Avaya Aura® 7.0.1.2 Release Notes

Release 7.0.1.2

Issue 2

January 2017

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

© 2015-2017 Avaya, Inc.

All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, https://support.avaya.com/LICENSEINFO, UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. 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.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.

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

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Change history

Date	Description
01/30/2017	Added information about Equinox Conferencing 9.0 Support.
12/20/206	Added section for Avaya Aura® Device services.
12/14/2016	Redesigned the Product Release Matrix – vertical flow.
12/07/2016	Updated Notices.
11/02/2016	Changed the file name from avaya-avp-7.0.0.0.0.21.zip to avaya-avp-7.0.0.0.0.21.iso in the File List table for Avaya Appliance Virtualization Platform.
10/10/2016	Added Communication Manager fixes for 7.0.1.1.1.
08/08/2016	The fourth release of the cumulative Avaya Aura® 7.0.1.1 release.
05/9/2016	The third release of the cumulative Avaya Aura® 7.0.1 release.
04/13/2016	Added a new Product Release Matrix table in the *Introduction* section.
04/11/2016	Added a table to the Compatibility section with columns for Version, Product and Description.
02/05/2016	The second release version of the cumulative Avaya Aura® 7.0.0.2 release.
12/21/2015	The first release version of the cumulative Avaya Aura® 7.0.0.0 and 7.0.0.1 release.

Introduction

This document provides late-breaking information to supplement Avaya Aura® 7.0.0.0, 7.0.0.1, 7.0.0.2 (service packs), 7.0.1 (feature pack), 7.0.1.1 (service pack) and 7.0.1.2 (service pack) 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.

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	**Release Number**						
	7.0.1.2.0	**7.0.1.1.0**	**7.0.1.0.0**	**7.0.0.3.0**	**7.0.0.2.0**	**7.0.0.1.0**	**7.0.0.0.0**
Avaya Aura® Communication Manager	X	X	X	X	X	X	X
Avaya Aura® Session Manager	X	X	X	NA	X	X	X
Avaya Aura® System Manager	X	X	X	NA	X	X	X
Avaya Aura® Presence Services	NA	X	X	NA	NA	X	X
Avaya Aura® Application Enablement Services	NA	X	X	NA	NA	NA	X
Avaya Aura® Utility Services	X	X	X	NA	NA	X	X
Avaya Aura® Communication Manager Messaging	NA	NA	NA	NA	NA	NA	X
Avaya Appliance Virtualization Platform	X	X	X	NA	NA	NA	X
Avaya Aura® G430 & G450 Media Gateways	X	X	X	NA	NA	X	X
Avaya Aura® WebLM on VMWare	X	X	X	NA	X	X	X
Avaya Aura® Device Services	X	First release					

Avaya Aura® Media Server Releases

Avaya Aura® Release	**Corresponding Avaya Aura® Media Server Release**
7.0.1.2.0	7.7.0.375 (FP1 SP2)
7.0.1.1.0	7.7.0.359 (FP1 SP1)
7.0.1.0.0	7.7.0.334 (FP1)
7.0.0.3.0	NA
7.0.0.2.0	7.7.0.292 (SP3)
7.0.0.1.0	7.7.0.281 (SP2)
7.0.0.0.0	7.7.0.236 (SP1)

What’s new in Avaya Aura®

What’s new in Avaya Aura® 7.0.0.0

The following table lists enhancements in this release.

Product	Enhancement	Description
Session Manager	SNMP Automatic Alarm Clearing for Avaya Aura® Session Manager Alarms	Currently, when an alarm is cleared in Session Manager there is no notification sent out via SNMP. This requires alarms to be manually cleared on systems monitoring Session Manager. With Release 7.0, Session Manager will automatically send a SNMP notice when an alarm has been cleared. This functionality applies to all alarms within Session Manager. This capability will ensure accurate reporting of response times for alarm clearing in SLA agreements.
Session Manager	Avaya Aura® Session Manager SIP Message Compaction	SIP by nature is an extensible protocol. Often, new enterprise features, particularly the ones for which no known standard/IETF mechanisms exist, results in the introduction of proprietary SIP headers and/or parameters using the SIP extension model. Avaya uses these SIP extensions from time to time to introduce Avaya proprietary headers/parameters for new features. Even though these extensions are correct as per SIP standards, customers have reported problems where a particular third-party SIP element could not handle the SIP messages from Avaya Aura® elements. It could be because the length of the full SIP message is too large and/or particular header(s) is too big to handle for a particular SIP element. In the past, in such conditions, customers had to find a way to deal with these incompatibilities. By adding a capability in Session Manager that removes the headers non-Avaya elements may not need, Avaya Aura® customers will be able to achieve better interoperability without needing assistance of third-party elements. This capability will be a part of the adaptation modules of Session Manager.
Session Manager	Avaya Aura® Session Manager Emergency Call Notification to an Adjunct Emergency Location Server	Emergency Notification partners have started offering advanced crisis-alert features to enterprise customers. In large campus type settings, advanced applications (using LED displays near the main entrances, as an example) guide the emergency crew to the right location of the emergency call origination. To accomplish this capability, these applications need to know the location of the emergency caller. Applications use the following capabilities exposed by the Avaya Aura® components for this purpose: Session Manager shares the IP address (which is used to compute the location) of the user’s SIP devices; Communication Manager shares the identity of the emergency caller. With the introduction of MDA (Multiple Device Access), a single user can register from multiple devices. This introduces an issue when establishing the exact location of the emergency caller. As part of the Emergency Call processing, Communication Manager notifies the identity of the emergency caller to the emergency application. However, because the caller has multiple devices registered, the

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Product	Enhancement	Description
		emergency application cannot establish the exact location from where the user initiated the emergency call. Enhancements in this release to the existing Session Manager AELS (Adjunct Emergency Location Server) will provide the specific device used by the user so more accurate location information can be determined.
Session Manager	Avaya Aura® Session Manager Maintenance Mode State	To support deployment and maintenance of large amounts of Branch Session Manager (BSM)s, a non-operational SM or BSM can be set to "Maintenance Mode". For consistency purposes both Core and Branch Session Managers will support "Maintenance Mode". An operational SM or BSM being set to "Maintenance Mode" is effectively taking a SM or BSM out of service. For complete details of the Avaya Aura® Session Manager 7.0 release, see the Avaya Aura® 7.0 Solution Offer Definition on the Avaya Sales Portal.
Session Manager	End To End Encryption Indicator	Session Manager and Communication Manager now support the ability for SIP end-points and clients (that support End to End Encryption Indicator) to display an indication that tells the end user whether the signaling and the media is secure end-to-end. The initial offer will only support SIP endpoint/clients on intra-enterprise point to point calls. This feature will be supported on the 96x1 SIP and the 1x-Communicator SIP soft client.
Presence Services	Presence Services (PS) is now deployed as a Snap-in on Engagement Development Platform (EDP) 3.1.	Presence Services is now delivered as a Snap-in application on Avaya Engagement Development Platform 3.1. All other deployment models have been deprecated (software-only, System Platform, Avaya Appliance Virtualization Platform).
Presence Services	Active – Active High Availability	The Presence Services High Availability (HA) feature now operates in active/active mode (it was active/standby in previous releases). The advantage of active/active is that service to the endpoints is not interrupted in the event of a nodal failure which results in a switchover of users to the standby nodes.
Presence Services	Support PS to PS federation with clustered deployments	Federation between presence systems is now possible even with clustered deployments. Previously the Presence Services (PS) to Presence Services federation feature was only available with single node deployments. As of release 7.0 it is now possible to federate clustered PS deployments.
Presence Services	Block IMs between users with different tenant IDs	In release 7.0 it is now possible to block the exchange of IMs between users who have different tenant IDs. This allows the deployment of multi-tenant solutions where each group of tenants is isolated from each other.
Presence Services	Improved capacity	It is now possible to scale a Presence Services solution to 250K users. In release 7.0 you can deploy 2 clusters (clusters must be federated to each other) of 125K users for a total of 250K users on a single Presence Services deployment.
Presence Services	Presence Services	Presence Services is now compatible with solutions using MDA.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Product	Enhancement	Description
	supported in Multi Device Access (MDA) solutions	Refer to the MDA whitepaper for further details at: https://downloads.avaya.com/css/P8/documents/100181252 Note that for MDA deployments the Presence Services application will support an average of 1.4 devices per user. For example, if the system is configured with 1000 users it can support up to 1400 devices. This means that 400 of the 1000 users can have 2 devices each or 200 of the 1000 users can have 3 devices each, and so on. On average, the system cannot have note than 1.4 devices per user.
Presence Services	Simplified administration for Lync Federation	Previously, for Lync integration, the administrator was required to enter/administer the PS handle of the Avaya Aura® users twice: once as the Avaya Presence/IM (formerly XMPP) handle and the second time as the Avaya SIP handle. The duplicate administration was required for proper routing of the Lync originated subscription and IM requests. PS 7.0.0 removes the need for duplicate administration of the PS handle.
Application Enablement Services		Out of band management
Application Enablement Services		Detect unreachable SIP endpoints and logout unreachable SIP agents
Application Enablement Services		Support Solution Deployment Manager (SDM) common services to enable VMware®
Application Enablement Services		Support VMware® for Avaya Appliance Virtualization Platform (AVP) for the appliance model
Utility Services		Utility Services supports both VMware Enablement (VE) and Avaya Appliance Virtualization Platform (AVP) deployments. AVP replaces System Platform in Avaya Aura® 7.0.
Utility Services		• Utility Services must be deployed if Avaya Appliance Virtualization Platform (AVP) is being used as the Host. When Utility Services is deployed on AVP, it provides the following features: ○ AVP Alarming and Log Harvesting. Utility Services acts as a proxy for AVP in generating alarm messages. This means that Utility Services needs to be deployed with a valid System Manager IP Address and Enrollment Password for the registration process to complete successfully; ○ Services Port access to AVP and all deployed Virtual Machines. Avaya's System Platform supported an internal routing mechanism that allowed a Services Laptop connected to the System Platform server to be able to connect to any deployed virtual machine. Such a mechanism does not exist in AVP. So Utility Services now supports an internal routing capability that emulates the System Platform feature.

Product	Enhancement	Description
		Enabling of SSH Access to AVP. Shell access to AVP is strictly controlled and enabled on a limited time window bases. Utility Services enables this feature.
Utility Services		Based on CentOS V6.6 – the previous release was based on CentOS V5.
Utility Services		IP Phone Firmware is now no longer included by default.
Utility Services		Addition of the Auditor Role – this new role on the VMware version emulates the previous Auditor role on the System Platform release. This user is able to browse many features of Utility Services, but is prohibited from making any changes.
Utility Services		Support for Utility Services specific Authentication File. The previous release of Utility Services supported a generic System Platform authentication file that could be installed on System Platform itself. Utility Services now supports its own authentication file.
Utility Services		Utility Services now supports a Deployment Mode. Utility Services can be initially deployed in one of three modes – it is not possible to change the mode after deployment: • Full Functionality - This mode supports all standard Utility Services features as well as AVP Alarming and Log Harvesting, and the Services Port feature. This is also the default deployment mode. • Utility Services Only -This mode supports all of the standard Utility Services features, but AVP Alarming and Log Harvesting, and the Services Port feature are disabled. This is designed for deployment on non-AVP hardware and must not be used with AVP Services Port Only- This mode only supports AVP Alarming and Log Harvesting and the Services Port feature. All of the standard Utility Services features are disabled. This mode also has a minimal set of firewall rules.
Utility Services		Addition of Out of Band Management (OOBM) Mode - Utility Services support OOBM to allow the Services Port Feature to access deployed Avaya Virtual Machines by either their Public or OOBM IP Address. The OOBM Mode allows this element to be enabled or disabled – the default being disabled. AVP also supports OOBM and Utility Services. However, the OOBM Mode must match AVP, i.e. they should both be either enabled or disabled.
Communication Manager Messaging		The CMM 7.0 release has been enhanced to support software currency and interoperability with the Avaya Aura® 7.0 solution.
Communication Manager Messaging		The Linux OS has been updated to version 6.
Communication Manager Messaging		The CMM application has been integrated with Avaya Appliance Virtualization Platform and Solution Deployment Manager.

Product	Enhancement	Description
Communication Manager Messaging		The CMM application has been updated to support the Avaya SIP Reference Architecture and Security guidelines for encryption protocols.
Media Gateways	hw140170	G430, G450 AES-256 media encryption support for voice, data, video. AES-256 is managed in the "Media Encryption" field of Communication Manager's ip-codec-set form.
Media Gateways	CMG4xx-234	G430, G450 Encrypted SRTCP bearer control channel support. Encrypted SRTCP is managed in the "Encrypted SRTCP" field of the Communication Manager's ip-codec-set form.
Media Gateways	CMG4xx-304	G430, G450 Online Certificate Status Protocol (OCSP) support has been added as an alternative certificate validation technique to Certificate Revocation Lists (CRLs). The following certificate-option commands have been added to support X.509 Certificate validation using OCSP: **set ocsp-validation [yes | no**] - Enables or disabled OSCP certificate validation. **set ocsp-local-url [url]** - Sets the URL to be used when validating a certificate using OCSP (default is no url). **set ocsp-url-precedence [certificate | local]** - Sets whether the certificate URL or the local URL should be used first whenever a certificate is validated using OCSP (default is certificate). Also, the "show certificate-options" command has been updated to display the setting of the above OCSP options.
Media Gateways	CMG4xx-265	G430, G450 Greenwich Mean Time (GMT) Time zone offset awareness added to provide greater accuracy when validating certificate expiration.
Media Gateways	hw140178	G430, G450 SHA-2 signed certificates supported for firmware images downloaded to the gateway.
Media Gateways	CMG4xx-251	G430, G450 Out Of Band Management Interface support added for VLAN and Fast-ethernet. OOB management includes the addition of the following new CLI commands: **oob-interface** - Configures the interface as an Out of Band Management interface. **no oob-interface** - Removes the out of band management interface. **show oob-interface** - Displays the out-of-band management interface. **set non-oob access <disable|enable>** - Disables and enables management access to the in-band network connection. Also, the "**show interface**" command has been updated to include information for OOB for VLAN and Fast-ethernet.
Media Gateways	hw140126	G430, G450 Gateway login password policy has been enhanced. The date and time of the last login and the number of login failures is now displayed on the console every time a user logs onto the gateway. In addition, the following new CLI commands have been added: **login authentication password-no-change-interval <hours>** - Set the number of hours before a password can be changed again

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Product	Enhancement	Description
		(default 24). **Login authentication passwords-don't-reuse command <n-passwords>** - set the number of previous passwords that cannot be reused (default 1).
Media Gateways	CMG4xx-338	G430, G450 TLS upgraded to include support of TLS version 1.2. SSLv2 and SSLv3 are no longer supported.
Media Gateways	CMG4xx-233	G430, G450 OpenSSL upgraded to version 1.0.1L.
Avaya Aura® WebLM on VMWare	WebLM migrated from Oracle JDK to OpenJDK 1.7 update 79 64-bit.	Infrastructure Updates.
Avaya Aura® WebLM on VMWare	Support for CentOS 6.5 and Apache Tomcat 8.0.18.	EULA.
Avaya Aura® WebLM on VMWare	Support for display and logging of EULA Acceptance.	Avaya Appliance.
Avaya Aura® WebLM on VMWare	Support for installing WebLM 7.0 OVA on the Avaya Appliance Virtualization Platform (AVP) that is being introduced in Avaya Aura® 7.0 as part of the Avaya-Provided Appliance.	Hosted Cloud Deployment.

What's new in Avaya Aura® 7.0.0.1

The following table lists enhancements in this release:

Product	Enhancement	Description
Session Manager	Increased capacity for SIP Users/Devices on a Single BSM	Branch Session Manager will support a maximum of 5000 SIP Users/Devices per instance. In an appliance model, BSM shall support 1000 SIP users/devices (on the S8300E) and 5000 SIP users/devices (on CSR2 and beyond or equivalent).
Session Manager	Increased capacity with a Single System Manager to 500 BSMs	A single System Manager will support up to 500 Branch Session Managers - This will still require at least two Communication Managers (250 max per CM).
System Manager	Security	In keeping with NIST guidelines and industry best practices, Avaya is rotating the security keys associated with remote maintenance access through the Avaya Security Gateway (ASG).
Avaya Aura® WebLM on VMWare	Security	In keeping with NIST guidelines and industry best practices, Avaya is rotating the security keys associated with remote maintenance

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Product	Enhancement	Description
		access through the Avaya Security Gateway (ASG).

What's new in Avaya Aura® 7.0.0.2

The following table lists enhancements in this release.

Product	Enhancement	Description
Communication Manager	SIP Endpoints Display	Ref. ID **CM-4468** - Endpoint Display and call log prefixed with an international or national format based on SIP endpoint or Multiple Device Access (MDA) location.
Media Gateways Release 7.0.0.2, build 37.21.30 – Russia only	CMG4xx-430	G430, G450 A separate firmware build with VPN disabled was created (Build 37.21.30 – for Russia only).
Media Server	Installation updates	Media Server update 7.7.0.292 now available.
		System Layer update 7.7.0.15 now available.
Session Manager	None	Fixes and new known issues listed.
WebLM	Installation updates	• Ref. ID SMGR7002002. WebLM 7.0.0.2 software now available. • Instructions for upgrading to 7.0.0.2 listed. • Fixes and new known issues listed.
System Manager	Installation updates	• Ref. ID SMGR7002001. System Manager 7.0.0.2 software now available. • Instructions for upgrading to 7.0.0.2 listed. • Fixes and new known issues listed.

The following products are up-to-date as of 7.0.0.1, and no further updates are required:

- Avaya Aura® Presence Services.
- Avaya Aura® Application Enablement Services.
- Avaya Aura® Utility Services.
- Avaya Aura® Communication Manager Messaging.
- Avaya Appliance Virtualization Platform.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

What’s new in Avaya Aura® 7.0.1

See *What's New in Avaya Aura® Release 7.0.1* (book number: 03-601818).

What’s new in Avaya Aura® 7.0.1.1

Product	Enhancement	Description
Avaya Aura®	Microsoft® Windows 10 support.	Solution Deployment Manager client supports Microsoft Windows 10, 64-bit Professional or Enterprise operating system.
Communication Manager	SIP Endpoints Display.	Ref. ID **CM-4468** - Endpoint Display and call log prefixed with an international or national format based on SIP endpoint or Multiple Device Access (MDA) location.
Communication Manager	All systems with IP endpoints.	Ref. ID **CM-10850 -** The CM-SAT (Communication Manager-System Access Terminal) command "list registered-ip-stations" will now display the type of socket used, TLS or TCP, for endpoint registrations.
Communication Manager	All systems with IP endpoints.	Ref. ID **CM-10851 -** The CM-SAT (Communication Manager-System Access Terminal) command "status socket-usage" will now display information on TLS sockets being used for endpoint registrations.
Communication Manager	Interop between CM & CS1K UNIStim endpoints.	Ref. ID **CM-7103 -** SRTP calls will work between CM and CS1K using UNIStim endpoints.
Communication Manager	Use of the "list trace button" SAT command when two stations need to be traced simultaneously.	Ref. ID **CM-9025 -** The "list trace button" SAT (System Access Terminal) command did not allow two endpoints to be traced.
System Manager - Element Manager	Officelinx 10.1 support.	None.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

What’s new in Avaya Aura® 7.0.1.2

Product	Enhancement	Description
Communication Manager	Special Application SA9130 enabled.	Enabling new Special Application "(SA9130) - Authorization Code COR Toll Restriction & RCL Overrides Station COR" on the "system-parameters special-applications" System Access Terminal (SAT) form causes the toll and Restricted Call List (RCL) features to use the Authorization Code Class of Restriction (COR) to check for restrictions. This is by design when the SA9130 is enabled.
Communication Manager	Use of the "list trace station" or "list trace tac" System Access Terminal (SAT) commands.	The "list trace station" and "list trace tac" System Access Terminal (SAT) commands have been enhanced to display whether private or public numbering is in use.
System Manager	Element Manager	In early 2017, Avaya will introduce the Avaya Equinox™ 9.0 Conferencing application. In preparation for that introduction, the framework for supporting Avaya Equinox™ from System Manager has been added to the 7.0.1.2 Service Pack. Planned support from System Manager includes: Single Sign On from the Elements Page; the ability to add an Equinox server into the Inventory; and a new Equinox Conferencing ‘Communication Profile’ in the User Management area. These features are not currently supported. An update to these release notes are planned for late January, prior to the GA release of Avaya Equinox™ 9.0. Avaya Equinox™ 9.0 GA documentation will also include further details.
		Avaya Equinox™ includes the convergence of all of our Avaya soft clients, Avaya Aura Conferencing and Avaya Scopia into a single channel calling, messaging, collaboration and Conferencing solution for mobiles, browsers, desktops and room systems.
Branch Gateway	New CLI commands	Two new CLI Commands are introduced:
		- set allow-unencrypted: System administrator can use this command to allow or disallow media encryption requests from Communication Manager.
		- set link-encryption: System administrator can use this command to specify what TLS versions will be offered by the gateway when connecting to a server.
Branch Gateway	OPUS Codec support	OPUS Codec - The MP120 and MP160 VOIP modules are now capable of supporting the Opus codec in narrowband mode.
Branch Gateway	FIPS-mode support	FIPS-mode support - FIPS-mode is a feature that is currently not supported in Release 7.0.1 since it is

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Product	Enhancement	Description
		pending FIPS certification by a 3rd-party at this time. FIPS-mode is not intended for use by our customers in Russia nor will it provide any additional encryption capabilities.
Avaya Aura® Media Server	AMS-3263	AAMS installer enhancements to simplify building Amazon AMI
AADS	With this release of Avaya Aura, Avaya Aura Device Services is now supported. See the Avaya Aura® 7.0.1 Offer Definition (Dec 2016) posted on the Avaya Sales Portal.	
AADS	Notification	The Notification service provides a common infrastructure that allows a client or endpoint to subscribe to receive events from a number of service resources using a single connection.
AADS	Dynamic Configuration	The Dynamic Configuration service provides discovery of configuration settings to UC Clients. You can customize these settings on a global, group, individual, or platform basis. The Dynamic Configuration service uses the automatic configuration feature of Avaya Equinox™ 3.0 to facilitate the configuration details to the UC clients. This helps the user to avoid manual configuration of their client. To log in to the client, the user needs to enter their credentials, such as, email address or Windows user id, along with their enterprise credentials. The Dynamic Configuration service is supported on the following Avaya Equinox™ 3.0 devices: • Avaya Equinox™ for Android • Avaya Equinox™ for iOS • Avaya Equinox™ for Mac • Avaya Equinox™ for Windows.
AADS	Contact	To use the Contact service, a user must be a provisioned user on LDAP Server. Using the contact service: • Manage the contact detail from any device. • Add, update, and delete a contact. • Perform an enterprise search of existing sources of contacts, such as, System Manager, multiple LDAPs, single LDAP multiple domains, and local only. Avaya Aura® Device Services supports directory search of up to 300 contacts. • Set and retrieve information, such as, AADSpreferred names, picture, and

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Product	Enhancement	Description
		preferences.
AADS	**Web Deployment**	The Web Deployment service publishes and deploys the UC client updates to the devices of the end users. The Web Deployment service is supported on the following devices of the Avaya Equinox™ 3.0: • Avaya Equinox™ for Mac • Avaya Equinox™ for Windows

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:

1. Log in to the Avaya Technical Support Web site https://support.avaya.com.
2. 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

Installation for Avaya Aura® Communication Manager 7.0.1.0.0

Required patches

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

Refer PCN 2007S for more details at https://downloads.avaya.com/css/P8/documents/101014491.

Note: A new CM duplex vAppliance OVA file named **CM-Duplex-07.0.0.0.441-e55-1.ova** is available in PLDS via PLDS ID CM000000626. It is required along with Communication Manager 7.0.1.0.0 or later Service Packs/Releases to support Common Server Release 3 hardware. Avaya Aura® adds support for HP DL360PG9 and Dell R630 in Avaya Virtual Deployment configurations.

Backing up and installing Communication Manager

Communication Manager 7.0 software includes certain third party components including Open Source Software. Open Source Software licenses are included in the Avaya Aura® 7.0.

Communication Manager Solution Templates DVD. To view the licenses:

1. Insert the Avaya Aura® 7.0 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.

Fixes in Communication Manager

Fixes in Communication Manager 7.0.0.2.0

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
CM-2415	The field "Per Station CPN - Send Calling Number" is set to "(r) restricted" on a SIP station A and another station B has a bridge appearance of A.	The Calling Party Number was not blocked when a call was made using the Bridge Appearance of A over an ISDN trunk.	6.3.0.0
CM-2837	All Configurations	On the Communication Manager System Access Terminal (SAT) window, the 'status mst' command displayed a misleading status when a trace was disabled by overload control	6.3.3.0
CM-2995	Avaya Aura® with Communication Manager, System Manager, Session Manager and Call Center components.	Communication Manager would not place and Agent into 'Aux' mode after receiving certain SIP messages from the Session Manager	6.3.0.0
CM-3355	Telecommuter mode with PSTN permanent SIP service link	Occasionally, a user or an agent would experience issues with talkpath when a SIP permanent service link is used.	6.3.8.0
CM-3510	A call to a SIP Extension with Multiple Device Access (MDA) configured is answered by two or more devices simultaneously under traffic conditions	Communication Manager underwent a reset	6.3.9.0
CM-3700	All Configurations	On the Communication Manager System Access Terminal (SAT) window, the command 'list calltype route-chosen <dialed string>' failed when the dialed string was longer than 17 numeric characters	7.0.0.0
CM-5093	A SIP extension capable of dual registrations as an H.323 as well as a SIP station being monitored by an Application Enablement Services (AES) application E.g. TSAPI Monitor	Communication Manager generated two ALERT messages towards TSAPI Monitor for a call made to a SIP station with dual registration	6.3.0.0
CM-5384	PRI trunks	"When a system went into an ISDN b channel overload state for more than 8 minutes, ISDN trunks went out of service.	6.3.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-5636	SIP station outgoing trunk call.	If the SIP station made an outgoing trunk call, and if the far end trunk did not send back any digits, then the SIP station's MDA device could not log any number in its call log. This device would not be able to call out.	6.3.0.0
CM-5667	1. XT H.323-registered to iView calls 1XC H.323. 2. 1XC H.323 uses second line appearance to dial SIP video endpoint. 3. 1XC H.323 transfers second call to XT H.323"	Users would not see video after the call transferred to the endpoint registered over iView.	6.3.0.0
CM-6047	Enforce SIPS URI for SRTP?" is disabled on the Signaling Group of the SIP trunk	A video call made over a SIP trunk to an H.323 video Call Center Agent was completed with an unencrypted audio stream when it should have been completed with an encrypted audio stream. In some cases "static noise" was heard on the call.	6.3.10.0
CM-6471	Caller, agent and observer are on a single port network, and the call is transferred by the agent to a VDN with a collect step.	Caller was unable to enter digits after being transferred.	6.3.5.0
CM-6500	SIP station transfers a call to another SIP station using AST1 Transfer or by not using the 'SIP Endpoint Managed Transfer' feature	After the transfer was completed, the Transferring Party's identity was displayed on the stations instead of the Connected Party’s identity	7.0.0.0
CM-6530	SIP Call Center with Service Observers and agents in auto-answer mode	Observers of auto-answer agents were not informed and put into a waiting state if their observed agent logged out by hanging up.	7.0.0.0
CM-6603	SIP stations	The Network Region used is now displayed when running the "list trace" SAT command on a SIP station.	6.3.112.0
CM-6703	Primary and Secondary session managers.	When a customer uses a secondary Session Manager for handling SIP phones the primary signaling links go into bypass mode when a large amount of SIP phones register to it even though the primary Session Manager is up	6.3.9.1
CM-6720	A SIP trunk with the field "Identity for Calling Party Display" set to "P-Asserted-Identity"	Under certain circumstances, for an incoming call over SIP trunk, the Calling Party’s name on the Called Party's display changed to the Trunk name.	6.3.6.0
CM-7049	SIP traffic	Communication Manager would undergo a warm reset when the SIP message transaction count	6.3.111.0

ID	Minimum Conditions	Visible symptoms	Release found in
		went beyond 10,000.	
CM-7075	1X Communicator in "Road warrior" mode with multiple button modules administered.	Buttons labels failed to get downloaded on the button modules	6.3.9.1
CM-7116	"PIN Check for Private Calls" Feature is enabled on the system	A Call made using this feature would fail once the caller dialed the Feature Access Code for "PIN Check for Private Calls" and then the administered PIN	6.3.5.0
CM-7142	1. Application Enablement Services (AES) 2. Communication Manager (CM) with call center setup	CM allowed agents logging in through AES associated Applications to login overriding Tenant Permissions.	6.3.5.0
CM-7251	One-X CES Application has the options "Ring Phone" and "Call Back Phone". Configure two different Mobile Numbers for "Ring Phone" and "Call Back Phone".	The mobile phone which was already busy on a call would get notification for a second incoming call overriding the One-X CES configuration	6.3.9.0
CM-7253	SIP Trunk calls as well as SIP Station calls under high traffic conditions.	Large number of Log files would be generated as a result of some unwanted Proc Errors being logged under high traffic conditions of SIP to SIP station and trunk calls.	7.1.0.0.0
CM-7327	A Conference Call involving an external Caller over a SIP trunk with "Network Call Redirection" enabled	One-way talkpath was experienced by the caller once the conference was established	6.3.8.0
CM-7328	1. An Enterprise Survivable Server (ESS) or a Local Survivable Processor (LSP) 2. Communication Manager (CM) with a G450 Media Gateway 3. Application Enablement Services (AES) application	Under very specific conditions the Media Gateway was prevented from registering to the Primary CM which had become available again after an LSP/ESS failover	6.3.10.0
CM-7430	1. Two station users in different tenant partitions with no calling permissions between them 2. The trunk group for one of the user's EC500 mapped extension in a third tenant. This tenant can talk to all other tenants 3. Trunk calls originated from the EC500 mapped station user's extension terminates at the other station user	Intermittently, Incoming trunk calls, once answered, would get disconnected after a few seconds	6.3.6.0
CM-7511	Audix Hunt Group	Calls to the Audix hunt group failed and dropped when Audix answered the calls	6.3.10.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-7569	One-x controlled station and destination configured for Authorization Code	While making One-x callback call to a destination requiring an Authorization Code, customer was not able to enter the Authorization code.	6.3.10.0
CM-7608	Congestion in the IP network and SIP trunk call traffic	Communication Manager experienced WARM resets	6.3.11.0
CM-7644	Entries present in the 'public-unknown-numbering; or 'private-unknown-numbering' forms but not in the Dial Plan Analysis Table.	Customer could not access entries that were not defined in the Dial Plan Analysis Table form when executing "change public-unknown-numbering" or "change private-numbering" command to remove or modify entries. Customer would see the "Ext code inconsistent with dialplan" error.	6.3.9.0
CM-7696	SIP Station calls under high traffic conditions.	Large number of Log files would be generated as a result of some unwanted Proc Errors being logged under high traffic conditions of SIP to SIP station calls.	7.0.0.0
CM-7717	SIP Trunk being used as a PSTN trunk with "Direct Media" disabled	When a SIP station originated a 911 call over a Service Provider SIP PSTN trunk a call back from Public Safety Answering Point (PSAP) failed to terminate on the 911 caller	6.3.11.0
CM-7724	1. VDN Origin Announcement (VOA). 2. Computer Telephony Integration (CTI) application for 3rd party call control (3PCC).	No ACK/NACK message was being sent to the CTI application for a third party call control (3PCC) call if a VDN Origin Announcement (VOA) was being played on the user's station. This caused CTI call control, for example transfers, to fail.	6.3.10.0
CM-7747	The field "Location to Route Incoming Overlap Calls" on "off-pbx-station mapping configuration-set" form is set to "trunk".	The mobile extension was being displayed on the called SIP station instead of EC500 mapped station's caller ID	6.3.9.1
CM-7780	Administered and connected Avaya Media Server (AMS)	The Load Factor field on the "status media-server" command output displayed inconsistent information	7.0.0.0
CM-7812	Communication Manager with co-resident Communication Manager Messaging or standalone Communication Manager Messaging system	Description field on a certain MIB group did not display data	6.3.1.0
CM-7815	An Avaya Aura® Voice Mail (AAM) system connected to the Communication Manager (CM) via a SIP trunk and an Attendant configured on the CM	When an incoming ISDN call made to a local station covered to an attendant who used the "Transfer to Voice Mail" Feature Access Code to transfer this call to the AAM system, the Attendant would be incorrectly identified as the originator of the call instead of the ISDN Calling number who left the voice mail	6.3.3.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
CM-7905	Communication Manager with 3rd Party Call Control (3PCC) enabled and integrated with an ASAI application to generate calls using Computer Telephony Integration (CTI)	When a call was originated using the ASAI application, '#' was outpulsed over the trunk once the call was answered	6.3.10.0
CM-7940	Media Server administered on a Communication Manager using a number greater than 99	Media Server numbers greater than 99 would be truncated to two characters	7.0.0.1.0
CM-7941	"Direct media" enabled on SIP signaling group.	There would be no talk path when a SIP station which answered a call on a bridged appearance tried to make an Unattended Transfer to another SIP station.	7.0.0.1.0
CM-7992	Port Network	An administered cabinet would not be removed unless the ip-interface PROCR was removed first	6.3.11.0
CM-8102	Use of Call Suppression feature	Call Suppression did not operate correctly if the called SIP endpoint's extension number was modified through the use of inserting digits using a route pattern entry.	6.3.111.0
CM-8136	A call made by a Third Party endpoint capable of Binary Floor Control Protocol (BFCP) presentation E.g. CISCO endpoint	The Third Party Endpoint could not join a call	6.3.11.1
CM-8146	Remote worker logged in to Avaya Aura® using Avaya Aura Session Border Controller for Enterprise (ASBCE)	Under very specific SIP messaging, signaling connection between CM & ASM disconnected.	6.3.10.0
CM-8169	IP Agent soft client	IP Agent 6.0 soft client couldn't register to CM after the CM was upgraded to 6.3.8.0 or higher	6.3.10.0
CM-8184	1. Hunt groups 2. BCMS/CMS or similar applications that utilize monitoring events.	In a very rare scenario where internal CM data ended up in a mismatched state, hunt groups were not being monitored when they were configured to be monitored.	6.3.8.0
CM-8221	QSIG, Path Replacement, Vectoring and Announcements configures on Communication Manager	When path replacement was used and an announcement had finished playing in a vector, it would propose a new path replacement, which could re-queue the call thus affecting the oldest call waiting statistics.	6.3.10.0
CM-8236	Intermittent ISDN trunk call made using Avaya OneX Communicator Redial feature.	Communication Manager experienced a WARM reset	6.3.6.0
CM-8247	1. SIP Call Center agents 2. Direct Media enabled on the OPTIM trunk used by the SIPCC agents.	Users experienced no talkpath when a direct media call was auto-answered by an agent administered with auto-answer ACD and logged in	6.2.0.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
		on a SIPCC station that was not administered as auto-answer.	
CM-8253	SIP, Duplex systems	On rare occasions, a system interchange would fail and leads to a system reload.	6.3.111.0
CM-8292	A video call made from an H323 Endpoint to a SIP Endpoint	Intermittently, video calls between H323 endpoint to Aura-SIP endpoint experienced poor video quality.	7.0.0.1.0
CM-8303	Communication Manager with Application Enablement Server (AES) and a voice-mail with Audix-recording capability	A message containing the incorrect extension number sent by Communication Manager caused applications like Proactive Outreach Manager (POM) to drop the entire on-going call instead of only the Audix Recorder which had been recording the call	5.2.1
CM-8307	IP Terminal Translation Initialization (TTI) is enabled	Under specific conditions misleading Proc Errors would be logged generating large number of Log Files	6.3.8.0
CM-8317	1. Application Enablement Services (AES). 2. Monitored stations. 3. AES integrated applications that utilize call identifiers for monitored stations.	CM failed to provide the call identifier for a monitored station in response to a value query from AES. This resulted in unexpected behavior from AES integrated applications utilizing this information, depending on how the information was being used.	6.3.11.0
CM-8337	1. Application Enablement Services (AES) with an application for redirection 2.SA8904 (location based calltype analysis) enabled on Communication Manager (CM)	Occasionally, CM failed to reroute a call correctly when SA8904 (Location Based Calltype Analysis) was enabled and an Application Enablement Server associated Application initiated a Redirection of the call	6.3.10.0
CM-8393	SIP Update message used for SIP session refresh.	Calls were dropped if CM sent a sips UPDATE with a sip contact header	6.3.10.0
CM-8399	An originator in Shared Control Mode on a SoftPhone	Call Logs would not get stored on the hard phones when the user placed a call through the Softphone by dialing the ARS Feature Access Code (FAC) followed by the Direct Inward Dialing (DID) Extension	6.3.6.0
CM-8400	Stub region connected to a core region and the core region connected to another region	Stub region test on a non-core region would fail leaving failures and alarms that were unresolvable	6.3.0.0
CM-8438	Any Avaya Aura Messaging or Communication Manager Messaging system that has one or more Trap Receiver Destination(s) configured	One or more GAM “Border Process Registration Failed” traps would be erroneously generated on the system	6.2.3.0
CM-8460	Changes being made to either the	On a Duplex system changes to the SNMP Trap	6.3.100.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
	SNMP Trap Filters or Alarm level Adjustments on a Duplex Communication Manager system	Filters or Alarm level Adjustments would not get file synchronized immediately to the Standby server	
CM-8496	Multiple Stations being accessed in the User Manager simultaneously	Occasionally, busying out an IP Station and then releasing it did not force the Station to unregister	6.3.11.0
CM-8525	Calls transferred to agents over SIP trunks when MOH is enabled	Under specific conditions, MOH was heard by both agent and the calling party	6.3.8.0
CM-8533	1. Very large Enhanced Call Pickup Alerting groups. 2. Heavy call traffic loads.	Use of the Enhanced Call Pickup Alerting feature sometimes caused a system reset with very large groups under heavy call traffic loads.	6.3.11.1
CM-8537	96X1SIP Stations	Under specific configurations for 96X1SIP Stations, a wrong number was displayed in the "Call-Limit" field on the 'off-pbx-telephone station-mapping' form	6.3.11.0
CM-8564	"Criteria for Logged Off/PSA/TTI Stations" is enabled on the form "system-parameters coverage-forwarding" On Communication Manager and the first point of coverage is not registered	Call did not cover to the second point of coverage	6.3.10.0
CM-8666	SIP trunk. Different session refresh timer values used at near end and far-end	Under a very specific SIP messaging sequence users experienced loss of talkpath after a transfer took place	6.3.10.0
CM-8768	Call Center Elite, IQ	IQ could not complete pumpup.	7.1.0.0.0
CM-8887	Presence of more than 1653 entries in the "ARS DIGIT CONVERSION TABLE" form for a single location	When there were greater than 1653 entries in the ARS DIGIT CONVERSION TABLE" form for a single location, this form could not be changed and the message "Error Encountered, Can't Complete Request" was displayed on the screen	6.3.12.0
CM-8907	Multiple Device Access (MDA) ISDN trunk	Call Logs on MDA devices were different if the incoming ISDN trunk and the called station are in different locations.	6.3.13.0
CM-9112	Administration on "Calling Party Number Conversion" (CPNC) form	After upgrade to CM7.0, the field "Deny Call" on the CPNC form would be set to "y"	7.0.0.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Fixes in Communication Manager 7.0.0.3.0

