Avaya Aura® Release Notes

Release 8.0.x.x

Issue 3.6

September 2019

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 https://support.avaya.com/security

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

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

Change history

Issue	Date	Description
1	04-July-2018	GA Release of Avaya Aura® Release 8.0 Release Notes.
1.1	06-July-2018	Updated the Avaya Aura® System Manager artifact information and added a note in Avaya Aura® Application Enablement Services section.
1.2	09-July-2018	Updated the SDM Client section for System Manager file name.
1.3	11-July-2018	Updated product release matrix. Added CM-22618 in known issues section of Communication Manager. Updated the Release Notes link for Avaya Aura® Device Services.
1.4	18-July-2018	Added information related to CM-22679 for Avaya Aura® Communication Manager Release 8.0.0.1.1.
1.5	13-August-2018	Added information related to CM-22879, CM-21875, CM-21734, CM-22809, and CM-21762 for Avaya Aura® Communication Manager Release 8.0.0.1.2.
2.0	04-Dec-2018	GA Release of Avaya Aura® Release 8.0.1 Release Notes.
2.1	10-Dec-2018	Updated the following Avaya Device Adapter sections: Installation section, Known Issues section, and Product Interop information.
2.2	28-Jan-2019	Added information related to Avaya Device Adapter Release 8.0.1.
3.0	11-March-2019	GA Release for Avaya Aura® Release 8.0.1.1 and Avaya Aura® Presence Services Release 8.0.2 Release Notes
3.1	21-May-2019	GA Release for Avaya Aura® Application Enablement Services Release 8.0.1.0.3
3.2	31-May-2019	Clarification of Future use fields for Session Manager
3.3	24-June-2019	Minor typo corrections
3.4	19-Aug-2019	GA Release of Avaya Aura® Release 8.0.1.2 Service Pack Release Notes
3.5	9-Sep-2019	Updates to Installation and Fixes for G430 and G450 Media Gateways Release 8.0.1.2 Builds 40.31.0 and 40.31.30
3.6	27- Sep-2019	Added information related to Security service pack for Avaya Aura® Session Manager

Introduction

This document provides late-breaking information to supplement Avaya Aura® 8.0.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/101050513

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	**8.0.1.1**	**8.0.1**	**8.0**
Avaya Aura® Communication Manager	X	X	X
Avaya Aura® Session Manager	X	X	X
Avaya Aura® System Manager	X	X	X
Avaya Aura® Presence Services	NA	X	X
Avaya Aura® Application Enablement Services	X	X	X
Avaya Aura® AVP Utilities	X	X	X
Avaya Device Adapter Snap-in	NA	X	X
Avaya Appliance Virtualization Platform	X	X	X
Avaya Aura® G430 and G450 Media Gateways	X	X	X
Avaya Aura® WebLM	X	X	X
Avaya Aura® Media Server Release 8.0	X	X	X
Avaya Aura® Device Services	NA	NA	NA
Avaya Aura® Communication Manager Messaging (supported through 7.0.x)	NA	NA	NA

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.
- Customers may use AADS 7.1.3 with the Aura 8.0 release line up. AADS will be releasing AADS 8.0 in December 2018.
- 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).

What's new in Avaya Aura®

For more information see ***What's New in Avaya Aura® Release 8.0.x*** document on the Avaya Support site.

Support for the next generation server platform

Avaya Aura Appliance Virtualization Platform (AVP) 8.0.1 introduces support for Avaya Converged Platform 120 (ACP 120 - Dell PowerEdge R640).

Avaya Aura® Release 8.0.1.1 introduces support for Avaya Converged Platform (ACP 130 - Dell PowerEdge R640).

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

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 Redhat 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 8.0.x.x.

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 8.0.x.x

What's new in Communication Manager Release 8.0.x

For more information see ***What's New in Avaya Aura® Release 8.0.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101050420

Installation for Avaya Aura® Communication Manager 8.0.x

Required patches

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

For more details see PCN2082S on the Avaya Technical Support site https://downloads.avaya.com/css/P8/documents/101038688

Installation for Avaya Aura® Communication Manager Release 8.0.1

For information about installation of Release 8.0.1 please follow the document **Upgrading Avaya Aura® Communication Manager** dated December 2018 (Issue 2 for Release 8.0.1)

Required patches

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

Installation for Avaya Aura® Communication Manager Release 8.0

Backing up and installing Communication Manager

Communication Manager 8.0 software includes certain third-party components including Open Source Software. Open Source Software licenses are included in the Avaya Aura® 8.0.

Communication Manager Solution Templates DVD. To view the licenses:

1. Insert the Avaya Aura® 8.0 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

What’s new in Communication Manager Release 8.0.x

What’s new in Communication Manager Release 8.0.1.2

For more information see ***What’s New in Avaya Aura® Release 8.0.x*** document on Avaya Support site.

ID	Minimum conditions	Visible symptoms
CM-24422	Call Transfer	CM generates a UCID with UTC timestamp and UUI data is preserved for Single Step or Consult Transfer
CM-28614	Jxx Series SIP Set Types	Busy Indication on SIP station for Jxx Series set types

What’s new in Communication Manager Release 8.0.1.1

For more information see ***What’s New in Avaya Aura® Release 8.0.1*** document on Avaya Support site.

ID	Minimum conditions	Visible symptoms
CM-23000	AS-SIP, MLPP, OPTIM, SIP	MLPP (Multilevel Precedence and Preemption) Call Diversion support for SIP Attendant
CM-24157	SA8157	SA8157 enhancement to collect digits from the caller without sending the CONNECT message to PSTN trunk

Known issues and workarounds in Communication Manager Release 8.0.x

Known issues and workarounds in Communication Manager Release 8.0.1.1

ID	Minimum conditions	Visible symptoms	Workaround
NA	NA	NA	NA

Known issues and workarounds in Communication Manager Release 8.0.1

ID	Minimum conditions	Visible symptoms	Workaround
NA	NA	NA	NA

Known issues and workarounds in Communication Manager Release 8.0

ID	Minimum conditions	Visible symptoms	Workaround
CM-22618	CM	“G3 Version” field on the CM (Customer Options) OPTIONAL FEATURES form that reflects the current license has a “?” (question mark) instead of V18.	None

Fixes in Communication Manager Release 8.0.x.x

Fixes in Communication Manager Release 8.0.1.2

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
CM-10028	Service link call with MST enabled.	CM did a restart	6.3.9.1

ID	Minimum Conditions	Visible symptoms	Release found in
CM-21075	SIP agent reachability or Domain Controlled SIP station reachability is enabled.	SIP Agent logged out before the maximum polling attempts for SIP agents were exhausted	7.1.3.0.0
CM-21102	SIP station with IP version preferred is IPv4, H323 station with IP version preferred is IPv4, Per Service Link with Attendant with IP version preferred is IPv4 Mode=telecommuter with Direct Media enabled	SIP station direct media call to H323 telecommuter attendant fails	7.0.1.1.1
CM-21364	H.248 Media Gateway	CM did restart after many proc errors	7.1.1.0.0
CM-21751	Announcement Audit	Occasionally, CM did reset and interchange	7.1.1.0.0
CM-21900	Backup	BACKUP completed successfully but with Warnings for OS backup set	7.1.3.0.0
CM-22058	SIP Station	Occasionally an agent did hear a beep on a call, a bridge button appeared on the station and station locked up.	7.0.1.3.0
CM-22549	1xc IP softphone has a telecommuter number via sip trunk, it's permanent media encryption is on	1XC IP softphone Telecommuter call over SIP trunk is dropped when media encryption is used	7.1.3.0.0
CM-22985	change user pwd from web interface	pwd was logged to secure log in clear text, thus indicating a security vulnerability	7.1.3.1.0
CM-23056	Service Observe, Conference	Service Observe (SO) tone suppressed when conferencing SO station too soon	6.3.118.0
CM-23350	Analog/DECT phone present in pickup group as LAST member.	Pickup group members did not receive the accurate enhanced pickup display update.	7.1.2.0.0
CM-23659	AMS with announcement configured	No denial event is logged when AMS announcement ports are out of service	7.1.2.0.0
CM-23712	Bandwidth management Option: shared-SM	Announcements in an audio group across regions could not be played	7.1.3.1.0
CM-23753	EC500 enabled station over ISDN/PRI trunk.	EC500 mobile connected over ISDN/PRI trunk would able to see the caller's name even when the incoming SIP trunk call had CPN restriction.	7.1.2.0.0
CM-23960	SA8967 is enabled. "Mask CLI/Name for internal/QSIG/ISDN Calls?" enabled on cor form. H.323 stations connected over a direct SIP trunk between two CMs.	When the caller conferences the call on its own CM, other members of the conference were able to see the identity of the called party on the trunk side.	6.3.115.1
CM-24005	VAL Announcement	VAL-PT Alarms seen after maintenance	6.3.111.0
CM-24017	Video Call, Call Recording	The Video call did not establish when call recording is enabled	7.1.3.0.0
CM-24032	Hunt Group with one member, An agent must be video enabled,	Video enabled softphone agent could not answer the same call coming out of	7.1.3.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
	Redirect on No Answer (RONA) feature enabled	queue, if the agent missed the call at the first time	
CM-24150	(SA8734) - Enhanced Extension Display enabled. Multinational and Multi Locations enabled. Country Code was set on locations form.	Call log entry of a SIP station was incorrect when station busy on all call-appearances.	7.1.3.0.0
CM-24460	Voice Recorder, Attendant	CM experienced reset when ASC Voice Recorder tries to register as shared control to an Attendant	7.1.3.1.0
CM-24502	Enable SA8481	An alternate Caller Line Identification (CLI) on the called device for a call over SIP trunk did not get displayed	6.3.118.0
CM-24562	OneX-agent with service link calling a SIP station and out pulsing of digits involved in the call scenario after answer at far end	DTMF ESIG rejected by G450 and logs denial event 3706	7.1.1.0.0
CM-24648	SA8608	Special Application SA8608 to Increase Crisis Alert Buttons could not be enabled	8.0.0.0.0
CM-24766	2 CMs connected with SIP and H.323 QSIG trunks and call scenario involves transfer which should trigger path replacement	50% of time QSIG path replacement fails with no user visible impact	7.1.2.0.0
CM-24767	Attendant	ASAI Connect Event was not received by CTI Application when attendant user made a call	8.0.1.0.0
CM-24770	Call Center with SIP-connected messaging adjunct	Agent calls out to voicemail which transfers to station with immediate coverage back to voicemail. CMS ignores the next call over that SIP trunk port	7.1.3.0.0
CM-24780	send-nn	EC500 Call failed when send-nn button mapped to VDN	7.1.3.2.0
CM-24899	ISDN Trunk, VDN	The display on the calling station was changed when the call made to a VDN over an ISDN trunk played an announcement as a part of the vector step	7.1.3.1.0
CM-25029	Direct Media, Music-on-hold	When call was put on hold on SIP station, the remote party over the SIP trunk did not hear the music on hold	7.1.3.1.0
CM-25032	VDN/Vector configured with SIP trunk	Call transferring into Vector over SIP Trunk did not hear music	7.1.3.1.0,
CM-25043	Call Center, CTI	CM sent wrong party information in response to ASAI party query request for a transferred call ringing on agent	7.1.3.2.0
CM-25133	LSP	During call reconstruction CM LSP rebooted for every few minutes while in active mode	7.0.1.3.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-25134	VDN with Voice Mail	VDN number was displayed on the voice mail box instead of the caller's number when the caller was connected to the VDN over an ISDN trunk	7.1.3.2.0
CM-25150	"Provide Forced Local Ringback for EC500" is disabled and "Cellular Voice Mail Detection: timed for 5 seconds" in off-pbx-telephone configuration-set form	The caller did not hear ring back when EC500 VM answers the call.	7.1.2.0.0
CM-25181	B179 Phone	Hold failed when attempted from B179 phone	7.1.1.0.0
CM-25182	EC500	EC500 call dropped when a conferencing in an announcement.	6.3.118.0
CM-25200	IVR, Call Transfer	IVR could not able to perform transfer after receiving the call because CM sent called party information (VDN extension) with wrong type of number (NPI_TOA)	7.1.2.0.0
CM-25218	96x1 SIPCC phone	Q-Stats/VuStats feature button push failed on 9611SIPCC phone if the preferred handle was administered differently on System Manager than CM extension	7.1.3.2.0
CM-25262	SEMT (SIP Endpoint Managed Transfer, Call Forwarding	The transferred call dropped if the transfer target had call forward enabled and the call forward destination was the transferrer extension	7.1.3.2.0
CM-25300	QSIG Trunk, Call Forward	Call forward did not work if call arrives from QSIG trunk	7.0.1.3.0
CM-25387	Emergency call across CMs over PRI trunk from a SIP station	Expected "Calling Party Number" ie ELIN is not displayed at the far end when SIP station originated an emergency call	7.0.1.3.0
CM-25410	Privileged administrator command line access	Unauthorized root privileges could be obtained using sudo a privileged administrator	7.1.3.2.0
CM-25463	SIP Station, Post Major Network Outage	Occasionally, SIP stations could not register or able to make SIP calls	7.1.3.2.0
CM-25510	UCID and predictive call	UCID changed in predictive call and there was no trunk ID information in the offer event.	8.0.1.0.0
CM-25527	Pickup Group	SIP phone gets alerted for another pickup-group where that SIP station is not a member	7.1.3.2.0
CM-25594	Vector VDN, Auto Answer, Call Recording	No Connected event sent for an incoming trunk calls that get transferred to a SIP agent which is in auto answer mode	7.1.3.1.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-25597	G650 Gateways	False alarms (CAB-MTCE and RING-GEN) raised against the IPSI maintenance board during network instability.	7.1.1.0.0
CM-25613	Hyperactive H.323 station	CM could experience heap corruption and reset if the H.323 station went into hyperactivity and consistently sent CM a huge amount of data in a short period time.	7.1.3.1.0
CM-25829	SIP station with call-fwd button	J169 SIP client could not cancel the call-fwd if the call-fwd button was pushed and only ARS/AAR FAC code was put in.	8.0.0.0.0
CM-25859	MDA	Equinox MDA (Multiple Device Access) SIP client displayed missed call log instead of incoming call log if the incoming call to the MDA extension was answered by the other MDA device.	7.1.3.2.0
CM-25871	Enabled (SA9108) - Local Time Support for CDRs	CDR printed incorrect local-time-to and local-time-from upon CDR link recovery	7.1.3.1.0
CM-25912	Call Coverage, Call Forward, EC500	Trunk call did not cover if call cover is configured to same destination as call forward destination with EC500 enabled	7.1.3.3.0
CM-25925	(SA8702) - CDR Enhancements for Network? y UNIVERSAL CALL ID Create Universal Call ID (UCID)? y UCID Network Node ID: 341 Copy UCID for Station Conference/Transfer? Y	Corrupt CDR records with strange binary characters in the UCID field	7.0.1.3.0
CM-25927	Stub Network Region, Fax	Fax mode set to fax relay when fax server in stub network region	7.1.3.1.0
CM-25938	Disabled "Media Encryption Over IP" on system-parameters customer-option Make SRTP capability negotiation video call from originator	The video is not established in the call	8.0.1.0.0
CM-26019	CTI, Announcement	In the conference call, missed Disconnect Event for announcement drop	7.1.3.0.0
CM-26032	SMI	Deep Secure to filter web traffic found incorrect syntax in SMI	7.1.3.1.0
CM-26068	ASM has two SIP entity links configured for CM, one is a TLS link, and one is a TCP link. CM configured with matching signaling groups for the TLS link, but not for the TCP link	An extreme inbound call traffic event drove CM into CPU overload	7.1.3.1.0
CM-26074	Group Page	If any SIP phone is unavailable and part of a group page, confirmation tone is delayed 6-8 seconds.	7.1.3.2.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-26183	Missed Call Log	The missed call log for SIP phone showed incoming trunk name instead of far end caller for a "covered-all" call	7.1.3.1.0
CM-26298	CTI	CTI links failed with CM sending a zero window at TCP level to AES	7.1.2.0.0
CM-26382	Call Center with Timed After Call Work	Sometimes an auto-in agent that dropped from a call due to a network transfer could not receive ACD calls before another work mode change	7.1.3.2.0
CM-26386	Equinox	Equinox could not make or receive calls because the call appearances got stuck	7.1.3.1.0
CM-26760	SIP station	If the field "Restrict Second Call Consult?" was turned on in the COR form, The SIP station couldn't make the second consult call if it cancelled the first consult call attempt.	7.1.3.2.0
CM-26851	Uniform Dial Plan	Lots of Denial Event 2400 UDP: too many conversions were generated	7.1.3.2.0
CM-27010	Attendant	Connect Event was not received by CTI-application when attendant user made a call termed to a SIP station	7.1.3.3.0
CM-27056	ASAI	In rare instances CM did reset	7.1.3.2.0
CM-27146	Avaya Device Adapter CS1K set type	If the transfer target or transferred phone are CS1K 1110/1210/2001 with only one call-appearance button allowed, the SEMT (SIP Endpoint Managed Transfer) would fail.	8.0.1.0.0
CM-27181	Station activating call forwarding and an audit updating its lamps at the same time	Occasionally CM servers did warm interchange due to system message buffer exhaustion	7.1.3.1.0
CM-27250	Call Forward	Call Forward Override by Team Button not working if coverage criteria all outside is set	7.1.3.3.0
CM-27266	Call pick-up group with a mix of SIP and non-SIP members	Non-sip pickup-group members were not sent alerting display	7.1.0.0.0
CM-27380	AES CTI, SIP Station	The UUI of old/held call was presented to the CTI for the consultation call from SIP station rather the updated UUI provided by CTI while originating a consult call.	8.0.1.1.0
CM-27391	AAR/ARS	Adding AAR/ARS call type in dial-plan analysis table allowed even if "ARS/AAR Dialing without FAC?" is disabled	7.1.3.0.0
CM-27407	One-X Attendant	One-X Attendant when transferring call to external number did not send Calling Party Number	7.1.3.3.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-27470	VDN, ASAI	Incorrect called party number (VDN number instead of original dialed number sent in ASAI notification	7.1.3.3.0
CM-27500	Enter trunk number as 4 in "Trunk Selection" field of the "change off-pbx-telephone station-mapping" form	Unable to set high numbered TGs into the off-pbx station-mapping form with error message generated as Error encountered, can't complete request; check errors before retrying	7.1.3.2.0
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-27524	CTI	CM sent wrong connected number info in domain control disconnect event report	7.1.2.0.0
CM-27544	Conference	Conference using bridged-appearance failed when call is answered from a VDN	7.1.3.1.0
CM-27648	Survivable Servers and H.323 phones connecting via Zscaler Private Access or other devices that send zero length packets.	Survivable Server registration alarms generated and/or H.323 phones could not register.	7.1.2.0.0
CM-27673	Incoming SIP trunk call to CM (which is measured) answered by agent and then agent attempts to transfer the call	Customer saw "IGNORED" calls in CMS reports and saw occupied ITN being used for new incoming call.	7.1.2.0.0
CM-27678	MCA bridging	CM reset when processing MCA bridge call.	8.0.1.0.0
CM-27679	DMCC configuration	A segmentation fault could happen when shared control AES (Avaya Aura Application Enablement Services) DMCC (Device, Media and Call Control) phone tried to transfer the media path in the middle of a call.	8.0.1.0.0
CM-27689	Unregistered SIP Stations as members in a hunt group	SIP Phones which are unregistered are not deactivated at hunt groups	7.1.3.2.0
CM-27695	CAG configured in coverage path and the trunk to MM should go through SM.	Number conversion not applied to the History-Info, if call goes through CAG in coverage path	7.1.3.3.0
CM-27697	A host that sends keep alive RRQ every 20ms	A bad host drives CM into overload/reset	8.0.1.0.0
CM-27726	CM configured with SIP trunk group	SIP trunk members cannot be decreased anymore, only increase is possible	8.0.1.1.0
CM-27741	Shared station registration	Memory leak when call is placed or received at a station which has a shared station	8.0.1.1.0
CM-27751	CM using AMS for media and audit is triggered	Bad internal AMS state resulting in AMS resource exhaustion	7.0.1.2.0
CM-27845	TTI enabled	Multiple ports unable to be assigned to stations. Data conflict detected, please	7.1.3.2.0

ID	Minimum Conditions	Visible symptoms	Release found in
		cancel and try again error. Softphones could not login.	
CM-28074	Incoming INVITE with "History-Info" headers but no "histinfo" tag in "Supported:" header	CM did not forward History-Info SIP header to Avaya Aura® Contact Center (AACC)	7.1.3.3.0
CM-28107	2 CMs, SIP trunk and auto callback	Auto-cback shows up on phone display as a national call only.	6.3.118.0
CM-28119	Call Center	During vector processing if DTMF tones are received, it caused no talk path on the call.	7.1.1.0.0
CM-28178	CM with one main at region 1 and one LSP at remote location n, ams1 local to the main in region 1, ams2 in the lsp region and is backup server for lsp region, only ams2 is added to lsp's MSRL -, shutdown ams2, then reboot ams1 issue seen when ams1 comes back into INS	no phone call can be placed	7.1.3.3.0
CM-28183	Button assignment section of station on SMGR	Extra digit "R" shown in button assignment section of a station through Element Cut-Through in SMGR	8.0.1.0.0
CM-28207	CM shuffles AEP station and SIP trunk with "rtp-payload"	DTMF fails after CM shuffles AEP station and SIP trunk with "rtp-payload"	7.1.3.3.0
CM-28255	Large CM configuration with more than 50 audio group entries.	Audio-group, integrated-annc-boards displayed only 50 entries on the audio-group form	8.0.1.1.0
CM-28276	Unregistered SIP Stations as members in a hunt group	SIP Phones which are unregistered, did not get deactivated at hunt groups	7.1.2.0.0
CM-28294	Addition of split stream recording station and corruption audit tool	BBE corruption audit tool that uses tcm NREAD_PREC broken because shared station ports were not saved to translations after addition of split stream recording.	8.0.1.0.0
CM-28627	Busy out of signaling group with 1500 trunk members.	Unexpected ALLOC_BUF restart & interchange caused by busy out of signaling group with 1500 trunk members.	8.0.1.1.0
CM-28795	Shared station registration, un-registration and a new stations addition	“Error encountered, can't complete request” error message seen while executing certain commands after shared station registration/un-registration and a new station addition	8.0.1.0.0
CM-28983	Upgrade from 7.0 or earlier release.	The "Cluster" field on the SAT Signaling Group form displays a "?" after an upgrade from an earlier release.	8.0.1.0.0.0

Fixes in Communication Manager Release 8.0.1.1

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
CM-17432	CDR, R2MFC Trunk	CM generated CDR as answered call for an outgoing call via R2MFC trunk and dropped before call answered	6.3.15.0
CM-18377	SIP Trunk call, Experience Portal (EP) or Voice Portal (VP)	Incoming SIP trunk call to Experience Portal (EP) or Voice Portal (VP) dropped around 15 seconds after call is transferred	6.3.17.0
CM-20577	On CO trunk Outgoing Dial Type: automatic Receive Answer Supervision? no	SIP station dials a CO trunk TAC followed by number and Session Establishment Timer expires dropping the call	6.3.14.0
CM-21023	CM	Occasionally, CM did warm reload	8.0.0.0.0, 6.3.12.0
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-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-23166	calltype analysis configured	User dialed from call log containing ARS/AAR code was shown in ASAI calledDevice IE on event orig went to cti-applications	7.1.3.0.0, 6.3.113.0
CM-23609	VDN, IP (H.323) Stations	The call dropped from AAEP due to missing UUI information. The UUI information did not get pass to AES and AAEP as CM fails to build and send ALERT and CONNECTED event to AES putting UUI information.	7.1.3.1.0
CM-23752	SIP	CM intermittently drop the call for scenarios involving SIP, sends “488 Not Accepted Here”	7.1.2.0.0, 7.1.0.0.0
CM-23779	Call Transfer, VDN with converse step	CM did not send disconnect event after hold on a converse on step of vector	8.1.0.0.0, 7.1.2.0.0
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-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-24161	SIP, AES	CM did not send calling number towards AES intermittently	7.1.3.1.0
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

ID	Minimum Conditions	Visible symptoms	Release found in
CM-24193	SIP trunk, Direct Media enabled	CM did reset	7.1.3.2.0
CM-24246	SIP, VDN, AES	More than one party on call and call is blind transferred to a SIP trunk via VDN, CM did not send the alert event to AES	7.1.2.0.0
CM-24260	Call Recording, ASAI	Outgoing calls from agents did not record intermittently	7.1.3.0.0
CM-24308	ASAI, Service Observe (SO), SIP, H.323	ASAI message flow for SIP versus H.323 SO of a SIP station was different For SIP SO, there was an alerting (extra message) followed by a connect. The difference in messaging caused Oceana to mishandle the call	7.1.3.0.0
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-24479	Call Coverage	Call to VDN/vector with route-to number with coverage failed to cover	7.1.3.1.0
CM-24480	SIP station using a route-pattern that is the same as a SIP trunk-group	SIP trunk-group could not be removed due to false positive usage by a SIP station that is using a routing pattern in the "SIP Trunk" field with the same number	7.1.3.2.0
CM-24490	Communication Manager Release 8.0 and above Changing agent skills from CMS with BCMS also enabled	When the 'Agent Skills' are changed from CMS supervisor the "BCMS Measured Agents:" count on the "display capacity" form gets incremented incorrectly. This causes failed agent logins when the count reaches its max value of 3000	8.0.0.1.1, 8.0.0.1.0
CM-24510	CM License, SMGR WebLM	SMGR 8.0 WebLM did not show license status for CM	7.1.2.0.0
CM-24515	Audit	Call record audit blocked from dropping stuck call.	7.1.3.2.0
CM-24548	Call Coverage	Unregistered SIP station with no bridges or EC500 failed to immediately cover to VM.	7.1.3.2.0
CM-24669	CDR	CM SMDR process did cause it to interchange	7.1.3.2.0
CM-24724	Call Forward	Enabling call forward remotely with large numbers caused last digit to be truncated if all the string exceeds 36 digits	7.0.1.3.0
CM-24735	Call Recording, Path Replacement	Call recording was getting terminated after path replacement	7.1.3.2.0
CM-24897	Network Call Redirection (NCR), VDN, SIP Trunk	Occasionally, calls did not clear	7.1.3.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-24975	Communication Manager 7.1.2.0.0 and Agent DAC calls.	Call handing preference, Service objective information not sent to CMS for DAC calls sent to agent	8.0.0.1.2, 7.1.2.0.0
CM-25004	One-X CTI	Calls generated from One-X CTI application get half ring	7.1.2.0.0
CM-25028	Bridge Appearances	Few SIP bridged appearances did not ring in	7.1.3.2.0
CM-25042	Security Code	IP Station Security code change with FAC not working	8.0.1.0.0
CM-25234	VDN, SIP Call	A call routed through collect step in vector failed to collect digits and hung at	7.1.3.1.0
CM-25237	Call Center Agent	Most idle agent did not receive calls for up to 30 minutes. If the agent logs out and back in agent starts to receive calls again	7.1.2.0.0

