MD5 Checksum 59dbf358241cb9ee8bb660807648953f Please refer to PSN020481 for additional details.
aesvcs-8.1.2.1.1-superpatch.bin	AES00000822	File Size: 108.33 MB (110934.34 KB)	AES-8.1.2.1.1.6-0	Avaya Aura® AE Services 8.1.2.1 Super Patch 1 MD5 Checksum: 94fbd3873a350ea0cc8afac631105346 SHA1: 59273c38977ca93445bcd6bce32f8a0563f13924 SHA256 : bedb39b7496dbe9402630aed3fdf87a3445214860257e12d8c8f1888b40e15a5 Please refer to PSN020489 for additional details

Required artifacts for Application Enablement Services Release 8.1.2

The following section provides Application Enablement Services downloading information.

Filename	PLDS ID	File size	Version number	Comments
AES-8.1.2.0.0.9.20200224-e67-00.ova	AES00000796	2,656.66 MB (2,720,420.5 KB)	8.1.2.0.0.9	Avaya Aura® Application Enablement Services 8.1.2 Aura® OVA Media MD5 Checksum: 2f2343ccd5d7688ca7f4661b6685d427

Filename	PLDS ID	File size	Version number	Comments
aesvcs-8.1.2.0.0.9-featurepack.bin	AES00000797	156.33MB (160082.92 KB)	8.1.2.0.0.9	Avaya Aura® Application Enablement Services 8.1.2 Feature Pack Installer MD5 Checksum: a81f57dfb396dc1a3ba16fa804b7fc54
81_LSUPatch2.bin	AES00000801	247 MB (253,932 KB)	LSU-8.1-2	Avaya Aura® AE Services 8.1 Linux Security Update Patch 2 Description: Avaya Aura® AE Services 8.1 Linux Security Update Patch 2. Please refer to PSN020434u for additional details.
811_LSUPatch2.bin	AES00000802	247 MB (253,932 KB)	LSU-8.1.1-2	Avaya Aura® AE Services 8.1.1 Linux Security Update Patch 2 Description: Avaya Aura® AE Services 8.1.1 Linux Security Update Patch 2. Please refer to PSN020452u for additional details.

Required artifacts for Application Enablement Services Release 8.1.1.0.2

The following section provides Application Enablement Services downloading information.

Filename	PLDS ID	File size	Version number	Comments
aesvcs-8.1.1.0.2-superpatch.bin	AES00000795	113.93 MB (116,666.8 KB)	8.1.1.0.2	Avaya Aura® AE Services 8.1.1 Super Patch 2 Please refer to ***PSN020440u- Avaya Aura® Application Enablement (AE) Services 8.1.1 Super Patches*** for additional details MD5 Checksum: 11257b87d584112f4bd1c911831d7cf8 SHA1: 79e6081df86a08f9126157e1b4470ec218d2a5cb SHA256 : b13a9ea912a1f704d1ecf5d72b6e4c9aa17c1d302603674610c0308e9e503413

Required artifacts for Application Enablement Services Release 8.1.1.0.1

The following section provides Application Enablement Services downloading information.

Filename	PLDS ID	File size	Version number	Comments
aesvcs-8.1.1.0.1-superpatch.bin	AES0000790	0.2191 MB (224.36 KB)	8.1.1.0.1	Avaya Aura® AE Services 8.1.1 Super Patch 1 Please refer to ***PSN020440u- Avaya Aura® Application Enablement (AE) Services 8.1.1 Super Patches*** for additional details MD5 Checksum: 75594f149cf7ae5be3bf2b707179d7c7 SHA1: 9ebe73c71842f78850b5441c7745175bbf5887fd SHA256:

Filename	PLDS ID	File size	Version number	Comments
				d7e2f679ee887a4d74f2c17873a0f11f4c814a30d53a415d876b2beff63adc52

Required artifacts for Application Enablement Services Release 8.1.1

The following section provides Application Enablement Services downloading information.

Note: AE Services 8.1.1 Super Patch 1 should be applied over AES 8.1.1 to address the issue identified in PSN020436. Please refer to **PSN020440** on the Avaya Technical Support site for AES 8.1.1 Deployment and Upgrade Instructions

Filename	PLDS ID	File size	Version number	Comments
swonly-8.1.1.0.0.8-20190930.iso	AES00000764	410.25 MB (420,100 KB)	8.1.1.0.0.8	Avaya Aura® Application Enablement Services Software Only 8.1.1 MD5 Checksum: 9fbfd3276e35f72a67c9b7058d3f9cae
AES-8.1.1.0.0.8.20190930-e65-00.ova	AES00000765	2,611.31 MB (2,673,990 KB)	8.1.1.0.0.8	Avaya Aura® Application Enablement Services 8.1.1 Aura® OVA Media MD5 Checksum: 116c66406cd775d39943aa5901d5802b
aesvcs-8.1.1.0.0.8-featurepack.bin	AES00000766	156.89 MB (160,655.53 KB)	8.1.1.0.0.8	Avaya Aura® Application Enablement Services 8.1.1 Feature Pack Installer MD5 Checksum: bc7117590afabfbfca3556b53ad318a8
AES-8.1.1.0.0.8.20190930-kvm-001.ova	AES00000767	2,604.86 MB (2,667,380 KB)	8.1.1.0.0.8	Avaya Aura® Application Enablement Services 8.1.1 KVM Support MD5 Checksum: 35580f846a5b6cfa2080df3727d9bed9

Required artifacts for Application Enablement Services Release 8.1.0.0.1

The following section provides Application Enablement Services downloading information.

Filename	PLDS ID	File size	Version number	Comments
aesvcs-8.1.0.0.1-superpatch.bin	AES00000762	109.6 MB (112,235 KB)	8.1.0.0.1	Avaya Aura® AE Services 8.1 Super Patch 1 Please refer to PSN020426u for additional details MD5 Checksum: 78035872fec3f863a207341b6fc7ca12 SHA1: e6faee397bac73917208558299a8be4a83b0c2dd SHA256: 078b79aa6cb482a037aed8f5b8a822ae87aea7c6abcce70b76d46b81a774d0d8

Required artifacts for Application Enablement Services Release 8.1

The following section provides Application Enablement Services downloading information.

Filename	PLDS ID	File size	Version number	Comments
AES-8.1.0.0.0.9.20190509-e65-00.ova	AES00000737	2878470 KB (2811.01 MB)	8.1.0.0.9	Avaya Aura® Application Enablement Services 8.1 Aura® OVA Media MD5 Checksum: 25edf7f8378a03c1cf3617a1cfbafdfb
AES-8.1.0.0.0.9.20190509-kvm-001.ova	AES00000738	2859070 KB (2792.06 MB)	8.1.0.0.9	Avaya Aura® Application Enablement Services 8.1 KVM Support MD5 Checksum: 13f9af0b233d57adc50ecd66169d3896
swonly-8.1.0.0.0.9-20190509.iso	AES00000736	419814 KB (409.97 MB)	8.1.0.0.9	Avaya Aura® Application Enablement Services Software Only 8.1 MD5 Checksum: 5b1e6050c86e9ab8241bfecb4a7ae3cb

Required patches for Application Enablement Services Release 8.1

For information about patches and product updates, see the Avaya Technical Support Web site https://support.avaya.com. For more details, see PCN2102S on the Avaya Technical Support site.

Installation for Avaya Aura® Application Enablement Services Release 8.1.x.x

Installation for Avaya Aura® Application Enablement Services Release 8.1.x

Backing up the AE Services software

Follow these steps to back up the AE Services server data:

1. Log in to the AE Services Management Console using a browser.
2. From the main menu, select Maintenance | Server Data | Backup. AE Services backs up the database and displays the Database Backup screen, that displays the following message: The backup file can be downloaded from here.
3. Click the "Here" link. A file download dialog box is displayed that allows you to either open or save the backup file (named as serverName_rSoftwareVersion_mvapdbddmmyyyy.tar.gz, where ddmmyyyy is a date stamp).

4. Click Save and download the backup file to a safe location that the upgrade will not affect. For example, save the file to your local computer or another computer used for storing backups.

Interoperability and requirements

Note: See the Avaya Compatibility Matrix application for full Avaya product compatibility information.

Installation for Avaya Aura® Application Enablement Services Release 8.1.x

Refer to the Deploying Avaya Aura® Application Enablement Services in Virtualized Environment or Deploying Avaya Aura® Application Enablement Services in a Software-Only Environment document for deployment instructions.

Additional references for Virtualized deployments:

- Deploying Avaya Aura® Appliance Virtualization Platform
- Upgrading Avaya Aura® Appliance Virtualization Platform
- Release Notes for Avaya Aura® Appliance Virtualization Platform Release 8.1.x
- Deploying Avaya Aura® AVP Utilities
- Release Notes section for Avaya Aura® AVP Utilities Release 8.1.x
- Deploying Avaya Aura® Application Enablement Services in Virtualized Environment Release 8.1.x
- Deploying Avaya Aura® Application Enablement Services in a Software-Only Environment Release 8.1.x
- Deploying Avaya Aura® Application Enablement Services in Virtual Appliance Release 8.1.x
- Upgrading Avaya Aura® Application Enablement Services Release 8.1.x

Note: For Communication Manager 8.0, AE Services 7.0.1 or later is required for DMCC first-party call control (1PCC) applications. DMCC 1PCC station registrations will fail when using Communication Manager 8.0 with AE Services 7.0 or earlier versions. When upgrading to Avaya Aura 8.1, it is recommended to upgrade the AE Services server before upgrading Communication Manager.

From AE Services 8.0, only the Transport Layer Security (TLS) 1.2 protocol is enabled by default. The lower level TLS protocols 1.0 and 1.1 are disabled by default. Note, according to the National Institute of Standards and Technology (NIST) Special Publication 800-52, TLS version 1.1 is required, at a minimum, to mitigate various attacks on the TLS 1.0 protocol. The use of TLS 1.2 is strongly recommended.

Note: For an upgrade from a previous AE Services 5.x or 6.x release to AE Services 8.0, any customer application relying on the old, Avaya provided server certificate for TLS will not be able to connect to the AE Services 8.0 server. If you have been using these certificates in a production environment, we strongly recommend that you prepare and execute a rollout plan, as soon as possible, to update your client applications and AE Services server with your own certificates. We strongly encourage customers to create this certificate prior to upgrading to the AE Services 8.0 release. Please refer to PSN004561u for more information.

Upgrading to AE Services 8.1.x

Upgrading to AE Services 8.1.3.1

Important Notes:

- An upgrade to AES 8.1.3.1 can be achieved only by upgrading an existing AES 8.1.3 system to AES 8.1.3.1 using the feature pack installer aesvcs-8.1.3.1.0.7-servicepack.bin.
- Prior to upgrading through the feature pack installer, it is **recommended** to install the Linux Security Update Patch 812Plus_LSUPatch4.bin. Please refer to PSN020481 for additional details.

Upgrading to AE Services 8.1.3

Important Notes:

- The following instructions are necessary to update to Avaya Aura® Application Enablement Services 8.1.3 (8.1 Feature Pack 3). Additional information is available in the AE Services Upgrade and Deployment guides available on support.avaya.com. In some cases, this requires a two-step upgrade process.

Current AES Version	Update LSU	Interim steps	Upgrade to 8.1.3
8.1	1) Install hotfix AES-21512. Refer PSN020482u for details 2) Update to latest 8.1.0 LSU.	**1)** Upgrade to 8.1.2 using 8.1.2 FP Installer *aesvcs-8.1.2.0.0.9-featurepack.bin; PLDS ID AES00000797* **2)** Update to latest 8.1.2Plus LSU	Upgrade to 8.1.3 using 8.1.3 FP Installer *aesvcs-8.1.3.0.0.25-featurepack.bin; PLDS ID AES00000823*
8.1.1	1) Install hotfix AES-21512. Refer PSN020482u for details 2) Update to latest 8.1.1 LSU	**1)** Upgrade to 8.1.2 using 8.1.2 FP installer *aesvcs-8.1.2.0.0.9-featurepack.bin; PLDS ID AES00000797* **2)** Update to latest 8.1.2Plus LSU	Upgrade to 8.1.3 using 8.1.3 FP Installer *aesvcs-8.1.3.0.0.25-featurepack.bin; PLDS ID AES00000823*
8.1.2.x	Update to latest 8.1.2Plus LSU	N/A	Upgrade to 8.1.3 using 8.1.3 FP Installer *aesvcs-8.1.3.0.0.25-featurepack.bin; PLDS ID AES00000823*

Note: For upgrading to AE Services 8.1.3 in a software-only environment, you must install AE Services 8.1 or 8.1.1 ISO, upgrade it to AE Services 8.1.2.x and then upgrade to AE Services 8.1.3.

- **Effect of TLS Certificate Hostname Validation after upgrading to AES 8.1.3**

  After the AE Services server is upgraded to 8.1.3, certificate hostname validation will be automatically enabled for external WebLM and all Communication Manager connections, that may cause the established connections to be dropped if the certificate validation fails.
  For more information and steps to re-establish the connection, please refer to *PSN020497u- Avaya Aura® Application Enablement (AE) Services 8.1.3 Certificate hostname and licensing impacts.*

Upgrading to AE Services 8.1.2.1 and 8.1.2.1.1

Important Notes:

- An upgrade to AES 8.1.2.1 can be achieved only by upgrading an existing AES 8.1.2 system to

AES 8.1.2.1 using the feature pack installer aesvcs-8.1.2.1.0.6-servicepack.bin.

- Prior to upgrading through the feature pack installer, it is **recommended** to install the Linux Security Update Patch 812Plus_LSUPatch1.bin. Please refer to PSN020481 for additional details.
- AES 8.1.2.1.1 is a super patch and can be applied only over AES 8.1.2.1. Please refer to PSN020489 for additional details.

Upgrading to AE Services 8.1.2

Important Notes:

- Upgrade from AES 8.1 or AES 8.1.1 to AES 8.1.2 through the feature pack installer aesvcs-8.1.2.0.0.9-featurepack.bin is supported.
- Prior to upgrading through the feature pack installer, it is **mandatory** to install the Linux Security Update Patch as follows:
    - Upgrade from AES 8.1 to AES 8.1.2 using feature pack: Install the 81_LSUPatch2.bin - Avaya Aura® AE Services 8.1 Linux Security Update Patch 2. Please refer to PSN020434u for additional details.
    - Upgrade from AES 8.1.1 to AES 8.1.2 using feature pack: Install the 811_LSUPatch2.bin - Avaya Aura® AE Services 8.1.1 Linux Security Update Patch 2. Please refer to PSN020452u for additional details.

Upgrading to AE Services 8.1.1

Important Notes:

- Upgrade from AES 8.x to AES 8.1 through the feature pack installer is not supported. All AES 8.1 deployments are required to be fresh installations
- AE Services 8.1.1 Super Patch 1 should be applied over AES 8.1.1 to address the issue identified in **PSN020436**. Please refer to **PSN020440** on the Avaya Technical Support site for AES 8.1.1 Deployment and Upgrade Instructions.

AE Services Server Upgrade Instructions

Note: For an AE Service 7.0.1 VMware offer upgrade to AE Service 8.x VMware offer using SDM, see “Upgrading Avaya Aura® Application Enablement Services”.

1. SSH into the AE Services server to be upgraded.
2. Using the AE Services CLI, execute the command "swversion".
3. Verify the release of the AE Services server. If the version is 6.3.3 SP3 or earlier, take the following steps:
    - Using PLDS, download the pre-upgrade patch, "AES7_PreUpgradePatch.bin", using the PLDS ID AES00000496.
    - Using the AE Services patch process, install the pre-upgrade patch on your existing AE Services server.

      Note that AES7_PreUpgradePatch needs to be applied before the backup is taken.

      AES7_PreUpgradePatch addresses the following issues:

        - AES-14089: TSAPI cannot log in using valid CT user credentials if the database is restored from the previous release.
        - AES-14250: Some data is missing after migrating from AE Services 5.2.4.
        - AES-14259: Some data is missing after migrating from AE Services 6.3.3.

4. Using the AE Services Management Console web page, note the configuration values for the following items on the specified web pages:
    - External LDAP checkbox setting on “Security > PAM > PAM Password Manager”
    - PAM MOTD checkbox setting on “Security > PAM > PAM MOTD”
    - Session Timeout values on “Security > Session Timeouts”
    - Product ID value on “Utilities > Product ID”
5. Take a backup of the AE Services server data. Refer to the topic “Backing up the AE Services software”
6. Download the backup file to a safe location that the upgrade will not affect.
7. Note the AE Services server hostname and IP address, and shutdown system.
8. Install AE Services 8.0.x. See the below sections for each platform.
9. Use the AE Services 8.0.x Management Console web page “Maintenance > Server Data > Restore” to restore previous backup data.

    Note: When using the AE Services 8.0.x Management Console to perform a restore, the “Restart Services Confirmation” page may be displayed again after the restore completes. To determine if a restore failed and is still pending, select the Restore link again (i.e. Maintenance > Server Data > Restore). If a Browser textbox is displayed the restore has completed. If the message “A database restore is pending” is displayed, the restore failed to complete.

10. Using AE Services 8.x Management Console, verify and update the values recorded in step 4 on the AE Services 8.x server.

Restoring AE Services software from the previous version

Use the AE Services 8.1 Management Console web page “Maintenance > Server Data > Restore” to restore any backup data.

Note: If the backup is from AE Services version 6.3.3 SP3 or earlier, verify the pre-upgrade patch, "AES7_PreUpgradePatch.bin", in Step 3 in the topic “Upgrading to AE Services 8.1.x” was executed before the previous backup was taken.

Note: When using the AE Services 8.x Management Console to perform a restore, the “Restart Services Confirmation” page may be displayed again after the restore completes. To determine if a restore failed and is still pending, select the Restore link again (i.e., Maintenance > Server Data > Restore). If a Browser textbox is displayed, the restore has completed. If the message “A database restore is pending” is displayed, the restore failed to complete.

RHEL 7.6 Support for AE Services 8.1

AE Services 8.1 is supported on RHEL 7.6. Upgrading AE Services 8.1 to any RHEL release greater than 7.6 is not supported and may cause the system to enter an unstable state

Installation for Avaya Aura® Application Enablement Services Software Only 8.1.3.1

Note: AE Services 8.1.3.1 Software Only can be achieved only by upgrading an existing AES 8.1.3 Software Only system to AES 8.1.3.1 using the feature pack installer aesvcs-8.1.3.1.0.7-servicepack.bin

Please see, *Deploying Avaya Aura® Application Enablement Services in a Software-Only Environment Release 8.1.x* and *Upgrading Avaya Aura® Application Enablement Services Release 8.1.x*.

Installation for Avaya Aura® Application Enablement Services Software Only 8.1.3

Note: AE Services 8.1.3 Software Only can be achieved only by upgrading an existing AES 8.1.2.x, AES 8.1.1 or AES 8.1 Software Only system to AES 8.1.3 using the feature pack installer aesvcs-8.1.3.0.0.25-featurepack.bin

Please see, *Deploying Avaya Aura® Application Enablement Services in a Software-Only Environment Release 8.1.x* and *Upgrading Avaya Aura® Application Enablement Services Release 8.1.x*.

Installation for Avaya Aura® Application Enablement Services Software Only 8.1.2.1

Note: AE Services 8.1.2.1 Software Only can be achieved only by upgrading an existing AES 8.1.2 Software Only system to AES 8.1.2.1 using the feature pack installer aesvcs-8.1.2.1.0.6-servicepack.bin

Please see, *Deploying Avaya Aura® Application Enablement Services in a Software-Only Environment Release 8.1.x* and *Upgrading Avaya Aura® Application Enablement Services Release 8.1.x*.

Installation for Avaya Aura® Application Enablement Services Software Only 8.1.2

Note: AE Services 8.1.2 Software Only can be achieved only by upgrading an existing AES 8.1.1 or AES 8.1 Software Only system to AES 8.1.2 using the feature pack installer aesvcs-8.1.2.0.0.9-featurepack.bin

Please see, *Deploying Avaya Aura® Application Enablement Services in a Software-Only Environment Release 8.1.x* and *Upgrading Avaya Aura® Application Enablement Services Release 8.1.x*.

Installation for Avaya Aura® Application Enablement Services Software Only 8.1.x

Note: The following steps are valid only for new/fresh installations.

Please refer to *Deploying Avaya Aura® Application Enablement Services in a Software-Only Environment*

Note: Occasionally, deployment of AES 8.1.1 SW-Only (swonly-8.1.1.0.0.8-20190930.iso) on AWS cloud fails. To install 8.1.1 SW-Only on AWS cloud, please refer to AES-19203 under the Known Issues Section for AES 8.1.1

Note: AE Services 8.1.1 Super Patch 1 should be applied over AES 8.1.1 to address the issue identified in PSN020436. Please refer to **PSN020440** on the Avaya Technical Support site for AES 8.1.1 Deployment and Upgrade Instructions.

Installation steps for Avaya Aura® Application Enablement Services 8.1.1 and 8.1.2 Aura® OVA Media

Note: The following steps are valid only for new/fresh installations.

See *Deploying Avaya Aura® Application Enablement Services in Virtualized Environment Release 8.1.x*

Note: AE Services 8.1.1 Super Patch 1 should be applied over AES 8.1.1 to address the issue identified in PSN020436. Please refer to **PSN020440** on the Avaya Technical Support site for AES 8.1.1 Deployment and Upgrade Instructions.

Installation steps for Avaya Aura® Application Enablement Services 8.1.2 Aura® KVM Support

Note: AE Services 8.1.2 KVM can be achieved only by upgrading an existing AES 8.1.1 or AES 8.1 KVM system to AES 8.1.2 using the feature pack installer aesvcs-8.1.2.0.0.9-featurepack.bin

See *Deploying Avaya Aura® Application Enablement Services in Virtualized Environment Release 8.1.x* and *Upgrading Avaya Aura® Application Enablement Services Release 8.1.x.*

Installation steps for Avaya Aura® Application Enablement Services 8.1.x Aura® KVM Support

Note: The following steps are valid only for new/fresh installations.

See *Deploying Avaya Aura® Application Enablement Services in Virtualized Environment.*

Note: AE Services 8.1.1 Super Patch 1 should be applied over AES 8.1.1 to address the issue identified in PSN020436. Please refer to **PSN020440** on the Avaya Technical Support site for AES 8.1.1 Deployment and Upgrade Instructions.

Functionality not supported

Functionality not supported for Release 8.1.3.1

- AE Services 8.1.3.1 does not support a fresh install of OVA Media, Software Only and KVM offers. Systems on these offers can upgrade from AES 8.1.3 to AES 8.1.3.1 using the feature pack installer, aesvcs-8.1.3.1.0.7-featurepack.bin

Functionality not supported for Release 8.1.3

- AE Services 8.1.3 does not support a fresh install of OVA Media, Software Only and KVM offers. Systems on these offers can upgrade from AES 8.1.2.x to AES 8.1.3 using the feature pack installer, aesvcs-8.1.3.0.0.25-featurepack.bin

Functionality not supported for Release 8.1.2.1

- AE Services 8.1.2.1 does not support a fresh install of OVA Media, Software Only and KVM offers. Systems on these offers can upgrade from AES 8.1.2 to AES 8.1.2.1 using the feature pack installer, aesvcs-8.1.2.1.0.6-servicepack.bin

Functionality not supported for Release 8.1.2

- AE Services 8.1.2 does not support a fresh install of Software Only and KVM offers. Systems on these offers can upgrade from older AES releases to AES 8.1.2 using the feature pack installer, aesvcs-8.1.2.0.0.9-featurepack.bin

Functionality not supported for Release 8.1.1

- AE Services 8.x does not support the “Bundled” and “System Platform” offers. Customers upgrading to AE Services 8.x must switch to the “Software-Only” offer or “VMware” (AE Services on AVP) offer.
- In AE Services 8.x, the Machine Preserving High Availability (MPHA) (aka VSST) feature is not available.
- **Upgrade from an older AES version to AES 8.x through the RPM-only installer is not supported**

  AES 8.1 is available in the three offers mentioned in the table “Required artifacts for Application Enablement Services Release 8.1”. All installations of AES 8.1 need to be fresh deployments. The AE Services 8.1 restore tool (i.e., Maintenance > Server Data > Restore) should be applied to restore data from an older version of AES to AES 8.1.

Changes and Issues

WebLM server compatibility

When using an external SMGR 8.x as WebLM server, the SMGR root CA certificate needs to be imported under Security | Certificate Management | CA Trusted Certificates. The WebLM server supports N-1 backward compatibility with its client component. The WebLM server does not support forward compatibility. This means the AE Services 8.x WebLM client will not work with the WebLM 7.x server.

Issues related to Enterprise Directory

For a customer to use their Enterprise Directory to access our OAM interface, the posix account is needed for RBAC (Role Based Access Control). Also, an unencrypted LDAP connection is no longer supported, and a certificate will be required using startTLS or LDAPS to connect to their Enterprise Directory for authentication purposes. In addition, the FQDN of the enterprise directory host is required.

Issues related to SNMP

- SNMP Traps with Snmpv3 and None as the encryption will be removed from the SNMP Trap destination screen.
- SNMP Traps with Inform will be switched to Trap..

Interaction between McAfee Antivirus and Executables

It has been observed that the following AES SDK files for Windows do not install successfully when McAfee Antivirus is installed on the system:

cmapijava-sdk-8.1.0.0.0.9.exe

cmapixml-sdk-8.1.0.0.0.9.exe

dmcc-dotnet-sdk-8.1.0.0.0.68.exe

smssvc-sdk-8.1.0.0.0.9.exe

telsvc-sdk-8.1.0.0.0.9.exe

jtapi-sdk-8.1.0.0.0.9.exe

Customers may attempt to add these to the exclusion list on the McAfee Application.

Speculative Execution Vulnerabilities (includes Meltdown and Spectre and also L1TF Vulnerabilities)

In order to help mitigate the Speculative Execution Vulnerabilities, the processor manufacturers and operating system developers provide software patches to their products. These are patches to the processors, hypervisors, and operating systems that the Avaya solutions utilize (they are not patches applied to the Avaya developed components of the solutions).

Once these patches are received by Avaya, they are tested with the applicable Avaya solutions to characterize any impact on the performance of the Avaya solutions. The objective of the testing is to reaffirm product/solution functionality and to observe the performance of the Avaya solutions in conjunction with the patches using typical operating parameters.

Avaya is reliant on our suppliers to validate the effectiveness of their respective Speculative Execution Vulnerability patches.

The customer should be aware that implementing these patches may result in performance degradation and that results may vary to some degree for each deployment. The customer is responsible for implementing the patches, and for the results obtained from such patches.

For more information about Speculative Execution Vulnerabilities fixes included in Avaya Aura® Release 8.x, see the following PSNs on the Avaya Support Site:

- PSN020346u - Avaya Aura® Meltdown and Spectre vulnerabilities
- PSN020369u - Avaya Aura® L1TF vulnerabilities

VM Foot Print Size and capacity

Note: The requirements for RAM and HDD have been increased in AE Services server 8.0.

		DMCC (Third-party call control: Microsoft OCS/Lync, IBM Sametime, Avaya Aura Contact Center)		**DMCC (First Party call control)**		**TSAPI/DLG/CVLAN**
Footprint	**Resources**	**Maximum # of users or agents**	**Maximum BHCC**	**Maximum # of users or agents**	**Maximum BHCC**	**Maximum Messages per second (MPS) Rate**
Small	1 CPU, 4 GB RAM 30 GB HDD	1K	20K BHCC	1K	9K BHCC	1K MPS
		10K	6K BHCC			
Medium	2 CPU 4 GB RAM 30 GB HDD	2.5K	50K BHCC	2.4K	18K BHCC	1K MPS
		12K	12K BHCC			
Large	4 CPU 6 GB RAM 30 GB HDD	5K	100K BHCC	8K	36K BHCC	2K MPS
		20K	24K BHCC			

Fixes in Application Enablement Services in Release 8.1.x.x

Fixes in Application Enablement Services in Release 8.1.3.1

ID	Minimum Conditions	Visible symptoms
AES-23832	AES 8.1.3 Windows 64 bits SDKs installed.	csta64.lib and attpriv64.lib were missing from Program Files/SDK/lib directory.
AES-23787	AES 7.1.3.6 AES 8.1.3	add AuthorizationCode did not work in SMS
AES-23771	AES 8.0	SNMP authentication traps were received on v1, while v3 was configured if authentication traps were enabled on OAM
AES-23763	AES 8.1.3	TSAPI & CVLAN client installation guide did not mention that “64 bits clients are only supported with 8.1.3 servers”
AES-23751	AES 7.1.3.6, CM 7.1.3	Customer faced call stuck problem on phones.