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
CM-1352	A conference call involving the following parties: 1. 96XX H323 Station on a local CM 2. One-X Communicator (1XC) H323 Station on a remote CM 3. Avaya Aura Communicator on iPad	A Video escalation button push from Avaya Aura Communicator on the iPad on a Communication Manager hosted audio conference resulted in the iPad turning non-responsive.	6.3.6.0
CM-4268	Using the Avaya Aura Messaging (AAM) Call Language Preservation feature on an AAM which has been configured to use Basic or Unattended Transfers.	Customer was required to re-enter language preference when the call had been transferred from the AAM to another station and covered back to AAM	6.3.6.0
CM-5063	A Call Center setup integrated with a Call Management System (CMS) and an Avaya Aura Application Enablement Services (AES) application	CMS would receive two AUX work events when a call answered by an agent in Automatic Call Distribution (ACD) mode was placed on hold by the AES application and merged with a second call to complete a conference	6.3.0.0
CM-6768	Automatic Call Back (ACB) invoked on a SIP station with Call Forward activated for all calls	Automatic Call Back (ACB) did not work for calls to a SIP station that had Call Forward activated for all calls. ACB would be activated, but the callback attempt would always fail returning busy tone to the originator even though the called party was idle.	7.0.0.0
CM-7566	Survivable Core Server or a Survivable Remote Server	Occasionally, the system would crash when executing the System Access Terminal (SAT) commands "list media-server" or "status media-server" on a Survivable Core Server or a Survivable Remote Server.	7.0.0.0
CM-7606	1. Direct Media, SRTP enabled on a SIP Station A with Network Region supporting RTP 2. Direct Media, SRTP enabled on a second SIP Station B with Network Region supporting SRTP	SIP stations displayed incorrect security indication on the call.	7.0.0.0
CM-7624	Survivable Remote Server or Survivable Core Server.	Occasionally, the system would continue rebooting when executing the System Access Terminal (SAT) commands "list media-server" or "status media-server" on a Survivable Core Server or a Survivable Remote Server.	7.0.0.0
CM-7939	"Direct IP-IP Audio Connections" is disabled on the SIP signaling-group.	After an Unattended Transfer was completed, SIP stations displayed incorrect security indication on the call.	7.0.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-8190	An incoming call over an R2MFC trunk answered by a SIP desk phone using the Call Pickup feature.	No Caller ID (CID) was displayed on SIP desk phones for incoming R2MFC trunk calls that were answered using the Call Pickup feature.	6.3.8.0
CM-8370	Either "Direct IP-IP Audio Connections" (Shuffling) is disabled or Music on Hold is enabled on the system	A video escalation in an 'Audio-only' call initiated by one of the Avaya Aura Communicator Windows (ACW) Endpoints in a two party call resulted in a blacked out screen at the escalating ACW	6.3.0.0
CM-8488	DECT stations, which are part of groups like Terminating Extension Groups (TEG) or Coverage Answer groups (CAG)	There was no alerting on the DECT endpoint when a call was made to the group	7.0.0.1.0
CM-8497	The "SIP Endpoint Managed Transfer" feature is enabled on the system	Park & Page feature for EDP (Engagement Development Platform) failed if both stations are 96x1SIP stations SEMT capable phones	7.1.0.0.0
CM-8513	Executing a "list trace station" command for an extension that has a large number of bridged stations	In rare instances, executing a "list trace station" command for an extension that had a large number (hundreds) of bridged stations caused a system reset.	6.3.11.0
CM-8678	1. "Client Room" is enabled on the COS-group of the Calling Party 2. Coverage path is set on the Called Party	When the covered call was answered and then dropped at the Called Party's coverage point, the call logs showed the Caller's identity as "unavailable".	6.3.11.0
CM-8679	1.'Allow VDN Override?' field is disabled on the Vector Directory Number (VDN) 2. Use of Basic Call Management System (BCMS)/Call Management System (CMS) or similar applications that utilize monitoring events	A call routing to a Vector Directory Number (VDN) with "Allow VDN Override" set to "no" (disabled) generates two call records in BCMS/CMS instead of one.	6.3.10.0
CM-8746	An Unattended Transfer initiated by a DECT station	Upon expiry of the Transfer Recall timer, the returned call on DECT phone was not shown as Priority Call.	6.3.11.0
CM-8749	Trunk to Trunk transfers failing over Central Office (CO) trunks with "No Disconnect Supervision" set.	Central Office (CO) trunk members remained active for failed transfers with "No Disconnect Supervision" set, even after all parties disconnected from the call.	6.3.4.0
CM-8784	Call Center Elite, Softphones	When the command "display capacity" was active on the system while a trace was being collected, a large number of log statements would get generated which proved difficult to interpret	6.3.11.0
CM-8791	Call Center Elite with Coverage Paths defined for agents	Calls failed to route to any coverage path after the first coverage path, for agents which were logged out.	6.3.9.1

ID	Minimum Conditions	Visible symptoms	Release found in
CM-8828	Presence of Off-pbx-telephone Station-mappings on the system	Occasionally, attempts to change the "Mapping Mode" for previously defined station mappings using SAT failed and the message "Error Encountered, Can't Complete Request" was displayed on the screen	6.3.2.0
CM-8840	SIP trunk call transfer from an Avaya Enterprise Portal to a Vector Directory Number (VDN) which has a "collect" step without a "wait" step before it.	When a SIP trunk call from an Avaya Experience Portal was transferred back to the VDN, the calling user was unable to enter any DTMF digits when prompted.	6.3.10.0
CM-8867	1. Communication Manager with "SA8481-Replace Calling Party Number with ASAI ANI" enabled. 2. 3PCC configured and integrated with an Avaya Aura Application Enablement Services (AES) application.	When a 3PCC call was made over a trunk, an incorrect Calling Party Number was displayed	6.3.0.0
CM-8875	Call Center setup integrated with an Avaya Aura Application Enablement Services (AES) application and Call Monitoring Applications.	When a device information query was launched through the AES application for various devices, other call monitoring applications ran into delays due to extra bytes being sent by CM	6.3.11.0
CM-8965	Communication Manager with Computer Telephony Integration (CTI) configured and integrated with a CTI adjunct requesting Single Step Conference (SSC)	Under certain call scenarios, a CTI SSC request failed without sending a negative acknowledgement back to the CTI adjunct. As a result, subsequent 3rd party CTI requests over the same CTI association failed with a protocol error. Furthermore, in cases where the SSC succeeded, the Connection IE for the party added in SSC was always incorrectly set to the extension value of '*****' instead of the actual extension of the SSC party.	7.0.0.0
CM-9014	1. Call Center setup with IP agents configured 2. Different network region resources preferred by the incoming call, agent and the service observer	Zip tone was being heard by the calling party as well as the observers on the call which was being observed when it should have been heard only by the agent.	6.3.11.0
CM-9059	Call Center agents logging in with "Forced Agent Logout Time" configured.	Agents that logged in with "Forced Agent Logout Time" configured did not get logged out after the logout time interval.	6.3.11.0
CM-9108	Executing the "status station" command on stations administered without a Network Address Translation (NAT) IP Address.	The "Native NAT Address" field displayed an IP address instead of "not applicable" when the "status station" command was executed on a station.	6.3.11.0
CM-9133	Media Gateway with no media resources administered.	Communication Manager experienced resets due to periodic background maintenance tests	7.0.1.0.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
		being executed on a Media Gateways.	
CM-9190	The 'acpsnmp' login was not logged in after a system reboots, or a user reset the SAT using the 'reset login-ID.'	The "snmpget" command fails on a Local Survivable Processor (LSP) or an Enterprise Survivable Server (ESS) the first time after a CM reboot.	6.3.111.0
CM-9207	The called party is a member of a Call Pickup group and answers a call made to it using the "Active Appearance Select" Feature Name Extension (FNE)	When the call was answered by the principal using the FNE, the other members of the pickup group continued to be alerted endlessly for the same call	6.3.12.0
CM-9492	Call Center Elite, Reporting adjunct such as Call Management System (CMS)	Executing Add/Remove skills would send a zero length physical extension to reporting which caused corruption in the SPI logs of the CMS	7.0.1.0.0
CM-10129	Using the Solution Deployment Manager to install Communication Manager (CM) patches when there is a patch installation issue other than "the patch is already installed".	Patching of Communication Manager via System Manager's Solution Deployment Manager returned the wrong exit code for most installations.	7.0.1.0.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Fixes in Communication Manager 7.0.1.0.0

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
CM-2837	All Configurations	On the Communication Manager System Access Terminal (SAT) window, the 'status mst' command displayed a misleading status when a trace was disabled by overload control	6.3.7.0
CM-5016	EC500 configured on extensions	When an EC500 user, mapped to an enterprise user A, placed a call to another enterprise user B, the extension of the EC500 user instead of that of Station A was displayed on Station B	7.0.0.0
CM-5789	H.323 stations or H.323 trunks	On rare occasions, Avaya Aura Communication Manager underwent a reset while sending messages to H.323 stations or trunks	6.3.0.0
CM-6471	1. Call Center Setup with the caller, agent and observer on a single port network. 2. A VDN (Vector Directory Number) administered with a "collect" step to collect digits	Caller was unable to enter digits after being transferred by the agent to a VDN with a collect step.	6.3.5.0
CM-7297	Systems where the CM logs were writing more than once per second.	The 'logv', 'logc', and 'logw' log evaluation commands had a race condition that occasionally caused unwanted prompts when examining log data on busy systems.	6.3.9.1
CM-7328	LSP (Local Survivable Processor) or ESS (Enterprise Survivable Server)	Under very specific conditions the Media Gateway was prevented from registering to the Primary Communication Manager (CM) which had become available again after an LSP/ESS failover	6.3.10.0
CM-7329	1. H.323 trunk administered between CM1 (Communication Manager 1) and CM2 (Communication Manager 2) 2. SIP trunk administered between CM2 and SM (Session Manager)	CDR (Call Detail Recording) for the second call leg was not generated, when a tandemed call, made from a station on CM1, to a Non-Optim SIP Station registered to an SM (Session Manager) was blind transferred to an H.323 station on CM2.	6.3.7.0
CM-7511	Audix Hunt Group	Calls to the Audix hunt group failed and dropped when Audix answered the calls	6.3.10.0
CM-7533	SIP Agent	Under a very specific SIP messaging sequence, a login attempt by a SIP agent would cause a segmentation fault	6.3.7.0
CM-7644	Entries present in the 'public-unknown-numbering; or 'private-unknown-numbering' forms but not in the Dial Plan Analysis Table.	Customer could not access entries that are not defined in the Dial Plan Analysis Table form when executing "change public-unknown-numbering" or "change private-numbering" command to remove or modify entries. Customer would see the "Ext code inconsistent with dialplan" error.	6.3.9.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
CM-7727	Third Party Call Control (3PCC) configured on Communication Manager (CM) integrated with an Application Enablement Server (AES)	Occasionally, calls involving SSC (Single Step Conferencing) would experience loss of talk path or would be abruptly dropped	6.3.10.0
CM-7992	Port Network	An administered cabinet could not be removed unless the ip-interface PROCR was removed first	6.3.11.0
CM-8102	Use of Call Suppression feature	Call Suppression did not operate correctly if the called SIP endpoint's extension number was modified through the use of inserting digits using a route pattern entry.	6.3.111.0
CM-8434	CTI (Computer Telephony Integration) applications performing call control in Communication Manager (CM) via Application Enablement Services (AES) and Adjunct Switch Application Interface (ASAI).	The "Simultaneous Active Adjunct Controlled Calls" count on the System Access Terminal (SAT) display capacity form kept growing, never decreasing when it should.	6.2.7.0
CM-8487	Administration of an H.323 trunk followed by other trunks in preference order in the route pattern which is being used.	Occasionally, owing to problems in the underlying IP Network, the Look Ahead Routing (LAR) feature would not be executed correctly for H.323 trunks.	6.3.6.0
CM-8578	Avaya OneX-Attendant receiving a call over a trunk	When an Avaya OneX-Attendant transferred an external incoming call to an external extension over any trunk, the far end did not receive the calling party's identity.	6.3.6.0
CM-8593	Team button and calls involving service links	Occasionally, team button interactions with calls involving service links caused Communication Manager to reset.	6.3.11.0
CM-8675	ISDN or H.323 trunks	Under rare circumstances, using ISDN or H.323 trunks caused CM to reboot.	6.3.10.0
CM-8732	Avaya SIP station	Under a very specific SIP messaging sequence, a registration attempt followed by a message summary event by a SIP station caused a segmentation fault.	6.3.11.0
CM-8951	1. Communication Manager (CM) with Computer Telephony Integration (CTI) configured and integrated with a CTI adjunct. 2. A incoming transfer request initiated by a SIP trunk to CM	Occasionally, on trunk initiated transfers to CM, the CTI Transferred Event would contain incorrect information, including reporting only a single party on the resultant call, which would cause call recording applications to fail to record the call. In some cases, such a call scenario caused all future CTI messages to be corrupt, requiring a reset system 4 on CM to recover.	7.0.0.0
CM-9011	1. EC500 enabled on a one-X Client Enablement Services station 2. "Busy" coverage criteria disabled on the	Calls to the one-X Client Enablement Services (CES) station, with EC500 enabled and all call appearances busy, routed to coverage instead of	6.3.12.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
	station's coverage path.	returning busy tone.	
CM-9012	An unregistered station with two call appearances and Restrict Last Appearance" enabled	A call made to the unregistered station when one of its call appearances was busy, returned ring back instead of the busy tone.	6.3.10.0
CM-9022	1. Communication Manager with CTI (Computer Telephony Integration) configured and integrated with a CTI adjunct 2. A VDN (Vector Directory Number) with a "collect" step	CTI applications were unable to pass DTMF tones to CM during digit collection steps of vector processing.	6.3.10.0
CM-9215	Communication Manager with CTI (Computer Telephony Integration) configured and integrated with a CTI adjunct	No Call Initiated Event message was being sent to the CTI application for a 3PCC (Third Party Call Control) originated call. Call recording failed for such calls.	6.3.10.0
CM-9217	Emergency Location Extension (ELE) configured on the system	The "status station" System Access Terminal (SAT) command showed a truncated call forward number for an ELE station.	6.3.12.0
CM-9235	SIP stations on SIP trunks configured on the system	The System Access Terminal (SAT) commands "list trace station" and "list trace tac" failed to display all SIP messages associated with the traced call.	6.3.3.0
CM-9255	Chained Call Forwarding enabled on the system.	When a call failed to forward because all the trunks were busy, the caller would hear silence instead of hearing reorder tone.	6.3.12.0
CM-9302	1. SIP trunk configured on Communication Manager 2. EC500 enabled on the Called party	When Communication Manager received an incoming SIP trunk call which had a very low Max-Forwards header value, the call failed to route to the EC500 extension.	6.3.11.0
CM-9327	Group Page	On rare occasions, calls to a group page caused the call appearance of a paged digital station to be left in a busy state for a few minutes until an audit cleared the call appearance.	6.3.12.0
CM-9344	1. 3PCC (Third Party Call Control) configured on Communication Manager integrated with an AES (Application Enablement Services) server 2. "SA8481 - Replace Calling Party Number with ASAI ANI" enabled on CM	A 3PCC call made over a trunk resulted in a modified Calling Party Number (CPN) being sent in the "P-Asserted-Identity", "Contact", and "From" headers in the SIP message	6.3.11.1
CM-9345	1. Call Center Elite system integrated with an Avaya AES (Application Enablement Server) Application. 2. Reporting Adjunct, such as CMS (Call Management Server)	When digits outside of the range of digits (0-9) were sent to reporting for the calling party number (ANI), the message was ignored by the reporting application.	6.3.11.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
CM-9357	1. Computer Telephony Integration (CTI) applications performing call control in Communication Manager (CM) via Application Enablement Services (AES) and Adjunct Switch Application Interface (ASAI). 2. 3PCC (Third Party Call Control) configured on Communication Manager (CM) integrated with the AES	When a call was originated using CTI by an ASAI application, '#' was outpulsed over the trunk once the call was answered	6.3.12.0
CM-9371	1. Communication Manager integrated with an Avaya AES (Application Enablement Server) application 2. Greater than 500 IP stations on the system	When there were more than 500 IP stations registered through AES which were sharing the same IP address, the "reset ip-station" command did not complete	6.3.12.0
CM-9396	1. H.323 IP stations using the E.164 international number format. 2. Call forwarding activated.	If an H.323 IP phone location-parameter used an E.164 international number format, and call forward was active on the phone, the phone call log did not include the "+" character or the country code.	6.3.9.1
CM-9399	Virtual Station administered with a coverage path with a Coverage Answer group as its first point of coverage and a Hunt group for a Messaging Server as its second point of coverage.	When a call termed on the virtual station and landed on the second point of coverage, a wrong greeting was played to the caller	6.3.6.0
CM-9413	1. Team button administered on a station 2. Monitoring station administered as 96x1 set type and registered on a Avaya One-X Communicator	No Team Button lamp update was seen if the monitoring station registered using Avaya OneX Communicator attempted to initiate a call.	6.3.12.0
CM-9428	1. VDN (Vector Directory Number) administered on the system 2. SIP adjunct, such as a Voice Mail Server, connected to the Communication Manager via SIP trunk.	A call landing on a VDN, when redirected to the Voice Mail Server, over a SIP trunk, resulted in an error and the caller was unable to leave a voice mail.	6.3.10.0
CM-9429	Announcement configured on a Communication Manager system.	When an announcement was in the process of being connected to a call, and the caller disconnected before the commencement of the announcement, the announcement media (e.g., VAL board) displayed errors on the system	6.3.12.0
CM-9477	X.25 data-module with translations	Under certain conditions where the cabinet had been removed first, Avaya services were unable not remove X.25 data-module translations.	6.3.9.1
CM-9489	Attendant, SIP station administered on Communication Manager	A call from a SIP station that dialed "0" to reach an attendant failed.	6.3.11.1
CM-9497	Systems running either Communication	The "statapp" command did not accurately report	7.0.0.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
	Manager Messaging (CMM) or AVAYA AURA Messaging (AAM).	Messaging "Up/Down" status.	
CM-9524	1. Communication Manager (CM) with CTI (Computer Telephony Integration) configured and integrated with a CTI adjunct 2. Service Observing (SO) warning tones enabled	CTI stations were unable to send DTMF tones to CM if Service Observing warning tones were enabled on CM.	6.3.11.0
CM-9546	1. Direct media enabled for calls involving SIP extensions or trunks 2. An unregistered SIP extension with EC500 activated 3. LAR (Look Ahead Routing) configured	Calls to the EC500 extension failed if LAR was used to route the call	6.3.12.0
CM-9547	One-X Communicator Soft Phone application using the file 'login.xml' to send data in the RRQ (Registration Request) message	When a One-X Communicator soft phone sent an RRQ message with the Network Region Number through the login.xml file, incorrect information caused media resources to be selected from incorrect Media Gateways.	6.3.8.0
CM-9565	Call Center Elite	Occasionally, an agent logging into an AWOH station (Administration Without Hardware) and then logging out caused the Communication Manager to restart	6.3.4.0
CM-9566	1. Communication Manager with CTI (Computer Telephony Integration) configured and integrated with a CTI application with 3PCC (Third Party Call Control). 2. Four digit Account Access codes used for CDR (Call Detail Recording)	Calls from CTI applications with 3PCC failed if the CDR access code was sent in the private data of the CSTA MakeCall event.	6.3.12.0
CM-9567	Multiple emergency calls placed from the same station through Communication Manager.	When multiple emergency calls were made from the same station, the PSAP (Public Safety Answering Point) call back call was not always treated as a priority call.	6.3.12.0
CM-9597	Communication Manager system administered with multiple locations and integrated with reporting adjuncts, such as CMS (Call Management Systems)	Occasionally, incorrect Location IDs for measured PRI trunks involving Media Gateways would be sent to CMS	6.3.12.0
CM-9627	ECPA (Enhanced Call Pickup Alerting) administered with the field "Caller ANI during pickup alert" disabled on the Calling Party's COR (Class of Restriction)	For a call terminating on the SIP members of a Call Pickup group, the Caller's ANI was incorrectly being displayed	6.3.12.0
CM-9628	1. Communication Manager with CTI (Computer Telephony Integration) configured and integrated with a CTI	Call recording using Single Step Conferencing failed	7.0.0.1.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
	adjunct supported by Avaya AES (Application Enablement Server). 2. An AES controlled Call recorder being used to record calls.		
CM-9653	Communication Manager system integrated with reporting adjuncts, such as CMS (Call Management Systems), or IQ	Under a very specific SIP messaging sequence for a call involving a Transfer, reporting adjuncts were unable to accurately track the call if the transferred leg was redirected to a number that failed to route successfully.	6.3.10.0
CM-9725	SIP traffic	Occasionally, Communication Manager underwent a system reset under conditions of heavy SIP traffic	6.3.14.0
CM-9767	Disable the field "Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers?" by setting it to "n" on the SIP signaling group CM SAT (System Access Terminal) form being used.	Occasionally, Communication Manager would experience a system restart when the far end SIP client sent an invite with an exceptionally long user string in the request URI.	6.3.10.0
CM-9778	A call center configuration with work at home agents (agents using service links) where agent calls are being recorded.	In rare call scenarios, calls for agents using service links (telecommuter/another telephone number/another phone mode) were not recorded.	6.3.11.0
CM-9825	A Call Center setup including a CMS (Call Management System) and integrated with SIP adjuncts, such as IVR (Interactive Voice Response), ICR (Intelligent Customer Routing), or AAEP (Avaya Aura Enterprise Portal)	Under a very specific SIP messaging sequence, CMS stopped tracking internal calls after routing out to a SIP adjunct.	6.3.12.0
CM-9828	A call center configuration with tandem Communication Managers using the VDN Return Destination feature.	An outgoing trunk call that was transferred to a Vector Directory Number (VDN) and answered by an agent, failed to route to the VDN return destination if the call routed to another trunk due to no disconnect supervision being set on the original outgoing trunk.	6.3.12.0
CM-9829	1. Call Center Elite 2. Communication Manager (CM) with CTI (Computer Telephony Integration) configured 3. Service observing	When a call with a service observer active used CTI to outpulse DTMF and attempted to transfer this call within five seconds, the transfer failed	6.3.11.1
CM-9837	"V6 Node Names" field administered on the "survivable-processor" SAT (System Access terminal) form on CM.	Removal of the "Service Type" entries for CDR (Call Detail Recording) on the "ip-services" SAT form failed and the message "Error Encountered, Can't Complete Request" was displayed on the screen	6.3.12.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
CM-9917	A configuration with SIP phones that have auto-dial buttons programmed with a code which is a concatenation of the "Call Park" Feature Access Code (FAC) and the "Answer Back" FAC.	Users were unable to park a call using an auto-dial button on a SIP phone.	6.3.12.0
CM-9921	Call Center Elite	Occasionally, an agent logging into an AWOH station (Administration Without Hardware) and then logging out caused the Communication Manager to restart	6.3.4.0
CM-9924	The SIP response message received by Communication Manager contained more media lines in SDP than what was sent in the outgoing INVITE	Communication Manager experienced a reset	6.3.1.0
CM-10006	1. "Display Information With Bridged Call" set to "y" on the CM SAT (System Access Terminal) form "system-parameters features" 2. A station Station-B administered with three bridged appearances of another station Station-A in place of the default three call-appearances.	With Station-A off-hook on its first call-appearance, the second off-hook attempt by its bridged station Station-B resulted in no dial tone being heard by Station-B.	6.3.12.0
CM-10010	Bridged Appearances, for the same principal station, administered on both a SIP station and an H.323 station.	Occasionally, when a call landed on the principal station and the subsequent dialog event state Publish message contained the H.323 station in the Request URI, the Bridged Appearance on the SIP Station did not alert.	6.3.10.0
CM-10024	1. MOH (Music on Hold) enabled on the system 2. SIP Stations sending media to a Media Gateway 3. Call recorder being used to record calls	Occasionally, VOA (VDN of Origin Announcement) played on a call which was being recorded, resulted in loss of talkpath.	6.3.12.0
CM-10038	SIP Stations configured on the system	Occasionally, Avaya Communication Manager experienced a system reboot under SIP call traffic.	6.3.12.0
CM-10126	A Call Center Elite system administered with skills some of which have 'Timed ACW (After Call Work)' active.	When an agent received a call for a skill with 'Timed ACW' and went into 'pending ACW' mode during the call then after the call dropped, the agent did not go into timed ACW mode as expected. If the next call received by the agent was for a skill that did not have 'Timed ACW' active, the information from the prior call was used and the agent went into 'Timed ACW' mode after the second call.	6.3.11.1
CM-	SIP Station administered with an Auto Call	The "call-back" call, triggered due to auto-	7.0.1.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
10138	Back button	callback feature, would get dropped.	
CM-10408	SIP traffic	Occasionally, Communication Manager underwent a system reset under conditions of heavy SIP traffic	6.3.5.0
CM-10426	1. "(SA8967) - Mask CLI and Station Name for QSIG/ISDN Calls?" is enabled (set to "y") on the "system-parameters special-applications" SAT (System Access Terminal) form. 2. The "send-nn" feature button is set as "permanent" on an H.323 extension. 3. The station lock feature button is used, or the on-hook dialing feature is used, or team button is used to answer calls.	When SA8967 was enabled and feature button “send-nn” was permanently active, users could not deactivate the station lock feature using the feature button, nor use the on-hook dialing feature, nor answer calls using team button.	6.3.11.1
CM-10428	Call scenarios, such as transfer, which generate display update messages, under SIP traffic comprising of tandem calls.	Communication Manager underwent a system reset	6.3.12.0
CM-10463	1. "(SA8967) - Mask CLI and Station Name for QSIG/ISDN Calls?" is enabled (set to "y") on the "system-parameters special-applications" SAT (System Access Terminal) form. 2. The "send-nn" feature button is set as "permanent" on a button module.	When SA8967 was enabled and feature button “send-nn” was permanently active, the "send-nn" feature button lamp did not get updated when administered on a button module.	6.3.12.0
CM-10465	SIP traffic	Occasionally, Communication Manager underwent a system reset under conditions of heavy SIP traffic	6.3.1.0
CM-10484	1. Communication Manager with Computer Telephony Integration (CTI) configured and integrated with a CTI adjunct supported by Application Enablement Server (AES). 2. On the CM SAT (System Access Terminal) form "system-parameter features", the field "Station Tone Forward Disconnect:" set to "busy" or "intercept".	Monitoring a station to station call using the CTI adjunct caused the link between CM and AES to restart.	7.0.0.1.0
CM-10501	Communication Manager with Computer Telephony Integration (CTI) configured and integrated with a CTI adjunct supported by Application Enablement Server (AES)	For an incoming call over a trunk to a SIP extension, no CTI events were sent to the AES	7.0.0.2.0
CM-10507	More than 242 "Service Hours Tables" administered with locations.	Removal of locations on the CM SAT (System Access Terminal) "Locations" failed and the message "Error Encountered, Can't Complete Request" was displayed on the screen	6.3.7.0
CM-	Communication Manager with Computer	Occasionally, when a soft-phone in AES shared	6.3.8.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
10522	Telephony Integration (CTI) configured and integrated with a CTI adjunct supported by AES (Avaya Aura Application Enablement Services)	control mode re-registered, it caused the base set's TCP socket to close causing an active call to be dropped and the base set to unregister.	
CM-10586	Communication Manager with Computer Telephony Integration (CTI) configured and integrated with a CTI adjunct supported by AES (Avaya Aura Application Enablement Services)	For trunk calls monitored by the AES application, the connect event received by AES contained an incorrect Called Party Number	7.0.0.1.0
CM-10703	Administration on the CM SAT (System Access Terminal) "tandem-calling-party-number" (Tandem CPN) form.	An unrecoverable corruption on the Tandem CPN form encountered when entering a new line whose trunk group column overlapped with an existing line in the table	6.3.12.0
CM-10815	A Call Center setup integrated with a CMS (Call Management System) which is used to administer Agent skills on the system.	Multi-agent skill changes took many seconds to complete, increasing the chances of encountering contention errors when multiple administrators attempted simultaneous changes.	6.3.10.0
CM-10922	1. Communication Manager with CTI (Computer Telephony Integration) configured and integrated with a CTI adjunct supported by AES (Avaya Aura Application Enablement Services). 2. SIP stations which support the blind transfer feature (e.g., Avaya E.129 SIP phone or Yealink SIP-T46G).	Under certain SIP blind transfer scenarios, a CTI message would be sent to AES, which caused the CTI link on AES to bounce, and required some AES services to be restarted to recover. Occasionally, It would also take a reset system 2 or greater on CM to clean up this corruption.	7.0.0.1.0
CM-11018	1. Communication Manager with Computer Telephony Integration (CTI) configured and integrated with a CTI adjunct supported by Application Enablement Server (AES). 2. EC500 configured on SIP extensions 3. Feature Name Extension (FNE) for "Idle Appearance Select" configured	When the EC500 mapped SIP station dialed the FNE for "Idle Appearance Select", no CTI events were sent to AES	7.0.0.3.0
CM-11061	The CM6.3.x translations from which the upgrade to CM7.x occurs must have at least one entry with the "Any CPN" column administered in the CM SAT "calling-party-num-conv" form.	The message "Translation Corruption" would be displayed on the CM SAT (System Access Terminal) when logging in.	7.0.0.2.0
CM-11214	1. Communication Manager with CTI (Computer Telephony Integration) configured and integrated with a CTI adjunct supported by Avaya AES (Application Enablement Server). 2. An AES controlled Call recorder being used to record calls.	For incoming PSTN calls to a station on the Communication Manager, monitored by the recorder via AES, the recorder did not receive the Calling Party Number and the Trunk Identification.	7.0.0.3.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
CM-11401	Group page administered with one member on a media gateway.	Occasionally, a call made by a station on the same media gateway to the group page extension resulted in no talkpath.	7.0.0.3.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Fixes in Communication Manager 7.0.1.1.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-4073	SIP Trunk, DCP Station and VDN (Vector Directory Number)	An incoming SIP trunk call to a DCP Station routed via a VDN did not create a missed call log entry when the call was disconnected by the caller before being answered by the called party.	6.3.10.0
CM-6803	SIP Station	Under rare circumstances, owing to corruption in a SIP station's internal data structure, the station's call appearances became unresponsive which made the station unable to make or receive calls.	6.3.9.1
CM-8536	SIP call	Missed History-Info for inbound calls from SBC.	6.3.11.0
CM-8786	1. "SIP Endpoint Managed Transfer" is enabled on the "system-parameter features" SAT (System Access Terminal) form 2. Network Transition that causes the IP Address of the SIP endpoints to change.	The SIP Soft Client endpoint was unable to join the existing call after a network outage.	7.0.0.0
CM-9105	Media Gateways	Occasionally, Communication Manager underwent a system reset due to corrupted data structures.	6.3.6.0
CM-9234	An Agent logged onto a station configured with a Bridge Appearance of another station.	A conference call initiated by an agent using the Bridged Appearance of a principal station, caused the call appearance of the Principal station to become unresponsive when the Agent dropped off from the conference	6.3.12.0
CM-9318	1. SIP stations 2. Voice Mail	When a SIP endpoint transferred a call using a Feature Access Code, that contained a special character, to a Voice Mail, the transfer failed	6.3.10.0
CM-9408	SIP or H.323 Endpoints in Dual Registration mode and using Extend Call functionality, such as EC500	When the H.323 station had the first call appearance active on a call, and had another incoming call ringing on the second call appearance, then in some cases when the second call would be extended to a mobile phone, the two calls would incorrectly merge into a conference call.	6.3.10.0
CM-9744	Duplex system	Under very rare circumstances, after a server interchange, the new standby server did not relinquish the Processor Ethernet's alias address causing all IP applications, such as stations or gateways to behave abnormally	6.3.4.0
CM-9960	1. X-port station 2. One-X Agent 3. Call recording in Shared Control mode	On rare occasions with call recording active, when a Forced Unregistration request was sent to the extension on which the agent is logged in, the agent continued to be logged in instead of being	6.3.4.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
		logged out.	
CM-10082	The SIP response message received by Communication Manager contains more media lines in SDP than what was sent in the outgoing INVITE	Communication Manager experienced a reset	6.3.11.1
CM-10095	1. System comprising of a Main CM (Communication Manager) and an ESS (Enterprise Survivable Server). 2. H.323 Stations	H.323 Station call dropped when the main Communication Manager took over from an ESS.	6.3.11.0
CM-10104	Odd length SIP UUI in SIP messages.	Communication Manager added an extra "0" to odd length SIP User-to-User Information (UUI), which caused the SIP UUI to be incorrect.	6.3.12.0
CM-10446	Announcements with Media-Gateway or TN2501 VAL Boards.	Occasionally, announcements were played for a very short duration.	4.0.0.0
CM-10451	1. Call vectoring configured on CM (Communication Manager) where the vector contained a "route-to" step with "~r" 2. Incoming SIP trunk that does not support REFER	The call did not proceed to the next step in the vector if the "route-to" step with " ~r" failed to complete.	6.3.10.0
CM-10462	Calls transferred to an extension with Bridged Appearances of an extension that has coverage to voice mail administered.	Occasionally, calls that were transferred to an extension with bridged appearances/stations that covered to voice mail failed to drop the ringing bridged stations.	6.3.12.0
CM-10474	1. SIP Direct Media Call to an Avaya H.323 Agent 2. Non-Avaya H.323 Call Recording Port	Call Recorder did not receive any audio.	6.3.12.0
CM-10491	VAL or Media-Gateway Announcements	Occasionally, announcements could not be recorded.	6.3.10.0
CM-10530	1. Outgoing calls with an Application Enablement Services (AES) integrated call recorder used to record them. 2. System configured to record calls that are not answered.	Outgoing Computer Telephony Integrated (CTI) calls that received busy tone or were not answered did not get recorded.	6.3.8.0
CM-10532	A Call Center setup that includes a CMS (Call Management System) and is integrated with SIP adjuncts, such as IVR (Interactive Voice Response), or AAEP (Avaya Aura Enterprise Portal)	Under a very specific SIP messaging sequence, CMS showed inaccurate "hold" and "acd" durations being recorded for an Agent on an ACD (Automatic Call Distribution) call	6.3.12.0
CM-10578	Call Center Elite System	Under high traffic conditions, a large number of innocuous but unwanted Proc Errors were generated when agents resumed the calls that they	6.3.12.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
		had previously kept on hold	
CM-10585	Conference performed using a SIP trunk with the field "Identity for Calling Party Display" configured as "P-Asserted-Identity".	When the display information received over the SIP trunk did not contain the "P-Asserted-Identity" header, the display of the H.323 Endpoint failed to be updated.	7.0.1.0.0
CM-10591	One-X Mobile/OPTIM used to transfer calls.	The same port was occasionally assigned to multiple stations when transfers were performed with one-X Mobile/OPTIM stations.	6.3.0.0
CM-10621	A Call Center configuration with multiple VDNs (Vector Directory Numbers), VDN1 and VDN2.	When a call that termed to a VDN1 and finally to an agent was transferred successfully to a second agent via VDN2, incorrect information was being displayed on the second agent's display	6.3.11.0
CM-10677	Coverage of calls, established using 3PCC (Third Party Call Control), to a SIP integrated voice mail	Voice mail greeting was terminated midway	6.3.12.0
CM-10699	1. Communication Manager configured with multiple network regions 2. Remaining Bandwidth between Network Regions sufficient for only one call	Various call scenarios like bridging or call pickup failed even though the remaining bandwidth was sufficient.	7.0.1.0.0
CM-10726	1. Communication Manager with CTI (Computer Telephony Integration) configured and integrated with a CTI adjunct supported by Avaya AES (Application Enablement Server). 2. A third party Call recorder being used to record calls. 4. An incoming call over an IP Trunk to an IP Agent. 5. Shuffling enabled on the system	Occasionally, when a third party device used Single Step Conference to join a call between an IP trunk caller and an IP Agent, it did not receive any audio. In such cases, call Recording was affected.	6.3.9.0
CM-10750	SIP trunk	Communication Manager did not tandem unknown headers in 4xx/5xx Response Message	6.3.13.0
CM-10846	1. SIPCC Agents receiving calls through a VDN (Vector Directory Number) that plays an announcement 2. Multiple Communication Managers (CMs) or AAEP (Avaya Aura Enterprise Portal)	The active VDN identity was not displayed on the SIP station that finally received a call that re-entered the CM system with a specific SIP message that was generated during a transfer, and terminated to a VDN that played an announcement prior to queue the call to the agent's skill or routing to the station.	6.3.13.0
CM-10948	Communication Manager configured with "Multi-National Locations" and Shuffling enabled.	An incoming call over a SIP trunk to a DCP agent did not have talkpath if the SIP trunk and the agent used different Location Parameters	6.3.12.0
CM-11004	SIP trunks being used along with an	Owing to incorrect data in the history-info header, Avaya Communicator iPad dropped calls over a	6.3.13.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
	Avaya Communicator iPad	SIP trunk.	
CM-11049	Duplicated TN2602 Media Processor Boards	Occasionally, for a brief period of time, when the SAT (System Access Terminal) command "status media-processor board" was executed for the duplicated TN2602 board, the "Standby Refreshed" field showed a blank value.	2.0.0.0
CM-11060	1. "Expand ISDN Numbers to International for 1XCES" enabled on the "system-parameters features" SAT (System Access Terminal) form. 2. One-X CES used to make national calls.	An incorrect ANI was sent for one-X® CES national calls when "Expand ISDN Numbers to International for 1XCES" was enabled.	7.0.0.3.0
CM-11119	1. "(SA8904) - Location Based Call Type Analysis" enabled on Communication Manager (CM). 2. Incoming trunk call to an Attendant in Night Service 3. Call routed to an external number via UDP (Uniform Dial Plan)	Calls to the Attendant became unresponsive when the Attendant was in Night Service.	6.3.9.1
CM-11145	SIP traffic	Occasionally, Communication Manager underwent a system reset under conditions of heavy SIP traffic	7.0.0.0
CM-11149	An incoming call over a SIP trunk terming on an extension that covers, or has “call forward no-answer” configured to a another extension over a SIP trunk.	When Communication Manager received the initial INVITE without the SDP, the call dropped once coverage or "call-forward no-answer" was initiated.	6.3.11.1
CM-11238	SIP Call forward	The CM-SAT (Communication Manager- System Access Terminal) commands "monitor traffic trunk" and "status trunk" displayed conflicting information	6.3.13.0
CM-11251	"Extend-Call" initiated by Avaya Communicator for Android/iOS to a cellular endpoint	Call Appearance on the Avaya Communicator that was used to answer the incoming call continued to display the active call indication even though the call had been disconnected	6.3.113.0
CM-11262	Call Center setup integrated with an Avaya Aura Application Enablement Services (AES) application, such as Avaya DMCC (Device, Media and Call Control) H.323 Agents	Occasionally, network congestion caused incorrect lamp updates for ACD (Automatic Call Distribution) buttons on DMCC H.323 stations which resulted in dropped calls until the Hunt group queue was drained out	6.3.13.0
CM-11284	SAT connections via the TN799 CLAN board	Under rare circumstances, the creation and abandonment of SAT connections made via the TN799 CLAN board caused resource exhaustion leading to a system reset	6.3.11.1
CM-11288	Specific SIP messaging sequence arising out of tandem calls	Communication Manager underwent a system reset	6.3.11.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
CM-11306	H.323 endpoints	Occasionally, Communication Manager experienced a system restart if the TCP connections to the endpoints fluctuated	6.3.10.0
CM-11310	Call Center Elite, Service Observing Coaching, and SIP endpoints	Pressing the "voa-repeat" button while there was a coaching service observer active on the call cleared the coaching, however, no indication was sent to the SIP endpoints.	7.0.1.0.0
CM-11327	Call Center Elite	With "ACW Agents Considered Idle" set to "n" on the "system-parameters features" CM SAT (System Access Terminal) form, when a non-SIP agent transferred an ACD (Automatic Call Distribution) call and then entered into the ACW (After Call Work) state, either "manual-in" or "pending ACW", the agent was incorrectly considered idle.	6.3.12.0
CM-11332	Call Center setup with a VDN (Vector Directory number) and an associated Hunt group that has the field "ISDN/SIP Caller Display" field set to "mbr-name"	Occasionally, Communication Manager experienced a segmentation fault when a call made to the VDN termed to an agent	7.0.0.3.0
CM-11364	Call Center agents that have "auto-answer" set to "station," logged onto SIPCC endpoints that have "auto-answer" set to "acd".	When a SIP ACD (Automatic Call Distribution) call was delivered to a SIPCC agent when "Initial IP-IP Direct Media" was enabled on the involved signaling group(s), there was no talkpath.	7.0.0.2.0
CM-11383	Attendant making a call over a SIP trunk	When attendant calls over a SIP trunk and far end tries to transfer the call over to the same Communication Manager where attendant is registered, the display on the attendant was incorrect	7.0.0.3.0
CM-11394	Communication Manager Hospitality feature	When a call was made to a station that was busy on another call, the call log on the called station showed the caller extension number instead of the room number	6.3.13.0
CM-11430	Communication Manager integrated with an Avaya Aura Application Enablement Services (AES) application, such as Avaya DMCC (Device, Media and Call Control) Recorder	Occasionally, call recording failed when an H.323 Endpoint answered a call using the bridged appearance button	6.3.9.1
CM-11464	Remote Worker connected via SBC (Session Border Controller) in a call center configuration where agent calls are being recorded.	Calls between a Remote Worker and an Agent call did not get recorded	6.3.0.0
CM-11538	A survivable processor server under control of SDM (Solution Deployment Manager).	Occasionally, the trust between an LSP (Local Survivable Processor) or an ESS (Enterprise Survivable Server) and an SDM would cease to	7.0.0.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
		exist after a file sync occurred between the main and the survivable servers	
CM-11539	A Call Center configuration with multiple VDNs (Vector Directory Numbers) and agents transferring VDN calls.	A wrong VDN identity was displayed on an agent's display when the agent transferred a VDN call to another VDN.	7.0.0.2.0
CM-11556	H.323 Endpoints administered as 96x1 set type	The display on H.323 Endpoint that initiated and then completed an unsupervised conference, continued to show the "join" soft key	7.0.1.0.0
CM-11563	Multiple Locations feature enabled and use of the "list ars route-chosen" command	The "list ars route-chosen" SAT (System Access Terminal) command displayed an incorrect output for outpulsed 7 digit numbers.	6.3.13.0
CM-11564	CTI applications performing call control in CM (Communication Manager) via AES (Application Enablement Services) and ASAI (Adjunct Switch Application Interface)	ASAI events were not reported for monitored stations after a blind call transfer was performed.	7.0.0.3.1
CM-11574	Duplex systems	On rare occasions, after a system interchange, the message "Translation Corruption" would be displayed on the Communication Manager System Access Terminal) when logging in, and the "save translations" SAT command would be blocked.	6.3.6.0
CM-11588	The link used between the MG (Media Gateway) and the CM (Communication Manager) is encrypted using SRTP on the "ip-codec-set" SAT (System Access Terminal) form that is used between the Network Regions of the CM and MG	RFC4040 Data Calls between two endpoints supported by data modules failed to complete with the message "CONNECTING" being displayed on both endpoints	7.0.0.0
CM-11641	BSR (Best Services Routing) configured for Local Treatment and interflowing over SIP trunks without Initial Direct Media.	BSR calls interflowing over SIP trunks without Initial Direct Media failed to play local treatment when administered to do so.	6.3.10.0
CM-11658	CM (Communication Manager) integrated with an AES (Avaya Aura Application Enablement Services) application, such as Avaya DMCC (Device, Media and Call Control) Client or recorder	Occasionally, when the network connection between the Communication Manager and the recorder was lost, and the recorder re-registered with a new IP address and port, there would be no further recording of that call or any subsequent calls.	6.3.112.0
CM-11662	CTI (Computer Telephony Integration) applications performing call control in CM (Communication Manager) via AES (Application Enablement Services) and ASAI (Adjunct Switch Application Interface)	A UCID query of an inactive call returned with a zero value instead of a message indicating "No Active Call" which was misleading.	7.0.0.3.1