Fixes in Communication Manager Release 8.0.1

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
CM-19559	Criteria for Logged Off/PSA/TTI Stations? N, No EC500, Coverage path configured, SIP Stations	Caller did not hear ring back on a call to station which has bridge appearance on another station	7.1.2.0.0
CM-19846	H.323 trunk between CMs with ip-codec-set set to aes/aea	No talk path if Medpro is used and call drops if GW is used	7.1.2.0.0
CM-20190	CLIENT ROOM turned on in COS SA8744 turned on	If the special application(SA) 8744 was turned on, a call to a station with "Client Room" enabled for its COS could potentially cause CM a segmentation fault when the call covered to a coverage point	7.1.2.0.0
CM-20447	SIP Avaya Onex-Communicator logged in as other phone mode	When SIP Avaya OneX-Communicator was logged using other phone mode, the other phone was not receiving calling line identification as per public/private numbering configuration	7.1.1.0.0
CM-20799	SIP trunk, auto-callback button. Far end did not send display name information	H.323 caller displayed gibberish characters on screen on auto-callback activation, for an outgoing call dialed over SIP trunk	7.0.1.2.0, 6.3.15.1
CM-20941	1.Administer a SIP CC station with SO functionality 2. In the off-pbx mapping choose "rp" as the routing option 3. Start Service Observing a station in	SIP Service Observer not able to switch between listen and talk-listen mode	7.1.2.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
	listen-only mode. After the call starts, try changing to talk-listen		
CM-20947	Conference call	CM did system reset in a rare instance	7.0.1.3.0
CM-20978	Configure send-nn button and press it before launching a call from a station monitored by ASAI	Call recording fails via AES if monitored calling party presses send-nn button before placing call	7.0.0.0
CM-21113	Avaya Aura Media Server	Media capacity for out of service AMS servers may show up as 50 channels instead of 0 on measurement reports	7.0.1.3.0
CM-21140	Incoming ISDN/H.323 trunk call and CPN contains '+'	Call fails to tandem if the incoming ISDN/H.323 trunk call contains '+' in the CPN	6.3.9.0
CM-21314	SIP Station	The page call would fail if SIP station made the page call through the autodial button	6.3.17.0
CM-21325	WebLM URL parameters are not being checked by the Web server, allowing invalid characters	Some vulnerabilities might happen	7.1.2.0.0
CM-21332	Outgoing trunk call. Call is answered and the connect event changed the NPI-TOA	CTI-application sends wrong NPI-TOA in connect event impacting 3rd party applications consuming that event	7.1.2.0.0
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-21393	Converse step configured in a VDN vector and stations being monitored	Transfer operation does not result in drop indication impacting 3rd party applications	7.0.1.3.0
CM-21434	ESS	Interchange of duplicated ESS or loss of service for simplex ESS	6.3.15.1
CM-21539	One-X Attendant, Call Transfer	One-X attendant could not able to transfer call to virtual station that covers to SIP station	6.3.17.0
CM-21565	SIP Domain	CM did an interchange multiple time	7.1.2.0.0
CM-21628	SIP Call	CM did not respond for an incoming SIP update if the “Retry-After” header values are more than 2899999999 and reported it as a parse error	6.3.15.1
CM-21698	Group Page more than 8 members, VDN	Call to group-page with more than 8 members via VDN/vector failed	6.3.16.0
CM-21711	SIP stations configured with pick-groups and enhanced call pickup alerting enabled on the change system parameters features form	Randomly, enhanced call-pickup alert notification was received by members not being a part of the called pickup-group	7.1.2.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-21749	Unregistered SIP Station, Criteria for Logged Off/PSA/TTI Stations? set to Yes	When SIP user is not registered and no coverage path for the station, caller kept hearing ring back.	7.1.2.0.0
CM-21853	SOSM (SA8475)	Monitoring with SOSM (SA8475) failed for IP and digital stations while redial or autodial feature used	7.1.1.0.0
CM-21875	"Send UCID" on the SIP trunk group form is enabled	SIP UUI in incoming Invite from AAEP is stored in CM as shared UUI but the same UUI was not sent in an outgoing Invite to CM2	7.1.2.0.0
CM-21915	Principal and bridge phones are monitored	ASAI did not receive principal station drop event after hold from principal and unhold from bridge thus causing recording application to hang when the caller dropped the call	7.0.1.2.0
CM-21944	SA9135 enabled. H.323 station logged in telecommuter mode IP-Agent logged into the H.323 station. One-X CES mapping configured for the H.323 station	OneX CES callback calls were blocked when the call was made for an IP-Agent logged into a H.323 station in telecommuter mode	7.1.3.0.0
CM-21980	LDN, Attendant	For LDN call coming from an attendant, an TSAPI event received only when the call was connected, not while it was ringing	7.1.2.0.0
CM-22015	Enable Criteria for Logged Off/PSA/TTI Stations? y on system-parameters coverage-forwarding form H.323 station A with team button configured for H.323 station B. H.323 station B has EC500 configured but disabled H.323 station B has Enhanced call forwarding (No reply) enabled to H.323 station C	Enhanced call forwarding failed when call was made using team button speed dial to a logged-out station	6.3.18.0
CM-22017	CM with port network, TN2602, H.323 trunks, non-CM far-end	CM IP trunk calls might stay anchored on Media Processor TN2602 and result in inefficient use of DSP resources	7.1.2.0.0
CM-22055	Fax over SIP trunk using G.711 pass-through mode	A call did not transition to XOIP (Fax over IP) type	7.0.0.0
CM-22061	SIP traffic	Possible Segmentation Fault at customer deployment.	8.0.0.0.0, 7.1.0.0.0
CM-22081	SIP traffic	Occasionally, CM did reset	8.0.0.0.0
CM-22176	ip-network-map not configured and administer "CPN, ANI for Dissociated Sets:" field on system-parameters features form	ELIN configured on "CPN, ANI for Dissociated Sets:" field is not sent properly over the outgoing trunk	6.3.16.0
CM-22191	SIP phones and trunks	On rare occasions the system may reset	8.0.0.0.0, 7.1.2.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-22382	Enable shuffling Change SIP headers associated with display while sending SDP answer to CM	One way talk path issue may be observed	7.1.0.0.0
CM-22429	SIP Endpoint Managed Transfer enabled in CM on system-parameters features form	SIP 96x1 transfers a call and missing ASAI events caused reporting malfunctions at TSAPI applications	7.1.2.0.0
CM-22447	Monitor VDN and do predictive calling from the VDN	ASAI message for incoming call, contains calling and the called number as the VDN number instead of correct calling party number in case of a predictive dialing call	7.1.2.0.0
CM-22540	Communication Manager (CM) Release 7.0 (or later) connected to a Call Management System (CMS) Release R18 (or later)	CMS Link Restarts when the Tenant Number is changed from CM Admin for an Externally Measured Skill while Agents are Logged In to the Skill	7.1.2.0.0
CM-22558	CM, AMS and filename with '&', i.e. AT&T_Greeting2	CM cannot play an AMS sourced announcement if the filename contains an '&' (ampersand)	7.1.1.0.0
CM-22559	Bridge Appearance	Bridge Appearance showed active/busy preventing calls to main number	7.0.1.2.0
CM-22561	Incoming ISDN call to OneX-C station with CES integration	A missed call was observed in logs for an established call when an incoming ISDN call was made to Avaya one-x communicator with CES (Customer Enhancement service) Integration	7.1.2.0.0
CM-22569	Configure personal-co line group button on two stations and make a direct connection of their media gateways.	Softkeys on station do not appear when taking a personal-COline off hold from another station where it was answered.	6.3.18.0
CM-22570	CDR, IVR	CDR did not generate for call transferred to VDN by IVR	7.0.1.3.0
CM-22594	BSR polling	CM did interchange, BSR polling did not work	7.1.3.0.0
CM-22599	SOSM application running a multi-party call	Under rare circumstances a reset occurred when running SOSM feature	7.1.1.0.0
CM-22618	Executing a "display system-parameters customer-options" command	When executing a "display system-parameters customer-options" command, the " G3 Version" field displays a "?" instead of "V18"	8.0.0.0.0
CM-22668	Call Transfer, Station Display	External number did not display when the transfer is completed.	7.1.3.0.0
CM-22670	SIP stations	Communication Manager (CM) could experience a memory leak if the far end does not respond	7.1.3.0.0
CM-22683	VDN with VOA configured	CM processing errors logged in traces	7.0.1.3.0
CM-22721	H.323 station with buttons administered	When any personalized button label on CM H.323 endpoint was changed to	8.1.0.0.0, 8.0.0.0.0, 7.1.3.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
		blank, the button was removed from the phone display	
CM-22729	SIP Trunk Call	External number did not display when the transfer is completed	6.3.16.0
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-22824	CM with PN with Medpros SIP trunk using RFC2833 for DTMF transmission Far-end SIP agent must respond with different telephony event payload type than was offered by CM	Entering digits for a remote system such as a conference bridge with password access may fail due to failure of DTMF digits to be recognized by the conference bridge	7.1.2.0.0
CM-22825	SIP trunk with DM on and the terminating station has DM off	Customer may not able to make successful calls in Direct Media mixed setting on SIP originating party and SIP terminating party	7.0.1.3.0
CM-22853	Port Network	TN2793 boards generated FATAL errors frequently	7.1.3.0.0
CM-22863	SA9114 (Expand Public Numbers to International for ASAI?) is enabled. On location-parameters form, International and country code configured with at-least 3 digits	Missing "CALLING PARTY NUMBER" in ASAI "Alert" event leading to display issues	7.1.3.0.0
CM-22928	CMS configured on CM. CMS should support SPI24 language. Hunt agent configured on CM. Have stroke count button configured for agent	CM sends stroke count code 3 to CMS when it supposed to send stroke count code as 8	7.1.1.0.0
CM-22969	CDR, VDN, Agent Call Transfer	CDR did not generate for an agent in case call is blind transferred to another agent or VDN	7.1.2.0.0
CM-22979	SIP stations	Barge tone was played continuously if the SIP station bridged in an EC500 call	7.1.3.0.0
CM-22986	Hunt Group	Re-hunt on No Answer did not ring back on all hunt group members	7.0.1.3.0
CM-23046	MST	MST call trace filter broken, trace captured a lot of other call trace messages, unrelated to the filter	7.1.3.0.0
CM-23047	Call into vdn with adjunct route getting UUI, then agent with 1XA pushes the uui info button	The UUI displayed is truncated when the Agent presses the 'uui-info' button	7.1.2.0.0, 7.1.1.0.0
CM-23086	LAI, IP ISDN interworking for max forward	Vectoring with LAI using 'route to step' looped continuously, after few loops the vectoring stopped	7.1.3.0.0
CM-23134	Monitor VDN and do predictive calling from the VDN	ASAI message for incoming call, contained default trunk number (#####)	7.1.3.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
		and the called number as the VDN instead of correct calling party number in case of predictive calling	
CM-23145	system with heavy traffic loaded and/or having a high number of measured trunks.	1) Hourly measurements not coming out at the top of the hour, but at random times within the hour 2) Every 13th hourly measurement is missing 3) Hourly measurements cover 65 minutes instead of 60 minutes, thus skewing the numbers (e.g., call counts are 8.3% too high)	8.0.0.1.0
CM-23148	Conference, Station Display	An incorrect CLI display at the end station added to the conference	7.1.3.0.0
CM-23149	SIP transfer	Network-region was retrieved from signaling group instead of the ip-network-map form resulting in a failed call	7.1.2.0.0, 6.3.18.0
CM-23188	Operator Transfer Call	Call dropped when call is transferred by attendant during the redirect tone	7.1.3.0.0
CM-23335	RONA	RONA did not work properly, RONA call directed to VDN to agent went to cover immediately	7.1.1.0.0
CM-23363	Team Button Monitoring station had COR enabled, to pick up incoming call at monitoring station by going off-hook	Team Button monitoring station was not able to pick up the incoming call at monitored station, by going off-hook	7.1.3.1.0
CM-23400	SNMP enabled	Occasional segmentation fault when SNMP is starting	7.1.3.1.0, 7.1.2.0.0
CM-23500	Conference, Station Display	An incorrect CLI display at the end station added to the conference	7.1.3.0.0
CM-23537	Enhanced Pickup Group	Enhanced pickup group members did not alert	7.1.3.1.0
CM-23579	Call Park	Parked Calls are getting disconnected when recording station disconnects	7.0.1.3.0
CM-23661	Domain control of a station, with a CTI selective drop request where the domain control is for a call that does not exist at that station	Calls are not recording, CM responding with error 98 to 3rd party selective drop	7.1.2.0.0
CM-23678	Signal button	Signal button got denial treatment when signaling an analog station	7.1.3.0.0
CM-23687	Hold, Misoperation Alerting	The call dropped when trunk call put on hold and SSC party drops with Misoperation Alerting enabled	7.1.2.0.0
CM-23786	SIP signaling group configured	Possible Server interchanges when SAT Signaling Group field "Peer Detection Enabled" set to 'n' on SIP signaling group	7.0.1.3.0
CM-23816	Conference, Station Display	An incorrect CLI display at the end station added to the conference	7.1.3.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-23902	Agent State	Agents noticed they could not change states anymore from Aux to Auto-In, After Call or another Aux	7.1.0.0.0

Fixes in Communication Manager Release 8.0

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
CM-21103	Avaya Aura Communication Manager configured to send LRQ(Location Request) message. Far end device did send LCF(Location Confirmation) with additional IP address	When LCF(Location Confirmation) message was received by Avaya Aura Communication Manager, in certain scenarios software trapped	7.0.1.2.0
CM-22679	CM configured the clustered signaling group with number above 255.	SIP Agent Reachability feature is not working	8.0.0.1.0
CM-22869	Configure maximum of 32767 (trunks and stations) Try to change the any field which takes value of y/n	When try to change the y/n fields it gives error message "Value is less than the number of administered station and trunk ports"	8.0.0.1.1
CM-21875	Incoming trunk call with ASAI-UUI to Outgoing SIP trunk with UCID enabled	SIP UUI is invalid and corrupted in the outgoing Invite. The receiving agent fails to get a proper screen pop	8.0.0.1.1
CM-21734	Enable measurements for AFR trunks. Save translation	Save translation was showing error.	8.0.0.1.1
CM-22809	Configure AFR trunk--1 with 9999 members on signaling-group 1. Configure AFR trunk-2 with 9999 members on signaling-group 2. Change the AFR Trunk-2 from signaling-group 2 to 1 and submit. Do server interchange	Server Interchange was creating core file and CM rebooted. Translations are corrupted.	8.0.0.1.1
CM-21762	Remove administered Media-Server	CM was rebooted	8.0.0.1.1

Avaya Aura® Session Manager

What's new in Session Manager Release 8.0.x.x

What's new in Session Manager Release 8.0.x

For more information see ***What's New in Avaya Aura® Release 8.0.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101050420

Future use fields visible in Avaya Aura® Session Manager Release 8.0

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 is intended for future use:

- Session Manager → Global Settings → Enable SIP Resiliency

Security Service Pack

Beginning with 8.0.1.2, Session Manager is releasing an 8.0 Security Service Pack (SSP). This SSP can be applied to any version of 8.0 and only includes Red Hat security updates. It is not necessary to apply the SSP on top of 8.0.1.2 itself because 8.0.1.2 includes all the same updates. For further information on contents and installation procedures, please see PCN**2109S**.

Installation for Session Manager 8.0.x.x

Backing up the software

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

Installing the Session Manager software

Upgrading

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 8.0.x are from:

   - 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 8.0.

2. Security Hardened Mode

   When upgrading an 8.0 Session Manager that is configured in Security Hardened mode to 8.0.1, the Cassandra DB will also be upgraded. Session Managers that are on 8.0.1 will not synchronize Cassandra data with Session Managers that remain on 8.0. Also, Cassandra repair operations will fail. These issues will clear up once all Session Managers are updated to 8.0.1.

3. VMware-based Session Manager

   The supported upgrade paths to Session Manager 8.0.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

4. KVM-based Session Manager

   The supported upgrade paths to Session Manager 8.0.x are:

   - SM 7.1.1 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

   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.

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

Important note regarding server support

The following servers are no longer supported with Session Manager 8.0:

- Avaya Common Server R1 (CSR1)
- S8300D

Troubleshooting the installation

Refer to Troubleshooting Avaya Aura® Session Manager.

Restoring software to previous version

Refer to product documentation.

Fixes in Session Manager Release 8.0.x.x

Fixes in Session Manager Release 8.0.1.2

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-75825	High alarming rates	Alarm failures and Serviceability Agent stops responding	7.1.3.0
ASM-75851	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-74062	The data center assignment for an SM is changed.	The operation partially fails and device data, and centralized call logs may be lost.	8.0.1.1
ASM-75830	Use of User Provisioning Rule to add/edit users Session Manager Profile.	The following fields are not properly committed to the database: "Block New Registration When Maximum Registrations" and "Enable Centralized Call History"	8.0.1.1
ASM-72976	N/A	Various TraceSM improvements	7.1.0.0
ASM-72072	Administration issue resulting SIP routing loops	BSM goes out of service due to failure to detect and break looping SIP invite.	7.1.2.0
ASM-75167	[RHSA-2019:0435-01] Moderate: java-1.8.0-openjdk security update	N/A	8.1.0.0
ASM-74970	[RHSA-2019:0483-01] Moderate: openssl security and bug fix update	N/A	8.1.0.0
ASM-74971	[RHSA-2019:0512-01] Important: kernel security, bug fix, and enhancement update	N/A	8.1.0.0
ASM-75288	[RHSA-2019:0679-01] Important: libssh2 security update	N/A	8.1.0.0
ASM-75310	[RHSA-2019:0710] Important python security update	N/A	8.1.0.0
ASM-75386	[RHSA-2019:0775] Important: java security update	N/A	8.1.0.0
ASM-75626	[RHSA-2019:0818-01] Important: kernel security and bug fix update	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-76337	[RHSA-2019:1619] Important: vim security update	N/A	8.1.0.0
ASM-75169	RHBA-2019:0689 tzdata bug fix and enhancement update	N/A	8.1.0.0

Fixes in Session Manager Release 8.0.1.1

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-73274	Adding 2nd Adaptation in System Manager Routing screen fails	Error displayed on System Manager when attempting to add a second Regular Expression route to a SIP entity.	8.0.1.0
ASM-74094	SIP Entity Monitoring shows down state with 500 server internal error(missing P-AV-Transport) if entity is added with adaptation to remove GSID	SIP Entity Monitoring will show a link as down if the P-AV-Transport if adaptation removes the Av-Global-SessionID header.	8.0.1.0
ASM-70803	Double missed call logs entry generated after logout and re-login if Call Journaling is enabled for the user	Call History Log on an endpoint will show duplicate records for a single call in some cases when user logs out and then back in.	8.0.0.0
ASM-70838	Session Manager License Expiration alarms should be logged daily	Previously alarms would be logged when a license expiration crosses a boundary. If SMGR is unavailable at that time, no alarm indication would be shown. Now the alarms are logged daily.	7.1.2.0
ASM-64731	Import of dial patterns with approximately 1500 originating locations severely impacts dial pattern administration performance	When a Dial Pattern had 1500+ originating locations assigned, the UI performance was very slow. Enhancements were made to how the UI handles large numbers of originating locations.	7.0.1.2
ASM-71699	Device values may not be updated on System Manager User Registrations page	Sometimes registered user device data (Vendor/Type/FW Version/etc) is not properly displayed in the User Registration Status screen for AST devices.	8.0.1.0
ASM-72786	DNS SRV override fails when using SRV records from enterprise DNS server instead of LHNR	Entity links configured to use DNS SRV Override will not establish. LHNR based entity links with DNS SRV override work fine.	8.0.0.0
ASM-69956	Unable to provide permission to custom role if role is created under default role other than under System Administrator role	When creating a role with Routing Administrator as the parent role, permissions for that new role cannot be modified.	7.1.0.0
ASM-60371	Cannot filter Entity Links listing in System Manager Routing screens, based on "Deny new Service" column	Attempting to filter a list of SIP entities based upon the “Deny New Service” column of the table, yields	6.3.13

ID	Minimum Conditions	Visible symptoms	Release found in
		no results, regardless of state of Deny New Service value.	
ASM-59821	User Data Storage backup host configuration cannot be cleared	A delete button was added to the User Data Storage Backup configuration to allow it to be cleared out.	7.0.1.2
ASM-64798	User Registration RBAC not working correctly for SM/Routing auditor	The User Registrations page on System Manager > Elements > Session Manager screens was not adhering to RBAC controls per the role administration.	7.1.0.0
ASM-73060	(RHSA-2018:3092) (tcp)	N/A	8.0.1.0
ASM-73025	[RHSA-2018:3059-01] Low: X.org X11 security, bug fix, and enhancement update	N/A	8.0.1.0
ASM-73024	[RHSA-2018:3324-01] Moderate: fuse security update	N/A	8.0.1.0
ASM-73050	(RHSA-2018:3083) (tcp)	N/A	8.0.1.0
ASM-72994	[RHSA-2018:3032-01] Low: binutils security, bug fix, and enhancement update	N/A	8.0.1.0
ASM-73028	[RHSA-2018:3221-01] Moderate: openssl security, bug fix, and enhancement	N/A	8.0.1.0
ASM-72991	[RHSA-2018:3041-01] Moderate: python security and bug fix update	N/A	8.0.1.0
ASM-73027	[RHSA-2018:3071-01] Low: krb5 security, bug fix, and enhancement update	N/A	8.0.1.0
ASM-72992	[RHSA-2018:3050-01] Moderate: gnutls security, bug fix, and enhancement update	N/A	8.0.1.0
ASM-73026	[RHSA-2018:3327-01] Low: libmspack security update	N/A	8.0.1.0
ASM-73029	[RHSA-2018:3249-01] Low: setup security and bug fix update	N/A	8.0.1.0
ASM-72993	[RHSA-2018:3052-01] Moderate: wget security and bug fix update	N/A	8.0.1.0
ASM-72990	[RHSA-2018:3157-01] Moderate: curl and nss-pem security and bug fix update	N/A	8.0.1.0
ASM-73054	(RHSA-2018:3140) (tcp)	N/A	8.0.1.0
ASM-73669	[RHSA-2018:3651-01] Low: kernel security and bug fix update	N/A	8.0.1.0
ASM-72794	RHBA-2018:3013 tzdata enhancement update	N/A	8.0.1.0
ASM-74160	RHSA-2019:0109 Perl Security Update	N/A	8.0.1.0
ASM-74078	[RHSA-2019:0049] Important: systemd update	N/A	8.0.1.0

Fixes in Session Manager Release 8.0.1

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-71615	Administration of button labels or related data on J100 series phones.	Some administered data was not being sent to the J100 series phones	8.0.0.0
ASM-72459	Use of SIP Entity Monitoring with reactive timer setting	Some values for the reactive timer were not accepted	8.0.0.0
ASM-70048	SIP registration from remote location	An endpoint registered to a remote location (i.e., a location different from its home location) is not notified if the administrator changes a device setting for that remote location.	7.1.3.1
ASM-66343	IPv6 route header showing up in SIP messages when IPv6 disabled	Some external SIP devices may be unable to parse the SIP message correctly, even though the V6 header can be safely ignored. This will cause SIP signaling failures.	7.1.3.1
ASM-68390	Changing the name of a Data Storage Cluster	When the name of a Data Storage cluster is changed via the System Manager GUI, the name change is not detected by Cassandra.	7.1.3.1
ASM-65199	Selection of high security settings using setSecurityPolicy command	When SM is set to operate in FIPS mode, Cassandra DB continues to operate in non-FIPS mode.	8.0.0.0
ASM-71581	[RHSA-2018:2384] Important kernel update	N/A	8.0.0.0
ASM-71580	[RHSA-2018:2349] Moderate: mariadb-libs update	N/A	8.0.0.0
ASM-70340	Postgres CVE-2018-1058 mitigation	N/A	8.0.0.0
ASM-70259	[RHSA-2018:1318-01] Important: kernel security, bug fix, and enhancement update	N/A	8.0.0.0
ASM-72789	[RHSA-2018:2942] Java Security Update	N/A	8.0.0.0
ASM-72360	[RHSA-2018:2748-01] Important: kernel security and bug fix update	N/A	8.0.0.0
ASM-72398	[RHSA-2018:2768-01] Moderate: nss security update	N/A	8.0.0.0

Fixes in Session Manager Release 8.0

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-64883	[RHSA-2017:1789-01] openjdk security update	N/A	

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-64882	[RHSA-2017:2292-01] gnutls security update	N/A	
ASM-64879	[RHSA-2017:2285-01] authconfig security update	N/A	
ASM-64881	[RHSA-2017:1916-01] glibc security update	N/A	
ASM-64158	[RHSA-2017:1481-01] glibc security update	N/A	
ASM-64157	[RHSA-2017:1680-01] bind security update	N/A	
ASM-64156	[RHSA-2017:1574-01] sudo security update	N/A	
ASM-68817	[RHSA-2018:0260-01] Moderate: systemd security update	N/A	
ASM-68814	[RHSA-2018:0158-01] Moderate: dhcp security update	N/A	
ASM-67618	[RHSA-2018:0007-01] Important: kernel security update	N/A	
ASM-67614	[RHSA-2018:0014-01] Important: linux-firmware security update	N/A	
ASM-67616	[RHSA-2018:0012-01] Important: microcode_ctl security update	N/A	
ASM-67611	[RHSA-2017:3315-01] Important: kernel security and bug fix update	N/A	
ASM-67610	[RHSA-2017:3263-01] Moderate: curl security update	N/A	
ASM-64880	[RHSA-2017:1865-01] X.org X11 libraries security update	N/A	
ASM-64878	[RHSA-2017:2192-01] mariadb security and bug fix update	N/A	
ASM-64856	[RHSA-2017:1931-01] Moderate: bash security and bug fix update	N/A	
ASM-64128	[RHSA-2017:0725-01] kernel security and bug fix update	N/A	
ASM-69446	[RHSA-2018:0395-01] Important: kernel security and bug fix update	N/A	
ASM-69933	[RHSA-2018:1191-01] Critical: java-1.8.0-openjdk security update	N/A	
ASM-64859	[RHSA-2017:1868-01] Moderate: python security and bug fix update	N/A	
ASM-64857	[RHSA-2017:1852-01] Moderate: openldap security, bug fix, and enhancement update	N/A	
ASM-64855	[RHSA-2017:1842-01] Important: kernel security, bug fix, and enhancement update	N/A	
ASM-64854	[RHSA-2017:2016-01] Moderate: curl security, bug fix, and enhancement update	N/A	

Known issues and workarounds in Session Manager 8.0.x.x

Known issues and workarounds in Session Manager Release 8.0.1.2

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

ID	Minimum conditions	Visible symptoms	Workaround

Known issues and workarounds in Session Manager Release 8.0.1.1

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

ID	Minimum conditions	Visible symptoms	Workaround
N/A	Session Managers on mixed releases (7.x and 8.x)	Endpoint device data is not shared between 7.x and 8.x realms. Changes made to an endpoint registered to an 8.x Session Manager will not be reflected on endpoints registered to a 7.x Session Manager.	Upgrade all SM nodes to 8.x
ASM-72976	Multipart SIP messages containing binary data, especially null characters (0x00, \000, ^@).	The messages get truncated at the NULL character by syslog when using traceSM.	Use SIP tracer's capability to log SIP messages directly to a file in its binary form or use tshark to capture the packets.

Known issues and workarounds in Session Manager Release 8.0.1

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

ID	Minimum conditions	Visible symptoms	Workaround
N/A	Session Managers on mixed releases (7.x and 8.x)	Endpoint device data is not shared between 7.x and 8.x realms. Changes made to an endpoint registered to an 8.x Session Manager will not be reflected on endpoints registered to a 7.x Session Manager.	Upgrade all SM nodes to 8.x
ASM-67518	Reinstallation of 8.0.1 on a system already running 8.0.1	If a Session manager running 8.0.1 is upgraded to 8.0.1 again, old Cassandra data may get restored during the upgrade.	To prevent this run the following command prior to performing the upgrade: `rm -f /var/avaya/cassandra/2.1.*/upgrade-2.1.*.zip`
ASM-72976	Multipart SIP messages containing binary data, especially null characters (0x00, \000, ^@).	The messages get truncated at the NULL character by syslog when using traceSM.	Use SIP tracer's capability to log SIP messages directly to a file in its binary

ID	Minimum conditions	Visible symptoms	Workaround
			form or use tshark to capture the packets.

Known issues and workarounds in Session Manager Release 8.0

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

ID	Minimum conditions	Visible symptoms	Workaround
ASM-70048	SIP registration from remote location	An endpoint registered to a remote location (i.e., a location different from its home location) is not notified if the administrator changes a device setting for that remote location.	Manually logout/login on the affected endpoints.
N/A	Session Managers on mixed releases (7.x and 8.0)	Endpoint device data is not shared between 7.x and 8.0 realms.	Upgrade all SM nodes to 8.0
ASM-66343	IPv6 route header showing up in SIP messages when IPv6 disabled	Some external SIP devices may be unable to parse the SIP message correctly, even though the V6 header can be safely ignored. This will cause SIP signaling failures.	Contact Support – PSN005101
ASM-68390	Changing the name of a Data Storage Cluster	When the name of a Data Storage cluster is changed via the System Manager GUI, the name change is not detected by Cassandra.	Execute a “restart mgmt.” command on the SM command line.
ASM-65199	Selection of high security settings using setSecurityPolicy command	When SM is set to operate in FIPS mode, Cassandra DB continues to operate in non-FIPS mode.	None. Will be addressed in 8.0.1.0 FP

Avaya Aura® System Manager

What's new in System Manager Release 8.0.x

What's new in System Manager Release 8.0.x

For more information see ***What's New in Avaya Aura® Release 8.0.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101050420

Security Service Pack

Beginning with 8.0.1.2, System Manger Manager is releasing an 8.0 Security Service Pack (SSP). This SSP can be applied to any version of 8.0 and only includes Red Hat security updates. Installing System Manager Security Service Pack through Software Upgrade Management(SDM) is not supported.

For further information on contents and installation procedures, please see **PCN2110S** for more details.