AES-23611	AES 8.1.3	False alarm for high CPU usage generated at midnight
AES-23593	AES 7.1.3	Display Hunt Group Returned Name for Extension & vice versa for Entries 601+
AES-23590	AES 8.0.1, CM 8.0.1	Customer got technical difficulty experienced message played on the IVR because the call was not fully established on AES connector side.
AES-23497	AES 8.0.1	While adding switchConnection using configAPI, if the switchname existed, it would allow another switch of same name but different cases to be added. While on OAM this is not allowed
AES-23331	AES 8.1.2Plus LSU2 must be installed, followed by AES 8.1.3 FP	If AES 8.1.2Plus LSU2 is installed, followed by AES 8.1.3 FP, then While uninstalling AES 8.1.3 FP, user management tab from the OAM has vanished.
AES-23256	AES 7.1.3.6 and above, CM 7.1.3	Call monitoring failed with cause value RESOURCE_LIMITATION_REJECTION.
AES-22913	AES 7.1.x with reserved licensing for DMCC configured.	Extra DMCC licenses were consumed from WebLM when reserved licensing was enabled.
AES-22783	AES 7.1.3 and above	While importing rsyslog certificate from pending requests, rsyslog option was not present on OAM
AES-21957	AES 8.1.2 should be present on AWS m4.medium or c4.large instances	Profile identification failed on AWS m4.medium,c4.large instances.
AES-21724	AES 8.1.2 with CTI application	ATT_SINGLE_STEP_CONFERENCE CONF message would show incorrect dynamic deviceID in conferenced event, if there was an off-pbx station on call.
AES-21218	AES 7.1.3.6, SMGR 7.1.3, CM 7.1.3	OAM pages (AE Services & Status) were stuck and TSAPI stopped processing CSTA traffic when WebLM was not reachable.
AES-20720	AES 7.1.3.6, CM 7.1.3	Application call recording stopped working due to application stopped receiving CSTA events
AES-23400	AES 8.0	The information on restarting of tomcat and httpd services was missing for the topic “Changing the server IP address – Software-Only server” in “Administering Avaya Aura® Application Enablement Services” document

Fixes in Application Enablement Services in Release 8.1.3

ID	Minimum Conditions	Visible symptoms
AES-22362	AES 7.1.3.x	AES stopped responding to TSAPI/DMCC requests when a ClamAV (clamscan) was in progress on the AE server.
AES-22099	AES 7.1.3.4 in GRHA	Virtual IP was not visible on HA Status page
AES-22068	AES 8.1.2.1 with survivable hierarchy (CM ESS / LSP) configured	When AES was restarted after a failover or failback the IP address of the CM did not get logged in the TSAPI log files.
AES-22057	AES-8.1.2,AES-8.1.1	Modifying a login on OAM under Security → Account Management caused the 'Days after password expired to lock account' to reset to -1. As the value was reset to -1, any changes on the other fields of the modify login page were not successful and displayed an error message "Value should be between 0 to 99999" on the screen.
AES-22055	AES 8.1.0 , AES 8.1.1, AES 8.1.2	PAM password rules failed to apply during adding or modifying logins through CLI. A password, set using the root login, was accepted even though it did not satisfy the PAM limit.
AES-21956	AES-8.1.1, AES-8.1.2 in GRHA mode.	When a GRHA setup was unconfigured and the secondary VM was redeployed with the same IP address, configuring of GRHA again with the redeployed AES resulted in error "Creating and exchanging ssh key failed"
AES-21933	AES 7.1.3.6 should be installed.	swversion command was showing the older PHP rpm version in case an upgrade happens for PHP.
AES-21895	AES 8.1.2.1 installed for Avaya IX Subscription setup	PPU data for last minute of the day was not captured
AES-21860	AES 8.0.1, CM 8.0	AES with reserved licenses count more than the weblm license count making local/embedded webLM to reject the license request saying "Too many licenses" causing TSAPI entering into 30 days grace period and showing LICENSE_ERROR mode.
AES-21852	AES 7.1.3	Occasionally, in a JTAPI call, conference failed because although metaCallMergeStartedEvent was received, the corresponding metaCallMergeEndedEvent was not received
AES-21851	AES 8.1.2.1 installed for Avaya IX subscription	Date in the filename was not consistent with the date for which the IX subscription data was captured for.
AES-21823	DMCC Programmers guide 8.x	The documentation for GetCallInformation API specific to SIP stations was not explicitly mentioned in the DMCC Programmers guide.

ID	Minimum Conditions	Visible symptoms
AES-21647	Telephony Web Service Application connecting to AES	Telephony Web Service didn't work after installing AES 8.1.2.1 Service patch.
AES-21512	AES 8.1/AES 8.1.1 which is present in the subnet which also has a DHCP server configured. Also applicable to AES 8.1.2 which is upgraded via FP.	Post installation of 8.1/8.1.1 LSU 2, once the AES is rebooted, AES is no longer accessible using the IP address. A dynamic IP address is assigned to the AES once it is rebooted.
AES-21509	AES with no NTP servers configured in /etc/ntp.conf	On OAM, Maintenance→Date Time → NTP Server Page was not accessible when there were no NTP Servers configured
AES-21503	AES 8.1.2.1 onwards Restart Linux License Server correctly configured and accessible	The PPU files were not accessible (permission denied) for SCP / logrotation after Linux restart.
AES-21407	AES 8.1.2	When ECD client sent Extend Timer Request without timer value and with valid Call ID, ECD session on CM was dropped and client received Abort Event from CM.
AES-21324	AES 8.1.2	On applying changes with a value of 0 in the 'dcredit', 'lcredit', 'ucredit', 'ocredit' fields on OAM under Security -> PAM -> PAM Password Manager, the fields displayed empty values.
AES-21309	AES 7.1.3.4	An unsuccessful monitor device request when followed by another CSTA request caused the TSAPI service to crash while auditing CSTA requests resulted in termination of all client connections.
AES-21284	AES JTAPI 8.1	When the provider received empty device history during ESTABLISHED or DELIVERED event, it shut down due to ArrayIndexOutOfBoundsException. However, having empty device history is normal in certain scenarios.
AES-21240	Un-Installation of 7.1.3.6 Featurepack (FP)	On uninstallation of 7.1.3.6 FP, the PHP rpms were reverted back to the GA version of 7.1.3 irrespective of the previous FP installed on the system.
AES-21237	TSAPI CTI application connected to AES.	TSAPI crashed with signal 11, Segmentation fault
AES-21196	AES 8.0.1 or above	The command "/opt/mvap/bin/networkingPorts dmcc -uact enabled -u 4721" returned error code 6 even though the port was enabled

ID	Minimum Conditions	Visible symptoms
AES-21190	AES 7.1.3	No alarms were generated when the TSAPI service stopped processing the CSTA requests as a result of a broken connection between TSAPI service and the WebLM server.
AES-21050	7.1.3.2 AES with incorrectly configured JavaManager.properties	Attempting to access OAM->Status->Status and Control->TSAPI Service Summary->TSAPI Service Status when JavaManager.properties was incorrectly configured caused a UI Exception to be raised
AES-21046	AES 8.0 or above JTAPI SDK 8.0 or above	getRegisteredEndpoints query from JTAPI for AES 8 and above was not being executed
AES-21035	AES 7.1.3.2.0.2-0	The CSTA snapshot query response for predictive call scenarios returned incorrect data to the CTI application. The local Connection Info State for the Calling device was displayed as 'None' instead of 'Connected' when Agent call was in ringing mode. Also, the DeviceID for calling party changed to VDN from Dynamic Device when state changed from ringing to answered.
AES-21032	AES 8.1.2, CM 8.1.2	Error message "G3PD error (channel_type) Error: field does not exist for current message" was logged in trace.out when a Single Step Conference(C_3PSSC_CONF) was executed.
AES-20988	AES 7.1.3.6	SMS Web test application was inaccessible
AES-20981	AES 7.1.3.6	SMS RPM warnings were being generated and seen in updatelog
AES-20883	AES 7.1.3.2.0.2-0	The CSTA snapshot query response for predictive call scenarios returned incorrect data to the CTI application. The information for calling party displayed connection state as 'None' and DeviceID as 'Dynamic Device' when the Agent was in Alert State.
AES-20808	DMCC Java SDK or XML SDK, Release 8.0.1 and above.	Description of newly added mediaContent and mediaTonesAnnc parameters to register-terminal API in AES release 8.0.1 was missing from customer-javadoc and customer-xmldoc available with DMCC Java SDK and DMCC XML SDK respectively.
AES-20773	AES 7.0 with CTI application	In snapshot query post the alerting message, AES sends the local connection state for called party as None.
AES-20755	AES-7.1.3.5, AES-8.1.2	When an incorrect file was uploaded on OAM under Security → Security Database → Worktops, wrong error message was displayed.
AES-20752	AES 8.1.2	All ECD calls made with private data version 16 were discarded with ECD timer expired error.

ID	Minimum Conditions	Visible symptoms
AES-20722	AES 8.1.2 with Data encryption enabled and Local Key Store configured.	On a Data Encryption enabled AES system with local key store configured. encryptionPassphrase list / encryptionRemoteKey list displayed "Passphrase" in the slot list for the entry of Local Key.
AES-20183	DMCC client 8.0.1 onwards. AES older than 8.0.1	DMCC client release 8.0.1 and above failed to send RegisterTerminal request with AE Server older than 8.0.1 unless mediaContent parameter was specified to 'FULL' explicitly in the RegisterTerminal request.
AES-20104	AES 7.1.3	An IP address, which was already in use by some other system, was accepted on the High Availability configuration page as a Virtual IP.
AES-20103	3 AES 7.1.x and above, out of which 2 AES are already configured for GRHA.	When an AES IP, which was already in GRHA running/configured state with other AES, was given as the secondary AES in a new GRHA configuration on a third server, it broke the initial GRHA configuration.
AES-20068	AES SWonly	In an SW-Only installation, if the ifcfg file contained prefix information, netmask was not displayed on OAM
AES-19907	JTAPI 7.0	Monitor for VDN failed with CSTA Error 12 " INVALID_CSTA_DEVICE_IDENTIFIER" , when the outgoing call was made over a SIP trunk to another endpoint that had the same extension as that of the VDN on the local CM.
AES-19809	AES 8.1.1.0.1 SWonly	Cron jobs were not running due to PAM errors
AES-19682	AES 7.1.3.0.0	AES listened to unknown IP Address 135.9.172.122 on port number 8180
AES-19556	AES 7.0.1 and later.	'FINE' level messages were also getting logged in the /var/log/avaya/aes/dmcc-trace.log file when the DMCC trace log level was set to 'WARNING'.
AES-19238	AES 8.1 and above in GRHA	The OAM of the secondary AES was not reachable via Virtual IP if the OAM connectivity was set to Virtual IP
AES-19022	AES 8.1.1	Snapshot call request displayed a maximum of 6 devices and did not display the status of all the registered bridge stations as 'Alerting'
AES-18999	AES 7.1.3.5, AES 8.1.1	When files were uploaded on the OAM, it would accept all the file types.
AES-18995	AES 8.1.1, CM 8.1	After a call was answered on the principal station, the snapshot call response displayed the bridged station as 'Alerting'
AES-18984	AES DMCC 8.0.1	Intermittently, only 'INFO' and 'ERROR' level messages were getting logged in the /var/avaya/aes/dmcc-trace.log file even when the logging level was set to 'FINEST'.

ID	Minimum Conditions	Visible symptoms
AES-18304	DMCC Javadocs for CallControlListener 8.x DMCC Java Programmers guide 8.x	The usage of terminated() callback method available with call control listener in DMCC Java SDK was not properly documented in Javadocs as well as DMCC Java Programmers guide.

Fixes in Application Enablement Services in Release 8.1.2.1.1

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms
Critical Updates	AES 8.1.2.1	Critical updates to usage data to ensure integrity of that data
AES-22068	AES 8.1.2.1 with survivable hierarchy (CM ESS / LSP) configured	Communication Manager (CM) IP is not available for TSAPI license logs for Pay Per Usage (PPU)when CM has an ESS/LSP configured.

Fixes in Application Enablement Services in Release 8.1.2.1

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms
AES-21190	AES 7.1.3	There are no alarms generated, when the PBX thread is in hung state causing the CSTA messages not getting processed by AES.
AES-21035	AES 7.1.3.2.0.2-0	The CTI application doesn't have the required information in snapshot query response in case of predictive call. The local Connection Info State for the Calling device is showing as None instead of Connected state when Agent call is ringing. The DeviceID for calling party is Dynamic Device when Agent call is ringing which is proper but changes to VDN when answered the call.
AES-20883	AES 7.1.3.2.0.2-0	The CTI application doesn't have the required information in snapshot query response in case of predictive call. The information for calling party shows connection state as None and DeviceID as Dynamic Device while Agent is in Alert State.
AES-20755	AES-7.1.3.5 AES-8.1.2	Incorrect error message was printed on OAM at Security -> Security Database -> Worktops
AES-20752	AES 8.1.2	In ECD configuration only, all ECD calls were dropped with an ECD timer expired error
AES-20722	AES 8.1.2 with Data encryption enabled and Local Key Store configured.	On a Data Encryption enabled AES system with local key store configured. encryptionPassphrase list / encryptionRemoteKey list displays "Passphrase" in the slot list for the entry of Local Key.
AES-19809	AES 8.1.1.0.1 SWonly	Cron jobs were not running due to PAM errors

ID	Minimum Conditions	Visible symptoms
AES-19022	AES 8.1.1	Snapshot call shows only up to 6 devices and does not show all the registered bridge stations status as Alerting state.
AES-18999	AES 7.1.3.5, AES 8.1.1	File of any type could be uploaded on the AES
AES-18995	AES 8.1.1, CM 8.1	After answer on principal, brdg still shows in Alerting state in snapshot call response.
AES-21529	AES 8.1.1	Monitor alarms like disk full alarms were not raised

Fixes in Application Enablement Services in Release 8.1.2

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms
AES-19605	AES 7.1.3.4 and later	Under the conditions mentioned below, the NMS server even though configured on the system and visible on the OAM, was not reflected in the snmpd.conf file: On 7.1.3.4 1. When SNMP version 2c was used 2. When SNMP version 3 was used and Authentication and Privacy protocols were not provided On 8.0 and above 1. When SNMP version 3 was used and Authentication and Privacy protocols were not provided
AES-19291	AES 8.x SWOnly Offer installed on RHEL 7.x	On a SWOnly system if the ifcfg files had values with double quotes, the OAM displayed incorrect network information
AES-19287	AES 6.3.3 onwards	The alarms.log files were being rotated twice per day instead of once resulting in retention of 5 days instead of 10
AES-19012	AES 7.1 and later	A user that was previously added to the usrsvc_admin group and later removed continued to be able to access the User Management page on OAM.
AES-17864	AES 7.1.3	Unnecessary kernel martian source logs were being written to alarm.log resulting in low retention of useful logging data
AES-19366	AES 8.1.1	In ECD configuration only, skills on CM continued to be controlled by ECD even after the ECD session was aborted by the TSAPI Client
AES-19558	CM 6.3.119.0, AES 7.1.3.4 and CM Special Application SA 9137 is enabled	In ECD configuration only, in rare cases calls in queue with available agents. Only applicable if CM Special Application SA 9137 is enabled. Reference PSN020412u – Required patch for CM 7.1.3.2 and 7.1.3.3 for systems implementing SA 9137

ID	Minimum Conditions	Visible symptoms
AES-19710	AES 7.1.3.5, CM 7.1.3.5	In ECD Configuration only, when ECD Activate and Deactivate Skill Responses are sent from the CM, any other application request, such as Make Call, Answer Call will fail with the error "DUPLICATE_INVOCATION_REJECTION"
AES-19632	AES 8.1	Event Name was not logged in g3pd trace.
AES-19025	AES 7.1.3.4, CM 7.1.3.4	"ConnectionClear" events were not received for the Call Monitors placed on calls. In addition, "MonitorStop" events were not received after call drop for Call Monitor requests.
AES-19023	AES 8.1, CM 7.1.3.5	In some high traffic Best Service Routing scenarios, the request queue gets full and further requests are rejected
AES-19022	AES 8.1.1	Snapshot call shows only up to 6 devices and doesn't show all the registered bridge stations status as Alerting state.
AES-19279	AES 8.1.1	The logrotate utility fails to rotate logs and the file system can run out of space. Changes made through the OAM | SecurityPAM Password Manager tab are not successful.
AES-19612	AES 8.1.x FP with GRHA configured.	Uninstallation of 8.1.x FP on a GRHA setup caused 404 error after logging in on OAM.
AES-19280	AES 8.1.x SWONLY	httpd service failed to restart after the update of httpd rpms on AES SWONLY systems
AES-19221	AES 8.x that has been upgraded to AES 8.1.1 using the featurepack, 8.1.1 FP	AES 8.1.1 that had been upgraded using the featurepack continued to use tomcat-8.5.34 instead of the newer version, tomcat-8.5.42-6
AES-19190	AES 8.1.1 OVA upgraded from AES 7.1.x or AES 8.x via SMGR SDM	Upgrading or migrating to AES 8.1.1 using the OVA, caused the DMCC service to fail.
AES-18983	AES 7.1.3	DMCC logs were not being compressed resulting in /var/log filling quickly
AES-18832	AES 7.1 OVA with AES 7.1.1 FP and SMGR SDM 7.x	When installing the AES OVA along with the patch using the SMGR SDM, deployed only the OVA. The patch installation was not triggered.
AES-17566	ASL trusted application trying to connect to AES when AES running in grace period.	When AES was running in grace period, ASL trusted application connection was not successful.
AES-14892	DMCC registrations on AES 7.0.1 onwards	Intermittently, DMCC registration failed
AES-18053	Executing "rtt" scripts on AES 7.1.3.3 and later	Execution of "rtt" scripts on a customer system that had the variable CSTATRACE defined, resulted in a segmentation fault. .
AES-19378	AES upgraded from 7.1.3.3 to 7.1.3.5 or from 8.0.1.0.x to 8.0.1.0.y, where y > x, and then reverted to the original service pack	GRHA status is corrupted when uninstalling AES 7.1.3.5 and reverting to 7.1.3.3 and when upgrading from AES 8.0.1.0.x to 8.0.1.0.y, where y > x, and then reverting to 8.0.1.0.x. On OAM, HA status at top of page shows running, but Status on HA page shows stopped and start button is available on HA page.

ID	Minimum Conditions	Visible symptoms
AES-19066	AES 7.1.3.5 and later	On a system that connects to SMGR WebLM for licenses, during high traffic, delays were observed in APIs that use licenses. This issue is also present with standalone WebLM if it is in a different network than the AES. Embedded WebLM in AES and Reserved Licensing on any configuration do not have this issue
AES-18557	Single Step Transfer with Avaya Media Server	The “Single Step Transfer” feature has been enhanced to accommodate network delays between CM and media resources
AES-19653	DMCC XML XSD Documentation, Release 7.1.3 onwards	In DMCC XML XSD documentation, it was incorrectly mentioned that 'call-type' value is not supported for MonitorType parameter in MonitorStart request. Both device-type and call-type values are supported.

Fixes in Application Enablement Services in Release 8.1.1.0.2

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms
AES-19287	AES 6.3.3 onwards	Alarm logs were stored for 5 days instead of 10 days
AES-17864	AES 7.1.3	Large number of kernel martian logs were generated in alarm.log
AES-19558	CM 6.3.119.0, AES 7.1.3.4 and CM Special Application SA 9137 is enabled	In an ECD configuration only, in rare cases calls remained in queue when agents were available (CIQAA). Reference PSN020412u Required patch for CM 7.1.3.2 and 7.1.3.3 for systems implementing SA 9137
AES-19366	AES 8.1.1	Skills on CM continued to be controlled by ECD even after the ECD session was aborted by the TSAPI Client
AES-19632	AES 8.1	Event Name was not logged in g3pd trace.
AES-18557	Single Step Transfer with Avaya Media Server	The “Single Step Transfer” feature has been enhanced to accommodate network delays between CM and media resources
AES-19025	AES 7.1.3.4, CM 7.1.3.4	"ConnectionClear" events were not received for the Call Monitors placed on calls. In addition, "MonitorStop" events were not received after call drop for Call Monitor requests.
AES-19023	AES 8.1, CM 7.1.3.5	In some high traffic Best Service Routing scenarios, the request queue gets full and further requests are rejected
AES-18983	AES 7.1.3	The directory /var/log becomes full because DMCC logs were not compressed
AES-14892	DMCC registrations on AES 7.0.1 onwards	Intermittently, DMCC registration failed
AES-19378	AES upgraded from 7.1.3.3 to 7.1.3.5 or from 8.0.1.0.x to 8.0.1.0.y, where y > x, and then reverted to the original service pack	GRHA status is corrupted when uninstalling AES 7.1.3.5 and reverting to 7.1.3.3 and when upgrading from AES 8.0.1.0.x to 8.0.1.0.y, where y > x, and then reverting to 8.0.1.0.x. On OAM, HA status at top of page shows running, but Status on HA page shows stopped and start button is available on HA page.

ID	Minimum Conditions	Visible symptoms
AES-19066	AES 7.1.3.5	On a system that connects to SMGR for licenses, during high traffic, delays were observed in APIs that use licenses This issue is also present with standalone WebLM if it is in a different network than the AES. Embedded WebLM in AES and Reserved Licensing on any configuration do not have this issue.

Fixes in Application Enablement Services in Release 8.1.1.0.1

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms
AES-19279	AES 8.1.1	1. The logrotate utility fails to rotate logs. 2. Changes made through the OAM | Security ->PAM Password Manager tab are not successful Reference PSN020436u - *Avaya Aura® Application Enablement (AE) Services 8.1.1 logrotate and password issues* for detailed instructions and guidance.

Fixes in Application Enablement Services in Release 8.1.1

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms
AES-18571	AES 8.1	When using private data version 15 and ASAI link version 10, the enhanced data added to the ATTQueryAgentLoginResp was not properly populated and contained default null values. This data is now properly populated. This JIRA, in conjunction with AES-18669, corrects the data returned for the query
AES-18669	AES 8.1	When using private data version 15 and ASAI link version 10, the logical agentID field was always populated as null. This JIRA, in conjunction with AES-18571, corrects the data returned for the query
AES-18768	Domain control on a skill and log an agent into that skill.	Logical Agent ID was NULL in Login Event Report
AES-18819	AES-7.1.3.5	The customer would see wrong permitted values (1-10000) ms for ECD timer. However the correct values were (100-10000)
AES-18936	AES 8.1 SP 1	Customer could see an array of ECD UUI fields instead of single field.
AES-18696	AES 8.0.1.0.2	On adding CTI user from command line, the OAM did not display CTI user under Security Database tab. However, it was present in ldap.
AES-18589	AES 7.1.3	Information, such as userid, common name, surname, etc, did not get written to the oam-audit.log during the process of adding a user through the OAM.

ID	Minimum Conditions	Visible symptoms
AES-18499	AES 7.1.3	After restoring the backup previously taken on an HA system on a newly deployed AES server, the HA configuration of the older AES system was incorrectly copied onto the new AES system.
AES-15881	AES-7.1	On restart services confirmation after restore, the message showed that "the page will be redirected to restore DB configuration". But it did not redirect and directly completed the restore
AES-14927	AES 7.0 and above	Multiple Logged on Events were being generated for a single object in JTAPI
AES-14762	AES 6.3.3	The documentation for SMS showed that it supported ASG logins. However it doesn't.
AES-18965	AES 8.1 SP1	1. If the application ended a session for any reason (or deactivated control on all-skills) and the skills under the control of the session became CCE-controlled while calls were in queue with outstanding SRRs on other sessions then the SRE was sent as a CSTARouteEndEvent to the application. Customer saw: TSAPI Error code seen is "INVALID_CALLING_DEVICE". 2. If the call had already been offered and queued to 3 skills and the application sent an SRS for an ECD controlled skill that the call was not offered to, the SRS was rejected, but the application got a chance to re-route the call. Here, the error code is sent within CSTAReRouteRequestEvent. Customer saw: TSAPI Error code seen is "GENERIC_SUBSCRIBED_RESOURCE_AVAILABILITY".
AES-18953	AES 8.1 SP1	Wrong error code was seen at client side.
AES-18671	AES 7.1.3.1	When alphanumeric character was sent in skill extension for skill and service route select msg, route register abort message was received, and all skills registered earlier were deregistered.
AES-18639	AES 8.1.0.0.0	When CCE sent an SRE with cause value CS3/40, customer did not see popup for reroute request.
AES-18520	AES 8.1.0.0.0	While installing TSAPI Client and SDK customer saw client SDK version 8.0 instead of 8.1
AES-17491	AES 8.0	Customer saw CVLAN/TSAPI client Readme files with version as 7.1 instead of 8.1

ID	Minimum Conditions	Visible symptoms
AES-18502	AES 7.1.3.3	On OAM, the field TSAPI Routing Application Configuration (6) could not be configured when the following steps were followed: 1. From AE Service Management Console main menu, Select Networking -> TCP Settings. 2. On the TCP Settings page, select: TSAPI Routing Application Configuration (6) 3. Select Apply Changes. 4. Confirmation page will be loaded, Select Apply 5. The previous page is re-loaded with default value "Standard Configuration (15)"
AES-18411	Start the SW-Only installation. 1. As part of the installation wizard., a screen with title "optional packages" , unselect cs-cusldap option 2. Complete the wizard. 3. Installation will be failed	Versions prior to 8.1.1, had a "cs-cusldap package" on optional packages screen of SW-only Installation wizard. If this package was not selected, installation failed with dependency error.
AES-18383	AES 8.0.1	On execution of following command "/usr/bin/systemctl status clamd@scan" , the output displayed "Active: failed"
AES-18945	AES 8.1.1 CM 7.1.3.4	Customer was not able to send ECD Route Select on ECD Route Request, resulting in ECD Route End (ECD timeout) from CM.
AES-18815	AES 8.1 SP1, CM 7.1.3.4.	ECD Skill Route Select send failed if ECDInfo was not selected or set to Undefined.
AES-18770	AES 8.1 SP1, CM 7.1.3.4	AgentID was NULL in Agent Logged off Event.
AES-18769	AES 7.1.3.1, CM 7.1.3.4	TSRV crashed and all the clients got disconnected.
AES-18656	AES 8.1, CM 7.1.3.4	When ECD client sent Agent Available Invoke with un-administered agentID, CM sent NAK resetting Session ID (-1) on AES. Thereafter when Skill Route End Event was received from CM, ECD session was dropped between AES and CM.
AES-18642	AES 8.1, CM 7.1.3.4	AES did not send the Skill Route End with cause value CS3/30 to multiple client sessions.
AES-18634	AES 8.1, CM 7.1.3.4	Skill Threshold Event and query display Skill Threshold Level as undefined.
AES-18580	AES 8.1, CM 7.1.3.4	ECD service and skill route requests coming on multiple were going to 1st client ECD session. The other client ECD sessions were not getting these events.
AES-18556	AES 8.1, CM 7.1.3.4	Skill List received from CM was not populated onto application.
AES-18533	AES 8.1 and CM 7.1.3.4	The TSAPI Link reset and client connection got closed.
AES-17580	AES 7.1.3.1, CM 7.1.3.4	Route Register Request failed with device not supported on Application.