ID	Minimum Conditions	Visible symptoms	Release found in
CM-11724	Mis-configured SBC (Session Border Controller)	Occasionally, Communication Manager underwent a system reset when transmission of SIP messages were delayed because of underlying network issues	6.3.11.0
CM-11734	Greater than 500 DMCC (Device, Media and Call Control) endpoints registered on the system	A few endpoints continued to be registered on the main server after the media-gateways correctly migrated to a survivable server, ESS (Enterprise Survivable Server) or LSP (Local Survivable Processor), when the SAT (System Access Terminal) command "disable nr-registration" was executed for the Network Regions to which the media-gateways belonged.	6.3.12.0
CM-11742	1. Call Center Elite 2. CM (Communication Manager) system integrated with reporting adjuncts, such as IQ	Communication Manager sent erroneous messages to the reporting adjunct that incorrectly indicated that calls had failed	7.0.1.0.0
CM-11838	Emergency call made over a SIP trunk	The Emergency call would fail to complete if the calling party's name contained a special character	6.3.12.0
CM-11839	1. Call Center Elite configured without EAS (Expert Agent Selection). 2. CM (Communication Manager) system integrated with reporting adjuncts, such as IQ	The reporting adjunct failed to send messages to Call Center Elite.	7.0.0.3.0
CM-11864	SIP Trunks	Under rare circumstances, calls made to AAAD (Avaya Aura Agent Desktop) would become unresponsive	6.3.14.0
CM-11869	H.323 Endpoint	When the cable connecting the H.323 Endpoint to the network was unplugged, and the SAT (System Access terminal) command, "list registered-ip-stations" was executed, "n(o" instead of "no" was seen under the 'Skt' field	7.1.0.0.0
CM-11874	H.323 Endpoint	When the cable connecting the H.323 Endpoint to the network was unplugged, and the SAT (System Access terminal) command, "list registered-ip-stations" was executed, the Endpoint continued to appear as registered	7.1.0.0.0
CM-11875	1. SIP trunks 2. CM (Communication Manager) system integrated with reporting adjuncts, such as CMS (Call Management System)	When a specific SIP INVITE message was received while a call was in the vector processing state, CMS was unable to correctly report the call in the summary report for the skill or split involved.	6.3.10.0
CM-11877	The SIP incoming INVITE message received by CM (Communication Manager) contained no m-line in the	Communication Manager was unable to initiate new SIP trunk calls.	6.3.12.0

ID	Minimum Conditions	Visible symptoms	Release found in
	SDP		
CM-11912	Loss of connectivity between Communication Manager and the far end of the SIP signaling channel that was being used during heavy SIP call traffic	Invocation of LAR (Look Ahead Routing) was delayed which caused several calls to fail.	6.3.12.0
CM-11915	Attendant transferring a call over a trunk	Attendant was prompted for an Authorization Code even when they were not required to do so	6.3.12.0
CM-11919	The noted list trace SAT commands are used.	The "list trace station digits" and "list trace tac calling number" SAT (System Access Terminal) commands did not capture digit strings of variable length.	7.0.1.0.0
CM-11950	Incoming call over a SIP trunk	When an incoming SIP trunk call had "anonymous" as part of the URI, then this call could not be forwarded.	6.3.13.0
CM-11952	1. Communication Manager with CTI (Computer Telephony Integration) configured and integrated with a CTI adjunct 2. VDN (Vector Directory Number) with the fields "Allow VDN Override" and "VDN Override for ASAI Messages" enabled	The CTI event messages for Alerting, Offered, and Connected contained incorrect information for the Called Number IE (Information Element) when the call was routed through the VDN with "Allow VDN Override" and "VDN Override for ASAI Messages" enabled.	7.0.0.3.1
CM-11992	1. Announcements with TN2501 VAL Boards. 2. Heavy load on the Announcement Boards	Occasionally, announcements were played for a very short duration.	6.3.10.0
CM-12045	Small platform server.	Trunk related SNMP MIBs (Management Information Base) failed on small platforms, such as S8300D	6.3.113.0
CM-12087	1. Call Center Elite configured without EAS (Expert Agent Selection). 2. CM (Communication Manager) system integrated with reporting adjuncts, such as IQ or CMS R18 (Call Management System)	When using the SPI language 24 with CMS R18, several of the SPI messages were formatted incorrectly which either prevented the SPI link from sending messages, or caused inaccurate reporting.	7.0.0.3.1
CM-12111	All CM (Communication Manager) 7.0 systems using SMI (System Management Interface)	Run a Communication Manager backup of the OS set from the SMI displayed an error stating that the "cs_detail" file was missing.	7.0.0.3.0
CM-12112	All CM (Communication Manager) 7.0 systems	Running a Communication Manager backup displayed error messages without affecting the functionality of the backup	7.0.0.0
CM-12117	1. IPv6 being used by media-gateways	On a server interchange, the IPv6 shared alias	7.0.0.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
	or IP endpoints 2. Duplex System	address was not taken over by the new active server causing the IP endpoints and media-gateways to be unable to register via the IPv6 alias address.	
CM-12141	Incoming calls route through VDNs to vectors with route-to steps configured.	Incoming calls that routed through a Vector Directory Number (VDN) route-to step did not display Caller ID (CID) numbers.	6.3.14.0
CM-12142	Call Center Elite system integrated with a CMS (Call Management System)	Executing Add/Remove skills using a CMS client under high traffic conditions would cause the Communication Manager to undergo a reset. Other means of performing add/remove skill e.g. via CM-SAT or telnet do not cause a CM reset.	7.0.0.3.1
CM-12182	Codec G.729B administered exclusively on the "ip-codec-set" SAT (System Access Terminal) form that is used between the Network Regions containing CM (Communication Manager) and AMS (Avaya Aura Media Server)	Calls using AMS as the media resource failed.	7.0.1.0.0
CM-12265	Announcements with Media-Gateway or TN2501 VAL Boards.	Announcements could not be recorded owing to busy channels.	6.3.14.0
CM-12292	1. CTI applications performing call control in CM (Communication Manager) via AES (Application Enablement Services) and ASAI (Adjunct Switch Application Interface). 2. 3PCC (Third Party Call Control) configured on Communication Manager (CM) integrated with the AES	Calls initiated using the 3PCC "Make Call" functionality while the station was off-hook failed.	7.0.1.0.0
CM-12416	Filesync executed between a main server on CM6.3 and LSP (Local Survivable Processor) on CM7.0	The trust between the LSP and SMGR (System Manager) was broken when a filesync occurred	7.0.0.3.0
CM-12439	Multiple TN2501 Announcement boards.	Occasionally, TN2501 Announcement boards did not provide service after being moved physically	7.0.0.3.1
CM-12477	Video SRTP (Secure RTP) call made when Initial Direct Media was enabled on the involved Signaling Group	The Video call would be established as an RTP call when it should have used SRTP	7.0.1.1.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Fixes in Communication Manager 7.0.1.1.1

ID	Minimum Conditions	Visible symptoms	Release found in
CM-13677	Announcements with Media-Gateway or TN2501 VAL Boards.	Announcement stopped playing.	7.0.1.1.0

Fixes in Communication Manager 7.0.1.2.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-1067	Session Border Controller (SBC), Avaya Aura Communication Manager (CM), Remote agents, Experience Portal (EP), Avaya Call Recorder (ACR).	ACR did not start recording calls for remote agents.	6.3.2.0
CM-8722	1. VDN Return Destination feature enabled. 2. One-X Agent using Telecommuter mode i.e. "Other phone" mode "Permanent" Service Link Mode. 3. SIP trunk used for Service Link	In a Call Center setup with feature "VDN Return Destination" enabled, a SIP inbound VDN (Vector Directory Number) call had no talk path after it was redirected by a One-X Agent in Telecommuter mode using a SIP trunk as the service link.	6.3.10.0
CM-9442	Incoming H.323 call on a shared signaling group.	Communication Manager restart occurred, if Fast start elements received in incoming H.323 SETUP message.	6.3.12.0
CM-9860	Avaya Aura Communication Manager (CM) with endpoints being monitored by a Computer Telephony Integration (CTI) software and using the call parking feature	When CTI monitored endpoints parked calls and then unparked them, CM did not send a "Call Connected" notification to the CTI application after the unpark operation.	7.0.0.0
CM-10136	Multiple CMs (Communication Manager) with ISDN/H323 trunks and an H.323 station that is out of service	An incorrect ISDN Cause Value generated by Communication Manager for a call to a station, that was busy on another call, triggered a routing loop that caused the calling party to listen to silence for 15 seconds before being dropped	6.3.7.0
CM-10641	1. Avaya Aura Contact Center Elite with Session Border Controller (SBC). 2. Avaya Aura Experience Portal (AAEP). 3. Agents on Avaya Aura Communication Manager (CM) with call recording on Avaya Aura Call Recording (ACR). 4. The Contact Center has SIP trunks coming from service provider.	Avaya Call Recording (ACR) did not record incoming calls to Avaya Aura CC Elite agents.	7.0.0.0
CM-10814	System with H.323 Endpoints that are continuously Registering and Unregistering	Under rare circumstances, when H.323 stations registered and unregistered consistently, the H.323 registration count audit could not be completed which resulted in inaccurate data being recorded	6.3.11.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
CM-10870	An incoming call over a SIP trunk that is finally transferred to a Voice Mail Application, such as AAM (Avaya Aura Messaging)	Incorrect Voice Mail greeting was heard by the caller when a call over a SIP trunk covered to an Endpoint user who then transferred the call to AAM over a direct SIP trunk	6.3.112.0
CM-10991	Voice Mail System.	Incorrect calling party information was logged in the Call Detail Record (CDR), when a station dialed into the Voice Mail.	6.3.11.0
CM-11008	1. CM (Communication Manager) with PNs (Port Networks) or Media Gateways. 2. An ACW SIP Endpoint supporting media codec G.722	During a transfer/conference/hold action, a SIP endpoint on an already established 'direct-ip' call failed to connect to CM media anchors and was dropped.	7.0.1.0.0
CM-11025	1. Agent and Service Observing station belong to different Network regions 2. Service Observing Stations support only codec Set G.711 and the IP-codec-set that is used during the call does not support G.711	The service observer observed a loss in voice path	6.3.12.0
CM-11071	1. "Criteria for Logged OFF/PSA/TTI" enabled on the "change system-parameters" SAT (System Access Terminal) form. 2. Coverage criteria set to "All Calls"	The team button on the monitoring station kept flashing even after the call was dropped. This occurred only for calls that covered to monitored station.	6.3.4.0
CM-11302	CM7.0 Configurations	Under rare scenarios, putting the machine into or out of FIPS mode resulted in a corrupt /boot/initramfs file. This rendered the machine unable to boot.	7.0.0.1.0
CM-11405	SIP trunk Call transfer to Voice Mail	Under rare circumstances, Communication Manager experienced a reset	6.3.13.0
CM-11591	MST (Message Sequence Tracer) for ASAI (Adjunct Switch Application Interface) enabled on CM SAT (Communication Manager System Access Terminal)	Occasionally, CM encountered a warm restart	6.3.12.0
CM-11592	1. SIP trunk 2. CS1K 3. AAC (Avaya Aura Conferencing)	Under a specific SIP messaging sequence, one-way audio path was experienced for a call that used a SIP trunk configured between CM (Communication Manager) and CS1K when : 1) "Initial IP-IP Direct Media" was configured to "y" on the associated Signaling Group and 2) SIP messages sent by CM were compliant with RFC2833	6.3.13.0
CM-11706	CTI (Computer telephony Integration) being used along with a domain controlled station configured with a bridged appearance.	A CTI third party answer request over a domain control to answer an alerting call at a bridged appearance failed	7.0.0.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
CM-11763	Emergency Extension Forwarding feature being used on a system with agents configured and an SSC (Single Step Conference) monitoring/recording application.	The Emergency Extension Forwarding feature did not work (disconnected calls were not returned to the agent) for agents with an SSC monitoring/recording party on the call.	6.3.9.1
CM-11806	SOSM (System of Operative Search Measures) API	Shadowing of calls failed	7.0.0.2.0
CM-11831	The use of H.323 trunks on Communication Manager.	Occasionally, calls did not complete when H.323 trunks were involved.	6.3.10.0
CM-11840	WATS (Wide Area Telephony Service) trunk administered with TAC (Trunk Access Code)	The "Timed Outgoing Trunk Call Disconnect" feature configured by administering the field "Outgoing Trunk Disconnect Timer" on the SAT (System Access Terminal) COR (Class or Restriction) form to a timer value, did not disconnect outgoing WATS trunk calls	6.3.8.0
CM-11897	1. DECT (Digital Enhanced Cordless Telecommunications) stations and H.323 stations configured in a call-pickup group. 2. Incoming call over a trunk with "Send Name" disabled and "Send Calling Number" enabled on the "change trunk-group" form on SAT (System Access Terminal).	The IP-DECT station incorrectly displayed the name of the trunk-group instead of the number of the caller.	6.3.13.0
CM-11904	Avaya Aura Communication Manager (CM) with call recording on Avaya Aura Call Recording (ACR) and CTI integration using TSAPI.	Call recording did not stop when users started recording calls using Audix-rec button on endpoints.	7.0.0.3.1
CM-11925	Transfer of CTI (Computer Telephony Integrated) SIP calls to a VDN (Vector Directory Number) where one or more of the following conditions are satisfied: 1. VDN was monitored. 2. The associated vector contained a "wait" step prior to queueing the call to a skill. 3. Agent who answered the call was in auto-answer mode.	An incorrect CTI event stream resulted in the call being unexpectedly cleared when the call was redirected to the VDN using a "Refer" without a Replace SIP message.	7.0.0.0
CM-11949	TAC (Trunk Access Code) being used for dialing over an R2-MFC trunk	Secondary dial tone was not provided if an R2-MFC trunk was accessed via TAC dialing.	6.3.7.0
CM-12013	1. Communication Manager configured with One-X Customer Enablement Services (One-X CES). 2. One-X Attendant / Attendant Console.	The call log of CES user client is not updated with calling party number, when the caller was an Attendant.	6.3.12.0
CM-12028	H.323 TTS (Time-To-Service) TLS Endpoints configured	After a DUP PE (Duplicate Processor Ethernet) server interchange, the CM-SAT (Communication Manager System Access Terminal) "status socket usage" command	7.0.1.0.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
		continued to show "0" TLS sockets even when CM created outgoing TLS sockets on the H.323 TTS TLS endpoints	
CM-12036	Communication Manager configured with One-X Customer Enablement Services (One-X CES)	Under rare circumstances, ring-back was heard instead of talk-path when call was answered by an EC500 device.	6.3.12.0
CM-12067	Button label administered	Due to infinite loop Communication Manager interchange was observed.	6.3.11.1
CM-12068	Non Optim SIP trunk	Under a very specific SIP messaging sequence, for a call over a non-OPTIM SIP trunk, the caller was unable to hear the other end.	6.3.12.0
CM-12116	1. Communication Manager Hospitality feature 2. Call coverage to a Coverage Answer Group.	When a call covered to a station that was active on another call, the room number of the active call was over-written by the room number of the new incoming call. This resulted in the same room number being displayed on both call appearances.	6.3.14.0
CM-12124	A trunk call made using a One-X Communicator, using the "cpn-blk" button administered on it, to an unrouteable extension.	Using the "cpn-blk" feature button on a One-X Communicator to invoke a call to an extension that could not be routed, resulted in the call terminating on the calling station	6.3.13.0
CM-12127	H.323 Endpoints	After a network outage, a few time-to-service H.323 stations remained unresponsive	6.3.13.0
CM-12169	Avaya Aura Communication Manager, Computer Telephony Interface (CTI) application on Avaya Enablement Server (AES), Outbound Dialer and agents.	Customer information from Outbound dialers was not visible to CTI applications.	7.0.0.0
CM-12201	Chime calling, multiple IP connect PNs (Port Networks)	Answer back of a chime call resulted in one-way talkpath when the answering user was on a different PN than that of the chime port.	6.3.12.0
CM-12202	The Opus codec used both in Communication Manager and on the Radvision MCU (Multipoint Control Unit)	Occasionally, calls to a Radvision MCU did not complete when the Opus codec was being used.	7.0.1.0.0
CM-12231	1. SIP trunk 2. Fax call	Under a very specific SIP messaging sequence, long-duration FAX calls over a SIP trunk failed	6.3.112.0
CM-12251	SIP phone calling Virtual extension with remote coverage enabled.	"UNKNOWN NAME" was displayed on SIP Station, if call was placed to virtual extension and then covered to remote coverage point.	6.3.14.0
CM-12262	Avaya Aura Communication Manager (CM), Application Enablement Server (AES) and remote SIP agents (in telecommuter mode)	If agents using SIP telecommuter softphones logged in using DMCC application and quickly made a call, but did not answer the	6.3.13.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
	connected to CM using Device Media Call Control (DMCC) API.	call on their SIP softphone within 5 seconds, the outgoing call was not placed.	
CM-12268	Call Center System configured with reporting adjuncts, such as CMS (Call Management System) or IQ and integrated with an AAEP (Avaya Aura Enterprise Portal)	Under a very specific SIP messaging sequence, CMS or IQ were unable to accurately track the call if SIP connected adjuncts, such as AAEP redirected the calls over a trunk to a different system	6.3.11.1
CM-12300	Call Center Elite	In a Call Center Elite environment, when a skill was added to an agent who was active on a call and after the call entered into a Timed ACW state, the agent could receive a call on the new skill while still in ACW. Occasionally, this would cause CMS (Call Management System) to reset because data related to the agent's new skill was not updated on the CMS in time.	6.3.12.0
CM-12313	Interchange or a warm restart on a system configured with AMS (Avaya Media Server)	Occasionally, AMS went out of service under conditions of heavy traffic on the system	7.0.1.1.0
CM-12314	Transfer of a call over a SIP trunk involving a Service Observer	Occasionally, when a SIP adjunct redirected a call or dropped trunks shortly after a call was answered or delivered, while a Service Observer was in the process of joining the call and there were only two other parties on the call, the whole call dropped.	7.0.1.0.0
CM-12323	1. SIP trunk with Cisco SBC (Session Border Controller). 2. Call covers to SIP voice mail.	No talk-path after the call covered to SIP voice mail	6.3.14.0
CM-12326	AAC (Avaya Aura Conference) and Avaya Communicator	Avaya Communicator was unable to drop a call after it was put in an AAC conference call.	7.0.1.1.0
CM-12337	All known releases of Communication Manager.	Frequent internal process resets would result in a WARM restart of the system.	6.3.10.0
CM-12339	ACW CSDK 190 (Avaya Communicator for Window Client Software Development Kit 190)	Scopia audio conference could not be escalated to video by Avaya Communication for the Window client	7.0.1.0.0
CM-12341	1. Call Center Elite 2. Reporting Application, such as CMS (Call Management System)	CMS received an error "Cannot Perform the requested Operation. Administration contention. Try again later." on skill/vdn/vector changes	6.3.5.0
CM-12422	Field 'SIP ANAT Supported' enabled on trunk group form	Outgoing SIP messages from Communication Manager had sdp-anat in Supported header even when field 'SIP ANAT Supported' was disabled on trunk group form.	7.0.1.0.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
CM-12431	ICHT for PSTN Trunk.	Avaya Client Enablement Services based callback Call was failing, if "INCOMING CALL HANDLING TREATMENT" configured for PSTN trunk.	6.3.113.0
CM-12433	1. Communication Manager configured with One-X Customer Enablement Services (One-X CES) 2. Incoming call over H.323/SIP trunk. 3. ARS FAC is added to the called number through "inc-call-handling-trmt trunk-group" or through Trunk Group form on SAT (System Access Terminal). 4. Incoming call is routed to an internal station via ARS digit conversion. 5. Multiple Locations configured on CM.	One-X CES mobile application had incorrect call log, when it dialed to another internal station over trunk.	6.3.12.0
CM-12435	AMS (Avaya Media Server) on an inconsistent network	After a CM (Communication Manager) restart, the AMS occasionally went out of service.	7.0.1.0.0
CM-12482	SIP phone with missed call log support.	For incoming trunk call, missed call log entry was not logged on SIP station, if call forward feature was activated.	6.3.12.0
CM-12490	H.323 IP Agent	When the far end RTP address was received as NULL, an H.323 IP agent was unable to make the call	6.3.13.0
CM-12514	Duplex CM (Communication Manager) servers with multiple Avaya Aura Media Servers	CM interchange resulted in a system restart.	7.0.1.1.0
CM-12519	Calls being made between Communication Manager and an AS 5300 server	Occasionally, calls between Communication Manager and an AS 5300 server failed if G.722 was selected as the voice codec.	7.0.1.0.0
CM-12530	1. A Communication Manager configuration with Hunt Groups and agents using SIP softphones. 2. Shuffling enabled on the call	Agents using SIP softphones on Avaya Aura Communication Manager experienced either call drop or talkpath issues	6.3.13.0
CM-12540	H.323 hard phone registered in ANNEXH mode	Occasionally, If an H.323 hard phone registered in ANNEXH mode was moved from "named" to "unnamed", then this phone would wrongly be logged out by Communication Manager.	6.3.9.1
CM-12563	Duplicated CMs (Communication Managers) and Avaya Media Servers	A network outage triggering a CM server interchange caused all media servers to go out of service and remain in that state until all the existing calls ended.	7.0.1.0.0
CM-12564	SIP trunk to an external service provider	Under a very specific SIP messaging sequence, one way talk path was initially	6.3.113.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
		observed on a call over the external SIP trunk which finally led the call being dropped	
CM-12565	H.323 stations or H.323 trunks	Under rare circumstances, Communication Manager would undergo a reset when using H.323 stations or H.323 trunks	6.3.14.0
CM-12566	Administered announcements with recordings that are generating statistics over days while announcements are being administered.	Occasionally, there was no output when the CM-SAT (Communication Manager- System Access Terminal) command "list measurement announcement yesterday" was executed	6.3.113.0
CM-12588	Avaya Aura Communication Manager (CM), Attendants configured using an Attendant group, extensions which are monitored using TSAPI applications, PRI trunks for incoming calls and SIP trunks for outgoing calls.	When an external call (via PRI trunk) was transferred out of the PBX by an Attendant (in the Attendant group via SIP trunk) was routed back in the CM for an extension which was monitored, the application monitoring the extension never received a Ringing message.	7.0.0.0.0
CM-12625	Execution of a "list trace station" System Access Terminal (SAT) command, log review or denial event review for the following call scenario: 1. A station to station call. 2. The call is put on hold. 3. Music on Hold (MOH) is enabled. 3. The held station has Data Restriction enabled.	A denial event was not logged causing it to be absent from the "list trace station" System Access Terminal (SAT) command output when a traced station to station call was put on hold, and the held station had Data Restriction and Music on Hold enabled.	6.3.112.0
CM-12636	Agent in Telecommuter Mode using a Shared Control client to answer a call	No announcement was played if the telecommuter agent answered the call through the Avaya Enablement Service (AES) shared control client that performed the auto answer before the service link was up.	6.3.10.0
CM-12644	Execution of "status ip-network-region" CM-SAT (Communication Manager System Access Terminal) command	The output of the SAT 'status ip-network-region' command was incorrect.	6.3.11.1
CM-12675	1. Call Center Elite 2. Reporting Application, such as CMS (Call Management System)	Occasionally, the timestamp in messages that went into the reporting application appeared to move backwards for some message sequences.	6.3.14.0
CM-12692	Execution of "status" and "monitor" "socket-usage" CM-SAT (Communication Manager System Access Terminal) commands	The "Registered IP Endpoints with TCP Signaling Socket Established" field on the "status" and "monitor" "socket-usage" forms included data for TLS sockets rendering the results incorrect.	6.0.1.0
CM-12701	Avaya Aura Communication Manager (CM), Avaya Call Management System (CMS) and	When agents using CTI software used an Autodial feature, error messages like "Agent	6.3.114.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
	agents using Computer Telephony integration (CTI) software (developed using TSAPI API).	XXXX has two calls connected" were received by the CMS following which the CMS application became unresponsive and the CM to CMS link was disconnected.	
CM-12703	CM standard installation	For some ciphers, sftp (Secure File Transfer Protocol) failed for backup and restore	7.0.1.0.0
CM-12710	1. Bridge appearance on DCP station. 2. Incoming call to station transferred to principal. 3. "Display Information with Bridged Call" is disabled on "change system-parameters features" form on SAT (System Access Terminal).	Incoming call transferred to principal caused a display update on the bridge appearance on DCP station. The display did not get cleared even after the call was dropped.	6.3.113.0
CM-12729	Communication Manager	Occasionally Communication Manager underwent a System Reset	6.3.13.0
CM-12732	Incoming ISDN call on a SIP station	The SIP station displayed "Anonymous" in the call log instead of "info restricted" or no number, if the incoming ISDN call had restriction in the presentation and had no name and no number in the SETUP message.	6.3.14.0
CM-12733	Call Center System configured with reporting adjuncts, such as CMS (Call Management System)	CMS lost track of a call after an incoming call to a VDN (Vector Directory Number) went through a vector that immediately tandemed out over a trunk that failed the look-ahead and then tried a different trunk. This issue was reported when the vector's first step was not set to 'wait 0 hearing ringback', as is typically recommended.	6.3.114.0
CM-12745	Opus Audio Codec	In rare cases and over a long period of time, the use of the Opus audio codec led to failing call scenarios.	7.1.0.0.0
CM-12749	Non Optim SIP trunk	Occasionally, a SIP call would eventually be dropped if the far end SIP trunk sent a 200OK response with inactive SDP (Session Description Protocol) to CM (Communication Manager).	6.3.15.0
CM-12764	Administration of Multiple announcements with audio-groups.	Announcements could not be added, changed, or removed because of translation corruption.	6.3.13.0
CM-12770	Messaging applications, such as AAM (Avaya Aura Messaging) or Communication Manager Messaging (CMM)	The performance of messaging applications was impacted causing them to run slowly	7.0.0.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
CM-12771	3PCC (Third Party Call Control) configured on Communication Manager (CM) integrated with CTI (Computer Telephony Integration)	For a 3PCC Merge Request, the acknowledgment contained incorrect CTI information causing inconsistent call behavior.	7.0.0.0
CM-12806	1.DCP station 2.Incoming call to SIP trunk routed via UDP/ARS	When a DCP station made an outgoing call over SIP trunk, no call log was registered on the DCP station.	6.3.12.0
CM-12831	Avaya Aura Communication Manager (CM) with SIP endpoints being monitored by an application on the Application Enablement Server (AES).	When SIP endpoints went off the hook, the "Call Initiated" event was not sent by CM to the AES application.	7.0.1.0.0
CM-12835	Avaya Aura Communication Manager (CM) with analog/robbed-bit type DS1 trunks using "ANI*DNIS DTMF ANI" feature and endpoints being monitored by an application on the Application Enablement Server (AES).	For incoming calls to CM using analog/robbed-bit type DS1 trunks (with DTMF ANI feature enabled), the AES application did not show the incoming calling number.	7.0.1.0.0
CM-12847	Avaya Aura Communication Manager (CM) agents that are monitored using TSAPI applications and are being service observed (SO), SIP trunks for incoming calls.	When the "Agent/Caller Disconnect Tones" was enabled on CM and the TSAPI application was monitoring the agent's endpoint, trying to disconnect the call on the agent using the TSAPI application failed.	6.3.114.0
CM-12849	1. CM (Communication Manager) system with AAMS (Avaya Aura Media Server) providing tones. 2. At least one complex customized tone definition added via the "change tone" CM SAT (System Access Terminal) form	Call Progress tones which have more than 5 individual steps were not heard distinctly when played by AAMS.	7.0.0.0.0
CM-12854	1. Communication Manager with Computer Telephony Integration (CTI) configured and integrated with a CTI adjunct. 2. Call Center Configuration with ACD (Automatic Call Distribution) and Agents using SIP softphones 3. Shuffling enabled on SIP trunks	Occasionally, calls that involved a CTI transfer experienced talkpath disturbances	6.3.13.0
CM-12875	Call Center System using FAC (Feature Access Codes) to change Agent work-modes	In a Call Center environment, when the workmode of an agent was changed from AUX to Auto-in using a FAC, the active call would be dropped.	6.3.15.0
CM-12886	G.729 or G.729A codecs being used on the system	Occasionally, Communication Manager's error logs erroneously logged errors when using G.729 or G.729A codecs	7.1.0.0.0
CM-12888	SIP call	The calling phone continued to see the called destination identity even when the far end set the Privacy ID header in the response	6.3.113.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
		message.	
CM-12889	Avaya Aura Communication Manager (CM), agents using H.323 endpoints monitored by a TSAP application, VDN of origin announcement (VOA) configured on the Vector directory number (VDN) extension.	If VOA was administered on the VDN extension, agents using H.323 endpoints and TSAPI based CTI software received extra call alerting messages on the CTI software.	7.0.1.0.0
CM-12892	Administration of a large number of busy-indicator buttons.	Busy-indicator buttons could not be added even when the system add capacity to add more such buttons	6.3.12.0
CM-12912	Call Center System configured with reporting adjuncts, such as CMS (Call Management System) or IQ/APC and integrated with an SIP connected adjuncts, such as AAEP (Avaya Aura Enterprise Portal)	In an ICR (Please provide the full form) scenario, occasionally, a trunk was idled prematurely, thus preventing the CMS from further tracking the call.	6.3.14.0
CM-12963	SIP Direct Media Call and Conferencing 9.0 server.	Avaya Communicator 3.0 was not able to join conference on Conferencing 9.0 Server via Auto-Attendant number.	7.0.1.1.0
CM-12972	CM (Communication Manager) system configured with DS1 boards, such as TN464, TN767, and/or TN2464.	Occasionally, DS1 boards generated and cleared alarms that resulted in a system WARM restart.	6.3.13.0
CM-12980	CM (Communication Manager) system configured with Media Gateways and IP timing Synchronization (How is this configured)	Translation Corruption was seen on the system with memory configuration being shown as "Larg" instead of "Large"	7.0.1.0.0
CM-12994	1. Call Center Elite 2. CMS (Call Management System), version R18	When connected to R18 CMS, VuStats displayed the number of agent calls as two times the number that the agent actually attended.	7.0.1.0.0
CM-13010	A trunk group that is administered with 255 members	The 'list bcms trunk' CM-SAT (Communication Manager- System Access Terminal) command for the trunk group displayed a blank for the 'Number of Trunks' field on the form displayed	6.3.14.0
CM-13053	Avaya Aura Communication Manager (CM) with endpoints being monitored by a Computer Telephone Integration (CTI) application using TSAPI protocol with the endpoints having Bridge appearance or 'send-nn' buttons.	When CTI monitored endpoints originated calls using the Bridge appearance or send-nn button, the 'Call Connected/Established' event was never sent to the CTI application.	7.0.1.0.0
CM-13095	Administer the "IP SoftPhone" phone field on the CM SAT (Communication Manager System Access Terminal) "Station" form to 'y'.	While running the "display capacity" CM SAT command, the values for the fields "Limit" and "Available" for "Administered IP Softphones", on page 8, and "Softphone Enabled on Station Form", on page 11, were blank	6.3.14.0
CM-13126	1. Special Application SA8481 enabled.	When Special Application "(SA8481) -	6.3.14.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
	2. Device, Media and Call Control (DMCC) stations/applications.	Replace Calling Party Number with ASAI ANI?" was enabled on the "system-parameters special-applications" System Access Terminal (SAT) form, Device, Media and Call Control (DMCC) stations/applications used the Calling Line Identification (CLID) of the DMCC station/application instead of the CLID of the desk phone.	
CM-13132	SIP trunk call	Occasionally, under a very specific SIP messaging sequence that cause the SIP UPDATE message to loop, Communication Manager experienced segmentation faults or warm restarts	6.3.13.0
CM-13150	1. Call Center Elite 2. FAC (Feature Access Code) configured for "Auto-In"	When the "Auto-In" FAC was used to change the work-mode of an agent from "After Call Work" to "Auto-In" (available), the agent did not receive any calls when there were calls in queue.	7.0.1.0.0
CM-13278	Avaya Aura Communication Manager (CM) with agents and Vector Directory Numbers (VDNs) are being monitored by a Computer Telephone Integration (CTI) application using TSAPI protocol on the Avaya Enablement Server (AES) and a CTI application deciding VDN steps using 'adjunct-route' feature.	If an agent did a blind transfer to a VDN with 'adjunct-route' feature, the CTI application monitoring the VDN did not get a Call Alerting message.	7.0.1.0.0
CM-13280	Avaya Aura Communication Manager (CM) with agents or stations being monitored by a Computer Telephone Integration (CTI) application using TSAPI protocol on the Avaya Enablement Server (AES).	When an agent did not receive a call and the call was diverted to another agent, the CTI application monitoring the second agent did not get a 'Call Diverted' message.	7.0.1.0.0
CM-13306	None	On Page 7 of mst form, UID masks showed wrong value on display.	7.0.1.0.0
CM-13327	1. SIP trunk with 'Network Call Redirection' enabled 2. VDN (Vector Directory Number) associated with a vector that contained a "~r" step	A call to the VDN dropped after the execution of the "~r" step in the vector.	6.3.13.0
CM-13334	1. CM (Communication Manager) with CTI (Computer Telephony Integration) configured 2. AAEP (Avaya Aura Enterprise Portal)	When an incoming call to the CM routed to the AAEP and was then transferred over a SIP trunk to a VDN (Vector Directory Number) and finally to an Agent, an incorrect CTI stream was generated causing inconsistent call behavior	7.0.0.0
CM-13446	1. "(SA8965) - SIP Shuffling with SDP" disabled on "system-parameters special-	An Incoming trunk call that was answered,	6.3.6.0

ID	Minimum Conditions	Visible symptoms	Release found in
	applications" CM SAT (Communication Manager - System Access Terminal) form. 2. The field 'Shuffling with SDP' is enabled on the trunk group that is being used	but dropped after 30 seconds.	
CM-13482	1. CM (Communication Manager) system with AAMS (Avaya Aura Media Server) providing tones. 2. Use of a customized tone, added via the "change tone" CM SAT (System Access Terminal) form, that includes a final short duration tone and a "goto" step that goes to the first step of that tone	The tone played by the AMS was indistinct	7.0.1.1.0
CM-13536	Call Center System configured with reporting adjuncts, such as CMS (Call Management System) or IQ/APC and integrated with an SIP connected adjuncts, such as AAEP (Avaya Aura Enterprise Portal)	When an agent, after conferencing a caller over a SIP trunk that resulted in the call being queued to a hunt group or an Agent (Direct Agent Call), dropped out of the call and changed its mode to "After Call Work", the CMS stopped tracking the call. Eventually, the link between CMS and CM was reset.	6.3.13.0
CM-13605	Configuration of Tandem Calling Party Number Conversion CM SAT (Communication Manager System Access Terminal) form with multiple entries sharing the following characteristics: 1) Len = Any Len 2) Two or more entries in which the CPN Prefix has the same length	Translation Corruption was seen on the system after upgrading it CM6.3 to CM7.0	7.0.0.1.0
CM-13706	Avaya Call Recorder (ACR), Application Enablement Server (AES), Avaya Aura Communication Manager with SIP endpoints being monitored by the Computer Telephony Integration (CTI) software using TSAPI protocol.	When SIP endpoint (whose calls were being recorded by ACR and were being monitored by the CTI applications) transferred a call to another SIP application, the ACR did not stop recording the call for the transferring SIP endpoint even after the transfer was complete.	6.3.14.0
CM-13784	Avaya Aura Communication Manager (CM) with endpoints being monitored by a Computer Telephony Integration (CTI) software and using the call parking feature	When CTI monitored endpoints parked calls and then unparked them, CM did not send a "Call Connected" notification to the CTI application after the unpark operation.	7.0.1.0.0
CM-13856	Calls involving MDA (Multiple Device Access) devices and Breeze applications	When one MDA device dropped out of the call, with the other MDA device still active on the call, the entire call was dropped if SRTP Capability Negotiation was involved in this call.	6.3.15.0
CM-13924	Call Center with the "Multiple Call Handling" feature enabled on skills and splits	The Multiple Call Handling feature did not allow agents to handle multiple calls.	6.3.15.1

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
CM-14061	Avaya Aura Communication Manager (CM), Computer Telephony Interface (CTI) applications using Application Enablement Server (AES) application.	When a call being monitored by a CTI application was transferred to another party, the CTI application did not get a "Call Established" event when the transferred call was answered.	7.0.1.1.0
CM-14062	Avaya Aura Communication Manager (CM), Computer Telephony Interface (CTI) applications using Application Enablement Server (AES) application, H.323 and SIP endpoints being monitored by the CTI application.	When a SIP endpoint to SIP endpoint call was transferred to a H.323 endpoint and was diverted (deflected) to another H.323 endpoint using the CTI application, the "Diverted" and "Delivered" notifications were not sent to the CTI application.	7.0.1.1.0
CM-14080	Audio-group with an AAMS (Avaya Aura Media Server)	When administering an announcement that uses the AAMS as an announcement source, the message "Error Encountered, Can't Complete Request" was displayed on the screen	7.1.0.0.0
CM-14089	A Call Center configuration utilizing Automatic Call Distribution (ACD).	Agents were not available to receive calls after transferring an Automatic Call Distribution (ACD) call.	6.3.15.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Enhancements in Communication Manager 7.0.0.2.0

The following table lists the enhancements in this release.