Installation for System Manager

Required artifacts for System Manager Release 8.0.1.2

The following section provides System Manager downloading information. For installation and upgrade procedure, see documents mentioned in Installation and Upgrade note.

Download ID	Artifact	Notes
SMGR8012GA1	Avaya Aura System Manager 8.0.1.2 Mandatory Patch bin file Post OVA deployment / Data Migration	Verify that the MD5 checksum for the downloaded file matches the number on the Avaya PLDS website. File Name: System_Manager_8.0.1.2_r801210177.bin File Size: 1663 MB MD5 Checksum: d930b1008b4e65a7796606e348adcb74
SMGR8012GA2	SDM Client for System Manager 8.0.1.2	Verify that the MD5 checksum for the downloaded file matches the number on the Avaya PLDS website. File Name: Avaya_SDMClient_win64_8.0.1.2.0033393_8.zip File Size: 210 MB MD5 Checksum: 1bc09a850660a66492cfe06cb352ce2d

Required artifacts for System Manager Release 8.0.1.1

The following section provides System Manager downloading information. For installation and upgrade procedure, see documents mentioned in Installation and Upgrade note.

Download ID	Artifact	Notes
SMGR8011GA1	Avaya Aura System Manager 8.0.1.1 Mandatory Patch bin file Post OVA deployment / Data Migration	Verify that the MD5 checksum for the downloaded file matches the number on the Avaya PLDS website. File Name: System_Manager_8.0.1.1_r801109340.bin File Size: 1643 MB MD5 Checksum: 01e472924b6ff76404c1208dad0a640e
SMGR8011GA2	SDM Client for System Manager 8.0.1.1	Verify that the MD5 checksum for the downloaded file matches the number on the Avaya PLDS website. File Name: Avaya_SDMClient_win64_8.0.1.1.0032640_15.zip File Size: 209 MB MD5 Checksum: 41cf7d0b13d5e9faadf1533773374b75

Required artifacts for System Manager Release 8.0.1

The following section provides System Manager downloading information. For installation and upgrade procedure, see documents mentioned in Installation and Upgrade note.

Download ID	**Artifact**	**Notes**
SMGR8010GA1	Avaya Aura System Manager 8.0.1 Mandatory Patch bin file Post OVA deployment / Data Migration	Verify that the MD5 checksum for the downloaded file matches the number on the Avaya PLDS website. File Name: System_Manager_8.0.1.0_r801008826.bin File Size: 1494 MB MD5 Checksum: 68e733c5c68a166afb8db92f76ffde0f
SMGR8010GA2	SDM Client for System Manager 8.0.1	Verify that the MD5 checksum for the downloaded file matches the number on the Avaya PLDS website. File Name: Avaya_SDMClient_win64_8.0.1.0.0332099_11.zip File Size: 234 MB MD5 Checksum: 33a3031477e22c9ba77f976f90e0a2a4

Required artifacts for System Manager Release 8.0

The following section provides System Manager downloading information. For installation and upgrade procedure, see documents mentioned in Installation and Upgrade note.

Download ID	**Artifact**	**Notes**
SMGR80GA001	Avaya Aura System Manager 8.0 OVA	Verify that the MD5 checksum for the downloaded file matches the number on the Avaya PLDS website. File Name: SMGR-8.0.0.0.931077-e65-19.ova File Size: 3267 MB MD5 Checksum: 03fc87d5a42007d5edffe98b0a8ac7bf
SMGR80GA002	Avaya Aura System Manager 8.0 High Capacity (Profile 3) OVA	Verify that the MD5 checksum for the downloaded file matches the number on the Avaya PLDS website. File Name: SMGR-PROFILE3-8.0.0.0.931077-e65-19.ova File Size: 3289 MB MD5 Checksum: 023461d8b5842f9062c56058659ab769
SMGR80GA013	SDM Client for System Manager 8.0	Verify that the MD5 checksum for the downloaded file matches the number on the Avaya PLDS website. File Name: Avaya_SDMClient_win64_8.0.0.0.0931322_6.zip File Size: 234 MB MD5 Checksum: 1797e24103f935ad5419821f4971e159
SMGR80GA014	System Manager 8.0 Mandatory Patch bin file Post OVA deployment / Data Migration	Verify that the MD5 checksum for the downloaded file matches the number on the Avaya PLDS website. File Name: System_Manager_R8.0_r800008090_mandatoryPatch.bin File Size: 922 MB MD5 Checksum: 03a19ed3c0c1e8ec983028fa9ba44308

Download ID	Artifact	Notes
SMGR80GA003	Avaya Aura System Manager 8.0 Amazon Web Service OVA	Verify that the MD5 checksum for the downloaded file matches the number on the Avaya PLDS website. File Name: SMGR-8.0.0.0.931077-AWS-18.ova File Size: 3283 MB MD5 Checksum: abb73e1bb3d9425354a6b491b127e616
SMGR80GA004	Avaya Aura System Manager 8.0 Amazon Web Service Profile-3 (High Capacity) OVA	Verify that the MD5 checksum for the downloaded file matches the number on the Avaya PLDS website. File Name: SMGR-PROFILE3-8.0.0.0.931077-AWS-18.ova File Size: 3296 MB MD5 Checksum: f3b14adb4164f1dc7168612272e558a0
SMGR80GA005	System Manager KVM OVA 8.0 GA OVA	Verify that the MD5 checksum for the downloaded file matches the number on the Avaya PLDS website. File Name: SMGR-8.0.0.0.931077-KVM-18.ova File Size: 3356 MB MD5 Checksum: fd624c57252d4e2c0cbc2e412897dac9
SMGR80GA006	System Manager KVM OVA 8.0 GA OVA Profile-3	Verify that the MD5 checksum for the downloaded file matches the number on the Avaya PLDS website. File Name: SMGR-PROFILE3-8.0.0.0.931077-KVM-18.ova File Size: 3358 MB MD5 Checksum: 1074c5bcf63e762dc40c999d8800fe17
SMGR80GA010	Avaya Aura System Manager 8.0 Software Only	Verify that the MD5 checksum for the downloaded file matches the number on the Avaya PLDS website. File Name: AvayaAuraSystemManager-8.0.0.0.931077_v6.iso File Size: 3067 MB MD5 Checksum: b9e41e5282842dfc7d8c09c402bd7d35

Download Data Migration Utility

This section gives the download information. For installation and upgrade procedure, see documents mentioned in the Installation and Upgrade note.

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 and 7.1.x. Ensure that you run the data migration utility only on 8.0 release. Refer to the document Upgrading Avaya Aura® System Manager to Release 8.0 for more details.

Download ID	Artifact	Notes
SMGR80GA012	Data Migration utility for System Manager 8.0	Verify that the MD5 checksum for the downloaded file matches the number on the Avaya PLDS website. File Name: datamigration-8.0.0.0.9-27.bin File Size: 533 KB MD5 Checksum: b4b530b398775054ab734fa5aab87bad

Must read:

1. New OVA files have been released SMGR 8.0 to support ACP 120 servers. The artifacts table above for System Manager 8.0 has the new file details.

2. For Release 8.0.1 GA Installation:
   - Fresh: Deploy 8.0 GA OVA + Apply 8.0.1 Feature Pack bin.
   - Upgrade: Deploy 8.0 GA OVA + 8.0 Data Migration Bin + 8.0.1 Feature Pack bin.

3. For Release 8.0 GA Installation:
   - Fresh: Deploy 8.0 GA OVA + Apply 8.0 GA Patch bin.
   - Upgrade: Deploy 8.0 GA OVA + 8.0 Data Migration Bin + 8.0 GA Patch bin.

4. 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 Log on page.
  The system displays the message: Installation of 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: System Manager Post installation configuration is In-Progress`.

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

5. Perform the following steps to enable EASG on System Manager 8.0
   - 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
     ```

6. For VMWare to VE System Manager Upgrade, remove all the snapshot from old VMWare System Manager otherwise rollback operation will fail.
7. The versions*.xml is published on PLDS. To download 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.
8. System Manager Login banner no longer supports html characters.

Software information:

Software	Version	Note
Database	Postgres 9.6	Used as a System Manager database. For more information, see: https://www.postgresql.org/docs/9.6/static/index.html
OS	RHEL 7.5 64 bit	Used as the operating system for the System Manager template
Open JDK	1.8 update 191 64 bit	For Solution Deployment Manager Client, Open JDK 1.8.0-internal

Software	Version	Note
Application Server	WildFly AS 10.1.0 Final	
Supported Browsers	Internet Explorer 11.x	Earlier versions of Internet explorer are no longer supported.
	Firefox 59, 60, 61	Earlier versions of Firefox are no longer supported.
VMware vCenter Server, vSphere Client, ESXi Host, VMware Web Client	6.0,6.5	Earlier versions of VMware are no longer supported.

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.

Troubleshooting the installation

Execute following command from System Manager Command Line Interface with customer user credentials to collect logs and contact 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 8.0.x

Fixes in System Manager 8.0.1.2

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-49100	Security Updates	(RHSA-2019:1168) Important: kernel security update	
SMGR-48476	Security Updates	(RHSA-2019:0679) Important: libssh2 security update	
SMGR-48512	Security Updates	(RHSA-2019:2019:0512) Important: kernel security, bug fix, and enhancement update	
SMGR-39711	Backup and Restore Management	After Restore earlier scheduled backup job is getting disabled	
SMGR-49607	Infrastructure	Database vacuum cron job does not work properly	
SMGR-49359	Infrastructure	Log roration for jboss_service_affects.log is missing.	
SMGR-47572	Infrastructure	Full vacuum reindex cron job does not work properly.	
SMGR-49029	Infrastructure	HttpThread Usage Monitor is not calculating the http thread percentage properly causing unnecessary Alarms being generated.	
SMGR-46344	Infrastructure	If CM also sends notification to secondary server when it is configured on CM syslog configuration file, then sometimes connection on CM goes into a bad state causing the syslog to stop working.	
SMGR-47633	Infrastructure	Log rotation for /var/log/Avaya/mgmt/geo/csync2.log is missing,	
SMGR-48106	Infrastructure	'powerOffVM' and 'rebootVM' commands using customer account does not work on fresh install of System Manager 8.0.1	
SMGR-49130	Infrastructure	Alias 'changePublicIPFQDN' command is not working	
SMGR-49317	Infrastructure	Alias 'status_vm' missing.	
SMGR-48565	Infrastructure	Cannot install System Manager 8.0.1.1 patch on System Manager 8.0.1.0 due to space issue.	
SMGR-48759	Infrastructure	8.0.1 installation stuck and hung while executing Global search component initialization.	
SMGR-49021	Infrastructure	Full path disclosure vulnerability associated with search config component.	
SMGR-48663	Infrastructure	Thread leak in Trust Management Component causing System Manager Crash.	

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-48334	Infrastructure	Metaspace running out of memory related to backward compatibility code.	
SMGR-49775	Infrastructure	/var/log/Avaya/postgres/postgres.log file not rotating and filling up disk space.	
SMGR-43554	Inventory Management	Unable to delete messaging element entry from manage elements page.	
SMGR-46682	Inventory Management	Blank page opens when user click on Create Profiles and Discover SRS/SCS link.	
SMGR-48161	Inventory Management	When a CM is deleted from System Manager UI, it does not log IP address of client machine from where System Manager UI is accessed.	
SMGR-47326	Inventory Management	Warning symbol and tool tip being displayed without any text associated with the Warning at Inventory.	
SMGR-48218	Inventory Management	Clicking on Certificate renewal Button does not redirect proper page.	
SMGR-44450	Geo Redundancy Management	GEO reconfiguration fails during Clean Up phase if Discovery Profile has entries associated with System Manager Element Type	
SMGR-49205	Geo Redundancy Management	Geo Redundancy backup files are stored in world readable folders.	
SMGR-49624	Global Search Component	Group membership data is not populated properly in Global search if multiple endpoints are viewed/edited one after another.	
SMGR-49149	Global Search Component	Global search for custom user doesn't work	
SMGR-49195	Global Search Component	Global Search with Russian Language doesn't work as expected	
SMGR-49316	Global Search Component	Global search feature does not show group membership records.	
SMGR-49072	Scheduler Management	“End by Date” field is missing from job schedule page.	
SMGR-46641	Scheduler Management	Due to the failure of CRLExpirationCheckerJob job, alarm gets generated.	
SMGR-49722	Role Management	User associated with custom role having permissions over group, gets blank page when user clicks on session manager dashboard or user registrations page.	
SMGR-49136	User Management	Not able to edit a user if "Other XMPP" type communication address is added to user.	
SMGR-48138	User Management	Self-provisioning to reset password sometime adds space (" ") in automatically generated password.	
SMGR-48345	User Management	No proper Error code occurs when webservice is used for user creation when it is not administered in CM dialplan.	

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-49626	Officelinx Element Manager	Cannot create Officelinx user using User Provisioning Rule in case "Application User Password" field set to "Use Mailbox" or "Reverse Mailbox".	
SMGR-49272	Communication Manager Management	Communication Manager communication profile cannot be unassigned from user if CM extension is part of coverage answer group.	
SMGR-49016	Communication Manager Management	Communication Manager Endpoint delete fails with foreign key constraint error on table "ipt_abbrdial_pers".	
SMGR-48810	Communication Manager Management	Unable to edit ARS digit conversion for specific entries from via "cut through" OR "ARS Digit Conversion" page.	
SMGR-48849	Communication Manager Management	Bulk Delete Endpoint doesn't throw validation error for wrong formatted Extensions.	
SMGR-48886	Communication Manager Management	Allow H.323 and SIP Endpoint Dual Registration" is not grayed out in CM endpoint profile for SIP endpoint templates.	
SMGR-49053	Communication Manager Management	Downloading the Excel template from the manage endpoints page and using it to delete stations does not work.	
SMGR-48695	Communication Manager Management	Coverage path is removed from existing station on CM when same extension is used while adding "CM endpoint profile".	
SMGR-48634	Communication Manager Management	Cannot modify an abbreviated dialing enhanced object on second (or next) page.	
SMGR-48717	Communication Manager Management	Coverage path is set to blank even if it is configured in UPR with custom template.	
SMGR-49242	Communication Manager Management	“Export All Endpoints” causes system to go out of memory.	
SMGR-48587	Communication Manager Management	If UPR uses a template has Voicemail Number entry set, user creation fails.	
SMGR-48574	Communication Manager Management	Selected endpoint records, do not clear after page reloads or when moved across table pages if the records are more than 15.	
SMGR-48549	Communication Manager Management	In System Manager 8.0.1, Cannot edit a user with communication manager profile from user management to change user’s first name, last name and login name.	
SMGR-48142	Communication Manager Management	Advanced search option from Communication Manager Manage endpoints page does not work after upgrade to 8.0.1.0	
SMGR-48453	Communication Manager Management	Blank page when user tries to EDIT / VIEW coverage path.	
SMGR-48294	Communication Manager Management	Edit VDN operation by custom user (with extension range) fails if VOA extension contains hyphen('-'), dot('.') OR space (' ').	

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-48293	Communication Manager Management	Few specific feature-access-codes are not listed in the System Manager	
SMGR-49257	Communication Manager Management	Cannot add more ip-network-map entries if ip-network-map already has >=500 entries.	
SMGR-49115	Communication Manager Management	Coverage time-of-day shows wrong values	
SMGR-48559	Communication Manager Management	"Bulk Delete Endpoint Confirmation" page shows duplicate buttons "Now", "Schedule", "Cancel".	
SMGR-48607	Communication Manager Management	Preferred Handle field is not getting updated to communication manager endpoint.	
SMGR-48140	Communication Manager Management	XML Parsing Error After Clicking on Create New Button on Coverage Path Page.	
SMGR-48610	Communication Manager Management	Usage of cssecurestore filling up the cssecurestore table to the extent that it causes Geo Redundancy workflow to fail.	
SMGR-49024	Communication Manager Management	Extension cannot be added to CAG from User management -> CM endpoint comm profile -> endpoint editor -> group membership tab	
SMGR-49421	Communication Manager Management	Not able to roll back station on CM if user creation fails on System Manager due to error noticed while creating other profiles.	
SMGR-49113	Report Management	Report generation fails for custom role when report (such as display/status) which requires Qualifier Value.	
SMGR-49154	Report Management	“list registered-ip-stations” and “list usage hunt-group” created by custom account does not populate data.	
SMGR-48545	Report Management	When multiple reports are run concurrently, some of the runs produce zero size (empty) reports.	
SMGR-48544	Report Management	Incorrect report is generated when pagination/order settings are changed.	
SMGR-48541	Report Management	Setdata report taken in SMGR has incorrect column alignments.	
SMGR-48490	Report Management	Custom user cannot generate report when he has multiple ranges defined under endpoint, VDN, Vector etc.	
SMGR-48484	Report Management	Display vector report generation fails for PDF format.	
SMGR-48439	Report Management	list registered-ip-stations report shows displays incorrect data under columns.	
SMGR-48340	Report Management	Custom user cannot generate report when he has multiple ranges defined under endpoint, VDN, Vector etc.	
SMGR-48260	Report Management	"Creation Time" does not show date and time in AM/PM in report generation and history pages.	

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-48538	Report Management	Report generation in pdf format fails for forms containing "&".	
SMGR-48317	Software Upgrade Management	User unable to remove the Upgrade Job Status of type Commit_Rollback.	
SMGR-48820	Software Upgrade Management	If Upgrade management jobs like analyze, pre-upgrade check are deleted from scheduler page, it does not clean the respective entries from Software Upgrade Management tables.	
SMGR-48863	Software Upgrade Management	AVP custom patches should not be displayed in download management as its not supported.	
SMGR-48728	Software Upgrade Management	Refresh Element job does not finish when elements of different types are selected.	
SMGR-48547	Software Upgrade Management	Upgrade of Media module of Media Gateway gets stuck in the pending state	
SMGR-48426	Software Upgrade Management	After clicking "Migrate with AVP install" checkbox new tab is not displayed while migrating from SP to AVP.	
SMGR-48228	Software Upgrade Management	Refresh Families and analyze fails as invalid company ID for freshly deployed System Manager.	
SMGR-48147	Software VM Management	Refresh Host gets stuck after changing host password through Software Upgrade Management.	
SMGR-49253	Software Upgrade Management	Gateway discovery does not work with SNMPv3 configurations.	
SMGR-48068	SDM Client	Unable to use SDM Client for upgrading vCenter based System Manager.	

Fixes in System Manager 8.0.1.1

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-48005	Security Updates	systemd (RHSA-2019:0201)	
SMGR-48001	Security Updates	kernel (RHSA-2019:0163)	
SMGR-48007	Security Updates	ruby (RHSA-2018:3738)	
SMGR-48008	Security Updates	bind (RHSA-2019:0194)	
SMGR-48002	Security Updates	perl (RHSA-2019:0109)	
SMGR-48004	Security Updates	systemd (RHSA-2019:0204)	
SMGR-48003	Security Updates	NetworkManager (RHSA-2018:3665)	
SMGR-48006	Security Updates	curl and nss-pem (RHSA-2018:3157)	
SMGR-48009	Security Updates	polkit (RHSA-2019:0230)	
SMGR-47545	Security Updates	(RHSA-2018:3651) Moderate: kernel security, bug fix, and enhancement update	

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-47418	Security Updates	(RHSA-2018:3059) Low: X.org X11 security, bug fix, and enhancement update	
SMGR-47871	Infrastructure	Import of Device Adapter Media Gateway xml file hangs	
SMGR-46433	Infrastructure	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 rows.	
SMGR-47938	Infrastructure	IP/FQDN change on System Manager causes issue while managing existing CMs.	
SMGR-47745	Backup and Restore Management	“XML Parsing Error” page appear when using remote restore SFTP	
SMGR-47750	Certificate Management	UI (page) gets stuck once certificate export is done.	
SMGR-47893	Certificate Management	Unable to replace/renew certs when Sub CA is configured.	
SMGR-48080	Shutdown Management	Shutdown System Manager functionality for working properly – some notifications missing, history is incorrect	
SMGR-46642	Scheduler Management	UserMgmtJob job execution is getting failed resulting in an alarm getting triggered.	
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-47921	License Management	Provide script (configureTLS) to disable TLS 1.0 for WebLM port 52233	
SMGR-45884	Directory Synchronization	If the same attribute from AD is mapped to login name and otherEmail and value of the attribute is in mixed case or upper case, then after each sync user shows as Modified after sync.	
SMGR-41634	Self-Provisioning	Self-provisioning does not work after providing windows user id if external authentication is configured.	
SMGR-45431	Communication Manager Management	number for autodial button does not get saved after commit.	
SMGR-47743	Communication Manager Management	Backup All Announcement job shows success even though it is unable to download all announcement file.	
SMGR-47133	Communication Manager Management	Filter enabled by one user is not cleared on Manage Endpoint page for another user once logged in.	
SMGR-47472	Communication Manager Management	IPTCM maintenance Job doesn’t cleanup ipt_cluster_sm_data_mem table.	
SMGR-47467	Communication Manager Management	Blank page will be displayed on Download announcement pages.	

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-47867	Communication Manager Management	CM IP gets interchanged on System Manager -> Communication Manager pages causing interchanged CM to disappear for user associated with custom role.	
SMGR-47826	Communication Manager Management	Cannot update preferred handle of CM communication profile using bulk edit option.	
SMGR-46901	Communication Manager Management	Click on View/Edit button for user management takes 2 to 3 minutes load to page if User has CM profile.	
SMGR-47840	Communication Manager Management	ip-network-map data is missing after sync between 8.0 CM and 8.0 System Manager.	
SMGR-47490	Communication Manager Management	Announcement backup fails to get audio files when local scp server is selected.	
SMGR-47168	Communication Manager Management	Custom user (any user other than admin user) cannot delete announcement backup manually	
SMGR-47986	Communication Manager Management	Edit endpoint operation is removing it from all groups like hunt, CAG, pickup group etc.	
SMGR-48015	Communication Manager Management	“Global Endpoint Change” deletes station Name when “Endpoint Display Name:” contains “~” character.	
SMGR-47848	Communication Manager Management	Using User Management edit option Coverage Path field is not getting set to blank once it assigned to a value.	
SMGR-46856	Communication Manager Management	Missing data module feature when custom template is chosen via User Management	
SMGR-47453	Communication Manager Management	XML Parsing Error when using “Bulk Add Agents” and “Bulk Delete Agents” options	
SMGR-47434	Communication Manager Management	Go to Communication Manager -> Call Center -> Agent page. Select any Agent and click View OR Edit. Page still shows General Options tab instead of Agent Skill tab.	
SMGR-48000	Communication Manager Management	Multiple issues when “data module” is enabled on WCBRI station.	
SMGR-47805	Communication Manager Management	Edit, View and Delete buttons are disabled on agent page “2”.	
SMGR-46896	Communication Manager Management	Preferred Handle attribute to “None” when name changes for user is performed.	
SMGR-47885	Communication Manager Management	Cannot configure Half/Full Screen Mode anymore on System Manager 8.0.1.0.	
SMGR-47751	Communication Manager Management	Extension lookup very slow on VND and hunt group pages causing system slowness.	
SMGR-47640	Remote Management	“REPORTS_CleanUp_System_Job” execution is failing.	

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-47887	Remote Management	User cannot configure Task Time, Recurrence and Range values if he wants to schedule report generation job later	
SMGR-48033	Remote Management	list extension-type report puts COR and COS field values in wrong place in report data.	
SMGR-47849	Remote Management	“list monitored-station” report generation is failing	
SMGR-46783	Remote Management	“list measurements ip dsp-resource” report doesn’t match column headings and values	
SMGR-46873	Remote Management	Issues with report definition when CM IP is changed in inventory	
SMGR-47538	Remote Management	Scheduling two report jobs for two different CMs for same time, one completes successfully but other creates empty file.	
SMGR-46818	Software Upgrade Management	System Platform upgrade using System Manager fails while trying to clean the previous backup from System Platform	
SMGR-47833	Software Upgrade Management	unable to discovery TN Boards when a CM is added / updated.	
SMGR-46742	Software Upgrade Management	Cannot upload file with .fdl extension to software library using My Computer option.	
SMGR-47714	SDM Client	SDM Client installer Windows Server 2016 (x64) support	

Fixes in System Manager 8.0.1

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release introduced
Various		Fixes for following RHEL security advisories: RHSA-2018:1629, RHSA-2018:1649, RHSA-2018:1700, RHSA-2018:1852, RHSA-2018:1957, RHSA-2018:1965, RHSA-2018:2123, RHSA-2018:2181, RHSA-2018:2242, RHSA-2018:2384, RHSA-2018:2439, RHSA-2018:2570, RHSA-2018:2748, RHSA-2018:2768, RHSA-2018:2942, RHSA-2018:3032, RHSA-2018:3041, RHSA-2018:3050, RHSA-2018:3052, RHSA-2018:3059, RHSA-2018:3071, RHSA-2018:3083, RHSA-2018:3092, RHSA-2018:3107, RHSA-2018:3140, RHSA-2018:3158, RHSA-2018:3221, RHSA-2018:3249, RHSA-2018:3324, RHSA-2018:3327, RHSA-2018:3408, RHSA-2018:3459	
SMGR-46404	Infrastructure	tzdata Linux RPM updated to tzdata-2018e	
SMGR-45959	Software Upgrade Management	SDM support for G430/G450 Gateway upgrades to release 38.21.x and above	
SMGR-46681	Alarm Management	Alarm Management settings configuration missing in online help	

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-46178	Alarm Management	Alarms not cleared when received in quick succession	
SMGR-47314	Backup and Restore	Inadequate validation during restore to check system FQDN value vs value in backup.info file	
SMGR-47304	Certificate Management	Unable to revoke certificates in 7.1.x (and 7.0.x) if the certificates were issues when you were on release 6.x	
SMGR-46746	Communication Manager Management	Cannot save valid values for 17-23 positions of Button Module for sets M3904/M3905/M2616	
SMGR-47357	Communication Manager Management	Announcement Management functionality not working correctly in R8.0	
SMGR-47307	Communication Manager Management	Hunt group addition fails if the user's role has all Communication Manager permissions and it also has defined ranges for Endpoint and hunt extensions	
SMGR-47207	Communication Manager Management	After selecting VDN record buttons(view/edit/delete) are not getting enabled	
SMGR-47052	Communication Manager Management	Backup All Announcement job shows success even though it is unable to download all announcement file	
SMGR-47041	Communication Manager Management	Import/Export feature on VDN form is not working for custom users	
SMGR-46741	Communication Manager Management	Announcement transfer to Avaya Media Server fails with error "jmx/invoker/RMIAdaptor is not bound in this server".	
SMGR-46738	Communication Manager Management	User cannot add Extension to Coverage Answer Group while editing user through Manage Endpoints if it contains 8 OR more members already	
SMGR-46736	Communication Manager Management	Custom users cannot utilize the Import/Export feature on Hunt group form	
SMGR-46723	Communication Manager Management	Custom users cannot use the Import/Export feature on VDN form	
SMGR-46604	Communication Manager Management	Broadcast announcement throws error "Special Character Not Allowed in Audio File"	
SMGR-46593	Communication Manager Management	Unable to configure COR value higher than 250 for Communication Manager 5.2.1 using System Manager Endpoint Editor	
SMGR-46357	Communication Manager Management	Using IE browser, changes are not getting committed after EDIT/ADD hunt group from Home / Elements / Communication Manager / Groups / Hunt Group	
SMGR-46056	Communication Manager Management	Audit report shows discrepancy when location.locationidex=null on Communication Manager and location.locationidex=0 on System Manager	

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-46047	Communication Manager Management	Uploading announcements via System Manager using special character in filename / announcement name introduces inconsistencies and issues between Communication Manager and Avaya Media Server	
SMGR-46041	Communication Manager Management	Notify Sync is not working for change agent-ID with auto option.	
SMGR-46050	Communication Manager Management	Uploading announcements via System Manager using special character in filename / announcement name introduces inconsistencies and issues between Communication Manager and Avaya Media Server.	
SMGR-45355	Communication Manager Management	Cluster ID in signaling group is not displayed in Signaling Group List form on SMGR	
SMGR-47310	Communication Manager Management	When all Remove Options are selected in Usage Options, sometimes when station gets deleted from User Management or Manage Endpoints, the delete station job gets stuck in running state	
SMGR-47134	Communication Manager Management	Error occurs when user provides Number Range for custom role in range field text boxes on screens in Vector, Coverage Answer Group, Coverage Path, Pickup Group.	
SMGR-46214	Communication Manager Management	User creation is failing because of incorrect handling of second features field for CS1000 Endpoints	
SMGR-47188	Communication Manager Management	In User Profile-Add, after selecting template “Cs1k-39xx_DEFAULT_CM_8_0” the phone Subtypes do not get populated in the drop-down field.	
SMGR-46467	Directory Synchronization	Directory synchronization fails to add new user when we have a mapping for "Microsoft Exchange Handle" along with a mapping for "email"	
SMGR-46724	Geographic Redundancy	Unable to manage Secondary System Manager's Identity or Trusted certificate from Primary System Manager in R8.0	
SMGR-46671	Geographic Redundancy	When Secondary System Manager is made Active, it does not send notifications to Elements that are managed	
SMGR-47091	Infrastructure	Security Issue - /tmp folder does not have the sticky bit set in 7.1.x and 8.0.x	
SMGR-46853	Infrastructure	SMGR (military mode) is not able to establish “trust” with the servers deployed in the environment	
SMGR-46808	Infrastructure	NTP Daemon fails to start after SMGR reboot	
SMGR-46651	Infrastructure	changeIPFQDN not working correctly for -dns option	
SMGR-46553	Infrastructure	editHosts command doesn't allow first character as digit in the FQDN	