ID	Minimum Conditions	Visible symptoms
AES-18924	AES 7.1.3 and above (SWOnly)	On Software only installation screen even after selecting cancel on "optional package" screen it redirected to next screen. This screen should be displayed only after selecting "yes"
AES-18235	AES 7.0.1 and above	There were unnecessary cron entries in wtmp
AES-18970	AES 8.0.1 with SMGR SDM 8.x	When upgrading AES to a higher version using the OVA upgrade process by SDM, the SDM would be in a 'stuck' state at the restore step which would fail the upgrade.
AES-18944	2 AES 7.1.x, one with OVA installation and other with a FP upgrade.	GRHA configuration failed between 2 AES servers, when one AES server was an OVA/SWonly installation, and the second AES was feature pack or a service pack upgrade.
AES-18942	AES 7.1.x with GRHA running	In an AES GRHA setup, if the standby was not reachable, then patch installation/uninstallation proceeded without any error resulting in software version mismatch between the servers.
AES-18899	AES 7.1.3.3 and SGMR 7.1.x.	When an SMGR that is used for licensing on AES was rebooted, the TSAPI (tsrv) process showed a CPU spike of 100 percent resulting in high CPU usage, which caused the TSAPI clients connected to AES to disconnect.
AES-18832	AES 7.1 OVA with AES 7.1.1 FP and SMGR SDM 7.x	When installing a AES OVA along with a patch together via SMGR SDM, only the OVA would be deployed. The patch installation would not be triggered.
AES-18672	AES 7.1.x	Customer could not login to OAM with user configured in LDAP Active Directory when "User ID Attribute Name" was changed from "uid" to "samAccountName" on the "Enterprise Directory" page of OAM.
AES-18585	AES 7.1.x SWonly with SMGR SDM 7.x or higher	When an AES swonly system was added as a host to SMGR SDM for Application Management, the Application Name, App Version, App Name was shown as UNKNOWN.
AES-17434	A CVLAN link on AES 8.0	Attempts to toggle the status of the CVLAN from AES OAM -> Status -> Status and Control -> CVLAN Service Summary failed with the error,"Error talking to MBean Server."
AES-18419	AES DMCC stations configured to use H.323 Security Profile as "pin-eke"	DMCC application did not get events from DMCC service after 5 days in high traffic when H.323 Security profile was configured as "pin-eke" on ip-network-region.
AES-18940	AES 8.1 OVA	OVA deployment of AES8.1 failed on ESXi 6.7 with Update 3
AES-18431	AES 6.3.3.10	AES sent connection clear after SSC, when call was answered by CAG user
AES-17701	AES 7.1.3	When AES was configured to use only TLS 1.2, while negotiating the TLS version, "sohd" tried to connect with versions 1.0 and 1.1. This failed and then eventually sohd connected to TLS 1.2

ID	Minimum Conditions	Visible symptoms
AES-17984	JTAPI client 6.3.3	The query getLoggedOnAgents() on JTAPI displayed incorrect results for a skill that was removed from an already logged-in agent using CM or CMS. A new provider instance needed to be created to reflect the changes.
AES-18695	Genesys T-Server DLG client application connected to AES and perform AES restart from OAM or from CL	Customer saw DLG service getting stuck in restart loop while performing AES restart activity. Please refer to PSN020417

Fixes in Application Enablement Services in Release 8.1.0.0.1

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms
AES-18571	AES 8.1	ATTQueryAgentLogin query through the TSAPI Exerciser returned Null as the agent ID instead of the logical extension
AES-18696	AES 8.0.1.0.2	On adding CTI user from command line, the OAM did not display CTI user under Security Database tab. However, it was present in ldap.
AES-18499	AES 7.1.3	Restoring the backup, previously taken on an HA system, on a newly deployed AES server incorrectly copied the HA configuration of the older AES system onto the new AES system.
AES-14927	AES 7.0	Multiple Logged on Events were being generated for a single object
AES-18502	AES 7.1.3.3	On OAM, the field TSAPI Routing Application Configuration (6) could not be configured when the following steps were followed: 1. From AE Service Management Console main menu, Select Networking -> TCP Settings. 2. On the TCP Settings page, select: TSAPI Routing Application Configuration (6) 3. Select Apply Changes. 4. Confirmation page will be loaded, Select Apply 5. The previous page is re-loaded with default value "Standard Configuration (15)"
AES-18672	AES 7.1.x	Customer could not login to OAM with user configured in LDAP Active Directory when "User ID Attribute Name" was changed from "uid" to "samAccountName" on the "Enterprise Directory" page of OAM.
AES-18585	AES 7.1.x SWonly with SMGR SDM 7.x or higher	When an AES SWonly system was added as a host to SMGR SDM for Application Management, the Application Name, App Version, App Name was shown as UNKNOWN.
AES-17434	A CVLAN link on AES 8.0	Attempts to toggle the status of the CVLAN from AES OAM -> Status -> Status and Control -> CVLAN Service Summary failed with the error, "Error talking to MBean Server."
AES-18419	AES DMCC stations configured to use H.323	DMCC application stopped receiving events from DMCC service after 5 days in high traffic when the H.323 Security profile was configured as "pin-eke" on CM's ip-network-region form

ID	Minimum Conditions	Visible symptoms
	Security Profile as "pin-eke"	
AES-17701	AES 7.1.3	When AES was configured to use only TLS 1.2, while negotiating the TLS version, "sohd" tried to connect with versions 1.0 and 1.1. This failed and then eventually sohd connected to TLS 1.2
AES-17984	JTAPI client 6.3.3	The query getLoggedOnAgents() on JTAPI displayed incorrect results for a skill that was removed from an already logged-in agent using CM or CMS. A new provider instance needed to be created to reflect the changes.
AES-18589	AES 7.1.3	Information, such as userid, common name, surname, etc, did not get written to the oam-audit.log during the process of adding a user through the OAM.

Fixes in Application Enablement Services in Release 8.1

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms
AES-18232	8.1	CSRF warning is displayed when accessing the WebLM server directly from AES. This can be ignored as password is being sent in encrypted form.
AES-17848	6.3.3 7.1 and 8.0	Insufficient documentation on the limit of 16 bridge appearances and other group features when using ASAI.
AES-17556	8.0	The default IPV6 address was displayed instead of the default IPV4 address.
AES-18071	7.1.3.1.1	Multiple SMS requests continue to result in SMS timeout. Additional Logging has been implemented to catch these errors
AES-17850	AES 7.1.3.1.1	The alarm viewer page was unavailable owing to creation of a large trapVarbinds.log.1 file
AES-17338	AES 7.1	snmpwalk did not display information for TsapiLicense
AES-18094	AES 7.1.2	The Monitor Call event failed with the DUPLICATE_INVOCATION_REJECTION error after the limit of 40000 Monitored calls was reached.
AES-17713	AES 7.1.3	CVLAN License acquisition failed with a WebLM timeout warning. OAM displayed the license in ‘Error Mode’.
AES-18008	AES 8.0.1	While installing AES using the SDM Client, changing the AES footprint failed when attempting to change the footprint through SDM Client-> Select AES VM -> Edit -> Change Flexi Footprint -> Change Flexi Footprint value. This step resulted in the error - "VM footprint did not match with any footprint definition in OVF".
AES-18003	AES 8.0.1	AES installation failed when McAfee endpoint protection was installed and enabled
AES-17997	AES 7.1.1	The older Mod_jk version has been updated to 1.2.46

ID	Minimum Conditions	Visible symptoms
AES-17956	AES 7.1.3	An older version of logrotate was being used. It has now been updated to logrotate-3.8.6-17.el7 or later.
AES-17861	AES 8.0.1	AES installation failed when McAfee endpoint protection was installed and enabled
AES-17860	AES 7.1.3	Users were unable to delete SNMP Trap Receivers with the Security Name as “avayadefaultsal”
AES-17565	AES 8.0	On OAM, the Alarm Viewer table was not being displayed
AES-17306	AES 7.1.3	On OAM -> Security->Audit->Login Audit ->, the field "Time to Begin Audit Each Day" did not accept any value greater than 10. The value reset to "00"
AES-18012	AES 6.3.3 or later.	AES 1 did not relinquish control of the snapshot device call on station 1 on which 3PTC was invoked. As a result, when AES 2 invoked ClearCall, it failed to take control of the call and resulted in an "Outstanding Request Limit Exceeded" message.
AES-17983	AES 8.0.1, CM 8.0.1	Predictive Call followed by Single Step Transfer failed
AES-17653	AES 7.1.3.1	In an ECD scenario, CM continued to remain in an Agent Surplus state because the ECD application was not notified when the ECD session was killed.
AES-17873	AES 7.1.x	Aesvcs service failed to execute because the softlink /usr/java/default did not refer to the latest OpenJDK version.
AES-18331	AES 7.1.x	A restore on the system incorrectly replaced the existing logging levels, that were set on the system prior to the restore, to the logging levels obtained from the backup file. This resulted in failure in generation of log files.
AES-18320	AES 7.1	The "Enterprise Directory" page on OAM failed to apply changes and failed to generate any error if the FQDN entry of the active directory was missing in the /etc/hosts file on AES. On restoring the backup data on AES, if Active directory is not present in not present in the file /etc/hosts, an error is generated for invalid FQDN which persists even after addition of the host entry in /etc/hosts
AES-18270	AES 8.0.1 with GRHA configuration.	The license state of the Standby AES continued to be in grace period even after the GRHA license was installed.
AES-18252	AES 7.1.3 (SWONLY offer)	After a database restore, users were unable to log in to the AES system.
AES-18110	AES 7.1.3.x	The setSELinux utility displayed incorrect status of SELinux
AES-18246	AES SMS Service logging set to Verbose and SMS Log Destination set to syslog	The log file /var/log/avaya/aes/ossicm.log did not get generated
AES-17754	HMDC configured to record TSAPI data	HMDC showed incorrect values for metrics related to TSAPI

ID	Minimum Conditions	Visible symptoms
AES-17061	AES 8.0 CVLAN or TSAPI client / SDKs installer ready	The version on CVLAN client, TSAPI client & SDKs displayed 7.1.1 instead of the latest version
AES-18151	Standalone SDM or SMGR ready for use.	SDM deployment of AES 8.0.1 along with a super patch failed.
AES-17738	AES 7.x	Incorrect configuration of logrotation resulted in large files being generated for the following log files - sssd_ldap_domain.log, sssd.log, sssd_nss.log, maillog, and cron
AES-17684	AES 7.1.2	The "sohd" service entered a restart loop if it was killed and restarted manually
AES-18403	AES 8.0.1	DMCC Java Programmers' Guide 8.0.1 referred to older versions of SDK files. This has been corrected in the 8.1 Programmers' Guides
AES-17781	AES 6.3.3 JTAPI Client	JTAPI application failed to create an address for a device that was added to SDB when the application was already running.
AES-17064	AES 7.1.1 JTAPI Client	Several expected Call Listener events/data were not displayed from AES 7.1.1.

Known issues and workarounds in Application Enablement Services 8.1.x.x

Known issues and workarounds Application Enablement Services in Release 8.1.3.1

The following table lists the known issues, symptoms, and workarounds in this release:

ID	Visible symptoms	Workaround
AES-23736	Virtual IP not displayed on GRHA page when configured using Maestro	
AES-23496	Unable to login into OAM, recovers only after tomcat restart	Restart tomcat service
AES-23757	State of calling party is cs_none after transfer event having one of the merge extension as hunt group	Placing explicit VDN monitor using Call Via Device API before the call gets routed to VDN.
AES-23482	DMCC Java Client 8.1.3 is incompatible with older versions of AES	Apply hotfix on DMCC 8.1.3 Java SDK/Client: https://downloads.avaya.com/css/P8/documents/101073383
AES-23401	If ServiceProvider.getServiceProvider() fails, two threads are left running	
AES-22592	RedirectMediaRequest fails silently if encryptionlist contains more than one entry, one of which is an SRTP type	Send only one value in encryptionList

AES-19032	If an application starts a Call Control monitor on a Call BEFORE monitoring a Skill, subsequent calls to GetAgentLogin for the skill will fail	Start skill monitor before call monitor
AES-15531	Re-Registration is required if any feature button added into station.	Re-Register the DMCC endpoint to get updated button information
AES-24090	asv: AES 8.1.3.1 - False alarm for high CPU usage after restarting AES server	
AES-23996	Invoking GetAgentLogin while a call monitor is active results in an exception in the DMCC module	
AES-23954	Weblm Host-ID changes in GRHA setup with virtual IP address	
AES-23682	The Host-ID of embedded weblm server changes when updating from 8.1.2 to 8.1.2.1 or 8.1.3. Because of this the license stands invalidated and server goes in grace period.	
AES-23797	Cannot access the Embedded weblm server on Internet Explorer	
AES-23767	DB restart on standby server causing alarms	
AES-23294	The help page under clear logs and clear traces does not have list of logs/ trace	Refer to the list under retention policy help page
AES-24194	Cylance get inactivate status after enabling SecureMode on AES (KVM deployment)	
AES-24201	AES8.1.3.1 - AES enabled secure mode will not ssh once it was upgraded to 8.1.3.1 or LSU due to sshd.service failed	
AES-24202	AES8.1.3.0 - AES is not licensed in the license file when secure mode was enabled on AES 8.1.3	
AES-24263	AES 8.1.3.1 - LSU patch should show warning alarm if the package already installed. However, it lets the patch to be installed	

Known issues and workarounds Application Enablement Services in Release 8.1.3

The following table lists the known issues, symptoms, and workarounds in this release:

ID	Visible symptoms	Workaround
AES-22783	While importing rsyslog ID cert from pending request to enroll, rsyslog alias is not present.	
AES-22782	Softphone sample app in cmapi-java sdk is not behaving correctly with TLS hostname validation TRUE	
AES-22776	Wrong number of parties in SSC Response	
AES-22774	Missing CSTA Diverted event in case of trunk call being answered by bridge.	
AES-22748	AES documentation inaccurately indicates support for all Java releases beyond version 8	
AES-22747	CSTA_MONITOR_CALL cause stale invokeID	
AES-22744	SO Activate with VDN observee and location > 2000 sends GENERIC_UNSPECIFIED error instead of VALUE_OUT_OF_RANGE	
AES-22742	AES is trying to connect to alarming.esp.avaya.com	
AES-22741	Sample Apps present in "Avaya\AE Services\SDKs\TSAPI\samples\Tsapicnf\Debug" doesn't work for 32 bits and 64 bits SDK	
AES-22740	AES 8.1.3 - TSAPI TSSPY prints binary data instead of decoded structure for 64 bits	
AES-22659	WebLM Server Address page displays port number 443 instead of 8443 when Restore Default button is clicked	
AES-22592	RedirectMediaRequest fails silently if encryptionlist contains more than one entry, one of which is an SRTP type	
AES-22559	Model Schema for IPAddressUsage displays wrong information	
AES-22498	AES Service page not opening post upgrade to AES 8.1.3	
AES-22399	Ethernet interfaces states on HA status page was shown as down where they were not.	
AES-22385	Automatic certificate enrollment gives error "Auto Enrollment failed, did not receive certificate from CA."	
AES-22191	Backup restore on a GRHA system does not backup the PAM parameters	
AES-22083	sohd process generated core when weblm server was rebooted	
AES-22017	CLONE - 12-party conf. - After merging two conferences, phone's display showed wrong count of conf. members. Also, on ACR-CTI monitor one station is not shown.	
AES-21957	Documented instance types for AWS are not detecting profiles.	
AES-21939	AES ignores register/un-register events subscription flags and blindly sends register/un-register events to AACC when it asks not to	
AES-21903	MonitorStart request throws InvalidDeviceIDException if there is case mismatch in DeviceID	

AES-21856	Connection clear event didn't come correctly for single step conference event	
AES-21645	OAM pages (AE Services & Status) stuck when WebLM is not reachable.	
AES-21543	CLONE - SIL - Oceana Performance Voice Only traffic run - all agents go NOT READY - AES ERROR:WARNING:terminates:Unexpected termination for primitive 61	
AES-21502	On GRHA setup, LSU installation on Standby AES creates issue with TOMCAT service and OAM was not accessible	
AES-21408	ECD session gets terminated if alphabets are sent in ECD requests instead of numbers	
AES-21271	Re-initialize tripwire database after installation of Service Patch or Super Patch	
AES-21218	TSAPI stops processing CSTA traffic when WebLM goes out of service	
AES-21191	ServiceInitiated and Held events contains "cause=normal" instead of "cause=transfer" in transfer scenario	
AES-21045	S/w only should not be installed if interface name is not "eth0"	
AES-21028	AES OAM not accessible from 8443 port if OAM connectivity is not set to ANY in AES SW Only 7.1.3.6	
AES-20999	After upgrading to AES 7.1.3.6, starting of subagent2 service errors are seen.	
AES-20815	OVA Deployment can't provide more than one NTP server	
AES-20786	Intermediate issue: Alarms did not get generate on GRHA setup	
AES-20720	PBX thread not processing further messages.	
AES-20587	Reboot of AES 8.1.2 Encryption Enabled takes approx. 4 mins to come Up	
AES-19767	The JTAPI SDK crashed due to the CSTA_CONNECTION_CLEARED event after an invalid number was called.	
AES-19711	asai_trace couldn't decode larger ASAI messages	
AES-19692	TSAPI client installation not overriding the older version files.	
AES-19396	Occasional DUPLICATE_INVOCATION_REJECTION error in response to a SetAgentState request	
AES-19395	OAM Help menu does not show Min and Max TSDI size	
AES-19383	JTAPI Null pointer exception while processing CSTA held event	
AES-19377	TSAPI & DMCC Links restarts on Active AES server when standby AES is powered On.	
AES-19365	Tomcat logs do not go through rsyslog partially	
AES-19364	cust password does not change from OAM	

AES-19226	After removing GRHA, AE services didn't start automatically on now separated two individual AES servers.	
AES-19215	Race condition in DMCC .Net SDK	
AES-19032	If an application starts a Call Control monitor on a Call BEFORE monitoring a Skill, subsequent calls to GetAgentLogin for the skill will fail	
AES-18967	During CM failover to ESS, dmcc extension does not register with ESS	
AES-18923	Rephrase software only optional package screen	
AES-18835	JTAPI queryLoggedOnAgents() returns wrong results when addressListener is placed on ACDAddress.	
AES-18588	AES OAM: High Availability status page is showing Intf1 and Intf2 status as unknow.	
AES-17735	RedirectMediaRequest not working in AES 6.3.3 SP10	
AES-17495	coreCastor error causes java.lang.NoSuchMethodException in DMCC Java Client	
AES-17367	Exception received during JTAPI testing with JTAPI exerciser	
AES-17332	Not getting DMCC Call Control events from JAVA SDK after an application shuts down and restarts the Service Provider.	
AES-17331	Client-side logging in DMCC Java programmers Guide	
AES-17260	MIB browser not able to connect AES Snmp server when SeLinux is Enable	
AES-16986	7.1.2 unable to install DMCC cmapi-xml/dotnet exes on Windows 10 Creator	
AES-16984	DMCC threads do not shut down when ServiceProvider.stopServiceProvider() is called after a network interruption	
AES-16970	haconctl to ignore the absence of eth1 if delayed option is given for setlocalkanetwork option	
AES-16552	Not all Call Control monitors receive MonitorStop events when TSAPI service stops	
AES-16140	Reset log are missing service name	
AES-16100	Redirect media doesn't work with media encryption "srtp-xxx" & "none"	
AES-16021	AES 7.1 build 13: "JVM exited unexpectedly" error in dmcc-wrapper.log	
AES-16009	Build 13 : Hostname is not taken by AES even after running netconfig	
AES-15951	Eth0-IPV6 in the OAM > Network Configure Page is hidden after disabling.	
AES-15531	Re-Registration is required if any feature button added into station.	Re-register the extension before invoking 'getButtonInfo' request to receive the latest and correct button info.

AES-15422	sohctl -lh replication failover command does not drop last two error entries	
AES-14801	JTAPI not getting call events for auto in calls	
AES-14676	No MediaStart events or RTP when a terminal is registered with a long list of codecs and encryption types	
AES-14659	ThirdPartyCallController.RouteSelect() throws "Object reference not set to an instance of an object." exception	
AES-14446	DMCC sample apps installed on AES will fail because DMCC sdk does not have the CA	
AES-14156	7.0 DMCC Softphone returns Java Exception Errors on Font Manager and phone cannot be registered as soft phone	
AES-13900	AES sometimes does not forward ToneDetectedEvents	
AES-13707	PlayMessage operation with Server Side Media add an unwanted "click" sound at the end of sound file	

Known issues and workarounds Application Enablement Services in Release 8.1.2.1 and 8.1.2.1.1

The following table lists the known issues, symptoms, and workarounds in this release:

ID	Visible symptoms	Workaround
AES-15531	Re-Registration is required if any feature button added into station.	Re-register the extension before invoking 'getButtonInfo' request to receive the latest and correct button info.
AES-15750	AES 6.3.3 SP6 - Incorrect days shown in Clearing grace period message.	
AES-17065	DLG service crash while stopping if there is connected client	
AES-17707	In SOAP import, the http import failed due to http port disable on newer AES versions	
AES-17864	Unnecessary kernel martian source logs were being written to alarm.log resulting in low retention of useful logging data	
AES-18984	Intermittently, only INFO and ERROR messages get logged in the /var/avaya/aes/dmcc-trace.log file even when the logging level is set to FINEST.	Use Java Appender instead of SyslogAppender in /opt/mvap/conf/dmcc-logging.properties file.
AES-19020	Spirit Agent CPU spike on AES	
AES-19226	After removing GRHA, AE services didn't start automatically on now separated two individual AES servers.	
AES-19238	AES OAM of secondary is not reachable via Virtual IP if OAM connectivity is set to virtual IP	
AES-19377	TSAPI & DMCC Links restarts on Active AES server when standby AES is powered On.	
AES-19383	If AES receives "HOLD" event with empty deviceID, JTAPI connector fetches errors and AES TSAPI provider shuts down	
AES-19406	SNMP subagent is in hung state. TSAPI/DLG/CVLAN/Switch page summary shows blank table.	
AES-19556	FINE messages would get logged in the /var/log/avaya/aes/dmcc-trace.log file even when the dmcc trace log level was set to WARNING	When logging level is set to 'WARNING' edit /opt/mvap/conf/dmcc-logging.properties file to replace all occurrences of 'WARNING' with 'WARN' as cust or root user
AES-19610	LDAP configuration option for TSAPI user (cus_ldap)	
AES-19682	AES listened to unknown IP Address 135.9.172.122 on port number 8180	
AES-19692	TSAPI client installation not overriding the older version files.	
AES-19724	RHSA-2019:4326 (fribidi) fix requested in 7.1.3	
AES-19767	JTAPI crash with nullpointer exception.	

AES-19907	The monitor for VDN fails with CSTA error 12 < INVALID_CSTA_DEVICE_IDENTIFIER > if Outgoing call over SIP trunk to another system which has Extension same as VDN extension on local CM.	
AES-20123	The long byte sequences were getting logged in dmcc-trace.log files at INFO log level.	
AES-20720	PBX thread not processing further messages.	
AES-20757	Enhancement to have alarms related to DBService on AES.	
AES-20773	In snapshot query post the alerting message, AES sends the local connection state for called party as None.	
AES-20789	OAM page gives 404 Request not found error for software only system	
AES-20871	Receiving error "Could not extract an x500 distinguished name" when attempting to renew third-party certificate with AES generated CSR	
AES-20874	Security Vulnerability - RHEL 7 : sudo (RHSA-2019:3209) Nessus Plugin ID: 130354 CVE-2019-14287	
AES-21046	getRegisteredEndpoints query from JTAPI for AES 8 and above was not being executed	
AES-21050	Empty TSAPI service summary due to exception while reading TSAPI variable "totalMemoryInUse"	
AES-21077	Red Hat Security advisory - RHSA-2020-0897 - icu security update	
AES-21078	RHEL 7 : kernel (RHSA-2020:0834) Nessus Plugin ID: 134671	
AES-21079	HEL 7 : php (RHSA-2020:1112) Nessus Plugin ID: 135040	
AES-21080	RHEL 7 : gettext (RHSA-2020:1138) Nessus Plugin ID: 135046	
AES-21081	RHEL 7 : bash (RHSA-2020:1113) Nessus Plugin ID: 135062	
AES-21082	RHEL 7 : expat (RHSA-2020:1011) Nessus Plugin ID: 135066	
AES-21083	RHEL 7 : kernel (RHSA-2020:1016) Nessus Plugin ID: 135080	
AES-21084	RHEL 7 : ImageMagick (RHSA-2020:1180) Nessus Plugin ID: 135041	
AES-21085	RHEL 7 : rsyslog (RHSA-2020:1000) Nessus Plugin ID: 135052	
AES-21218	TSAPI stops processing CSTA traffic when WebLM goes out of service	
AES-21237	TSAPI crashes with signal 11, Segmentation fault	
AES-21284	JTAPI provider shutdown if EstablishedEvent has empty deviceHistory	
AES-21309	TSAPI Service crash and all the client connections with AES is down.	

AES-21473	Documentation change : external WebLM Server Access will not work in the same way because of CSRF security fix.	
AES-21509	Cannot access the dateAndTime NTP page under the maintenance tab on AES OAM	
AES-21512	AES goes into DHCP mode after LSU 2 installation on 8.1.1	
AES-20587	Reboot of AES 8.1.2 Encryption Enabled takes approx. 4 mins to come Up	

Known issues and workarounds Application Enablement Services in Release 8.1.2

The following table lists the known issues, symptoms, and workarounds in this release:

ID	Visible symptoms	Workaround
AES-19907	JTAPI is sending CSTA monitor device for VDN extension	
AES-19767	JTAPI crash due to ConnectionCleared event.	
AES-19724	RHSA-2019:4326 (fribidi) fix requested in 7.1.3	
AES-19692	TSAPI client installation not overriding the older version files.	
AES-19682	AES listens to unknown IP Address 135.9.172.122 on port number 8180	
AES-19658	LSU installation on AES GRHA documentation	
AES-19654	LSU installation on GRHA server	
AES-19556	DMCC log level "INFO" & "WARNING" are dumping "FINE" logsFINE messages get logged in the /var/log/avaya/aes/dmcc-trace.log file even when the dmcc trace log level is set to WARNING	When logging level is set to 'WARNING' edit /opt/mvap/conf/dmcc-logging.properties file to replace all occurrences of 'WARNING' with 'WARN' as cust or root user
AES-19406	SNMP issue due to hung subagent1 and subagent2SNMP subagent is in hung state. TSAPI/DLG/CVLAN/Switch page summary shows blank table.	
AES-19383	JTAPI Null pointer exception while processing CSTA held eventIf AES receives "HOLD" event with empty deviceID, JTAPI connector fetches errors and AES TSAPI provider shuts down	
AES-19377	TSAPI & DMCC Links restarts on Active AES server when standby AES is powered On.	
AES-19238	AES Secondary OAM after failover is not reachable through virtual IPAES OAM of secondary is not reachable via Virtual IP	
AES-19226	After removing GRHA, AE services didn't start automatically on now separated two individual AES servers.	
AES-19064	Private IP address disclosed	
AES-19020	Spirit Agent CPU spike on AES	
AES-18999	File upload security concern	
AES-18984	DMCC logs reduce from Finest to InfoIntermittently, only INFO and ERROR messages get logged in the /var/avaya/aes/dmcc-trace.log file even when the logging level is set to FINEST.	Use Java Appender instead of SyslogAppender in /opt/mvap/conf/dmcc-logging.properties file. Refer to PSN PSN020455 for more details.
AES-18978	Browser remembers user credentials and provide autocomplete facility	
AES-15531	Re-Registration is required if any feature button added into station.	Re-register the extension before invoking 'getButtonInfo' request to receive the latest and correct button info.
AES-14374	sohd exits on SIG_ABRT raised in weblm client library	

AES-20722	encryptionPassphrase list/encryptionRemoteKey list displays slot as "passphrase" for local key	
AES-20723	Exception while trying to access TSAPI status page.	
AES-20587	Reboot of AES 8.1.2 Encryption Enabled takes approx. 4 mins to come Up	
AES-20741	while enabling port 80 from standard Reserved ports, iptables needs to be restarted	

Known issues and workarounds Application Enablement Services in Release 8.1.1.0.2

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Visible symptoms	Workaround
AES-19406	SNMP subagent is in hung state. TSAPI/DLG/CVLAN/Switch page summary shows blank table.	Restart snmpd, subaget1 and subaget2 services
AES-19383	If AES receives "HOLD" event with an empty deviceID, JTAPI connector fetches errors and AES TSAPI provider shuts down	
AES-19238	AES OAM of secondary is not reachable via the Virtual IP	Select "ANY" as the OAM interface
AES-19654	LSU installation fails if GRHA is enabled on a system	Remove GRHA before installing LSU
AES-19302	AES OAM (UI) is not accessible using httpd port (443 / 80)	Manually restart the httpd service
AES-19682	AES listens to unknown IP Address 135.9.172.122 on port number 8180	
AES-19377	TSAPI & DMCC Links restart on the Active AES server when the standby AES is powered on.	
AES-19226	After removing GRHA, AE services do not start automatically on the now separated two individual AES servers.	
AES-19020	Spirit Agent CPU spike is seen on AES	
AES-14374	SOHD exits on SIG_ABRT raised in weblm client library	
AES-19556	‘FINE’ messages get logged in the /var/log/avaya/aes/dmcc-trace.log file even when the dmcc trace log level is set to ‘WARNING’.	Replace all occurrences of ‘WARNING’ to ‘WARN’ by manually editing /opt/mvap/conf/dmcc-logging.properties file as a root user.
AES-18984	Intermittently, only INFO and ERROR messages get logged in the /var/avaya/aes/dmcc-trace.log file even when the logging level is set to ‘FINEST’.	Use Java Appender instead of Syslog Appender to get all the messages in /var/log/avaya/aes/Dmcc-trace.log file.