ID	Minimum Conditions	Visible symptoms	Release found in
CM-4468	SIP Endpoints Display	Endpoint Display and call log prefixed with an international or national format based on SIP endpoint or Multiple Device Access (MDA) location.	N/A

Enhancements in Communication Manager 7.0.1.1.0

The following table lists the enhancements in this release.

ID	Minimum Conditions	Visible symptoms	Release found in
CM-10850	All systems with IP endpoints	The CM-SAT (Communication Manager-System Access Terminal) command "list registered-ip-stations" will now display the type of socket used, TLS or TCP, for endpoint registrations	N/A
CM-10851	All systems with IP endpoints	The CM-SAT (Communication Manager-System Access Terminal) command "status socket-usage" will now display information on TLS sockets being used for endpoint registrations	N/A
CM-7103	Interop between CM (Communication Manager) and CS1K UNIStim endpoints	SRTP calls will work between Communication Manager and CS1K using UNIStim endpoints	N/A
CM-9025	Use of the "list trace button" SAT (System Access Terminal) command	The "list trace button" SAT (System Access Terminal) command did not allow two endpoints to be traced The "list trace button" command can now be used to trace two endpoints simultaneously.	N/A

Enhancements in Communication Manager 7.0.1.2.0

The following table lists the enhancements in this release.

ID	Minimum Conditions	Visible symptoms	Release found in
CM-11427	Special Application SA9130 enabled.	Enabling new Special Application "(SA9130) - Authorization Code COR Toll Restriction & RCL Overrides Station COR" on the "system-parameters special-applications" System Access Terminal (SAT) form causes the toll and Restricted Call List (RCL) features to use the Authorization Code Class of Restriction	

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
		(COR) to check for restrictions. This is by design when the SA9130 is enabled.	
CM-12734	Use of the "list trace station" or "list trace tac" System Access Terminal (SAT) commands.	The "list trace station" and "list trace tac" System Access Terminal (SAT) commands have been enhanced to display whether private or public numbering is in use.	

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

Known issues and workarounds in Communication Manager 7.0.0.0 and 7.0.0.1

The following table lists the known issues, symptoms, and workarounds in Communication Manager 7.0.0.0 and 7.0.0.1

ID	Minimum conditions	Visible symptoms	Workaround
CM-6294		When the Communication Manager IP codec set was configured with 10-SRTP, 1-SRTP and None, the call between the H323 phone and the SIP phone did not shuffle.	
CM-6295		In high SIP call traffic situations involving Avaya Media Server resources, Communication Manager CPU Occupancy remained high.	
CM-6451		When the agent, caller and service observer were on a call using the VOA repeat button on the agent phone, the SO warning tones were played to all participants.	
CM-7120, **CM-7702,** **CM-7939**		Secure Indicator was not visible on a SIP phone, in any of the following circumstances: 1. If "Initial INVITE with SDP for secure calls?" on system parameter feature is set to N(o) 2. Call transferred on a SIP Phone as unattended or blind 3. Call transferred on a SIP Phone by other non SIP Phone	In the condition 3, do the following: Set Block Sending Calling Party Location in INVITE to (Y)es on SIP Trunk Group between Avaya Aura Communication Manager & Session Manager.
CM-7327		When three SIP phones were involved in a conference and SIP Network Call Redirection (NCR) was invoked, the resulting call had one-way talk path.	
CM-7566		Incorrect configuration of ESS resulted in the server performing multiple restarts.	
CM-7651		Secured call over H.323 trunk did not work between Avaya Aura Communication Manager 6.3 and Avaya Aura Communication Manager 7.0 with Avaya Media Server (AMS).	
CM-7865		While using the Solution Deployment Manager (SDM) of Avaya Aura System Manager, the System Management Interface (SMI) configuration pages for Communication Manger Duplex System did not restore.	

Known issues and workarounds in Communication Manager 7.0.0.3

The following table lists the known issues, symptoms, and workarounds in Communication Manager 7.0.0.3.

ID	Minimum conditions	Visible symptoms	Workaround
CM-9194	Duplex CM servers with a large number of IP endpoints.	Occasionally, sockets would get stranded after a server interchange on systems with a large number of IP endpoints.	

Known issues and workarounds in Communication Manager 7.0 for Avaya Video Conferencing Solutions

The following table lists the known issues, symptoms, and workarounds in Communication Manager 7.0 for Avaya Video Conferencing Solutions.

ID	Minimum conditions	Visible symptoms	Workaround
CM-A28		Far End Camera Control (FECC) does not work on point-to-point calls between Scopia XT H.323 endpoints and SIP video endpoint that supports FECC.	
CM-A92		Scopia Elite dialout calls to SIP video endpoints using H.323 protocol, for example, dialing the outbound call using a mismatched protocol type should go to the SIP trunk to Session Manager. Instead it results in the call flowing over the H.323 trunk to Communication manager. The call flow results in an audio-only call.	While creating terminals or endpoints on the Scopia Management server, be sure to properly assign the matching protocol type, SIP to SIP stations, and H.323 to H.323 stations.
CM-866		When the Avaya Communicator for Windows endpoint (feature sequenced by Communication Manager #1) is transferred into an XT SIP room system with an embedded MCU (feature sequenced by Communication Manager #2) that has an existing video call, the Avaya Communicator call might get dropped from the XT SIP MCU conference call.	
CM-1093		When a 9600 series endpoint conferences two OneX Communicator H.323 video endpoints that are both registered to a 2nd Communication Manager, the call results in ’audio only’ connection.	
CM-1117		When a OneX Communicator H.323 endpoint calls into a Scopia Elite MCU virtual room via the Session Manager to Scopia Management /Scopia Elite MCU SIP link using SRTP, the call results in ’audio only’ connection.	
CM-1352		When a 9600 series H.323 endpoint registered to Communication Manager 1 (CM1) calls an OneX Communicator H.323 endpoint registered to CM2 and then conferences in an Avaya Communicator for iPad that is sequenced by CM1, the Avaya Communicator for iPad is dropped from the conference call.	

ID	Minimum conditions	Visible symptoms	Workaround
CM-2079		When an OneX Communicator H.323 endpoint is on a video call and then receives another incoming video call from a SIP trunk that is originating from an H.323 video endpoint that is registered to a different Communication Manager, the 2nd incoming call might result in an audio only connection when answered.	
CM-4408		When a 9600 series endpoint conferences in two SIP video endpoints, the call results in 'audio only' connection.	
CM-5061		When a OneX Communicator SIP endpoint, that is in an encrypted enabled ip-network-region, is transferred to another OneX Communicator SIP endpoint, that is also in an encrypted enabled ip-network-region, via an endpoint that is in a non-encrypted ip-network-region, the call results in 'audio only' connection.	
CM-5368		When a video call is made from a SIP video endpoint to another SIP video endpoint that traverses over a Communication Manager H.323 trunk, the call results in audio only 'audio only' connection.	
CM-5684		When the consulted transfer of an XT H.323 room system to a SIP video endpoint is orchestrated by a OneX Communicator H.323 endpoint or a 96x1 audio endpoint, the transfer results in an 'audio only connection'.	
CM-6651		When an Avaya Communicator for Windows endpoint makes a video call to an XT SIP room system, de-escalates the call to audio, places that call on hold, makes a 2nd video call to a 2nd XT SIP room system and de-escalates that call to audio, and then transfers the 2nd XT SIP room system to the 1st XT SIP room system, the call results in 'audio only' connection.	
CM-6842		When an H.323 OneX Communicator dials into an virtual conference room that is hosted on an embedded MCU of an XT SIP Aura registered room system as a non-first participant, it connects as 'audio only'.	
CM-7768, CM-7806, CM-7880, CM-7890		Point-to-point video calls that result in an adhoc Communication Manager (CM) hosted conference, via endpoint associated features or subsequent feature invocation, may result in audio only connections. Features that can trigger an adhoc CM hosted conference include, but are not limited to, Avaya Call Recording (ACR), NICE call recording, One Touch Recording, or Service Observing.	
CM-8145		Non-SRTP video calls from a pre-7.0 CM to a CM 7.0 CM SRTP video endpoint; hold/resume results in dropped call.	
CM-8215		An SRTP video call from a 7.0 CM to a pre-7.0 CM non-SRTP video endpoint; hold/resume results in an audio-only call.	
CM-8292		When a OneX Communicator H.323 endpoint registered to Communication Manager #1 (CM1) makes a video call to a SIP video endpoint that is feature sequenced by Communication Manager #2 (CM2), and where CM1 and CM2 are connected via a SIP trunk, the call will result in poor video quality. When an XT H.323 endpoint makes a video call to a SIP video endpoint, the call will result in poor video quality. When an OneX Communicator H.323 endpoint registered to Communication Manager #1 (CM1) makes a video call to a OneX Communicator H.323 registered to Communication Manager #2 (CM2), and where CM1 and CM2 are connected via a SIP trunk, the call may drop.	

ID	Minimum conditions	Visible symptoms	Workaround
N/A		Video SRTP with OneX Communicator Release 6.2 has the following known issues: * SRTP video with H.323 endpoints is not supported. A best effort negotiation results in unencrypted video with encrypted audio. * When Communication Manager-based conferencing is used: - There may be a loss of video when a third audio-enabled or video-enabled endpoint is conferenced or bridged onto a point-to-point video call. - After the third endpoint drops from the conference, the video re-established between the other two endpoints will be RTP, not SRTP.	
N/A		With TLS and SRTP encryption enabled, video calls may sometimes lose video when the call is transferred or conferenced (CM-hosted conference).	
N/A		Video calls involving SIP video endpoints or video calls that traverse a SIP trunk might connect with audio only if the "Initial IP-IP Direct Media" field is not enabled in the SIP Signaling Group. This includes SIP Signaling Groups associated with SIP trunks that are used for feature sequencing of the SIP endpoints or any SIP trunk that is traversed as part of video call flow.	"Initial IP-IP Direct Media" field in the SIP Signaling Group must be enabled by setting it to "y".

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Known issues and workarounds in Communication Manager 7.0 Avaya Video Interop

The following table lists the known issues, symptoms, and workarounds in this release in Communication Manager 7.0 for Avaya Video Interop.

ID	Minimum conditions	Visible symptoms	Workaround
CM-866	Avaya Communicator for Windows endpoint XT SIP room system with an embedded MCU	When an Avaya Communicator for Windows endpoint (feature sequenced by Communication Manager #1) is transferred into an XT SIP room system with an embedded MCU (feature sequenced by Communication Manager #2) that has an existing video call, the Avaya Communicator call might get dropped from the XT SIP MCU conference call.	
CM-1093	9600 series endpoint Avaya OneX Communicator	When a 9600 series endpoint conferences two OneX Communicator H.323 video endpoints that are both registered to a 2nd Communication Manager, the call results in audio only.	
CM-1117	Avaya OneX Communicator Session Manager to Scopia Management / Scopia Elite MCU SIP link using SRTP	When an OneX Communicator H.323 endpoint calls into a Scopia Elite MCU virtual room via the Session Manager to Scopia Management / Scopia Elite MCU SIP link using SRTP, the call results in audio only.	
CM-1352	9600 series endpoint Avaya Communicator for iPad	When a 9600 series H.323 endpoint registered to Communication Manager 1 (CM1) calls an OneX Communicator H.323 endpoint registered to CM2 and then conferences in an Avaya Communicator for iPad that is sequenced by CM1, the call results in audio only and the call cannot be escalated to video from either client.	
CM-2079	Avaya OneX Communicator H.323 video endpoint	When an OneX Communicator H.323 endpoint is on a video call and then receives another incoming video call from a SIP trunk that is originating from an H.323 video endpoint that is registered to a different Communication Manager, the second incoming call might result in an audio only connection when answered.	
CM-4408	9600 series endpoint SIP video endpoints	When a 9600 series endpoint conferences in two SIP video endpoints, the call results in audio only.	
CM-5061	Avaya OneX Communicator SIP endpoint Encryption enabled /disabled ip-network-region	When an OneX Communicator SIP endpoint that is in an encrypted enabled ip-network-region, is transferred to another OneX Communicator SIP endpoint that is also in an encrypted enabled ip-network-region, via an endpoint that is in a non-encrypted ip-network-region, the call results in audio only.	
CM-5268	SIP video endpoints H.323 trunk	When a video call is made from a SIP video endpoint to another SIP video endpoint that traverses over a Communication Manager H.323 trunk, the call results in audio only.	

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum conditions	Visible symptoms	Workaround
CM-5667	XT H.323 room system SIP video endpoints	The consulted transfer of an XT H.323 room system to a SIP video endpoint results in an audio only connection when the transfer is orchestrated by an OneX Communicator H.323 endpoint or a 96x1 audio endpoint.	
CM-5684	SIP video endpoints	Video endpoints calling into a VDN (Vector Directory Number) and its associated vector routes the call to another video endpoint, this might result in an audio only connection.	
CM-6651	XT SIP room system Avaya Communicator for Windows endpoint	When an Avaya Communicator for Windows endpoint makes a video call to an XT SIP room system, de-escalates the call to audio, places that call on hold, makes another video call to another XT SIP room system and de-escalates that call to audio, and then transfers the that call to an XT SIP room system to the first XT SIP room system, the call results in audio only.	
CM-6842	H.323 OneX Communicator Embedded MCU of an XT SIP Aura	When an H.323 OneX Communicator dials into an virtual conference room that is hosted on an embedded MCU of an XT SIP Aura registered room system as a non-first participant, it connects as audio only.	
CM-8145	SRTP video endpoint Non-SRTP video calls	Non-SRTP video calls from a pre-7.0 CM to a CM 7.0 CM SRTP video endpoint; hold/resume results in dropped call.	
CM-8215	Non SRTP video endpoint SRTP video calls	An SRTP video call from a 7.0 CM to a pre-7.0 CM non-SRTP video endpoint; hold/resume results in audio only call.	
CM-8292	OneX Communicator H.323 endpoint XT H.323 endpoint SIP video endpoint SIP Trunk	When a OneX Communicator H.323 endpoint registered to Communication Manager #1 (CM1) makes a video call to a SIP video endpoint that is feature sequenced by Communication Manager #2 (CM2), and where CM1 and CM2 are connected via a SIP trunk, the call will result in poor video quality. When an XT H.323 endpoint makes a video call to a SIP video endpoint, the call will result in poor video quality. When a OneX Communicator H.323 endpoint registered to Communication Manager #1 (CM1) makes a video call to a OneX Communicator H.323 registered to Communication Manager #2 (CM2), and where CM1 and CM2 are connected via a SIP trunk, the call may drop.	
CM-A92		Scopia Elite dialout calls to SIP video endpoints using H.323 protocol, for example, dialing the outbound call using a mismatched protocol type, results in the call flowing over the H.323 trunk to Communication manager instead of the SIP trunk to Session Manager. The call flow results in an audio-only call.	While creating terminals or endpoints on the Scopia Management server, be sure to properly

ID	Minimum conditions	Visible symptoms	Workaround
			assign the matching protocol type, SIP to SIP stations and H.323 to H.323 stations.
CM-A28		Far End Camera Control (FECC) does not work on point-to-point calls between Scopia XT H.323 endpoints and SIP video endpoint that support FECC.	
N/A		Video SRTP with OneX Communicator Release 6.2 has the following known issues: * SRTP video with H.323 endpoints is not supported. A best effort negotiation results in unencrypted video with encrypted audio. * When Communication Manager-based conferencing is used: - There may be a loss of video when a third audio-enabled or video-enabled endpoint is conferenced or bridged onto a point-to-point video call. - After the third endpoint drops from the conference, the video re-established between the other two endpoints will be RTP, not SRTP.	"Initial IP-IP Direct Media" field in the SIP Signaling Group must be enabled by setting it to "y".
CM-7768 **CM-7806** **CM-7880** **CM-7890**		Point-to-point video calls that result in an adhoc Communication Manager (CM) hosted conference, via endpoint associated features or subsequent feature invocation, may result in audio only connections. Features that can trigger an adhoc CM hosted conference include, but are not limited to, Avaya Call Recording (ACR), NICE call recording, One Touch Recording, or Service Observing.	

Avaya Aura® Session Manager

Installation for Session Manager 7.0.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

Refer “Upgrading Avaya Aura® Session Manager" for more detailed information about upgrading your Session Manager. Note: the S8510 and S8800 servers are not supported on Session Manager 7.0 and later. Upgrades from prior releases running on those servers must include planning for a Server replacement.

All upgrades to 7.0.0.1 must be performed on a system running 7.0. Once the system is running 7.0, 7.0.0.1 will be applied as a patch using the System Manager - Solution Deployment Manager (SDM).

Special Case Upgrade Paths

1. From bare metal Session Managers

The supported upgrade paths to Session Manager 7.0 are from:

- SM 6.0 SP1 and subsequent service packs

- SM 6.1 and subsequent service packs

- SM 6.2 and subsequent 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 7.0.

2. VMware-based Session Manager

The supported upgrade paths to Session Manager 7.are from:

- SM 6.2 Service Pack 3 and SM 6.2 Service Pack 4 – after an upgrade of the OS

- SM 6.3.2 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 VE upgrade guide.

Troubleshooting the installation

Refer to Troubleshooting Avaya Aura® Session Manager.

Restoring software to previous version

Refer to product documentation.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

What's new in Session Manager Release 7.0.x.x

What's new in Session Manager Release 7.0.0.0

The following table lists enhancements in this release.

Enhancement	Description
SNMP Automatic Alarm Clearing for Avaya Aura® Session Manager Alarms	Currently, when an alarm is cleared in Session Manager there is no notification sent out via SNMP. This requires alarms to be manually cleared on systems monitoring Session Manager. With Release 7.0, Session Manager will automatically send a SNMP notice when an alarm has been cleared. This functionality applies to all alarms within Session Manager. This capability will ensure accurate reporting of response times for alarm clearing in SLA agreements.
Avaya Aura® Session Manager SIP Message Compaction	SIP by nature is an extensible protocol. Often, new enterprise features, particularly the ones for which no known standard/IETF mechanisms exist, results in the introduction of proprietary SIP headers and/or parameters using the SIP extension model. Avaya uses these SIP extensions from time to time to introduce Avaya proprietary headers/parameters for new features. Even though these extensions are correct per the SIP standards, customers have reported problems where a particular third-party SIP element could not handle the SIP messages from Avaya Aura® elements. It could be because the length of the full SIP message is too large and/or particular header(s) is too big to handle for a particular SIP element. In the past, in such conditions, customers had to find a way to deal with these incompatibilities. By adding a capability in Session Manager that removes the headers those non-Avaya elements may not need, Avaya Aura® customers will be able to achieve better interoperability without needing assistance of third-party elements. This capability will be a part of the adaptation modules of Session Manager.
Avaya Aura® Session Manager Emergency Call Notification to an Adjunct Emergency Location Server	Emergency Notification partners have started offering advanced crisis-alert features to enterprise customers. In large campus type settings, advanced applications (using LED displays near the main entrances, as an example) guide the emergency crew to the right location of the emergency call origination. To accomplish this capability, these applications need to know the location of the emergency caller. Applications use the following capabilities exposed by the Avaya Aura® components for this purpose: Session Manager shares the IP address (which is used to compute the location) of the user's SIP devices; Communication Manager shares the identity of the emergency caller. With the introduction of MDA (Multiple Device Access), a single user can register from multiple devices. This introduces an issue when establishing the exact location of the emergency caller. As part of the Emergency Call processing, CM notifies the identity of the emergency caller to the emergency application. However, because the caller has multiple devices registered, the emergency application cannot establish the exact location from where the user initiated the emergency call. Enhancements in this release to the existing SM AELS (Adjunct Emergency Location Server) will provide the specific device used by the user so more accurate location information can be determined.
Avaya Aura® Session Manager Maintenance Mode State	In order to support deployment and maintenance of large amounts of BSMs, a non-operational SM or BSM can be set to "Maintenance Mode". For consistency purposes both Core and Branch Session Managers will support "Maintenance Mode". An operational SM or BSM being set to "Maintenance Mode" is effectively taking a SM or BSM out of service. For a complete detailing of the Aura® Session Manager 7.0 release see the Avaya Aura® 7.0

Enhancement	Description
	Solution Offer Definition on the Avaya Sales Portal.
End To End Encryption Indicator	Session Manager and Communication Manager now support the ability for SIP end-points and clients (that support End to End Encryption Indicator) to display an indication that tells the end user whether the signaling and the media is secure end-to-end. The initial offer will only support SIP endpoint/clients on intra-enterprise point to point calls. This feature will be supported on the 96x1 SIP and the 1x-Communicator SIP soft client.
System License vs. Connection License	With the release of Avaya Aura® Session Manager 7.0, Connection licenses will no longer be required. Avaya Aura® Session Manager will now be available with unlimited connection use. A single system level license is now required for each Session Manager/Branch Session Manager instance. See the product ordering section of the offer definition for the codes required. Any instance upgrading from a previous release of Avaya Aura® Session Manager will automatically have their connection licenses converted to the system license at no charge.

What's new in Session Manager Release 7.0.0.1

The following table lists enhancements in this release.

Enhancement	Description
Increased Capacity for SIP Users/Devices on a Single BSM	Branch Session Manager will support a maximum of 5000 SIP Users/Devices per instance. In an appliance model, BSM shall support 1000 SIP users/devices (on the S8300E) and 5000 SIP users/devices (on CSR2 and beyond or equivalent).
Increased Capacity with a Single System Manager to 500 BSMs	A single System Manager will support up to 500 Branch Session Managers. This will still require at least two Communication Managers (250 max per CM).

What's new in Session Manager Release 7.0.1

The following table lists enhancements in this release.

Enhancement	Description
TLS Mutual Authentication Enhancement for SIP Devices	Session Manager (SM) 7.0.1 provides the ability for administrators to choose either No Mutual Authentication (NONE,) Soft Mutual Authentication (OPTIONAL,) or Hard Mutual Authentication (MANDATORY) when authenticating SIP devices. The default for upgrades, as well as greenfield installs, will be OPTIONAL (Soft Mutual Authentication in Avaya language.) Customers can decide to change it to None or MANDATORY, if needed. If the checkbox on System Manager indicates Hard Mutual Authentication (MANDATORY,) Session Manager shall reject the connection request if: • A client does not provide a cert or, • The client cert is not valid or trusted by SM.
Hunt Group Log in/Log out button for SIP phones in a non-CC Environment	H.323 users have the capability today to log in and out of hunt groups from a button on their set. They also see their status via a light on the set. These users cannot move to SIP desk phones until this same button capability is supported on those desk phones with SIP software. 9600 Series IP Desk phones with Desk phone SIP 7.0.1 or later software will now have a

Enhancement	Description
	button that a non-CC user may press to log themselves out of a hunt group. They can then press the button again to log back into the hunt group. The phone will have a visual indication of the user's status.
Validate with ESXi 6.0 in Virtualized Environment Offer	Besides ESXi 5.5, OVA files for Aura 7.0.1 components (SM, CM, SMGR, PS (via Avaya Breeze™), AES, US and WebLM) can now be deployed under VMWare ESX6i using the VE deployment model. (Note: this does not apply to the AVP deployment model.) This is the current shipping version of the VMWare Hypervisor offering and customers expect to be able to deploy Aura 7.X into this environment.
Support for new Avaya Common Servers (CSR3)	Adds support for HP DL360PG9 and Dell R630 in Avaya Virtual Deployment configurations.

What's new in Session Manager Release 7.0.1.2

The following table lists enhancements in this release.

Enhancement	Description
AADS	With this release of Avaya Aura, Avaya Aura Device Services is now supported. See the Avaya Aura® 7.0.1 Offer Definition (Dec 2016) posted on the Avaya Sales Portal.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Fixes in Session Manager Release 7.0.x.x

Fixes in Session Manager Release 7.0.0.1

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-159	Application must reference a SIP Entity with a "(" or ")" character in its name.	Administrator sees an XML parsing error when clicking on an Application in Application Sequence screen	6.3.4
ASM-51934	Input invalid Adaptation Matching Patterns via import of web service interfaces.	Call outage caused by Adaptation processing. Unable to save imported Adaptation Digit Conversion in Adaptation Details screen.	6.3.12
ASM-530	Do not configure ARS FAC1, but configure ARS FAC2.	There will be extra entries in dial plan sent to the endpoint. This can cause extra dial plan processing by the endpoint.	7.0.0.0
ASM-53012	Occurs when inbound INVITE has a PAI header that contains mixed case domain name (i.e. not all lower case domain name).	Session Manager does not generate proper Diversion header with STN in outbound INVITE during egress processing using Verizon adapter. As a result, the call may fail.	6.3.13
ASM-52831	Occurs due to race condition between processing of multiple calls with bandwidth needs in the same location. Requires that bandwidth limits be set on the location.	SM may intermittently deny calls with 488 response indicating insufficient bandwidth in location even though unused bandwidth is available.	6.3.12
ASM-52391	Call transfer or conference operation must be performed at the referenced user in order for the issue to be observed.	Calls originated with a Request-URI containing a user=phone parameter value (or other parameters) are not being counted for CAC	7.0.0.0
ASM-52247	Multiple SM's and PS cluster large enough such that PS may send PS-PS federated SUBSCRIBE request to an SM that is not the primary SM of the target user.	SM fails to route presence SUBSCRIBE for a user that is administered on a different SM. Presence status for the user is not available at the requesting user.	7.0.0.0
ASM-52213	[RHSA-2015:1699-01] Moderate: nss-softokn security update	N/A	7.0.0.0
ASM-52212	[RHSA-2015:1640-01] Moderate: pam security update	N/A	7.0.0.0
ASM-52170	[RHSA-2015:1457-01] Moderate: gnutls security and bug fix update	N/A	7.0.0.0
ASM-52054	[RHSA-2015:1459-01] Moderate: ntp security, bug fix,	N/A	7.0.0.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
	and enhancement update		
ASM-52051	[RHSA-2015:1634-01] Moderate: sqlite security update	N/A	7.0.0.0
ASM-52019	[RHSA-2015:1272-01] Moderate: kernel security, bug fix, and enhancement update	N/A	7.0.0.0
ASM-52017	[RHSA-2015:1513-01] Important: bind security update	N/A	7.0.0.0
ASM-192	[RHSA-2014:0321-01] Moderate: net-snmp security and bug fix update	N/A	7.0.0.0

Fixes in Session Manager Release 7.0.0.2

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-54030	SIP Call routing encounters a 503 response	Excessive alternate routing would occur in trying to complete the call.	6.3.15
ASM-53401	In slower networks, excessive Call Admission Control traffic occurs.	Numerous CAC queries were launched in an attempt to find available bandwidth for the call, resulting is system overload.	6.3.12
ASM-53711	Using SDM to apply a patch to a Branch Session Manager	Resulted in the patch not being displayed on the “Installed Patches” page. This incorrect status left the user without the ability to commit the patch.”	7.0.0.0

Fixes in Session Manager Release 7.0.1

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-53947	Use of white space in Application Sequence name	Application sequence is not invoked during call processing.	6.3.14
ASM-53486	Display SIP performance graphs for TLS connected entities	Performance graphs are not displayed properly for TLS connected SIP entities.	6.3.14
ASM-51713	[RHSA-2015:1447-01] Low: grep security, bug fix, and enhancement update.	N/A	6.3.15
ASM-318	[RHSA-2015:0794-01] Moderate: krb5 security update	N/A	6.3.13.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-350	Oracle Java Critical Patch Update	N/A	6.3.13.0
ASM-351	[RHSA-2015:0863-01] Moderate: glibc security and bug fix update	N/A	7.0.0.0
ASM-400	[RHSA-2015:1081-2] Important: kernel security and bug fix update	N/A	7.0.0.0
ASM-51714	[RHSA-2015:1460-01] Moderate: wireshark security, bug fix, and enhancement update	N/A	6.3.15
ASM-51715	[RHSA-2015:1254-02] Moderate: curl security, bug fix, and enhancement update	N/A	6.3.15
ASM-51716	[RHSA-2015:1330-01] Moderate: python security, bug fix, and enhancement update	N/A	6.3.15
ASM-51718	[RHSA-2015:1419-01] Low: libxml2 security and bug fix update	N/A	6.3.15
ASM-51720	[RHSA-2015:1482-01] Important: libuser security update	N/A	6.3.15
ASM-53364	[RHSA-2015:1981-01] nss, nss-util, and nspr security update	N/A	6.3.15
ASM-54041	[RHSA-2015:2549-01] Moderate: libxml2 security update	N/A	6.3.16
ASM-54042	[RHSA-2015:1930-01] Important: ntp security update	N/A	6.3.16
ASM-54306	[RHSA-2015:2617-01] Moderate: openssl security update	N/A	6.3.16
ASM-54307	[RHSA-2015:2636-01] Important: kernel security and bug fix update	N/A	6.3.16
ASM-54329	[RHSA-2016:0012-01] Moderate: gnutls security update	N/A	6.3.16
ASM-55185	[RHSA-2016:0063-01] Important: ntp security update	N/A	6.3.16

Fixes in Session Manager Release 7.0.1.1

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-55635	Use of external polling application.	Database outage caused by use of external application. See PSN4727u for details.	6.3.14
ASM-53368	Use of traceSM via customer login.	With this release we allow cust login account to read PPM traces (trace_ppm.log) generated with traceSM.	6.3.8
ASM-51713	Use of traceSM with PPM logs enabled.	Extensive logging could lead to system performance degradation.	7.0.0.2

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-56577	Use of endpoint managed transfer with odstd adaptation module.	Endpoint managed transfer operation may fail when there is an adaptation administered on the CM SIP Entity involved in the call that overrides the destination domain (‘odstd’ or ‘overrideDestinationDomain’ parameter).	6.3.15
ASM-55669	[RHSA-2016:0370-01] Critical: nss-util security update.	N/A	6.3.17
ASM-56234	[RHSA-2016:0428-01] Moderate: libssh2 security update.	N/A	6.3.17
ASM-56236	[RHSA-2016:0466-01] Moderate: openssh security update.	N/A	6.3.17
ASM-56237	[RHSA-2016:0494-01] Moderate: kernel security, bug fix, and enhancement update.	N/A	6.3.17
ASM-56240	[RHSA-2016:0459-01] Important: bind security update.	N/A	6.3.17
ASM-55667	[RHSA-2016:0301-01] "DROWN" Important: openssl security update.	N/A	6.3.17
ASM-57295	[RHSA-2016:0780-01] Moderate: ntp security and bug fix update.	N/A	6.3.17

Fixes in Session Manager Release 7.0.1.2

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-56235	A mixed TCP/UDP configuration where SIP adaptation is administered with the “reduceRtHdrs” (reduce Route headers) parameter	Call failures due to dropped SIP signaling messages	7.0.0.1
ASM-56119	SIP endpoint sends a SUBSCRIBE message to Session Manager at precisely the same time that Session Manager is trying to send a NOTIFY message to the endpoint.	Possible deadlock of SIP services. All calls fail.	6.3.15
ASM-57993	SM 7.0 systems	Large groups of old alarms randomly show up on System Manager / SNMP trap receivers	7.0.0.0
ASM-57976	System Manager 7.0 with pre 7.0 Session Managers that require NIC bonding administration.	Unable to administer NIC bonding for Session Managers running pre-7.0.	7.0.0.0
ASM-58351	Trace logging enabled for Routing Element Manager.	Error message appears on Dial Pattern administration screen when adding new dial	7.0.0.1

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
		pattern.	
ASM-56037	Multiple Session Managers deployed	Location Performance -> Bandwidth Usage graph "Total BW Available" value is excessive (multiplied by # of Session Managers).	6.3.10
ASM-58736	SM 7.0 systems	When adding an Entity Link from the SIP Entity page "endpoint conc" was not an available option for Connection Policy column.	7.0.1.0
ASM-51743	Using Root CA certificate without the Authority Key identifier extension.	HTTP (PPM) TLS connection failures and initial trust (initTM) configuration may have error logged for NULL Authority Key ID.	6.3.12
ASM-59263	Communication Manager configured with multiple locations and location specific dial plan entries.	96x1 endpoints will have default dialplan loaded instead of location specific dialplan.	7.0.0.1
ASM-58269	SIP session is refreshed with long session-refresh timer	SM may expire session after 60 minutes and further in-dialog messages for the call fail. User may experience call failures/drop.	7.0.0.0
ASM-57757	INVITE is sent to an entity that does not respond, except for 100 Trying.	Call counts on Session Manager dashboard continually climbing (for each call occurrence) and never decrements.	6.3.12
ASM-58528	Upgrade from an old SM release to 6.3 or later	After upgrade VerizonAdapter adaptation generates Diversion header without the username portion of the URI.	6.3.16
ASM-57972	[RHSA-2013:0668] Update for boost	N/A	7.0.0.0
ASM-57971	[RHSA-2014:0164] Update for MySQL	N/A	7.0.0.0
ASM-58021	[RHSA-2016:1292-01] libxml2 security update	N/A	7.0.0.0
ASM-58518	[RHSA-2016:0591-01] nss, nss-util, and nspr security, bug fix	N/A	7.0.0.0
ASM-58918	[RHSA-2016:1664-01] kernel security and bug fix update	N/A	7.0.0.0
ASM-58916	[RHSA-2016:1626-01] python security update	N/A	7.0.0.0
ASM-59502	[RHSA-2016:1940-01] openssl security update	N/A	7.0.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-58917	PostgreSQL 2016-08-11 Security Update Release	N/A	7.0.0.0
ASM-59501	[RHSA-2016:1944-01] bind security update	N/A	7.0.0.0
ASM-57694	[RHSA-2016:0760-01] file security, bug fix, and enhancement update	N/A	7.0.0.0

Known issues and workarounds in Session Manager 7.0.x.x

Known issues and workarounds in Session Manager Release 7.0.0.0

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

ID	Minimum conditions	Visible symptoms	Workaround
N/A	N/A	In Session Manager 7.0 additional validation has been added to ensure proper administration of server ports for SIP endpoint communications. Prior to completing an installation or upgrade for any SM or BSM that serves SIP endpoints, take care to ensure listen ports are added in the "Listen Ports" section on Home / Elements / Routing / SIP Entities page of the SMs and BSMs. In the case of upgrades, listen ports should be added after the Session Manager or Branch Session Manager is put into Deny New Service mode and upgraded, but before it's put back into Accept New Service mode. If no listen ports are configured on the SM or BSM, endpoints will fail to obtain correct sever information via PPM.	N/A
N/A	N/A	Whenever a new System Manager OVA is installed, or when the System Manager IP address is changed, all existing Session Manager licenses will become invalid. In this case it is necessary to obtain and install a new Session Manager license per normal procedures as described in the Deploying Avaya Aura® Session Manager 7.0 on VMware® guide.	N/A
N/A	N/A	If Pluggable Adaptation Modules (PAM) is installed on Session Manager, they will be removed as part of the upgrade process. Contact Avaya Professional Services (the PAM supplier) to re-install these after the upgrade.	N/A
N/A	N/A	If out-of-band management is being utilized on Session Manager, and both ports (eth0, eth2) are configured on different subnets, then it will be necessary to swap the port cables after the upgrade to preserve the intended connectivity.	N/A
ASM-32877	Changing Session Manager hostname without changing IP address	Loss of connectivity between System Manager and Session Manager.	Reboot the System Manager
ASM-392	Session Manager administration	The Session Manager communication profile does not get automatically checked when you select a value for primary Session Manager from the drop down.	Explicitly check the Session Manager Communication profile checkbox when creating a SIP user. If the box is unchecked then even if you fill in the values they won't be persisted in

ID	Minimum conditions	Visible symptoms	Workaround
			the database and you will need to edit the user again to fill in the values.
ASM-51741	Upgrade of a system where Centralized Call History is in use.	It is possible that SIP call logs maintained on the server will be lost upon the upgrade to Session Manager 7.0. This will result in the loss of logs the next time users login their SIP phone.	Restore the call logs on Session Manager from the last nightly or manual backup

Known issues and workarounds in Session Manager Release 7.0.0.1

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

ID	Minimum conditions	Visible symptoms	Workaround
ASM-53486	Display SIP performance graphs for TLS connected entities	Performance graphs are not displayed properly for TLS connected SIP entities.	None
ASM-51741	Upgrade of a system where Centralized Call History is in use.	It is possible that SIP call logs maintained on the server will be lost upon the upgrade to Session Manager 7.0.0.1. This will result in the loss of logs the next time users login their SIP phone	Restore the call logs on Session Manager from the last nightly or manual backup

Known issues and workarounds in Session Manager Release 7.0.0.2

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

ID	Minimum conditions	Visible symptoms	Workaround
ASM-53486	Display SIP performance graphs for TLS connected entities	Performance graphs are not displayed properly for TLS connected SIP entities.	None
ASM-	Upgrade of	It is possible that SIP call logs maintained on the server will be lost upon the	Restore the call

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum conditions	Visible symptoms	Workaround
51741	Session Manager	upgrade to Session Manager 7.0.0.2. This will result in the loss of logs the next time users login their SIP phone	logs on Session Manager from the last nightly or manual backup
ASM-53947	Use of white space in Application Sequence name	Application sequence is not invoked during call processing.	Remove white space from Application Sequence name

Known issues and workarounds in Session Manager Release 7.0.1

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

ID	Minimum conditions	Visible symptoms	Workaround
ASM-56461	Upgrading from Session Manager 6.3.X to 7.0.1.	For users with Centralized call history enabled, call logs will not be preserved across the upgrade.	Manually backup the call logs on 6.3.X. Once the first upgrade step to 7.0 has been accomplished, manually restore the call logs at that point. Then proceed with the upgrade to 7.0.1.
ASM-54129	Session Manager receives a SIP message with two Supported headers, one of which is empty.	In this case, Session Manager may forward the message with a malformed Supported header.	Eliminate the empty Supported header from the original SIP message.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Known issues and workarounds in Session Manager Release 7.0.1.1

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

ID	Minimum conditions	Visible symptoms	Workaround
ASM-56037	Use of Session manager performance graphs.	The "Location Performance" -> "Bandwidth Usage" graph shows an incorrect value of "Total BW Available". Same problem exists on the "Bandwidth Available" graph where the "Total BW A." and "Multimedia BW A." are also incorrect.	Divide the reported bandwidth number by the number of core Session Managers.
ASM-54129	Session Manager receives a SIP message with two Supported headers, one of which is empty.	In this case, Session Manager may forward the message with a malformed Supported header.	Eliminate the empty Supported header from the original SIP message.
ASM-57039	Adding a SIP phone contact with IM handle where case does not match administered IM handle.	The contact will be added as a private contact instead of an enterprise contact, and presence will not be available for the contact.	Ensure the added contact case matches the administered contact.
ASM-57976	Using System Manager 7.x to administer NIC bonding on a 6.x Session Manager.	The GUI method of administering NIC bonding no longer exists on 7.x System Manager.	A script has been created to work around this issue. Contact Avaya Services.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Known issues and workarounds in Session Manager Release 7.0.1.2

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

ID	Minimum conditions	Visible symptoms	Workaround
ASM-59577	HP G7/G8 server	Slow I/O on HP G7/G8 related to failed RAID Battery, and no alarm indication of the hardware problem	Use hardware_info command on the Session Manager server to status the RAID battery on HP G7/G8 Servers.
ASM-60090	CDR usage	Call Detail Records showing calls of duration of 9:59:54.	Contact Avaya Services
ASM-57039	Adding a SIP phone contact with IM handle where case does not match administered IM handle.	The contact will be added as a private contact instead of an enterprise contact, and presence will not be available for the contact.	Ensure the added contact case matches the administered contact.
ASM-58750	Move SIP Endpoints from one primary Session Manager to another.	Some users that have the primary Session Manager changed could lose the labels of the buttons.	Re-administer the button labels from System Manager.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Avaya Aura® System Manager

Installation for System Manager 7.0.x.x

Required patches for System Manager 7.0.0.0

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

Download ID	Patch	Notes
SMGR70GA001	Download System Manager 7.0 VE OVA from the Avaya PLDS website.	Verify that the md5sum for the downloaded OVA image matches the number on the Avaya PLDS website. SMGR-7.0.0.0.16266-e55-43-29-II.ova PLDS Download ID: SMGR70GA001 Size: 3,323 MB MD5SUM: 4cc7bb1ac1d1772d04832f0b79768323
SMGR70GA003	Download System Manager 7.0 SDM Client from the Avaya PLDS website.	Avaya_SDMClient_win64_7.0.0.1.17824_7.zip PLDS Download ID: SMGR70GA003 Size: 212 MB MD5SUM: 68c57b545feeaa6e09d0ad1f853d8ba8
SMGR70GA005	Download System Manager 7.0 VE Profile-3 OVA from the Avaya PLDS website	SMGR-PROFILE3-7.0.0.0.16266-e55-43-29-II.ova PLDS Download ID: SMGR70GA005 Size: 3,402 MB MD5SUM: 0a0de2f3cfaaa63489f34668e2793946

Note: To leverage deployment via Service Port using SDM client, get the SDM client Software from Avaya support site. The SDM client version available in the media does not support Service Port deployment.