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-46857	Infrastructure	Extended Hostname Validation implementation needs to be corrected because Java now enables Endpoint identification by default on LDAPS connections	
SMGR-47455	Infrastructure	Cross site scripting vulnerability	
SMGR-46943	Infrastructure	Logging in with EASG on the System Manager website enables FIPS mode at the JVM level which caused Pre-upgrade check in SDM to fail	
SMGR-46431	Infrastructure	Unable to change password from password change page if user id has space at beginning or end	
SMGR-46337	Infrastructure	Database transactions are getting stuck in some scenarios	
SMGR-43652	Infrastructure	Non-supported characters need to be removed from default login banner text	
SMGR-46341	Inventory Management	After upgrading System Manager 7.1.3 GA to 7.1.3.1, Communication Manager Entitled Upgrade version in Upgrade Management shows N/A even - though the user is entitled for a valid Communication Manager version.	
SMGR-46304	Inventory Management	Device type entries are missing in the System Manager 7.1 upgraded from release 6.3.4	
SMGR-46271	Inventory Management	Alternate IP address is not updating if discovery failed during editing Communication Manager duplex entry in inventory.	
SMGR-46220	Inventory Management	SDM shows incorrect Entitled Update Version.	
SMGR-46046	Inventory Management	Clear text password in inventory logs	
SMGR-46386	Office Linx Management	Certain types of data are not getting refreshed from Office Linx to System Manager	
SMGR-46189	Office Linx Management	Creation of Officelinx Messaging & Collab users fails in SMGR 8.0	
SMGR-46517	Report Management	Unable to delete reports by user associated custom role	
SMGR-46002	Report Management	In detailed report when all fields are selected report runs as empty for VDN.	
SMGR-45886	Report Management	Report for “Display error” for Communication Manager is blank	
SMGR-45808	Report Management	For detailed VDN report, Name and Destination number fields do not show proper data.	
SMGR-45766	Role Management	Unable to store value in range field if custom role is created under communication manager admin.	
SMGR-46631	Software Upgrade Management	Pre-Upgrade Task is disabled for certain upgrade scenarios	

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-46191	Software Upgrade Management	Administrator can schedule the Pre- upgrade Job for Media Gateway, Media Modules and TN Boards even if is not applicable for them.	
SMGR-46151	Software Upgrade Management	SDM support for G430/G450 Gateway upgrades to release 38.21.x and above	
SMGR-39714	Software Upgrade Management	SDM upgrade job status not displayed correctly in certain scenarios	
SMGR-46506	Software Upgrade Management	VM management page refresh causes de-selecting of the VM while doing Re-establish Connection	
SMGR-46033	Software Upgrade Management	Clear text password in upgrade logs.	
SMGR-46620	Software Upgrade Management	Analyze and Refresh Families activities not working due to change in PLDS certificate.	
SMGR-46797	Software Upgrade Management	Gateway Discovery using discovery profile doesn't work for G430 version 39.12.0	
SMGR-46282	Software Upgrade Management	After performing refresh elements & analyze operation on CM 7.0 entry, SDM shows un-entitled symbol even if customer is entitled for CM 7.1 and Update/Upgrade option is disabled.	
SMGR-31891	Software Upgrade Management	Files get deleted from Software Library automatically due to schedule job for cleanup being enabled by default	
SMGR-46664	Solution Deployment Manager	Inadequate validation of DNS field causes failure in deploying SMGR using SDM client fails if you enter "0.0.0.0" in the field	
SMGR-46693	Solution Deployment Manager	Misleading error / log message when downloading files using the download manager	
SMGR-46668	Solution Deployment Manager	Incorrect tool tip mentioned in AVP Bulk import spread sheet for System Platform IP Address	
SMGR-46769	Solution Deployment Manager	If we select multiple hosts and perform Set Login Banner operation, it works only for one host and for other hosts it gets stuck	
SMGR-44958	Solution Deployment Manager	Unable to unmanage vCenter mapped hosts from VM Management	
SMGR-46564	Trust Management	Key change functionality not regenerating one file	
SMGR-46697	User Management	First Name column displayed incorrectly when adding contact from user management	
SMGR-46843	User Management	Bulk Import/Export JobType is not unique and adds a new jobtype with every new import/export job	
SMGR-46647	User Management	Unable to delete user export job from export list if its already deleted from scheduler	

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-45301	User Management	Export of User data fails if user has SIP and CM profiles that have set their font(text) size on phone to Large	
SMGR-45911	User Management	Null Exception on UI when user check the Dual Registration box for H.323 user on CM profile section	
SMGR-46557	User Management	Range field is missing from UI while configuring Communications Manager permissions for a role	
SMGR-47324	User Management	User view/edit gets stuck in 'Loading' after SMGR upgrade from 7.1.3 GA to 8.0 GA	
SMGR-47202	User Management	Error is displayed during creation of User with Messaging profile using User Provisioning Rule in certain scenarios	
SMGR-47147	User Management	SMGR does not validate Avaya Aura Messaging password rules in End User Self provisioning	
SMGR-46638	User Management	UI loading indicator needs to be shown till user list gets populated in the User Management page	
SMGR-46632	User Management	Editing a User causes error messages to be shown	
SMGR-46614	User Management	cannot change the domain of e164 handle using bulk edit operation	
SMGR-46609	User Management	Option " Auto Generate Communication Profile Password" selection does not update existing communication password for users using bulk edit user operation.	
SMGR-46595	User Management	Generate button for creating Communication Profile password is missing	
SMGR-46510	User Management	Edit functionality of Communication Profiles not working in certain scenarios	
SMGR-46503	User Management	Switching off and back on the Communication Profile renders the UI for new Profile instead of showing earlier settings	
SMGR-46418	User Management	Advanced Search fails when using the default "Equals" option on Manage Users screen	
SMGR-46026	User Management	Error “Invalid Email Address” if email address domain part contains digit for user.	
SMGR-45929	User Management	System does not send mail for user's communication password change in some scenarios.	

Fixes in System Manager 8.0

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-44959	Infrastructure	SMGR 8.0 includes the Red Hat updates to support mitigation of the Meltdown/Spectre vulnerabilities. However, this has the potential to affect performance – so there is now a small script that allows the setting of kernel options to control how these vulnerabilities are handled. The effect of running the kernel configuration script is both immediate and will persist across reboots. The script should be called from the CLI using the admin user and is called kernel_opts.sh. It has the argument “status” to display the current status of the kernel options, “enable” to enable all flags to provide maximum protection, and “disable” to disable all flags to provide maximum performance.	
SMGR-43351	Infrastructure	Creating new CA from UI restricted to 3 years validity instead of 10 years	
SMGR-44288	Infrastructure	SMGR Web UI is not available after SMGR powered down for over 7 days	
SMGR-43139	Infrastructure	Application server HTTP Header reveals software version details	
SMGR-44678	Infrastructure	Memory leak issue in OpenJDK 8u144 causes JBoss application server to terminate	
SMGR-43579	Infrastructure	"changeVFQDN" does not update /etc/hosts file with new VFQDN value, which further causes issue with GEO configuration or Data Replication Issue.	
SMGR-41117	Infrastructure	Invalid alarm “Default ASG Auth file found on System Manager alarm” getting generated	7.1.0.0
SMGR-44337	Infrastructure	SMGR goes into unusable state after upgrade to SMGR 7.1.2 due to /tmp partition getting full	
SMGR-43331	Communication Manager Management	Announcement files are not getting pushed by SCP to CF enabled gateway	
SMGR-44448	Communication Manager Management	Add/Edit agent is not allowed if "Business Advocate" field is disabled even though it is not always required	
SMGR-43527	Communication Manager Management	Communication Manager details not getting removed completely on deleting from Inventory if that Communication Manager had notification sync enabled and it is unreachable during removal	
SMGR-43074	Communication Manager Management	Communication Manager initial synchronization is failing at hunt-group with error "EJB_EXCEPTION : Removing a detached instance"	
SMGR-44869	Communication Manager Management	Communication Manager initial synchronization is fails at "service-hours-table". Also "change service-hours-table" command from element cut-through does not work.	

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-43827	Communication Manager Management	The existing EC500 entries in off-pbx-telephone station are getting deleted on Communication Manager when adding a check mark to “Allow H.323 and SIP Endpoint Dual Registration” on an existing users' CM Endpoint Profile	
SMGR-43744	Communication Manager Management	Re-Calculate route pattern fails if there are large number of users	
SMGR-43743	Communication Manager Management	Error thrown when user provides values in Range for custom role	
SMGR-43189	Communication Manager Management	Detailed Reports page not working in CM Element Manager	
SMGR-44522	Communication Manager Management	Detailed Reports not getting generated properly	
SMGR-43745	Communication Manager Management	Editing of existing report does not work properly	
SMGR-44377	Communication Manager Management	SMGR going "out of memory" due to memory leak in Reports Output Panel	
SMGR-44170	Solution Deployment Manager	Unable to add / discover hosts under VM Management using vCenter if the hosts have a lot of datastores configured	
SMGR-44588	Solution Deployment Manager	Refresh Element fails for Duplex ESS Communication Manager with encryption enabled. This is blocking upgrade.	
SMGR-41580	User Management	Subject Common Name -CN" gets removed if other options from left panel are selected on Provision User Certificate Authentication page.	
SMGR-41841	User Management	Error thrown while adding Administrative user having a comma character in Full Name	
SMGR-43081	User Management	admin user loses System Administrator role while doing certain operations	
SMGR-41621	End User Self Provisioning	After Certificate based authentication fails for End User Self Provisioning, the fall back option for authentication does not work with normal login credentials	
SMGR-43352	User Management	Change Presence/IM Domain using "Bulk Edit Users" does not update xmpp handle in other users which are Associated contacts	
SMGR-38071	User Management	Translation is not happening correctly for First and last name having Umlaut characters(ä,ö,ü,ß)	
SMGR-44774	License Management	SMGR still shows no license installed after installing license file having certain values	

Known issues and workarounds in System Manager in Release 8.0.x

Known issues and workarounds in System Manager in Release 8.0.1.2

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

ID	Minimum conditions	Visible symptoms	Workaround
	IP Office	System Manager 8.0.1 (or 8.0) does not support IP Office.	
SMGR-43249	Infrastructure	When System Manager is being accessed using FQDN using certificate-based authentication, then time zone is not displaying according client browser time zone	
SMGR-40715	Infrastructure	SSL handshake fails on JMX port connection if revocation checking set to OCSP	
SMGR-47391	Routing Management	Adaptation filter option is not working properly after removal of few entries from the data received in matched pattern	
SMGR-46363	Certificate Management	Trying to replace a PEM certificate with a third-party CA issued certificate which is signed using Elliptical Curve signing algorithm results in the certificate to get corrupted and removed from the Manager Identity certificate UI	
SMGR-49488	Global Search Component	Global search shows less results than filtered table search in some scenarios.	
SMGR-46088	Geographic Redundancy	Cannot login to Secondary System Manager UI using EASG after Secondary System Manager is activated	
SMGR-44830	Geographic Redundancy	Geographic Redundancy configuration will fail if we set option Maximum Sessions Per User: 1 on the Primary Server	
SMGR-49264	Geographic Redundancy	GEO configuration fails if port 8193 is blocked between both System Manager servers	Refer PSN005273u for more details.
SMGR-45913	User Administration	User gets system error while updating existing role having permissions for group once group is renamed.	
SMGR-46415	License Management	If System Manager with centralized license is upgraded from 7.0.x to 7.1.x using SDM client, it allows installation of new centralized license with same Centralized Licensing ID.	
SMGR-45856	User Management	Latin transcription of “First Name” and “Last Name" in the Identity Tab of User in System Manager are not happening properly for Russian name with the Cyrillic alphabet	
SMGR-39756	User Management	Edit button on User view page should be disabled if User does not have permission for User edit	
SMGR-48028	User Management	Error while deleting contact from endpoint when Session Manager is 7.0.1.2 and System Manager is 8.0.1	
SMGR-48621	User Management	AD sync OR user creation fails if endpoint template having favorite checkbox enabled for autodial button without Dial Number.	
SMGR-48181	User Management	While create/edit of user or role gets error "Invalid request received. Please contact your system	Remove space at beginning or end.

ID	Minimum conditions	Visible symptoms	Workaround
		administrator" if a field value has space at beginning or end.	
SMGR-48555	Communication Manager Management	In exported list of users, ‘Attendant’ header missing in CM Endpoint Profile.	
SMGR-43445	Communication Manager Management	Shortcut keys indicated on Management Endpoints UI are not working	
SMGR-49635	Communication Manager Management	Preferred Handle field cannot be added/removed while Edit operation.	
SMGR-49611	Communication Manager Management	Cannot permanently delete user if it's associated with CM extension which is part of pickup group	Remove extension from pickup group manually before deleting the user.
SMGR-48200	Backup and Restore Management	Unable to take remote backup on HDI (Hitachi Data Ingestor) Linux appliance remote server.	
SMGR-47622	Role Management	Customer users able to see other CMs even if they don't have permission. User can see CMs but cannot manage them as expected.	
SMGR-49620	Role Management	Unable to parse comma (“ , “) in role description field, While creating new or updating the role	Do not use comma (“ , “) in role description field, While creating new or updating the role.
SMGR-46905	Solution Deployment Manager	Trust establishment fails if VM is associated with multiple datastores resulting from migration of VM to another datastore and if snapshot is present on old datastore	
SMGR-48086	Solution Deployment Upgrade Management	Issue with downloading g450 fdl file using My Computer option.	

Known issues and workarounds in System Manager in Release 8.0.1.1

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

ID	Minimum conditions	Visible symptoms	Workaround
	IP Office	System Manager 8.0.1 (or 8.0) does not support IP Office.	Do not upgrade to System Manager 8.0.1 if IP Office elements are being managed. System Manager 7.1.3 has support for IP Office 11.
SMGR-43249	Infrastructure	When System Manager is being accessed using FQDN using certificate-based authentication, then	Login to System Manager using IP Address

ID	Minimum conditions	Visible symptoms	Workaround
		time zone is not displaying according client browser time zone	
SMGR-47572	Infrastructure	Database vacuum jobs are working as expected.	
SMGR-40715	Infrastructure	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).
SMGR-47391	Routing Management	Adaptation filter option is not working properly after removal of few entries from the data received in matched pattern	Refresh the table data using Refresh icon.
SMGR-46641	Scheduler Management	CRLExpirationCheckerJob job execution is failing	None
SMGR-39711	Backup and Restore	After Restore operation earlier scheduled and executed daily Backup job is getting disabled	Enable job again.
SMGR-46363	Certificate Management	Trying to replace a PEM certificate with a third-party CA issued certificate which is signed using Elliptical Curve signing algorithm results in the certificate to get corrupted and removed from the Manager Identity certificate UI	None
SMGR-46088	Geographic Redundancy	Cannot login to Secondary System Manager UI using EASG after Secondary System Manager is activated	None
SMGR-44830	Geographic Redundancy	Geographic Redundancy configuration will fail if we set option Maximum Sessions Per User: 1 on the Primary Server	Set option Maximum Sessions Per User: 5 on the Primary Server
SMGR-47633	Geographic Redundancy	No log rotates for /var/log/Avaya/mgmt/geo/csync2.log	
SMGR-45913	User Administration	User gets system error while updating existing role having permissions for group once group is renamed	Remove permissions referencing old group name and add again the permissions for new group name.
SMGR-45856	User Management	Latin transcription of “First Name” and “Last Name" in the Identity Tab of User in System Manager are not happening properly for Russian name with the Cyrillic alphabet	None
SMGR-39756	User Management	Edit button on User view page should be disabled if User does not have permission for User edit	None
SMGR-48028	User Management	Error while deleting contact from endpoint when Session Manager is 7.0.1.2 and System Manager is 8.0.1	
SMGR-43445	Communication Manager Management	Shortcut keys indicated on Management Endpoints UI are not working	Use mouse-based navigation

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-47952	Communication Manager Management	Export All Endpoints causes system to go out of memory	Export endpoints with range 100 to 500.
SMGR-47622	Role Management	Customer users able to see other CMs even if they don't have permission. User can see CMs but cannot manage them as expected.	
SMGR-46905	Solution Deployment Manager	Trust establishment fails if VM is associated with multiple datastores resulting from migration of VM to another datastore and if snapshot is present on old datastore	Delete existing snapshots for the VM
SMGR-47708	Software Upgrade Management	If Upgrade management jobs like analyze, pre-upgrade check are deleted from scheduler page, it does not clean the respective entries from Software Upgrade Management tables.	

Known issues and workarounds in System Manager in Release 8.0.1

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

ID	Minimum conditions	Visible symptoms	Workaround
	IP Office	System Manager 8.0.1 (or 8.0) does not support IP Office.	Do not upgrade to System Manager 8.0.1 if IP Office elements are being managed. System Manager 7.1.3 has support for IP Office 11.
SMGR-47467	Communication Manager Management	Announcement page Download option shows a blank page if you navigate away and come back.	Logout from System Manager and login again and navigate to the Announcement page.
SMGR-47453	User Management	XML Parsing Error when using "Bulk Add Agents" and "Bulk Delete Agents" options	None
SMGR-47434	Communication Manager Management	Clicking on Agent Skill tab does not switch to Agent Skill page	None
SMGR-47391	Routing Management	Adaptation filter option is not working properly after removal of few entries from the data received in matched pattern	Refresh the table data using Refresh icon.
SMGR-47133	Communication Manager Management	Filter enabled by one user on Manage Endpoint page is not cleared if another user logs in and opens Manage Endpoint	Clear the filter before user logouts.
SMGR-46905	Solution Deployment Manager	Trust establishment fails if VM is associated with multiple datastores resulting from migration of VM to another datastore and if snapshot is present on old datastore	Delete existing snapshots for the VM
SMGR-46901	Communication Manager Management	Click on View/Edit button in Manage Users takes 2 to 3 minutes load to page if User has Communication Manager profile	None
SMGR-46896	User Management	Preferred Handle attribute gets set to "None" when name changes for user is performed using webservice API	None
SMGR-46872	Shutdown Management	Shutdown System Manager functionality for working properly - some notifications missing, history is incorrect	None
SMGR-46642	User Management	UserMgmtJob job execution is failing	None
SMGR-46641	Trust Management	CRLExpirationCheckerJob job execution is failing	None
SMGR-46433	Infrastructure	Logout does not work on IE 11	None
SMGR-46363	Certificate Management	Trying to replace a PEM certificate with a third-party CA issued certificate which is signed using Elliptical Curve signing algorithm results in the certificate to get corrupted and removed from the Manager Identity certificate UI	None

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-46088	Geographic Redundancy	Cannot login to Secondary System Manager UI using EASG after Secondary System Manager is activated	None
SMGR-45913	User Administration	User gets system error while updating existing role having permissions for group once group is renamed	Remove permissions referencing old group name and add again the permissions for new group name.
SMGR-45884	Directory Synchronization	If the same attribute from Active Directory 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 System Manager	Remove mapping of otherEmail in System Manager Directory Synchronization settings OR change the value to lower case for the Active Directory attribute mapped to loginname and otherEmail OR map different attributes of Active Directory (both the attributes can have same value) to loginname and otherEmail in System Manager
SMGR-45856	User Management	Latin transcription of "First Name" and "Last Name" in the Identity Tab of User in System Manager are not happening properly for Russian name with the Cyrillic alphabet	None
SMGR-45074	User Management	Additional SIP handle gets created for User through User Management Web Services (replace option) or from UI import (partial/replace)	Manually delete the additional handle from User Management UI
SMGR-44830	Geographic Redundancy	Geographic Redundancy configuration will fail if we set option Maximum Sessions Per User: 1 on the Primary Server	Set option Maximum Sessions Per User: 5 on the Primary Server
SMGR-43445	Communication Manager Management	Shortcut keys indicated on Management Endpoints UI are not working	Use mouse-based navigation
SMGR-43249	Infrastructure	When System Manager is being accessed using FQDN using certificate-based authentication, then time zone is not displaying according client browser time zone	Login to System Manager using IP Address
SMGR-41634	End User Self Provisioning	End user self-provisioning does not work after providing windows username if external authentication is configured on System Manager	None
SMGR-39756	User Management	Edit button on User view page should be disabled if User does not have permission for User edit	None
SMGR-39711	Backup and Restore	After Restore operation earlier scheduled and executed daily Backup job is getting disabled	None

Known issues and workarounds in System Manager in Release 8.0

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

ID	Minimum conditions	Visible symptoms	Workaround
	IP Office	System Manager 8.0 does not support IP Office.	Do not upgrade to System Manager 8.0 if IP Office elements are being managed. System Manager 7.1.3 has support for IP Office 11.
SMGR-41595	Communication Manager Element Manager	After soft deleting user and restoring it back users button assignment is not restored	None
SMGR-44123	Communication Manager Element Manager	Description of CM and its sub-page are not mentioned correctly	None
SMGR-44353	Communication Manager Element Manager	CM sync status of schedule job disappears once status icon is clicked on the CM sync GUI.	None
SMGR-41275		Not able to view Security link with user assigned with custom role in MUDG enabled System Manager	None
SMGR-45893	Geographic Redundancy	Change IPFQDN is failing in Geo Configured System Manager	Remove the *ifcfg-eth0:0* file and restart the network service.
SMGR-45794	Communication Manager Element Manager	Hard delete of user is failing with Communication Manager Communication profile if it is created using Duplicate option	From CM Endpoint editor remove the values for “Emergency location Ext and Message Lamp Ext” attributes.
SMGR-43770	Data Migration	Showing Wrong Data Migration Path Information in Data migration log file	None
SMSG-1100	User Provisioning, Communication Manager Messaging, Avaya Aura Messaging	Unable to create users using UPR, if UPR contains messaging communication profile	None

Solution Deployment Manager Adopter Matrix

Solution Deployment Manager Adopter Matrix	**Adopting Product (System Manager Release 8.0)**												
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
OVA Deployment R 7.0.0/7.1/8.0 (Configuration and Footprint)	N	N	Y	Y	n/a	Y	Y	Y	Y	Y	Y	Y	Y
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
Patching Deployment (hotfixes)	Y [Other than AVP hosting System Manager]	N	Y	Y	n/a	Y	Y	Y	N	N	N	Y	N
Custom Patching Deployment	n/a	N	Y	Y	n/a	Y	Y	Y	N	N	Y [7.0.1 onwards]	Y	N
Service/Feature Pack Deployment	Y [Other than AVP hosting System Manager]	N	Y	Y	n/a	Y	Y	Y	N	N	N	Y	N

Solution Deployment Manager Adopter Matrix	**Adopting Product (System Manager Release 8.0)**												
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
Automated Migrations R7.x to R8.0 (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
Automated Migrations R6.x to R7.x/8.0 (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
Automated Migrations R6.x to 7.x/8.0 [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

Solution Deployment Manager Adopter Matrix	Adopting Product (System Manager Release 8.0)												
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
Automated Migrations R6.x to 7.x/8.0 [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
Automated Migrations R 5.2.1 to 7.x/8.0	N	N	N	Y	N	N	N	Y	N	N	N	N	N
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
Scheduler (upgrades and patching)	Y	Y	Y	Y	Y	Y	Y	Y	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
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
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

Solution Deployment Manager Adopter Matrix	**Adopting Product (System Manager Release 8.0)**												
System Manager Solution Deployment Manager - Centralized	Appliance Virtualization Platform	System Manager	Session Manager	Communication Manager	CM Adjuncts (MM, TN Boards, Gateways)	Branch Session Manager	AVP Utilities	CM Messaging	Breeze	Secure Access Gateway	WebLM	Application Enablement Services	Avaya Aura®
Functionality									(w/ Presence Snap-in)				Media Server
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
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: Not Applicable Y: Yes N: No

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

AVP: Appliance Virtualization Platform

VMWare: Virtualized Environment

Avaya Aura® Presence Services

What's new in Presence Services 8.0.x.x

What's new in Presence Services Release 8.0.2

Presence Services 8.0.2 includes the following new functionality:

- Support for iOS Push Kit
    - This feature is applicable to users who use the Avaya Equinox client and provides a mechanism to notify the end user that there is an incoming message.
- Support multiple LDAPs for Authentication
    - Provides a mechanism for authentication, based on the domain of the user, IWA is supported only via default group
    - See "Enabling Enterprise Basic authentication to authenticate Avaya Equinox" in the PS SNAP-IN guide for additional information.
- Enhanced PS connector API
    - This feature is applicable to developers creating custom SNAP-IN application on Avaya Breeze which require the integration with user presence states,

What's new in Presence Services Release 8.0.x

For more information see ***What's New in Avaya Aura® Release 8.0.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101050420

Installation for Avaya Aura® Presence Services 8.0.x.x

Required patches for Presence Services 8.0.2

Patches in 8.0.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 8.0.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.

Required patches for Presence Services 8.0.x

Patches in 8.0.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 8.0.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.

File list for Presence Services 8.0.1

Filename	PLDS ID	File size	Version number
PresenceServices-Bundle-8.0.2.0.125.zip	PS080002000	195 MB	PresenceServices-8.0.2.0.246.svar

Installing the release

Refer to chapters 5 and 6 of the customer documentations for instructions related to the deployment of the PS 8.0.2 release.

Note – In order to install the PS 8.0.2 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.

Troubleshooting the installation

Refer to chapter 13 of the PS customer documentation for troubleshooting instructions.

Restoring software to previous version

In order to revert to the previous version of the PS Snap-in refers to the upgrade instructions in chapter 6 of the customer instructions. The procedure to install the older SNAP-IN software is the same as the procedure for installing the new SNAP-IN software.

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.

Migrating to the PS 8.0 release from a PS 6.2.X release

Changes Affecting Migrations to 8.0

Avaya Aura® Presence Services 6.X loads cannot be migrated directly to PS 8.0.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 8.0.

- **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 general availability of Presence Services 8.0.2 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 8.0.x deployments.

Note – In order to install the PS 8.0.2 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 releases.

Migrations to release 8.0.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-7.0.1.0.871.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-7.1.2.0.224.svar + any additional patch(es)

Upgrade References to Presence Services 8.0.

Upgrade Quick Reference	Download	Prerequisite Downloads
Presence Services Customer Documentation	PresenceServices-Bundle-8.0.2.0.125.zip (PLDS ID: PS080002000)	**Breeze 3.6 or Breeze 3.5.0.1 plus available patches Platform OVA – PS 8.0.2 is only compatible with Breeze 3.5.0.1+patches and newer platform loads.**

Interoperability and requirements/Applicability

Presence Services 8.0 is compatible with the following applications.

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

The following table lists the compatibility changes in this release.

Application	Certified version	Minimum supported version	Mandatory/Optional
Avaya Breeze Platform	3.6	3.5.0.1+patches	M
Avaya Aura® System Manager	8.0.1	8.0.1	M
Avaya Aura® Session Manager	8.0.1	8.0.1	M
Avaya Aura® Communication Manager	8.0.1	8.0.1	O
Avaya Appliance Virtualization Platform	8.0.1	8.0.1	O
Avaya Aura® Application Enablement Services	8.0.1	8.0.1	O

Application	Certified version	Minimum supported version	Mandatory/Optional
Avaya Multimedia Messaging	Not Supported	Not Supported	N/A
Avaya one-X® Client Enablement Services	6.2.5 + Patch 3	6.2.5 + Patch 3	O
Avaya Aura Device Services	7.1.5	7.1.3.2	M
IBM® Domino®	9.0.1	8.5.3	O
Microsoft Lync®	Lync 2013	Lync 2010	O
Microsoft Exchange	Exchange 2016	Exchange 2010 SP1	O
Microsoft Skype for Business	6.0.9319.0	6.0.9319.0	O
Avaya Session Border Controller for Enterprise	8.0.0.1-07-12030	8.0.0.1-07-12030	O

Software Development Kit

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

SDK File name	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 8.0.1.x

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 8.0.2 now supports all of the AMM feature set and in some cases the AMM application can simply be eliminated.