Known issues and workarounds Application Enablement Services in Release 8.1.1.0.1

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Visible symptoms	Workaround
AES-18247	While executing the list agent and list station queries on CM (where a large number of agents and stations are configured) via the SMS interface, the SMS application returned error	
AES-18588	AES OAM: High Availability status page is showing Intf1 and Intf2 status as unknown	
AES-18641	Registration Query API will fail for 4 or more registered devices	
AES-18707	DLG service fails to come up after AES restart when DLG client application is connected to AES during the restart	
AES-18771	ECD session takes ~15 mins to be cleaned up if ECD client goes out of network	
AES-18835	The result for skill extension query using JTAPI API getLoggedOnAgents() yielded wrong result if the skill extension in question had an addressListener placed on it. It returned the agent information which was removed from skill recently. Also, vice-versa, it didn't always return the agent information that was added to the skill recently	
AES-18923	Rephrase software only optional package screen	
AES-18930	OAM throws error when user disables server media and allocate RTP UDP port to local UDP port range	
AES-18955	While resetting the password on enterprise directory page, the passwords with $ in old passwords are not reset	Edit "/etc/sssd/sssd.conf" file and remove $ from the password and restart sssd service.
AES-18978	For password fields the browser remembers the credentials although autocomplete=off is set	
AES-18994	AES TSAPI & CVLAN Client SDK guide should mention RHEL as supported OS instead of Linux OS.	
AES-19066	Delays in response from WebLM in high traffic scenarios	Use Reserved Licensing
AES-19190	Occasionally, after upgrading from AES 7.1.3.4 or AES 8.0.1.0.4 using SDM, the DMCC service failed to get activated	To restart this service please choose any one of the following options: 1.Through CLI, run the command “service aesvcs restart” OR 2.Through OAM, Maintenance | Service Controller, select “AE Server” and click on “Restart Service”

AES-19203	Occasionally, Deployment of AES 8.1.1 ISO on AWS cloud fails	Perform these Steps to upgrade to AES 8.1.1 SWOnly 1. Deploy AES 8.1 SWOnly (swonly-8.1.0.0.0.9-20190509.iso). 2. Upgrade to AES 8.1.1 using aesvcs-8.1.1.0.0.8-featurepack.bin

Known issues and workarounds Application Enablement Services in Release 8.1.1

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Visible symptoms	Workaround
AES-18247	While executing the list agent and list station queries on CM (where a large number of agents and stations are configured) via the SMS interface, the SMS application returned error	
AES-18588	AES OAM: High Availability status page is showing Intf1 and Intf2 status as unknown	
AES-18641	Registration Query API will fail for 4 or more registered devices	
AES-18707	DLG service fails to come up after AES restart when DLG client application is connected to AES during the restart	
AES-18771	ECD session takes ~15 mins to be cleaned up if ECD client goes out of network	
AES-18835	The result for skill extension query using JTAPI API getLoggedOnAgents() yielded wrong result if the skill extension in question had an addressListener placed on it. It returned the agent information which was removed from skill recently. Also, vice-versa, it didn't always return the agent information that was added to the skill recently	
AES-18923	Rephrase software only optional package screen	
AES-18930	OAM throws error when user disables server media and allocate RTP UDP port to local UDP port range	
AES-18955	While resetting the password on enterprise directory page, the passwords with $ in old passwords are not reset	Edit "/etc/sssd/sssd.conf" file and remove $ from the password and restart sssd service.
AES-18978	For password fields the browser remembers the credentials although autocomplete=off is set	
AES-18994	AES TSAPI & CVLAN Client SDK guide should mention RHEL as supported OS instead of Linux OS.	
AES-19066	Delays in response from WebLM in high traffic scenarios	Use Reserved Licensing
AES-19190	Occasionally, after upgrading from AES 7.1.3.4 or AES 8.0.1.0.4 using SDM, the DMCC service failed to get activated	To restart this service please choose any one of the following options: 1.Through CLI, run the command “service aesvcs restart” OR 2.Through OAM, Maintenance | Service Controller, select “AE Server” and click on “Restart Service”

AES-19203	Occasionally, Deployment of AES 8.1.1 ISO on AWS cloud fails	Perform these Steps to upgrade to AES 8.1.1 SWOnly 1. Deploy AES 8.1 SWOnly (swonly-8.1.0.0.0.9-20190509.iso). 2. Upgrade to AES 8.1.1 using aesvcs-8.1.1.0.0.8-featurepack.bin
AES-19279	Cron Jobs for logrotate not running due to PAM errors	1. The logrotate utility fails to rotate logs. 2. Changes made through the OAM | Security ->PAM Password Manager tab are not successful Reference PSN020436u - *Avaya Aura® Application Enablement (AE) Services 8.1.1 logrotate and password issues* for detailed instructions and guidance

Known issues and workarounds Application Enablement Services in Release 8.1.0.0.1

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Visible symptoms	Workaround
AES-17566	When AES running in grace period, ASL trusted application connection is not successful.	Resolve AES license error mode.
AES-17415	OCI trunk info and OCI trunk group missing in Delivered and Establish event received on station monitor after consultation call.	
AES-16960	Delivered Events is missing many fields when AES Server version is 7.1 or older	
AES-15383	DMCC process gets restarted with Out of Memory error.	Block connection from any TR87 which has no valid certificate or install valid certificate
AES-18641	Did not get Query Endpoint Info Conf for more than 4 endpoints	
AES-17332	Call control events are not received by the application once the service provider has been shut down and restarted.	

Known issues and workarounds Application Enablement Services in Release 8.1

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Visible symptoms	Workaround
AES-18520	Installation of TSAPI Client and TSAPI SDK for Windows shows incorrect AES version	
AES-18420	Upgrading the AES through the SDM fails to upgrade the secondary AES	Upgrade AES through the command line interface.
AES-17701	When AES is configured to use only TLS 1.2, while negotiating the TLS version, "sohd" tries to connect with versions 1.0 and 1.1. This fails and then eventually sohd connects to TLS 1.2	
AES-18434	On OAM, the counts displayed on “AE Services -> CVLAN -> CVLAN links" and "Status -> Status and Control -> CVLAN Service Summary" are different	
AES-15629	SIGBUS error generates multiple core files.	
AES-17415	OCI trunk info and OCI trunk group date are omitted in Delivered and Establish events that are received on a station monitor after a consultation call.	
AES-17332	DMCC Application stops receiving Call Control events after the service provider has been restarted.	Shutdown JVM and restart the DMCC application.
AES-16960	Multiple fields are omitted in the Delivered Event messages when the AES Server version is 7.1 or older.	Upgrade AES to 7.1.1 or later.
AES-15383	AES DMCC service restarts generating an "Out Of Memory" error once in 3 weeks.	Configure the TR87 clients to use a valid certificate.
AES-14892	1 out of 1000 DMCC registration is rejected with error code "63773"	
AES-18404	1PCC Phone display does not display any 1PCC activity if the phone monitor is started while the station is registering	
AES-17984	The query getLoggedOnAgents() on JTAPI displays wrong results. If a skill is removed from an already logged-in agent through CM or CMS, this will not be reflected on the client immediately	Restart the JTAPI application
AES-14927	Different numbers of logged on and logged off events are received on each listener placed on all the agent skills.	

Avaya Aura® AVP Utilities

What's new in AVP Utilities Release 8.1.3.1

What's new in AVP Utilities Release 8.1.3

For more information see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

What's new in AVP Utilities Release 8.1.2.1

Avaya Aura® AVP Utilities 8.1.2**.**1 has introduced a new security service pack. This is useful for customers who want to get only the security updates and not the full feature pack or service pack. The feature pack and the service pack will continue to bundle security updates like before.

Please refer to PCN AVPU SSP 8.1.x – PCN 2123S for details about downloading and installing the security service pack.

What's new in AVP Utilities Release 8.1.2

Avaya Aura® AVP Utilities 8.1.2 has introduced the following features as a security measure:

1. A system administrator can configure certain log files on AVP Utilities to be retained for a certain number of days (between 0 and 180 days). After the configured duration, the log files will be deleted from the system.
2. A system administrator can install AVP Utilities OVA with certain partitions encrypted (available with 8.1E OVA). The encryption can be configured to be passphrase based, or key server based (either local or remote key server supported).

Please note that a system administrator must apply AVP Utilities 8.1.2 patch to use the above features. For more details, refer to the product documentation and Data Privacy Guideline (DPG) document.

What's new in AVP Utilities Release 8.1

For more information see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

Security Service Packs

AVP Utilities releases Platform Security Service Packs (SSPs) aligned with the application release cycle.

Beginning December 2020, SSPs will also be released on a more frequent cadence. This means that SSPs may also be available between application Service Packs/Feature Packs. SSP required artifacts and fix IDs will no longer be tracked in the Release Notes. For further information on contents and installation procedures, please see PCN AVPU SSP 8.1.x – PCN 2123S.

AVP Utilities releases Security Service Packs (SSPs) Only without any SP/FP. Beginning December 2020, SSPs will also be released on a more frequent cadence.

Download ID	Patch	Notes
AVPU0000027	util-PLAT-8.1-004-01.zip	Use this PLAT patch to for AVP Utilities security service pack update only and does not contain any code fixes. This security service pack can be installed on any 8.1.x AVP Utilities installation after the **util_preupgrade (**AVPU0000017**) CLI patch needed for this SSP update.**

Download ID	Patch	Notes
		All the new deployment of AVP Utilities OVA using 8.1.2.1 later SDM applies the above preupgrade patch automatically (So no need to apply separately from CLI).
AVPU0000025	util-PLAT-8.1-003-01.zip	Use this PLAT patch to for AVP Utilities security service pack update only and does not contain any code fixes. This security service pack can be installed on any 8.1.x AVP Utilities installation after the **util_preupgrade (**AVPU0000017**) CLI patch needed for this SSP update.** All the new deployment of AVP Utilities OVA using 8.1.2.1 later SDM applies the above preupgrade patch automatically (So no need to apply separately from CLI).
AVPU0000021	util-PLAT-8.1-002-07.zip	Use this PLAT patch to for AVP Utilities security service pack update only and does not contain any code fixes. This security service pack can be installed on any 8.1.x AVP Utilities installation. util_preupgrade patch needed for this SSP update.
AVPU0000019	util-PLAT-8.1-001-02.zip	Use this PLAT patch to for AVP Utilities security service pack update only and does not contain any code fixes. This security service pack can be installed on any 8.1.x AVP Utilities installation. Util_preupgrade patch needed for this SSP update.

Installation for Avaya Aura® AVP Utilities Release 8.1.x.x

Installation for Avaya Aura® AVP Utilities Release 8.1.3

Installation for Avaya Aura® AVP Utilities Release 8.1.2

To install Avaya Aura AVP Utilities 8.1.2, the administrator has to deploy a new 8.1E OVA if encryption features are required or can continue with the existing installation if encryption features are not needed.

The administrator can then deploy patches as described in *Deploying Avaya Aura® AVP Utilities*.

Installation for Avaya Aura® AVP Utilities Release 8.1

Please note that System Manager SDM or SDM Client is required to upgrade AVP Utilities on during AVP upgradation.

AVP has a single footprint size and so this will not appear as a list of options during deployment.

There are three deployment modes depending on the security hardening required – the features are identical regardless of the mode of deployment. Please see the documentation suite for a full explanation of the differences in each deployment mode:

- Standard Mode
- Hardened Mode
- Hardened Mode DoD

Required artifacts for AVP Utilities Release 8.1.x.x

Download ID	Patch	Notes
AVPU0000026	util_patch_8.1.3.1.0.01.zip	Use this patch to upgrade AVP Utilities from 8.1, 8.1.1, 8.1.2 or 8.1.2.1 and 8.1.3.0 to 8.1.3.1 FP with bundled security updates PLAT-8.1-004.
AVPU0000027	util-PLAT-8.1-004-01.zip	Use this PLAT patch to for AVP Utilities security service pack update only and does not contain any code fixes. This security service pack can be installed on any 8.1.x

Download ID	Patch	Notes
		AVP Utilities installation. **util_preupgrade patch needed for this SSP update.**
AVPU0000017	util_preupgrade_001-02.zip	One time pre-upgrade patch needed for the applying new SP and SSP. If patches applied using CLI not using SDM, then this patch installation is mandatory.

Required artifacts for AVP Utilities Release 8.1.3

Download ID	Patch	Notes
AVPU0000017	util_preupgrade_001-02.zip	One time pre-upgrade patch needed for the applying new SP and SSP**. If patches applied using CLI not using SDM, then this patch installation is mandatory**.
AVPU0000020	util_patch_8.1.3.0.0.12.zip	Use this patch to upgrade AVP Utilities from 8.1, 8.1.1, 8.1.2 or 8.1.2.1 to 8.1.3 FP with bundled security updates PLAT-8.1-002.
AVPU0000021	util-PLAT-8.1-002-07.zip	Use this PLAT patch to for AVP Utilities security service pack update only and does not contain any code fixes. This security service pack can be installed on any 8.1.x AVP Utilities installation. **util_preupgrade patch needed for this SSP update.**

Required artifacts for AVP Utilities Release 8.1.2.1

The following section provides AVP Utilities downloading information.

Download ID	Patch	Notes
AVPU0000017	util_preupgrade_001-02.zip	One time pre-upgrade patch needed for the applying new SP and SSP.
AVPU0000018	util_patch_8.1.2.1.0.01.zip	Use this patch to upgrade AVP Utilities from 8.1 or 8.1.1 or 8.1.2 to 8.1.2.1 with bundled security updates.
AVPU0000019	util-PLAT-8.1-001-02.zip	Use this PLAT patch to for AVP Utilities security service pack update only and does not contain any code fixes. This security service pack can be installed on any 8.1.x AVP Utilities installation. Util_preupgrade patch needed for this SSP update.

Required artifacts for AVP Utilities Release 8.1.2

The following section provides AVP Utilities downloading information.

Download ID	Patch	Notes
AVPU0000015	AVPU-8.1.0.0.0.09-e65-1E_OVF10.ova	Use this OVA to deploy AVP Utilities 8.1 with optional disk encryption support.
AVPU0000016	util_patch_8.1.1.0.0.10.zip	Use this patch to upgrade AVP Utilities from 8.1 or 8.1.1 to 8.1.2 and security updates.

Required artifacts for AVP Utilities Release 8.1.1

The following section provides AVP Utilities downloading information.

Download ID	Patch	Notes
AVPU0000014	util_patch_8.1.1.0.0.06.zip	Use this patch to upgrade AVP Utilities from 8.1 to 8.1.1.

Required artifacts for AVP Utilities Release 8.1

The following section provides AVP Utilities downloading information.

Download ID	Patch	Notes
AVPU000009	AVPU-8.1.0.0.0.06-e65-127_OVF10.ova	Use this OVA to deploy AVP Utilities 8.1.

For more details see PCN2098S on the Avaya Technical Support site.

Enhanced Access Security Gateway (EASG)

EASG provides a secure method for Avaya services personnel to access the Avaya Aura® Application remotely and onsite. Access is under the control of the customer and can be enabled or disabled at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck.

Refer to the *Deploying Avaya Aura® AVP Utilities Release 8.1.x* document for instructions on enabling and disabling EASG, and for instructions on installing the EASG site certificates.

Speculative Execution Vulnerabilities (includes Meltdown and Spectre and L1TF Vulnerabilities)

In order to help mitigate the Speculative Execution Vulnerabilities, the processor manufacturers and operating system developers provide software patches to their products. These are patches to the processors, hypervisors, and operating systems that the Avaya solutions utilize (they are not patches applied to the Avaya developed components of the solutions).

Once these patches are received by Avaya, they are tested with the applicable Avaya solutions to characterize any impact on the performance of the Avaya solutions. The objective of the testing is to reaffirm product/solution functionality and to observe the performance of the Avaya solutions in conjunction with the patches using typical operating parameters.

Avaya is reliant on our suppliers to validate the effectiveness of their respective Speculative Execution Vulnerability patches.

The customer should be aware that implementing these patches may result in performance degradation and that results may vary to some degree for each deployment. The customer is responsible for implementing the patches, and for the results obtained from such patches.

For more information about Speculative Execution Vulnerabilities fixes included in Avaya Aura® Release 8.x, see the following PSNs on the Avaya Support Site:

- PSN020346u - Avaya Aura® Meltdown and Spectre vulnerabilities
- PSN020369u - Avaya Aura® L1TF vulnerabilities

Fixes in AVP Utilities Release 8.1.3.1

ID	Minimum Conditions	Visible symptoms	Found in Release
AVPUTIL-1220	AVP Utilities 8.1 installed	RHSA-2020:5566 openssl-1:1.0.2k-21.el7_9.x86_64 RHSA-2020:5443 gd-2.0.35-27.el7_9.x86_64 RHSA-2020:5023 kernel-3.10.0-1160.11.1.el7.x86_64	8.1.3.1

Fixes in AVP Utilities 8.1 SSP#3

ID	Minimum Conditions	Visible symptoms	Found in Release
AVPUTIL-1209	AVP Utilities 8.1 installed	RHSA-2020:5083 microcode_ctl-2:2.1-73.2.el7_9.x86_64 RHSA-2020:5023 kernel-3.10.0-1160.6.1.el7.x86_64 RHSA-2020:5011 bind-libs-32:9.11.4-26.P2.el7_9.2.x86_64 RHSA-2020:5009 python-2.7.5-90.el7.x86_64 RHSA-2020:5002 curl-7.29.0-59.el7_9.1.x86_64 RHSA-2020:4908 libX11-1.6.7-3.el7_9.x86_64 RHSA-2020:4907 freetype-2.8-14.el7_9.1.x86_64 RHSA-2020:4350 java-1.8.0-openjdk-1:1.8.0.272.b10-1.el7_9.x86_64 RHSA-2020:4276 kernel-3.10.0-1160.2.2.el7.x86_64 RHSA-2020:4076 nss-3.53.1-3.el7_9.x86_64 RHSA-2020:4072 libcroco-0.6.12-6.el7_9.x86_64 RHSA-2020:4060 kernel-3.10.0-1160.el7.x86_64 RHSA-2020:4041 openldap-2.4.44-22.el7.x86_64 RHSA-2020:4032 dbus-1:1.10.24-15.el7.x86_64 RHSA-2020:4026 mariadb-libs-1:5.5.68-1.el7.x86_64 RHSA-2020:4011 e2fsprogs-1.42.9-19.el7.x86_64 RHSA-2020:4007 systemd-219-78.el7.x86_64 RHSA-2020:4005 libxslt-1.1.28-6.el7.x86_64 RHSA-2020:4003 NetworkManager-1:1.18.8-1.el7.x86_64 RHSA-2020:3996 libxml2-2.9.1-6.el7.5.x86_64 RHSA-2020:3978 glib2-2.56.1-7.el7.x86_64 RHSA-2020:3971 hunspell-1.3.2-16.el7.x86_64 RHSA-2020:3952 expat-2.1.0-12.el7.x86_64 RHSA-2020:3916 curl-7.29.0-59.el7.x86_64 RHSA-2020:3915 libssh2-1.8.0-4.el7.x86_64 RHSA-2020:3911 python-2.7.5-89.el7.x86_64 RHSA-2020:3908 cpio-2.11-28.el7.x86_64 RHSA-2020:3902 libtiff-4.0.3-35.el7.x86_64	8.1.3

ID	Minimum Conditions	Visible symptoms	Found in Release
		RHSA-2020:3901 libpng-2:1.5.13-8.el7.x86_64 RHSA-2020:3864 cups-libs-1:1.6.3-51.el7.x86_64 RHSA-2020:3861 glibc-2.17-317.el7.x86_64 RHSA-2020:3848 libmspack-0.5-0.8.alpha.el7.x86_64	

Fixes in AVP Utilities Release 8.1.3

ID	Minimum Conditions	Visible symptoms	Found in Release
AVPUTIL-1051	AVP Utilities 8.0.x or 8.1.x installed	Documentation: Add a SSL Certificate for Avaya Aura® AVP Utilities Serviceability Agent.	8.1.3
AVPUTIL-846	AVP Utilities 8.1.x installed	RHSA-2020:1113 - Moderate: bash security update	8.1.3
AVPUTIL-1053	AVP Utilities 8.1.x installed	RHSA-2020:3217 - Moderate: grub2 security and bug fix update	8.1.3
AVPUTIL-970	AVP Utilities 8.1.x installed	RHSA-2020:2663 - Moderate: ntp security update	8.1.3
AVPUTIL-969	AVP Utilities 8.1.x installed	RHSA-2020:2642 - Important: unbound security update	8.1.3
AVPUTIL-969	AVP Utilities 8.1.x installed	RHSA-2020:2414 - Important: unbound security update	8.1.3
AVPUTIL-967	AVP Utilities 8.1.x installed	RHSA-2020:2664 - Important: kernel security and bug fix update	8.1.3
AVPUTIL-891	AVP Utilities 8.1.x installed	RHSA-2020:2432 - Moderate: microcode_ctl security, bug fix and enhancement update	8.1.3
AVPUTIL-891	AVP Utilities 8.1.x installed	RHSA-2020:2344 - Important: bind security update	8.1.3
AVPUTIL-891	AVP Utilities 8.1.x installed	RHSA-2020:2082 - Important: kernel security and bug fix	8.1.3
AVPUTIL-955	AVP Utilities 8.1.x installed	RHSA-2020:2968 - Important: java-1.8.0-openjdk security	8.1.3
AVPUTIL-891	AVP Utilities 8.1.x installed	RHSA-2020:2894 - Important: dbus security update	8.1.3
AVPUTIL-891	AVP Utilities 8.1.x installed	RHSA-2020:3220 - Important: kernel security and bug fix	8.1.3

Fixes in AVP Utilities Release 8.1.2.1

ID	Minimum Conditions	Visible symptoms	Found in Release
AVPUTIL-855	AVP Utilities 8.1.x installed.	RHSA-2020:1512 Important/Sec. java-1.8.0-openjdk-1:1.8.0.252.b09-2.el7_8.x86_64	8.1.2

ID	Minimum Conditions	Visible symptoms	Found in Release
AVPUTIL-854	AVP Utilities 8.1.x installed.	RHSA-2020:1190 Moderate/Sec. libxml2-2.9.1-6.el7.4.x86_64	8.1.2
AVPUTIL-853	AVP Utilities 8.1.x installed.	RHSA-2020:1181 Low/Sec. unzip-6.0-21.el7.x86_64	8.1.2
AVPUTIL-852	AVP Utilities 8.1.x installed.	RHSA-2020:1180 Moderate/Sec. emacs-filesystem-1:24.3-23.el7.noarch	8.1.2
AVPUTIL-851	AVP Utilities 8.1.x installed.	RHSA-2020:1176 Low/Sec. avahi-libs-0.6.31-20.el7.x86_64	8.1.2
AVPUTIL-850	AVP Utilities 8.1.x installed.	RHSA-2020:1138 Low/Sec. gettext-0.19.8.1-3.el7.x86_64	8.1.2
AVPUTIL-849	AVP Utilities 8.1.x installed.	RHSA-2020:1135 Low/Sec. polkit-0.112-26.el7.x86_64	8.1.2
AVPUTIL-848	AVP Utilities 8.1.x installed.	RHSA-2020:1131 Moderate/Sec. python-2.7.5-88.el7.x86_64	8.1.2
AVPUTIL-845	AVP Utilities 8.1.x installed.	RHSA-2020:1112 Moderate/Sec. php-5.4.16-48.el7.x86_64	8.1.2
AVPUTIL-844	AVP Utilities 8.1.x installed.	RHSA-2020:1100 Moderate/Sec. mariadb-libs-1:5.5.65-1.el7.x86_64	8.1.2
AVPUTIL-843	AVP Utilities 8.1.x installed.	RHSA-2020:1080 Moderate/Sec. atk-2.28.1-2.el7.x86_64	8.1.2
AVPUTIL-842	AVP Utilities 8.1.x installed.	RHSA-2020:1061 Moderate/Sec. bind-32:9.11.4-16.P2.el7.x86_64	8.1.2
AVPUTIL-841	AVP Utilities 8.1.x installed.	RHSA-2020:1050 Moderate/Sec. cups-libs-1:1.6.3-43.el7.x86_64	8.1.2
AVPUTIL-840	AVP Utilities 8.1.x installed.	RHSA-2020:1022 Low/Sec. file-5.11-36.el7.x86_64	8.1.2
AVPUTIL-839	AVP Utilities 8.1.x installed.	RHSA-2020:1021 Moderate/Sec. gsettings-desktop-schemas-3.28.0-3.el7.x86_64	8.1.2
AVPUTIL-838	AVP Utilities 8.1.x installed.	RHSA-2020:1020 Low/Sec. curl-7.29.0-57.el7.x86_64	8.1.2
AVPUTIL-837	AVP Utilities 8.1.x installed.	RHSA-2020:1016 Moderate/Sec. kernel-3.10.0-1127.el7.x86_64	8.1.2
AVPUTIL-836	AVP Utilities 8.1.x installed.	RHSA-2020:1011 Moderate/Sec. expat-2.1.0-11.el7.x86_64	8.1.2
AVPUTIL-834	AVP Utilities 8.1.x installed.	RHSA-2020:1000 Moderate/Sec. rsyslog-8.24.0-52.el7.x86_64	8.1.2
AVPUTIL-833	AVP Utilities 8.1.x installed.	RHSA-2020:0630 Important/Sec. ppp-2.4.5-34.el7_7.x86_64	8.1.2
AVPUTIL-832	AVP Utilities 8.1.x installed.	RHSA-2020:0834 Important/Sec. kernel-3.10.0-1062.18.1.el7.x86_64	8.1.2
AVPUTIL-831	AVP Utilities 8.1.x installed.	RHSA-2020:0897 Important/Sec. libicu-50.2-4.el7_7.x86_64	8.1.2

Fixes in AVP Utilities Release 8.1.2

ID	Minimum Conditions	Visible symptoms	Found in Release
AVPUTIL-383	AVP Utilities 8.1.x installed.	RHSA-2019-3128 - Important: java-1.8.0-openjdk security update	8.1.1
AVPUTIL-382	AVP Utilities 8.1.x installed.	RHSA-2019:4326 - Important: fribidi security update	8.1.1
AVPUTIL-381	AVP Utilities 8.1.x installed.	RHSA-2019:3976 -Low: tcpdump security update	8.1.1
AVPUTIL-380	AVP Utilities 8.1.x installed.	RHSA-2019:3197 - Important: sudo security update	8.1.1
AVPUTIL-379	AVP Utilities 8.1.x installed.	RHSA-2019:4190 - Important: nss, nss-softokn, nss-util security update	8.1.1
AVPUTIL-378	AVP Utilities 8.1.x installed.	RHSA-2019:2829 - Important: kernel security update	8.1.1
AVPUTIL-377	AVP Utilities 8.1.x installed.	RHSA-2019:3055 - Important: kernel security update	8.1.1
AVPUTIL-376	AVP Utilities 8.1.x installed.	RHSA-2019:3834 - Important: kernel security update	8.1.1
AVPUTIL-375	AVP Utilities 8.1.x installed.	RHSA-2019:3872 -Important: kernel security update	8.1.1
AVPUTIL-374	AVP Utilities 8.1.x installed.	RHSA-2019:3979 -Important: kernel security and bug fix update	8.1.1
AVPUTIL-781	AVP Utilities 8.1.x installed.	RHSA-2020:0374 - Important: kernel update	8.1.1
AVPUTIL-782	AVP Utilities 8.1.x installed.	RHSA-2020:0196 - Important: java update	8.1.1
AVPUTIL-783	AVP Utilities 8.1.x installed.	RHSA-2020:0227 - Important: sqlite update	8.1.1
AVPUTIL-784	AVP Utilities 8.1.x installed.	RHSA-2020:0540 - Important: sudo update	8.1.1

Fixes in AVP Utilities Release 8.1.1

The following table lists the fixes in Release 8.0 which were derived from the previous Utility Services 7.1 release.

ID	Minimum Conditions	Visible symptoms	Found in Release
AVPUTIL-320	AVP Utilities 8.1 installed	126302 - RHEL 7 / 8: vim (RHSA-2019:1619) (tcp)	8.1
AVPUTIL-299	AVP Utilities 8.1 installed	update kernel for RHEL7 per RHSA-2019:1481	8.1
AVPUTIL-334	AVP Utilities 8.1 installed	[RHSA-2019:1815] java-1.8.0-openjdk-1:1.8.0.222.b10-0.el7_6.x86_64 [RHSA-2019:1884] libssh2-1.4.3-12.el7_6.3.x86_64	8.1

ID	Minimum Conditions	Visible symptoms	Found in Release
		[RHSA-2019:2030] python-2.7.5-86.el7.x86_64 [RHSA-2019:2046] polkit-0.112-22.el7.x86_64 [RHSA-2019:2049] libmspack-0.5-0.7.alpha.el7.x86_64 [RHSA-2019:2052] libjpeg-turbo-1.2.90-8.el7.x86_64 [RHSA-2019:2053] libtiff-4.0.3-32.el7.x86_64 [RHSA-2019:2057] bind-libs-32:9.11.4-9.P2.el7.x86_64 [RHSA-2019:2060] dhclient-12:4.2.5-77.el7.x86_64 [RHSA-2019:2075] binutils-2.27-41.base.el7.x86_64 [RHSA-2019:2077] ntp-4.2.6p5-29.el7.x86_64 [RHSA-2019:2079] libX11-1.6.7-2.el7.x86_64 [RHSA-2019:2091] systemd-219-67.el7.x86_64 [RHSA-2019:2110] rsyslog-8.24.0-38.el7.x86_64 [RHSA-2019:2118] glibc-2.17-292.el7.x86_64 [RHSA-2019:2136] libssh2-1.8.0-3.el7.x86_64 [RHSA-2019:2143] openssh-7.4p1-21.el7.x86_64 [RHSA-2019:2159] unzip-6.0-20.el7.x86_64 [RHSA-2019:2162] blktrace-1.0.5-9.el7.x86_64 [RHSA-2019:2169] linux-firmware-20190429-72.gitddde598.el7.noarch [RHSA-2019:2177] libsss_idmap-1.16.4-21.el7.x86_64 [RHSA-2019:2181] curl-7.29.0-54.el7.x86_64 [RHSA-2019:2189] procps-ng-3.3.10-26.el7.x86_64 [RHSA-2019:2197] elfutils-0.176-2.el7.x86_64 [RHSA-2019:2237] nspr-4.21.0-1.el7.x86_64 [RHSA-2019:2304] openssl-1:1.0.2k-19.el7.x86_64 [RHSA-2019:2327] mariadb-libs-1:5.5.64-1.el7.x86_64 [RHSA-2019:2571] pango-1.42.4-4.el7_7.x86_64 [RHSA-2019:2600] kernel-3.10.0-1062.1.1.el7.x86_64	

Fixes in AVP Utilities Release 8.0.1.1

The following table lists the fixes in Release 8.0, which were derived from the previous Utility Services 7.1 release.