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, and 6.3.x. Ensure that you run the data migration utility only on 7.0 release. Do not run the data migration utility on System Manager Release higher than 7.0 release. Refer to the document *Upgrading Avaya Aura® System Manager to Release 7.0* for more details.

Software	Notes
Download System Manager Data Migration Utility.	**Data_Migration_Utility_7.0.1.0_r96.bin** **PLDS Download ID**: SMGR70GA002 **Size**: 1 MB **MD5SUM:** 882b2c824f12e480aa656288d6b5905b

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Required patches for System Manager Release 7.0.0.1

Download ID	Patch	Notes
SMGR7001001	System_Manager_7.0.0.1_r70014212.bin	System Manager 7.0.0.1 software. System Manager 7.0.0.1 can be installed only on System Manager Release 7.0.0.0. **Size:** 806 MB **MD5SUM:** e3feb619a20eef411eccbcfe0bd0c068

Required patches for System Manager Release 7.0.0.2

Download ID	Patch	Notes
SMGR7002001	System_Manager_7.0.0.2_r70024416.bin	System Manager 7.0.0.2 software. System Manager 7.0.0.2 can be installed only on System Manager Release 7.0.0.0 or 7.0.0.1. **Size**: 910 MB **MD5SUM**: a91ea29e245f79be3d859f9c750b956d

Required patches for System Manager Release 7.0.1

Download ID	Patch	Notes
SMGR7010001	System_Manager_7.0.1.0_r701064859.bin	System Manager 7.0.1 software. System Manager 7.0.1 can be installed only on System Manager Release 7.0.0.0 or 7.0.0.1 or 7.0.0.2. **Size**: 1162 MB **MD5SUM:** 22e258da95c3060b52a8390cad682dc2
SMGR7010002	Download System Manager 7.0.1 SDM Client from the Avaya PLDS website.	**Avaya_SDMClient_win64_7.0.1.0.0620211_43.zip Size**: 243 MB **MD5SUM:** e8fed2ef03b1588a646a466cf7db7688

Required patches for System Manager Release 7.0.1.1

Download ID	Patch	Notes
SMGR7011001	System_Manager_7.0.1.1_r701105378.bin	System Manager 7.0.1.1 software. System Manager 7.0.1.1 can be installed only on System Manager Release 7.0.0.0 or 7.0.0.1 or 7.0.0.2 or 7.0.1.0 release. **Size**: 1270 MB **MD5SUM:** 81e7b0b45783e1259c08117504c310a3
SMGR7011002	Download System Manager 7.0.1.1 SDM Client from the Avaya PLDS website.	**Avaya_SDMClient_win64_7.0.1.1.0021752_58.zip Size**: 234 MB **MD5SUM:** a90e3f615ad5410d8c3ce61f6a2cfb3a

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Required patches for System Manager Release 7.0.1.2

Download ID	Patch	Notes
SMGR7012001	System_Manager_7.0.1.2_r701216007.bin	System Manager 7.0.1.2 software. System Manager 7.0.1.1 can be installed only on System Manager Release 7.0.0.0 or 7.0.0.1 or 7.0.0.2 or 7.0.1.0 or 7.0.1.1 release. **Size**: 1.2 GB **MD5SUM:** 9a34158086171426f930fe3bdb22c52f
SMGR7012002	Download System Manager 7.0.1.2 SDM Client from the Avaya PLDS website.	**Avaya_SDMClient_win64_7.0.1.2.0023440_2.zip** **Size**: 234 MB **MD5SUM:** 3a7a4c0dd44c1b549c2450048d01b0a9

Backing up System Manager Software

- Perform VMWare snapshot of the System Manager VM.

- Take System Manager Backup from System Manager Web console prior to upgrade activity.

Installing System Manager Release 7.0.0.1

Note: Patch install will not work with ASG login's init/inads and craft user. You must login as admin user to perform patch installation.

1. *Create a snapshot of System Manager virtual machine.*

   ***Note**: This activity might impact the services of System Manager and does not impact any other Avaya Aura Products, such as Session Manager, Presence Server, and Communication Manager.*

2. *Copy the patch installer file to the System Manager server.*
3. *Log in to the System Manager virtual machine as admin.*
4. *Verify md5sum of the bin file with the value from PLDS. (e3feb619a20eef411eccbcfe0bd0c068).*
5. *Run the patch installer using the following command:*

   # SMGRPatchdeploy <absolute path to the System_Manager_7.0.0.1_r70014212.bin file>

   When the system prompts, accept the EULA to continue the installation of the patch.

6. *Wait for the system to execute the patch installer and display the installer prompt.*
7. *Verify the service pack installation from below steps*
   - *Log on to the System Manager Web console.*
   - *On the top-right corner click on the settings icon and then select About. Verify that About page contains as below:*

     System Manager 7.0.0.1

     Build No. - 7.0.0.0.16266-7.0.9.7001011

     Software Update Revision No: 7.0.0.1.4212

   ***Note**: If the patch installation or upgrade is successful and the virtual application is functional, you can delete the snapshot.*

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

8. *If the Service Pack installation fails, use the VM snapshot manager to revert to a snapshot taken prior to patch installation.*

9. *After you upgrade the system to service pack 7.0.0.1, reboot the System Manager from System Manager CLI to get the updated kernel running in memory.*

Installing System Manager Release 7.0.0.2

Important Note: *Refer to section "resolution" mentioned in the PSN* PSN004602u *and apply if required, before installing System Manager Release 7.0.0.2 release.*

Patch install will not work with ASG login's init/inads and craft user. You must login as admin user to perform patch installation.

1. *Create a snapshot of System Manager virtual machine.*

   Note*: This activity might impact the services of System Manager and not of any other Avaya Aura Products like Session Manager/Presence Server/Communication Manager etc.*

2. *Copy the patch installer file to the System Manager server.*

3. *Log in to the System Manager virtual machine as admin.*

4. *Verify md5sum of the bin file with the value from PLDS. (*a91ea29e245f79be3d859f9c750b956d*).*

5. *Run the patch installer using the following command:*

   # SMGRPatchdeploy <absolute path to the System_Manager_7.0.0.2_r70024416.bin *file>*

   Note*: you will be prompted to accept the EULA. You must accept the EULA in order to install the patch.*

6. *Wait for the system to execute the patch installer and display the installer prompt.*

7. *Verify the service pack installation from below steps*

   - *Log on to the System Manager Web console.*
   - *On the top-right corner click on the settings icon and then select About. Verify that the About page contains as below:*

     System Manager 7.0.0.2

     Build No. - 7.0.0.0.16266-7.0.9.7002010

     Software Update Revision No: 7.0.0.2.4416

   Note*: If the patch installation or upgrade is successful and the virtual application is functional, you can delete the snapshot.*

8. *If the Service Pack installation fails, use the VM snapshot manager to revert to a snapshot taken prior to patch installation.*

9. *After you upgrade the system to service pack 7.0.0.2, reboot the System Manager from System Manager CLI to get the updated kernel running in memory.*

Installing System Manager Release 7.0.1

One can upgrade System Manager using Solution Deployment Manager (SDM) Client. For details, refer *Upgrading Avaya Aura® applications to Release 7.0.1 for upgrading Aura applications using Solution Deployment Manager (SDM)*. Alternatively,

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Note: This activity might impact the services of System Manager and does not impact any other Avaya Aura Products, such as Session Manager, Presence Server, and Communication Manager.

Patch install will not work with ASG login's init/inads and craft user. You must login as admin user to perform patch installation.

1. Create a snapshot of System Manager virtual machine.
2. Copy the patch installer file to the System Manager server.
3. Log in to the System Manager virtual machine as admin.
4. Verify md5sum of the bin file with the value from PLDS. (e02633e1b114f2fa23cd41b618da3f97).
5. Run the patch installer using the following command:

   # SMGRPatchdeploy <absolute path to the System_Manager_R7.0.1.0_S6_701064818.bin file>

   When the system prompts, accept the EULA to continue the installation of the patch.
6. Wait for the system to execute the patch installer and display the installer prompt.
7. Verify the feature pack installation from below steps
   - Log on to the System Manager Web console.
   - On the top-right corner click on the settings icon and then select About. Verify that About page contains as below:

     System Manager 7.0.1.0

     Build No. - 7.0.0.0.16266

     Software Update Revision No: 7.0.1.0.064841

   Note: If the patch installation or upgrade is successful and the virtual application is functional, you can delete the snapshot.
8. If the Feature Pack installation fails, use the VM snapshot manager to revert to a snapshot taken prior to patch installation.
9. After you upgrade the system to feature pack 7.0.1.0, reboot the System Manager from System Manager CLI to get the updated kernel running in memory.

Installing System Manager Release 7.0.1.1

One can upgrade System Manager using Solution Deployment Manager (SDM) Client. For details, refer "Using the Solution Deployment Manager client". https://downloads.avaya.com/css/P8/documents/101023857

Alternatively,

Note: This activity might impact the services of System Manager and does not impact any other Avaya Aura Products, such as Session Manager, Presence Server, and Communication Manager.

Patch install will not work with ASG login's init/inads and craft user. You must login as admin user to perform patch installation.

1. Create a snapshot of System Manager virtual machine.
2. Copy the patch installer file to the System Manager server.
3. Log in to the System Manager virtual machine as admin.
4. Verify md5sum of the bin file with the value from PLDS. (81e7b0b45783e1259c08117504c310a3).

5. Run the patch installer using the following command:

   # SMGRPatchdeploy <absolute path to the System_Manager_7.0.1.1_r701105378.bin file>

   When the system prompts, accept the EULA to continue the installation of the patch.
6. Wait for the system to execute the patch installer and display the installer prompt.
7. Verify the feature pack installation from below steps
   - Log on to the System Manager Web console.
   - On the top-right corner click on the settings icon and then select 'About'. Verify that About page contains as below:

     System Manager 7.0.1.1

     Build No. - 7.0.0.0.16266

     Software Update Revision No: 7.0.1.1.065378

     Service Pack 1

   Note: If the patch installation or upgrade is successful and the virtual application is functional, you can delete the snapshot.
8. If the Feature Pack installation fails, use the VM snapshot manager to revert to a snapshot taken prior to patch installation.
9. After you upgrade the system to feature pack 7.0.1.1, reboot the System Manager from System Manager CLI to get the updated kernel running in memory.

Software information

Software information Software	Version
CentOS	6.5 64-bit
OpenJDK	1.8 update 77 64-bit
Postgres	9.3.4
VMware vCenter Server, vSphere Client, ESXi Host	5.0, 5.1, 5.5, 6.0
JBoss	6.1
Supported Browsers	
Microsoft® Internet Explorer	9.x, 10.x, and 11.x
Mozilla® Firefox	40, 41,42

Note:

The SMGR command-line interface (CLI) password expires after 60 days. Geographic redundancy operation will stop working. Set new password on both primary and secondary System Manager then Geographic redundancy operation will start working.

Installing System Manager Release 7.0.1.2

IMPORTANT: If System Manager Installation is a Geo-Redundancy enabled deployment, disable Geo-Redundancy and apply the patch on both Primary and Secondary System Manager Systems, and then re-enable Geo-Redundancy

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

One can upgrade System Manager using Solution Deployment Manager (SDM) Client. For details, refer “Using the Solution Deployment Manager client”. https://downloads.avaya.com/css/P8/documents/101023857

Alternatively,

Note: This activity might impact the services of System Manager and does not impact any other Avaya Aura Products, such as Session Manager, Presence Server, and Communication Manager.

Patch install will not work with ASG login’s init/inads and craft user. You must login as admin user to perform patch installation.

1. Create a snapshot of System Manager virtual machine.
2. Copy the patch installer file to the System Manager server.
3. Log in to the System Manager virtual machine as admin.
4. Verify md5sum of the bin file with the value from PLDS (9a34158086171426f930fe3bdb22c52f).
5. Run the patch installer using the following command:

   # SMGRPatchdeploy <absolute path to the System_Manager_7.0.1.2_r701216007.bin file>

   When the system prompts, accept the EULA to continue the installation of the patch.
6. Wait for the system to execute the patch installer and display the installer prompt.
7. Verify the feature pack installation from below steps
   - Log on to the System Manager Web console.
   - On the top-right corner click on the settings icon and then select About. Verify that About page contains as below:

     System Manager 7.0.1.2

     Build No. - 7.0.0.0.16266

     Software Update Revision No: 7.0.1.2.086007

     Service Pack 2

   Note: If the patch installation or upgrade is successful and the virtual application is functional, you can delete the snapshot.
8. If the Feature Pack installation fails, use the VM snapshot manager to revert to a snapshot taken prior to patch installation.
9. After you upgrade the system to feature pack 7.0.1.2, reboot the System Manager from System Manager CLI to get the updated kernel running in memory.

Software information

Software information Software	Version
CentOS	6.5 64-bit
OpenJDK	1.8 update 77 64-bit
Postgres	9.3.4
VMware vCenter Server, vSphere Client, ESXi Host	5.0, 5.1, 5.5, 6.0
JBoss	6.1

Software information Software	Version
Supported Browsers	
Internet Explorer	9.x, 10.x, and 11.x
Firefox	43.0, 44.0, and 45.0

Note

The System Manager command-line interface (CLI) password expires after 60 days. Geographic redundancy operation will stop working. Set new password on both primary and secondary System Manager then Geographic redundancy operation will start working.

Troubleshooting the installation

- Execute following command from System Manager CLI with admin user credentials to collect logs and contact support team.

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

This will create a file (LogsBackup_xx_xx_xx_xxxxxx.tar.gz) @ /tmp location.

- Download the following user manuals from https://support.avaya.com.

Download ID	Patch	Notes
Not available	Not applicable	Administering Avaya Aura® System Manager for Release 7.0.1 for administering System Manager.
Not available	Not applicable	Deploying Avaya Aura® System Manager 7.0.1 on VMware for System Manager on VMware installation, configuration, and upgrade information.
Not available	Not applicable	Upgrading Avaya Aura® System Manager to 7.0.1 on Vmware for System Manager Upgrade on VMware information.
Not available	Not applicable	Deploying Avaya Aura® applications for deploying Aura applications using System Manager Solution Deployment Manager (SDM) and Solution Deployment Manager – Client (SDM-Client).
Not available	Not applicable	Upgrading Avaya Aura® applications to Release 7.0.1 for upgrading Aura applications using Solution Deployment Manager (SDM).
Not available	Not applicable	Migrating from System Platform to Avaya Appliance Virtualization Platform for installing and upgrading AVP.
Note: Deploying Avaya Aura® applications and Upgrading Avaya Aura® applications include the Installing SDM client procedure.		

Restoring software to previous version

The versions*.xml is published on ftp://ftp.avaya.com/incoming/Up1cku9/tsoweb/SUM/

If the Feature Pack installation fails, use the VM snapshot manager to revert to a snapshot taken prior to patch installation.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

What’s new in System Manager Release 7.0.x.x

What’s new in System Manager Release 7.0.1

The following table lists enhancements in this release.

Enhancement	Description
Solution Deployment Manager (SDM) Client	• Support for port flexibility while installing Solution Deployment Manager (SDM) Client. • Direct upgrade to System Manager Release 7.0.0.x and System Manager release 7.0.1 using SDM Client. • Support for certificate management for Appliance Virtualization Platform (AVP) host, ESXi host and vCenter. This will come into picture while adding and editing host and vCenter. One can also re-generate and accept the certificate for AVP. For VE, it will be marked as failure if the certificate mismatches. • To enhance security while using vCenter, SDM supports use of a FQDN for the vCenter. vCenter does not put IP addresses in its certificates and therefore the FQDN is required to confirm server identity via the certificate in SDM.
Solution Deployment Manager (SDM)	• Solution Deployment Manager (SDM) UI supports real-time application state display. • SDM UI supports displaying and changing AVP Host Settings (Network Settings Display and Control): As an AVP customer, user can display and change the network settings from SDM on an AVP host with regards to NIC teaming and port speed setting. • Support for real time data update for hosts (License Status) and virtual machine state (VM State). • Support for new SDM Dashboard and VM deployment page (Wizard based). • SDM UI Support for Host Reset and Shutdown. • SDM supports Avaya Aura 7.0.x Applications in an ESXi 6.0 VE environment. • Direct Service Pack and Feature Pack upgrade to release 7.0.0.x and release 7.0.1 using SDM upgrade manager. Products supports: Communication Manager, Session Manager, Branch Session Manager and Utility Services. • Support for save and edit upgrade configurations. • Support for cleanup of scheduled upgrade jobs. It will bring the products to ready for upgrade state on SDM upgrade manager. • Support for CLI utility to enable/disable SSH on AVP • Support for certificate management for AVP host, ESXi host and vCenter. This will come into picture while adding and editing host and vCenter. One can also re-generate and accept the certificate for AVP. For VE, it will be marked as failure if the certificate mismatches. • To enhance security while using vCenter, SDM supports use of a FQDN for the vCenter. vCenter does not put IP addresses in its certificates and therefore the FQDN is required to confirm server identity via the certificate in SDM.

Enhancement	Description
	• Support for Custom Patching for elements: Session Manager, Branch Session Manager, Utility Services, Communications Manager and WebLM (R7.0.1 onwards). • New Upload Component integrated with Download Management. Following is supported: o Upload up to 2GB file from Firefox. o Upload up to 4 GB file from Chrome. o Microsoft® Internet Explorer is not supported. • Enhanced TN Boards and Media Modules User Interface(UI) and work flow to include different use cases: o TN boards and Media modules will now show hardware version and slot number on SDM UI.(Upgrade flow is not supported for previously added TN/MM which do not show hardware in the name) o Re-run CM/MG discovery to remove and re-add TN/MM with new UI on name. o Use cases includes: ▪ Support for any type of TN or Media module whose type is not added in Manage Elements, they will get added as others. ▪ Swapping and removing of TN /MM and re-running discovery of CM/MG. ▪ Upgrade flow with the new UI.
Communication Manager (CM) Concurrency	• Enhanced System Manager-Communication Manager reliability by pooling CM Connections. • User Interface (UI) is provided to configure the number of connection pools. The administrator can view the connection usage through GUI. For NCM and cut-through objects, connections will be picked up from this connection pool for processing and once the pool gets exhausted, live connections will be thereafter created for the CM. • This will address the concern that when 3rd party applications were exhausting CM connections, System Manager were failing to connect to CM. • Support for add/remove Agent Skill from SIP Phone. • Support for VOA Repeat/Interrupt for SIP CC Phone. • Support for Live Streaming MOH on Media Server from an external source. • Support for Analog Phone Types: CallrId and K2500 • Support for hunt group busy position button for 96x1 SIP phones in a non-Contact Center Environment. **Note:** In System Manager web console, Manage Endpoints → Endpoint Editor, button 'hntpos-bsy' is introduced in Communication Manager 7.0.1. One can configure Endpoint Templates version 7.0 with this button but for applying this template, one will need to upgrade the Communication Manager 7.0.1.
Localization	• Support for Localization of System Manager User Management UI in Canadian French.
Capacity	• Increased User/Device Capacities on Branch Session Manager • Support up to 500 Branch Session Managers (BSMs)

Enhancement	Description
Platform Upgrade	- OpenJDK upgraded to 1.8 update 77. - Support for ESXi 6.0.
System Manager Geographic Redundancy	- Enhanced System Manager Geographic Redundancy to remove the pre-requisite of having the Primary and Secondary Server with same hardware such as Dell PowerEdge R620 Server. Primary and Secondary server must possess the similar hardware architecture (For e.g. both servers should have 64 bit architecture). Geographic Redundancy setup checklist has been updated in the Admin guide.
Avaya Aura® Device Services	- Support for off-pbx-telephone feature-name-extensions in CM Sync.
User bulk import and export Enhancements	- An option to export user data by using Excel or XML files - Time zone field for Avaya Aura Messaging subscribers - Support for CallrId and K2500 Set types: displayCallerId; callerIdMsgWaitingIndication and recallRotaryDigit in Endpoint schema file. - Fields auxAgentConsideredIdleMIA added in Agent schema file.

Note:

1. As vCenter operation is blocked by IP, for old vCenter which has been added, user need to provide new valid FQDN in EDIT vCenter, and save it.
2. Regarding Host Certificate Management feature:
    - For existing VE Host, generate the valid certificate on host and update the host certificate in SDM.
    - For existing AVP host, regenerate the Host cert from **More** options.
    - For existing vCenter, Edit vCenter and accept the vCenter valid certificate.

What's new in System Manager Release 7.0.1.1

Enhancement	Description
Element Manager	- Support for Officelinx 10.1.

What's new in System Manager Release 7.0.1.2

Enhancement	Description
Element Manager	On January 23, 2017, Avaya will introduce the Avaya Equinox™ 9.0 Conferencing application. To support that introduction in an Avaya Aura environment, the framework for supporting Avaya Equinox™ from System Manager has been added to the 7.0.1.2 Service Pack. Planned support from System Manager includes: Single Sign On from the Elements Page; the ability to add an Equinox server into the Inventory; and a new Equinox Conferencing 'Communication Profile' in the User Management area. To support Avaya Equinox™ 9.0 on System Manager 7.0.1.2, customers should load patch mentioned in PSN004799u on to System Manager 7.0.1.2. The patch is available on PLDS downloads under Avaya Aura System Manager. The patch provides one security fix and enhances rollback and failure scenarios. Refer PSN004799u - https://downloads.avaya.com/css/P8/documents/101035680 more details.

Enhancement	Description
	In upcoming releases of System Manager additional integration of User Management features will be available. The following System Manager features will be available in a future release: 1. Support the Equinox Conferencing 'Communications Profile' associated with a User from the following User Management utilities: • Bulk Import/Export Utility (XML and Excel) for User Management • User Profile Rules to include Equinox Conferencing 'Communications Profile' • Web Services API to include Equinox Conferencing 'Communications Profile' • Self-Provisioning Portal (Password change) to include Equinox Conferencing Password • Bulk Editor to include Equinox Conferencing 'Communications Profile' 2. Integrate Equinox Software Management into the System Manager Solution Deployment Manager Avaya Equinox™ includes the convergence of all of our Avaya soft clients, Avaya Aura Conferencing and Avaya Scopia into a single channel calling, messaging, collaboration and Conferencing solution for mobiles, browsers, desktops and room systems.

Fixes in Avaya Aura® System Manager 7.0.x.x

Fixes in System Manager 7.0.0.1

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-34575	Infrastructure	In keeping with NIST guidelines and industry best practices, Avaya is rotating the security keys associated with remote maintenance access through the Avaya Security Gateway (ASG).	7.0.0.0
SMGR-34414	Security Updates	Oracle Java Critical Patch Update (October 2015)	7.0.0.0
SMGR-34207	Security Updates	[RHSA-2015:1920-01] Critical: java-1.7.0-openjdk security update (RHSA-2015-1920)	7.0.0.0
SMGR-34001	Security Updates	[RHSA-2015:0863-01] Moderate: glibc security and bug fix update (RHSA-2015-0863)	7.0.0.0
SMGR-33993	Security Updates	[RHSA-2015:1330-01] Moderate: python security, bug fix, and enhancement update	7.0.0.0
SMGR-33955	Security Updates	[RHSA-2015:1457-01] Moderate: gnutls security and bug fix update (RHSA-2015-1457)	7.0.0.0
SMGR-33951	Security Updates	[RHSA-2015:1471-01] Important: bind security update (RHSA-2015-1471)	7.0.0.0
SMGR-33941	Security Updates	[RHSA-2015:1081-01] Important: kernel security, bug fix, and enhancement update (RHSA-2015-1081) (RHSA-2015-1272)	7.0.0.0
SMGR-33911	Security Updates	[RHSA-2015:1185-01] Moderate: nss security update (RHSA-2015-1185)	7.0.0.0
SMGR-33909	Security Updates	[RHSA-2015:1419-01] Low: libxml2 security and bug fix update	7.0.0.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release introduced
		(RHSA-2015-1419)	
SMGR-33840	Security Updates	[RHSA-2015:1482-01] Important: libuser security update (RHSA-2015-1482)	7.0.0.0
SMGR-33832	Security Updates	[RHSA-2015:1459-01] Moderate: ntp security, bug fix, and enhancement update	7.0.0.0
SMGR-33681	Security Updates	[RHSA-2015:1840-01] Important: openldap security update	7.0.0.0
SMGR-33600	Security Updates	[RHSA-2015:1640-01] Moderate: pam security update	7.0.0.0
SMGR-33597	Security Updates	[RHSA-2015:1699-01] Moderate: nss-softokn security update	7.0.0.0
SMGR-33595	Security Updates	[RHSA-2015:1708-01] Important: libXfont security update	7.0.0.0
SMGR-33591	Security Updates	[RHSA-2015-1623] kernel security and bug fix update	7.0.0.0
SMGR-33589	Security Updates	[RHSA-2015:1634-01] Moderate: sqlite security update	7.0.0.0
SMGR-34425	Security Updates	Java Security Provider changes for Elliptic Curve cryptography	7.0.0.0
SMGR-34406	Infrastructure	Update for Turkey 2015 DST changes	N/A
SMGR-34198	Infrastructure	System Manager (Quartz Component) sending traffic to external server (www.terracotta.org/157.189.192.67) for version update check.	6.3.x
SMGR-34570	Infrastructure	Define idle timeout explicitly in the data source to reduce the database connections.	6.3.x
SMGR-33182	Infrastructure	Disable JMS failure delivery to Dead Letter Queue to avoid unwanted memory accumulation.	6.3.x
SMGR-33255	Data Replication Management	Out of memory on EDP JBoss Component when lot of data is being synched through Data Replication.	7.0.0.0
SMGR-32813	Data Replication Management	Data Replication Sync tables size increases due to monitor batch thread not sending the batch error notification if it fails the first time.	6.3.x
SMGR-34442	User Management	Unable to update user with Communication Profile password only if "History" is checked in Communication Profile Password Policy and also Enforce policy against previously used passwords is not getting applied to user while changing the communication profile password for a user.	6.3.x
SMGR-34439	User Management	Unable to delete user permanently due to database constraints associated with user private contact and private contact information.	6.3.x
SMGR-33695	User Management	If telephone number in AD does not start with ‘+’ prefix then the first digit of telephone number is getting replaced with prefix ‘+’ in E164 handle.	6.3.x
SMGR-33694	User Management	Allow admin user to provide only '+' value in ‘Prefix for Avaya E164 Handle’ attribute in User Provisioning Rule configuration.	6.3.x
SMGR-33579	User Management	Rename label "Authentication Type" to “User Type” in Identity section of User Management Page.	6.3.x

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-33330	User Management	Updating the existing users for Avaya E164 handle with new directory synchronization mapping “Telephone Number -> Phone Number” will result in failure if the existing users are created through UPR and DSE having mapping “Telephone Number -> businessPhone”	6.3.x
SMGR-33211	User Management	Communication profile (SIP) password change done through self-provisioning is not transmitted other elements like AAC so authentication is failing for member on AAC.	6.3.x
SMGR-32951	User Management	Provide correct error message if user creation is failed due to missing value for User Provisioning Rule name value in user’s associated data in AD.	6.3.x
SMGR-34526	Global Search Component	Global search filter does not give any result if search started with character "?", "*" or "+".	7.0.0.0
SMGR-34524	Global Search Component	Global search filter does not open user details window if Localize Display name or Endpoint Display Name contains special characters	6.3.x
SMGR-30520	Global Search Component	Chinese, Japanese and Korean) characters are displaying as “?”	7.0.0.0
SMGR-29041	Global Search Component	Search Component behaves inconsistently if search by object type	7.0.0.0
SMGR-34690	Tenant Management	Error message is shown if user is updated from user associated with Tenant admin role.	7.0.0.0
SMGR-33581	Inventory Management	Change IP FQDN is failing in Primary System Manager. Enable Geo Replication is failing after executing Pair IP FQDN in Primary System Manager. Change IPFQDN-Corresponding System Manager Manage Elements attributes not updated	7.0.0.0
SMGR-32909	Inventory Management	IP Office / UCM / App Server Elements display a warning in manage elements as GEO unaware elements.	7.0.0.0
SMGR-33187	Inventory Management	Corporate Directory, IPsec, Numbering Groups, Patches, Secure FTP Token, SNMP Profiles, Software Deployment element links from Element Manager page is not opening correct linked page.	7.0.0.0
SMGR-33663	Role Management	Non admin user is unable to make System Configuration changes on IPOfficev2 even when all the IPO Permissions are provided for user.	7.0.0.0
SMGR-32391	Trust Management	Certificates are not auto renewed on Secondary (standby) System Manager Server.	6.3.x
SMGR-34810	Communication Manager Management	If an agent is updated using an agent template the skills are not updated properly.	6.3.14
SMGR-34795	Communication Manager Management	Error noticed while launching global endpoint change page.	7.0.0.0
SMGR-34448	Communication	Wrong System Manager administrator getting set on Communication	6.3.x

ID	Minimum Conditions	Visible symptoms	Release introduced
	Manager Management	Manager logs via the "change secondary-user" command before an administration task is performed	
SMGR-34390	Communication Manager Management	Unable to add buttons that have a second option via System Manager User Interface when the endpoint had a set type that is an alias	6.3.14
SMGR-34180	Communication Manager Management	Endpoint data is getting replaced by other user's data if multiple users are accessing endpoint editor at same time.	6.3.14
SMGR-33973	Communication Manager Management	User associated with custom role unable to configure just buttons in spite of role having permission to edit the button.	6.3.x
SMGR-33970	Communication Manager Management	Station profile settings revert back to default if station associated user's first name, last name, display name or extension voicemail, security code updated from User Management or Web Service or Directory Synchronization. Missing Label names on station form after changing the Endpoint Display Name on Identity tab of User Management.	6.3.x
SMGR-33924	Communication Manager Management	Stations available list show the station that are already in use while adding new station.	6.3.14
SMGR-33321	Communication Manager Management	For CM 7.0, add/edit Station of XMOBILE set type not able to configure Mobility Trunk Group field from System Manager.	7.0.0.0
SMGR-33895	Communication Manager Management	Triple ring option not available for call pickup feature on Endpoint editor	7.0.0.0
SMGR-34623	Solution Deployment Manager	Solution Deployment Manager server URL does not allow for tcp port to be specified.	7.0.0.0
SMGR-33633	Solution Deployment Manager-Client	If a previously defined AVP Host becomes unavailable, e.g. crash, network issue, a Host Refresh continues indefinitely and cannot be stopped, even if the host becomes available again.	7.0.0.0
SMGR-33216	Solution Deployment Manager-Client	After deployment of Utility server OVA, the manual refresh operation of AVP host is never ending, this results no other OVAs can be deployed on the AVP.	7.0.0.0
SMGR-34418	Solution Deployment Manager	“Resume” on SDM Upgrade management populates an additional tab “Upgrade / Upgrade to” when Refresh button is clicked.	7.0.0.0
SMGR-34421	Solution Deployment Manager	Upgrade or migration of Communication Manager from 5.2.1 to CM 7.0 using Solution Deployment Manager fails in some scenarios.	7.0.0.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-33585	Software Upgrade Management	Analyze is not working as expected for Media Gateways and Media Modules if Hardware info is empty.	6.3.x
SMGR-34217	Software Upgrade Management	If user download file from PLDS using FTP protocol in Linux system, Download manager page show download has been completed 100 %,but actually file didn't get download the in software library.	6.3.x
SMGR-33532	Software Upgrade Management	Scheduling more than one patch to apply on a CM is not working properly.	6.3.x
SMGR-32874	Software Upgrade Management	Write community is not marked as mandatory while adding the SNMP detail of Communication Manager Inventory.	6.3.x
SMGR-33333	Solution Deployment Manager	No error description is getting displayed on the Analyze status page if it is failing.	7.0.0.0

Fixes in System Manager 7.0.0.2

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-35174	Security Updates	[RHSA-2015:1930-01] Important: ntp security update	7.0.0.0
SMGR-35172	Security Updates	[RHSA-2015:1930-01] Important: ntp security update	7.0.0.0
SMGR-34553	Security Updates	RHSA-2015:1980-01] Critical: nss, nss-util, and nspr security update	7.0.0.0
SMGR-33993	Security Updates	[RHSA-2015:1330-01] Moderate: python security, bug fix, and enhancement update	7.0.0.0
SMGR-30163	Infrastructure	Change of 'admin' password on CLI is not asked when user is logged in via console through VCenter	7.0.0.0
SMGR-35454	Infrastructure	BackupRestoreAgent standard session objects not getting released	6.3.15
SMGR-35353	Infrastructure	Comet objects not getting cleared from memory in 24 hours in some cases.	6.3.15
SMGR-34846	Backup and Restore	Backup job success but file is in corrupted state causing restore results in loss of svar files.	7.0.0.1
SMGR-34496	Data Replication	Manual replication repair of a large number of EDPs while under traffic load fails to synchronize	7.0.0.1
SMGR-35472	User Management	While Importing Users using xml file having newLoginName field creates unexpected user	6.3.15
SMGR-35466	Software Upgrade Management	Some UI fields of System Platform element are missing from Inventory after System Manager upgrade from 6.2.x.	7.0.0.0
SMGR-35049	Software Upgrade Management	Incorrect / multiple discoveries of TN's packs, if removed / replaced / swapped with same TN pack with different H/W and F/W.	7.0.0.0
SMGR-35048	Software Upgrade Management	CM deletion from inventory is not deleting TN's from inventory.	7.0.0.0
SMGR-34869	Software Upgrade Management	GetInventory is not working if System Platform and Communication Manager both are added.	6.3.14
SMGR-34867	Software Upgrade Management	Unable to upgrade firmware of TN2312BP, not showing its parent in Upgrade Management.	7.0.0.0
SMGR-35290	Inventory Management	Change host name for a host from VM management, the change of the name is not reflected in Manage Elements.	7.0.0.0
SMGR-35253	Communication Manager Management	After deleting the report from the ‘Generation’ tab, ‘Edit’, ‘Run Now’, and ‘Delete’ buttons are still enabled.	7.0.0.0
SMGR-35571	Communication Manager Management	Communication Manager Management objects accumulating in the heap causing slowness	6.3.15
SMGR-35120	Communication	Role based authentication is not working properly for some objects	6.3.15

ID	Minimum Conditions	Visible symptoms	Release introduced
	Manager Management	like Hunt Group in case of Duplex CM once interchange happens	
SMGR-34888	Communication Manager Management	"list holiday-table count 50" didn’t work while init Sync, if CM have license for 10,	6.3.14
SMGR-34840	Communication Manager Management	Unable to edit the station, if keeping empty fields before or in between extensions in the intercom-group page	6.3.14
SMGR-35665	Communication Manager Management	Error message when editing station by user assigned particular role.	6.3.12
SMGR-35115	Communication Manager Management	Button labels/modules/profiles settings reverted back to default values in custom template if template is created from user management-> endpoint editor or CM -> Manage Endpoints	6.3.15
SMGR-35243	Trust Management	Trust fails between System Manager and elements (ex: PS and AMS), when Two CA’s are in active state in System Manager Certificate authorities (New and old CA).	7.0.0.0
SMGR-34942	Geo Redundancy	GEO configuration should fail if VFQDN is different on Primary server and Secondary Server.	6.3.x

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Fixes in System Manager 7.0.1

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-35064	Alarm Management	Minor alarms regarding weblm_legacy certificate was prevalent on upgraded System Manager.	7.0.0.1
SMGR-31346	Geographic Redundancy	Geographic Redundancy configuration fails as the setup of CND replication fails in case System Manager has Sub CA configured.	7.0.0.0; 6.3.11
SMGR-31270	Certificate Management	Auto Renew or Manual Certificate renewal is not working	6.3.1.0
SMGR-32391	Certificate Management	Certificates are not auto renewed on Secondary(standby) System Manager server	6.3.1.0
SMGR-33330	User Management	Updating the existing users for Avaya E164 handle with new mapping “Telephone Number → Phone Number” will result in failure if the existing users are created through UPR and DSE having mapping “Telephone Number → businessPhone”.	6.3.14
SMGR-35768	SDM Client	Unable to install SDM client on system where System Extensions directory contains jar conflicting with bundled in SDM client.	7.0.0.0
SMGR-33211	User Management	Communication profile(SIP) password change done through System Manager self-provisioning is not transmitted to Adopters(AAC) so authentication is failing for member on Adopter(AAC)	6.3.14
SMGR-34177	Communication Manager Management	The data on the Communication Manager cut-through pages need to align properly per the data.	6.3.15
SMGR-27780	Inventory Management	Disallow creation of multiple application systems with same type and IP	6.3.2
SMGR-33679	Security Update	[RHSA-2015:1840-01] Important: openldap security update	6.3.15
SMGR-33437	Infrastructure	Disable the JBoss automatic discovery happening on the default multicast address 230.0.0.4.	6.3.2

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Fixes in System Manager Solution Deployment Manager Release 7.0.1 and Solution Deployment Manager Client Release 7.0.1

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release introduced
SDM-570	Avaya Aura® Virtualized Environment with Avaya Aura® System Manager Solution Deployment Manager and VMware vCenter	VM deployment fails on vCenter managed host within a cluster due to invalid CPU resource calculation.	7.0
SDM-679	Avaya Aura® Virtualized Environment with Avaya Aura® System Manager Solution Deployment Manager and VMware vCenter	Occasionally, VM deployment fails on vCenter managed hosts with the error, "Error in getting host details."	7.0
SDM-725	Avaya Aura® Solution Deployment Manager Client	Occasionally, the VM Deployment Status page shows "VM Deployment failed" with "Unable to run the sanity plugin" error message although the deployment was successful.	7.0
SDM-727	Avaya Aura® System Manager Solution Deployment Manager or Solution Deployment Manager Client	After changing a VM IP address the update to the static route fails.	7.0
SDM-751	Avaya Aura® System Manager Solution Deployment Manager or Solution Deployment Manager Client	After changing a VM IP address the update in System Manager inventory operation fails.	7.0
SDM-767	Avaya Aura® System Manager Solution Deployment Manager	Occasionally, upgrading Avaya Aura® Session Manager 7.0 or Branch Session Manager 7.0 to 7.0.0.1 from the Avaya Aura® System Manager Upgrade Management page shows the Patch-Install has failed with "Error in install patch…" message even though the actual patch install has succeeded.	7.0.0.1
SDM-770	Avaya Aura® Solution Deployment Manager Client	Deleting a running virtual machine (VM) without first stopping the VM seems to get the VM in an unknown state. Further stopping and deleting the VM shows "HTTP Status 500 …" error.	7.0
SDM-771	Avaya Aura® Solution Deployment Manager Client	On a rare occasion, deleting a virtual machine from the VM Management page fails with a "VM Delete failed" message.	7.0
SDM-828	Avaya Aura® Virtualized Environment with Avaya Aura® System Manager Solution Deployment Manager and VMware vCenter	Deleting multiple Virtual Machines from the VM Management page deletes the selected VMs but continues to display the deleted VMs in the VM Management table for the selected host.	7.0.0.1
SDM-889	Avaya Aura® System Manager Solution Deployment Manager or Solution Deployment Manager Client	Occasionally, changing the server's switch NIC speed hangs with "In progress" status.	7.0
SDM-906	Avaya Aura® Solution Deployment Manager Client	After deployment of a VM, changing the VM footprint size from the Solution Deployment Manager Client via the Services Port fails.	7.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release introduced
SDM-910	Avaya Aura® System Manager Solution Deployment Manager or Solution Deployment Manager Client	Occasionally, installing Avaya Aura® Appliance Virtualization Platform host patch via Solution Deployment Manager can hang at HOST_RESTART.	7.0.0.1
SDM-942	Avaya Aura® Solution Deployment Manager Client	VM refresh and trust management fails with Avaya Aura® Communication Manager and Application Enablement Services after Network Parameter Change.	7.0.0.1