Fixes in Presence Services 8.0.x.x

Fixes in Release 8.0.1.2

The following issues have been resolved in cumulative updates to the 8.0.1 release:

ID	Minimum conditions	Visible symptoms	Release found in

Fixes in Release 8.0.2

The following issues have been resolved in cumulative updates to the 8.0.1 release:

ID	Minimum conditions	Visible symptoms	Release found in

Fixes in Release 8.0.1

The following issues have been resolved in cumulative updates to the 8.0.1 release:

ID	Minimum conditions	Visible symptoms	Release found in
PSNG-4437	Avaya Equinox client is exchanging instant messages with an Avaya 1XC client.	Delayed-offline IMs incorrectly saved for Equinox client users. This is incorrect as the message was delivered to the Equinox client.	8.0.0

Fixes in Release 8.0

The following issues have been resolved in cumulative updates to the 8.0 release:

ID	Minimum conditions	Visible symptoms	Release found in
Zephyr-58971	The PS/Breeze application is deployed in JITC/Hardened mode.	High Availability DB fails to startup after importing 3rd party certs and enabling FIPS mode	7.1.2
PSNG-4154	Avaya Aura is federated with Microsoft Lync	Lync/S4B federation: Hybrid user: Aura user can't send IM to MS device of hybrid user (Avaya phone on desktop and MS messaging client)	7.1.2
PSNG-4137	Avaya Aura is federated with Microsoft Lync	Lync/S4B federation: Hybrid user: Aura manual states removed by MS automatic states.	7.1.2

Known issues and workarounds in Presence Services 8.0.x.x

Known issues and workarounds in Presence Services Release 8.0.1.2

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

ID	Minimum conditions	Visible symptoms	Workaround

Known issues and workarounds in Presence Services Release 8.0.2

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 chat message to 1XC in DND state,	There is no work-around 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.
Note		After an Avaya contact is removed from a XMPP federated client, presence does not render if the Avaya	Use either of the two solutions:

ID	Minimum conditions	Visible symptoms	Workaround
		contact is re-added to the federated user.	1. Toggle the favorite flag for the federated user in the Avaya client 2. Logout and log back in to 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 Messaging clients.	It is mandatory that Equinox clients 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.

Known issues and workarounds in Presence Services Release 8.0.1

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 chat message to 1XC in DND state,	There is no work-around 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.
Note		After an Avaya contact is removed from a 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 in to 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 Messaging clients.	It is mandatory that Equinox clients 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.

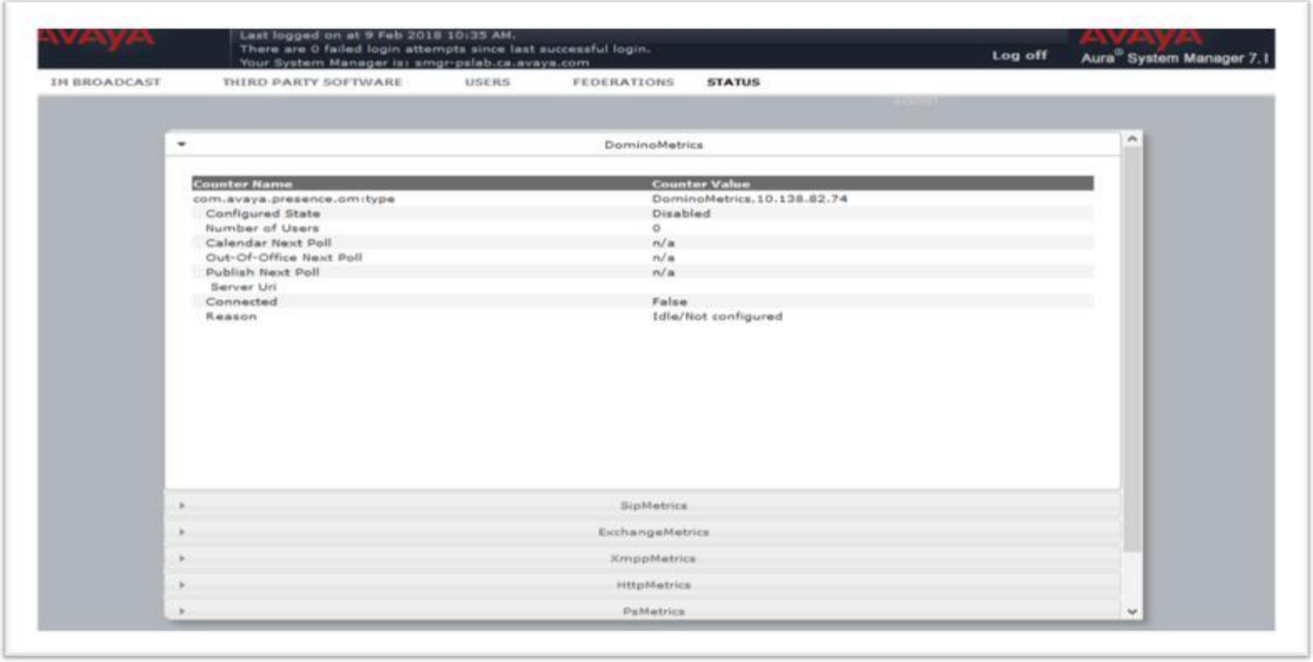
ID	Minimum conditions	Visible symptoms	Workaround
Note	Existing AMM deployments	There is no direct upgrade path from existing AMM deployments to use the PS 8.0.1 application.	Existing AMM deployments that are to migrate to PS 8.0.1 should be treated as new installs.
Note	Existing AMM deployments	All PS 8.0.1 users must be administered in SMGR.	There is no work-around. Administration of all users in SMGR is mandatory in PS 8.0.1.

Known issues and workarounds in Presence Services Release 8.0

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

ID	Minimum conditions	Visible symptoms	Workaround
PSNG-4437	Avaya Equinox client is exchanging instant messages with an Avaya 1XC client.	Delayed-offline IMs incorrectly saved for Equinox client users. This is incorrect as the message was delivered to the Equinox client.	There is no work-around for this issue. It will be fixed in release 8.0.1.
PSNG-2630	Avaya Aura is federated with Microsoft Lync	There is no message notification when Lync sends chat message to 1XC in DND state,	There is no work-around 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.
Note		After an Avaya contact is removed from a 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 in to 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: The Presence Services Admin Web GUI, as shown below, is disabled by default in PS 8.0.



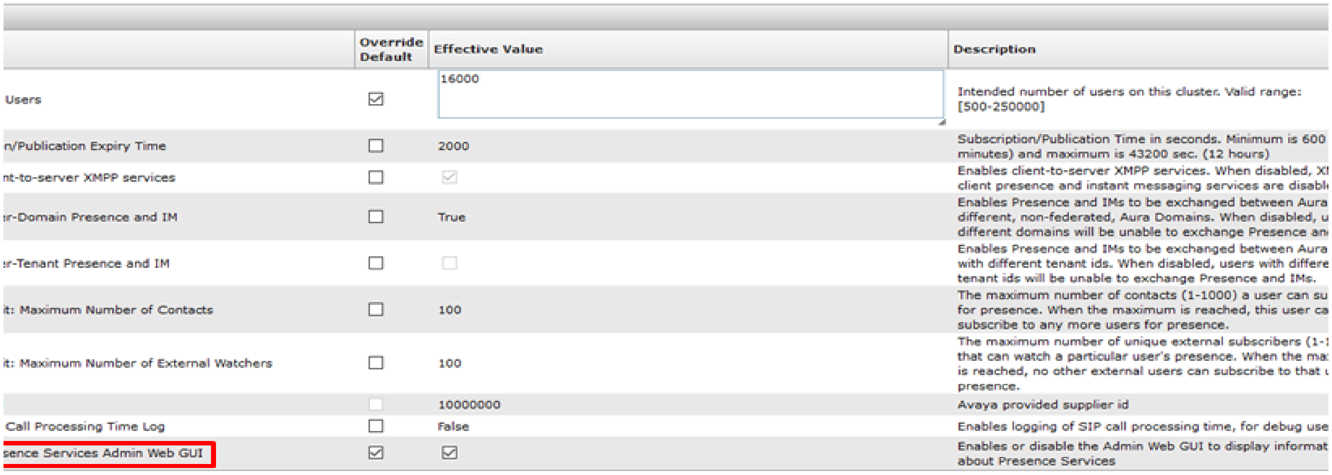
Last logged on at 9 Feb 2018 10:35 AM.
There are 0 failed login attempts since last successful login.
Your System Manager is: smgr-pslab.ca.avaya.com

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

Avaya Aura® Application Enablement Services



	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, X 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.
it: 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.
it: Maximum Number of External Watchers	☐	100	The maximum number of unique external subscribers (1- that can watch a particular user's presence. When the ma is reached, no other external users can subscribe to that 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

What’s new in Application Enablement Services 8.0.x.x

What’s new in Application Enablement Services Release 8.0.x

For more information see ***What’s New in Avaya Aura® Release 8.0.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101050420

Installation for Avaya Aura® Application Enablement Services Release 8.0.x.x

Backing up the AE Services software

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

1. Log into 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 8.0.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 documents for installation and migration instructions.

Additional references for Virtualized deployments:

- Migrating and Installing Avaya Appliance Virtualization Platform
- Release Notes for Avaya Appliance Virtualization Platform Release 8.0
- Deploying Avaya Aura® AVP Utilities in Virtualized Environment
- Release Notes for Avaya Aura® AVP Utilities Release 8.0
- Deploying Avaya Aura® applications Release 8.0
- Upgrading and Migrating Avaya Aura® applications Release 8.0

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 8.0, it is recommended to upgrade AE Services server before upgrading Communication Manager.

In 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.

This change may cause older AE Services clients (version AE Services 7.0 or earlier) that are using TLS to fail to establish a secure socket connection to the AE Services 8.0 server. To achieve a more secure client/server socket connection, we encourage current client applications to use an AE Services 7.0 or later SDK where the TLS 1.2 protocol is supported. Note, the initial released AE Services 7.0 Windows TSAPI client (tsapi-client-win32) did not initially support TLS 1.2 and has been updated to support TLS 1.2. All the latest versions of the AE Services 8.0 SDKs support TLS 1.2. If upgrading to AE Services 8.0 SDK is not a viable option, an AE Services administrator can enable the TLS 1.1 and/or TLS 1.0 protocol via the AE Services Management Console web interface.

Note: All three TLS protocol versions can be active at the same time. This allows a gradual migration of current client applications to move towards a more secure TLS protocol over a period.

For the AE Services 8.0 release, the AE Services server will discontinue the use of a default server certificate signed by Avaya. Customers are required to install their own certificates signed by either their own Private Key Infrastructure (PKI) or a third-party PKI vendor. If such resources are not available immediately, they may use the temporary AE Services server self-signed certificate. It should be noted that this self-signed certificate is based on SHA2, which may not work with some older clients, and the certificate is valid for only 1 year. It is expected that customers will deploy their own certificates before this certificate expires.

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.

Note: For the AE Services 5.x and 6.x releases, all versions of the default installed server certificate are scheduled to expire no later than January 2018. For any customer using this certificate, once this certificate expires, an AE Services based client using a TLS connection will not be able to communicate with the AE Services server.

Possible customer options to create the new AE Services server certificate:

- Use your own PKI
- Use Avaya Aura's System Manager (SMGR) Trust Management PKI feature **
- Use an Open Source PKI (e.g. EJBCA)*
- Use a third-party vendor (e.g. Verisign)*
- Use OpenSSL to create your own Certificate Authority (CA) ***

* Avaya does not endorse or require the use of this product or vendor. You may use any product or vendor of your choosing.

** See the System Manager Trust Management section in the AE Services 8.0 Administration and Maintenance document

*** See the OpenSSL section in the AE Services 8.0 Administration and Maintenance document.

If for some reason none of the above options fit your immediate need, contact Avaya Services for additional assistance.

Upgrading to AE Services 8.0.x

Important Notes:

- Upgrade from AES 8.0 to AES 8.0.1 through the RPM-only installer is supported for VMWare and KVM deployments. It is not supported for Software-only offers. Refer the upgrade instructions using Feature Pack installer for more details.
- After installing AES 8.0.1, you must install the following updates:
  - AES 8.0.1.0.1 Super Patch

AE Services Server Upgrade Instructions using Feature Pack installer from AES 8.0 to AES 8.0.1

Note: Upgrading using the Feature Pack installer is not supported for AES 8.0 Software-only systems.

AES 8.0.1 provides a feature pack installer (rpm-installer) which facilitates upgrade from AES 8.0 to AES 8.0.1 using a bin file. Prior to installing the AE Services Feature Pack Installer, a pre-upgrade patch needs to be applied on the AES 8.0 system.

SSH into the AE Services 8.0 server to be upgraded.

1. Using PLDS, download the pre-upgrade patch, "AES801_PreUpgradePatch.bin", using the PLDS ID AES00000701. This pre-upgrade patch will upgrade the tomcat version to 8.5.34 along with other security updates. This pre-upgrade patch also contains the L1TF remediation.

2. Using the AE Services patch process, install the pre-upgrade patch on your existing AE Services server.
3. Once the pre-upgrade patch installation is successful, the AE Services 8.0.1 Feature pack installer (aesvcs-8.0.1.0.0.5-featurepack.bin) can be downloaded using the PLDS ID AES00000700.
4. Using the AE Services RPM-only installation process, install the feature pack on the system.

AE Services Server Upgrade Instructions

Note: For an AE Service 7.0.1 VMware offer upgrade to AE Service 8.0.x VMware offer using SDM, see Chapter 7 in the document "Deploying Avaya Aura® Application Enablement Services in Virtualized Environment"

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 login 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 below sections for each platform.
9. Use the AE Services 8.0.x Management Console web page "Maintenance > Server Data > Restore" to restore previously 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 the AE Services 8.0 Management Console, verify and update the values recorded in step 4 on the AE Services 8.0.x server.

Restoring AE Services software to previous version

Use the AE Services 8.0.x 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 8.0” was executed before the previous backup was taken.

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.

RHEL 7.4 Support for AE Services 8.0.x

AE Services 8.0.x is supported on RHEL 7.4. Upgrading AE Services 8.0.x to RHEL 7.5 or greater is not supported and may cause the system to enter an unstable state

Important: After installing AES 8.0.1, you must install the AES 8.0.1 Super Patch 1 (aesvcs-8.0.1.0.1-superpatch.bin) using PLDS ID AES00000704. Please refer to PSN020381u for additional details.

Installation for Avaya Aura® Application Enablement Services 8.0.1 Super Patch 4

AE Services 8.0.1 Super Patch 4 (aesvcs-8.0.1.0.4-superpatch.bin) can be downloaded using PLDS ID AES00000761. This patch can be installed on top of AES 8.0.1 or AES 8.0.1.0.1 or AES 8.0.1.0.2 or AES 8.0.1.0.3 system. Please refer to PSN020381u for additional details.

Installation for Avaya Aura® Application Enablement Services 8.0.1 Super Patch 3

AE Services 8.0.1 Super Patch 3 (aesvcs-8.0.1.0.3-superpatch.bin) can be downloaded using PLDS ID AES00000735. This patch can be installed on top of AES 8.0.1 or AES 8.0.1.0.2 or AES 8.0.1.0.2 system. Please refer to PSN020381u for additional details.

Installation for Avaya Aura® Application Enablement Services 8.0.1 Super Patch 2

AE Services 8.0.1 Super Patch 2 (aesvcs-8.0.1.0.2-superpatch.bin) can be downloaded using PLDS ID AES00000729. This patch can be installed on top of AES 8.0.1 or AES 8.0.1.0.1 system. Please refer to PSN020381u for additional details.

Installation for Avaya Aura® Application Enablement Services Software Only 8.0.1

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

Install Avaya Aura® Application Enablement Services Software Only 8.0.1 (swonly-8.0.1.0.0.5-20181122.iso).

Installation steps for Avaya Aura® Application Enablement Services 8.0.1 Aura® OVA Media

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

Install Avaya Aura® AE Services 8.0.1 Aura® OVA Media (AES-8.0.1.0.0.5.20181122-e65-00.ova)

Installation steps for Avaya Aura® Application Enablement Services 8.0.1 Aura® KVM Support

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

Install Avaya Aura® Application Enablement Services 8.0.1 KVM Support (AES-8.0.1.0.0.5.20181122-kvm-001.ova)

Installation steps for Avaya Aura® Application Enablement Services 8.0.1 Aura® Feature Pack Installer

Note: Not applicable for Software-only systems. The following steps are valid only for installation of AES 8.0.1 on AES 8.0 via feature pack installer.

1. Install Avaya Aura® Application Enablement Services 8.0.1 Pre-Upgrade Patch(AES801_PreUpgradePatch.bin)
2. Install Avaya Aura® Application Enablement Services 8.0.1 Feature Pack Installer (aesvcs-8.0.1.0.0.5-featurepack.bin)

Installation for Avaya Aura® Application Enablement Services Software Only 8.0

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

Install Avaya Aura® Application Enablement Services Software Only 8.0 (swonly-8.0.0.0.0.6-20180605.iso).

Installation steps for Avaya Aura® Application Enablement Services 8.0 Aura® OVA Media

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

Install Avaya Aura® AE Services 8.0 Aura® OVA Media (AES-8.0.0.0.0.6.20180605-e65-00.ova)

Installation steps for Avaya Aura® Application Enablement Services 8.0 Aura® KVM Support

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

Install Avaya Aura® Application Enablement Services 8.0 KVM Support (AES-8.0.0.0.0.6.20180605-kvm-001.ova)

Functionality not supported

- AE Services 8.0.x does not support the “Bundled” and “System Platform” offers. Customers upgrading to AE Services 8.0.x must switch to the “Software-Only” offer or “VMware” (AE Services on AVP) offer.
- In AE Services 8.0.x, the Machine Preserving High Availability (MPHA) (aka VSST) feature is not available.
- **Upgrade from an older AES version to AES 8.0 through the RPM-only installer is not supported**

  AES 8.0 is available in the three offers mentioned in the table “Required artifacts for Application Enablement Services Release 8.0” below. All installations of AES 8.0 need to be fresh deployments. The AE Services 8.0 restore tool (i.e., Maintenance > Server Data > Restore) should be applied to restore data from an older version of AES to AES 8.0.

Installation of Avaya Aura® Application Enablement Services 8.0

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

Required artifacts for Application Enablement Services Release 8.0.x

Required artifacts for Application Enablement Services Release 8.0.1.0.4

The following section provides Application Enablement Services downloading information.

PLDS Product ID	Download Title and Description
AES00000761	Avaya Aura® AE Services 8.0.1 Super Patch 4 Description: Avaya Aura® AE Services 8.0.1 Super Patch 4. Please refer to PSN020381u for additional details. File Name: aesvcs-8.0.1.0.4-superpatch.bin File Size: 222.9 MB (228,245.2 KB) MD5 Checksum: 1d0b8a3f84289241b6683f9907b821c8 SHA1: b5d1ffcd4e3fe6d817837eed9c1bceaaefd8083c SHA256: b7e8eb9d9a3409a3e5004170faa2ccb84534e91642ae072bf0136d25d6e72216

Required artifacts for Application Enablement Services Release 8.0.1.0.3

The following section provides Application Enablement Services downloading information.

PLDS Product ID	Download Title and Description
AES00000735	Avaya Aura® AE Services 8.0.1 Super Patch 3 Description: Avaya Aura® AE Services 8.0.1 Super Patch 3. Please refer to PSN020381u for additional details. File Name: aesvcs-8.0.1.0.3-superpatch.bin File Size: 111.46 MB (114,135.9 KB) MD5 Checksum: 2a4d8ec1814f3c485a9d7600dc16bf87

PLDS Product ID	Download Title and Description
	SHA1: db1add11ed7b1a9975aff7c8b8584b770f50b4b7 SHA256: df29e510001aec9a8423189cd16415ed5e3fb1fbc315f86e3121df343f7330d8

Required artifacts for Application Enablement Services Release 8.0.1.0.2

The following section provides Application Enablement Services downloading information.

PLDS Product ID	Download Title and Description
AES00000729	Avaya Aura® AE Services 8.0.1 Super Patch 2 Description: Avaya Aura® AE Services 8.0.1 Super Patch 2. Please refer to PSN020381u for additional details. File Name: aesvcs-8.0.1.0.2-superpatch.bin File Size: 111.17 MB (113,844 KB) MD5 Checksum: cc733a3f8f66f62ca1793d9f2e0e9772

Required artifacts for Application Enablement Services Release 8.0.1

The following section provides Application Enablement Services downloading information.

PLDS Product ID	Download Title and Description
AES00000698	Avaya Aura® Application Enablement Services Software Only 8.0.1 Description: Avaya Aura® Application Enablement Services Software Only 8.0.1 File Name: swonly-8.0.1.0.0.5-20181122.iso File Size: 396.14 MB (405,652 KB) MD5 Checksum: 3d72eb79bc0f6184634c9069e2debcd1
AES00000699	Avaya Aura® AE Services 8.0.1 Aura® OVA Media Description: Avaya Aura® Application Enablement Services 8.0.1 Aura® OVA Media File Name: AES-8.0.1.0.0.5.20181122-e65-00.ova File Size: 2,693.36 MB (2,758,000 KB) MD5 Checksum: cc91e84daf833a9fa08becf848175be3
AES00000700	Avaya Aura® Application Enablement Services 8.0.1 Feature Pack Installer Description: Avaya Aura® Application Enablement Services 8.0.1 Feature Pack Installer File Name: aesvcs-8.0.1.0.0.5-featurepack.bin File Size: 156.3 MB (160,055.82 KB) MD5 Checksum: 17f396d600caed56f2f6ca94d6a61b4c
AES00000701	Avaya Aura® Application Enablement Services 8.0.1 Pre-Upgrade Patch Description: Avaya Aura® Application Enablement Services 8.0.1pgrade Patch File Name: AES801_PreUpgradePatch.bin

PLDS Product ID	Download Title and Description
	File Size: 233.18 MB (238,771.21 KB) MD5 Checksum: 62fdebef187e57c838fdcafdd1dcc775
AES00000702	Avaya Aura® Application Enablement Services 8.0.1 KVM Support Description: Avaya Aura® Application Enablement Services 8.0.1 KVM Support File Name: AES-8.0.1.0.0.5.20181122-kvm-001.ova File Size: 2,657.75 MB (2,721,540 KB) MD5 Checksum: 7f2f6267678dbd3f4610a88c567cb9fd
AES00000704	Avaya Aura® AE Services 8.0.1 Super Patch 1 Description: Avaya Aura® AE Services 8.0.1 Super Patch 1. Please refer to PSN020381u for additional details. File Name: aesvcs-8.0.1.0.1-superpatch.bin File Size: 6.46 MB (6,611.49 KB) MD5 Checksum: c5c913d93e4199430b380263fee2fa14

Required artifacts for Application Enablement Services Release 8.0

The following section provides Application Enablement Services downloading information.

PLDS Product ID	Download Title and Description
AES00000667	Avaya Aura® Application Enablement Services Software Only 8.0 Description: Avaya Aura® Application Enablement Services Software Only 8.0 The following RPMs need to be present on the base VM before installing SW only AES 8.0: nspr-4.19.0-1.el7_5.x86_64.rpm nss-3.36.0-5.el7_5.x86_64.rpm nss-softokn-3.36.0-5.el7_5.x86_64.rpm nss-softokn-freebl-3.36.0-5.el7_5.x86_64.rpm nss-util-3.36.0-1.el7_5.x86_64.rpm File Name: swonly-8.0.0.0.0.6-20180605.iso File Size: 386.47 MB (395,748 KB) MD5 Checksum: def033d550540499e043d2897835ea57
AES00000665	Avaya Aura® AE Services 8.0 Aura® OVA Media Description: Avaya Aura® Application Enablement Services 8.0 Aura® OVA Media File Name: AES-8.0.0.0.0.6.20180605-e65-00.ova File Size: 2,590.07 MB (2,652,230 KB) MD5 Checksum: 960eaf5cfdc72ade376bb4c6d4ac665d
AES00000666	Avaya Aura® Application Enablement Services 8.0 KVM Support Description: Avaya Aura® Application Enablement Services 8.0 KVM Support File Name: AES-8.0.0.0.0.6.20180605-kvm-001.ova File Size: 2,553.5 MB (2,614,790 KB) MD5 Checksum: 2e46d1345b0b4fa06ffe14ad48042da4

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			

Enhanced Access Security Gateway (EASG)

EASG provides a secure method for Avaya services personnel to access the Avaya Aura® AE Services server 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.

Changes and Issues

Issues related to Backup and Restore

The following fields are not restored correctly during the restore process. Using the AE Services Management Console, make note of the referenced data on the following specified screens once the backup is taken and manually configure to the saved values after the restore completes.

- 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”

Upgrading issues related to licenses and the AE Services 8.0 embedded WebLM server

- After an upgrade all customers will be required to obtain a new license based on the new HostID of the embedded WebLM.
- If the AE Services server is in a GRHA configuration, GRHA must be disabled and then the active and standby AE Services server must be upgraded. Before enabling GRHA, the administrator must log into WebLM on both AE Services servers to obtain the WebLM HostID of each server. These two HostIDs will be required to obtain the new AE Services license file.

WebLM server compatibility

The AE Services server incorporates embedded WebLM 7.1 server and its client components. When using an external SMGR 8.0 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. This means the WebLM 8.0 server can support connectivity to WebLM 6.x clients. Note the WebLM 6.x clients are used in the AE Services 6.x release. The WebLM server does not support forward compatibility. This means the AE Services 7.x WebLM client will not work with the WebLM 6.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.

Alarm Viewer Change

Prior to the AE Services 7.1 release, the Management Console’s, “Status > Alarm Viewer”, screen would display an “Alarm Status” column. The Alarm Status column would display the current status of an alarm as Unacknowledged, Acknowledged or Cleared. The latter two states are set by the system administrator using the Alarm Viewer screen. Note, acknowledging or clearing an alarm using the Alarm Viewer screen did not mean the alarm was resolved. Starting with AE Services 7.1, the Alarm Viewer page has been redesigned. The Alarm Status column and the configuration options have been removed. For AE Services 8.0, the Alarm Viewer screen will only display the list of raised alarms.