ID	Minimum Conditions	Visible symptoms	Found in Release
AVPUTIL-196	Install service pack on AVP Utilities	AVP, auto reboots without installing the service pack and corrupts the system	8.0.1

Known issues and workarounds in AVP Utilities Release 8.1.x.x

Known issues and workarounds in AVP Utilities Release 8.1.3

ID	Minimum Conditions	Visible symptoms	Workaround
AVPUTIL-1133	Install service pack 002 on AVP Utilities	Red Hat curl local file overwrite (CVE-2020-8177)	None

Known issues and workarounds in AVP Utilities Release 8.1.2

ID	Minimum conditions	Visible symptoms	Workaround
AVPUTIL-829	AVP 8.1 or later on older OVA deployments	Pre-upgrade patch is not getting installed on AVPU 8.1 GA build of older OVA deployments	Workaround is user needs to login through root and remove the patchins folder using following command. #rm -rf /tmp/patchins After this one can proceed with patch installation operation.
AVPUTIL-779	AVP 8.1 or later.	Test alarms on AVPU are not working when triggered from the SMGR Inventory->Manage Serviceability Agents->Serviceability Agents-> Generate	Test alarms can be generated from the command line. Please refer to section **Generating test alarms from AVP Utilities** in **Administering Avaya Aura® AVP Utilities**.
AVPUTIL-780	AVP 8.1.2 New Encrypted OVA or later using hardened mode.	If we try to deploy AVP Utilities 8.1 Encrypted OVA via SMGR SDM/SDM client in Hardened mode dod and if we try to select the option as require passphrase at boot time then it gets stuck. The AVPU gets stuck because it enables the FIPS mode and reboots the machine and it gets stuck asking for passphrase while boot time.	If customer deploys AVPU 8.1E ova in hardened or hardened_DOD mode with encryption enabled, then while filling the configuration details, customer must make sure that he unchecks the box for 'Encryption Passphrase required at boot time'. This indicates to create a local key store which is required for uninterrupted deploy through SDM. On

ID	Minimum conditions	Visible symptoms	Workaround
			failing to uncheck the box, customer will have to manually open the VM console of the AVPU machine, and enter the encryption passphrase. Until the passphrase isn't entered, the deployment won't be marked as complete.

Known issues and workarounds in AVP Utilities Release 8.1.1

ID	Minimum conditions	Visible symptoms	Workaround

Known issues and workarounds in AVP Utilities Release 8.1

ID	Minimum conditions	Visible symptoms	Workaround

Avaya Aura® Communication Manager Messaging

Installation for Avaya Aura® Communication Manager Messaging 7.0.x.x

Backing up the software

To upgrade from earlier releases of Avaya Aura® Communication Manager Messaging, refer to one of the following guides, depending on your configuration:

- Upgrading and Migrating Avaya Aura® applications to 7.0.
- Migrating and Installing Avaya Aura® Appliance Virtualization Platform 7.0.
- Implementing Avaya Aura® Communication Manager Messaging.
- Deploying Avaya Aura® Communication Manager Messaging.

Note: Before beginning an upgrade, or any such installation or maintenance task, it is important to have a current backup of the system.

Upgrade Paths (from/to System Platform)

You can directly upgrade to CMM 7.0 from the following CMM releases:

- CMM 6.3.100 SP5 and higher server packs
- CMM 6.3 FP4 SP4, SP5, and higher server packs
- CMM 6.2 SP3 **only**
- CMM 6.0.1 SP5 **only**
- CMM 5.2.1 RFUs C1317rf+i & A9021rf+k **only**

Note: If the version of your currently installed CMM software is not listed above, you will need to upgrade to one of the latest release versions listed above **prior** to upgrading or migrating to Avaya Aura® Communication Manager Messaging 7.0.0 Service Pack 1.

File list

Download ID	Filename	File size	Notes

Note: Customers can install CMM 7.0.0.1 on a new AVP 8.0 Host. The same applies for upgrades of other Avaya Aura VMs on a shared AVP host with CMM 7.0.0.1, they also can upgrade to 8.0.

VMware vSphere (for VE installations)	Filename	PLDS File ID	PCN/PSN

Avaya Aura Communication Manager Messaging	Filename	PLDS File ID	PCN/PSN
Avaya Aura Communication Manager Messaging 7.0 VMware vAppliance OVA	CMM-07.0.0.0.441-e55-0.ova	CMM70000003	Not applicable.
Avaya Aura® Communication Manager 7.0.x VMware Tools Service Pack	KERNEL-2.6.32-573.18.1.el6.AV2.tar’	Not applicable.	Not applicable.

Avaya Aura Communication Manager Messaging	Filename	PLDS File ID	PCN/PSN
Avaya Aura® Communication Manager 7.0 Kernel Service Pack 3	KERNEL-2.6.32-642.15.1.el6.AV5.tar	CM000000710	PCN2028S
Avaya Aura® Communication Manager 7.0 Security Service Pack 4	PLAT-rhel6.5-0060.tar	CM000000709	PCN2008Su
Avaya Aura® Communication Manager 7.0.1.3 Service Pack #23853	00.0.441.0-23853.tar	CM000000708	PCN2007S-s4
Avaya Aura Communication Manager Messaging 7.0.0 Service Pack 1	CMM-00.0.441.0-0101.tar	CMM70000010	Not applicable.

Installing the release

Installation of the Communication Manager Messaging 7.0 release software from its VMware OVA is described in the Deploying Avaya Aura® Communication Manager Messaging documents.

In addition, the installation will also require Service Packs per the software reference list provided below. Read the PCN's for each of the Service Packs to familiarize oneself with the nuances of each Service Pack since some might involve reboots and commit steps. Also, wait until messaging is completely up after each install before proceeding with the next Service Pack install.

For new installations, refer to one of the following guides, depending on your configuration:

- Upgrading and Migrating Avaya Aura® applications to 7.0.
- Migrating and Installing Avaya Aura® Appliance Virtualization Platform 7.0.
- Implementing Avaya Aura® Communication Manager Messaging
- Deploying Avaya Aura® Communication Manager Messaging

Then complete the initial configuration and administration by following:

- Administering Avaya Aura® Communication Manager Messaging guide.

Troubleshooting the installation

Hardware compatibility

For hardware platform information, refer to the *Deploying Communication Manager Messaging using VMware® in the Virtualized Environment* guide.

Interoperability and requirements

See the Avaya Compatibility Matrix for full Avaya product compatibility information.

What's new in Avaya Aura® Communication Manager Messaging Release 7.0.x.x

What's new in Communication Manager Messaging 7.0.0.0

The CMM 7.0 release has been enhanced to support software currency and interoperability with the Avaya Aura® 7.0 solution.

- The Linux OS has been updated to Red Hat Enterprise Linux version 6.
- The CMM application has been integrated with the Avaya Aura® Appliance Virtualization Platform and Solution Deployment Manager.
- The CMM application has been updated to support the Avaya SIP Reference Architecture and Security guidelines for encryption protocols.

Note: The following deprecated capabilities have been removed from the CMM application with this release:

- The CMM application is no longer supported as an embedded application in the Communication Manager. With Release 7.0, the application is installed as an instance of its own virtual machine.
- The H.323/Q.Sig integration is no longer supported and has been removed. Customers should convert their CMM application to SIP integration before an upgrade to Release 7.0.
- The application migrations from Intuity Audix and Intuity Audix LX are no longer supported and have been removed in prior CMM 6.x releases. This capability to migrate within the backup and restore procedure is no longer supported in CMM

Fixes in Communication Manager Messaging Release 7.0.x.x

Fixes in Communication Manager Messaging 7.0.0.0

Fixes for the CMM 7.0 release will be provided for customer support, in periodic Service Pack patches after the GA Launch of the release.

Fixes in Communication Manager Messaging 7.0.0.1

The following table lists the fixes in this release.

ID	Visible symptoms	Release found in
MSG-13887	Fax receive failed when far-end sends PRI-EOP	
MSG-21019	COS: msgPasswordAllowed may have garbage in it, causing problems with custom COS.	
MSG-21079	/tmp/*instance has 0666 permissions	
MSG-21143	Outlook 2010: Address book: "Unknown error" when searching 'Display by Name' on 'Advanced Find'.	
MSG-21321	CMM Notify in response to subscribe malformed.	
MSG-21428	super.tab allows global viewing of postfix log files.	
MSG-21458	Outlook Address Book Search fails when there are over 2000 subscribers.	
MSG-21464	Removed set -x from getMinMaxTrustedServers.	
MSG-21539	TUI disconnects with "This Call Experiencing Difficulties" when changing a PIN within the Minimum time allowed and PIN Expiration is turned off.	
MSG-21620	Restore fails due to multiple copies of the OcTime LDAP attr.	
MSG-21660	MCAPI events not sent for some configurations (e.g., Message Manager) datadict handles Uint64 as if it is Uint32.	
MSG-21711	Possible dead air issue on attended call transfer if phone-context is present in the Contact URI.	
MSG-21865	Changing mailbox to new mailbox number, the NumericAddress is not changed; thus, creating a new subscriber with the old mailboxnumber causes a: Duplicate Mailbox error when the NumericAddress is the same as the MailboxNumber.	
MSG-21899	Resent messages generate corrupt mb inbox counts if there is an active login for the subscriber - this can cause an incorrect MWI state.	
MSG-21948	SipAgent could core-dump during an MWI operation.	
MSG-21961	Unencrypted insecure SMTP login mechanisms allowed.	
MSG-21999	Multi-page fax failing.	
MSG-22000	SMTP: Remove support for anonymous SSL/TLS ciphers.	

ID	Visible symptoms	Release found in
MSG-22027	syslog messages could be lost if too many come from one process in too short a time period.	
MSG-22070	The T38Fax timeout mechanism is broken, which could lead to fax transmission failures.	
MSG-22093	Reserved space on forwarded CA messages not reclaimed, so cstone thinks the system is out of space until an spDskMgr restart.	
MSG-22116	When a remote subscriber on an LDAP node has an email change, the MboxName attribute is incorrectly added/changed.	
MSG-22123	Dormant mailbox report takes too long with 40K users' web server can time out.	
MSG-22125	iim log files are missing after a migration due to bad /iim/admin/trace_loc file.	
MSG-22185	Reserved space on forwarded messages not reclaimed, so cstone thinks the system is out of space until a spDskMgr restart. Add additional debugging.	
MSG-22199	Can't see all IIM logs contents (e.g. some email addresses) in IE because it interprets <X> as an X tag instead of data.	
MSG-22237	MsgCore audits erroneously removing messages with missing media.	
MSG-22255	Auto Attendant dial by name to mailbox hear silence and disconnects.	
MSG-22291	CM's statapp function cannot accurately determine whether Messaging is up or down.	
MSG-22334	SMI Subscriber traffic report for remote components is wrong on SMI (for daily and monthly) but correct on the Fc.	
MSG-22335	triple_des.pm fails when calling triple_des_encrypt and triple_des_decrypt.	
MSG-22341	Occasionally garbage is seen in IMAP4 keywords results (most often seen on broadcast messages) because IMAP4 user-defined keyword performance enhancement for AM6.3 did not consider CMM - garbage in some IMAP4 user-defined keywords.	
MSG-22448	Unable to parse (and deliver) a GSM message from Aura Messaging.	
MSG-22513	LDAP FE UTP commands do not work (they hang).	
MSG-22521	SipAgent should support TLSv1.2	
MSG-22529	AAM incorrectly using SIPS URI for all outgoing SIP calls when the transport is TLS.	
MSG-22546	Anonymous Authentication advertised for SMTP.	
MSG-22568	Enhance SMTP configuration options: Allow removal of port 25 from corporate LAN.	
MSG-22600	Message Delivery fails to a local subscriber from a remote reply-able ELA list for messages initiated by a local subscriber due to authentication required for messages sent by local subscribers.	
MSG-22633	Modify default slapd log level to match openlap recommendations.	
MSG-22683	SipAgent could consume 100% CPU on the shutdown of messaging relying on the watchdog to kill the process.	
MSG-22689	cornerstone authmon process could consume ~100% CPU if rsyslog service is restarted.	

ID	Visible symptoms	Release found in
MSG-22743	AE_BADEMAIL error generated when adding an Auto-Attendant when Server-Alias is defined and not specifying an email address. Probably get the same error if 3rd party adds any mailbox w/out an email address.	
MSG-22753	The banner page uses the term Federal when the product is no longer Federal-only	
MSG-22767	Remove possibility for file-descriptor link in libmime_lib.so	
MSG-22815	abs_web_cache incorrectly assumes an average of 180 bytes/subscriber, which causes unnecessary rebuilds of that cache.	
MSG-22850	The call is dropped when Call-Answer-Disclaimer and Call-Answer-Disable features are both enabled, a subscriber has the 'disclaimer' Call-Answer permission type, and they attempt to use Call-Answer-Disable.	
MSG-22851	When the green-feature: 'Call Answer Disclaimer' is enabled, the 'Permission Type' label: 'disclaimer' label is blank on the COS SMI form and the Custom COS section of the Subscriber SMI form.	
MSG-22898	Limits form: Label for 'Maximum List Entries' is wrong.	

Known issues and workarounds in Communication Manager Messaging Release 7.0.x.x

Known issues and workarounds in Communication Manager Messaging Release 7.0.0.1

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Minimum conditions	Visible symptoms	Workaround
MSG-22700	If an administrative account (dadmin, craft, etc.) gets locked-out, the mechanism to notify someone is broken.		Restart of syslog or restart of the messaging VM will resolve this problem. The steps to restart rsyslog and restart messaging via the command-line are as follows: • To restart rsyslog on CMM: */etc/init.d/rsyslog restart* • To restart messaging: Run *stopapp -s Audix* to stop messaging and wait a few minutes for messaging to stop completely. Then, run *startapp -s Audix* to restart messaging.

Avaya Aura® Appliance Virtualization Platform

What's new in Avaya Aura® Appliance Virtualization Platform Release 8.1.3.x

What's new in Avaya Aura® Appliance Virtualization Platform Release 8.1.3.1

vmware_flags tool to enable the Guest VM flags for MCEPSC vulnerability mitigation now takes for each VMs individually

Pulling out ethernet cable or setting eth port down to produce ETH_FAULT event for active-active and active-standby use cases

What's new in Avaya Aura® Appliance Virtualization Platform Release 8.1.3

For more information see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

What's new in Avaya Aura® Appliance Virtualization Platform Release 8.1.2.1

Avaya Aura® Appliance Virtualization Platform 8.1.2.1 has introduced new security service pack bundle. This is useful for customers who want to get only the security updates and not the full feature pack or service pack. The ISO, feature pack or service pack will continue to bundle security updates like before.

Please refer to PCN AVP SSP 8.1.x – PCN 2122S for instructions on how to download and install the security service pack.

What's new in Avaya Aura® Appliance Virtualization Platform Release 8.1.2

Avaya Aura® Appliance Virtualization Platform 8.1.2 has ability to automatically delete snapshots. An administrator can configure snapshot to be deleted between 1 and 30 days after being generated. If this feature is enabled, the snapshot alarm will be generated 3 days prior to snapshot deletion.

For more information see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

What's new in Avaya Aura® Appliance Virtualization Platform Release 8.1.1

For more information see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

Security Service Packs

AVP releases ESXi 6.5 Platform Security Service Packs (SSPs) Only without any SP/FP.

Beginning December 2020, SSPs will also be released on a more frequent cadence. This means that SSPs may also be available between application Service Packs/Feature Packs. SSP required artifacts and fix IDs will no longer be tracked in the Release Notes. For further information on contents and installation procedures, please see PCN AVP SSP 8.1.x – PCN 2122S.

AVP releases Security Service Packs (SSPs) Only without any SP/FP. Beginning December 2020, SSPs will also be released on a more frequent cadence.

Download ID	Filename	File size	Notes
AVP00000078	PLAT-avaya-avp-e65-004.tar	330 MB	AVP Security service pack #4. Use this security service pack on any 8.1.x system to get the latest ESXi security till 2nd updates of November 2020.
AVP00000073	PLAT-avaya-avp-e65-003.tar	462 MB	AVP Security service pack #3. Use this security service pack on any 8.1.x system to get the latest ESXi security updates till November 2020.
AVP00000068	PLAT-avaya-avp-e65-002.tar	461 MB	AVP Security service pack #2. Use this security service pack on any 8.1.x system to get the latest security updates.
AVP00000065	PLAT-avaya-avp-e65-001.tar	460 MB	AVP Security service pack #1. Use this security service pack on any 8.1.x system to get the latest security updates.

Required artifacts for Avaya Aura® Appliance Virtualization Platform Release 8.1.3.1

Download ID	Filename	File size	Notes
AVP00000076	avaya-avp-8.1.3.1.0.03.iso	454 MB	Use this ISO file for new AVP 8.1.3.1 new installations. This ISO also contains the upgrade-avaya-avp-8.1.3.1.0.03.zip upgrade bundle
AVP00000077	upgrade-avaya-avp-8.1.3.1.0.03.zip	187 MB	upgrade-avaya-avp- 8.1.3.1.0.03.zip upgrade bundle. Use this ZIP file for an upgrade from pervious 7.x, 8.0.x or 8.1.x releases.
AVP00000078	PLAT-avaya-avp-e65-004.tar	330 MB	AVP Security service pack #4. Use this security service pack on any 8.1.x system to get the latest security updates.

Required artifacts for Avaya Aura® Appliance Virtualization Platform Release 8.1.3

Download ID	Filename	File size	Notes
AVP00000066	avaya-avp-8.1.3.0.0.15.iso	454 MB	Use this ISO file for new AVP 8.1.3 new installations. This ISO also contains the upgrade-avaya-avp-8.1.3.0.0.15.zip upgrade bundle
AVP00000067	upgrade-avaya-avp-8.1.3.0.0.15.zip	187 MB	upgrade-avaya-avp- 8.1.3.0.0.15.zip upgrade bundle. Use this ZIP file for an upgrade from pervious 7.x, 8.0.x or 8.1.x releases.
AVP00000068	PLAT-avaya-avp-e65-002.tar	461 MB	AVP Security service pack. Use this security service pack on any 8.1.x system to get the latest security updates.

Required artifacts for Avaya Aura® Appliance Virtualization Platform Release 8.1.2.1

The following section provides Avaya Aura® Appliance Virtualization Platform downloading information.

Find patch information at https://support.avaya.com. For more details, see PCN2097S on the Avaya Technical Support site.

Download ID	Filename	File size	Notes
AVP00000063	avaya-avp-8.1.2.1.0.06.iso	465 MB	Use this ISO file for new AVP 8.1.2 new installations. This ISO also contains the upgrade-avaya-avp-8.1.2.1.0.06.zip upgrade bundle

Download ID	Filename	File size	Notes
AVP00000064	upgrade-avaya-avp-8.1.2.1.0.06.zip	193 MB	upgrade-avaya-avp- 8.1.2.0.0.09.zip upgrade bundle. Use this ZIP file for an upgrade from pervious 7.x, 8.0.x or 8.1.x releases.
AVP00000065	PLAT-avaya-avp-e65-001.tar	460 MB	AVP Security service pack. Use this security service pack on any 8.1.x system to get the latest security updates.

Required artifacts for Avaya Aura® Appliance Virtualization Platform Release 8.1.2

The following section provides Avaya Aura® Appliance Virtualization Platform downloading information.

Find patch information at https://support.avaya.com. For more details, see PCN2097S on the Avaya Technical Support site.

Download ID	Filename	File size	Notes
AVP00000057	avaya-avp-8.1.2.0.0.09.iso	465 MB	Use this ISO file for new AVP 8.1.2 new installations. This ISO also contains the upgrade-avaya-avp-8.1.2.0.0.09.zip upgrade bundle
AVP00000058	upgrade-avaya-avp-8.1.2.0.0.09.zip	193 MB	upgrade-avaya-avp- 8.1.2.0.0.09.zip upgrade bundle. Use this ZIP file for an upgrade from pervious 7.x, 8.0.x or 8.1.x releases.
AVP00000059	avaya-avp-src-8.1.2.0.0.09.iso	8.5 MB	Open-source component used and publish for 8.1.2. Release in iso.

Required artifacts for Avaya Aura® Appliance Virtualization Platform Release 8.1.1

The following section provides Avaya Aura® Appliance Virtualization Platform downloading information.

Find patch information at https://support.avaya.com. For more details, see PCN2097S on the Avaya Technical Support site.

Download ID	Filename	File size	Notes
AVP00000048	avaya-avp-8.1.1.0.0.17.iso	487 MB	Use this ISO file for new AVP 8.1.1 new installations. This ISO also contains the upgrade-avaya-avp-8.1.1.0.0.17.zip upgrade bundle.
AVP00000049	upgrade-avaya-avp-8.1.1.0.0.17.zip	199 MB	upgrade-avaya-avp- 8.1.1.0.0.17.zip upgrade bundle. Use this ZIP file for an upgrade from AVP 7.x or 8.0.x or 8.1.
AVP00000050	avaya-avp-src-8.1.1.0.0.17.iso	8.5 MB	Open-source component used and publish for 8.1.1. Release in iso.

Required artifacts for Avaya Aura® Appliance Virtualization Platform Release 8.1

The following section provides Avaya Aura® Appliance Virtualization Platform downloading information.

Find patch information at https://support.avaya.com. For more details, see PCN2097S on the Avaya Technical Support site.

Download ID	Filename	File size	Notes
AVP00000040	avaya-avp-8.1.0.0.0.13.iso	476 MB	Use this ISO file for new AVP 8.1 new installations. This ISO also contains the upgrade-avaya-avp-8.1.0.0.0.13.zip upgrade bundle.

Download ID	Filename	File size	Notes
AVP00000041	upgrade-avaya-avp-8.1.0.0.0.13.zip	197 MB	Use this ZIP file for upgrade from AVP 7.x or 8.0 or 8.0.x.
AVP00000042	avaya-avp-src-8.1.0.0.0.13.iso	8.5 MB	Avaya AVP Source iso for open source components
AVP00000043	listmem.sh	2.7 KB	Pre-upgrade memory check utility script

Enhanced Access Security Gateway (EASG)

EASG provides a secure method for Avaya services personnel to access the Avaya Aura® Application remotely and onsite. Access is under the control of the customer and can be enabled or disabled at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management, and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck.

Refer to *the Deploying Avaya Aura® Appliance Virtualization Platform Release 8.1.x* document for instructions on enabling and disabling EASG, and for instructions on installing the EASG site certificates.

Speculative Execution Vulnerabilities (includes Meltdown and Spectre and also L1TF Vulnerabilities)

In order to help mitigate the Speculative Execution Vulnerabilities, the processor manufacturers and operating system developers provide software patches to their products. These are patches to the processors, hypervisors, and operating systems that the Avaya solutions utilize (they are not patches applied to the Avaya developed components of the solutions).

Once these patches are received by Avaya, they are tested with the applicable Avaya solutions to characterize any impact on the performance of the Avaya solutions. The objective of the testing is to reaffirm product/solution functionality and to observe the performance of the Avaya solutions in conjunction with the patches using typical operating parameters.

Avaya is reliant on our suppliers to validate the effectiveness of their respective Speculative Execution Vulnerability patches.

The customer should be aware that implementing these patches may result in performance degradation and that results may vary to some degree for each deployment. The customer is responsible for implementing the patches, and for the results obtained from such patches.

For more information about Speculative Execution Vulnerabilities fixes included in Avaya Aura® 7.x Products, see the following PSNs on the Avaya Support Site:

- PSN020346u - Avaya Aura® Meltdown and Spectre vulnerabilities
- PSN020369u - Avaya Aura® L1TF vulnerabilities

Installation for Avaya Aura® Appliance Virtualization Platform Release 8.1.x.x

Installation for Avaya Aura® Appliance Virtualization Platform Release 8.1.3

Procedure to install Appliance Virtualization Platform 8.1.3 remains the same as previous releases.

Installation for Avaya Aura® Appliance Virtualization Platform Release 8.1.2

Procedure to install Appliance Virtualization Platform 8.1.2 remains the same as that of 8.1.1.

Installation for Avaya Aura® Appliance Virtualization Platform Release 8.1.1

The customers can now migrate from System Platform to AVP 8.1.1 on the same hardware using the standard migration process. Note that migration from System Platform to AVP 8.1 still requires workarounds mentioned in section **Migrating from SP 6.x to AVP 8.1 on the same hardware** below. Also, the memory requirements mentioned to install or migrate to AVP 8.1 still apply to AVP 8.1.1.

Installation of Avaya Aura® Appliance Virtualization Platform Release 8.1

This release can be used as a new install of AVP 8.1 or as an upgrade to an existing AVP 7.x or 8.0.x installation or migration from System Platform 6.x. For an upgrade from AVP, it will not be necessary to reinstall the guest VMs.

Please note that VMware ESXi 6.5 hypervisor on AVP 8.1 uses about 600 MB of more memory than ESXi 6.0 did on AVP 8.0 – 8.0.x. If you're using Avaya Aura® System Manager Solution Deployment Manager 8.1 or SDM Client 8.1 to perform the upgrade to AVP 8.1, SDM will check for available memory on the server before continuing with the upgrade. If there is insufficient memory available on the server, SDM will display a message to either upgrade the memory on the common server or upgrade to a later generation of the common server with more memory before upgrading to AVP 8.1. A memory check is not required on the S8300E server.

The memory check can also be performed manually, as shown below. Make sure all Virtual Machines (VMs) are running before performing the memory check.

Following amount of free memory must be available for successful upgrades:

1. For upgrade from System Platform (XEN) to AVP 7.1.2 or greater (ESXI 6.0) > **3700** MB.
2. For upgrade from AVP 7.0.x (ESXI 5.5) to AVP 7.1.2 or greater (ESXI 6.0) > **1126** MB.
3. For upgrade from AVP 7.0.x (ESXI 5.5) to AVP 8.1 (ESXI 6.5) > **1800** MB.
4. For upgrade from AVP 7.1.2 or greater (ESXI 6.0) to AVP 8.1 (ESXI 6.5) > **600** MB.
5. For upgrade from System Platform to AVP 8.1 (ESXI 6.5) > **4300** MB.

Manual steps to be executed on an existing AVP installation to check is sufficient memory is available to upgrade to AVP 8.1:

- Log on to AVP host using an SSH client.
- Execute the following command:

```
memstats -r group-stats -s name:availResv:consumed -l 1 -u mb
```

- Look for an output similar to the following:

```
~ # memstats -r group-stats -s name:availResv:consumed -l 1 -u mb
GROUP STATS
-----------
   Start Group ID   : 0
   No. of levels    : 1
   Unit             : MB
   Inclusion filter : (all)
   Exclusion filter : (none)
   Selected columns : gid:name:availResv:consumed

-----------------------------------------------------------
     gid                        name  availResv   consumed
-----------------------------------------------------------
       0                        host       4919       4585
-----------------------------------------------------------
```

- Note the value displayed underneath the "availResv" column and ensure that this value is > 600 MB if you are migrating from AVP 7.1.2 or greater (ESXI 6.0) to AVP 8.1 (ESXI 6.5).
- If this value is < 600 MB, then before being able to upgrade to AVP 8.0.x, either the memory of the server must be upgraded, or the server must be upgraded to a later generation with more memory.