Fixes in System Manager Solution Deployment Manager Release 7.0.1.2 and Solution Deployment Manager Client Release 7.0.1.2

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release introduced
SDM-1148	Avaya Aura® System Manager Solution Deployment Manager or Solution Deployment Manager Client	Solution Deployment Manager Support for vCenter6.	7.0.1

Fixes in System Manager 7.0.1.1

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-35178	Infrastructure	Change of 'admin' password on CLI is not prompted if user is logged in via console through VCenter.	7.0.0.0
SMGR-35882	Report Management	System Manager is not able to generate reports (Report type as "List" and Communication manager object as "Measurements call-summary") in CSV, PDF and Text formats.	6.3.14
SMGR-36151	Inventory Management	Service Profile record for Session Manager gets wiped out by discovery of Session Manager.	7.0.0.0
SMGR-36457	Security Updates	(CESA-2016:0459) [RHSA-2016:0459-01] Important: bind security update	7.0.0.0
SMGR-36579	Trust Management	Given CN not used for identity-cert creation.	7.0.0.0
SMGR-36612	Directory Synchronization	Directory Sync job gets terminated for failed user instead of processing remaining users.	6.3.16
SMGR-36633	Trust Management	Unable to add 3rd party trusted certificate to CS1K truststore.	6.3.15
SMGR-36720	Communication Manager Management	Favorite checkbox and Button Label is in enabled mode even if the button is “None” in Main Button/ Feature Button/ Button Module tab of Button Assignment UI.	7.0.1

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-36726	Infrastructure	Oracle Java SE Critical Patch Update for April 2016.	6.3.17
SMGR-36744	SDM Client	SDM client installer is showing wrong windows name when installed on Windows 10 OS.	7.0.1
SMGR-36749	Bulk Import and Export Management	Bulk import of users with public contact fails in certain scenarios.	6.3.10
SMGR-36825	User Management	User contacts section is not loading if the unit separator characters get added in "Contact Address" section of the user private contact.	6.3.15
SMGR-36826	Out of Band Management	System Manager interface eth0 (OOBM) which is no longer reachable(ping) from other VMs(US/SM/CM/AES) and vice versa on the AVP if OOBM is enabled.	7.0.0.0
SMGR-36834	Directory Synchronization	Unable to create new user in System Manager using AD sync with UPR if subscriber is already exist in Messaging without any user association.	6.3.16
SMGR-36860	Software Upgrade Management	Reestablish trust is in freeze state to obtain element's current status.	7.0.0.0
SMGR-36953	Security Updates	(CESA-2016:0741) [RHSA-2016:0741-01] Moderate: openssh security, bug fix, and enhancement update	7.0.0.0
SMGR-36973	Security Updates	(CESA-2016:0855) [RHSA-2016:0855-01] Moderate: kernel security, bug fix, and enhancement update	7.0.0.0
SMGR-36985	Communication Manager Management	Provided support for “IPDECToption” for CM version 6.0 and above.	7.0.0.0
SMGR-36987	Communication Manager Management	Global Endpoint Change: user is not able to put more than 4 characters under “SIP trunk” field.	7.0.1
SMGR-37013	Software Upgrade Management	Error message is not coming constantly on Edit configuration page if user is trying to upgrade elements by choosing a host which has invalid certificate.	7.0.1
SMGR-37050	Security Updates	(CESA-2016:0591) [RHSA-2016:0591-01] Moderate: nss, nss-util, and nspr security, bug fix, and enhancement update	7.0.0.0
SMGR-37061	Security Updates	(CESA-2016:0996) [RHSA-2016:0996-01] Important: openssl security update	7.0.0.0
SMGR-37099	Security Updates	[RHSA-2016:0760-01] Moderate: file security, bug fix, and enhancement update	7.0.0.0
SMGR-37103	Security Updates	[RHSA-2016:0855-01] Moderate: kernel security, bug fix, and enhancement update.	7.0.0.0
SMGR-37106	Software Upgrade Management	Software Upgrade Management fails to update Session Manager using SFTP remote library.	7.0.0.2
SMGR-	User Management	On Assign Groups page for a user, pagination is not provided to	6.3.16

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release introduced
37142		select group record other than from default row count records.	
SMGR-37152	Software Upgrade Management	Analyze operation getting stuck if user execute analyze on multiple products simultaneously.	7.0.1
SMGR-37185	Communication Manager Management	Unable to check status of an extension even though there are appropriate permissions.	7.0.0.2
SMGR-37243	Geographic Redundancy	Provided validation for admin user password expiry check during Geo Configuration and Enable workflow.	7.0.0.0
SMGR-37251	Role Management	Templates added to a group are not listed while adding/editing an Endpoint.	7.0.0.2
SMGR-37253	Communication Manager Management	Communication Manager cut-through does not work in certain scenarios.	7.0.0.2
SMGR-37315	Communication Manager Management	Init sync fails at hunt group.	6.3.17
SMGR-37332	Security Updates	[RHSA-2016:1141-01] Moderate: ntp security update.	7.0.0.0
SMGR-37395	Software Upgrade Management	Software Upgrade Management discovers duplicate entries of TN boards after interchange.	7.0.1
SMGR-37421	User Management	Turning off Auto Transliteration flag in Settings does not work as expected	7.0.0.2
SMGR-37422	User Management	Filter in User Management does not work as expected.	7.0.0.2
SMGR-37449	Security Updates	Disable CBC mode cipher.	7.0.0.0
SMGR-37461	Security Updates	(CEBA-2016:1266) CentOS 6 tzdata 2016e BugFix Update.	7.0.1
SMGR-37472	Bulk Import and Export Management	Unable to import external contacts.	7.0.1
SMGR-37501	Communication Manager Management	Enhance CM full sync logic to fix the data model state for extensions which are already there on CM but have the wrong representation in the System Manager (ipt_extension table).	6.3.15
SMGR-37519	Role Management	User with ‘System Administrator’ access rights can’t see the assigned Messaging templates	7.0.0.2
SMGR-37522	Software Upgrade Management	VM Refresh under VM Management cleans / removes all SNMP credentials under SNMP Attribute Tab in inventory /Home/Services/Inventory/Manage Elements.	7.0.1
SMGR-37525	Communication Manager Management	Unable to delete station if station is given as team button for other station under Feature option.	6.3.17
SMGR-37528	Communication Manager Management	IPTCM cleanup job don't clean the “Ipt_cm_notify” table entries having “notificationreplayed” value as 3.	6.3.16

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-37549	Data Replication Service	Accumulation of staged files (files which are used to stream the batches instead of holding them in memory) causing system to go out of memory on JVM systems having limited memory this could cause memory to be filled up when there are huge batches being replicated.	7.0.1
SMGR-37553	User Management	Improve performance while adding contacts through PPM.	7.0.1
SMGR-37565	User Management	Improve user management performance for users associated with custom role.	7.0.0.2
SMGR-37664	SDM Client	SDM client installation completes with errors on a non-default partition.	7.0.1
SMGR-37694	Software Upgrade Management	Patch files are not able to sync from software library management.	7.0.1
SMGR-37711	Backup and Restore	Remote Backup not working if the remote system is a Communication Manager.	6.3.17
SMGR-37725	Communication Manager Management	Improve endpoint management performance for users associated with custom role.	7.0.0.2
SMGR-37737	Inventory Management	Breeze element not getting deleted from inventory if delete Breeze instance after renaming Breeze SIP entity.	7.0.0.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Fixes in System Manager 7.0.1.2

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-38935	Security Updates	[RHSA-2016:2141-01] Important: bind security update	7.0.1.1
SMGR-38930	Security Updates	[RHSA-2016:2079-01] Critical: java-1.8.0-openjdk security update	7.0.1.1
SMGR-38915	Security Updates	[CESA-2016:2105] [RHSA-2016:2105-01] Important: kernel security update	7.0.1.1
SMGR-38910	Security Updates	[CESA-2016:1940] [RHSA-2016:1940-01] Important: openssl security update	7.0.1.1
SMGR-38906	Security Updates	[CESA-2016:1944] [RHSA-2016:1944-01] Important: bind security update	7.0.1.1
SMGR-36522	Security Updates	PostgreSQL 2016-02-11 Security Update Release	7.0.1.1
SMGR-38343	Security Updates	[postgresql] 2016-08-11 Security Update Release	7.0.0.0
SMGR-38330	Security Updates	[RHSA-2016:1664-01] Important: kernel security and bug fix update	7.0.0.0
SMGR-38292	Security Updates	[CESA-2016:1626][RHSA-2016-1626]Moderate: python security update	7.0.0.0
SMGR-38196	Security Updates	[CESA-2016:1547] Important: libtiff security update	7.0.1.0
SMGR-37764	Security Updates	Oracle Java SE Critical Patch Update for Oct 2016 Update	7.0.1.0
SMGR-37657	Security Updates	CESA-2016:1406) Important CentOS 6 kernel Security Update	7.0.1.0
SMGR-37653	Security Updates	(CEEA-2016:1388) CentOS 6 tzdata 2016f Enhancement Update	7.0.1.0
SMGR-37585	Security Updates	(CESA-2016:1292) [RHSA-2016:1292-01] Important: libxml2 security update	7.0.1.0
SMGR-39121	Infrastructure	IP/FQDN change is not working in AWS environment	7.0.1.0
SMGR-39006	Infrastructure	Improve performance in console framework as the performance delay observed due to threads accumulation during permission check	7.0.0.2
SMGR-36719	Authorization	Accessing System Manager with short hostname or IP takes you to the certificate login page even though there is no E-token connected	6.3.15
SMGR-38481	Authorization	Insufficient authorization checks allow privilege escalation for Auditor to become administrator.	7.0.1.0
SMGR-38480	Authorization	Password are sent in clear text for External Identity Repository (LDAP)	7.0.1.0
SMGR-38232	Authorization	Case-sensitivity in user name is causing issues while access	7.0.1.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release introduced
		Engagement Designer UI	
SMGR-28263	Alarming Management	Spirit RPM delivers trust store file with obsoleted entries.	6.3.8
SMGR-31443	Role Management	Unable to use the same group name for permission mapping if the same group was already deleted from system earlier.	6.3.8
SMGR-37938	Role Management	UI performance issues when accessing System Manager Web console via custom roles and multiple concurrent logins, issues observed in RBAC (role based authentication check) process.	7.0.0.2
SMGR-35692	Role Management	If you create a role which is a "copy all" from the Auditor role it enabled the "Administrators" link and when user adds the Communication Manager Auditor role to the role it still allows the creation or edit of stations and other CM objects that are managed via System Manager.	7.0.0.1
SMGR-38638	User Management	User associated with custom role having permission on Users only, unable to see user list in user management in certain scenarios.	6.3.16
SMGR-38307	User Management	User update fails while adding new handle (Sip or E164) after successful commit and continue operation.	7.0.0.2
SMGR-38482	User Management	Slow rendering of contacts page when user has 250 contacts.	7.0.1.1
SMGR-38071	User Management	Translation is not happening correctly for First and last name having Umlaut characters(ä,ö,ü,ß).	6.3.17
SMGR-38971	User Management	Under advanced search option, “AND/OR” function does not work with multiple E164 handle values.	7.0.0.2
SMGR-38363	User Management	Connection Reset Error on User edit page	7.0.0.2
SMGR-38224	User Management	User creation fails without proper error if user has duplicate handle (Communication address).	7.0.0.2
SMGR-38212	User Management	Handle view expired exception in User Management.	7.0.0.2
SMGR-37949	User Management	User management changes with respect to Single Sign on context and console framework thread accumulation.	7.0.0.2
SMGR-38134	User Management	Error Message on User Management page on first login	7.0.0.2
SMGR-38306	User Management	Concurrent user modification fails with EJBTransactionRolledbackException error.	7.0.0.2
SMGR-38145	Bulk Import and Export Management	PPR error is seen on bulk import page when user uploads a file and click on refresh icon in Manage Job section while upload is in progress.	7.0.0.2
SMGR-36244	Bulk Import and Export	Bulk Import of contacts with associated users is taking long time.	7.0.1.0

ID	Minimum Conditions	Visible symptoms	Release introduced
	Management		
SMGR-38975	Trust Management	Auto renewal of certificate fails for first service if enrollment password is not set already.	7.0.0.2
SMGR-38719	Trust Management	Unable to access “Configure Identity/Trusted Certificates” page for Secondary System Manager from Primary System Manager Manage Elements section.	7.0.1.0
SMGR-38833	Trust Management	Any user associated with permission on Security tab or having role “Security Administrator” access the security tab, user gets internal error.	6.3.16
SMGR-38712	Search Component	User cannot edit/view/delete a user via global search component if user contains special (Umlaut) German characters in surname/first name/localized display name.	7.0.1.0
SMGR-38658	Search Component	Performance issue noticed if user having custom roles perform endpoint search from Global Search component.	7.0.0.2
SMGR-38558	Search Component	User having custom role associated with permission on User Management unable to search users from global user search component.	6.3.8
SMGR-38370	Geographic Redundancy	GEO pair having identical hostname (before first dot) fails to get converted to standalone.	7.0.0.1
SMGR-37627	Geographic Redundancy	GEO disable from Primary server is failing if GEO is already disabled on secondary server.	6.3.14
SMGR-37993	Inventory Management	Error Message on Element Manager page showing conversation end or time out.	7.0.1.1
SMGR-39080	Software Upgrade Management	CM Update patch status is not appearing correctly (always appearing with failed symbol) on software inventory page	7.0.1.1
SMGR-38818	Software Upgrade Management	“sdmadmin” user doesn't have permissions to write to its home folder.	7.0.1.1
SMGR-38770	Software Upgrade Management	If current version of gateway is not available in upgrade management then analyze job should not stuck, it should fail with proper error message.	7.0.1.1
SMGR-38767	Software Upgrade Management	Support for migration from Avaya FTP (FTP.AVAYA.COM) for Software Deployment Management and Software Upgrade Management to PLDS	7.0.0.0
SMGR-38565	Software Upgrade Management	After performing analyze operation, it is showing as "Unknown" under Update Status for some Media Modules	7.0.1.1
SMGR-38798	Software Upgrade Management	Analyze operation stuck for Media Modules when executed in bunch.	7.0.1.1

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-37751	Software Upgrade Management	User unable to select & download Breeze ova in "Download Management ' of Software Deployment Management	7.0.1.0
SMGR-39200	Data Replication Management	Data replication fails when replicating large batches especially to slower nodes like CSR1 Session Manage servers.	7.0.0.0.
SMGR-38921	Data Replication Management	Data Replication stuck in Synchronizing state instead of Synchronized during Geo failback scenario in System Manager 7.0.x if System Manager was upgraded from 6.x release.	7.0.0.2
SMGR-37894	Report Management	Report generation is failing due to large data present in multiple communication manager systems.	7.0.0.2
SMGR-38963	Report Management	User having all access for report is unable to delete report.	7.0.1.0
SMGR-38215	Communication Manager Management	Handle view expired exception in Communication Manager Management.	7.0.0.2
SMGR-37884	Communication Manager Management	Error when viewing pickup group.	7.0.0.2
SMGR-38252	Communication Manager Management	Performance issue due to accumulation of PCCT threads	7.0.0.2
SMGR-38230	Communication Manager Management	Performance issue due to accumulation of Global search thread (notify task) during bulk operation.	7.0.0.2
SMGR-38463	Communication Manager Management	Issues observed while adding off-pbx or changing stations or any other operation through element cut through.	7.0.0.2
SMGR-38227	Communication Manager Management	Generic error message after clicking on cancel on Managed end points page on the edit screen of a station.	7.0.0.2
SMGR-38381	Communication Manager Management	Thread hung state caused all cut through functionality (irrespective of the Communication Manager to stop working.	7.0.0.2
SMGR-39204	Communication Manager Management	Logged in user unable to sort broadcast destinations by clicking on the “Source” or “System” columns.	7.0.0.2
SMGR-38221	Communication Manager Management	PPR error on group membership tab while moving groups.	7.0.0.2
SMGR-38218	Communication Manager	Concurrent request timeout exception on Communication Manager	7.0.0.2

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release introduced
	Management	Management pages and element cut through pages.	
SMGR-38204	Communication Manager Management	PPR Error after clicking on Enter Button Endpoint Management pages.	7.0.0.2
SMGR-38050	Communication Manager Management	Exception in Element Cut Through (Communication Manager Management) is resulting in PPR errors.	7.0.0.2
SMGR-38028	Communication Manager Management	Export of user fails if the SIP trunk has a digit value	7.0.0.2
SMGR-38005	Communication Manager Management	Change error message to meaning full message for endpoint CRUD operations if error is retrieved from CM due to command conflict at CM.	7.0.0.2
SMGR-38842	Communication Manager Management	User unable to schedule announcement option if user edit from quick search option.	6.3.17
SMGR-39130	Communication Manager Management	Schedule job failed for announcement if user edit and schedule a job from quick search field.	7.0.1.1
SMGR-39146	Communication Manager Management	New user creation failed if custom template is used and template is associated with message lamp extension or emergency location extension values are different than the new extension value.	7.0.1.1
SMGR-39113	Communication Manager Management	Announcement transfer is successful on AMS but the details of the transferred announcement file (size, time stamp and Icon corresponds a successful file transfer) are not reflecting on System Manager web console.	7.0.1.1
SMGR-39105	Communication Manager Management	Failed to navigate “List Trace Station” page from Communication Manager->Endpoints->Manage Endpoints User Interface.	7.0.1.1
SMGR-39091	Communication Manager Management	Add/edit operation for VDN by user having permission on Communication Manager, if user provide out of range number in vector entry, user is not provided with proper validation message.	7.0.1.0
SMGR-39017	Communication Manager Management	Display and Hide extension ranges links for add/duplicate/Swap/edit endpoint extension operations on Manage Endpoints, Add Agents user interface and also for Add Endpoint/Agent from user communication profile user interface.	7.0.0.0
SMGR-38954	Communication Manager Management	Synchronization between System Manager and Communication Manager fails with duplicate key error for "off-pbx-telephone feature-name-extension" value.	7.0.1.0
SMGR-38553	Communication Manager Management	Importing user with alias set type template fails.	7.0.0.2

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-38127	Communication Manager Management	Performance improvement related to Authorization checks for Granular field level RBAC.	7.0.0.2
SMGR-38942	Communication Manager Management	Status Station not showing Firmware Version in System Manager	7.0.0.2
SMGR-38836	Communication Manager Management	Re-Calculate Route Pattern feature doesn't work properly.	7.0.1.1
SMGR-38824	Communication Manager Management	Announcements when backed up by System Manager go into the /opt/ partition which can cause the disk space issue with /opt/ partition.	7.0.0.2
SMGR-38819	Communication Manager Management	Performing duplicate option for user from user management, changing of Communication Manager template for Communication Manager communication profile is not working.	7.0.0.2
SMGR-38763	Communication Manager Management	Increase the width of the text boxes which contain phone number in the endpoint editor user interface	7.0.0.2
SMGR-38755	Communication Manager Management	Unable to permanently delete user due to error from communication profile workflow during delete operation.	7.0.0.2
SMGR-37177	Communication Manager Management	unable to check status of an extension even though there are appropriate permissions	7.0.0.2
SMGR-38744	Communication Manager Management	Unable to edit user associated with communication profile or endpoint if alias station name contains single quote.	6.3.17
SMGR-38612	Communication Manager Management	Template creation failed from User Management Endpoint Editor page if “select endpoint” is checked.	7.0.1.0
SMGR-38595	Communication Manager Management	PPR error in in communication profile section on user management user interface due to Java Script functions.	7.0.1.1
SMGR-38590	Communication Manager Management	Permission mapping for "IP interfaces" resources for Communication Manager missing in 7.0 release	7.0.0.0

Known issues and workarounds in System Manager 7.0.x.x

Known issues and workarounds in System Manager on VMWare in Release 7.0.0.0

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

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-33581 **SMGR-33617** **SMGR-33602**		Change IP FQDN is failing in Primary System Manager. Enable Geo Replication is failing after executing Pair IP FQDN in Primary SMGR. Change IPFQDN - Corresponding SMGR Manage Elements attributes not updated	A hotfix is available. Contact Avaya Technical Support for information.
SDM-708		Unable to add vCenter	
SMGR-33187		Corporate Directory, IPsec, Numbering Groups, Patches, Secure FTP Token, SNMP Profiles, Software Deployment element links from Element Manager page is not opening correct linked page.	User can access these links from HOME/Users/Administrators.
SMGR-32844		Not able to download reports from Home / Services / Reports / History page sometimes.	While downloading the generated reports, if we get following exception on page "/pages/reports/reportsHistory.xhtml @39, 99 value="#{reportHistoryDataBean.percentSpaceUsed()}": Illegal Syntax for Set Operation", then click on left navigation and retry operation once again.
SMGR-32589		Unable to access the Home / Services / Configurations / Settings / SMGR / SMGR Element Manager page on the 6.0 SP2 to 7.0 upgrade path.	
SMGR-30883 **SMGR-32504**		In case of start/stop/restart VM, the VM IP/FQDN is not getting updated if browser F5 button is done while the operations are in progress and also vm state goes in inconsistent state.	Do not navigate away from the VM MGMT page or refresh the browser if start/stop/restart is triggered from that browser.
		There is no option to configure the network parameters again if CMM migration is failing.	
SMGR-31822		For CMM, we do not have the pre-populate script to pre fill the configuration details (i.e., the IP, subnet gateway etc.). The reason for this is that since the CMM is residing on CM itself as a service, we would be changing the IP and other details during migration (to make it a new VM), hence we cannot pre populates this data. Thus user is advised to fill in CMM configuration details	

ID	Minimum conditions	Visible symptoms	Workaround
		carefully and correctly. In case CMM migration fails(due to incorrect network configurations provided) , one needs to do the following:- 1) Delete VM from ESXi. 2) Deploy a new CMM OVA. 3) Restore the CMM backup (which is taken manually on CM 5.2.1 box with CMM RFUs installed, as already mentioned).	
		The Session Manager license becomes invalid when a new System Manager OVA is installed or when the System Manager IP address is changed.	Obtain and install a new license per normal procedures as described in the Administration guide.
SDM-444			Recommend to use local vCenter user.
SMGR-31407		Upgrade Management web console page displays issues on IE 10 and IE11 browsers.	
		Change of 'admin' password on CLI is not asked when user is logged in using console through vCenter.	
SMGR-29964		Security page: Download JKS file should display password as encrypted.	
SMGR-30502		Out-of-Band Hostname is prompting FQDN when System Manager is installed using vCenter and short name when System Manager is installed using ESXi host.	
SMGR-30272		System Manager dashboard does auto refresh after every 10 to 20 seconds on IE11.	
SMGR-31122		Issue for pre-upgrade check for first time after analyzes operation on System Manager.	

Known issues and workarounds in System Manager 7.0.0.1

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

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-30713	Infrastructure	Encrypted alert packets being retransmitted even after connection reset from Session Manager.	No Workaround
SMGR-32589	Configurations Management	Unable to access the Home / Services/Configurations / Settings / SMGR / SMGR Element Manager page once the 6.0 Service Pack #2 release is upgraded to 7.0.	No Workaround
SMGR-34897	Alarm Management	Unable to assign target profiles to Serviceability agent if System Manager is installed through SDM client.	Refer SOLN280161 for details.
SMGR-30883	VM Management	In case of start/stop/restart VM, the VM IP/FQDN is not getting updated if browser F5 button is done while the operations are in progress and also VM state goes in inconsistent state.	Do not navigate away from the VM MGMT page or refresh the browser if start/stop/restart is triggered from that browser.
SMGR-31822	Software Upgrade Management	There is no option to configure the network parameters again if CMM migration is failing.	For CMM, we do not have the pre-populate script to pre fill the configuration details (i.e., the IP, subnet gateway etc.) .The reason for this is that since the CMM is residing on CM itself as a service, we would be changing the IP and other details during migration (to make it a new VM), hence we cannot pre populates this data .Thus user is advised to fill in CMM configuration details carefully and correctly. In case CMM migration fails(due to incorrect network configurations provided) , one needs to do the following:- 1) Delete VM from ESXi. 2) Deploy a new CMM OVA. 3) Restore the CMM backup (which is taken manually on CM 5.2.1 box with CMM RFUs installed , as already mentioned)
SMGR-32313	Software Upgrade Management	TN board status didn't change from "Schedule upgrade" to "Failed" if update gets failed while downloading the file.	No Workaround
SDM-836	Software Upgrade	Software Upgrade Management only displays vSphere Standard Switch networks and doesn't show the	No Workaround

ID	Minimum conditions	Visible symptoms	Workaround
	Management	vSphere Distributed Switch networks	
SMGR-30502	Out-of-Band Management	Out-of-Band Hostname is prompting FQDN when System Manager is installed using vCenter and short name when System Manager is installed using ESXi host.	No Workaround
SMGR-34871	Out-of-Band Management	CMM messaging Element Sync is not working in OOBM environment	• CMM must be present in a network outside the public network subnet of System Manager. • CMM must be reachable from and to System Manager Management interface.
SMGR-34861	Out-of-Band Management	AAM Messaging Element Sync is not working in OOBM environment.	• AMM must be present in a network outside the public network subnet of System Manager. • AMM must be reachable to and from System Manager Management interface.
SMGR-34817	User Management	Last Name (Latin Translation) and First Name (Latin Translation) for user does not get updated if user is partial merged through Web Services or user bulk Import option.	Update the user completely through web Services or user bulk Import option.
SMGR-28978	User Management	User having custom role associated with permission on User Management unable to search users from global user search filter.	No Workaround
SMGR-28439	User Management	While adding new user(s), the default language preference is set to random language preference value.	No Workaround
SMGR-34466	User Provisioning Rule	After upgrade to System Manager 7.0 from 6.3.x, view/edit/duplicate operations for existing User Provisioning rule may fail if Session Manager Profile with Secondary Session Manager is selected in existing rule.	Refer SOLN278139.
SMGR-34782	Role Management	User associated with Messaging System Admin role clicks on subscriber, response is not redirected to valid	Refer SOLN280163

ID	Minimum conditions	Visible symptoms	Workaround
		link, and it just hangs.	
SMGR-34780	Role Management	The default 'Messaging System admin' role does not provide permission on Messaging Templates.	Refer SOLN280163
SMGR-29811	Geo Redundancy	System Manager Primary server UI becomes very slow or unable to access when the secondary System Manager gets into a weird state. Whenever request is made on UI, Primary server waits till the connection times out - 5 minutes and navigates to the requested page.	Restart JBoss service on Secondary System Manager Server.
SMGR-22580	Trust Management	Unable to see profile details in “Home / Services / Configurations / Settings / SMGR / Trust Management” if System Manager 6.3.x and 7.0.x is upgraded from earlier releases.	Refer PSN004597u for more details
SMGR-34486	Communication Manager Management	Initially CM is added in System Manager then later if a CM interchange happens due to which when admin executes the discovery in System Manager, after discovery the new active CM server as well be added so System Manager will sync with both Active and Standby CM servers.	Contact Avaya Support Team
SMGR-34885	Communication Manager Management	Remote server should not get deleted from Home / Services / Reports / Remote Server Configuration if remote server is used in existing Report Definition in Home / Services / Reports / Generation.	Edit the existing Report Definition in Home / Services / Reports / Generation with correct remote server configuration.
N/A	Geo Redundancy/CS1K	Unable to access CS1K Elements from Secondary System Manager Web console once Secondary System Manager activated.	Refer PSN004598u for the details.

Known issues and workarounds in System Manager 7.0.0.2

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

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-30713	Infrastructure	Encrypted alert packets being retransmitted even after connection reset from Session Manager.	No Workaround
SMGR-33437	Infrastructure	Disable the JBoss automatic discovery happening on the default multicast address 230.0.0.4.	No Workaround
SMGR-35670	Infrastructure	changeIPFQDN script should validate that domain name should not have number at highest-level component at validation phase instead at end of the process.	No Workaround

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-32589	Configurations Management	Unable to access the Home / Services/Configurations / Settings / SMGR / SMGR Element Manager page once the 6.0 Service Pack #2 release is upgraded to 7.0.	No Workaround
SMGR-34897	Alarm Management	Unable to assign target profiles to Serviceability agent if System Manager is installed through SDM client.	Refer SOLN280161 for details.
SMGR-30883	VM Management	In case of start/stop/restart VM, the VM IP/FQDN is not getting updated if browser F5 button is done while the operations are in progress and also VM state goes in inconsistent state.	Do not navigate away from the VM MGMT page or refresh the browser if start/stop/restart is triggered from that browser.
SMGR-31822	Software Upgrade Management	There is no option to configure the network parameters again if CMM migration is failing.	For CMM, we do not have the pre-populate script to pre fill the configuration details (i.e., the IP, subnet gateway etc.) .The reason for this is that since the CMM is residing on CM itself as a service, we would be changing the IP and other details during migration (to make it a new VM), hence we cannot pre populates this data .Thus user is advised to fill in CMM configuration details carefully and correctly. In case CMM migration fails(due to incorrect network configurations provided) , one needs to do the following:- 1) Delete VM from ESXi. 2) Deploy a new CMM OVA. 3)Restore the CMM backup (which is taken manually on CM 5.2.1 box with CMM RFUs installed , as already mentioned)
SMGR-32313	Software Upgrade Management	TN board status didn't change from "Schedule upgrade" to "Failed" if update gets failed while downloading the file.	No Workaround
SMGR-35669	Software Upgrade Management	If Alternate source path is not proper or user settings are bad then Analyze job get stuck in running state.	Contact Avaya Support Team
SMGR-35119	Software Upgrade Management	Select any "Discover Profile" field under Discover Profile table and click on delete. The Profile that you selected for delete and profile that pop on Delete page is different in some cases.	No Workaround
SDM-836	Software	Software Upgrade Management only displays	No Workaround

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum conditions	Visible symptoms	Workaround
	Upgrade Management	vSphere Standard Switch networks and doesn't show the vSphere Distributed Switch networks	
SMGR-30502	Out-of-Band Management	Out-of-Band Hostname is prompting FQDN when System Manager is installed using vCenter and short name when System Manager is installed using ESXi host.	No Workaround
SMGR-34871	Out-of-Band Management	CMM messaging Element Sync is not working in OOBM environment	• CMM must be present in a network outside the public network subnet of System Manager. • CMM must be reachable from and to System Manager Management interface.
SMGR-34861	Out-of-Band Management	AAM Messaging Element Sync is not working in OOBM environment.	• AMM must be present in a network outside the public network subnet of System Manager. • AMM must be reachable to and from System Manager Management interface.
SMGR-34817	User Management	Last Name (Latin Translation) and First Name (Latin Translation) for user does not get updated if user is partial merged through Web Services or user bulk Import option.	Update the user completely through web Services or user bulk Import option.
SMGR-28978	User Management	User having custom role associated with permission on User Management unable to search users from global user search filter.	No Workaround
SMGR-28439	User Management	While adding new user(s), the default language preference is set to random language preference value.	No Workaround
SMGR-35116	User Management	Allow to set 'Block New Registration when Maximum Registrations Active?' option via the "Bulk Edit Users" (from "Manage Users" -> "More Actions") section for existing users associated with Session Manager profiles.	No Workaround
SMGR-34422	User Management	SIP handle is not created for user through bulk edit user feature, if Session Manager profile is applied through bulk edit feature	Add SIP handle to each user once with Session Manager profile is applied through bulk edit feature.
SMGR-34466	User Provisioning Rule	After upgrade to System Manager 7.0 from 6.3.x, view/edit/duplicate operations for existing User Provisioning rule may fail if Session Manager Profile with Secondary Session Manager is	Refer SOLN278139.

ID	Minimum conditions	Visible symptoms	Workaround
		selected in existing rule.	
SMGR-34782	Role Management	User associated with Messaging System Admin role clicks on subscriber, response is not redirected to valid link, and it just hangs.	Refer SOLN280163
SMGR-34780	Role Management	The default 'Messaging System admin' role does not provide permission on Messaging Templates.	Refer SOLN280163
SMGR-35692	Role Management	If you create a role which is a "copy all" from the Auditor role it enabled the "Administrators" link and when user adds the Communication Manager Auditor role to the role it still allows the creation or edit of stations and other CM objects that are managed via System Manager.	Instead of "copy all" create new role.
SMGR-29811	Geo Redundancy	System Manager Primary server UI becomes very slow or unable to access when the secondary System Manager gets into a weird state. Whenever request is made on UI, Primary server waits till the connection times out - 5 minutes and navigates to the requested page.	Restart JBoss service on Secondary System Manager Server.
SMGR-22580	Trust Management	Unable to see profile details in "Home / Services / Configurations / Settings / SMGR / Trust Management" if System Manager 6.3.x and 7.0.x is upgraded from earlier releases.	Refer PSN004597u for more details
SMGR-34486	Communication Manager Management	Initially CM is added in System Manager then later if a CM interchange happens due to which when admin executes the discovery in System Manager, after discovery the new active CM server as well be added so System Manager will sync with both Active and Standby CM servers.	Contact Avaya Support Team
SMGR-34885	Communication Manager Management	Remote server should not get deleted from Home / Services / Reports / Remote Server Configuration if remote server is used in existing Report Definition in Home / Services / Reports / Generation.	Edit the existing Report Definition in Home / Services / Reports / Generation with correct remote server configuration.
SMGR-34991	Communication Manager Management	Not able to Edit Fields of Communication Manager via Element cut through when user hit Enter instead of clicking Send Button	Use Send button to make changes on Communication Manager via Element cut through.
N/A	Geo Redundancy/CS1K	Unable to access CS1K Elements from Secondary System Manager Web console once Secondary System Manager activated.	Refer PSN004598u for the details.
SMGR-33437	Infrastructure	Disable the JBoss automatic discovery happening on the default multicast address 230.0.0.4.	No Workaround

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Known issues and workarounds in System Manager 7.0.1

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

ID	Minimum conditions	Visible symptoms	Workaround
	Installation	When attempting to install 7.0.1 via the CLI command SMGRPatchdeploy on top of 7.0 GA (#29 – old 7.0 GA OVA), the patch install fails with following error: Executing checkForPatchRequisite This System has a bad CA certificate. It is recommended to either use the latest System Manager 7.0 template available on PLDS in case a fresh installation is in progress or use the System Manager 7.0 CA Re-generation Utility, available on PLDS, before patch execution.	It is recommended to either use the latest System Manager 7.0 template available on PLDS in case a fresh installation is in progress or use the System Manager 7.0 CA Re-generation Utility, available on PLDS, before patch execution.
		vSphere client displays and error 'not able to access VM console' for the AVP host where certificate has been regenerated.	Reboot the host
SMGR-35304	Infrastructure	System Manager /opt partition full.	SMGR 7.0.x.x is sometimes prone to issues of /opt partition getting filled up. This issue is going to be addressed in next beta release.Manual procedueres below to clean up space on /opt partition. Steps to clean up /opt partition 1. Use the following command to check the partition sizes: df -h 2. Use the following command to check size of all files and sub-directories in the current directory: du -sh * | sort -h 3. Remove SPIRIT derby.log if it is too big. Execute command: rm /opt/Avaya/SPIRIT/7.0.9/derby.log 4. Remove (or transfer to somewhere else) the contents of /opt/Avaya/Mgmt/7.0.9/bulkadministration/export directory if it is too big. Execute command: rm /opt/Avaya/Mgmt/7.0.9/bulkadministration/export/*

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-35976	User Management	Template creation failed from UPM Endpoint Editor page if “select endpoint” is checked.	No Workaround
SMGR-34977	Infrastructure	Not able to restart JBoss from admin account on System Manager R7.0.1	Use Alias serviceJBossRESTART
SMGR-30713	Infrastructure	Encrypted alert packets being retransmitted even after connection reset from Session Manager.	No Workaround
SMGR-31822	Software Upgrade Management	There is no option to configure the network parameters again if CMM migration is failing.	For CMM, there is no pre-populate script to pre fill the configuration details (i.e., the IP, subnet gateway etc.) .The reason for this is that since the CMM is residing on CM itself as a service, we would be changing the IP and other details during migration (to make it a new VM), hence we cannot pre populates this data .Thus user is advised to fill in CMM configuration details carefully and correctly. In case CMM migration fails(due to incorrect network configurations provided) , one needs to do the following:- 1) Delete VM from ESXi. 2) Deploy a new CMM OVA. 3)Restore the CMM backup (which is taken manually on CM 5.2.1 box with CMM RFUs installed , as already mentioned)
SMGR-32313	Software Upgrade Management	TN board status didn't change from "Schedule upgrade" to "Failed" if update gets failed while downloading the file.	No Workaround
SMGR-35119	Software Upgrade Management	Select any "Discover Profile" field under Discover Profile table and click on delete. The Profile that you selected for delete and profile that pop on Delete page is different in some cases.	No Workaround
SDM-836	Software Upgrade Management	Software Upgrade Management only displays vSphere Standard Switch networks and doesn’t show the vSphere Distributed Switch networks	No Workaround
SMGR-30502	Out-of-Band Management	Out-of-Band Hostname is prompting FQDN when System Manager is installed using vCenter and short name when System Manager is installed using ESXi host.	No Workaround
SMGR-34861	Out-of-Band Management	AAM Messaging Element Sync is not working in OOBM environment.	• AMM must be present in a network outside the public network subnet of System Manager. • AMM must be reachable to and from System Manager Management

ID	Minimum conditions	Visible symptoms	Workaround
			interface.
SMGR-28978	User Management	User having custom role associated with permission on User Management unable to search users from global user search filter.	No Workaround
SMGR-28439	User Management	While adding new user(s), the default language preference is set to random language preference value.	No Workaround
SMGR-35116	User Management	Allow to set ‘Block New Registration when Maximum Registrations Active?’ option via the “Bulk Edit Users” (from “Manage Users” -> “More Actions”) section for existing users associated with Session Manager profiles.	No Workaround
SMGR-34422	User Management	SIP handle is not created for user through bulk edit user feature, if Session Manager profile is applied through bulk edit feature	Add SIP handle to each user once with Session Manager profile is applied through bulk edit feature
SMGR-34885	Communication Manager Management	Remote server should not get deleted from Home / Services / Reports / Remote Server Configuration if remote server is used in existing Report Definition in Home / Services / Reports / Generation.	Edit the existing Report Definition in Home / Services / Reports / Generation with correct remote server configuration.
N/A	Geographic Redundancy/ CS1K	Unable to access CS1K Elements from Secondary System Manager Web console once Secondary System Manager activated.	Refer PSN004598u for the details.
SMGR-36456	User Management	Security code disappears while new user is added from user management page, if UPR is selected and Endpoint Editor button is clicked.	No Workaround
SMGR-35997	Software Upgrade	Simultaneous upgrade of the TN Boards using Software Upgrade Management is not working. This is applicable to Communication Manager R7.0.x.	No workaround

Known issues and workarounds in System Manager 7.0.1.1

ID	Minimum conditions	Visible symptoms	Workaround
N/A	Installation	When attempting to install 7.0.1.1 via the CLI command SMGRPatchdeploy on top of 7.0 GA (#29 – old 7.0 GA OVA), the patch install fails with following error: Executing checkForPatchRequisite This System has a bad CA certificate. It is recommended to either use the latest System Manager 7.0 template	It is recommended to either use the latest System Manager 7.0 template available on PLDS in case a fresh installation is in progress or use the System Manager 7.0 CA Re-generation Utility, available on PLDS, before patch execution.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum conditions	Visible symptoms	Workaround
		available on PLDS in case a fresh installation is in progress or use the System Manager 7.0 CA Re-generation Utility, available on PLDS, before patch execution.	
N/A		vSphere client displays and error ‘not able to access VM console’ for the AVP host where certificate has been regenerated.	Reboot the host.
SMGR-35976	User Management	Template creation failed from UPM Endpoint Editor page if “select endpoint” is checked.	No Workaround.
SMGR-34977	Infrastructure	Not able to restart JBoss from admin account on System Manager R7.0.1	Use Alias serviceJBossRESTART.
SMGR-30713	Infrastructure	Encrypted alert packets being retransmitted even after connection reset from Session Manager.	No Workaround.
SMGR-31822	Software Upgrade Management	There is no option to configure the network parameters again if CMM migration is failing.	For CMM, there is no pre-populate script to pre fill the configuration details (i.e., the IP, subnet gateway etc.) .The reason for this is that since the CMM is residing on CM itself as a service, we would be changing the IP and other details during migration (to make it a new VM), hence we cannot pre populates this data .Thus user is advised to fill in CMM configuration details carefully and correctly. In case CMM migration fails(due to incorrect network configurations provided) , one needs to do the following:- 1) Delete VM from ESXi. 2) Deploy a new CMM OVA. 3) Restore the CMM backup (which is taken manually on CM 5.2.1 box with CMM RFUs installed, as already mentioned).
SMGR-32313	Software Upgrade Management	TN board status didn't change from "Schedule upgrade" to "Failed" if update gets failed while downloading the file.	No Workaround
SMGR-35119	Software Upgrade Management	Select any "Discover Profile" field under Discover Profile table and click on delete. The Profile that you selected for delete and profile that pop on Delete page is different in some cases.	No Workaround
SDM-836	Software Upgrade Management	Software Upgrade Management only displays vSphere Standard Switch networks and doesn’t show the vSphere Distributed Switch networks.	No Workaround
SMGR-	Out-of-Band	Out-of-Band Hostname is prompting FQDN when	No Workaround

ID	Minimum conditions	Visible symptoms	Workaround
30502	Management	System Manager is installed using vCenter and short name when System Manager is installed using ESXi host.	
SMGR-34861	Out-of-Band Management	AAM Messaging Element Sync is not working in OOBM environment.	• AMM must be present in a network outside the public network subnet of System Manager. • AMM must be reachable to and from System Manager Management interface.
SMGR-28978	User Management	User having custom role associated with permission on User Management unable to search users from global user search filter.	No Workaround
SMGR-28439	User Management	While adding new user(s), the default language preference is set to random language preference value.	No Workaround
SMGR-35116	User Management	Allow to set ‘Block New Registration when Maximum Registrations Active?’ option via the “Bulk Edit Users” (from “Manage Users” -> “More Actions”) section for existing users associated with Session Manager profiles.	No Workaround
SMGR-34422	User Management	SIP handle is not created for user through bulk edit user feature, if Session Manager profile is applied through bulk edit feature	Add SIP handle to each user once with Session Manager profile is applied through bulk edit feature
SMGR-36456	User Management	Security code disappears while new user is added from user management page, if UPR is selected and Endpoint Editor button is clicked.	No Workaround
SMGR-37796	Search Component	Cannot edit/view/delete a user via global search component if user contains special German chars in surname/first name/localized display name.	Use user management filter to view/edit/delete such users.
SMGR-34885	Communication Manager Management	Remote server should not get deleted from Home / Services / Reports / Remote Server Configuration if remote server is used in existing Report Definition in Home / Services / Reports / Generation.	Edit the existing Report Definition in Home / Services / Reports / Generation with correct remote server configuration.
SMGR-37755	Communication Manager Management	Synchronization of "off-pbx-telephone feature-name-extension" faile with duplicate key error.	Contact Avaya Support Team.
SMGR-37311	Communication Manager Management	Can't enable or disable H.323 and SIP Endpoint Dual Registration option while editing user.	No Workaround
N/A	Geographic Redundancy/ CS1K	Unable to access CS1K Elements from Secondary System Manager Web console once Secondary System	Refer PSN004598u for the details.