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-8.0.0.0.0.419.exe

cmapixml-sdk-8.0.0.0.0.419.exe

dmcc-dotnet-sdk-7.1.1.0.0.54.exe

smssvc-sdk-8.0.0.0.0.419.exe

telsvc-sdk-8.0.0.0.0.419.exe

jtapi-sdk-8.0.0.52.exe

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

Known issues and workarounds in Application Enablement Services 8.0.x.x

Known issues and workarounds Application Enablement Services in Release 8.0.1.0.4

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

ID	**Visible symptoms**	**Workaround**
AES-18672	Customer cannot login to OAM with user configured in LDAP Active Directory when "User ID Attribute Name" is changed from "uid"	1. Add the following line in the file /etc/sssd/sssd.conf

ID	Visible symptoms	Workaround
	to "samAccountName" on the "Enterprise Directory" page of OAM.	ldap_user_name = sAMAccountName 2. Restart SSSD service.
AES-18420	In a GRHA setup, when a service pack is installed on primary AES server via SDM, the patch is not installed on the secondary server	Install the service on the primary server via the command line interface.
AES-15383	DMCC process gets restarted with Out of Memory error.	
AES-18434	The Active Link status displays incorrect information on the OAM page, AEServices→CVLAN Client	Correct Active Link Status information is displayed on Status→ and Control→ CVLAN Service Summary
AES-18431	A call answered by a Coverage Answer Group User on Communication Manager gets disconnected.	
AES-17434	Changing the status of the CVLAN link On AES OAM -> Status -> Status and Control -> CVLAN Service Summary fails and displays the following error: "Error talking to MBean Server". Customer unable to take CVLAN link online or offline.	Go to AES OAM → Networking → AE Service IP (Local IP). For “Client Connectivity” set the correct interface from dropdown, instead of the default “any”

Known issues and workarounds Application Enablement Services in Release 8.0.1.0.3

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

ID	Visible symptoms	Workaround
AES-15383	The DMCC process gets restarted.	
AES-18320	The enterprise directory page on OAM does not apply changes nor does it throw any error if the FQDN entry of the active directory is missing in the /etc/hosts file on AES. In addition, while restoring the backup data on AES, if the entry of the Active directory is not present in /etc/hosts file, the system displays an error for invalid FQDN which persists even after the addition of the host entry in /etc/hosts file.	For both the scenarios, add the FQDN entry of the active directory in /etc/hosts file before configuring the Enterprise Directory page on OAM.
AES-18420	Secondary AES fails to get upgraded when the primary AES is upgraded using SDM.	Upgrade the Superpatch through command line.
AES-17701	Even while 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	

Known issues and workarounds Application Enablement Services in Release 8.0.1.0.2

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

ID	**Visible symptoms**	**Workaround**
AES-18183	After configuring and starting GRHA, a newly created CTI user on the active server is not replicated to the standby server.	Add the CTI users before configuring GRHA.
AES-18098	After Database backup restore, SNMP component value does not get restored	After restoring database, navigate to SNMP->SNMP Agent on OAM and click on Apply Changes.
AES-18051	Delivered event is missing on monitored station after AutoCallBack.	
AES-18033	Cannot redirect to External WebLM by clicking on WebLM server access on OAM	Reload the page manually.
AES-17985	DMCC .Net J-script is not supported in modern browsers(Firefox, Chrome).	DMCC .Net J-script is only supported in IE 6 on windows OS.
AES-17984	The result for skill extension query using JTAPI API getLoggedOnAgents() yields wrong result. It returns the agent information which was removed from skill recently which causes client application to assume that agent still belongs to the same skill.	For the 2nd getLoggedOnAgents() query attempt, use different JTAPI provider
AES-17913	Linux version of cmapijava-sdk will not have Javadocs	Install Zip file or windows version of cmapijava-sdk to obtain the javadocs.
AES-17874	Yum update-minimal –security command will fail because libuuid rpm has multiple architectures installed on AES	Add libuuid into exclude list in /etc/yum.conf file. Example: exclude=axis-**,bash-**,mon-**,tomcat-**,libuuid-*
AES-17861	AES swonly-iso installation fails if McAfee endpoint protection is enabled	Disable McAfee endpoint protection and then install AES swonly-iso
AES-17781	Any administrative changes made to security database does not get reflected in the active JTAPI application immediately.	Restart the JTAPI application for the new security database changes to be reflected correctly in the JTAPI application.
AES-17701	TLS 1.1 and TLS 1.2 not disabled on sohd port 9041	
AES-17635	The "mvap.sh" command doesn't shows correct number for DMCC licenses acquired	
AES-17565	If hostname is provided in uppercase, alarm viewer is not shown on OAM	If hostname is provided in uppercase, alarm viewer is not shown on OAM

AES-17337	After performing backup restore from AES with RHEL release <=5 to AES with RHEL release >=6, AES is not reachable through all interfaces.	Change rp_filter value in /etc/sysctl.conf to 2.
		net.ipv4.conf.all.rp_filter = 2
		net.ipv4.conf.default.rp_filter = 2
		net.ipv4.conf.eth0.rp_filter = 2
		net.ipv4.conf.eth1.rp_filter = 2

AES-17332	DMCC Application stops receiving events after Service Provider is restarted.	Shutdown JVM and restart application.

ID	**Visible symptoms**	**Workaround**
AES-17064	The JTAPI Exerciser does not output all call listener events/data.	Refer debug trace for seeing the events.
AES-14924	TerminalLoggedOffEvent not generated via removeAgent	
AES-14927	Incorrect number of ACD Address logged on and off events	

Known issues and workarounds Application Enablement Services in Release 8.0.1

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

ID	**Visible symptoms**	**Workaround**
AES-17913	Linux version of cmapijava-sdk will not have Javadocs	Install Zip file or windows version of cmapijava-sdk to obtain the javadocs.
AES-17874	Yum update-minimal –security command will fail because libuuid rpm has multiple architectures installed on AES	Add libuuid into exclude list in /etc/yum.conf file. Example: exclude=axis-**,bash-**,mon-**,tomcat-**,libuuid-*
AES-17864	Kernel martian source logs are logged in alarm.log file which results in low retention of useful logging data	
AES-17861	AES swonly-iso installation fails if McAfee endpoint protection is enabled	Disable McAfee endpoint protection and then install AES swonly-iso
AES-17860	User cannot delete the “avayadefaultsal” trap receiver	
AES-17781	Any administrative changes made to security database does not get reflected in the active JTAPI application immediately.	Restart the JTAPI application for the new security database changes to be reflected correctly in the JTAPI application.
AES-17738	Listed log files (sssd_ldap_domain.log, sssd.log, sssd_nss.log, maillog, cron) have no rotation configured, hence the file sizes may grow to a very large size.	
AES-17701	TLS 1.1 and TLS 1.2 not disabled on sohd port 9041	
AES-17635	The "mvap.sh" command doesn't shows correct number for DMCC licenses acquired	
AES-17565	If hostname is provided in uppercase, alarm viewer is not shown on OAM	If hostname is provided in uppercase, alarm viewer is not shown on OAM
AES-17347	Running 'mvap.sh info' will show unexpected exceptions output.	
AES-17338	SNMP query for AVAESTSAPILICENSETABLE_OID does not return SNMP OIDs. snmpwalk -v 2c -c Avaya 127.0.0.1 .1.3.6.1.4.1.6889.2.27.2.1.3.24	

ID	Visible symptoms	Workaround
	SNMPv2-SMI::enterprises.6889.2.27.2.1.3.24 = No Such Object available on this agent at this OID	

AES-17337	After performing backup restore from AES with RHEL release <=5 to AES with RHEL release >=6, AES is not reachable through all interfaces.	Change rp_filter value in /etc/sysctl.conf to 2.
		net.ipv4.conf.all.rp_filter = 2
		net.ipv4.conf.default.rp_filter = 2
		net.ipv4.conf.eth0.rp_filter = 2
		net.ipv4.conf.eth1.rp_filter = 2

AES-17332	DMCC Application stops receiving events after Service Provider is restarted.	Shutdown JVM and restart application.
AES-17064	The JTAPI Exerciser does not output all call listener events/data.	Refer debug trace for seeing the events.
AES-14924	TerminalLoggedOffEvent not generated via removeAgent	
AES-14927	Incorrect number of ACD Address logged on and off events	

Known issues and workarounds Application Enablement Services in Release 8.0

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

ID	Visible symptoms	Workaround
AES-14924	TerminalLoggedOffEvent not generated via removeAgent	
AES-14927	Incorrect number of ACD Address logged on and off events	
AES-16068	CFD: Utility Services MyPhone user cannot log in due to CM UTF8 native name improperly handled by OSSICM/SMS	The user's native language name should not contain D0 in byte position 18 on the Communication Manager
AES-16099	[AES 7.0.1.0.3.15-0 (SP3)] DN call: DeviceIDType changing between explicitPrivateUnknown and implicitPublic	
AES-16150	sohd fills up logs if certificate is invalid	
AES-16960	DMCC Java Client 7.1.1 does not receive Delivered events from older AE Services	
AES-16985	Misconfigured JSF ViewStates can lead to severe RCE vulnerabilities	
AES-17058	Incorrect switch version is shown in TSAPI Service Summary.	
AES-17059	DMCC use duplicate crossRefID	
AES-17064	JTAPI Exerciser doesn't output all Call Listener events/data	
AES-17097	WebLM IP address changed after removal of GRHA	

ID	**Visible symptoms**	**Workaround**
AES-17134	SMS service: "IPServices" Model does not return response when Field specific request is sent.	
AES-17223	DLG service license mode shows "N/A" and cause as "UNKNOWN".	
AES-17232	Cannot create CSR if using complex password	Use passwords without special characters e.g., &, % $ etc.
AES-17260	MIB browser not able to connect AES SNMP server when SeLinux is Enable	
AES-17283	Intermittently, 7.1.3 "List All Users" page giving exception after restoring the backup file	
AES-17332	Not getting DMCC Call Control events from JAVA SDK after an application shuts down and restarts the Service Provider.	
AES-17337	AES upgrade - eth0 & eth2 are not establishing TCP connection as expected	
AES-17338	SNMP query for TSAPI License Table (AVAESTSAPILICENSETABLE_OID) does not return SNMP OIDs.	
AES-17347	mvap.sh does not returns expected result	
AES-17351	GeoHA failover does not work if AES hostname is in DNS	
AES-17385	AEP up/down SNMP trap with wrong OID	
AES-17386	AES 7.1 restore does not restore linux password (/etc/shadow)	
AES-17399	AES713B7 - secure mode: External LDAP authentication does not work after switching to secure mode.	
AES-17415	AES 8.0.0.0.4: Unable to populate OCI trunk info and OCI trunk group in Delivered and Establish event of consultation call	
AES-17420	High CPU utilization is observed for 2 AES VM.	
AES-17434	"Error talking to MBean service" while creating TSAPI or CVLAN link.	
AES-17439	"ANI_Reqd" field in AAR Analysis table cannot be modified	
AES-17454	SNMP Trap receiver not properly configured in AES restore	Manually reconfigure SNMP trap receiver
AES-17489	AES 8.0 has Embedded WebLM of version 7.1	
AES-17492	AES 8.0 SWonly: Secondary WebLM details	

ID	**Visible symptoms**	**Workaround**
AES-17502	HTTPD service affected by Instance name on Google Cloud Platform (GCP)	It is recommended that customer keeps the hostname short. If the FQDN in /etc/hosts file is greater than 45 characters, then follow the steps below: 1. Remove FQDN from /etc/hosts 2. Install AES on GCP 3. Restart the VM This is applicable only to GCP
AES-17518	RHEL becomes unstable/unusable after AES swonly uninstallation	Avaya does not recommend uninstallation. However, if AES SW only uninstallation is performed then third-party rpms must not be installed.
AES-17523	Commented SSLVerifyDepth Value causes "Certificate Chain Too Long" error	Modify the file "/etc/https/conf.d/ssl.conf" to add the entry “SSLVerifyDepth 10”. This allows for multiple chain certificate
AES-17526	remote logging not working in secure mode	Manually add the following data to mvap.conf: 1. Uncomment line “#call logremote” 2. Add ipaddress in “target=’remote-host-IP-Address’”
AES-17527	Allow Secure Mode users to use a "." in the username	
AES-17565	Alarm viewer not seen on OAM. This is caused by a mismatch in hostname in the files /etc/hosts and /etc/hostname when Uppercase/LowerCase characters are used	Use lowercase characters as hostnames Manually modify the hostnames in /etc/hosts and /etc/hostname so that they are same. If using Uppercase characters, a reboot will cause the issue to reappear
AES-17546	Running Sanity Plugin Step Failed while deploying AES8.0 swonly iso through SMGRSDM	Though the error is seen along with the message “VM deploy failed”, the Virtual Machine does get deployed successfully.
AES-17562	Tomcat localhost_access_log is not automatically cleaned up	Manually delete older /var/log/tomcat/localhost_access_log
AES-17556	AES 8.0: In installation of AES via vSphere it shows IPv6 default IP instead of IPv4 IP	Don’t use default values populated for network configuration during first boot of AES.
AES-17551	Import SDB not working properly in 7.1.2	Create CTI security database configuration manually or use full database backup taken on an older AES.
AES-17550	Restoring older backup on 7.1.x breaks OAM login	Applicable when restoring from AES 4.x which contains deprecated pam_stack.so. The file /etc/pam.d/oam_login_service should be manually edited to contain only the following entries:

ID	**Visible symptoms**	**Workaround**
		#%PAM-1.0 auth include system-auth auth required pam_nologin.so account include system-auth password include system-auth session include system-auth session optional pam_lastlog.so.

Fixes in Application Enablement Services in Release 8.0.x.x

Fixes in Application Enablement Services in Release 8.0.1.0.4

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms
AES-18696	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	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.
AES-18104	7.1.3.3	TWS logs failed to get generated due to wrong port redirection of logs
AES-18502	AES 7.1.3.3	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
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 the generation of log files.
AES-18320	AES 7.1	The enterprise directory page on OAM did not apply changes nor did it display any error if the FQDN entry of the active directory was missing in the /etc/hosts file on AES. On restoring of backup data on AES, if the entry of the Active directory was not present in /etc/hosts, it generated an error for invalid FQDN which persisted even after adding the host entry in /etc/hosts
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

Fixes in Application Enablement Services in Release 8.0.1.0.3

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms
AES-18252	AES 7.1.3 (SWONLY offer)	Post DB restore, a user was unable to log in to the AES system.
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-18246	SMS service is used	SMS logging did not get enabled when either of SMS logging or CM Proxy Trace Logging was enabled from OAM.
AES-18270	AES 8.0.1 with GRHA configured.	Post installing license for GRHA, the standby AES shows license state in grace period.

ID	Minimum Conditions	Visible symptoms
AES-18088	AES 7.1.3 LSU 4	Slapd entered into an unusable state.

Fixes in Application Enablement Services in Release 8.0.1.0.2

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms
AES-18110	AES 7.1.3	setSELinux utility could not properly set the SELinux mode.
AES-18101	AES DMCC SDK 8.0.1/7.1.1	DMCC SDK 8.0.1 or 7.1.1 could not receive channelType in DeliveredEvent.
AES-18071	AES 7.1.3.x	SMS would get timed out intermittently.
AES-18012	AES 6.3.3	AES could not relinquish control of a call after a snapshot on the station is performed.
AES-17997	AES 7.1.x	Log Entry in /var/log/httpd/mod_jk.log. “init_jk::mod_jk.c (3591): mod_jk/1.2.46 initialized”
AES-17995	AES 7.1.3	The potentially vulnerable HTTP ‘DELETE’ and ‘OPTIONS’ method requests could be sent
AES-17870	AES 7.1.3	AES didn't send "Connection Clear" event to CTI application for service observer dropping off the call to observed party for the 2nd time.
AES-17864	AES 7.1.3	Huge amount of kernel martian logs were generated in alarm.log file
AES-17860	AES 7.x	The ‘avayadefaultsal’ SNMP trap receiver could not be deleted after database restore
AES-17738	AES 7.x	Listed log files (sssd_ldap_domain.log, sssd.log, sssd_nss.log, maillog, cron) do not have a correct log rotation configuration from the third-party RPMs, hence the file sizes may grow to a very large size.
AES-17565	AES 8.0	Alarm Viewer could not be seen on OAM due to conflict in hostname in /etc/hosts and /etc/hostname files.
AES-17347	AES 7.1.1	Running 'mvap.sh info' will show unexpected exceptions output.
AES-17338	AES 7.1	Snmpwalk on AES did not show information for TsapiLicense

Fixes in Application Enablement Services in Release 8.0.1

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms
AES-17873	AES 7.1 and above	AE Services failed to come online due to obsolete "/usr/java/default" softlink
AES-17850	AES 7.1.3 and above	Customer could not view alarm viewer page due to large trapVarbinds.log.1 file
AES-17676	AES 7.1.3 and above	TSAPI SDK compilation failed.

ID	Minimum Conditions	Visible symptoms
AES-17673	AES 7.1.2 and above	DST changes for Brazil time zone (2018)
AES-17667	AES 7.1.3	When ROOT CA cert was removed, and Tomcat restarted, the Tomcat did not come up.
AES-17633	AES 7.1.2	Port administration on OAM failed with exception.
AES-17579	AES 7.0.1	In a single step transfer scenario, when the transfer was completed the extension of the party that transferred the call was sent in the "Established" event" instead of the party that was being transferred.
AES-17562	AES 7.1.x	Tomcat localhost_access_log is not automatically clean up.
AES-17556	AES 8.0	On Dual stack server instead of default IPv4, default IPv6 Address will be displayed when server is deployed for the first-time using vSphere.
AES-17551	AES 7.1.2	On successfully importing security database, the data(table is not properly populated) is not visible on Devices page under Security tab.
AES-17550	AES 7.1	Restoring older backup on 7.1.x breaks OAM login
AES-17546	AES 8.0	Deploying AES 8.0 swonly through SMGRSDM caused the “Running Sanity Plugin” Step to fail
AES-17489	AES 8.0	When accessing embedded WebLM via AES 8.0 OAM, the version of WebLM showed as v7.1
AES-17460	AES 7.1.3	The pages on OAM that have auto refresh enabled (High Availability, Status -> Status and Control pages) redirects to crossSiteError page and logged out the user from the active session.
AES-17439	AES 7.1.2 and CM 7.x	"ANI_Reqd" field in AAR Analysis table could not be modified
AES-17352	AES 6.3.3	CSRF vulnerability made a user perform unintended operations on OAM while the user is authenticated on OAM.
AES-17351	AES 7.1	Failover did not work when FQDN is entered on the Network Configuration Page on OAM.
AES-17097	AES 7.1.1	WebLM IP address changed after removal of GRHA

Fixes in Application Enablement Services in Release 8.0

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms
AES-15539	AES 7.0.1 with libssh2-1.2.x library	SMS services stopped working after some time. The OSSICM process went into an inactive or a non-responsive state.
AES-16575	AES 6.3.3 and above	In case of CSTAFailed event, JTAPI SDK did not generate the necessary events due to missing deviceID

ID	Minimum Conditions	Visible symptoms
AES-16604	AES version: 6.3.3.7	When the TSAPI client initiated TSAPI request, it received a DUPLICATE INVOCATION REJECTION error response.
AES-16824		Under a very specific call scenario, the TSAPI service did not forward the CSTAClearConnectionEvent message to the application.
AES-16926	AES 7.1.2 and above with GRHA setup.	The HTTPD service failed to start after a session time out change on a GRHA configured AES setup.
AES-16942	AES 7.1.2	DB operation failed and provided undesired results on query.
AES-16968	AES-7.1.2	AES logs failed to rotate causing disk space to get full on heavy logging.
AES-16971	AES 7.1	AES and CM failed to connect after an AES interchange if mismatched hostname entries existed in CM and AES.
AES-16975	AES 6.3.3 and on wards with CM which did not have alarms enabled i.e. on logoff from sat, CM did not prompt for user input.	On a CM with alarms or busied out resources, the SAT logoff will generate "Proceed With Logoff" prompt. On a "clean" CM without the "Proceed With Logoff" prompt, it was observed that when the AES SMS invoked a Release, the OSSI connection between the AES and CM did not disconnect immediately.
AES-16998	AgentTerminal has Terminal Listener.	JTAPI Client did not send TERMINALLOGGEDOFFEVENT for TSAgent over the Terminal Listener to the application when the application logged off the agent successfully.
AES-17003	AES 7.1	Using the AES hostname as the FQDN while deployment caused alarming to fail
AES-17043	AES 7.1	When GRHA was removed from a system that previously used a Virtual IP to connect to the OAM, the OAM failed to connect to the primary server.
AES-17053	AES 7.1.2 and above.	The title tag on AES OAM showed the IP address of AES
AES-17054	Change DMCC logging to FINEST level and issue can be seen intermittently in case of high to moderate traffic run.	Logging on DMCC when set to FINEST intermittently resulted in a deadlock condition for log4j third party components. Causing the aesvcs service to become unresponsive. Workaround for this situation was to restart the aesvcs service or AES Server and change DMCC logs to FINE or FINER level.

ID	Minimum Conditions	Visible symptoms
AES-17100	AES 7.1.1 and above	Restarting the web server through OAM, eventually exhausted the maximum logging limit causing the AES OAM to display a limited menu when logged in as a "cust" user.
AES-17105	AES version: 7.1.1	The CTI application did not receive an agent change event from TSAPI in an unsupervised transfer scenario.
AES-17108	AES 6.x with CM 6.x	Owing to the existence of an ampersand in the field values on a CM, SMS failed to parse the string and returned a truncated string or an empty result.
AES-17245	7.1.2 with SMS transactions	Alarm.log when set to weekly rotation would greatly increase in size due to SMS logging when "VERBOSE" mode was set.
AES-17262	AES 7.1.3	After installation on KVM, the post installation configuration process required user input two times instead of one to proceed.
AES-17299	7.1.3 High Availability Configuration in Secure Mode	SSH connection failed.
AES-17313	Server or any alias certificate shall be added on AES.	Server certificate renew operation from OAM failed.
AES-17325	AES 7.1.1 and above	The "maxrepeat" field did not get disabled after the field "set enforce limit" was unchecked on PAM password manager page at OAM
AES-17330	AES 7.1.1 and above	The fields, "Enforce password limits" and "Failed login Response" on OAM Pam Password Manager screen could not be disabled
AES-17346	AES 7.1.2 and above and GRHA setup	GeoHA Virtual IP configured in Client connectivity (AE Service IP - Local IP) did not get synchronized with the standby
AES-17405	AES 7.0.1. onwards	The log files ossicm.log did not rotate
AES-17406	AES 7.1.3	Uppercase hostname was converted to lowercase when installed on VMware and KVM
AES-17410	AES 7.0.1 onwards	When modifying account via OAM, the following password policy rules fail: 'maxrepeat' and 'Number of previous passwords that cannot be reused'. Note: All password rules are applicable when modifying account via CLI.
AES-17413	SWOnly, AES prior to 8.0	The error ‘The ntp rpm is not installed’ was displayed when NTP options were modified

ID	Minimum Conditions	Visible symptoms
AES-17455	AES 7.1.3	PAM (Pluggable Authentication Module) "issue" messages were not displayed if configured through OAM.
AES-17463	AES with DMCC service used.	CSTA Delivered and CSTA Established event private data did not populate some required fields like trunkGroup, trunkMember and acdGroup information.

Avaya Aura® AVP Utilities

What’s new in AVP Utilities Release 8.0.x

What’s new in AVP Utilities Release 8.0.1

For more information see ***What’s New in Avaya Aura® Release 8.0.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101050420

Installation for Avaya Aura® AVP Utilities Release 8.0.x.x

Installation for Avaya Aura® AVP Utilities Release 8.0.1.2

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.

Download ID	Patch	Notes
AVPU0000013	**util_patch_8.0.1.2.0.04.zip**	File Size : Size:238 MB MD5 Checksum: 85188d8e4cb7cfb951f6fbff8ac89c21 Sha256sum : 0c6a018a31fae6517c70d48df6fdc46c2f669325da0df6997e56bef36ccdab1e

Installation for Avaya Aura® AVP Utilities Release 8.0.1.1

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.

Download ID	Patch	Notes
AVPU0000008	**util_patch_8.0.1.1.0.04.zip**	File Size: 232 MB (236,573 KB) MD5 Checksum: 5e9d4d1b56f49053049b6d88dda6f0a1 Sha256sum: 86cda3aba5ddf805daf6777a995e7b17595776cb4521e2957687b66041bfa76a

Installation for Avaya Aura® AVP Utilities Release 8.0.1

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.

Download ID	Patch	Notes
AVPU0000007	**util_patch_8.0.1.0.0.02.zip**	File Size: 182 MB (186,630KB) MD5 Checksum: 1294e7575a959e19b5c6de157d4e9c74 Sha256sum

Download ID	Patch	Notes
		869eed571a091319cfeaa786f49a1620cc24bb4512acb732783e053dfcea22c8

Installation for Avaya Aura® AVP Utilities Release 8.0

Please note that System Manager SDM or SDM Client is required to deploy AVP Utilities on AVP.

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

Download ID	Patch	Notes
AVPU0000004	AVPU-8.0.0.0.0.10-e60-16_OVF10.ova	File Size: 1,005.48 MB (1,029,610 KB) MD5 Checksum: eded106c4c5bef364b3e3cb1a4d62dbc

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 8.0** 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® 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 8.0.x

Fixes in AVP Utilities Release 8.0.1.2

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-319	AVPU 8.0 OVA deployed	126302 - RHEL 7 / 8 : vim (RHSA-2019:1619) (tcp)	8.0.1.1
AVPUTIL-315	AVPU 8.0 OVA deployed	[RHSA-2019:1587] Important/Sec. python.x86_64	8.0.1.1
AVPUTIL-313	AVPU 8.0 OVA deployed	[RHSA-2019:0368] Important/Sec. systemd-219-62.el7_6.5.x86_64	8.0.1.1
AVPUTIL-309	AVPU 8.0 OVA deployed	[RHSA-2019:1294] Important/Sec. bind-32:9.9.4-74.el7_6.1.x86_64	8.0.1.1
AVPUTIL-308	AVPU 8.0 OVA deployed	[RHSA-2019:0775] Important/Sec. java-1.8.0-openjdk-1:1.8.0.212.b04-0.el7_6.x86_64	8.0.1.1
AVPUTIL-307	AVPU 8.0 OVA deployed	[RHSA-2019:0679] Important/Sec. libssh2-1.4.3-12.el7_6.2.x86_64	8.0.1.1
AVPUTIL-306	AVPU 8.0 OVA deployed	[RHSA-2019:0483] Moderate/Sec. openssl-1:1.0.2k-16.el7_6.1.x86_64	8.0.1.1
AVPUTIL-304	AVPU 8.0 OVA deployed	[RHSA-2019:1228-01] Important: wget security update	8.0.1.1
AVPUTIL-302	AVPU 8.0 OVA deployed	[RHSA-2019:1481] Update kernel for RHEL7	8.0.1.1
AVPUTIL-294	AVPU 8.0 OVA deployed	[RHSA-2019:0818] Update kernel for RHEL7	8.0.1.1

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-275	AVPU 8.0 OVA Deployed	LOW [2.1] - 121452 - RHEL 7 : systemd (RHSA-2019:0201)	8.0.1
AVPUTIL-274	AVPU 8.0 OVA Deployed	MEDIUM [4.4] - 121528 - RHEL 7 : polkit (RHSA-2019:0230)	8.0.1
AVPUTIL-273	AVPU 8.0 OVA Deployed	MEDIUM [5.4] - 121451 - RHEL 7 : bind (RHSA-2019:0194)	8.0.1
AVPUTIL-272	AVPU 8.0 OVA Deployed	MEDIUM [6.8] - 121449 - RHEL 7 : kernel (RHSA-2019:0163)	8.0.1
AVPUTIL-271	AVPU 8.0 OVA Deployed	HIGH[7.5] - 121280 - RHEL 7 : perl (RHSA-2019:0109)	8.0.1
AVPUTIL-258	AVPU 8.0 OVA Deployed	Important: systemd security update (RHSA-2019:0049)	8.0.1
AVPUTIL-255	AVPU 8.0 OVA Deployed	Updated tzdata RPM (to tzdata-2018g) for timezone change fixes	8.0.1

ID	Minimum Conditions	Visible symptoms	Found in Release
AVPUTIL-254	AVPU 8.0 OVA Deployed	119172 - RHEL 7 : NetworkManager (RHSA-2018:3665) (tcp)	8.0.1
AVPUTIL-252	AVPU 8.0 OVA Deployed	108988 - RHEL 7 : gcc (RHSA-2018:0849) (tcp)	8.0.1
AVPUTIL-241	AVPU 8.0 OVA Deployed	118540 - RHEL 7 : fuse (RHSA-2018:3324) (tcp)	8.0.1
AVPUTIL-240	AVPU 8.0 OVA Deployed	118529 - RHEL 7 : wpa_supplicant (RHSA-2018:3107) (tcp)	8.0.1
AVPUTIL-239	AVPU 8.0 OVA Deployed	118726 - RHEL 7 : GNOME (RHSA-2018:3140) (tcp)	8.0.1
AVPUTIL-238	AVPU 8.0 OVA Deployed	118517 - RHEL 7 : wget (RHSA-2018:3052) (tcp)	8.0.1
AVPUTIL-237	AVPU 8.0 OVA Deployed	118520 - RHEL 7 : X.org X11 (RHSA-2018:3059) (tcp)	8.0.1
AVPUTIL-236	AVPU 8.0 OVA Deployed	118541 - RHEL 7 : libmspack (RHSA-2018:3327) (tcp)	8.0.1
AVPUTIL-235	AVPU 8.0 OVA Deployed	118514 - RHEL 7 : binutils (RHSA-2018:3032) (tcp)	8.0.1
AVPUTIL-234	AVPU 8.0 OVA Deployed	118538 - RHEL 7 : setup (RHSA-2018:3249) (tcp)	8.0.1
AVPUTIL-233	AVPU 8.0 OVA Deployed	118186 - RHEL 7 : java-1.8.0-openjdk (RHSA-2018:2942) (tcp)	8.0.1
AVPUTIL-232	AVPU 8.0 OVA Deployed	118532 - RHEL 7 : curl and nss-pem (RHSA-2018:3157) (tcp)	8.0.1
AVPUTIL-231	AVPU 8.0 OVA Deployed	118516 - RHEL 7 : gnutls (RHSA-2018:3050) (tcp)	8.0.1
AVPUTIL-230	AVPU 8.0 OVA Deployed	118523 - RHEL 7 : krb5 (RHSA-2018:3071) (tcp)	8.0.1
AVPUTIL-229	AVPU 8.0 OVA Deployed	118515 - RHEL 7 : python (RHSA-2018:3041) (tcp)	8.0.1
AVPUTIL-228	AVPU 8.0 OVA Deployed	118534 - RHEL 7 : openssl (RHSA-2018:3221) (tcp)	8.0.1
AVPUTIL-227	AVPU 8.0 OVA Deployed	118527 - RHEL 7 : glibc (RHSA-2018:3092) (tcp)	8.0.1
AVPUTIL-226	AVPU 8.0 OVA Deployed	118533 - RHEL 7 : sssd (RHSA-2018:3158) (tcp)	8.0.1
AVPUTIL-225	AVPU 8.0 OVA Deployed	118539 - RHEL 7 : jasper (RHSA-2018:3253) (tcp)	8.0.1
AVPUTIL-224	AVPU 8.0 OVA Deployed	118525 - RHEL 7 : kernel (RHSA-2018:3083) (tcp)	8.0.1
AVPUTIL-205	AVPU 8.0 OVA Deployed	[RHSA-2018:2123-01] Moderate: python security update	8.0.1