Using the memory check script on an existing AVP installation to check if sufficient memory is available to upgrade to AVP 8.1:

```
[admin@avpu816:~] sh listmem.sh

Please select one of the options below:

              1. For upgrade from System Platform (XEN) to AVP 7.1.2 or greater(ESXI
6.0)
              2. For upgrade from AVP 7.0.x (ESXI 5.5) to AVP 7.1.2 or greater (ESXI
6.0)
              3. For upgrade from AVP 7.0.x (ESXI 5.5) to AVP 8.1 (ESXI 6.5)

              4. For upgrade from AVP 7.1.2 or greater (ESXI 6.0) to AVP 8.1 (ESXI
6.5)
              5. For upgrade from System Platform to AVP 8.1 (ESXI 6.5)


2

Checking mem for upgrade from AVP 7.0.x (ESXI 5.5) to AVP 7.1.2 (ESXI 6.0)

Memory > 1126. No upgrade required (47344MB unreserved memory available)
```

Manual steps to be executed on an existing System Platform installation to check is sufficient memory is available to migrate to AVP 8.1:

Using System Platform Web console:

- Logon to System Platform Web console as user admin.
- Navigate to Server Management → System Information → Memory
- Note the Available value displayed and ensure that this is > 4300 MB. If < 4300MB, then before being able to upgrade to AVP 8.1, either the memory of the server must be upgraded, or the server must be upgraded to a later generation with more memory.

Using Dom0 Command Line Interface:

- Logon to System Platform Dom0 CLI as user admin using an SSH client.
- Switch user to root: su - root
- Execute the following command on System Platform >= 6.4: `xl info | grep memory`
- Execute the following command on System Platform < 6.4: `xm info | grep memory`
- Look for output similar to the following:

```
[root@Dom0 ~]# xl info | grep memory
total_memory           : 65501
free_memory            : 24879
```

- Note the free_memory value displayed and ensure that this is > 4300MB.
- If < 4300MB, then before being able to upgrade to AVP 8.1, either the memory of the server must be upgraded, or the server must be upgraded to a later generation.

A memory check script is also available to determine if you will need additional memory before upgrading to 8.1.x.

Reference PSN027060u – Avaya Aura® Appliance Virtualization Platform Release 7.1.2 and higher Memory Upgrade Instructions and RDIMM Replacement Guidelines for details and where to download the script, “listmem.sh”

Using the memory check script on an existing System Platform installation to check if sufficient memory is available to upgrade to AVP 8.1:

```
[root@sysplat ~]# sh listmem.sh
Please select one of the options below:
              1. For upgrade from System Platfrom (XEN) to AVP 7.1.2 or greater(ESXI
6.0)
              2. For upgrade from AVP 7.0.x (ESXI 5.5) to AVP 7.1.2 or greater (ESXI
6.0)
              3. For upgrade from AVP 7.0.x (ESXI 5.5) to AVP 8.1 (ESXI 6.5)
              4. For upgrade from AVP 7.1.2 or greater (ESXI 6.0) to AVP 8.1 (ESXI
6.5)
              5. For upgrade from System Platfrom to AVP 8.1 (ESXI 6.5)


5
Checking mem for upgrade from System Platfrom (XEN) to AVP 8.1 (ESXI 6.5)
Low memory, upgrade required (4108MB free memory available)
Memory Device
        Size: 2048 MB
        Locator: DIMM_A1
Memory Device
        Size: 2048 MB
        Locator: DIMM_A2
Memory Device
        Size: 2048 MB
        Locator: DIMM_A3
Memory Device
        Size: 2048 MB
        Locator: DIMM_A4
Memory Device
        Size: 2048 MB
        Locator: DIMM_A5
Memory Device
        Size: 2048 MB
        Locator: DIMM_A6
Memory Device
        Size: No Module Installed
        Locator: DIMM_B1
Memory Device
        Size: No Module Installed
        Locator: DIMM_B2
Memory Device
        Size: No Module Installed
        Locator: DIMM_B3
Memory Device
        Size: No Module Installed
        Locator: DIMM_B4
Memory Device
        Size: No Module Installed
        Locator: DIMM_B5
Memory Device
        Size: No Module Installed
        Locator: DIMM_B6
```

If the memory check shows that extra memory is needed before upgrading to AVP 8.1, please refer to **PSN027060u – Avaya Aura® Appliance Virtualization Platform Release 7.1.2 and higher Memory Upgrade Instructions and RDIMM Replacement Guidelines** for details on the memory kit and instructions on upgrading the server memory.

Note: Memory check is not required on the S8300E server.

Refer to the *Deploying Avaya Aura® Appliance Virtualization Platform Release 8.1***.**x and *Upgrading Avaya Aura® Appliance Virtualization Platform Release 8.1*.x documents for instructions on new installs and upgrades of AVP. Ensure to upgrade SDM to Release 8.1.x first before using it to upgrade AVP.

Restoring software to the previous version

Backup the Virtual application Machines using the applications' standard backup procedures before rolling back AVP. This is just a precaution in case anything goes wrong, and you have to reinstall and restore.

For rolling back from AVP 8.1 to AVP 8.0.x:

From AVP root prompt execute the following command to stop all Virtual Machines:

```
/opt/avaya/bin/stopallvms.py
```

Unzip the `upgrade-avaya-avp-8.0.0.0.0.06.zip` file and copy the `avaya-avp-8.0.0.0.0.06.zip` file to the system's local disk, `/vmfs/volumes/server-local-disk`.

Run the rollback command and reboot the host. The full pathname to the rollback patch is required. You cannot use a relative path.

```
/opt/avaya/bin/rollback_bootbank.sh /vmfs/volumes/server-local-disk/avaya-avp-8.0.0.0.0.06.zip
/opt/avaya/bin/avpshutdown.sh –r
```

If SDM has trouble connecting with the AVP, you may need to generate a new AVP certificate by selecting the AVP host on SDM then selecting "More Actions" → "Generate/Accept Certificate".

For rolling back to any other release, please refer to **Upgrading Avaya Aura® Appliance Virtualization Platform Release 8.0.x** document for instructions.

Migrating from SP 6.x to AVP 8.1 on the same hardware

AVP 8.1 uses more memory during the bootup sequence than AVP 8.0.x or 7.1.x. As a result, the System Platform bootloader cannot load all AVP 8.1 modules. Hence, the migration step from System Platform 6.x to AVP 8.1 on the same hardware has an intermediate step of migrating to AVP 8.0.1.1. However, the virtual machines installed on System Platform 6.x will be upgraded to release 8.1 in a single step. So we need to use AVP8.0.1.1 iso as well as its version.xml file for intermediate migration platform followed by upgradation of platform OS.

The upgrade steps will be as follows:

- Step 1: SDM 8.1 upgrades System Platform 6.x and VMs 6.x to AVP 8.0.1.1 and VMs to their respective 8.1 versions. To do this step, the customer must sync AVP 8.0.1.1 ISO file and 8.1 versions of the VM OVAs in the SMGR SDM being used to upgrade the System Platform during remote installation. The customer must then proceed with the migration steps as documented in 'Upgrading Avaya Aura® Appliance Virtualization Platform' guide.
- Step 2: (Manual step) SDM upgrades AVP 8.0.1.1 to AVP 8.1. VMs stay on their 8.1 versions. To do this step, the customer must select the AVP 8.1 upgrade zip file in the SMGR SDM being used to upgrade AVP to 8.1. The customer must then proceed with the AVP upgrade steps documented in the same document mentioned in the above step.

Fixes in Avaya Aura® Appliance Virtualization Platform Release 8.1.3.1

ID	Minimum Conditions	Visible symptoms	Found in Release
AVP-1285	AVP 8.1.3 is installed	VMSA-2020-0026 – Vmware ESXi 6.5 Multiple Vulnerabilities of use-after-free error exists in the XHCI USB controller and privilege escalation (CVE-2020-4004, CVE-2020-4005)	8.1.3
AVP-1251	AVP 8.1.3 is installed	VMSA-2020-0023 - VMware ESXi updates address multiple security vulnerabilities (CVE-2020-3981, CVE-2020-3982, CVE-2020-3992, CVE-2020-3993, CVE-2020-3994, CVE-2020-3995)	8.1.3
AVP-1325	AVP 8.1.3 is installed	The AVP SSP patch cannot be applied on AVP version 8.1 and 8.1.2	8.1.3
AVP-1293	AVP 8.1.3 is installed	s8300e still not recognized in gateway and applications	8.1.3
AVP-1226	AVP 8.1.3 is installed	Need a generic 'swversion -s' command output as parse-able	8.1.3
AVP-1047	AVP 8.1.3 is installed	Tool to enable the Guest VM flags for MCEPSC vulnerability mitigation now takes for each VMs individually	8.1.3
AVP-717	AVP 8.1.3 is installed	Pulling out ethernet cable or setting eth port down to produce ETH_FAULT event for active-active and active-standby use cases	8.1.3

Fixes in Avaya Aura® Appliance Virtualization Platform 8.1.3

ID	Minimum Conditions	Visible symptoms	Found in Release
AVP-1027	AVP 8.1.3 is installed	METco: PSOD on AVP 8.1.1.0.0.17 (esxi iLO driver issue)	8.1.1
AVP-1030	AVP 8.1.x is installed	Get error applying 3rd party certificate to AVP	8.1

ID	Minimum Conditions	Visible symptoms	Found in Release
AVP-1140	AVP 8.1.x is installed	port 9080 is open on AVP and see if we can disable it OR needs to be documented in port matrix	8.1.2
AVP-1134	AVP 8.1.x is installed	VMSA-2020-0011 : Client updates address multiple security vulnerabilities (CVE-2020-3957, CVE-2020-3958, CVE-2020-3959)	8.1.2
AVP-1167	AVP 8.1.x is installed	VMSA-2020-0015 - ESXi security vulnerabilities (CVE-2020-3962, CVE-2020-3963, CVE-2020-3964, CVE-2020-3965, CVE-2020-3966, CVE-2020-3967, CVE-2020-3968, CVE-2020-3969, CVE-2020-3970, CVE-2020-3971)	8.1.2
AVP-1166	AVP 8.1.x is installed	VMSA-2020-0012 - VMware ESXi updates address out-of-bounds read vulnerability (CVE-2020-3960)	8.1.2
AVP-1184	AVP 8.1.x is installed	VMSA-2020-0018: Partial denial of service vulnerability via authentication services (CVE-2020-3976)	8.1.2

Fixes in Avaya Aura® Appliance Virtualization Platform 8.1.2.1

ID	Minimum Conditions	Visible symptoms	Found in Release
None			

Fixes in Avaya Aura® Appliance Virtualization Platform 8.1.2

ID	Minimum Conditions	Visible symptoms	Found in Release
AVP-948	AVP 8.1.x is installed	VMSA-2019-0022 - ESXi DaaS updates address OpenSLP remote code execution vulnerability (CVE-2019-5544	8.1.1
AVP-951	AVP 8.1.x is installed	VMSA-2019-0019 - ESXi denial-of-service vulnerability (CVE-2019-5536)	8.1.1
AVP-917	AVP 8.1.x is installed	VMSA-2019-0014 - address use-after-free and denial of service vulnerabilities. (CVE-2019-5527, CVE-2019-5535)	8.1.1
AVP-873	AVP 8.1.x is installed	VMSA-2019-0011 - Partial denial of service vulnerability in ESXi hostd process (CVE-2019-5528)	8.1.1
AVP-936	AVP 8.1.x is installed	VMSA-2019-0020 - Hypervisor-Specific Mitigations for Denial-of-Service and Speculative-Execution Vulnerabilities (CVE-2018-12207, CVE-2019-11135)	8.1.1
AVP-1069	AVP 8.1.x is installed	VMSA-2020-0008 : Stored Cross-Site Scripting (XSS) vulnerability (CVE-2020-3955)	8.1.1

ID	Minimum Conditions	Visible symptoms	Found in Release
AVP-907	AVP is installed in hardened mode and the license mode is changed.	Custom banners were overwritten in hardened system on license mode change	8.1.x or 7.1.x

Fixes in Avaya Aura®Appliance Virtualization Platform 8.1.1

Note: AVP 8.1 is based on VMware ESXi 6.5.

ID	Minimum Conditions	Visible symptoms	Found in Release
AVP-865	AVP 8.1 installed	Patching AVP from SDM failed	8.1
AVP-836	AVP upgraded to 8.1 and remote syslog over TLS enabled	AVP 8.1 was not able to forward syslogs over syslog-tls port(6514)	8.1
AVP-817	Upgrade from System Platform to AVP 8.1	Upgrade from System Platform to AVP 8.1 failed and a workaround had to be applied	8.1
AVP-866	AVP 7.1.3.3 or higher installed	SYS_FAULT alarm was being generated on AVP systems	7.1.3.3
AVP-750	AVP with S8300E card	On running ‘show mm’ on a gateway or ‘list configuration media-gateway’ on CM S8300E hardware and firmware versions are not reported	7.1.3.2
AVP-704	AVP 7.1.2 or higher installed	On HP G9 DISK_FAULT alarm could only be cleared by graceful reboot	7.1.3
AVP-898	AVP 7.1.3.3 or higher installed	AVP CPU occupancy spiked up to 100% for 10 minutes when SMGR jboss was restarted	7.1.3.3
AVP-876	AVP on dual CPU ACP-120 systems	The following CPU alarm was observed ‘System Board 1 Riser 2 alarm on single CPU ACP120’	8.0.1
AVP-860	AVP installed	No easy way to recover if the customer selected the Equinox license during AVP installation.	7.1
AVP-908	AVP 8.1 installed	VMSA-2019-0013 - Address command injection and information disclosure vulnerabilities. (CVE-2017-16544, CVE-2019-5531, CVE-2019-5532, CVE-2019-5534)	8.1
AVP-842	AVP 8.1 installed	VMSA-2019-0008 - Microarchitectural Data Sampling (MDS) Vulnerabilities for Hypervisors	8.1

Fixes in Avaya Aura® Appliance Virtualization Platform 8.1

Note: AVP 8.1 is based on VMware ESXi 6.5.

ID	Minimum Conditions	Visible symptoms	Found in Release
AVP-821	NA	Addressed VMSA-2019-0006: VMware ESXi updates address multiple out-of-bounds read vulnerabilities	NA
AVP-815	NA	Addressed VMSA-2019-0005: Multiple vulnerabilities (Remote Check) (tcp)	NA
AVP-737	Upgrade from AVP 7.0.1.0.0.5 to AVP 8.0.1	AVP upgrade failed due to insufficient free space in bootbank	8.0.1

ID	Minimum Conditions	Visible symptoms	Found in Release
AVP-730	AVP installed	AVP alarms were not getting generated	8.0.1
AVP-704	AVP installed on Dell R630 underwent an ungraceful shutdown	AVP reported a DISK_FAULT warning alarm	7.1.2
AVP-769	Shutdown or reboot AVP from SDM or web UI	VM may have degraded performance or report corrupted disk and fail to boot	7.1.3

Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform Release 8.1.x.x

Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform Release 8.1.3

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Minimum conditions	Visible symptoms	Workaround
AVP-1122	AVP on Dell R630 systems	RAID Battery failure on Dell R630 generates BATTERY_FAULT instead of DISKBATTERY_FAULT	None
AVP-1182	AVP on any server type	NTP server details on AVP are not updated properly through SDM	None

Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform Release 8.1.2

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Minimum conditions	Visible symptoms	Workaround
AVP-1041	AVP on any server type	Adding AVP to a vCenter system breaks AVP datastore and functionality.	This currently does not have a workaround. vCenter connectivity to AVP is not supported.
AVP-1027	AVP on HP systems	Occasional restarts of the AVP are observed.	None
AVP-976	AVP on Dell R630 systems	Alarms may not be seen on Dell R630 for up to 12 hours after the event	None

Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform Release 8.1.2

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Minimum conditions	Visible symptoms	Workaround
AVP-881	AVP on Dell systems	While patching AVP Utilities from SMGR SDM on Dell systems, a warning message is displayed suggesting that the hardware model name is not known.	This warning can be ignored.

ID	Minimum conditions	Visible symptoms	Workaround
AVP-1027	AVP 8.1.1 running on an HP DL360 G8 server, and is seeing occasional restarts of the ESXi host.	If customer enabled iLO on this G8 even though they shouldn't on AVP, but nonetheless, we should probably make sure to pick up this updated driver to prevent this from potentially causing an outage anyways.	NA

Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform Release 8.1.1

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Minimum conditions	Visible symptoms	Workaround
AVP-656	AVP on HP systems	AVP syslog.log and US remote.log filling with 'handler could not derive port number messages'	Please reach out to Avaya services to resolve this alarm using a workaround
AVP-706	AVP 8.1 on HP systems	AVP shows redundancy lost on single power supply systems	Please reach out to Avaya services to resolve this alarm using a workaround

Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform Release 8.1

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Minimum conditions	Visible symptoms	Workaround
AVP-762	AVP installed	The command **/opt/avaya/bin/weblmurl** resulted in a failure.	None
AVP-816	Installation of AVP on S8300E	AVP does not come up after the DVD drive is ejected during installation	Manually restarting the S8300E card by removing it from the MG chassis and putting it back in solves the problem.
AVP-777	Delete a VM from AVP and install a new one from SDM and power on the new VM	After the new VM gets deployed, it cannot power on because of lack of memory	Wait for about 30 minutes before powering on the new VM.
AVP-774	Upgrade from AVP 8.0 to 8.1 on CSR2 HP P1 server	AVP cannot be upgraded to 8.1 because of resource check failure	Please check the upgrade section above
AVP-750	Run 'show mm' on the G4xx gateway or 'list configuration media-gateway' on CM	S8300E hardware and firmware versions are not reported	None
AVP-747	AVP running on HP systems	AVP incorrectly reports RAID battery failure alarms	Update to the latest Avaya provided BIOS on the HP server

ID	Minimum conditions	Visible symptoms	Workaround
AVP-817	SP to AVP same box migration failure	The migration process stops midway during the host migration stage	Need to use AVP8.0.1.1 iso and its version.xml to use 2 stage migration as SP→AVP8.0 migration→AVP8.1 host upgrade
AVP-836	Upgrade AVP 7.x or 8.x to 8.1 and configure encrypted syslog	After upgrading to AVP 8.1 from a previous version of AVP, configuring syslog over TLS transport fails on port 6514	None

Languages supported

Languages supported in this release:

- English

Avaya Aura® G430 and G450 Media Gateways

What's new in Avaya Aura® G430 and G450 Media Gateways Release 8.1.x.x

What's new in G430 and G450 Media Gateways Release 8.1.3

Enhancement	Description
G450 Hardware	Added support for the new G450 DC power supply.

What's new in G430 and G450 Media Gateways Release 8.1.2

The following table lists enhancements in this release.

Enhancement	Description
G430/G450 Data Privacy, Security	Two new CLI commands were added to provide the ability to set the duration that logs are retained: • **set logging file retention <retention_days>** retention_days defines the period of time in days that log content will be retained. It must be either: ○ a value between 1 and 9999, inclusive (default value is 30 days) ○ unlimited • **show logging file retention**
G430/G450 Data Privacy, Security	The following CLI commands now require "**admin**" level permission to invoke: 'show events' 'show logging file content' 'show logging file retention' 'set logging file condition' 'set logging file enable' 'set logging file disable' 'set logging cdr file content' 'set logging session condition' 'set logging session enable' 'set logging session disable' 'set logging server' 'set logging server enable' 'set logging server disable' 'set logging server facility' 'set logging server access-level' 'set logging file retention' 'clear logging cdr file'

What's new in G430 and G450 Media Gateways Release 8.1.1

For more information see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

Installation for Avaya Aura® G430 and G450 Media Gateways Release 8.1.x.x

Required patches

The following version of firmware is only applicable for G430 and G450 Media Gateways. Find patch information for other Avaya Aura® Media Branch Gateway products at https://support.avaya.com.

IMPORTANT!

- **G430 Gateways running a release prior to Release 7.1.2 Build 39.5.0** MUST first install Release 7.1.0.4 (Build 38.21.02 or Build 38.21.32) or newer 38.xx.yy release before installing Release 8.1.x.y.

- **G450 Gateways running a release prior to Release 7.1.2 Build 39.5.0** MUST first install Release 7.1.0.5 (Build 38.21.03 or Build 38.21.33) or newer 38.xx.yy release before installing Release 8.1.x.y.

If you attempt to download Release 8.1.x.y prior to having installed Release 7.1.0.4 or Release 7.1.0.5 and execute the "`show download software status 10`" command, the system will display the following error message:

> Incompatible software image for this type of device.

After installing Release 7.1.0.4 or Release 7.1.0.5, you must enable or disable Avaya Logins before downloading Release 8.1.x.y via CLI or SNMP. You can enable or disable Avaya Logins by using one of the following CLI commands:

- `login authentication services` – To enable Avaya Logins.
- `no login authentication services` – To disable Avaya Logins.

If you neglect to enable or disable Avaya Logins by using one of the above commands, you will be prompted to do so when any of the following CLI commands are used to perform a firmware download:

- `copy ftp SW_imageA`
- `copy ftp SW_imageB`
- `copy scp SW_imageA`
- `copy scp SW_imageB`
- `copy tftp SW_imageA`
- `copy tftp SW_imageB`
- `copy usb SW_imageA`
- `copy usb SW_imageB`

Notes:

- The special "dadmin" login account previously associated with ASG in releases earlier than Release 7.1.2 is no longer available.
- The gateway defaults to using TLS 1.2, PTLS, and unencrypted H.248 communication with CM. Refer to the "set link-encryption" command to adjust these settings.
- The G430 will only download the G430 firmware specific to its vintage. Firmware for G430 Vintage 3 must only use firmware having "g430v3_" indicated in the firmware image's filename. All other G430 vintages must only use firmware having "g430_" indicated in the firmware image's filename.

Customer impacting gateway issues will be addressed in new firmware versions within each supported gateway firmware series (e.g., 36.xx.xx is considered a firmware series). This ensures customer impacting fixes will be delivered and available within each supported gateway firmware series until the end of manufacturer support. The latest gateway firmware version within a given firmware series should be used since it will have all the latest fixes. New gateway features and functionality will not be supported in configurations running newer series of gateway firmware with older Communication Manager Releases.

To help ensure the highest quality solutions for our customers, Avaya recommends the use of like gateway firmware series and Communication Manager releases. This means the latest version within the GW Firmware Series is recommended with the following Communication Manager software releases:

Gateway Firmware Series	Communication Manager Release
36.xx.xx	6.3.6
37.xx.xx	7.0.0
38.xx.xx	7.1.2
39.xx.xx	7.1.3
40.xx.xx	8.0.1
41.xx.xx	8.1.x

Newer gateway firmware versions running with older Communication Manager software releases are still supported. For example, running gateway firmware version series 36.xx.xx with Communication Manager 6.3 is still supported. However, prolonged running in this type of mixed configuration is not recommended. Avaya recommends running in a mixed configuration only if necessary, to support gateway upgrades before upgrading Communication Manager software. Newer Communication Manager software releases running with older gateway firmware versions are not supported.

Gateway firmware support follows the Communication Manager software end of the manufacturer support model. This means that as soon as a Communication Manager release goes end of manufacturer support, new gateway firmware will no longer be supported with that Communication Manager release.

For example, when Communication Manager 6.3.6 goes end of manufacturer support, gateway firmware series 36.xx.xx will no longer be supported.

Pre-Install Instructions

The following is required for installation:

- Avaya Communication Manager Release 6.3.6 or later should be used since earlier versions are no longer supported.
- Browser access to the Customer Support Web site (http://support.avaya.com), or another way to get the Target File.
- SCP, FTP, or TFTP applications on your PC or Local Computer or a USB drive formatted FAT32 file system.
- G430 or G450 Media Gateways hardware version 1 or greater.
- An EASG service login or a customer administrator login is required for gateway configuration

File Download Instructions

Before attempting to download the latest firmware, read the "Upgrading the Branch Gateway Firmware" section in the following documents:

- Deploying and Upgrading Avaya G430 Branch Gateway
- Deploying and Upgrading Avaya G450 Branch Gateway

.

Note: To ensure a successful download, from the system access terminal (SAT) or ASA, issue the command 'busyout board v#' before issuing 'copy tftp' command. Upon completion, from the SAT or ASA issue the command 'release board v#'.

Backing up the software

For information about G430 and G450 Gateway backup and restore, refer to the "Backup and Restore" section in the following documents:

- Deploying and Upgrading Avaya G430 Branch Gateway
- Deploying and Upgrading Avaya G450 Branch Gateway

Installing the release

IMPORTANT!

- **G430 Gateways running a release prior to Release 7.1.2 Build 39.5.0** MUST first install Release 7.1.0.4 (Build 38.21.02 or Build 38.21.32) or newer 38.xx.yy release before installing Release 8.1.x.y.

- **G450 Gateways running a release prior to Release 7.1.2 Build 39.5.0** MUST first install Release 7.1.0.5 (Build 38.21.03 or Build 38.21.33) or newer 38.xx.yy release before installing Release 8.1.x.y.

If you attempt to download Release 8.1.x.y prior to having installed Release 7.1.0.4 or Release 7.1.0.5 and execute the "`show download software status 10`" command, the system will display the following error message:

> Incompatible software image for this type of device.

After installing Release 7.1.0.4 or Release 7.1.0.5, you must enable or disable Avaya Logins before downloading Release 8.1.x.y via CLI or SNMP. You can enable or disable Avaya Logins by using one of the following CLI commands:

- `login authentication services` – To enable Avaya Logins.
- `no login authentication services` – To disable Avaya Logins.

If you neglect to enable or disable Avaya Logins by using one of the above commands, you will be prompted to do so when any of the following CLI commands are used to perform a firmware download:

- `copy ftp SW_imageA`
- `copy ftp SW_imageB`
- `copy scp SW_imageA`
- `copy scp SW_imageB`
- `copy tftp SW_imageA`
- `copy tftp SW_imageB`
- `copy usb SW_imageA`
- `copy usb SW_imageB`

Notes:

- The special "dadmin" login account previously associated with ASG in releases earlier than Release 7.1.2 is no longer available.
- The gateway defaults to using TLS 1.2, PTLS, and unencrypted H.248 communication with CM. Refer to the "set link-encryption" command to adjust these settings.
- The G430 will only download the G430 firmware specific to its vintage. Firmware for G430 Vintage 3 must only use firmware having "g430v3_" indicated in the firmware image's filename.

All other G430 vintages must only use firmware having “g430_” indicated in the firmware image’s filename.

- The G450 will only download the G450 firmware specific to its hardware vintage. Firmware for G450 Vintage 4 must only use firmware having "g450v4_" indicated in the firmware image's filename. All other G450 vintages must only use firmware having "g450_" indicated in the firmware image's filename.

For information about installing G430 and G450 Gateway firmware, refer to the “Installing the Branch Gateway” section in the following documents:

- Deploying and Upgrading Avaya G430 Branch Gateway.
- Deploying and Upgrading Avaya G450 Branch Gateway.

Troubleshooting the installation

For information about troubleshooting G430 and G450 Gateway issues, Refer to the “Troubleshooting” section in the following documents:

- Deploying and Upgrading Avaya G430 Branch Gateway.
- Deploying and Upgrading Avaya G450 Branch Gateway.

Restoring software to the previous version

For information about G430 and G450 Gateway backup and restore, refer to the “Backup and Restore” section in the following documents:

- Deploying and Upgrading Avaya G430 Branch Gateway.
- Deploying and Upgrading Avaya G450 Branch Gateway.