ID	Minimum conditions	Visible symptoms	Workaround
		Manager activated.	
SMGR-37627	Geographic Redundancy	GEO disable from Primary server is failing if GEO is already disabled on secondary server.	Contact Avaya Support Team.
SMGR-37608	Report Management	Report generation job is failing intermittently if the report data is very large	No Workaround
SMGR-36804	Trust Management	Any user having permission on Security tab or having role "Security Administrator" access the security tab, then it throws internal error	Access System Manager Web console using FQDN instead IP address.

Known issues and workarounds in System Manager 7.0.1.2

ID	Minimum conditions	Visible symptoms	Workaround
	Installation	When attempting to install 7.0.1.1 via the CLI command SMGRPatchdeploy on top of 7.0 GA (#29 – old 7.0 GA OVA), the patch install fails with following error: Executing checkForPatchRequisite This System has a bad CA certificate. It is recommended to either use the latest System Manager 7.0 template available on PLDS in case a fresh installation is in progress or use the System Manager 7.0 CA Re-generation Utility, available on PLDS, before patch execution.	It is recommended to either use the latest System Manager 7.0 template available on PLDS in case a fresh installation is in progress or use the System Manager 7.0 CA Re-generation Utility, available on PLDS, before patch execution.
		vSphere client displays and error 'not able to access VM console' for the AVP host where certificate has been regenerated.	Reboot the host
SMGR-30713	Infrastructure	Encrypted alert packets being retransmitted even after connection reset from Session Manager.	No Workaround
SMGR-39202	Roe Management	Issue noticed in roles page, if role page is accessed from security – roles link present on right pane.	Access role page from Security-Roles (child node) or from Group and Roles Page,
SMGR-38790	Trust Management	Unable to access System Manager web console using IE11 browser if huge number of trusted certificates (>150) present in the System Manager trust store.	Access System Manager Web console from Firefox browser
SMGR-31822	Software Upgrade Management	There is no option to configure the network parameters again if CMM migration is failing.	For CMM, there is no pre-populate script to pre fill the configuration details (i.e., the IP, subnet gateway etc.) .The reason for this is that since the CMM is residing on CM itself as a service, we would be changing the IP and other details during migration (to make it a new VM), hence we cannot pre populates this data .Thus user is

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum conditions	Visible symptoms	Workaround
			advised to fill in CMM configuration details carefully and correctly. In case CMM migration fails(due to incorrect network configurations provided) , one needs to do the following:- 1) Delete VM from ESXi. 2) Deploy a new CMM OVA. 3)Restore the CMM backup (which is taken manually on CM 5.2.1 box with CMM RFUs installed , as already mentioned)
SMGR-32313	Software Upgrade Management	TN board status didn't change from "Schedule upgrade" to "Failed" if update gets failed while downloading the file.	No Workaround
SMGR-35119	Software Upgrade Management	Select any "Discover Profile" field under Discover Profile table and click on delete. The Profile that you selected for delete and profile that pop on Delete page is different in some cases.	No Workaround
SDM-836	Software Upgrade Management	Software Upgrade Management only displays vSphere Standard Switch networks and doesn't show the vSphere Distributed Switch networks	No Workaround
SMGR-30502	Out-of-Band Management	Out-of-Band Hostname is prompting FQDN when System Manager is installed using vCenter and short name when System Manager is installed using ESXi host.	No Workaround
SMGR-34861	Out-of-Band Management	AAM Messaging Element Sync is not working in OOBM environment.	• AMM must be present in a network outside the public network subnet of System Manager. • AMM must be reachable to and from System Manager Management interface.
SMGR-28439	User Management	While adding new user(s), the default language preference is set to random language preference value.	No Workaround
SMGR-35116	User Management	Allow to set 'Block New Registration when Maximum Registrations Active?' option via the "Bulk Edit Users" (from "Manage Users" -> "More Actions") section for existing users associated with Session Manager profiles.	No Workaround
SMGR-34422	User Management	SIP handle is not created for user through bulk edit user feature, if Session Manager profile is applied through	Add SIP handle to each user once with Session Manager profile is

ID	Minimum conditions	Visible symptoms	Workaround
		bulk edit feature	applied through bulk edit feature
SMGR-36456	User Management	Security code disappears while new user is added from user management page, if UPR is selected and Endpoint Editor button is clicked.	No Workaround
SMGR-34885	Communication Manager Management	Remote server should not get deleted from Home / Services / Reports / Remote Server Configuration if remote server is used in existing Report Definition in Home / Services / Reports / Generation.	Edit the existing Report Definition in Home / Services / Reports / Generation with correct remote server configuration.
SMGR-37311	Communication Manager Management	Can't enable or disable H.323 and SIP Endpoint Dual Registration option while editing user.	No Workaround
N/A	Geographic Redundancy/ CS1K	Unable to access CS1K Elements from Secondary System Manager Web console once Secondary System Manager activated.	Refer PSN004598u for the details.

Known issues and workarounds in System Manager Solution Deployment Manager Release 7.0.0.1 and Solution Deployment Manager Client Release 7.0.0.1

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

ID	Minimum conditions	Visible symptoms	Workaround
SDM-715	Avaya Aura® Solution Deployment Manager Client	Avaya Aura® Solution Deployment Manager Client displays the deployed application version as "0.0.0.0"	Use the Avaya Aura® System Manager Solution Deployment Manager to display the deployed application version.
SDM-725	Avaya Aura® Solution Deployment Manager Client	Occasionally, the VM Deployment Status page shows "VM Deployment failed" with "Unable to run the sanity plugin" error message although the deployment was successful.	Refresh the VM Deployment Status page to show the status of the deployed VM.
SDM-767	Avaya Aura® System Manager Solution Deployment Manager	Occasionally, upgrading Avaya Aura® Session Manager 7.0 or Branch Session Manager 7.0 to 7.0.0.1 from the Avaya Aura® System Manager Upgrade Management page shows the Patch-Install has failed with "Error in install patch…" message even though the actual patch install has succeeded.	
SDM-770	Avaya Aura® Solution Deployment Manager Client	Deleting a running virtual machine (VM) without first stopping the VM seems to get the VM in an unknown state. Further stopping and deleting the VM shows "HTTP Status 500 …" error.	Refresh the VM management tree and verify that the VM has been deleted.
SDM-771	Avaya Aura® Solution Deployment Manager	On a rare occasion, deleting a virtual machine from the VM Management page	Make sure the virtual machine is stopped and delete the virtual

ID	Minimum conditions	Visible symptoms	Workaround
	Client	fails with a "VM Delete failed" message.	machine again. Refresh the VM management tree and verify that the VM has been deleted.
SDM-828	Avaya Aura® Virtualized Environment with Avaya Aura® System Manager Solution Deployment Manager and VMware vCenter	Deleting multiple Virtual Machines from the VM Management page deletes the selected VMs but continues to display the deleted VMs in the VM Management table for the selected host.	Perform a host refresh from the Avaya Aura® System Manager Solution Deployment Manager.
SDM-836	Avaya Aura® Virtualized Environment deployment with vSphere Distributed Switch network	Avaya Aura® System Manager Solution Deployment Manager cannot be used to deploy virtual machines when VMware vSphere Distributed Switch networks are used.	Use VMware vCenter to deploy the virtual machine.
SDM-846	Avaya Aura® System Manager Solution Deployment Manager	If a patch was installed on an application virtual machine using the Command Line Interface (CLI) instead of using Avaya Aura® System Manager Solution Deployment Manager, then the same patch cannot be uninstalled using Solution Deployment Manager. A CLI-installed patch will not show up on the **Installed Patches** page of the Solution Deployment Manager.	A CLI-installed patch can be uninstalled from the CLI.

Known issues and workarounds in System Manager Solution Deployment Manager Release 7.0.1 and Solution Deployment Manager Client Release 7.0.1

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

ID	Minimum conditions	Visible symptoms	Workaround
SDM-715	Avaya Aura® Solution Deployment Manager Client	Avaya Aura® Solution Deployment Manager Client displays the deployed application version as "0.0.0.0" after VM refresh.	Use the Avaya Aura® System Manager Solution Deployment Manager to display the deployed application version or check on the application itself.
SDM-836	Avaya Aura® Virtualized Environment deployment with vSphere Distributed Switch network	Avaya Aura® System Manager Solution Deployment Manager cannot be used to deploy virtual machines when VMware vSphere Distributed Switch networks are used.	Use VMware vCenter to deploy the virtual machine.
SDM-846	Avaya Aura® System Manager Solution Deployment Manager	If a patch was installed on an application virtual machine using the Command Line Interface (CLI) instead of using Avaya Aura® System Manager Solution Deployment Manager, then the same patch cannot uninstall using Solution	A CLI-installed patch can be uninstalled from the CLI.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum conditions	Visible symptoms	Workaround
		Deployment Manager. A CLI-installed patch will not show up on the Installed Patches page of the Solution Deployment Manager.	
SDM-931	Avaya Aura® System Manager Solution Deployment Manager or Solution Deployment Manager Client	Making changes to VM settings, like changing the time zone setting, while VM is being upgraded are not reflected on the system. The restore part of the process will revert the system to match its pre-upgrade configuration.	If you wish to change VM settings, complete the upgrade and then change the values on the application after the upgrade is complete.
SDM-940	Avaya Aura® Virtualized Environment with Avaya Aura® System Manager Solution Deployment Manager and VMware vCenter	With Single sign-on (SSO) enabled, VM deployment page on Solution Deployment Manager takes about 10 seconds to load.	Wait while the page loads.
SDM-973	Avaya Aura® System Manager Solution Deployment Manager or Solution Deployment Manager Client, and Avaya Aura® Communication Manager (CM)	Occasionally, an installed CM patch cannot be uninstalled via SDM.	This problem is usually caused by installing a CM patch without SDM. To prevent this problem, use SDM to install and activate the patch. A CM patch that cannot be uninstalled via SDM can be uninstalled via the CM web interface.
SDM-974	Avaya Aura® System Manager Solution Deployment Manager and Avaya Aura® Appliance Virtualization Platform (AVP)	Occasionally, certificate error is seen with AVP host after upgrading System Manager and accepting the certificate for the AVP host.	Regenerate and accept the certificate for the AVP host.
SDM-980	Avaya Aura® System Manager Solution Deployment Manager and Avaya Aura® Appliance Virtualization Platform (AVP)	Cannot successfully change the AVP IP address to an address in a different subnet via SDM.	AVP does not support changing AVP hosts to different network remotely. When changing the AVP host IP address to a different network, connection should be made via the SDM client to the Services Port and the IP address change made from there. The IP address and default gateway of AVP cannot be changed in a single step and once the IP address changes the remote connection is lost. Changes to a different network should be made locally for AVP. If it is required to change the network configuration remotely, activate the SSH session on the AVP host and

ID	Minimum conditions	Visible symptoms	Workaround
			log in. Run the command /opt/avaya/bin/serverInitialNetworkConfig Enter all the network values. As the script runs you will lose connection to the system as the IP address changes. The new host IP will need to be added into SDM. Once done log in to the new assigned IP address after the other network alterations have been made (such as connecting AVP host to its new network via physical connection or switch reconfiguration). Confirm all required network changes have been made to AVP via SDM including DNS and NTP settings. If this process does not work correctly you will need to connect to the Services Port of AVP and re-address the host from there.
SDM-981	Solution Deployment Manager Client and Avaya Aura® Appliance Virtualization Platform (AVP)	On rare occasion, adding AVP host to SDM fails while retrieving host details with the error "Unable to find AVP version number"	Stop SDM Client Service and Start SDM Client Service and add the AVP host again.
SDM-983	Avaya Aura® System Manager Solution Deployment Manager	A Virtual Machine (VM) host cannot be added to SDM using its IP address.	Add the VM host to SDM using the host's FQDN.
SDM-988	Avaya Aura® Virtualized Environment with Solution Deployment Manager and VMware vCenter	Deployment of Avaya Aura® Device Services (AADS) or Avaya Media Server (AMS) on a Virtualized Environment (VE) with vCenter 6.0 and ESXi 5.5 may fail.	Deploy AADS or AMS from SDM directly connected to the VM host or from vCenter without SDM.
SDM-1011	Solution Deployment Manager and Avaya Aura® Utility Services	Solution Deployment Manager incorrectly allows a deployed Utility Services footprint to be lowered.	A deployed Utility Services footprint cannot be lowered. Utility Services must be reinstalled to lower its footprint.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Avaya Aura® Presence Services

Installation for Avaya Aura® Presence Services 7.0.x.x

Required patches for Presence Services 7.0.0.0

Patches in 7.0 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 7.0 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 7 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 7.0.0.0

Filename	Modification time stamp	File size	Version number	Prerequisite Downloads
PS-7.0.0.0.295.zip **(PLDS ID: PS070000000)**				**EDP 3.1 SP1 Platform OVA** **Download ID:** CE000000111 **Size:** 2,510 MB **Release date:** Sep 15, 2015 **md5sum**: ee130b9e6fa117b826d6294066bcf313 **File version:** EDP-3.1.0.1.310107_OVF10.ova **ISO:** 112 > EDP 3.1 SP1 Upgrade **ISO File version:** aus-installer-3.1.0.1.310107.iso

Required patches for Presence Services 7.0.0.1

Patches in 7.0 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 7.0 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 7 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 7.0.0.1

Filename	Modification time stamp	File size	Version number
PS-7.0.0.1.361.zip **(PLDS ID is PS070000010)**			

Required patches for Presence Services 7.0.1

Patches in 7.0 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 7.0 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 7 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 7.0.1

Filename	Modification time stamp	File size	Version number	Prerequisite Downloads
PS-7.0.1.0.358.zip **(PLDS ID is PS070001000)**				**Avaya Breeze 3.1 FP1 Platform OVA** **Download ID:** CE000000126 **Size:** 2,712 MB **Release date:** Dec. 14, 2015 **md5sum**:51723d1a004a85e7d0b37a2cc39e2c17 **File version:** EDP-3.1.1.0.311006_OVF10.ova **ISO File version:** aus-installer-3.1.1.0.311006.iso

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Required patches for Presence Services 7.0.1.1

Patches in 7.0 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 7.0 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 7 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 7.0.1.1

Filename	Modification time stamp	File size	Version number	Prerequisite Downloads
PS-7.0.1.0.447.zip **(PLDS ID is PS070001000)**				**Avaya Breeze 3.1 FP1 Platform OVA** **Download ID:** CE000000126 **Size:** 2,712 MB **Release date:** Dec. 14, 2015 **md5sum**:51723d1a004a85e7d0b37a2cc39e2c17 **File version:** EDP-3.1.1.0.311006_OVF10.ova **ISO File version:** aus-installer-3.1.1.0.311006.iso

Backing up the software

Presence Services software is mastered on the SMGR. If you wish to back-up presence services configuration data refer to SMGR documentation.

Installing the 7.0.0.0 release

Download and install the Avaya Aura Presence Services 7.0 Software (PS-7.0.0.0.1395.svar) on a clean system per the Avaya Aura® Presence Services Snap-in Reference.

New Installations

New installation quick reference	Download	Prerequisite Downloads
Presence Services Snap-in on EDP	PS-7.0.0.0.295.zip (PLDS ID: PS070000000)	**EDP 3.1 SP1 Platform OVA** **Download ID:** CE000000111

New installation quick reference	Download	Prerequisite Downloads
		Size: 2,510 MB **Release date:** Sep 15, 2015 **md5sum**: ee130b9e6fa117b826d6294066bcf313 **File version:** EDP-3.1.0.1.310107_OVF10.ova **ISO:** 112 > EDP 3.1 SP1 Upgrade **ISO File version:** aus-installer-3.1.0.1.310107.iso

New installations of Presence Services 7.0.0.0, on platforms that are not currently running Presence Services, are only supported using the following deployment method:

- Presence Services Snap-in on EDP Download and install the Avaya Aura Presence Services 7.0 Software (PS-7.0.0.0.1395.svar) on a clean system per the *Avaya Aura® Presence Services Snap-in Reference Guide*.

Note: At the time general availability of Presence Services 7.0 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 7.0 deployments.

Upgrades/Migrations from 6.2.x to 7.0

Changes Affecting Migrations to 7.0

Avaya Aura® Presence Services 7.0 introduces significant changes that affect migrations to PS 7.0:

- Avaya Presence Services inventory elements are no longer automatically created; they must be configured on System Manager. There should only be one Presence Services on EDP element defined per cluster.
- Presence Profile (System Manager Home > Users > User Management > Manage Users > Communication Profile > Presence Profile) is mandatory in order to enable presence for a user.
- In order to be presence-enabled, a user must be administered with a Presence Profile (Users > User Management > Manage Users > Communication Profile > Presence Profile) that is associated with a Presence Services server. In pre-PS 7.0.0.0 releases, a user's Presence Profile is associated with a Managed Element (Services > Inventory > Managed Elements) of type / sub-type Presence Services / Presence Services. In PS 7.0.0.0 or higher, a user's Presence Profile is associated with a Managed Element of type / sub-type Presence Services / Presence Services on Engagement Development Platform. If migrating users from pre-PS 7.0.0.0 to PS 7.0.0.0, the Presence Profile for those users must be updated. A script (ps-commprofile) is available to perform this action.
- Obtain the ps-commprofile script from PLDS (PLDS ID = PS070000001)
- If necessary, rename the file to ps-commprofile.sh
- Copy ps-commprofile.sh to a temporary directory on System Manager, for example /tmp/
- Log in to System Manager as a root user
- Change to the temporary directory (e.g. cd /tmp)
- Run the command chmod +x ps-commprofile.sh to ensure the file is executable
- To modify the Presence Profile of one user, execute the following command:

```
./ps-commprofile.sh --modify-user <user> <new-ps>
```

where

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

<user> is the login name of the user (Users > User Management > Manage Users > Identity > Login Name)

<new-ps> is the name of the Presence Services / Presence Services on Engagement Development Platform Managed Element that will be associated with the user

- To modify the Presence Profile of multiple users, execute the following command:

./ps-commprofile.sh --modify-sys <existing-ps> <new-ps>

where

<existing-ps> is the name of the Presence Services / Presence Services Managed Element currently associated with the users at Users > User Management > Manage Users > Communication Profile > Presence Profile > System

<new-ps> is the name of the Presence Services / Presence Services on Engagement Development Platform Managed Element that will be associated with the user

- The script also supports some query options. To view all options:
- ./ps-commprofile.sh --help
- A "Presence Services Cluster FQDN" must be defined. This FQDN will represent an EDP "Core Platform" Cluster running the Presence Services Snap-in on one or more EDP server instances.
    - The "Presence Services Cluster FQDN" must be configured in the customer's DNS as a "CNAME" record resolving to all EDP server instance's Security Module addresses (round-robin equal weight).
    - All EDP server instances must be provisioned in System Manager's Local Host Name Resolution table. The "Presence Services Cluster FQDN" must be mapped to each EDP server instance's Security Module address with equal weight.
    - A single SIP Entity must be created of Type "Presence Services" using the "Presence Services Cluster FQDN" as the target. This entity must have SIP Entity Links to all Session Managers in the deployment from port 5061 (TLS) to Session Manager port 5062 (TLS).
    - SIP Entity / SIP Entity Links must also be created for each EDP server instance's Security Module address per standard EDP deployment guidelines.
- Applications using 6.2 or earlier versions of LPS will be unable to integrate with Presence Services 7.0. Applications must use the Presence Services 7.0 compatible LPS client. This includes:
    - Avaya one-X Client Enablement Services
    - Avaya one-X Attendant
- Avaya Multimedia Messaging (AMM) XMPP federation is not supported in Presence services 7.0.0. Current GA versions of AMM (<2.1) are not supported with Presence Services 7.0.0. AMM 3.0 will support REST-based integration and will be fully compatible with Presence services 7.0.1 and above.
- All presence-related configuration on Avaya Aura® System Manager will be migrated automatically when System Manager is upgraded to release 7.0 however, Presence Services 6.2 XCP configuration data (collectors and federation), Archived/Offline IMs and user retained manual presence states will not be migrated. It is essential administrators backup the Presence Services 6.2 data before proceeding as it is not recoverable. In addition, manual re-provisioning of collectors and federation will be required when initially deploying Presence Services 7.0.
- The ps-commprofile.sh script must be run as part of the migration of existing PS 6.2.X users to PS 7.0. The PS-CommProfile script can be downloaded from the Avaya Support site (PLDS ID = PS070000001).

In order to run Presence Services 7.0.0.0, migrations should be performed using the following method:

- Presence Services Snap-in on EDP:

Download and install the Avaya Aura Presence Services 7.0.0.0 Software (PS-7.0.0.0-1395.svar) on an EDP 3.1 Core cluster.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Note: At the time general availability of Presence Services 7.0.0.0 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 7.0.0.0 deployments.

Migrations to release 7.0.0.0 are supported from the following releases only:

Minimum required versions by Release

Release	Minimum Required Version
Avaya Aura® Presence Services 6.2 Feature Pack 4	PS-6.2.4.4-641 + any additional patch(es)
Avaya Aura® Presence Services 6.2 Service Pack 5	PS-6.2.5.5-85 + any additional patch(es)
Avaya Aura® Presence Services 6.2 Service Pack 6	PS-6.2.6.10-38 + any additional patch(es)

Upgrade References to Presence Services 7.0.0.0

Upgrade Quick Reference	Download	Prerequisite Downloads
Presence Services Snap-in on EDP	PS-7.0.0.0.295.zip (PLDS ID: PS070000000)	**EDP 3.1 SP1 Platform OVA** **Download ID:** CE000000111 **Size:** 2,510 MB **Release date:** Sep 15, 2015 **md5sum**: ee130b9e6fa117b826d6294066bcf313 **File version:** EDP-3.1.0.1.310107_OVF10.ova **ISO:** 112 > EDP 3.1 SP1 Upgrade **ISO File version:** aus-installer-3.1.0.1.310107.iso

Installing the 7.0.0.1 release

All Presence Services 7.0 software is cumulative. For new installations you may install the 7.0.0.1 service pack directly without installing the 7.0.0.0 load. For new installations:

Download and install the Avaya Aura Presence Services 7.0 Software (PS-7.0.0.1.1428.svar) on a clean system per the Avaya Aura® Presence Services Snap-in Reference.

Installation on an existing Presence Services 7.0.0.0 EDP cluster

To apply a service pack update to an EDP cluster already running a 7.0.0.0 release, perform the following steps:

Important: Applying a Service Pack Update is service affecting to all snap-ins on the EDP cluster. This action should only be performed during maintenance windows. Ensure you perform the steps (below) in order; failure to do so can lead to loss of configuration and real-time data as well as loss of service.

1. Download the new service pack update from PLDS to your desktop.
2. Log in to the Avaya Aura® System Manager Web interface.
3. Navigate to Home / Elements / Engagement Development Platform / Cluster Administration.
4. Find the cluster you will be updating and tick the check box next to it.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

5. Click “Cluster State”, then “Deny New Service”.
6. Navigate to Home / Elements / Engagement Development Platform / Service Management.
7. Click “Load” then “Browse” to the PresenceServices-7.x.x.x.x.svar file, then click the “Load” button.
8. Find the Presence Services version you are currently running and check the box next to it.
9. Click “Uninstall”, select the Cluster Name of the presence cluster you wish to update, tick the check box to force the uninstall, and then click **Commit** in the dialog box.
10. Find the Presence Services version you want to update to and tick the check box next to it.
11. Click “Install”, select the Cluster Name of the presence cluster you wish to update then click **Commit** in the dialog box.
12. Find the Presence Services version you were previously running and check the box next to it.
13. Click “Delete” then click the “Delete” button in the dialog box.
14. Navigate to Home / Elements / Engagement Development Platform / Cluster Administration.
15. Find the cluster you updated and tick the check box next to it.
16. Click “Cluster State”, then “Accept New Service”.

Installing the 7.0.1.0 release

Download and install the Avaya Aura Presence Services 7.0 Software (PS-7.0.1.0.832.svar) on a clean system per the Avaya Aura® Presence Services Snap-in Reference.

New Installations

New installation quick reference	Download	Prerequisite Downloads
Presence Services Snap-in on EDP	PS-7.0.1.0.358.zip (PLDS ID: PS070001000)	**Avaya Breeze 3.1 FP1 Platform OVA** **Download ID:** CE000000126 **Size:** 2,712 MB **Release date:** Dec. 14, 2015 **md5sum**:51723d1a004a85e7d0b37a2cc39e2c17 **File version:** EDP-3.1.1.0.311006_OVF10.ova **ISO File version:** aus-installer-3.1.1.0.311006.iso

New installations of Presence Services 7.0.1.0, on platforms that are not currently running Presence Services, are only supported using the following deployment method:

- Presence Services Snap-in on EDP Download and install the Avaya Aura Presence Services 7.0 Software (PS-7.0.1.0.832.svar) on a clean system per the *Avaya Aura® Presence Services Snap-in Reference Guide*.

Note: At the time general availability of Presence Services 7.0 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 7.0 deployments.

Installation on an existing Presence Services 7.x.x.x Avaya Breeze cluster

To apply a service pack update to an Avaya Breeze cluster already running a 7.x.x.x release, perform the following steps:

Important: Applying a Service Pack Update is service affecting to all snap-ins on the Avaya Breeze cluster! This action should only be performed during maintenance windows. Ensure you perform the steps (below) in order; failure to do so can lead to loss of configuration and real-time data as well as loss of service.

Important: Presence Services 7.0.1 must be deployed on Avaya Breeze 3.1.1 or newer. It is important that existing instances of Avaya Breeze be upgraded to release 3.1.1 prior to upgrading the presence services SVAR to release 7.0.1.

1. Download the new PS software release update from PLDS to your desktop.
2. Log in to the Avaya Aura® System Manager Web interface.
3. Navigate to Home / Elements / Avaya Breeze / Cluster Administration.
4. Find the cluster you will be updating and tick the check box next to it.
5. Then "Click "Cluster State Deny New Service".
6. Navigate to Home / Elements / Avaya Breeze / Service Management.
7. Click "Load" then "Browse" to the PresenceServices-7.x.x.x.x.svar file, then click the "Load" button.
8. Find the Presence Services version you are currently running and check the box next to it.
9. Click "Uninstall", select the Cluster Name of the presence cluster you wish to update, tick the check box to force the uninstall, and then click **Commit** in the dialog box.
10. Find the Presence Services version you want to update to and tick the check box next to it.
11. Click "Install", select the Cluster Name of the presence cluster you wish to update then click **Commit** in the dialog box.
12. Find the Presence Services version you were previously running and check the box next to it.
13. Click "Delete" then click the "Delete" button in the dialog box.
14. Navigate to Home / Elements / Avaya Breeze / Cluster Administration.
15. Find the cluster you updated and tick the check box next to it.
16. Click "Cluster State", then "Accept New Service".

Upgrades/Migrations from 6.2.x to 7.0.1

Changes Affecting Migrations to 7.0.1

Avaya Aura® Presence Services 7.0 introduces significant changes that affect migrations to PS 7.0:

- Avaya Presence Services inventory elements are no longer automatically created; they must be configured on System Manager. There should only be one Presence Services on each Avaya Breeze element defined per cluster.
- Presence Profile (System Manager Home > Users > User Management > Manage Users > Communication Profile > Presence Profile) is mandatory in order to enable presence for a user.
- In order to be presence-enabled, a user must be administered with a Presence Profile (Users > User Management > Manage Users > Communication Profile > Presence Profile) that is associated with a Presence Services server. In pre-PS 7.0.0.0 releases, a user's Presence Profile is associated with a Managed Element (Services > Inventory > Managed Elements) of type / sub-type Presence Services / Presence Services. In PS 7.0.0.0 or higher, a user's Presence Profile is associated with a Managed Element of type / sub-type Presence Services / Presence Services on Avaya Breeze. If migrating users from pre-PS 7.0.0.0 to PS 7.0.1.0, the Presence Profile for those users must be updated. A script (migrate.sh) is available to perform this action.
- Obtain the migrate.sh script from the PresenceServices-Migration-Bundle.zip in PLDS (PLDS ID = PS070000001)
- Copy the bundle to a temporary directory on System Manager, for example /tmp/
- Log in to System Manager as a root user

- Change to the temporary directory (e.g. cd /tmp)
- Unzip the bundle
- To modify the Presence Profile users, execute the following command:

  ```
  ./migrate.sh -v7 -m <existing-ps> <new-ps>
  ```

  where

  <existing-ps> is the name of the Presence Services / Presence Services Managed Element currently associated with the users at Users > User Management > Manage Users > Communication Profile > Presence Profile > System

  <new-ps> is the name of the Presence Services / Presence Services on Engagement Development Platform Managed Element that will be associated with the user
- For more migration details refer to the PresenceServices-Migration-Bundle help.pdf file in the zip.
- A "Presence Services Cluster FQDN" must be defined. This FQDN will represent an Avaya Breeze "Core Platform" Cluster running the Presence Services Snap-in on one or more Avaya Breeze server instances.
  - The "Presence Services Cluster FQDN" must be configured in the customer's DNS as a "CNAME" record resolving to all Avaya Breeze server instance's Security Module addresses (round-robin equal weight).
  - All Avaya Breeze server instances must be provisioned in System Manager's Local Host Name Resolution table. The "Presence Services Cluster FQDN" must be mapped to each Avaya Breeze server instance's Security Module address with equal weight.
  - A single SIP Entity must be created of Type "Presence Services" using the "Presence Services Cluster FQDN" as the target. This entity must have SIP Entity Links to all Session Managers in the deployment from port 5061 (TLS) to Session Manager port 5062 (TLS).
  - SIP Entity / SIP Entity Links must also be created for each Avaya Breeze server instance's Security Module address per standard Avaya Breeze deployment guidelines.
- Applications using 6.2 or earlier versions of LPS will be unable to integrate with Presence Services 7.0. Applications must use the Presence Services 7.0 compatible LPS client. This includes:
  - Avaya one-X Client Enablement Services
  - Avaya one-X Attendant
- Avaya Multimedia Messaging (AMM) XMPP federation is not supported in Presence services 7.0.0. Current GA versions of AMM (<2.1) are not supported with Presence Services 7.0.0. AMM 3.0 will support REST-based integration and will be fully compatible with Presence services 7.0.1 and above.
- All presence-related configuration on Avaya Aura® System Manager will be migrated automatically when System Manager is upgraded to release 7.0 however, Presence Services 6.2 XCP configuration data (collectors and federation), Archived/Offline IMs and user retained manual presence states are not automatically migrated. The PresenceServices-Migration-Bundle.zip in PLDS (PLDS ID = PS070000001) does provide support for migrating most of these configurations if desired. Refer to documentation contained in the bundle for detailed instructions.

In order to run Presence Services 7.0.1.0, migrations should be performed using the following method:

- Presence Services Snap-in on Avaya Breeze:

Download and install the Avaya Aura Presence Services 7.0.1.0 Software (PS-7.0.1.0-832.svar) on an EDP 3.1.1 Core cluster.

Note: At the time general availability of Presence Services 7.0.1.0 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 7.0.1.0 deployments.

Migrations to release 7.0.1.0 are supported from the following releases only:

Minimum required versions by Release

Release	Minimum Required Version
Avaya Aura® Presence Services 6.2 Feature Pack 4	PS-6.2.4.4-641 + any additional patch(es)
Avaya Aura® Presence Services 6.2 Service Pack 5	PS-6.2.5.5-85 + any additional patch(es)
Avaya Aura® Presence Services 6.2 Service Pack 6	PS-6.2.6.13-38 + any additional patch(es)
Avaya Aura® Presence Services 6.2 Service Pack 7	PS-6.2.7.2-58 + any additional patch(es)

Capacity Limits

Endpoint Type	Max # of users	Max # of devices	Max avg. # of contacts per user	Default max # of contacts per user***	Max # Subscriptions/ minute/node	Max # of presence updates per second/node	Max # of XMPP IMs per second/node
SIP	Up to 16,000 on a single node, 125,000 on an 8 node cluster* 250,000 on two 8 node clusters*	175,000 (single cluster) / 350,000 (dual cluster)**	25	100	300	30	44
H.323 (XMPP)	Up to 16,000 on a single node, 125000 on an 8 node cluster* 250,000 on two 8 node clusters*	125,000 (single cluster) / 250,000 (dual cluster)	25	100	300	30	44

Important Notes

- *Clustered deployments of Presence Services are limited to a maximum of 8 nodes in a cluster and all nodes in the cluster must reside on the same subnet. A total of 250,000 users can be supported if two 8 node clusters are deployed. For cluster deployments all nodes in the cluster must use the same resource profile (12 vCPUs, 27 GB of RAM, 28,800 MHz of CPU reservation).
- **When the MDA feature is used, presence services can support an average of 1.4 devices per user for a maximum total of 175,000 devices per cluster or 350,000 devices per Aura system (max two 8 node PS clusters).
- ***By default the maximum number of contacts permitted per user is 100. This is a configurable option and the maximum can be increased but it is important to remember that a fully loaded PS system can only support an average of 25 contacts per user.
- There are a number of significant changes to basic administration required for Presence Services in this release. Refer to the Administering Avaya Aura® Presence Services Snap-in reference guide for complete details.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Installing the 7.0.1.1 release

Download and install the Avaya Aura Presence Services 7.0.1.1 Software (PS-7.0.1.0.842.svar) on a clean system per the Avaya Aura® Presence Services Snap-in Reference.

New Installations

New installation quick reference	**Download**	**Prerequisite Downloads**
Presence Services Snap-in on EDP	PS-7.0.1.0.447.zip (PLDS ID: PS070001000)	**Avaya Breeze 3.1 FP1 Platform OVA** **Download ID:** CE000000126 **Size:** 2,712 MB **Release date:** Dec. 14, 2015 **md5sum**:51723d1a004a85e7d0b37a2cc39e2c17 **File version:** EDP-3.1.1.0.311006_OVF10.ova **ISO File version:** aus-installer-3.1.1.0.311006.iso

New installations of Presence Services 7.0.1.1, on platforms that are not currently running Presence Services, are only supported using the following deployment method:

- Presence Services Snap-in on EDP Download and install the Avaya Aura Presence Services 7.0 Software (PS-7.0.1.0.842.svar) on a clean system per the *Avaya Aura® Presence Services Snap-in Reference Guide*.

Note: At the time general availability of Presence Services 7.0 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 7.0 deployments.

Installation on an existing Presence Services 7.x.x.x Avaya Breeze cluster

To apply a service pack update to an Avaya Breeze cluster already running a 7.x.x.x release, perform the following steps:

Important: Applying a Service Pack Update is service affecting to all snap-ins on the Avaya Breeze cluster! This action should only be performed during maintenance windows. Ensure you perform the steps (below) in order; failure to do so can lead to loss of configuration and real-time data as well as loss of service.

Important: Presence Services 7.0.1 must be deployed on Avaya Breeze 3.1.1 or newer. It is important that existing instances of Avaya Breeze be upgraded to release 3.1.1 prior to upgrading the presence services SVAR to release 7.0.1.

1. Download the new PS software release update from PLDS to your desktop.
2. Log in to the Avaya Aura® System Manager Web interface.
3. Navigate to Home / Elements / Avaya Breeze / Cluster Administration.
4. Find the cluster you will be updating and tick the check box next to it.
5. Then "Click "Cluster State Deny New Service".
6. Navigate to Home / Elements / Avaya Breeze / Service Management.
7. Click "Load" then "Browse" to the PresenceServices-7.x.x.x.x.svar file, then click the "Load" button.
8. Find the Presence Services version you are currently running and check the box next to it.
9. Click "Uninstall", select the Cluster Name of the presence cluster you wish to update, tick the check box to force the uninstall, and then click **Commit** in the dialog box.
10. Find the Presence Services version you want to update to and tick the check box next to it.

11. Click “Install”, select the Cluster Name of the presence cluster you wish to update then click **Commit** in the dialog box.
12. Find the Presence Services version you were previously running and check the box next to it.
13. Click “Delete” then click the “Delete” button in the dialog box.
14. Navigate to Home / Elements / Avaya Breeze / Cluster Administration.
15. Find the cluster you updated and tick the check box next to it.
16. Click “Cluster State”, then “Accept New Service”.

Interoperability and requirements/Applicability

Application	Certified Version	Minimum Supported Version	Mandatory / Optional
Avaya Breeze Platform	3.1.1	3.1.1	M
Avaya Aura® System Manager	7.0.1	7.0.0	M
Avaya Aura® Session Manager	7.0.1	7.0.0	M
Avaya Aura® Communication Manager	7.0.1	6.3.x	O
Avaya Appliance Virtualization Platform	7.0.1	7.0.0	O
Avaya Aura® Application Enablement Services	7.0.1	6.3.3	O
Avaya one-X® Client Enablement Services	6.2.5	6.2.5	O
IBM® Domino®	8.5.3	8.5.3	O
Microsoft Lync®	Lync 2013	Lync 2010	O
Microsoft Exchange	Exchange 2013	Exchange 2010 SP1	O
Avaya Session Border Controller for Enterprise	6.3.3	6.3.3	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-7.0.1.0.833.zip	7.0.1.0-833	7.0.0.0.1395 or higher
PresenceServices-LPS-SDK-7.0.1.0.824.zip	7.0.1.0-824	7.0.0.0.1395 or higher
PresenceServices-LPS-SDK-7.0.0.1.910.zip	7.0.0.1-910	7.0.0.0.1395 or higher
PresenceServices-Connector-SDK-7.0.0.1-862.zip	7.0.0.0-862	7.0.0.0.1395 or higher

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

Troubleshooting the installation

See the troubleshooting section of the Avaya product documentation.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Functionality not supported in Presence Services 7.0.x.x

Avaya Multimedia Messaging (AMM) XMPP federation is not supported in Presence services 7.0. Current GA versions of AMM (<2.1) are not supported with Presence Services 7.0.0. AMM 3.0 will support REST-based integration and will be fully compatible with Presence services 7.0.1 and above.