Fixes in AVP Utilities Release 8.0.1

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-198	AVPU 8.0 OVA Deployed	Patch update script does not start auto reboot timer till completion of rpm installations and not auto rebooting.	8.0
AVPUTIL-160	AVPU 8.0 OVA Deployed	Auditor swversion does not work	8.0

ID	Minimum Conditions	Visible symptoms	Found in Release
AVPUTIL-184	AVPU 8.0 OVA Deployed	add_spirit_certs support for non-FIPS mode was not working	8.0
AVPUTIL-211	AVPU 8.0 OVA Deployed	kernel_opts V3 support for L1TF 'Foreshadow' Speculative Execution	8.0
AVPUTIL-210	AVPU 8.0 OVA Deployed	[RHSA-2018:2748-01] Important: kernel security and bug fix update	8.0
AVPUTIL-200	AVPU 8.0 OVA Deployed	[RHSA-2018:2571-01] Important: bind security update (RHSA-2018-2570)	8.0
AVPUTIL-192	AVPU 8.0 OVA Deployed	[RHSA-2018:2285] Important: yum-utils security update	8.0
AVPUTIL-173	AVPU 8.0 OVA Deployed	[RHSA-2018:0666] Important: krb5 security update	8.0
AVPUTIL-169	AVPU 8.0 OVA Deployed	[RHSA-2018:1455] Important: dhcp security update	8.0
AVPUTIL-171	AVPU 8.0 OVA Deployed	[RHSA-2018:1649] Important: java-1.8.0-openjdk security update	8.0
AVPUTIL-209	AVPU 8.0 OVA Deployed	[RHSA-2018:2768-01] Moderate: nss security update	8.0
AVPUTIL-206	AVPU 8.0 OVA Deployed	[RHSA-2018:2123-01] Moderate: python security update	8.0
AVPUTIL-213	AVPU 8.0 OVA Deployed	[RHSA-2018:2181] Moderate: gnupg2 security update	8.0
AVPUTIL-212	AVPU 8.0 OVA Deployed	[RHSA-2018:2439] Low: mariadb security update	8.0
AVPUTIL-168	AVPU 8.0 OVA Deployed	[RHSA-2018:1852] Important: kernel security update	8.0
AVPUTIL-174	AVPU 8.0 OVA Deployed	[RHSA-2018:0805] Low: glibc security update	8.0
AVPUTIL-178	AVPU 8.0 OVA Deployed	[RHSA-2018:0980] Low: openssh security update	8.0
AVPUTIL-176	AVPU 8.0 OVA Deployed	[RHSA-2018:0849] Moderate: gcc security update	8.0
AVPUTIL-177	AVPU 8.0 OVA Deployed	[RHSA-2018:0855] Moderate: ntp security update	8.0
AVPUTIL-170	AVPU 8.0 OVA Deployed	[RHSA-2018:0913] Moderate: policycoreutils security update	8.0
AVPUTIL-175	AVPU 8.0 OVA Deployed	[RHSA-2018:1700] Moderate: procps-ng security update	8.0
AVPUTIL-167	AVPU 8.0 OVA Deployed	[RHSA-2018:0998] Moderate: openssl security update	8.0

Fixes in AVP Utilities Release 8.0

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-76	Initial Install	Extend SSH Timeout to allow for incorrect or inaccessible DNS Servers as originally implemented in Utility Services 7.1.3	8.0

ID	Minimum Conditions	Visible symptoms	Found in Release
AVPUTIL-113	Initial Install	Addition of Kernel Configuration Script as originally implemented in Utility Services 7.1.3	8.0

Known issues and workarounds in AVP Utilities Release 8.0.x.x

Known issues and workarounds in AVP Utilities Release 8.0.1.2

ID	Minimum conditions	Visible symptoms	Workaround
N/A			

Known issues and workarounds in AVP Utilities Release 8.0.1.1

ID	Minimum conditions	Visible symptoms	Workaround
N/A			

Known issues and workarounds in AVP Utilities Release 8.0.1

ID	Minimum conditions	Visible symptoms	Workaround
N/A			

Known issues and workarounds in AVP Utilities Release 8.0

ID	Minimum conditions	Visible symptoms	Workaround
AVPUTIL-160	Initial Install	The swversion command does not execute correctly for the Auditor user role.	The swversion command works correctly for the Administrator user role. This will be addressed in 8.0.1.

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 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)	File name	PLDS File ID	PCN/PSN

Avaya Aura Communication Manager Messaging	File name	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	File name	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, 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 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 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 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 prior to 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.	
MSG-22027	syslog messages could be lost if too many come from one process in too short a time period.	

ID	Visible symptoms	Release found in
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 local subscriber from remote reply-able ELA list for message 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 shutdown of messaging relying on 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	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	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 completely stop. Then, run *startapp -s Audix* to restart messaging.

Avaya Appliance Virtualization Platform

What's new in Avaya Appliance Virtualization Platform Release 8.0.1.2

For more information see *What's New in Avaya Aura® Release 8.0.x* document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101050420

Installation for Avaya Appliance Virtualization Platform Release 8.0.1.2

File list

Find patch information at https://support.avaya.com.

Download ID	Filename	File size	Notes
AVP00000046	avaya-avp-8.0.1.2.0.04.iso	512 MB (523,708 KB)	Use this ISO file for new AVP 8.0.1.2 installations. This ISO also contains the upgrade-avaya-avp-8.0.1.2.0.04.zip upgrade bundle.
AVP00000047	upgrade-avaya-avp-8.0.1.2.0.04.zip	214 MB (218,304 KB)	Use this ZIP file for upgrade from AVP 7.x, 8.0 or 8.0.x

What's new in Avaya Appliance Virtualization Platform Release 8.0.1.1

For more information see ***What's New in Avaya Aura® Release 8.0.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101050420

Installation for Avaya Appliance Virtualization Platform Release 8.0.1.1

File list

Find patch information at https://support.avaya.com.

Download ID	Filename	File size	Notes
AVP00000038	avaya-avp-8.0.1.1.0.06.iso	510 MB	Use this ISO file for new AVP 8.0.1 installations. This ISO also contains the upgrade-avaya-avp-8.0.1.1.0.06.zip upgrade bundle.
AVP00000039	upgrade-avaya-avp-8.0.1.1.0.06.zip	213 MB	Use this ZIP file for upgrade from AVP 7.x or 8.0 or 8.0.1

Installation for Avaya Appliance Virtualization Platform Release 8.0.1

File list

Find patch information at https://support.avaya.com.

Download ID	Filename	File size	Notes
AVP00000032	avaya-avp-8.0.1.0.0.08.iso	509 MB	Use this ISO file for new AVP 8.0.1 installations. This ISO also contains the upgrade-avaya-avp-8.0.1.0.0.08.zip upgrade bundle.
AVP00000033	upgrade-avaya-avp-8.0.1.0.0.08.zip	212 MB	Use this ZIP file for upgrade from AVP 7.x or 8.0.

Installation for Avaya Appliance Virtualization Platform Release 8.0

File list

Find patch information at https://support.avaya.com.

Download ID	Filename	File size	Notes
AVP00000027	avaya-avp-8.0.0.0.0.06.iso	507 MB	Use this ISO file for new AVP 8.0 installations. This ISO also contains the upgrade-avaya-avp-8.0.0.0.0.06.zip upgrade bundle.
AVP00000028	upgrade-avaya-avp-8.0.0.0.0.06.zip	211 MB	Use this ZIP file for upgrade from AVP 7.0.x or 7.1.x.

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 8.0.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

Installing the release

This release can be used as a new install of AVP 8.0.1 or as an upgrade to an existing AVP 7.x or 8.0 installation. For an upgrade, it will not be necessary to reinstall the guest VMs.

Please note that VMware ESXi 6.0 hypervisor on AVP 8.0.x uses about 1 GB of more memory than ESXi 5.5 did on AVP 7.0 – 7.1.0.1. If you're using Avaya Aura® System Manager Solution Deployment Manager 8.0.x or SDM Client 8.0.x to perform the upgrade to AVP 8.0.x, 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 8.0.x. 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.

Memory check when upgrading from AVP 7.0 – 7.1.0.1 to AVP 8.0.x:

- 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 > 1126 MB.
- If this value is < 1126 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.

Memory check when upgrading from System Platform 6.x to AVP 8.0.x:

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 > 3700 MB. If < 3700MB, 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 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 an 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 > 3700MB.
- If < 3700MB, then before being able to upgrade to AVP 8.0, either the memory of the server must be upgraded, or the server must be upgraded to a later generation.

If the memory check shows that extra memory is needed before upgrading to AVP 8.0.x, please refer to **PSN027060u Avaya Appliance Virtualization Platform Release 8.0 Memory Upgrade Instructions** 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 8.0.x** and **Upgrading Avaya Aura Appliance Virtualization Platform Release 8.0.x** documents for instructions on new installs and upgrades of AVP. Be sure to upgrade SDM to Release 8.0.x first before using it to upgrade AVP.

Restoring software to previous version

Back up the application Virtual 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 8.0.1 to AVP 8.0:

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.

Fixes in Avaya Appliance Virtualization Platform Release 8.0.x.x

Fixes in Avaya Appliance Virtualization Platform 8.0.1.2

Note: AVP 8.0.1 is based on VMware ESXi 6.0, Releasebuild-10719132.

ID	Minimum Conditions	Visible symptoms	Found in Release
AVP-896	AVP upgraded from any previous versions	After upgrade from AVP 8.0.1.1 to AVP 8.0.1.2 Dell R630 show disk status degraded	8.0.1.1

ID	Minimum Conditions	Visible symptoms	Found in Release
AVP-868	AVP 7.1.3.3 installed	SYS_FAULT alarm was getting generated on AVP 7.1.3.3 and later	7.1.3.3
AVP-838	AVP 8.0.x installed on HP or Dell system	On a fresh install of AVP, the command ‘esxcli storage device list’ showed the main raid disk status degraded.	AVP 8.0.1 or AVP 8.0.1.1
AVP-824	AVP 7.1.3.4 or later installed	AVP Shutdown/Reboot powered off VMs resulting in VM disk corruption	AVP 7.1.3
VMSA-2019-0005	AVP 7.1.2 or later installed	See VMware security advisory VMSA-2019-0005.1 at https://www.vmware.com/security/advisories/VMSA-2019-0005.html	AVP 7.1.2 or later
VMSA-2019-0008	AVP 7.1.2 or later installed	See VMWare security advisory VMSA-2019-0008.1 at https://www.vmware.com/security/advisories/VMSA-2019-0008.html	AVP 7.1.2 or later

Fixes in Avaya Appliance Virtualization Platform 8.0.1.1

Note: AVP 8.0.1 is based on VMware ESXi 6.0, Releasebuild-10719132.

ID	Minimum Conditions	Visible symptoms	Found in Release
AVP-712	AVP installed on Dell 630	DISK_FAULT alarms are cleared only after graceful reboot	7.1.3
AVP-739	AVP 7.0.x	Upgrade failed from AVP 7.0.1.0.0.5 to AVP 7.1.3 or later due to limited bootbank space	7.1.3
AVP-741	AVP 7.1.x on Dell hardware	Updated utilities for Dell RAID hardware.	8.0

Fixes in Avaya Appliance Virtualization Platform 8.0.1

Note: AVP 8.0.1 is based on VMware ESXi 6.0, Releasebuild-10719132.

ID	Minimum Conditions	Visible symptoms	Found in Release
AVP-643	AVP 7.1.2, 7.1.3 or 8.0 on Avaya S8300E Server	The S8300E front panel shutdown button and the LEDs (Application, Active and Alarm LEDs) do not function.	7.1.2, 7.1.3, 8.0
AVP-653	Upgrade AVP to 7.1.3 or 8.0	Upgrade to AVP 7.1.3 or 8.0 fails with the message “Error Code-GENERIC_ERROR:: AVP Patch Installation Failed”	7.1.3, 8.0
AVP-666	Installing AVP 7.1.3 or 8.0 on an Equinox spec’d server	When installing AVP 7.1.3 or 8.0 on an Equinox-spec’d server, it does not accept upper-case ‘Y’ or ‘N’ at the following prompt: "Equinox deployment option is available to this system. Do you want to configure the system using this option? [Y]es/[N]o"	7.1.3, 8.0

ID	Minimum Conditions	Visible symptoms	Found in Release
VMSA-2018-0012.1	Avaya Appliance Virtualization Platform 7.x or 8.0	See VMware Security Advisory VMSA-2018-0012.1 for details. http://www.vmware.com/security/advisories/VMSA-2018-0012.html	7.x, 8.0
VMSA-2018-0018	Avaya Appliance Virtualization Platform 7.x or 8.0	See VMware Security Advisory VMSA-2018-0018 for details. http://www.vmware.com/security/advisories/VMSA-2018-0018.html	7.x, 8.0
VMSA-2018-0020	Avaya Appliance Virtualization Platform 7.x or 8.0	See VMware Security Advisory VMSA-2018-0020 for details. http://www.vmware.com/security/advisories/VMSA-2018-0020.html This VMware update includes L1TF mitigations. See the above VMSA and Avaya PSN027074u for information on possible performance impacts and enabling the mitigation for the concurrent-context attack vector.	7.x, 8.0
VMSA-2018-0027	Avaya Appliance Virtualization Platform 7.x or 8.0	See VMware Security Advisory VMSA-2018-0027 for details. http://www.vmware.com/security/advisories/VMSA-2018-0027.html	7.x, 8.0
ESXi600-201807001	Avaya Appliance Virtualization Platform 7.1.2, 7.1.3 or 8.0	See VMware patch release notes for VMware ESXi 6.0, Patch Release ESXi600-201807001 (53627)	7.1.2, 7.1.3, 8.0

Fixes in Avaya Appliance Virtualization Platform 8.0

None.

Note: Appliance Virtualization Platform 8.0 provides the same Spectre and Meltdown remediation's that were included with Appliance Virtualization Platform 7.1.3. AVP 8.0 is based on VMware ESXi 6.0, Releasebuild-7967664.

Known issues and workarounds in Avaya Appliance Virtualization Platform Release 8.0.x

Known issues and workarounds in Avaya Appliance Virtualization Platform Release 8.0.1.2

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

ID	Minimum conditions	Visible symptoms	Workaround
AVP-803	AVP 7.1.1 or later	AVP syslog.log and Utility Services remote.log filling with 'handler could not derive port number' messages	The messages can be disabled on AVP Utilities 8.0.1.2 by Avaya representative.
AVP-784	AVP 7.1.3 or later on HP G8 Nd G9 systems	AVP experiencing RAID battery failure alarms. (Fixed by BIOS upgrade)	The alarm is gone after upgrading the BIOS provided by Avaya to the latest GA version.

ID	Minimum conditions	Visible symptoms	Workaround
AVP-734	AVP 7.1.3 or later on HP systems	AVP showed redundancy lost on single power supply systems	The messages can be disabled on AVP Utilities 8.0.1.2 by Avaya representative.
AVP-750	AVP installed on S8300 cards	“list config media-gateway” executed from CM shows empty data on S8300E and S8300D for Suffix, HW vintage and firmware vintage. EG: S8300X HW00 FW00.	None

Known issues and workarounds in Avaya Appliance Virtualization Platform Release 8.0.1.1

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

ID	Minimum conditions	Visible symptoms	Workaround
AVP-767	AVP Installed and try updating weblmurl	Seg fault when trying to set weblmurl	Please escalate a case to Avaya Services.
AVP-706	AVP 7.1.3 and HP DL360 G8 or G9 servers	An HP DL360 G8 or G9 server with a single power supply may incorrectly show degraded redundant power supply status: POWER_FAULT,Power Supply 3 Power Supplies,POWER_FAULT, MAJ	Ignore the alarm.
AVP-750	AVP installed on S8300 cards	“list config media-gateway” executed from CM shows empty data on S8300E and S8300D for Suffix, HW vintage and firmware vintage. EG: S8300X HW00 FW00.	This is a cosmetic issue and does not impact functionality.
AVP-707	AVP installed on S8300D cards	S8300D thermal interrupt floods vmkwarning log	None
AVP-747	AVP installed on HP hardware	RAID battery failure alarms on HP gen 8 and gen 9	None
AVP-656	AVP installed.	AVP syslog.log and US remote.log filling with handler could not derive port number messages	None

Known issues and workarounds in Avaya Appliance Virtualization Platform 8.0.1

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

ID	Minimum conditions	Visible symptoms	Workaround
AVP-157	Initial installation of Avaya	When Out of Band Management network is set to “yes,” VMNIC are not set	Ensure you have the correct network setup prior to installing AVP. Ensure Ethernet connections are to the correct networks. If

ID	Minimum conditions	Visible symptoms	Workaround
	Appliance Virtualization Platform 8.0	up correctly. If you run the command esxcli network vswitch standard list from SSH on AVP after OOBM is set to yes, port group “Public” should be attached to vSwitch0 and “Out of Band Management” port group should be connected to vSwitch2. When OOBM is set to no, “Public” and “Out of Band Management” port groups are both attached to vSwitch0. If this setup is not present the installation has encountered an error and should be re-attempted ensuring networks are currently connected at deployment time. See deployment documentation for further details.	the networks are connected incorrectly and IP traffic is seen on the incorrect interface by the server during installation, the AVP network setup may not be done correctly and the installation will need to be done again.
AVP-410	AVP 8.0 with duplicate IP address in the subnet	Cannot change the IP address of the AVP if there is a duplicate IP address on the subnet.	Follow the directions in the VMware Knowledge Base https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1020647
AVP-429	Attended installation of AVP 8.0	Cannot administer IPv6 address using the firstboot.sh script during an attended installation.	Use the kickstart generator and use the USB key to install AVP 8.0 with an IPv6 address or administer IPv6 address using System Manager SDM or AVP CLI command “/opt/avaya/bin/set_dualstack enable”
AVP-466	Enabling OOBM via CLI command on AVP 8.0	Enabling Out-of-Band Management (OOBM) via the CLI command ‘/opt/avaya/bin/set_oobm enable’ may display the following error message although the command was successful: “Error performing operation: Sysinfo error on operation returned status: Bad parameter. See the VMkernel log for detailed error information"	This error message can be ignored if the next line shows “Out of Band Management is now enabled on the host”.
AVP-704	Dell R630 server with AVP 7.x or 8.0.x.	On a Dell R630 server DISK_FAULT alarms are generated after an	Perform a graceful shutdown/reboot of the server.

ID	Minimum conditions	Visible symptoms	Workaround
		ungraceful shutdown or reboot.	
AVP-706	AVP 7.1.3 and HP DL360 G8 or G9 servers	An HP DL360 G8 or G9 server with a single power supply may incorrectly show degraded redundant power supply status: POWER_FAULT,Power Supply 3 Power Supplies,POWER_FAULT, MAJ	Ignore the alarm.
AVP-739	Upgrade from AVP 7.x to AVP 8.0.1	In rare cases, upgrade of AVP from 7.x to 8.0.1 may fail due to the bootbank running out of space on the ESXi host.	See PSN027076u – Avaya Aura® Appliance Virtualization Platform Upgrade Failures.
ESXi 6.0 Update 3	Active Directory is enabled on AVP	Active Directory settings are not retained post-upgrade. The Active Directory settings configured in the ESXi host before upgrade are not retained when the host is upgraded to ESXi 6.0. See VMware ESXi 6.0 release notes for details: https://docs.vmware.com/en/VMware-vSphere/6.0/rn/vsphere-esxi-60u3-release-notes.html	1. Logon to the AVP host using the VMware Embedded Host Client via a web browser. Use the local management IP address of the AVP host in the following URL: https://<AVP host IP address>/ui If necessary, enable access to the VMware vSphere Host Client … • Logon to AVP host using an SSH client. • Note: Ensure SSH enabled, see Enable SSH Access for AVP Host section. • Enter the local management IP address of the AVP host. • Logon using admin or another Administrator user. Execute the following command on the AVP CLI: `/opt/avaya/bin/set_ehc enable` Logon using user admin or another Administrator user. 2. Where previously defined, confirm that the Active Directory domain is configured for the host and if not, configure this: In the left-hand Navigator window, select Manage under Host. In the central Manage window, select the Security & Users tab. Select Authentication Click on the Join domain link and ensure the following configuration data is defined (where applicable):

ID	Minimum conditions	Visible symptoms	Workaround
			• Domain Name: <Active Directory Domain Name> • Use authentication proxy: <tick box> • User name: <user name> • Password: <password> Click on the Join domain button.
General issues and workarounds			If watching an Avaya Appliance Virtualization Platform (AVP) installation via a monitor Note the following: A message about the scratch partition will appear briefly in red after which the screen will go black for 10 minutes while the installation continues. This is expected, and no action should be taken. After the black screen the system will reboot, and the installation will continue. When the CD is ejected, remove the CD and the USB stick and the installation will continue. If the installation continues to show a black screen after 30 minutes, the AVP network setup may not be correct and will need to be re-installed. Verify that the correct values were used to generate the kickstart file, check the USB stick and re-attempt the installation.
General issues and workarounds			The Avaya Appliance Virtualization Platform (AVP) End User License Agreement (EULA) must be accepted and Enhanced Access Security Gateway EASG selection made by logging into the AVP via an SSH client. If virtual machine deployments are attempted prior to accepting the EULA and making EASG selection, the deployments will fail. The VMs will not power on failing the deployment flow.
General issues and workarounds			After the EULA is accepted, SSH to AVP will be disabled after 24 hours and activation after that is via the onboard AVP Utilities VM or via SDM.
General issues and workarounds			If the system is to be set with Out of Band Management, the AVP host should be installed with Out of Band Management on or should be set to use Out of Band Management before VMs are deployed. When Out of Band Management is enabled on the host, all VMs must be set up to use Out of Band Management.
General issues and workarounds			It is always required to deploy an AVP Utilities VM with AVP. AVP Utilities provides key alarming and security functions to the AVP host and is mandatory to deploy.

ID	Minimum conditions	Visible symptoms	Workaround
General issues and workarounds			Snapshots are not generally supported for AVP and should only be present as part of applying an update via SDM. If a snapshot is left on an AVP system, it is detrimental to system performance and over time will use up all the available disk space. As such, it is important to ensure that snapshots are not left on the AVP system for an extended period and should be removed at the earliest opportunity. Snapshots can be viewed and removed using the Solution Deployment Manager Snapshot Manager function.

Known issues and workarounds in Avaya Appliance Virtualization Platform 8.0

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

ID	Minimum conditions	Visible symptoms	Workaround
AVP-157	Initial installation of Avaya Appliance Virtualization Platform 8.0	When Out of Band Management network is set to "yes," VMNIC are not set up correctly. If you run the command esxcli network vswitch standard list from SSH on AVP after OOBM is set to yes, port group "Public" should be attached to vSwitch0 and "Out of Band Management" port group should be connected to vSwitch2. When OOBM is set to no, "Public" and "Out of Band Management" port groups are both attached to vSwitch0. If this setup is not present the installation has encountered an error and should be re-attempted ensuring networks are currently connected at deployment time. See deployment documentation for further details.	Ensure you have the correct network setup prior to installing AVP. Ensure Ethernet connections are to the correct networks. If the networks are connected incorrectly and IP traffic is seen on the incorrect interface by the server during installation, the AVP network setup may not be done correctly and the installation will need to be done again.
AVP-410	AVP 8.0 with duplicate IP address in the subnet	Cannot change the IP address of the AVP if there is a duplicate IP address on the subnet.	Follow the directions in the VMware Knowledge Base https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1020647

ID	Minimum conditions	Visible symptoms	Workaround
AVP-429	Attended installation of AVP 8.0	Cannot administer IPv6 address using the firstboot.sh script during an attended installation.	Use the kickstart generator and use the USB key to install AVP 8.0 with an IPv6 address or administer IPv6 address using System Manager SDM or AVP CLI command "/opt/avaya/bin/set_dualstack enable"
AVP-466	Enabling OOBM via CLI command on AVP 8.0	Enabling Out-of-Band Management (OOBM) via the CLI command '/opt/avaya/bin/set_oobm enable' may display the following error message although the command was successful: "Error performing operation: Sysinfo error on operation returned status: Bad parameter. See the VMkernel log for detailed error information"	This error message can be ignored if the next line shows "Out of Band Management is now enabled on the host".
AVP-643	AVP 8.0 on Avaya S8300E Server	The S8300E front panel shutdown button and the LEDs (Application, Active and Alarm LEDs) do not function.	For the shutdown button, please shutdown the server using Solution Deployment Manager, AVP ESXi command line, or VMware Embedded Host Client. For LED workaround, please check status from Communication Manager.
AVP-653	Upgrade AVP to 8.0	Upgrade to AVP 8.0 fails with the message "Error Code-GENERIC_ERROR::AVP Patch Installation Failed"	Restart the ESXi management agent from the Direct Console User Interface (DCUI) or restart the hostd service using AVP CLI command "/etc/init.d/hostd restart" and then retry the AVP update. See VMware KB article for more info: https://kb.vmware.com/s/article/1003490
AVP-666	Installing AVP 8.0 on an Equinox spec'd server	When installing AVP 8.0 on an Equinox-spec'd server, it does not accept upper-case 'Y' or 'N' at the following prompt: "Equinox deployment option is available to this system. Do you want to configure the system using this option? [Y]es/[N]o"	Use lower-case 'y' or 'n'.
ESXi 6.0 Update 3	Active Directory is enabled on AVP	Active Directory settings are not retained post-upgrade. The Active Directory settings configured in the ESXi host before upgrade are not retained when the host is upgraded to ESXi 6.0. See VMware ESXi 6.0 release notes for details: https://docs.vmware.com/en/VMware-	1. Logon to the AVP host using the VMware Embedded Host Client via a web browser. Use the local management IP address of the AVP host in the following URL: https://<AVP host IP address>/ui If necessary, enable access to the VMware vSphere Host Client: • Logon to AVP host using an SSH client.

ID	Minimum conditions	Visible symptoms	Workaround
		vSphere/6.0/rn/vsphere-esxi-60u3-release-notes.html	• Note: Ensure SSH enabled, see Enable SSH Access for AVP Host section. • Enter the local management IP address of the AVP host. • Logon using admin or another Administrator user. Execute the following command on the AVP CLI: `/opt/avaya/bin/set_ehc enable` Logon using user admin or another Administrator user. 2. Where previously defined, confirm that the Active Directory domain is configured for the host and if not, configure this: In the left-hand Navigator window, select Manage under Host. In the central Manage window, select the Security & Users tab. Select Authentication Click on the Join domain link and ensure the following configuration data is defined (where applicable): • Domain Name: <Active Directory Domain Name> • Use authentication proxy: <tick box> • User name: <user name> • Password: <password> Click on the Join domain button.
General issues and workarounds			If watching an Avaya Appliance Virtualization Platform (AVP) installation via a monitor Note the following: A message about the scratch partition will appear briefly in red after which the screen will go black for 10 minutes while the installation continues. This is expected, and no action should be taken. After the black screen the system will reboot, and the installation will continue. When the CD is ejected, remove the CD and the USB stick and the installation will continue. If the installation continues to show a black screen after 30 minutes, the AVP network setup may not be correct and will need to be re-installed. Verify that the correct values were used to generate

ID	Minimum conditions	Visible symptoms	Workaround
			the kickstart file, check the USB stick and re-attempt the installation.
General issues and workarounds			The Avaya Appliance Virtualization Platform (AVP) End User License Agreement (EULA) must be accepted and Enhanced Access Security Gateway EASG selection made by logging into the AVP via an SSH client. If virtual machine deployments are attempted prior to accepting the EULA and making EASG selection, the deployments will fail. The VMs will not power on failing the deployment flow.
General issues and workarounds			After the EULA is accepted, SSH to AVP will be disabled after 24 hours and activation after that is via the onboard AVP Utilities VM or via SDM.
General issues and workarounds			If the system is to be set with Out of Band Management, the AVP host should be installed with Out of Band Management on or should be set to use Out of Band Management before VMs are deployed. When Out of Band Management is enabled on the host, all VMs must be set up to use Out of Band Management.
General issues and workarounds			It is always required to deploy an AVP Utilities VM with AVP. AVP Utilities provides key alarming and security functions to the AVP host and is mandatory to deploy.
General issues and workarounds			Snapshots are not generally supported for AVP and should only be present as part of applying an update via SDM. If a snapshot is left on an AVP system, it is detrimental to system performance and over time will use up all the available disk space. As such, it is important to ensure that snapshots are not left on the AVP system for an extended period and should be removed at the earliest opportunity. Snapshots can be viewed and removed using the Solution Deployment Manager Snapshot Manager function.