Fixes in G430 and G450 Media Gateways Release 8.1.x.x

Fixes in G430 and G450 Media Gateways Release 8.1.3 (Builds 41.34.01 and 41.34.31)

ID	Minimum Conditions	Visible symptoms	Found in Release
CMG4XX-1733	G430, G450 Nessus Scan	Fixed an issue where multiple Nessus security scans using SSH would sometimes cause the gateway to reboot.	8.1

Fixes in G430 and G450 Media Gateways Release 8.1.3 (Builds 41.34.00 and 41.34.30)

ID	Minimum Conditions	Visible symptoms	Found in Release
CMG4XX-1594	G430, G450 Missing, Invalid or Expired TLS certificates.	Reduced the number of error log messages and traps when gateway cannot communicate with CM due to TLS certificate errors. Now only the error occurrence will be reported every half hour instead of every second. The TLS connection retry rate was also reduced since it is more CPU intensive for both CM and the gateways.	7.1.3
CMG4XX-1640	G430, G450 Internal Timer Rollover.	Several internal timer calculations were fixed to prevent the possibility of premature rollover. For example, the internal OSPF timer was fixed so that it should now only rollover once every 136 years. Originally the OSPF timer was incorrectly rolling over every 248 days.	7.1.3

ID	Minimum Conditions	Visible symptoms	Found in Release
CMG4XX-1653	G430, G450 No Tone Detectors available.	Fixed a memory leak that caused the gateway to reboot as a result of the log being flooded with an excessive number of 'No tone detector' log entries.	7.0.1
CMG4XX-1669	G430, G450 DSP Busy-out.	Busy-out of a DSP that is not present will no longer cause an alarm.	7.1.3
CMG4XX-1670	G430, G450 DSP Busy-out.	Fixed a condition that only occurred when a DSP is busied out whereby the gateway would sometimes use the local RTP port range instead of the RTP range configured for the IP Network-Region.	7.1.3

Fixes in G430 and G450 Media Gateways Release 8.1.2 (Builds 41.24.00 and 41.24.30)

ID	Minimum Conditions	Visible symptoms	Found in Release
CMG4XX-1568	G430, G450 DHCP Server	In some cases when the gateway was used as a DHCP Server, IP bindings that were no longer in use were not cleared and the gateway would reboot if the CLI command "clear ip dhcp-server bindings" was used.	6.3.2
CMG4XX-1576	G430, G450 Logging	The “show logging file content” CLI command displayed an incorrect IP address in the logs for unsuccessful login attempts made by a user logging in remotely.	7.1.3.4
CMG4XX-1585	G430, G450 SCP	In rare cases, upload operations using the “copy file scp” commands would cause the gateway to reboot	8.1

Fixes in G430 and G450 Media Gateways Release 8.1.1 (Builds 41.16.00 and 41.16.30)

ID	Minimum Conditions	Visible symptoms	Found in Release
CMG4XX-1493 CMG4XX-1500 CMG4XX-1525	G430, G450, Firmware download	The gateway is now more tolerant of the time it takes to download larger firmware image sizes. In addition, the size of the firmware download image also has been reduced.	7.1.3.3
CMG4XX-1508	G430, G450, Primary Search Timer	The primary search timer was incorrectly getting set to a value of 1 minute when set to a value greater than 30 minutes.	7.0.1.2
CMG4XX-1530	G430v3	The traceroute command in the G430v3 was not working correctly and indicated "request timeout" in the last route entry.	7.1.3.4
CMG4XX-1540	G430, G450, Spanning Tree disabled	While powering up the Gateway, spanning-tree packets were being sent even that spanning tree was disabled.	7.1.3.4
CMG4XX-1549	G430, G450, SSH	In some cases, SSH connections were being refused after many SSH connections have occurred over an extended period of time.	8.1

Fixes in G430 and G450 Media Gateways Release 8.1.0.1 (Builds 41.10.00 and 41.10.30)

ID	Minimum Conditions	Visible symptoms	Found in Release
CMG4XX-1541	G430, G450	This version contains fixes for the Wind River TCP/IP stack security vulnerabilities discovered in July 2019 and known as Urgent/11.	7.1.3

Fixes in G430 and G450 Media Gateways Release 8.1 (Builds 41.09.00 and 41.09.30)

Note: There are no fixes listed here since this is the first release.

Known issues and workarounds in G430 and G450 Media Gateways Release 8.1.x.x

Known issues and workarounds in G430 and G450 Media Gateways Release 8.1.3, 8.1.2, and 8.1.1

The following table lists the known issues, symptoms, and workarounds in this release:

ID	Visible symptoms	Workaround
None	G430, G450 This Branch Gateway version does not support multiple IPv6 VLAN interfaces.	Use a single VLAN interface with IPv6.

Languages supported

- English

Documentation errata

- None

Avaya Aura® Media Server

For latest information refer to Avaya Aura® Media Server Release 8.0.x Release Notes on the Avaya Support website at: https://downloads.avaya.com/css/P8/documents/101073830

Avaya WebLM

What's new in Avaya WebLM for 8.1.x.x

What's new in Avaya WebLM for 8.1.3

For more information see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

Security Service Pack

Beginning with 8.1, WebLM is releasing an 8.1 Security Service Pack (SSP). This SSP can be applied to any version of 8.1 and only includes Red Hat security updates.

Installing WebLM Security Service Pack through Solution Deployment Manager (SDM) is not supported.

This patch does not apply to WebLM 8.1.x Software Only deployments. This patch should NOT be installed on WebLM 8.1.x Software Only deployments.

Beginning December 2020, SSPs will also be released on a more frequent cadence. This means that SSPs may also be available between application Service Packs/Feature Packs. SSP required artifacts and fix IDs will no longer be tracked in the Release Notes. For further information on contents and installation procedures, please see PCN2124S for more details

What's new in Avaya WebLM for 8.1.2

For more information see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

Note: WebLM does not have encrypted OVAs in Release 8.1.2 and later.

What's new in Avaya WebLM for 8.1.1

For more information see ***What's New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

Required artifacts for Avaya WebLM Release 8.1.x.x

Required artifacts for Avaya WebLM Release 8.1.3.1

The following section provides Avaya WebLM downloading information.

Filename	PLDS ID	File size (MB)	Comments
WebLM_8.1.3.1_r81322169.bin	SMGR8131GA3	404 MB	138ab684a979efd6ec8df991f9c9d22c

Required artifacts for Avaya WebLM Release 8.1.3

The following section provides Avaya WebLM downloading information.

Filename	PLDS ID	File size (MB)	Comments
WebLM_8.1.3.0_r81311777.bin	SMGR8130GA3	395	7e068289a87e54cc1eb1ff6a22462ef3
WebLMSSP_R8.1.0.0_Patch5_81011775.bin	SMGR81SSP07	376	144b59a66206b5eaa974e75d0922cd8f

Required artifacts for Avaya WebLM Release 8.1.2

The following section provides Avaya WebLM downloading information.

Filename	PLDS ID	File size (MB)	Comments
WebLM_8.1.2.0_r81211102.bin	SMGR8120GA3	350	WebLM 8.1.2.0 Release Md5sum: e31442c909018bf7a5987325c370555a

Required artifacts for Avaya WebLM Release 8.1.1

The following section provides Avaya WebLM downloading information.

Filename	PLDS ID	File size (MB)	Comments
WebLM_8.1.1.0_r81110398.bin	SMGR8110GA3	348	WebLM 8.1.1.0 Release Md5sum: 2fa367d60c84685cd9794e220b5048cb

Required artifacts for Avaya WebLM Release 8.1

The following section provides Avaya WebLM downloading information.

Filename	PLDS ID	File size (MB)	Comments
WebLM-8.1.0.0.7-32857-e65-8.ova	SMGR81GA014	1606	WebLM 8.1 OVA MD5 Checksum: 3d25c974d78902e9871cccbca643d51a
WebLM-8.1.0.0.7-32857-AWS-8.ova	SMGR81GA015	1599	WebLM 8.1 AWS OVA MD5 Checksum: 80f222d39d0e3076a1fa47efb9a0a4e5
WebLM-8.1.0.0.7-32857-KVM-8.ova	SMGR81GA016	3442	WebLM 8.1 KVM OVA MD5 Checksum: f194423a7d1a5829704cee857772e774
AvayaAuraWebLM_8.1.0.0.7-32857_8.iso	SMGR81GA017	265	WebLM 8.1 Software Only ISO MD5 Checksum: f34c5529bded49be816cc739e688272c

For more details, see PCN2101S on the Avaya Technical Support site.

Installation for Avaya WebLM Release 8.1.x.x

Installation for Avaya WebLM Release 8.1.3

Installation for Avaya WebLM Release 8.1.2

Installing the release 8.1.1

Important Notes

1. Characters required in the hostname

   WebLM hostnames must include only letters, numbers, and hyphens (-) and not underscores. For example, WebLM_62 is an invalid hostname.

2. Cloning WebLM on VMware.

   A user cannot change the IP of a WebLM OVA system that is cloned to another host. To change the IP, rename the ifcfg-eth0 file to ifcfg-eth0.old. Create the file (ifcfg-eth0). Add the MAC address of the newly cloned VM into the ifcfg-eth0 file with correct network configuration and restart the network service.

3. Restoring WebLM Backup.

   Ensure that the Application Server service is restarted after the WebLM restore functionality.

4. Rehost of licenses.

   - In VE deployments, the host ID of the WebLM server is a function of IP address and UUID of the system. So, if either change, a re-host of license files will be required. A re-host is required in the following scenarios:
     - Upgrade: This involves setting up a new VM with new UUID and restoring data on the same. Since UUID changes, host ID would change, and any existing files would become invalid. Re-host of licenses is required.
     - Migration (from SP to VE): Since the host ID would change, a re-host of license files will be required.
   - An IP address is changed: If the IP address is changed, host ID changes and a re-host of license files is required.
   - VMware cloning of WebLM: This would cause the UUID to change, and therefore, the host ID would change. A re-host of license files will be required.
   - Re-host is not required for vMotion moves.

Resource allocation and reservation for standalone WebLM on VMware

VMware resource	Profile 1 Values that can support up to 5000 license requests (Default)	Profile 2 Values that can support more than 5000 license requests
vCPUs	1	1
CPU reservation	2290 MHz	2290 MHz
Memory	1 GB	2 GB
Memory reservation	1 GB	2 GB
Storage reservation	40 GB	40 GB
Shared NIC	1	1

WebLM requires more memory to scale to more than 5000 license requests at any point in time.

To update the memory for WebLM on VMware:

1. Log in to your VMware vSphere Client, and turn off the WebLM virtual machine.

2. If WebLM VM is not visible in the navigation pane, then navigate to Home > Inventory > Hosts and Clusters.
3. Right-click the WebLM VM in the navigation pane.
4. Select the Edit Settings option from the available context menu.
5. In the Edit Settings or Virtual Machine Properties dialog box, select the Memory option on the Hardware tab.
6. Specify 2048 in the text field and MB in the drop-down box.
7. In the Hardware tab, type 2 in the CPU option.
8. Click OK.
9. In the navigation pane, right-click the WebLM VM and select the Power-On option from the context menu.

Software information

Software	Version
OS	RHEL 7.6
Java	OpenJDK version "1.8.0_242" 64-bit
Application Server	WildFly AS 10.1.0
Supported Browsers	Internet Explorer 11.x
	Firefox 65, 66, 67

- Download *Deploying standalone Avaya WebLM in Virtualized Environment* and *Upgrading standalone Avaya WebLM* documents from Avaya Support Site for WebLM on VMware deployment and upgrade.

Troubleshooting the installation

Collect logs and other information as specified below, and contact the support team.

- The status of the WebLM software. If the software is an upgrade, then the release from which the software is upgraded.

Execute the following command from Command Line Interface with customer user credentials to collect logs.

```
#collectLogs
```

This will create a file (WebLM_Logs_xxxxxxxxxxxxx.zip) at /tmp location.

Speculative Execution Vulnerabilities (includes Meltdown and Spectre and also L1TF Vulnerabilities)

In order to help mitigate the Speculative Execution Vulnerabilities, the processor manufacturers and operating system developers provide software patches to their products. These are patches to the processors, hypervisors, and operating systems that the Avaya solutions utilize (they are not patches applied to the Avaya developed components of the solutions).

Once these patches are received by Avaya, they are tested with the applicable Avaya solutions to characterize any impact on the performance of the Avaya solutions. The objective of the testing is to reaffirm product/solution functionality and to observe the performance of the Avaya solutions in conjunction with the patches using typical operating parameters.

Avaya is reliant on our suppliers to validate the effectiveness of their respective Speculative Execution Vulnerability patches.

The customer should be aware that implementing these patches may result in performance degradation and that results may vary to some degree for each deployment. The customer is responsible for implementing the patches, and for the results obtained from such patches.

For more information about Speculative Execution Vulnerabilities fixes included in Avaya Aura® Release 8.x, see the following PSNs on the Avaya Support Site:

- PSN020346u - Avaya Aura® Meltdown and Spectre vulnerabilities
- PSN020369u - Avaya Aura® L1TF vulnerabilities

Contacting support

Contact support checklist

Avaya Technical Support provides support for WebLM 8.1

For any problems with WebLM 8.1, you can:

1. Retry the action. Carefully follow the instructions in the printed or online documentation.
2. See the documentation that is shipped with your hardware for maintenance or hardware-related problems.
3. Note the sequence of events that led to the problem and the messages that the system displays. See the troubleshooting section of the Avaya product documentation.

If you continue to have problems, contact Avaya Technical Support by logging in to the Avaya Support website at http://support.avaya.com.

Before contacting Avaya Technical Support, keep the following information handy:

- Problem description.
- Detailed steps to reproduce the problem, if any.
- The release version in which the issue occurs.

Note: To know the release version and build number, log in to WebLM and click **About** on the user interface. If WebLM Console is inaccessible, you can log in to the WebLM SSH interface and run the **swversion command** to get the WebLM version.

- The status of the WebLM software. If the software is an upgrade, then the release from which the software is upgraded.
- Execute the following command from Command Line Interface with customer user credentials to collect logs.

  ```
  #collectLogs
  ```

  This will create a file (WebLM_Logs_xxxxxxxxxxxxx.zip) at /tmp location.

You might be asked to send by email one or more files to Avaya Technical Support for an analysis of your application and the environment.

For information about patches and product updates, see the Avaya Support website at http://support.avaya.com.

Fixes in Avaya WebLM on VMware for 8.1.x.x

Fixes in Avaya WebLM on VMware for 8.1.3.1

The following table lists the fixes in this release:

ID	Description
SMGR-58378	Block unused ports 8080 & 8443.

ID	Description
SMGR-58581	Session Cookie Not Marked as Secure

Fixes in Avaya WebLM on VMware for 8.1.3

The following table lists the fixes in this release:

ID	Description
SMGR-55563	Customer Issue: configureTLS is not working in Standalone WebLM
SMGR-48582	Customer Issue: IPO based WebLM fails to generate hosts ID when system language is set to local language like de_DE.UTF-8 i.e. Germany (other than English)
SMGR-57111	Customer Issue: ntpd service does not start up automatically after Standalone WebLM Virtual Machine is rebooted
SMGR-53657	Customer Issue: In WebLM 8.1 system, kernel.randomize_va_space=2 is missing in /etc/sysctl.conf

Fixes in Avaya WebLM on VMware for 8.1.2

The following table lists the fixes in this release:

ID	Description
SMGR-50799	WebLM audit log enhancement for more readability
SMGR-52876	WebLM patch installed failed due to rpm version mismatch
SMGR-50918	kernel security update
SMGR-53061	tcpdump security update
SMGR-53065	fribidi security update
SMGR-51367	linux-firmware security, bug fix, and enhancement update
SMGR-53077	nss, nss-softokn, nss-util security update
SMGR-53069	kernel security update
SMGR-53081	kernel security and bug fix update
SMGR-53073	kernel security update
SMGR-50664	WebLM server logs filling up disk space
SMGR-53774 (SMGR-53927)	(RHSA-2020:0374) Important: kernel security and bug fix update

Fixes in Avaya WebLM on VMware for 8.1.1

The following table lists the fixes in this release:

ID	Description
SMGR-49140	Enterprise System Manager WebLM shows negative value for Currently Available AES license count when AES is pointed directly to master WebLM and when clicked on Allocations link
SMGR-50237	special characters are showing when viewing allocations on WebLM 8.1

Fixes in Avaya WebLM on VMware for 8.1

The following table lists the fixes in this release:

ID	Description
None	

Known issues and workarounds in Avaya WebLM for 8.1.x.x

Known issues and workarounds in Avaya WebLM for 8.1.3.1

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Visible symptoms	Workaround
None		

Known issues and workarounds in Avaya WebLM for 8.1.3

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Visible symptoms	Workaround
None		

Known issues and workarounds in Avaya WebLM for 8.1.2

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Visible symptoms	Workaround
None		

Known issues and workarounds in Avaya WebLM for 8.1.1

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Visible symptoms	Workaround
None		

Known issues and workarounds in Avaya WebLM for 8.1

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Visible symptoms	Workaround
None		

Avaya Device Adapter Snap-in

What’s new in Avaya Device Adapter Snap-in Release 8.1.x.x

What’s new in Avaya Device Adapter Snap-in for 8.1.3

For more information see ***What’s New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

What’s new in Avaya Device Adapter Snap-in for 8.1.2

For more information see ***What’s New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

What’s new in Avaya Device Adapter Snap-in for 8.1

For more information see ***What’s New in Avaya Aura® Release 8.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101057859

Required artifacts for Avaya Device Adapter Release 8.1.3.1

The following section provides Avaya Device Adapter downloading information.

Download ID	Artifacts	Notes
ADA0000011	DeviceAdapter-8.1.3.1.42273.svar	MD5: 86081C7BACC616980648F448FAC0983A

Required artifacts for Avaya Device Adapter Release 8.1.3

The following section provides Avaya Device Adapter downloading information.

Download ID	Artifacts	Notes
ADA0000010	DeviceAdapter-8.1.3.0.102231.svar	MD5: A6726BE56C2468AA7ED69E39E8F668DB

Required artifacts for Avaya Device Adapter Release 8.1.2.1

The following section provides Avaya Device Adapter downloading information.

Download ID	Artifacts	Notes
ADA0000009	DeviceAdapter-8.1.2.1.2050.svar	MD5: 6C0A823F2C09A1ACE71C5D857B86EB38

Required artifacts for Avaya Device Adapter Release 8.1.2

The following section provides Avaya Device Adapter downloading information.

Download ID	Artifacts	Notes
ADA0000008	DeviceAdapter-8.1.2.0.1932.svar	MD5: EE827F21C5B9241F8B46899A3A8F95A8

Required artifacts for Avaya Device Adapter Release 8.1.1

The following section provides Avaya Device Adapter downloading information.

Download ID	Artifacts	Notes
ADA0000007	DeviceAdapter-8.1.1.0.421855.svar	MD5: ad3a83f634f19f3005c81caef5e3455a

Required artifacts for Avaya Device Adapter Release 8.1

The following section provides Avaya Device Adapter downloading information.

Download ID	Artifacts	Notes
ADA0000006	DeviceAdapter-8.1.0.0.1649.svar	MD5: 3721EDE1550DDCF1219363286001858E

Installation for Avaya Device Adapter Snap-in for 8.1.x.x

Installation for Avaya Device Adapter Snap-in for 8.1.3

Refer to the Avaya Device Adapter Snap-in Reference Guide for installation instructions.

https://downloads.avaya.com/css/P8/documents/101058250

Installation for Avaya Device Adapter Snap-in for 8.1.2

Refer to the Avaya Device Adapter Snap-in Reference Guide for installation instructions.

https://downloads.avaya.com/css/P8/documents/101058250

Installation for Avaya Device Adapter Snap-in for 8.1

Refer to the Avaya Device Adapter Snap-in Reference Guide for installation instructions.

https://downloads.avaya.com/css/P8/documents/101058250

Fixes in Avaya Device Adapter Snap-in for 8.1.3.1

ID	Problem
SETADAPT-9086	IP phones cannot register if TPS is disabled on active Breeze
SETADAPT-9094	The SDP from Device Adapter has multiple entries for the same code (g.722).
SETADAPT-9114	DSA Coredump
SETADAPT-9089	Coredump
SETADAPT-9057	During MGC Reboot see Message: BERR0504 HI EXC 504: Task: "tISSS" SUSPENDED on MGC during reboot.
SETADAPT-9056	UNIStim phone has blank display after connecting to TPS
SETADAPT-9054	MGC cannot be upgraded to ADA MGC via RPC

ID	Problem
SETADAPT-9047	UNISTim IP Phone When display "New callers", if press Callers but "New callers" always display can't disappear, even delete all callers,"New callers"still show up
SETADAPT-9024	Coredump from clientsdk::CSDPOfferAnswerManager::SetRemoteMediaCapabilities
SETADAPT-9003	A lot of "ERROR: [25165] CSDK << Publish[presence]: Unable to end background task. PowerManagement object is null" messages in dsa.log.
SETADAPT-8984	Nessus vulnerability scan tool causes SSH failure on MGC
SETADAPT-8940	Unistim Phones are required to send MAC addr as part of SM Registration
SETADAPT-8906	The version of Avaya Device Adapter is mismatched on two SMGR's
SETADAPT-8874	SMGR:MGC failover timer for ADA shows minutes instead of seconds
SETADAPT-8790	During MGC Reboot see Message: BERR0504 HI EXC 504: Task: "tISSS" SUSPENDED on MGC during reboot. Impact is that MGC Reboot takes slightly longer than expected (This problem existed on all ADA Release from 8.0.1, and before that on CS1000 Releases).
SETADAPT-2763	MESSAGE: [HURRICANE] - CALLS: dsa.log contains a lot of warnings like "WARNING: CSDK << Call[]: CSDPOfferAnswerManager::ProgressAnswerActivatesMedia(): Same early media response is received"
SETADAPT-2692	MESSAGE: ERROR: CSDK << Call[414]: [404:Not Found (No route available)] response received for INVITE when in SIPCallSessionStateMachine::Initiating

Fixes in Avaya Device Adapter Snap-in for 8.1.3

ID	Problem
SETADAPT-8609	Cust user does not have permission to run the adaSetReconfigure command
SETADAPT-8686	adaSetReconfigure command does not work with 1230 type phone
SETADAPT-8883	TDM phones stuck intermittently after swap TNs
SETADAPT-6164	Ring Again busy with brdg-appr line . No autocallback call
SETADAPT-8684	Support subset, terminal number, systemid, Feature1 and Feature 2 fields in endpoint export for CS1k endpoint
SETADAPT-8826	Agent cannot make call to Supervisor via SBC by using Assist key.
SETADAPT-8831	Supervisor Forced Agent mode does not work via SBC (all FACs that require reason code are not working via SBC)
SETADAPT-8835	The first call from every Endpoint (after registration) via SBC always fail (all subsequent calls are OK)

ID	Problem
SETADAPT-8836	User cannot use FAC for Agent work mode via SBC (all FACs that require reason code are not working via SBC)
SETADAPT-8914	All phones go to logged out by end of each day and stuck in this state
SETADAPT-8791	two DSA (CSDK) coredumps observed on high traffic
SETADAPT-8830	MGC cannot register in multi-breeze cluster (if MGC has ELAN and TLAN in different subnets)
SETADAPT-8909	MGC link with ADA Breeze server goes DOWN and UP several times per day
SETADAPT-8963	DSA (CSDK) core dump (segfault) occurs in clientsdk::CSIPSubscription::ActiveOnEntry()
SETADAPT-8967	MGC phones are unusable after re-connecting to ADA
SETADAPT-7967	A2 PVN (Private Line) doesn’t indicate other set (A1 PVR) on an outgoing call
SETADAPT-8763	Phone Unable to register. Phone Display Shows: "Server RegistrationError". All phones affected at the same time
SETADAPT-8764	The Callers List displays “Server Error”
SETADAPT-8896	Phone still display previous extension on CPND after some actions
SETADAPT-8886	Can't change agent skill during active call

Fixes in Avaya Device Adapter Snap-in for 8.1.2.1

ID	Problem
SETADAPT-8841	MGC cannot register in multi-breeze cluster (if MGC has ELAN and TLAN in different subnets)
SETADAPT-8794	MGC cannot register if IPSec is enabled with default PSK
SETADAPT-8795	Specific Configuration: SBC between AURA and Breeze/ADA: ADA fixes provided to allow this config to work properly.
SETADAPT-8816	Update UNIStim firmware in ADA to version C98 to extend SHA-1 certification expiry date
SETADAPT-8789	two DSA (CSDK) coredumps observed in high traffic
SETADAPT-8842	MGC link with ADA Breeze server goes DOWN and UP several times per day

ID	Problem
SETADAPT-8825	MGC is no longer registered
SETADAPT-8829	Phone still display previous extension on CPND after some actions

Fixes in Avaya Device Adapter Snap-in for 8.1.2

ID	Problem
SETADAPT-4260	EQUINOX CONF SPECIFIC: Cannot join adhoc conf to Equinox MeetMe conf
SETADAPT-4968	Digital phone 3903 does not return idle state after pressing call-appr then goodbye button.
SETADAPT-5403	Media Security: Call is dropped after 1 second, when call between extensions in different clusters with different media security settings.
SETADAPT-5417	MSB (Media Security Best Effort) is not working
SETADAPT-5979	MEDIA SECURITY: MSAW set hears overflowtone/reordertone during MSNV set call
SETADAPT-6139	SERVICEABILITY: Add vgwShow to the GUI on SMGR
SETADAPT-6363	NO OVERFLOWTONE WHEN CALL PICKUP FAILS
SETADAPT-6543	CLID is displayed twice on ADA phone display
SETADAPT-6950	NUMBERING PLAN OF 11 DIGITS. CALL APP 11 DIGITS. ONLY 10 DIGITS DISPLAYED AGAINST UNISTIM PHONE CALL APP
SETADAPT-7213	CLID is displayed twice on ADA phone display
SETADAPT-7217	VIRTUAL OFFICE (VO): Failed VO Login from two sets perform VO Login to the same set at the same time
SETADAPT-7562	DSA coredumps are generated during upgrade of ADA Snap-in
SETADAPT-7581	Phones re-register automatically after assigning KEM
SETADAPT-7622	5000 DTLS traffic: "Timer wasn’t found" error in DSA log causing some sets to re-register after 5 minutes
SETADAPT-7661	SOME ADA PHONES HAD "AURA" DISPLAYED ON SCREEN, BUT NOTHING ELSE (NO KEYS/BUTTONS)
SETADAPT-7663	VO (Virtual Office): Virtual softkey disappears after transferring the call
SETADAPT-7710	VO (Virtual Office): "Virtual" button is not usable while system is busy with MGC actions (intermittently)
SETADAPT-7720	Error message: CSIPPresenceManager::EndBackgroundTask()Unable to end background task. PowerManagment object is null

ID	Problem
SETADAPT-7790	NO WAY SPEECHPATH WITH DIGITAL PHONE 3901 TYPE, AFTER SWITCHING FROM HANDSFREE TO HANDSET
SETADAPT-7848	No tones on card slot 0 for MGXPEC
SETADAPT-7851	Emergency label does not display after Virtual Office log out for phones 1210, 2001, 1110
SETADAPT-7854	MDA Phone does not display NodeID and TN register field after pressing "Home" if enable VOLO on Attributes.
SETADAPT-7959	No dialtone to digital stations on slot 0 of MGXPEC
SETADAPT-8336	Unable to go offhook on 3902 phone with handset (speaker activated instead of handset)
SETADAPT-8516	Unable to use voicemail button 3902 phone
SETADAPT-5773	BREEZE: Cannot reset MGC passwords using Breeze Cluster attributes
SETADAPT-6935	SMGR: 1220 Phone: Mismatch feature button between SMGR and CM
SETADAPT-6940	SMGR: 2002 Phone: Shift key does not work
SETADAPT-7365	SM: 1165 Phone: Button Label not removed from phone, when removed from SMGR
SETADAPT-7972	SMGR: Cannot remove button labels using CM Endpoint editor

Fixes in Avaya Device Adapter Snap-in for 8.1.1

ID	Problem
SETADAPT-5278	SMGR, Users > User management > Manage Users > select New user > check the Profile Set. A checkmark is shown in the wrong position.
SETADAPT-5881	SMGR doesn't provide any way to search ADA Endpoint by TN / System ID
SETADAPT-6129	SMGR: Cannot delete or restore users on SMGR when CM/SM is unreachable
SETADAPT-6200	SMGR assigns wrong KEMs type for 12xx
SETADAPT-6202	2nd KEM (12 keys) does not work on phone 12xx
SETADAPT-6216	SMGR displays duplicate template fields after selecting a system of CM when add or duplicate User Profile
SETADAPT-6226	MDA: 2nd Transfer Key Displayed on Aura SIP phone which does not work
SETADAPT-6212	MDA Feature: J-series phones cannot get any feature key from ADA users (except call-appr).

ID	Problem
SETADAPT-4171	Unexpected SNMP alarms are displayed on SMGR while restarting pbxserver/tps/dsa
SETADAPT-6193	ADA set (i2050) is not kicked out properly when another ADA set (1140) gets registered again its station
SETADAPT-6227	MGC can't register to ADA after Breeze upgrade
SETADAPT-6230	Ring again: No Icon of the ring again on phone display against ring-again softkey
SETADAPT-6252	Ring Again: message "Ring Again ready, the select line" isn't displayed after autocallback, only name and number
SETADAPT-6315	No Overflowtone when call pickup fails
SETADAPT-6539	Autodial label on the phone does not change, when autodial number changed
SETADAPT-6576	Numbering Plan of 11 digits. Call App 11 digits. Ten most significant digits displayed against Unistim Phone Extension. Needs to be ten less significant digits.

Fixes in Avaya Device Adapter Snap-in for 8.1

ID	Problem
SETADAPT-4264	No overflow tone when a pickup is not succeeded
SETADAPT-5275	Device adapter page displays duplicated highlights in SMGR
SETADAPT-5638	CFW ALL CALLS (CFWAC): ADA users do not keep last forwarded number (IP Unistim and Digital (TDM) are affected)
SETADAPT-5649	SERVICEABILITY: No alarms are generated when plugging unsupported card to MGC
SETADAPT-5728	SERVICEABILITY: mgcShow doesn't provide any info what MGC is in the process of upgrade
SETADAPT-5752	REDIAL LIST UNISTIM PHONE: Phones cannot make a call over SIP trunk by using Redial List
SETADAPT-5759	QOS PARAMETERS: DSCP values in RTP frames are not changed.
SETADAPT-5769	Hotline with abbr list - unexpected tone when the call is established.
SETADAPT-5823	Unexpected icon for an active call after retrieving a call from hold
SETADAPT-5826	RTCP statistics is not sent for pure TDM calls
SETADAPT-5830	CLID: Some trunk calls have invalid CLID: 16133918024;phone-context=vacant

ID	Problem
SETADAPT-5841	Cannot swap Primary Cluster of MGC from Cluster has multiple servers to Cluster has 1 server
SETADAPT-5846	No Speechpath when ADA digital user uses codec G.729A
SETADAPT-5855	ROBUSTNESS: ADA for the whole system is stuck after FORCED upgrade of 3904 phone with established call
SETADAPT-5856	ROBUSTNESS: ADA for the whole system is stuck/Freeze after getting HW/Serial ID for the unsupported card
SETADAPT-5864	SERVICEABILITY: SMGR Device Adapter interface shows wrong information about MGC loadware.
SETADAPT-5866	SECURITY: MGC password is printed in DeviceAdapter.log when sending a notification to ADA
SETADAPT-5869	UNISTIM TO H323 PHONE: sRTP One-way speechpath for a basic call between ADA_Unistim phone and CM H323 phone
SETADAPT-5873	ADA coredumps are generated when restarting DSA service where there's MGC registered
SETADAPT-5874	BRIDGED APPEARANCE: Principal phone cannot bridge into the call, MDA =2+ scenario broken for incoming call
SETADAPT-5875	A lot of unnecessary messages are printed in Device Adapter.log during UNISTIM traffic. Causing high CPU usage, and system thus becomes unresponsive
SETADAPT-5879	SERVICEABILITY: daversion doesn't display info about user MGCC/MGCA loads
SETADAPT-5888	JavaCoredumps and Overload are detected in DA after plugging the ALCs without configuration
SETADAPT-5889	MGC can't register after Gold Image upgrade
SETADAPT-5921	duplicate TNs assigned for card slot 9 and 10 on MGC
SETADAPT-6018	Some IP Unistim Phones are in a strange state, where they cannot originate any calls (no dialtone), but they can receive incoming calls ok
SETADAPT-6115	"ELAN is Down" Message printed, ADA is down, after Breeze Powered-down and Powered-up again.
SETADAPT-5892	The display name is shown incorrectly in PD (Personal Directory)
SETADAPT-6012	PD (Personal Directory) server cannot connect to database server until service restart
SETADAPT-6112	If A call B then coverage to C that C display cannot see B information when C Ringing
SETADAPT-5839	If there are some stuck jobs in the database, then there might be issues with importing Media Gateway XML file to SMGR
SETADAPT-6207	IP Unistim phone cannot make outgoing call after off-hook dialing timeout (after link connection between ADA and SM going down/up)

ID	Problem
SETADAPT-6049	IP UNISTIM 1210 PHONE: Cannot put a call on hold for a second time
SETADAPT-6234	After Network Outage for > 5 mins, then recovery, ADA phones cannot register, and the screen of phones displays "Unequipped". Reinstall ADA Snap-in to recover
SETADAPT-6227	MGC cannot register to ADA after Breeze Upgrade
SETADAPT-4378	SMGR: If there is ‘Synchronization Failure’ on the Replication page of Breeze in SMGR, that can be due to SMGR running out of space in /var/log.
SETADAPT-5929	Breeze Command: tnInfo with no parameters prints multiple phones with TN 0-0-0-0

Known issues and workarounds for Avaya Device Adapter Snap-in for 8.1.x.x

Known issues and workarounds for Avaya Device Adapter Snap-in for 8.1.3.1

ID	Problem	Workaround
SETADAPT-5890	COREDUMP: ADA pbxserver coredumps are generated when restart DSA service when we have MGC's registered (This Coredump is not service impacting)	No Workaround
SETADAPT-8587	Only half of the MGC’s are upgraded after upgrading ADA	Workaround 1: stop/start dsa service via command line "dasrvstart stop/start dsa". Workaround 2: stop/start ADA services via SMGR service management.

Known issues and workarounds for Avaya Device Adapter Snap-in for 8.1.3

ID	Problem	Workaround
SETADAPT-5890	COREDUMP: ADA pbxserver coredumps are generated when restart DSA service when we have MGC's registered (This Coredump is not service impacting)	No Workaround
SETADAPT-8587	Only half of the MGC’s are upgraded after upgrading ADA	Workaround 1: stop/start dsa service via command line "dasrvstart stop/start dsa". Workaround 2: stop/start ADA services via SMGR service management.
SETADAPT-8790	During MGC Reboot see Message: BERR0504 HI EXC 504: Task: "tISSS" SUSPENDED on MGC during reboot. Impact is that MGC Reboot takes slightly longer than expected (This problem existed on all ADA Release from 8.0.1, and before that on CS1000 Releases).	No Workaround
SETADAPT-8990	CC (Contact Center) Agent Traffic failed, DSA Coredump generated on Cluster 1 + 1 profile 4 with DTLS enabled. This problem is ONLY seen with CC (Contact	No Workaround. Currently not recommended to use this ADA 8.1.3 GA load with CC (Agents configured and logged in on ADA Phones). A fix will be provided for this problem in an updated

ID	Problem	Workaround
	Center) traffic, and NOT seen with UC (Unified Comms) traffic.	ADA 8.1.3 “field” load within approx. 1 month from GA.

Known issues and workarounds for Avaya Device Adapter Snap-in for 8.1.2.1

ID	Problem	Workaround
SETADAPT-8835	With specific setup: SBC between AURA and ADA: The first call from every Endpoint via SBC always fail (all subsequent calls are OK)	No Workaround. Please refer to this SOLN for SBC setup/config: https://support.avaya.com/ext/index?page=content&id=SOLN351429
SETADAPT-8836	With specific setup: SBC between AURA and ADA: User cannot use FAC for Agent work mode via SBC (all FACs that require reason code are not working via SBC)	No workaround. Please refer to this SOLN for SBC setup/config: https://support.avaya.com/ext/index?page=content&id=SOLN351429
SETADAPT-8831	With specific setup: SBC between AURA and ADA: Supervisor Forced Agent mode does not work via SBC (all FACs that require reason code are not working via SBC)	No workaround. Please refer to this SOLN for SBC setup/config: https://support.avaya.com/ext/index?page=content&id=SOLN351429
SETADAPT-8886	With specific setup: SBC between AURA and ADA: Can't change agent skill during active call	No workaround. Please refer to this SOLN for SBC setup/config: https://support.avaya.com/ext/index?page=content&id=SOLN351429
SETADAPT-8826	With specific setup: SBC between AURA and ADA: Agent cannot make call to Supervisor via SBC by using Assist key.	No workaround. Please refer to this SOLN for SBC setup/config: https://support.avaya.com/ext/index?page=content&id=SOLN351429

Known issues and workarounds for Avaya Device Adapter Snap-in for 8.1.2

ID	Problem	Workaround
SETADAPT-7699	Softphone 2050: Call timer stops working after Personal Directory menu opened	Restart softphone
SETADAPT-8271	Call timer is not displayed on a phone if a call is made from the second call-appr	No workaround.
SETADAPT-7026	Call Info is not displayed in pop-up notification when press ShiftForCall with 2 ringing calls	No workaround
SETADAPT-8101	Overflow/reorder tone when transfer on ringing, when ringing call is “covered” to voicemail	No workaround. Transfer is still successful. Press Release Key on transferring phone to return to idle.
SETADAPT-8545	Traffic: A Few ADA calls take slightly longer than expected to ring on Agents (a few seconds more)	Disable caching in breeze attributes
SETADAPT-8546	When MGXPEC motherboard card is not in service ALL KEYs of 39xx phone disappear on phone connected to MGXPEC daughterboard card. Also log message printed: A31: STUCK interrupt on daughter board.	Reboot MGXPEC Daughterboard card or disable and enable Digital line Card (DLC)

ID	Problem	Workaround
SETADAPT-8602	New callers and redial lists still available even if attribute is disabled on breeze	Disable “Personal Directory” attribute in “Contacts” tab of breeze
SETADAPT-8603	Configuring passwords with 16 symbols for MGC breaks admin2/pdt2 access to MGC (used for MGC upgrade/configuration/SSH access)	Use max length of password up to 15 symbols.
SETADAPT-8587	Only half of the MGC’s are upgraded after upgrading ADA	Workaround 1: stop/start dsa service via command line "dasrvstart stop/start dsa". Workaround 2: stop/start ADA services via SMGR service management.
SETADAPT-8609	Cust does not have permission to adaSetReconfigure Command	Root access is required to run this command on ADA 8.1.2 GA load.

Known issues and workarounds for Avaya Device Adapter Snap-in for 8.1.1

ID	Problem	Workaround
SETADAPT-4260	IP Unistim Phone and TDM Phone: Cannot add an existing Adhoc conference (e.g., a three-party conference on AURA that involves Device Adapter Phones) into an Equinox MeetMe conference	Each Device Adapter user that needs to connect to the Equinox MeetMe conference needs to dial into the Equinox MeetMe conference
SETADAPT-4968	Digital phone 3903 does not return idle state after pressing call-appr then goodbye button.	The user goes onhook using the handset
SETADAPT-6935	SMGR for 1220 phone allows configuration of > 4 buttons	1220 Phone only supports 4 buttons (0,1,2,3). Ignore additional buttons on SMGR.
SETADAPT-6940	SMGR for 2002 phone allows configuration of > 4 buttons	2002 Phone only supports 4 buttons (0,1,2,3). Ignore additional buttons on SMGR.
SETADAPT-7217	Virtual Office (VO): Failed VO Login from two sets performing VO Login to the same set at the same time	No Workaround
SETADAPT-7349	The principal bridged phone does not lose CONFERENCE 2 when one of the participants presses the Privacy Release button	Other party in the call presses Privacy Release
SETADAPT-7351	Phone type 2001 is not automatically updating time after DST period starts when Phone 1165 is Virtual Office logged into it	No Workaround
SETADAPT-7582	Cannot export excel file for selected users in SMGR. In SMGR, Users -> Manage Users -> select user then choose “Export Selected Users” at More Actions. The select export file type is Excel -> press Export. Download and open zip file in Export List. Does not have an excel file in a ZIP file	No Workaround
SETADAPT-5163	TDM Phone: SMGR allows to add any model phones in the same card. This is	Admin should check it manually. On Breeze use command line tool tnInfo to

ID	Problem	Workaround
	misconfiguration, so SMGR is allowing this misconfiguration to take place.	determine what loop-shelf-card is used by digital, analog or Unistim sets. ipeShow command should be used to get info about configured cards. Ensure that you only configure Analog Phones on an Analog Line Card, and only configure Digital Phones on a Digital Line Card.
SETADAPT-5601	TDM Phone: No Call Park RECALL for analog phones	No Workaround
SETADAPT-6164	IP Unistim Phone and TDM Phone: Ring Again Busy does not work if the busy phone has brdg-app line to Ring Again activator.	No Workaround
SETADAPT-7363	Cannot remove button labels using the CM Endpoint Editor	Use the CM Element Manager instead of User Management. So for the CM EM workaround, choose Elements -> Communication Manager -> Endpoints -> Manage Endpoints. You will be able to clear out a button label.
SETADAPT-7581	Phones restart automatically after configuring KEM (add-on unit)	No Workaround
SETADAPT-7663	Virtual Office (VO): Virtual softkey disappears after transferring the call	User can press Goodbye Key, and the Virtual Softkey will appear.
SETADAPT-7791	MGC-XPEC: No tones on card slot 0	Do not use Card Slot 0 with MG-XPEC Or Install a new field version of ADA 8.1.1 with a fix for this problem that will be available approx. 1-month post GA via SOLN344794. Contact Avaya Services for assistance.

Known issues and workarounds for Avaya Device Adapter Snap-in for 8.1

ID	Problem	Workaround
SETADAPT-5199	IP Unistim Phone and TDM Phone: Call is not redirected when there are both SAC (SEND ALL CALLS) and Busy criteria in coverage path, phone has set busy activated and is in active call	No
SETADAPT-4260	IP Unistim Phone and TDM Phone: Cannot add an existing Adhoc conference (e.g. a three-party conference on AURA that involves Device Adapter Phones) into an Equinox MeetMe conference	Each Device Adapter user that needs to connect to the Equinox MeetMe conference needs to dial into the Equinox MeetMe conference
SETADAPT-6164	IP Unistim Phone and TDM Phone: Ring Again Busy does not work if a busy phone has brdg-app line to Ring Again activator.	None
SETADAPT-6185	IP Unistim Phone and TDM Phone: MDA arrangement of ADA Analog + 96x1 phone. 96x1 phone displays incorrectly when bridging into an active call. SIP	None

ID	Problem	Workaround
	96x1 displays its number instead of the caller's name and number.	
SETADAPT-6212	IP Unistim Phone and TDM Phone: MDA Feature - J-series phones cannot get any feature key from ADA users (except call-appr).	Use Call App only
SETADAPT-6165	IP Unistim Phone and TDM Phone: MDA: 2nd transfer or conference key displayed on Aura SIP phone which does not work	None. Only transfer or conf key in the context-sensitive part of the display will work. The additional Transfer or conf key is displayed by mistake.
SETADAPT-6202	IP Unistim Phone: 2nd KEM (12 keys) does not work on phone 12xx	Use CM to configure: Go to CM > SAT mode > "change station xxx" > page 1, edit "button per page" to 12 > Commit.
SETADAPT-6200	IP Unistim Phone: SMGR assigns the wrong KEM type for 12xx type phones. 12 button KEM is not available	Use CM to configure. Users can assign correct KEM type in CM.
SETADAPT-5840	TDM Phone: When the SIP interface (TLAN) on the Active Load Balancer Breeze server goes down and then comes back again, MGC cannot redirect to that Server. After that, all MGC cannot register to cluster. If there is a network outage on both the interfaces of the Breeze node, then the MGCs will automatically register.	After the SIP interface (TLAN) for Active Load Balancer Breeze server recovers, then manually reboot all MGCs.
SETADAPT-5601	TDM Phone: No Call Park RECALL for analog phones	No
SETADAPT-5163	TDM Phone: SMGR allows to add any model phones in the same card. This is misconfiguration, so SMGR is allowing this misconfiguration to take place.	Admin should check it manually. On Breeze use command line tool tnInfo to determine what loop-shelf-card is used by digital, analog or Unistim sets. ipeShow command should be used to get info about configured cards. Ensure that you only configure Analog Phones on an Analog Line Card, and only configure Digital Phones on a Digital Line Card.
SETADAPT-5471	TDM Phone: Redial List over SIP Trunk does not work on 3904 Digital phone type	None
SETADAPT-6216	SMGR displays duplicate template field after selecting a system of CM when add or duplicate User Profile	disable CM Endpoint Profile then enable it again, and the duplicated template field will disappear

Avaya Device Adapter General Limitations

Avaya Device Adapter General Limitations for 8.1.3

Avaya Device Adapter General Limitations for 8.1.2

Breeze doesn't have full FIPS support. This can lead to installation issue for Device Adapter Snap-in. It is recommended to disable FIPS on Breeze and then retry installation if such issue occurred.

Contacts handling logic limitation

When User adds new contact into his contact list from Personal directory there could occur 2 different situations:

- Newly added contact has exactly same phone number (extension of the station) as station number configured via SMGR
  - after contact added it will have same First and Last names as it was in PD search/or manually entered values unless:
    - station experienced network recovery
    - station re-registers
    - admin change any value for the station via SMGR/CM
  - if one of scenarios from previous bullet occurs new Contact information will be shown to the user - First and Last name exactly same as configured for station with same phone number/extension. This is known as **Associated contact**
    - **Associated contact**s can't be edited from endpoint site. Result of operation is **SUCCESS** but user will see exactly same First and Last name as station with same phone number/extension.
    - **Associated contact** can be changed only by admin via SMGR - change user's (with phone number as contact) First/Last name.
- Newly added contact does not have matching phone number (extension of the station) as station number configured via SMGR
  - after contact added it will have same First and Last names as it was in PD search/or manually entered values
  - user is able to edit contact - no limitations.

Avaya Device Adapter General Limitations for 8.1.x

- SMGR, SM, CM, AMS, Breeze server installation, and initialize configuration must be ready to use. Refer to these product release notes for more information.

  IMPORTANT: For upgrades of Avaya Device Adapter (ADA), from 8.0.1 to 8.1.x. Due to a compatibility issue between Session Manager (SM) 8.1.x and ADA 8.0.1, the upgrade procedure to ADA 8.1.x has to be modified.

  Release 8.0.1 to 8.1.x upgrade steps:

  On Aura Release 8.0.1 system (SMGR, SM, Breeze, ADA), FIRST upgrade ADA to 8.1.x

  Then upgrade Aura to 8.1.x as per current procedure (first SMGR, then SM then Breeze).

Specific requirements for Avaya Device Adapter include:

1. TLS links should be enabled for all Entities (Breeze and CM to SM, AMS links to CM, you can skip AMS if you have Media Gateway to provide DSP for your CM)
2. Certificates installation and configuration
3. Administrator user should have a dialing plan, a user (stations), signaling, and trunk groups to Session Manager be configured and ready to use before installing and using Avaya Device Adapter snap-in.
4. Activate root access for: SMGR, Breeze, Session Manager

- The NODE IP of the CS1000 TPS mapping is not required anymore. Automatically it will be set to Secure/SIP IP address of the Breeze server (in case of a single server) or in case of using multiple Breeze servers within a cluster, the NODE IP automatically maps to the Cluster IP.

5. If you use the existing IP address, then the CS1000 phone admin doesn't need to change
6. If you use a new IP address, then you will have to have the phone admin change, but this is useful if you want to take a subset of your CS1000 population to test out the new configuration before cutting all your users.

   - Confirm your enrollment password is NOT expired before upgrading/installing new Breeze nodes.
   - Call Park is now supported for Unistim sets starting from Device Adapter 8.0 Service Park 1. To configure Call Park, need to install Call Park and Page Snap-in on a separate Breeze server.

For **each node** in the cluster, we require:

1. An additional SIP Entity of the "Endpoint Concentrator" type
2. An Entity Link from the above SIP Entity to every "relevant" SM in the solution (the Connection Policy of the Entity Link must be set to "Endpoint Concentrator")

   - You must uninstall **and delete** all previous Avaya Device Adapters on SMGR before loading the **SVAR** file of the new Device Adapter.

   In this case, SMGR will display a pop-up message about the necessity to restart Device Adapter when a user updates the attributes.

1. The "Signaling Security Error" message is displayed on the IP Deskphone display during the registration process.

   The following items should be checked:

   DTLS settings have been propagated to TPS form SMGR. Check /opt/Avaya/da/shared/config/config.ini
   Please note that snapin root path was changed from /opt/Avaya/snap_in/da/ to /opt/Avaya/da.

   ```
   # cat /opt/Avaya/da/shared/config/config.ini
   …
   [UNIStim DTLS]
   TPS_DTLS=1                    // 0 – Off, 1 – Best effort, 2 - Always
   DTLSClientAuthentication=0
   ```

   Note: Avaya Device Adapter snap-in must be restarted in SMGR UI after changing the attribute.

2. Check Port and action byte configured at the phone.

   Following security levels with DTLS (the terminology is kept from CS1000):
   • Basic. The DTLS policy is configured as Best effort. Phones are configured with action byte 1 and Port 4100. There is a brief period of insecure signaling at the beginning of registration. If IP Deskphone has installed the CA Root certificate, then it continues registration using DTLS after a brief period of insecure. In case of certificates, mismatch registration will fail.

- Advanced. The policy is configured as Best Effort. DTLS-capable phones are configured with action byte of 7 and Port 4101. DTLS incapable configured with action byte of 1. If IP Deskphone is DTLS capable, configured with action byte of 1 and Port 4100, and has installed CA Root certificate, then it continues registration using DTLS after a brief period of insecure. In the case of a certificate mismatch registration will fail.

- Complete. The policy is configured as Always. All IP Phones are DTLS-capable and configured with action byte 7 and Port 4101. Insecure registrations are not permitted. In the case of a certificate mismatch registration will fail.

3. Check that DTLS ports are open by csv and tps:

```
# netstat -unap | grep -E "4101|5101|8301"
udp     0     0 192.168.96.115:8301     0.0.0.0:*                  9190/tps
udp     0     0 192.168.96.115:4101     0.0.0.0:*                  15320/csv
udp     0     0 192.168.96.115:5101     0.0.0.0:*                  9190/tps
```

Important: If you have made keystore and truststore cert changes after snap-in installation, then following commands should be executed from Breeze cli as root:

```
# cd /opt/Avaya/da/
# ./avaya_securitymodule_pki_tool init da dauser > sm_pki_descriptor_da.txt
```

4. Try to reset the phone to factory defaults to delete the previous CA root certificate that was on the set. Procedure for resetting IP Deskphones factory defaults can be found in NN43001-368 "IP Deskphones Fundamentals Avaya Communication Server 1000".
   Then install the SMGR root CA again as described in NN43001-368 "IP Deskphones Fundamentals Avaya Communication Server 1000".

5. In case for 2050 CA certificate should be installed into Trusted Root Certification Authorities->Local Machine. By default, the certificate manager installs it into Trusted Root Certification Authorities->Registry (at least in Windows 7, see https://superuser.com/questions/647036/view-install-certificates-for-local-machine-store-on-windows-7).

- Mnemonics for Hotline buttons emulated using the brdg-appr or call-appr buttons
- Personal Directory: Stores up to 100 entries per user of user names and DNs.
- Callers List: Stores up to 100 entries per user of caller ID information and most recent call time
- Redial List: Stores up to 20 entries per user of dialed DNs and received Call Party Name Display with time and date.

MGC configuration

1. For MGC previously registered in Security Domain at CS1000 system:
   - Login to Call Server in CS1000 option;
   - Enable PDT2 mode for admin2 account at CS;
   - login to overlay supervisor -
     ld 17:

     REQ: chg

     TYPE: pwd

ACCOUNT_REQ: chg

USER_NAME: admin2

PDT: pdt2

2. If you know your MGC ELAN IP address, you can skip this step:

2.1 Physically connect MGC (COM RS232 port) to your PC via COM-USB cable. Run any terminal application (For example, PuTTY) and use a SERIAL connection with following settings:

Port: COM3

Baud Rate: 9600

Data Bits: 1

Parity: None

Flow Control: None

2.2 With **mgcinfoshow** command at MGC you can determine your MGC ELAN IP address.

3. MGC Loadware upgrade.

3.1 **MGC Loadware upgrade from CS1000 release**.

1. Turn on "Enable legacy loadware upgrades" Breeze attribute and set it to "yes"
2. From MGC in ldb shell under pdt2 user:
3. enter “leaveSecDomain”, “isssDecom” command;
4. run “portAccessOff”;
5. run mgcsetup with changing the IP of DA.
6. From SMGR Inventory page, add new DA Media Gateway

3.2 **MGC manually Loadware upgrade**.

1. Connect to your MGC ELAN IP address via SSH connection and pdt2/2tdp22ler or admin2/0000 credentials.
2. Go to debug mode by pressing **ctrl+l+d+b** and enter pdt2/admin2 credentials
3. Run **ftpUnprotectP** command to unprotect **/p** partition.
4. Connect to your MGC ELAN IP address via SFTP.

   Now all MGC loadware is integrated inside snapin. All upgrade procedure for MGC loads NA08 and upper will be done automatically.

   To upgrade from old MGC release, need take MGC load file placed at /opt/Avaya/da/mgc/loadware/current on your Breeze server. The filename will be similar to MGCCNXXX.LD. Copy it on your machine.
5. Extract with zip archiver mainos.sym and mainos.sym files from *.LD loadware file and copy them to /p partition of MGC
6. Reboot MGC with **reboot** command from ldb.

MGC registration:

- Create new one or make changes at SMGR->Inventory->Manage elements->MGC

  - Recommended to use Mu-law for companding law settings for MGC and Avaya Device Adapter attributes;
  - Assign new MGC to Breeze cluster;
  - Commit changes
- Connect to your MGC via SSH and run **mgcsetup** command:

  1. Enter ELAN IP: **192.168.127.91** (for example) (enter)

     An important tip. Do not try to erase with Delete or BackSpace buttons. It does not work. Just input new values and push Enter.

  2. Enter ELAN subnet mask: **255.255.255.0** (in my example) (enter)
  3. Enter ELAN gateway IP: **192.168.127.1** (in my example) (enter)
  4. Enter Primary CS IP: **192.168.39.26** (Breeze node's SIP/Secure interface in my example) (enter)
  5. Configure IPsec now? (y/[n]) : **n** (enter)
  6. Change MGC advanced parameters? (y/[n]) : **n** (enter)
  7. Is this correct? (y/n/[a]bort) : **y** (enter)
  8. Reboot MGC
- You can validate new configuration parameters at MGC with **cat /u/db/mgcdb.xml** from ldb **ONLY** with next successful connection establishing between MGC and Breeze.

Digital and analog sets registration

- Create new one user with **CS1k-1col_DEFAULT_CM_8_1, CS1k-2col_DEFAULT_CM_8_1, CS1k-39xx_DEFAULT_CM_8_1 or CS1k-ana_DEFAULT_CM_8_1** template at CM Endpoint profile. Select valid Sub type and Terminal number (System ID if need):

- Plug-in your digital or analog sets to DLC/ALC card at MGC.

- Validate your registration at SMGR with Session Manager->System status->User registrations

  You can verify digital sets registration with:

  At SMGR with Session Manager->System status->User registrations

  At digital phone by itself (keymap is presented)

From Breeze side: dsaShell dsaShow

From Breeze side - IPE card status with: ipeShow <loop>-<shelf>-<card>-<unit>

If your DLC card is still blinking red, remove the card from the cabinet and plug-in again, for re-detecting.

From Breeze side VGW channel status with: vgwShow <loop>-<shelf>-<card>-<unit>

- You can verify analog sets registration at SMGR with Session Manager->System status->User registrations

IPSEC configuration

- You must enable and fill PSK key (generate it according to description) at Avaya Breeze -> Configuration -> Attributes -> Service Globals -> DeviceAdapter service

  You can check created files (activate.txt and ipsec.xml) and configuration parameters at: /opt/Avaya/da/shared/config/MGC/ folder.
- Run **mgcsetup** at MGC and following the IPsec configuration procedure and **reboot**.
- To stop IPsec, run the following command:
  - Disable checkbox at Breeze attributes.
  - i**sssDecom** at MGC

Corporate Directory (AADS) configuration

For activation of Corporate directory necessary:

- Set CRPA flag in feature field on the phone;
- Configure AADS server (and LDAP server) on SMGR;
- Enable AADS server for cluster or global and fill URL and port for the AADS server.

Creating and configuration of users on LDAP.

For used Corporate Directory necessary to create a user on LDAP server with the next parameters: login and password should be as an extension for the user.

Device Adapter Limitations

There is no method to migrate customer settings for Call Forward feature.

Avaya Device Adapter Feature Interaction Limitations for 8.1.3

Avaya Device Adapter Feature Interaction Limitations for 8.1.2

- No hold conference feature button.

  The destination cannot be the Vector Directory Number.

  Pressing the Hotline or Speed Call key will abort the no hold conference feature and the phone screen will display the following message: invalid number.
- Merging of 2 conference calls into a single conference is not supported regardless of conference type CM or IX Conferencing.
- In case when password is not configured for Agent login and user will provide any password or text login operation will successfully finishes – there is no password check from CM side if password not configured.

Avaya Device Adapter Feature Interaction Limitations for 8.1.1

CM does not support ACB (Ring Again) across CMs to a station with Call Forwarding active.
The following scenarios do work:

- ACB to a forwarded station when all endpoints are on the same CM;
- ACB to a remote station that has coverage active (instead of forwarding);
- inter-CM ACB attempt does work if you wait 30 or more secs between attempts.

These are additional limitations of Avaya Aura® CM:

- Bridged line appearance ringing cannot be restricted by Device Adapter's media security policy setting.
- CM anchors the call in the call transfer scenario, having one leg secured (SRTP), and another leg not secured (RTP).

Avaya Device Adapter Product Interoperability for 8.1.3

Product	Release Details
Avaya Aura® System Manager	8.1.3
Avaya Aura® Session Manager	8.1.3
Avaya Aura® Communication Manager	8.1.3
Avaya Aura® Media Server	8.0.2
Avaya Aura® Device Services	8.1.3
SBCE	8.1
Avaya Breeze	3.8
Avaya Aura® Workspaces	3.6

Avaya Aura® Device Services

For the latest information, refer to Avaya Aura® Device Services Release 8.0.x Release Notes on the Avaya Support site at https://downloads.avaya.com/css/P8/documents/101060095