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 8.0.x.x

What's new in G430 and G450 Media Gateways Release 8.0.x

For more information see ***What's New in Avaya Aura® Release 8.0.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101050420

Installation for Avaya Aura® G430 and G450 Media Gateways Release 8.0.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 8.0.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 8.0.x.y.

If you attempt to download Release 8.0.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 8.0.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.
- In Release 8.0.x.y 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 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 use of like gateway firmware series and Communication Manager releases. This means the latest version within the GW Firmware Series are recommended with the following Communication Manager software releases:

Gateway Firmware Series	Communication Manager Release
33.xx.xx	6.3
34.xx.xx	6.3.2
35.xx.xx	6.3.5
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

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 prior to 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 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 goes end of manufacturer support, gateway firmware series 33.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.

- Inads, dadmin, craft or a customer login that has been enabled for system maintenance.

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 8.0.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 8.0.x.y.

If you attempt to download Release 8.0.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 8.0.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.
- In Release 8.0.x.y 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.

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 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 8.0.x.x

Fixes in G430 and G450 Media Gateways Release 8.0.1.2 (Builds 40.31.00 and 40.31.30)

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.	7.1.3.3

Fixes in G430 and G450 Media Gateways Release 8.0.1.1 (Builds 40.25.00 and 40.25.30)

ID	Minimum Conditions	Visible symptoms	Found in Release
CMG4XX-1335	G430v3 Restore	Performing a restore of a backup on a G430v3 did not restore the TLS certificates.	7.1.3.2

ID	Minimum Conditions	Visible symptoms	Found in Release
CMG4XX-1343	G430, G450 M3K, DS1, V.150 Viper IP Phone	When an M3K system is connected to a gateway by way of DS1 trunk and an IP-Viper to IP-Viper call is placed over that DS1 trunk, it might fail to go secure when initiated from the G450 side.	7.1
CMG4XX-1353	G430, G450 V.150 Viper IP Phone	Reduced the time it takes for IP Viper to go secure during v.32 modem session establishment	7.1.3.3
CMG4XX-1398	G430, G450 Non-existent username	Sometimes an invalid, not existent user was listed in the ‘show username’ output after an ‘nvram init’ command. It was cleared after a ‘copy running-config startup-config’ command.	7.1.3
CMG4XX-1412	G430, G450 telnet and ssh	A read-only user can now run the ‘show ip telnet’, ‘show ip ssh’ CLI commands, previously reserved for administrators.	6.3.10
CMG4XX-1418	G430v3 DSPs and reset	On rare occasions after a G430v3 reset, one MP120 DSP core may not be allowed into service	7.1.3.3
CMG4XX-1423	G430v3 SLA Monitor Agent	The G430v3 did not support the Avaya SLAMON network monitoring traffic.	7.1.3.3
CMG4XX-1360	G430, G450	Improvements have been made in V.32 modem and secure-phone session establishment and tolerance to longer than expected V.32 AC signals.	7.1.3.2

Fixes in G430 and G450 Media Gateways Release 8.0.1.0 (Builds 40.20.00 and 40.20.30)

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Found in Release
CMG4XX-1104	G430/G450 SNMP	The cmgVoipTotalChannelsEnforcedbyCM SNMP Object ID (OID) is now a supported in the G430 and G450 MIB. Previously, any combination of SNMP commands attempting to get a response from the cmgVoipTotalChannelsEnforcedbyCM object ID (.1.3.6.1.4.1.6889.2.9.1.4.10) would fail.	7.0.1
CMG4XX-1131, CMG4XX-1153	G430/G450 V.150 Viper IP Phones	Fixed an issue with Viper IP secure phones responding to V.32 modem answer tone too quickly. This resulted in the far-end not always being able to initiate a secure session. The gateway now detects when this behavior occurs and correspondingly institutes a V.32 recommended delay in the AA response when needed.	6.3.17
CMG4XX-1148, CMG4XX-1167	G430/G450 Clock Sync Over IP (CSOIP)	Clock sync failures could occur if CM requests a codec that performs silent suppression when establishing Clock Sync over IP (CSoIP) communication between master and slave gateways. The gateway will now override codec requests that should not be used for CSoIP and will now select an appropriate codec to be used instead.	6.3.17
CMG4XX-1164	G430/G450 V.150 Viper IP Phones	Fixed an issue where IP Viper to IP Viper V.150 calls might not go secure when using a specific service provider's media-path having longer than 100ms round-trip delay.	6.3.18

ID	Minimum Conditions	Visible symptoms	Found in Release
CMG4XX-1180	G430/G450 Security Scans	Fixed an issue where Nessus Security Scan were causing the gateway to reset as a result of TCP sockets being exhausted.	7.1.3
CMG4XX-1206	G430/G450 Announcements, SCP	Fixed an issue where uploads or downloads of announcements using scp would fail if a ssh login banner is present.	6.3.16
CMG4XX-1006	G430/G450 Camp-on-busy-out	Performing a "campon-busyout voip-dsp" would immediately busy-out the DSP and cause all active calls using that DSP to be dropped. This would occur when there is only one DSP installed or if all the channels on all other DSPs are completely in use or busied-out.	6.3.14
CMG4XX-1018	G430/G450 with MP-160 DSP	In rare cases, an MP160 DSP core would fail when an SRTCP encrypted packet was received in an unexpected format. When an unexpected packet was received, the core would become unavailable and a reset of the DSP was required to resolve the problem.	7.0.1.3
CMG4XX-1063	G430/G450	Improvements were made for calls using V.150 in V.32 mode in the presence of long round trip delay. A long round trip delay would prevent secure-sessions to be established when the far-end tries to initiate a secure session.	6.3.16
CMG4XX-1216	G430, G450	A sixth party may now be added to a Service Observed call.	7.1.3
CMG4XX-1231	G430, G450 FTP	In rare cases, FTP transfer failures caused by network impairments could cause a gateway to reset.	6.3.14
CMG4XX-1262	G430, G450	Fan Faults were not being displayed by the “show faults” CLI command.	6.1.13
CMG4XX-1300	G430, G450	In rare cases, MP160 and MP120 DSP hardware failures still appear to be in service.	7.1.2
CMG4XX-1279	G430, G450	A 64-bit SNMP request to OID 1.3.6.1.2.1.31.1.1.1.6 was returning a 32-bit response (with lowest 32 bits as zero) instead of a 64-bit response.	7.0.1.3
CMG4XX-1296	G430, G450	v.32 modem rekey success rate has been improved by making it more tolerant of DC signal bias.	7.1.3.2

Fixes in G430 and G450 Media Gateways Release 8.0 (Builds 40.10.00 and 40.10.30)

Note: There are no fixes listed here since this is the first release.

Known issues and workarounds in G430 and G450 Media Gateways Release 8.0.x.x

Known issues and workarounds in G430 and G450 Media Gateways

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 single VLAN interface with IPv6.
hw090790	G430, G450 EM_WEB doesn't work via dial in session (usb modem).	Use another network interface, such as the PMI, for connecting to Embedded Web.

Languages supported

- English

Documentation errata

- None

Avaya Aura® Media Server

For latest information refer to Avaya Aura® Media Server Release 8.0 Release Notes on the Avaya Support site at: https://downloads.avaya.com/css/P8/documents/101053837

Avaya Aura® WebLM

What's new in Avaya Aura® WebLM for 8.0.x

What's new in Avaya Aura® WebLM for 8.0.x

For more information see ***What's New in Avaya Aura® Release 8.0.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101050420

Installation for Avaya Aura® WebLM

Installation for Avaya Aura® WebLM Release 8.0.1.2

Download ID	Artifacts	Notes
SMGR8012GA3	WebLM 8.0.1.2 GA Patch Bin	Verify that the MD5 checksum for the downloaded file matches the number on the Avaya PLDS website. File Name: WebLM_8.0.1.2_r80130087.bin File Size: 358 MB MD5 Checksum:ec89dbb5b2054bf12d4b182bc8557d7e

Installation for Avaya Aura® WebLM Release 8.0.1.1

Download ID	Artifacts	Notes
SMGR8011GA3	WebLM 8.0.1.1 GA Patch Bin	Verify that the MD5 checksum for the downloaded file matches the number on the Avaya PLDS website. File Name: WebLM_8.0.1.1_r80119268.bin File Size: 354 MB MD5 Checksum: 54d698520b58f59040106b2d25848d2f

Installation for Avaya Aura® WebLM Release 8.0.1

Download ID	Artifacts	Notes
SMGR8010GA3	WebLM 8.0.1 GA Patch Bin	Verify that the MD5 checksum for the downloaded file matches the number on the Avaya PLDS website. File Name: WebLM_8.0.1.0_r801008761.bin File Size: 332 MB MD5 Checksum: dae9a82030aca2537c5f7d44ecb012a2

Installation for Avaya Aura® WebLM Release 8.0

Download ID	Artifacts	Notes
SMGR80GA007	WebLM 8.0 GA OVA	Verify that the MD5 checksum for the downloaded file matches the number on the Avaya PLDS website. File Name: WebLM-8.0.0.0.9-31370-e65-14.ova File Size: 1373 MB MD5 Checksum: 593597508ec8a21c61293b3f9688473f
SMGR80GA008	WebLM AWS OVA 8.0 GA OVA	Verify that the MD5 checksum for the downloaded file matches the number on the Avaya PLDS website.

Download ID	Artifacts	Notes
		File Name: WebLM-8.0.0.0.9-31370-AWS-13.ova File Size: 1403 MB MD5 Checksum: 88e83cb2d4cfc6c02aa52a425cad5ae2
SMGR80GA009	WebLM KVM OVA 8.0 GA OVA	Verify that the MD5 checksum for the downloaded file matches the number on the Avaya PLDS website. File Name: WebLM-8.0.0.0.9-31370-KVM-13.ova File Size: 1391 MB MD5 Checksum: 55b7496744d774a9f17fe974ffacd5a3
SMGR80GA011	WebLM 8.0 Software Only	Verify that the MD5 checksum for the downloaded file matches the number on the Avaya PLDS website. File Name: AvayaAuraWebLM_8.0.0.0.9-31370_13.iso File Size: 265 MB MD5 Checksum: f5d3337d4f75142ced0e33701190e896

Installing the release 8.0.x

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 host name.

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, 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 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.
   - IP address is changed: If 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 of 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 7.5
Java	OpenJDK version "1.8.0_191" 64-bit
Application Server	WildFly AS 10.1.0
Supported Browsers	Internet Explorer 11.x
	Firefox 59, 60, 61

- Download *Deploying standalone Avaya WebLM on VMware* from Avaya Support Site for WebLM on VMware installation and upgrade.

Troubleshooting the installation

Collect logs and other information as specified below and contact support team.

- The status of the WebLM software. If the software is an upgrade, then the release from which the software is upgraded.

Execute 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 8.0

For any problems with WebLM 8.0, 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 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 Aura® WebLM on VMWare for 8.0.x

Fixes in Avaya Aura® WebLM on VMWare for 8.0.1.2

The following table lists the fixes in this release:

ID	Description
SMGR-49313	(RHSA-2019:1481) Important: kernel security update
SMGR-49304	(RHSA-2019:1168) Important: kernel security update
SMGR-49298	(RHSA-2019:1235) Important: ruby security update
SMGR-49290	(RHSA-2019:1228) Important: wget security update
SMGR-49282	(RHSA-2019:1294) Important: bind security update
SMGR-49277	(RHSA-2019:0775) Important: java-1.8.0-openjdk security update
SMGR-48757	(RHSA-2019:0818) Important: kernel security and bug fix update
SMGR-48597	(RHSA-2019:0710) Important: python security update
SMGR-48532	(RHSA-2019:0435) Moderate: java-1.8.0-openjdk security update
SMGR-48525	[RHSA-2019:0483) Moderate: openssl security and bug fix update
SMGR-48518	(RHSA-2019:2019:0512) Important: kernel security, bug fix, and enhancement update
SMGR-48511	(RHSA-2019:0368) Important: systemd security update
SMGR-48482	(RHSA-2019:0679) Important: libssh2 security update
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-48569	Provide a command line utility (importCACertificate) to add certificates to trust store. Refer Admin guide for more details on utility usage.

Fixes in Avaya Aura® WebLM on VMWare for 8.0.1.1

The following table lists the fixes in this release:

ID	Description
SMGR-47921	Provide script (configureTLS) to disable TLS 1.0 for WebLM port 52233
SMGR-47971	When attempting to install a valid license on System Manager, getting an error "Solution License can be installed through Collector only"
SMGR-47549	(RHSA-2018:3651) Moderate: kernel security, bug fix, and enhancement update
SMGR-47421	(RHSA-2018:3059) Low: X.org X11 security, bug fix, and enhancement update
SMGR-48001	kernel (RHSA-2019:0163)
SMGR-48002	perl (RHSA-2019:0109)
SMGR-48003	NetworkManager (RHSA-2018:3665)
SMGR-48004	systemd (RHSA-2019:0204)

ID	Description
SMGR-48006	curl and nss-pem (RHSA-2018:3157)
SMGR-48007	ruby (RHSA-2018:3738)
SMGR-48008	bind (RHSA-2019:0194)
SMGR-48009	polkit (RHSA-2019:0230)

Fixes in Avaya Aura® WebLM on VMWare for 8.0.1

The following table lists the fixes in this release:

ID	Description
SMGR-47110 / SMGR-47138	Added back the support for the deprecated “renewAll” API call from older WebLM clients
Various	RHEL security updates for following advisories: RHSA-2018:2181, RHSA-2018:2242, RHSA-2018:2384, RHSA-2018:2439, RHSA-2018:2570, RHSA-2018:2748, RHSA-2018:2768, RHSA-2018:2942, RHSA-2018:3032, RHSA-2018:3041, RHSA-2018:3050, RHSA-2018:3052, RHSA-2018:3071, RHSA-2018:3083, RHSA-2018:3107, RHSA-2018:3158, RHSA-2018:3221, RHSA-2018:3249, RHSA-2018:3324, RHSA-2018:3327, RHSA-2018:3408
SMGR-46084 / SMGR-47204	/var/log/ partition going full due to inadequate log rotation
SMGR-46860	changeIPFQDN does not work properly for -dns option
SMGR-46078	User craft cannot execute swversion command
SMGR-44904	[Customer Issue] In System Manager enterprise WebLM configuration, "Usage by WebLM" does not show the local PC timezone

Fixes in Avaya Aura® WebLM on VMWare for 8.0

The following table lists the fixes in this release:

ID	Description
SMGR-44855	“weblm_password reset” CLI command does not work in standalone WebLM 7.1.1
SMGR-44427	Previous version of WebLM C++ client does not work with standalone WebLM 7.1.2 due to different configuration of Tomcat 9

Known issues and workarounds in Avaya Aura® WebLM for 8.0.x

Known issues and workarounds in Avaya Aura® WebLM for 8.0.1.2

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

ID	Visible symptoms	Workaround
SMGR-45891	Change IPFQDN script giving extra Usage information in WebLM Standalone	None

Known issues and workarounds in Avaya Aura® WebLM for 8.0.1.1

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

ID	Visible symptoms	Workaround
SMGR-45891	Change IPFQDN script giving extra Usage information in WebLM Standalone	None

Known issues and workarounds in Avaya Aura® WebLM for 8.0.1

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

ID	Visible symptoms	Workaround
SMGR-45891	Change IPFQDN script giving extra Usage information in WebLM Standalone	None

Known issues and workarounds in Avaya Aura® WebLM for 8.0

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

ID	Visible symptoms	Workaround
SMGR-45891	Change IPFQDN script giving extra Usage information in WebLM Standalone	None

Avaya Device Adapter Snap-in

What's new in Avaya Device Adapter Snap-in for 8.0.1.0.25

For more information see ***What's New in Avaya Aura® Release 8.0.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101050420

Installation for Avaya Device Adapter Snap-in for 8.0.1.0.25

Refer to Avaya Device Adapter Snap-in Reference Guide for installation instructions.

https://downloads.avaya.com/css/P8/documents/101050717

Download ID	Artifacts	Notes
ADA0000004	DeviceAdapter-8.0.1.0.25.svar	MD5: F13276FFA53B83C31CE0B261828AACCC

Fixes in Avaya Device Adapter Snap-in for 8.0.1.0.25

ID	Problem
SETADAPT-5563	Avaya Device Adapter services are not up due to corrupted crontab on Breeze profile #2
SETADAPT-5637	BSM PPM caching is not working for languages
SETADAPT-3026	Phone display mess of dialed numbers when dial number then press key call-appr more times
SETADAPT-3050	EC500 desk phone does not ring when make call from Aura Sip user
SETADAPT-3175	Bridged key at button 0 does not ring for incoming calls.
SETADAPT-3233	Incoming call to call-appr line on 2d KEM does not work.
SETADAPT-3240	Call-appr key ring instead of bridge key when Unistim phones bridge SCA to non-CS1000 phones.
SETADAPT-4370	All Unistim phones display "Call Forward canceled" when register to ADA.
SETADAPT-5081	No Speech path when Avaya Device Adapter user uses codec G.729A for Unistim sets
SETADAPT-5227	Cannot answer the call by lifting the handset in case of two simultaneous incoming calls when key 0 is silent ringing bridge appearance and key 1 is silent ringing call appearance
SETADAPT-5641	Calling party number and name are not displayed on phone if there is incoming call to bridge appearance (MADN scenario))
SETADAPT-5654	The call on first line of analog phone is not automatically restored when remote party on second line ends the call
SETADAPT-5671	The bridged key does not display CLID for incoming calls.

ID	Problem
SETADAPT-1225	Added old CS1000 commands: activeDlogShow, dnldFailShow and inactiveDlogShow
SETADAPT-4195	PD coredump may occur while executing "pdShow" command during phones traffic registration
SETADAPT-4340	Implement endpointUnlockSCPW <TN | Extension>
SETADAPT-4344	TPS crashes during execution of "isetShow <phone_IP>" command for two phones registered behind NAT and having same IP
SETADAPT-4399	Corrected work of dsetDelayHookswitchSet command
SETADAPT-5059	DST (Daylight Saving Time) change did not take effect for all Avaya Device Adapter phones
SETADAPT-5481	1210/1230 phones are not automatically updating time on display when DST period ends
SETADAPT-5519	1110/1120 phones are not automatically updating time on display when DST period ends
SETADAPT-5521	DST: 2001/2002 phones are not automatically updating time on display when DST period ends
SETADAPT-3444	Cache endpoint configuration data in Cluster DB (aka BSM PPM cache)
SETADAPT-5730	MEDIA SECURITY (MSEC): User with always enabled Media Security able make successful unsecure call to user with disabled Media Security
SETADAPT-5639	Log of received SIP-messages printed truncated
SETADAPT-4349	Personal Directory does not update Caller list when Caller number has a plus
SETADAPT-4955	SCPW password guessing protection mechanism is working incorrectly for "Change Protection Mode" menu. After 4-th input attempt it wasn't be blocked.
SETADAPT-2545	Added QoS support for voice & control DSCP.
SETADAPT-5754	QoS: Can't save attributes after enabling/disabling "VoIP Monitoring Manager IP address" attribute
SETADAPT-5673	All phones hang after changing the bridged phone from SCA to MCA, and vice versa
SETADAPT-5505	Cannot make call by Speed dial from List 1 of Abbreviated Call Dialing (List 1 would be very commonly used in the field) from Unistim sets
SETADAPT-5776	Insecure call is established when MSBT user transfers active call with MSNV user to MSAW user
SETADAPT-5775	Bridged appearance line is ringing in case of MSNV-MSAW call

Known issues and workarounds for Avaya Device Adapter Snap-in for 8.0.1.0.25

ID	Problem	Workaround
SETADAPT-5855	Whole system is stuck after FORCED upgrade of 3904 phone with established call (edge case, not usual to do this with established call)	Not recommended to initiate firmware upgrade for sets out of maintenance time. In case if this situation happened in order to recover recommended: case 1: restart dsa under cust/root user in Breeze CLI: ~]# dasrvstart stop dsa ~]# dasrvstart start dsa In case 1 system will be recovered quicker than in case 2. case 2: or start/stop snapin via SMGR: Elements -> Avaya Breeze -> Service Management -> Services.
SETADAPT-5846	No Speech path when Avaya Device Adapter digital user uses codec G.729A	Not recommended to use G.729A codec.
SETADAPT-5845	Codec G.723 does not work on MGC (Speech path is ok, as system instead selects codec G.711)	Not recommended to use G.723 codec
SETADAPT-5841	Intermittent issue. Cannot swap Primary Cluster of MGC from Cluster has multiple servers to Cluster has 1 server, that cause that MGC can’t be migrated without reconfig and reboot.	Login on MGC in ldb shell under pdt2 user and run mgcsetup, after it reboot MGC.
SETADAPT-5840	When the SIP i/f (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 SIP i/f (TLAN) for Active Load Balancer Breeze server recovers then manually reboot all MGCs.
SETADAPT-5839	If there are some stuck jobs in the database, then there might be issues with importing Media Gateway xml file to SMGR	- Go to SMGR CLI and remove your 'PENDING EXECUTION' related jobs from bulkimportstatus table in database. root >mgmtia avmgmt=> select * from bulkimportstatus; avmgmt=> delete from bulkimportstatus where id=...; - Clear all the ‘Import Users’ job-related data from the DB (below mentioned tables) and run the ‘Import Application System’ job. 1. sched_job_status_type 2. sched_job_type_args 3. sched_job_type_params 4. sched_job_types

ID	Problem	Workaround
SETADAPT-5831	CS1000 MGC cannot be upgraded to Avaya Device Adapter MGC version without additional manual steps as mentioned in workaround section. These manual steps are not required when upgrading Avaya Device Adapter to newer Avaya Device Adapter release.	• Go to SMGR: Elements -> Avaya Breeze -> Configuration -> Attributes and click Service Cluster tab • Select appropriate Breeze cluster and Device Adapter snapin. Turn off "Enable legacy loadware upgrades" and press commit • Turn off "Enable SSH access on Secure Link" and press commit Wait a minute to make sure Breeze receives information from SMGR • Turn on "Enable SSH access on Secure Link" and press commit Turn on "Enable legacy loadware upgrades" and press commit
SETADAPT-5826	RTCP statistics for MGC calls are not forwarded to SMGR	No
SETADAPT-5823	Call Appearance icon on the set remains in winking state after hold/unhold operation.	No
SETADAPT-5781	Phone is stuck for a couple of minutes after making call to a call-appr assigned to KEM 2. The phone automatically recovers without manual intervention.	DO NOT assign call-appr to KEM 2.
SETADAPT-5638	Avaya Device Adapter Unistim and Digital users do not keep last forwarded number for Call Forward All Calls feature	No
SETADAPT-5199	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	Cannot add an existing Adhoc conference (for example, a three-party conference on AURA that involves Device Adapter Phones) into an Equinox MeetMe conference	Each individual Device Adapter user that needs to connect to the Equinox MeetMe conference needs to dial into the Equinox MeetMe conference
SETADAPT-5833	User cannot clear Speed Call feature on CM Endpoint Profile Page from SMGR	Use Edit Endpoint on Search User from Users->User Management -> Manage Users page
SETADAPT-5773	After you change the default MGC password then you cannot ever change it to a blank password.	No
SETADAPT-5704	Incoming call to call-appr line on 2nd KEM does not work	DO NOT assign call-appr to KEM 2.
SETADAPT-5688	One of possible cause for "Unable to retrieve MGC list" errors on Dashboard may be an issue with failed nginx service on Breeze server.	Check that problematic Breeze have created /var/cache/nginx/. If not, then create it and restart nginx service manually.
SETADAPT-5601	No Call Park RECALL for analog phones	No

ID	Problem	Workaround
SETADAPT-5163	SMGR allows to add any model phones in the same card. This is misconfiguration.	Admin should check it manually. On Breeze may be used tnInfo tool to see what loop-shelf-card is used by digital, analog or Unistim sets. ipeShow command should be used to get info about configure cards.
SETADAPT-4378	If there is 'Synchronization Failure' on Breeze in Replication page in Breeze in SMGR, that can be due to SMGR running out of space in /var/log.	Go to /var/log/Avaya/mgmt/drs/errordump under root on SMGR and remove .dump files
SETADAPT-3474	When admin edit/view an existing user station, and update the CM profile through user management, admin may get a blank screen and can't get expected results	Issue with search mechanism in SMGR UI. As workaround it's possible to change TN (without loss any data) via Manage Element menu item.
SETADAPT-2761	Autodial programming is not working on 2nd KEM	Not recommended to use autodial on 2nd KEM.

Avaya Device Adapter General Limitations for 8.0.1.0.25

- SMGR, SM, CM, AMS, Breeze server installation and initialize configuration must be ready to use. Refer to these product release notes for more information.

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 dialing plan, 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 any more. Automatically it will be set to Secure/SIP IP address of the Breeze server (in case of single server) or in case if using multiple Breeze servers within a cluster, the NODE IP automatically map 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 prior to 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 **SVAR** file of the new Device Adapter.

In this case SMGR will display a pop-up message about necessity to restart Device Adapter when a user updates the attributes. The "Signaling Security Error" message is displayed on IP Deskphone display during registration process.

Following items should be checked:

1. 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.

This change cause changes in upgrade procedure - need to uninstall GA version and install SP1 version to Upgrade.

```
# 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 (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 CA Root certificate, then it continues registration using DTLS after the 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 the brief period of insecure. In case of certificates 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 case of certificates 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
```

5. 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".

6. In case for 2050 CA certificate should be installed into Trusted Root Certification Authorities->Local Machine. By default, 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 (e.g. PuTTY) and use SERIAL connection with settings below:

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.

   Upgrade from #1392 load or less to #1444 should be done only via manual upgrade procedure. See item 3.2

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 **Automatic MGC Loadware upgrade from prev load**. Automatic upgrade supported only from #1317 snapin(Avaya Device Adapter Ph2 Beta load)

1. Sometimes auto-upgrade is not started (please raise ticket if you see it), so to start auto upgrade for MGC - it should be rebooted. For this need to login on MGC in ldb shell and run **reboot** command.
2. After it upgrade procedure will be started automatically and at the end of this procedure MGC will be rebooted finally.

3.3 **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. File name 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_0, CS1k-2col_DEFAULT_CM_8_0, CS1k-39xx_DEFAULT_CM_8_0 or CS1k-ana_DEFAULT_CM_8_0** 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 (key map is presented)

From Breeze side: dsaShell dsaShow

From Breeze side - IPE card status with: ipeStatus <loop> <shelf> <card> <unit>

If your DLC card is still blink red, just remove card from 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 IPsec configuration procedure and **reboot**.
- To stop IPsec, run the following command:
  - Disable checkbox at Breeze attributes.
  - i**ssDecom** at MGC

Corporate Directory (AADS) configuration

For activation of Corporate directory necessary:

- Set CRPA flag in feature field on phone;
- Configure AADS server (and LDAP server) on SMGR;
- Enable AADS server for cluster or global and fill URL and port for AADS server.

Creating and configuration of users on LDAP.

For used Corporate Directory necessary to create user on LDAP server with the next parameters: login and password should be as extension for user.

Device Adapter Limitations

There is no method to migrate customer setting for Call Forward feature.
Current Device Adapter does not support:

- Malicious Call Trace feature for all types of sets.
- Ring Again for analog and digital sets.

Avaya Device Adapter Feature Interaction Limitations for 8.0.1.0.25

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 8.0.1.0.25

Product	Release Details
Avaya Aura® System Manager	8.0.1
Avaya Aura® Session Manager	8.0.1
Avaya Aura® Communication Manager	8.0.1
Avaya Aura® Media Server	8.0.0.173
Avaya Breeze	3.6

Avaya Aura® Device Services

For latest information refer to Avaya Aura® Device Services Release 7.1.x Release Notes on the Avaya Support site at: https://downloads.avaya.com/css/P8/documents/101045822