What's new in Presence Services 7.0.x.x

What's new in Presence Services Release 7.0.0.0

The following table lists enhancements in this release:

Enhancement	Description
Presence Services (PS) is now deployed as a Snap-in on Engagement Development Platform (EDP) 3.1	Presence Services is now delivered as a Snap-in application on Avaya Engagement Development Platform 3.1. All other deployment models have been deprecated (software-only, System Platform, Avaya Appliance Virtualization Platform).
Active – Active High Availability	The Presence Services HA feature now operates in active/active mode (it was active/standby in previous releases). The advantage of active/active is that service to the endpoints is not interrupted in the event of a nodal failure which results in a switchover of users to the standby nodes.
Support PS to PS federation with clustered deployments	Federation between presence systems is now possible even with clustered deployments. Previously the PS to PS federation feature was only available with single node deployments. As of release 7.0 it is now possible to federate clustered PS deployments.
Block IMs between users with different tenant IDs	In release 7.0 it is now possible to block the exchange of IMs between users who have different tenant IDs. This allows the deployment of multi-tenant solutions where each group of tenants is isolated from each other.
Improved capacity	It is now possible to scale a Presence Services solution to 250K users. In release 7.0 it is you can now deploy 2 clusters (clusters must be federated to each other) of 125K users for a total of 250K users on a single Presence Services deployment.
Presence Services supported in Multi Device Access (MDA) solutions	Presence Services is now compatible with solutions using MDA. Refer to the MDA whitepaper for further details. https://downloads.avaya.com/css/P8/documents/100181252. Note that for MDA deployments the presence services application will support an average of 1.4 devices per user. For example, if the system is configured with 1000 users it can support up to 1400 devices. This means that 400 of the 1000 users can have 2 devices each or 200 of the 1000 users can have 3 devices each, and so on. On average the system cannot have note than 1.4 devices per user.
Simplified administration for Lync Federation	Previously, for Lync integration, the administrator was required to enter/administer the PS handle of the Avaya Aura® users twice: once as the Avaya Presence/IM (formerly XMPP) handle and the second time as the Avaya SIP handle. The duplicate administration was required for proper routing of Avaya Aura® Presence Services 7.0.0.0 Page 14 of 24 Issue 1.02, November 2015 the Lync originated subscription and IM requests. PS 7.0.0 removes the need for duplicate administration of the PS handle.

What's new in Presence Services Release 7.0.0.1

Refer to previous release notes and PCNs for information about updates introduced in earlier releases.

What’s new in Presence Services Release 7.0.1

The following table lists enhancements in this release:

Enhancement	Description
Support for XMPP federation	Support for XMPP federation is a feature that provides equivalency to the PS 6.2.X feature set. Although this feature was delivered as part of the PS 7.0.1 release it was patched back to PS 7.0.0.0 in early September of 2016. So any existing PS 7.0.0.X deployment will already have this capability.
IM and enhanced presence API support for PS connector	Presence Services release 7.0.1 adds support for Instant Messaging and Eventing (subscribing for presence updates) via the PS connector deployed on the Avaya Breeze general purpose cluster. This gives developers the ability to create their own SNAP-INs for Avaya Breeze which integrate Presence and Instant Messaging.
Presence domain sharing	In release 7.0.1 it is now possible to share a presence domain with federated systems like Lync, Cisco Jabber or Openfire. Presence Services 7.0.1 also allows for the sharing of domains between multiple PS clusters which are administered by the same SMGR. In previous releases each PS cluster required a unique domain.
Option to forward all IM traffic to AMM	In release 7.0.1 it is now possible to forward all XMPP Instant Messages to AMM when AMM is deployed as part of the solution. This capability can be enabled on a per user basis or for groups of users.
Geographic Redundancy	Presence Services 7.0.1 now supports the deployment of geographically redundant systems. In the event that there is a total outage in one of the datacenters the PS cluster in the backup datacenter will take over without users experiencing any loss of service.
Federation with Cisco Jabber	Presence Services can now be federated with Cisco Jabber via XMPP. This allows the exchange of Presence states and Instant Messages between users hosted by Avaya Aura and users hosted by Cisco Jabber.
Note aggregation from various clients	Note aggregation is a PS 6.2.X equivalency feature that was not available in PS 7.0.0.X. As part of PS 7.0.1 support for note aggregation has been re-introduced.
Upgrade scripts for XCP controller data (PS 6.2.X -> PS 7.0.X)	These upgrade scripts simplify the migration of existing 6.2.X system to the new PS 7.0.X releases.
Serviceability enhancements	The following serviceability enhancements have been included in PS 7.0.1: • The tracePS tool provides a consolidated, graphical view of SIP and XMPP messages flowing in & out of the system. For system administrator and Avaya support use only. • A new Command line tool to view Gigaspaces objects using SQL-like syntax. For Avaya support use only. • Web tool for admin to broadcast an IM to all users logged in. For system administrator use, or optionally for use by select individual users to whom the system administrator has made the tool available. • Command line tool to see a list of all clients logged into the server and their latest presence information. For Avaya support use only. • Improved logging mechanism at a module level. For Avaya support use only.

Enhancement	Description
	System administrators should leave the default logging levels in place. - Periodic health checks to determine if a misconfiguration has occurred and raise alarms.
Simplified solution administration for large deployments	In PS release 7.0.1 the cluster to cluster connectivity (used in large deployments with 125K+ users) is now created automatically. The administrator no longer needs to create the inter cluster connections. In the case of upgrades where the administrator has previously already created the inter cluster links, the existing links do not need to be removed.

Fixes in Presence Services 7.0.x.x

Fixes in Release 7.0.0.X

This Presence Services release addresses all known issues that previously existed on PS 6.2. The following issues have been resolved in cumulative updates to the 7.0.0.1 release:

Cumulative Update Version: PresenceServices-Bundle-7.0.0.0.274	
Tracking #	**Issue**
PSNG-814	Implement presstatus serviceability command for Avaya Services
CR-PSNG-742	Implement OpenFire XMPP federation support
PSNG-1961	Message Archives are not uploaded to SFTP server when using presence HA cluster
PSNG-2012	Presence Services unavailable after EDP instance reboot. While in this state Presence Services responds to SIP messages with a SIP 500/503 Service Unavailable.
PSNG-1810	Watcher of a dual registration presentity does not receive correct channel presence
PSNG-2242	A logged out presentity can erroneously appear as Available
PSNG-2315	Improve service start-up time
PSNG-2336	Support custom channel attributes for Avaya one-X® Agent presentity
PSNG-2407	Empty Message Archive files remain on EDP in /var/avaya/
Cumulative Update Version: PresenceServices-Bundle-7.0.0.0.295	
Tracking #	**Issue**
PSNG-2439	Watcher of an AES collected presentity receives inconsistent presence
PSNG-2454	Improve service recovery when failed service instance is returned to cluster
Service Pack Version: PresenceServices-Bundle-7.0.0.1.361	
Tracking #	**Issue**
PSNG-1810	Dual registration: Channel presence not working correctly
PSNG-2242	Presence state of OneX in logout state is displayed as "Available". Aura 7.0 specific
PSNG-2319	XMPP Fed does not work if disabled at startup
PSNG-2322	When removing a Service Profile from a user, the User Default Access Control policy does not get

Cumulative Update Version: PresenceServices-Bundle-7.0.0.0.274	
	removed in the PRE
PSNG-2332	HandleDao: Incorrect algorithm to lookup handles
PSNG-2395	XMPP Fed: rosters table "isexternalcontact" field not set when Aura SIP W adds fed contact
PSNG-2336	1XA: Preserve vClass for watchers
PSNG-2407	Orphaned Message Archive zip files in /var/avaya
PSNG-2439	1XC H323 user with AES collection enabled - watching is inconsistent
PSNG-2454	Improve Recovery Mechanism when Failed Node Returned to Cluster
PSNG-2462	PS responds to adhoc subscription with self PIDF
PSNG-2341	XMPP Fed Robustness: PSNG multi-domain, OF sends stream error (invalid from)
PSNG-2612	PS continues to send NOTIFYs for deleted contacts
PSNG-2707	XMPP Federation: Openfire user sees presence status of Aura user as "Offline" after logging out/logging in
PSNG-2792	Enhance cluster monitor's homing algorithm

Fixes in Release 7.0.1

Cumulative Update Version: PresenceServices-Bundle-7.0.1.0.358	
Tracking #	**Issue**
PSNG-2637	Traffic on Standalone cause DataGridException
PSNG-2022	DRS Repair does not recreate any PRE's with external federation contacts.
PSNG-2012	Presence Service Unavailable after Avaya Breeze server Rebooted
PSNG-1768	NTPD time update (~ +4hr delta) causes problems for AES collector - not all users counted properly by AesMetrics
PSNG-1578	PS fails to persist the first DB operation after a cluster DB switchover
PSNG-1452	When the IP Address has changed in a EDP Cluster the Admin must resubmit the associated Presence Element in the Manage Elements page
PSNG-1372	Changing the name of the EDP Cluster causes the Cluster to be removed from the Presence Services Element in the Inventory table
PSNG-1184	PS on EDP Element Manager Provisioning - EDP Cluster IP address not auto filled on Microsoft® Internet Explorer (IE)

Fixes in Release 7.0.1.1

Cumulative Update Version: PresenceServices-Bundle-7.0.1.0.447	
Tracking #	**Issue**
PSNG-3457	GSQL tool doesn't work with non-default cust and root passwords
PSNG-3526	PS is dropping from resource id in messages sent to AMM

Cumulative Update Version: PresenceServices-Bundle-7.0.1.0.447	
PSNG-3535	Exchange Integration: There isn't event time period in Exchange calendar tuple
PSNG-3536	Domino Integration: There isn't event time period in Domino calendar tuple
PSNG-3561	PS Tasks fails to deploy
PSNG-3576	Calendar tuples timed-status element should conform to rfc4481 (for Exhange & Domino)
PSNG-3597	Lync presence not sent to subscribed clients
PSNG-3670	CFD: Users not getting updated when on calls or in meetings in Outlook

Known issues and workarounds in Presence Services 7.0.x.x

Known issues and workarounds in Release 7.0.0.0

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

ID	Minimum conditions	Visible symptoms	Workaround
PSNG-2722	Users with presence IM handles that contain upper case characters deployed in conjunction with Lync or InterPS federation.	In cases where Lync Federation or Inter PS federation is enabled presence updates will not be sent over federation boundaries.	Edit user handles so that they are all lower case.
PSNG-2022	DRS Repair does not recreate any PRE's with external federation contacts.	When the administrator performs a DRS repair on SMGR, any presence relationships involving external federation contacts will not get re-created. This would affect Lync and Inter-PS federation in 7.0.0 and XMPP Federation in 7.0.0.1. Result would be no presence from federated contacts. Note: The action taken to trigger this problem is a manual step to perform a DRS repair. If the administrator never does a DRS repair, then they should not run into this problem.	Restart PS service, or disable/re-enable the configured federation in the Service Attributes.
PSNG-2012	Presence Service Unavailable after EDP server Rebooted	Occasionally if the server on which the EDP platform is rebooted the PS application does not recover, The issue is the result of the EDP application not sending an indication to the PS SNAP-IN letting the PS application know that the EDP platform is ready to provide service.	Manually restart the PS application after the EDP platform has recovered from the server reboot. A fix for this issue will be delivered in PS 7.0.0.1 which will become GA no later than Sept 8th 2015.
PSNG-1768	NTPD time update (~ +4hr delta) causes problems	When Linux first comes up it loads the current time from the internal clock h/w (thru VMware), if this clock is 4 hours or more off the actual time	Adjust & save the Linux clock (contact Avaya support for assistance with making this

ID	Minimum conditions	Visible symptoms	Workaround
	for AES collector - not all users reacquired	-Everything starts up OK including WAS, EDP & PS (+ AES collector). -But when an NTP update comes in and corrects the clock, the AES Collector will lose its connection to the AES server. The AES Collector does automatically recover its link to the AES server however not all users are re-acquired.	change) such that a reboot will not trigger the AES Collector restart to the server. If the problem does occur, recover all users by stop & restart the AES Collector via SMGR (disable & re-enable component).
PSNG-1578	PS fails to persist the first DB operation after a cluster DB switchover	After a DB switchover in a multi node cluster the first DB operation fails to persist. For example if user A is in the manual state "Busy" prior to the DB switchover and user A switcher to a different manual state after the s/o, that first change does not persist and watchers do not see the updated state. This only happens with the first change. All subsequent changes by User A are reflected properly. Additionally this only happens with the first change by any of the users on the system. As soon as a single user makes a change all subsequent changes by all other users work properly.	
PSNG-1452	When the IP Address has changed in a EDP Cluster the Admin must resubmit the associated Presence Element in the Manage Elements page	When the EDP Cluster IP address changes the PS on CE Manage Element must be resubmitted. The Admin will see text in red on the Manage Element edit page for that element that indicates the IP address is "updated".	
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.	
PSNG-1372	Changing the name of the EDP Cluster causes the Cluster to be removed from the Presence Services Element in the Inventory table	If the name of the EDP cluster is changed the cluster will be removed from the presence services element in the inventory table.	The simple solution is to simply not change the name of the EDP cluster until this issue is fixed. Alternatively if the administrator feels that the cluster name must be changed, then the cluster can be manually added back into the inventory table.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum conditions	Visible symptoms	Workaround
PSNG-1184	PS on EDP Element Manager Provisioning - EDP Cluster IP address not auto filled on Microsoft® Internet Explorer (IE)	The EDP cluster IP address is not auto filled when using Microsoft® Internet Explorer.	Use either Chrome or Firefox instead of Microsoft® Internet Explorer.
ASM-447	PS-PS federation in a single SMGR(multi SMs): SM1 cannot route SUBSCRIBE message to federated PS	In deployments which use PS to PS federation with both PS clusters hosted by the same System Manager there is an intermittent issue which results in the failure of presence subscription requests. If the subscription request from the watcher is routed to the home SM node of the presentity no issue is encountered. But if the subscription request is sent routed to an SM that is not the home node of the watcher the subscription request will fail.	If the subscription request fails the watcher should simply try again and the next attempt will work.
Note		In cases where a multi node cluster is deployed in Non HA mode (not protected) the administrator will need to manually stop and then restart the service from SMGR in the event that one of the nodes in the cluster fails. This limitation does not apply to multi node cluster deployments with HA (protected deployments) and it does not apply to single node deployments which are non HA (not protected).	
Note		Presence Services 7.0.0 is not compatible with Avaya Multimedia Messaging 2.1. Users that have deployed PS 6.2.6 and AMM 2.1 need to wait until AMM 3.0 is delivered before upgrading to PS 7.0.0.	
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: Toggle the favorite flag for the federated user in the Avaya client. Logout and log back in to the Avaya client.
Note		Installations with Lync Federation using Avaya Aura SIP endpoints cannot use an Aura SIP Domain that is the same as the Lync SIP TLS Federated Domain. Doing so will result in lack of presence for Aura SIP endpoints.	Ensure that the Aura SIP Domain used by SIP endpoints is different than the Lync Federation domain. This limitation will be addressed in PS 7.0.1 which will allow Lync

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum conditions	Visible symptoms	Workaround
			and Aura to share SIP domains.

Known issues and workarounds in Release 7.0.0.1

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

ID	Minimum conditions	Visible symptoms	Workaround
PSNG-2637	Traffic on large systems Standalone cause DataGridException	In large deployments (2000+ users) where Instant Message archiving is enabled the system experiences Data Grid Exceptions which will cause both presence and IM to become temporarily unavailable.	For deployments with IM archiving disabled no work around is required as this issue will not occur. For deployments with IM archiving enabled if the problem occurs there is no need to take corrective action as the system will recover on its own. Note: A fix for this issue is being developed and will be delivered via a cumulative update as soon as it is available.
PSNG-2722	Users with presence IM handles that contain upper case characters deployed in conjunction with Lync or InterPS federation.	In cases where Lync Federation or Inter PS federation is enabled presence updates will not be sent over federation boundaries.	Edit user handles so that they are all lower case.
PSNG-2022	DRS Repair does not recreate any PRE's with external presentities	When the administrator performs a DRS repair on SMGR, any presence relationships involving external presentities (i.e. federation contacts) will not get re-created. This would affect Lync and Inter-PS federation in 7.0.0 and XMPP Federation in 7.0.0.1. Result would be no presence from federated contacts.	Restart PS service, or disable/re-enable the configured federation in the Service Attributes. Note: The action taken to trigger this problem is a manual step to perform a DRS repair. If the administrator never does a DRS repair, then they should not run into this problem.
PSNG-1768	NTPD time update (~ +4hr delta) causes problems for AES collector - not all users reacquired	When Linux first comes up it loads the current time from the internal clock h/w (thru VMware), if this clock is 4 hours or more off the actual time -Everything starts up OK including WAS, EDP & PS (+ AES collector). -But when an NTP update comes in and corrects the clock, the AES Collector will lose its connection to the AES server. The AES Collector does automatically recover its link to the AES server however not all users are re-acquired.	Adjust & save the Linux clock (contact Avaya support for assistance with making this change) such that a reboot will not trigger the AES Collector restart to the server. If the problem does occur, recover all users by stop & restart the AES Collector via SMGR (disable & re-enable component).
PSNG-1578	PS fails to persist the first DB operation	After a DB switchover in a multi node cluster the first DB operation fails to	

ID	Minimum conditions	Visible symptoms	Workaround
	after a cluster DB switchover	persist. For example if user A is in the manual state “Busy” prior to the DB switchover and user A switcher to a different manual state after the s/o, that first change does not persist and watchers do not see the updated state. This only happens with the first change. All subsequent changes by User A are reflected properly. Additionally this only happens with the first change by any of the users on the system. As soon as a single user makes a change all subsequent changes by all other users work properly. This issue will be fixed when PS 7.0.1 is released.	
PSNG-1452	When the IP Address has changed in an EDP Cluster the Admin must resubmit the associated Presence Element in the Manage Elements page.	When the EDP Cluster IP address changes the PS on CE Manage Element must be resubmitted. The Admin will see text in red on the Manage Element edit page for that element that indicates the IP address is "updated".	
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.	
PSNG-1372	Changing the name of the EDP Cluster causes the Cluster to be removed from the Presence Services Element in the Inventory table.	If the name of the EDP cluster is changed the cluster will be removed from the presence services element in the inventory table.	The simple solution is to simply not change the name of the EDP cluster until this issue is fixed. Alternatively if the administrator feels that the cluster name must be changed, then the cluster can be manually added back into the inventory table.
PSNG-1184	PS on EDP Element Manager Provisioning - EDP Cluster IP address not auto filled on Microsoft® Internet Explorer (IE)	The EDP cluster IP address is not auto filled when using Microsoft® Internet Explorer.	Use either Chrome or Firefox instead of Microsoft® Internet Explorer.
ASM-447	PS-PS federation in a single SMGR(multi SMs): SM1 cannot route SUBSCRIBE message to federated PS	In deployments which use PS to PS federation with both PS clusters hosted by the same SMGR there is an intermittent issue which results in the failure of presence subscription requests. If the subscription request from the watcher is routed to the home SM node of the presentity no issue is encountered. But if the subscription request is sent routed to an SM that is not the home	If the subscription request fails the watcher should simply try again and the next attempt will work.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum conditions	Visible symptoms	Workaround
		node of the watcher the subscription request will fail.	
Note		In cases where a multi node cluster is deployed in Non HA mode (not protected) the administrator will need to manually stop and then restart the service from SMGR in the event that one of the nodes in the cluster fails. This limitation does not apply to multi node cluster deployments with HA (protected deployments) and it does not apply to single node deployments which are non HA (not protected).	
Note		Presence Services 7.0.0 is not compatible with Avaya Multimedia Messaging 2.1. Users that have deployed PS 6.2.6 and AMM 2.1 need to wait until AMM 3.0 is delivered before upgrading to PS 7.0.0.	
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 Installations with Lync Federation using Avaya Aura SIP endpoints cannot use an Aura SIP Domain that is the same as the Lync SIP TLS Federated Domain. Doing so will result in lack of presence for Aura SIP endpoints. Ensure that the Aura SIP Domain used by SIP endpoints is different than the Lync Federation domain. This limitation will be addressed in PS 7.0.1 which will allow Lync and Aura to share SIP domains.

Known issues and workarounds in Release 7.0.1

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

ID	Minimum conditions	Visible symptoms	Workaround
PSNG-3229	AES collector attribute descriptions provide misleading	The attribute descriptions related to the PS AES collector indicate that changes to the attribute are NOT dynamic. This is incorrect; changes to these attributes are	No workaround is required. Attribute changes are dynamic and take effect right away. The attribute descriptions

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum conditions	Visible symptoms	Workaround
	information.	indeed dynamic and take effect right away.	will be updated in a future release.
PSNG-2722	Users with presence IM handles that contain upper case characters deployed in conjunction with Lync or InterPS federation.	In cases where Lync Federation or Inter PS federation is enabled presence updates will not be sent over federation boundaries.	Edit user handles so that they are all lower case.
PSNG-2630	There is no message notification when Lync sends chat message to 1XC in DND state	When Aura users are in the DND state, and inbound instant messages are archived and not delivered to the user in a DND state. Normally when this occurs a message is sent to the originator indicating that the message was not delivered, but if the originator is a Lync client this non delivery indication is not delivered.	No workaround is available.
PSNG-2268	Calendar collectors for Exchange & Domino cannot run simultaneously	It is not possible to configure calendar collectors for both MS Exchange and IBM Domino at the same time. One of the two can be configured.	No workaround is available.
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.	
ASM-447	PS-PS federation in a single SMGR(multi SMs): SM1 cannot route SUBSCRIBE message to federated PS	In deployments which use PS to PS federation with both PS clusters hosted by the same SMGR there is an intermittent issue which results in the failure of presence subscription requests. If the subscription request from the watcher is routed to the home SM node of the presentity no issue is encountered. But if the subscription request is sent routed to an SM that is not the home node of the watcher the subscription request will fail.	If the subscription request fails the watcher should simply try again and the next attempt will work.
Zephyr-40511	Temporary network outages between nodes in a PS cluster result in the failure of the mirror service which can then trigger a system outage.	In deployment where a multi node PS cluster is deployed (issue does not occur with single node clusters) a total system outage may occur if the connectivity between the nodes in the cluster is interrupted.	This issue will only occur when Avaya Breeze 3.1.1.1 is used. The problem will NOT occur when Avaya Breeze 3.1.1 is used. The work around is to use Avaya Breeze 3.1.1 instead of 3.1.1.1. PS 7.0.1 will not be supported on Avaya Breeze deployments using release 3.1.1.1 until Zephyr-40511 is fixed.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum conditions	Visible symptoms	Workaround
Note		In cases where a multi node cluster is deployed in Non HA mode (not protected) the administrator will need to manually stop and then restart the service from SMGR in the event that one of the nodes in the cluster fails. This limitation does not apply to multi node cluster deployments with HA (protected deployments) and it does not apply to single node deployments which are non HA (not protected).	
Note		Presence Services 7.0.1 is not compatible with Avaya Multimedia Messaging 2.1. Users that have deployed PS 6.2.6 and AMM 2.1 need to wait until AMM 3.0 is delivered before upgrading to PS 7.0.1.	
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 Installations with Lync Federation using Avaya Aura SIP endpoints cannot use an Aura SIP Domain that is the same as the Lync SIP TLS Federated Domain. Doing so will result in lack of presence for Aura SIP endpoints. Ensure that the Aura SIP Domain used by SIP endpoints is different than the Lync Federation domain. This limitation will be addressed in PS 7.0.1 which will allow Lync and Aura to share SIP domains.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Avaya Aura® Application Enablement Services

Installation for Avaya Aura® Application Enablement Services Release 7.0.x.x

Installation for Avaya Aura® Application Enablement Services Release 7.0

Required patches for 7.0 installation

Download ID	Patch	Notes
AES00000528	7-0-0-0-Patch2.zip	This patch is cumulative and contains updates to the AE Services Server to resolve network, SNMP, DAPI link, LDAP restarts in HA mode, Tomcat, and licensing issues. Refer to PSN # PSN004634 for details.
AES00000531	700_LSUPatch1.bin	This patch contains security updates to the Red Hat 6.5 OS for the AE Services VMware offer. Refer to PSN # PSN004622u for details.

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 7.0.0.0**
- **Deploying Avaya Aura® Utility Services in Virtualized Environment**
- **Release Notes for Avaya Aura® Utility Services Release 7.0.0.0**
- **Deploying Avaya Aura® applications Release 7.0**
- **Upgrading and Migrating Avaya Aura® applications Release 7.0**

For the AE Services 7.0 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 7.0, any customer application relying on the old, Avaya provided server certificate for TLS will not be able to connect to the AE Services 7.0 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 7.0 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.

Note: For any AE Services release, where the installed AE Services server certificate has been replaced with a customer provided certificate, the client/server TLS connection will not be affected by the aforementioned certificate expiration or replacement.

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 7.0 Administration and Maintenance document

*** See the OpenSSL section in the AE Services 7.0 Administration and Maintenance document

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

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*

Upgrading

Application Enablement Services 7.0 Server Pre-Upgrade Instructions

The following steps must be performed on every AE Services 5.x or 6.3.3.4 and older releases. For AE Services server running 6.3.3.5 release before upgrading to the AE Services 7.0 release:

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 is 5.x or 6.x*
4. *Using the AE Services patch process, install the pre-upgrade patch on your existing AE Services server.*
5. *Take a backup of your AE Services server.*
6. *Install AE Services 7.0.*
7. *Using the backup data, perform a restore on the newly installed AE Services 7.0 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.*

Interoperability and requirements

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

Restoring AE Services software to previous version

*Refer to the topic **AE Services 7.0 Server Pre-Upgrade Instructions** above.*

Installation for Avaya Aura® Application Enablement Services Release 7.0.1

*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:

- ***M**igrating and Installing Avaya Appliance Virtualization Platform*
- ***Release Notes for Avaya Appliance Virtualization Platform Release 7.0.1***
- ***Deploying Avaya Aura® Utility Services in Virtualized Environment***
- ***Release Notes for Avaya Aura® Utility Services Release 7.0.1***
- ***Deploying Avaya Aura® applications Release 7.0.1***
- ***Upgrading and Migrating Avaya Aura® applications Release 7.0.1***

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

In AE Services 7.0.1, 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, in order 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 and earlier) that are using TLS to fail to establish a secure socket connection to the AE Services 7.0.1 server. In order to achieve a more secure client/server socket connection, we encourage current client applications to use an AE Services 7.0 SDK where the TLS 1.2 protocol is supported. Note, the previously 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 7.0 SDKs support TLS 1.2. If upgrading to AE Services 7.0 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 of time.

For the AE Services 7.0.1 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 7.0.1, any customer application relying on the old, Avaya provided server certificate for TLS will not be able to connect to the AE Services 7.0.1 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 7.0 release.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

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 7.0.1 Administration and Maintenance document

*** See the OpenSSL section in the AE Services 7.0.1 Administration and Maintenance document.

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

Required patches for 7.0.1 installation

Download ID	Patch	Notes
AES00000536	7-0-1-0-SuperPatch_2.zip	This patch contains updates to the AE Services 7.0.1 server to resolve some DMCC, ASAI, certificate management and server related issues. Refer to PSN # PSN004730u for details.

Installation for Avaya Aura® Application Enablement Services Release 7.0.1

*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:

- ***M**igrating and Installing Avaya Appliance Virtualization Platform*
- ***Release Notes for Avaya Appliance Virtualization Platform Release 7.0.1***
- ***Deploying Avaya Aura® Utility Services in Virtualized Environment***
- ***Release Notes for Avaya Aura® Utility Services Release 7.0.1***
- ***Deploying Avaya Aura® applications Release 7.0.1***
- ***Upgrading and Migrating Avaya Aura® applications Release 7.0.1***

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

In AE Services 7.0.1, 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, in order to mitigate various attacks on the TLS 1.0 protocol. The use of TLS 1.2 is strongly recommended.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

This change may cause older AE Services clients (version AE Services 7.0 and earlier) that are using TLS to fail to establish a secure socket connection to the AE Services 7.0.1 server. In order to achieve a more secure client/server socket connection, we encourage current client applications to use an AE Services 7.0 SDK where the TLS 1.2 protocol is supported. Note, the previously 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 7.0 SDKs support TLS 1.2. If upgrading to AE Services 7.0 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 of time.

For the AE Services 7.0.1 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 7.0.1, any customer application relying on the old, Avaya provided server certificate for TLS will not be able to connect to the AE Services 7.0.1 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 7.0 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 7.0.1 Administration and Maintenance document

*** See the OpenSSL section in the AE Services 7.0.1 Administration and Maintenance document.

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

Installation for Avaya Aura® Application Enablement Services Software Only 7.0.1

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

1. Install Avaya Aura® Application Enablement Services Software Only 7.0.1 (700511328_swonly-7.0.1.0.0.15-20160413.iso).
2. Install Avaya Aura® AE Services 7.0.1 Super Patch 2 (7-0-1-0-SuperPatch_2.zip).

Installation steps for Avaya Aura® Application Enablement Services 7.0.1 Aura® OVA Media

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

1. Install Avaya Aura® AE Services 7.0.1 Aura® OVA Media (700511327_AES-7.0.1.0.0.15.20160413-e50-00.ova)
2. Install Avaya Aura® AE Services 7.0.1 Super Patch 2 (7-0-1-0-SuperPatch_2.zip)

Installation steps for Avaya Aura® Application Enablement Services 7.0.1 RPM-only Installer

Important: Before performing an upgrade or update, a backup of the Application Enablement Services data should be performed.

1. Avaya Aura® AE Services 7.0 Aura® Bundled Media VMWare Template OVA or Avaya Aura® AE Services Software Only 7.0 is installed.
2. Avaya Aura® AE Services 7.0 Linux Security Update Patch 1.
3. Avaya Aura® AE Services 7.0 Patch 2.
4. Avaya Aura® AE Services 7.0.1 RPM-only Installer.
5. Avaya Aura® AE Services 7.0.1 Super Patch 2 (7-0-1-0-SuperPatch_2.zip) or later.

Upgrading to Release 7.0.1

AE Services Virtual Appliance upgrade steps:

1. Upgrade Appliance Virtualization Platform to feature pack release 7.0.1.
2. Upgrade Utility Services to feature pack release 7.0.1.
3. Upgrade AE Services to Release 7.0.1. For the AE Services 7.0.1 upgrade process, see Installation steps for Avaya Aura® Application Enablement Services 7.0.1 RPM-only Installer.

AE Services Software Only and Virtual Environment upgrade steps:

For the AE Services 7.0.1 upgrade process, see Installation steps for Avaya Aura® Application Enablement Services 7.0.1 RPM-only Installer.

Functionality not supported

- AE Services 7.0 does not support the “Bundled” and “System Platform” offers. Customers upgrading to AE Services 7.0 must switch to the “Software-Only” offer or “VMware” (AE Services on AVP) offer.

- In AE Services 7.0, the Machine Preserving High Availability (MPHA) (aka VSST) feature is not available.

What’s new in Application Enablement Services 7.0.x.x

What’s new in Application Enablement Services 7.0.0.0

- AE Services server default certificate has been replaced by a new certificate signed by the installed AE Services server. Reference the Installing section for important information.
- Support for Avaya Aura® 9601 SIP endpoint as a 9608 SIP endpoint.
- Device, Media, and Call Control (DMCC) scale has increased from 4,000 to 8,000 station registrations on one server.
- Shared memory implementation instead of mapped memory.
- Increased support domain control associations from 4 to 8
- Refresh of all third party packages including Red Hat Enterprise Linux (RHEL) 6.5 OS, OpenJDK 1.8, .NET Framework 4.5.2 and IE 11 support.
- Enhance GEOHA with FRHA capabilities.
- Out of band management.
- Detect unreachable SIP endpoints and logout unreachable SIP agents.
- Support Solution Deployment Manager (SDM) common services to enable VMware®.
- Support VMware® for the Avaya Appliance Virtualization Platform (AVP) for the appliance model.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

For additional information, reference the Avaya Aura® Application Enablement Services Overview and Specification on the Avaya Support Site.

What's new in Application Enablement Services 7.0.1

The following table lists enhancements in this release.

Feature	Description
Embedded WebLM in AES to support allocation mode in VMware platform	WebLM server is now included in all AES offers so that there is no need to have separate WebLM server. In EWL configuration, each AES server can have license allocation mode because of embedded WebLM from AES 7.0.1. **Beginning with AE Services 7.0.1, a new license is required to use Embedded WebLM for Software-Only and VMWare offers.**
Support SNMP V3	SNMP v3 is now supported by HMDC.
Validate with ESXSi 6.0 in Virtualized Environment Offer	VMware ESXi 6.0 is supported with AES 7.0.1.
Common Server 3 Support	Support for new Avaya Common Servers (CSR3). Avaya Aura® adds support for HP DL360PG9 and Dell R630 in Avaya Virtual Deployment configurations.
TLS 1.2 support	TLS 1.2 is supported in AES 7.0.1 and it is enabled as a default. AE Services 7.0 Windows based SDKs for TSAPI, CVLAN and DMCC .NET has been updated to support the TLS 1.2 protocol. The remaining AE Services 7.0 SDKs already support TLS 1.2.
AES Log Export	AES 7.0.1 implement rsyslog so that it is possible to send log to a remote server. It is required to configure a remote server, but exporting log files is now automatic.
Changes in AES config logged via syslog	In AES 7.0.1, all logging use syslog. Because of this change, some of file names for logging have been changed.

Fixes in Application Enablement Services 7.0.x.x

Fixes in Release 7.0.0.0

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release found in
AES-14147	Use Device, Media and Call Control (DMCC)	Historic Metric Data Collector (HMDC) -The HMDC service has been updated to use SNMPv3 when retrieving data from the SNMP agent on AE Services. This fixes an issue where the HMDC service was not able to fetch metric data from some components.	6.2
AES-14328	AE Services Server	Management Console-On the TSAPI User Status page, the Time Opened and Time Closed fields are not shown if the time zone is changed to CEST or any other time zone with 4 or more characters. This issue has been fixed.	6.3.3
N/A	AE Services	Security-The version of Apache Tomcat has been updated from 6.0.39 to 6.0.43. For a list of security issues fixed in this version, refer to http://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.43. The version of PHP has been updated from 5.4.23 to 5.4.39-1. For a list of issues fixed in this version, refer to http://php.net/ChangeLog-5.php#5.4.43. AE Services 7.0 has been updated to Red Hat Enterprise Linux (RHEL) 6.5. In addition, the following Red Hat security advisories (RHSA) have been incorporated into AE Services 7.0 – RHSA-2014:0370 – Moderate: httpd security update RHSA-2014:0595 – Important: gnutls security update RHSA-2014:0596 – Moderate: libtasn1 security update RHSA-2014:0625 - Important: openssl security update RHSA-2014:0626 – Important: openssl097a and openssl098e security update RHSA-2014:0771 - Important: kernel security and bug fix update RHSA-2014:0917 – Critical: nss and nspr security, bug fix, and enhancement update RHSA-2014:0981 - Important: kernel security, bug fix, and enhancement update RHSA-2014:1052 - Moderate: OpenSSL security update RHSA-2014:1307 – Important: nss security update RHSA-2014:1389 – Moderate: krb5 security and bug fix update RHSA-2015:0066 – Moderate: OpenSSL security update RHSA-2015:0715 – Moderate: OpenSSL security update RHSA-2015:1081 – Important: kernel security, bug fix, and	7.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
		enhancement update.	

Fixes in Release 7.0.1

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release found in
AES-14403	AE Services Server	AE Services port cannot be disabled from the standard reserve port.	**7.0**
AES-14443	AE Services Server	Logging with an updated Linux or OpenLDAP password creates issues with the User Management Services display. The User Management tab will not display when logging in with a Linux password. When logging in with an OpenLDAP password, the User Management, Status, and Help links will be displayed; however, all other security tabs will not display.	**7.0**
AES-13803	AE Services Server	A new option field has been added under "Utilities->Email Notification" to allow customers to administer the "From" email address. A default value for the 'From" email address is set to the "Hostname" of the AE Services server.	**N/A**
AES-14410	High Availability (HA)	If a restored configuration came from a GRHA enabled AE Server, then after restoring the configuration data, the High Availability page wrongly displays HA to be partially configured.	**7.0**
AES-14830	Must have TSAPI CTI traffic sent to Communication Manager for that CTI link while it is transitioning from the down state to the up state.	When a CTI link state transitions from down to up, TSAPI and DMCC clients may not receive a system status report with status of CTI link up.	**3.0**
AES-14632	Must have UCID enabled with a UCID Network Node ID greater than 255.	TSAPI service sometimes populates the uSourceVDN component of LookaheadInfo parameter with invalid data when it receives "Lookahead Interflow" IE in Call Offered and Route Request ASAI messages from Communication Manager.	**3.0**

Known issues and workarounds in Application Enablement Services 7.0.x.x

Known issues and workarounds Application Enablement Services in Release 7.0.0.0

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

ID	Minimum conditions	Visible symptoms	Workaround
		AE Services Server	
AES-14403	AE Services	AE Services port cannot be disabled from the	From the AE Services Management

ID	Minimum conditions	Visible symptoms	Workaround
	Server	standard reserve port.	Console (OAM) web-pages, click on "Security | Standard Reserved Ports", disable (uncheck) the "Tomcat HTTPS" check box and click "Apply Changes". This should prevent external web-browsers from connecting to the OAM on port 8443 of the AE Services server. In reality, AE Services continues to listen on port 8443. Continuing to listen on port 8443 could be flagged as a security hole by network port scanners (e.g. nMap). However, since this port is used for secure HTTP (HTTPS) connections to Tomcat, the security impact is minimal. This issue has been resolved in AE Services release 7.0.1.
None	AE Services Server	AE Services Server Warning: cannot change directory to /home/root: No such file or directory" is displayed.	When logged in as root, if "su: warning: cannot change directory to /home/root: No such file or directory" is displayed, then open /etc/passwd file and make the following change: Change "root:x:0:0::/home/root:/bin/bash" to "root:x:0:0::/root:/bin/bash". This will change "/home/root" to just "/root".
None	AE Services Server	AE Services Server date and time change process: When the server time is changed by more than five minutes, several of the AE Services must be restarted.	While these services will be restarted on their own, the following procedure is recommended for changing the AE Services Software-Only or Avaya Aura® Bundled Media VMware Template OVA server time: 1. Log into the AE Services Management Console. 2. Select "Maintenance | Service Controller". 3. Set the check boxes for the ASAI Link Manager, CVLAN Service, DLG Service, Transport Layer Service and TSAPI Service, and then click on "Stop". 4. When the confirmation screen is displayed, click on "Stop".

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum conditions	Visible symptoms	Workaround
			5. Select "Maintenance | Date Time/NTP Service", make the appropriate - changes on the web-page and click "Apply Changes". 6. When the confirmation screen is displayed, click on "Apply". 7. Select "Maintenance | Service Controller". 8. Set the check boxes for the ASAI Link Manager, CVLAN Service, DLG Service, Transport Layer Service and TSAPI Service, and then click on "Start".
AES-14443	AE Services Server	Logging with an updated Linux or OpenLDAP password creates issues with the User Management Services display. The User Management tab will not display when logging in with a Linux password. When logging in with an OpenLDAP password, the User Management, Status, and Help links will be displayed; however, all other security tabs will not display.	After changing the Linux password, go to 'User Management' | 'User Admin' | 'Change User Password' to change an OpenLDAP password. This will sync the Linux password with the OpenLDAP password and make all of the links displayed correctly. This issue has been resolved in AE Services release 7.0.1.
		CallVisor Local Area Network (CVLAN) Linux Client	
	CallVisor Local Area Network (CVLAN) Client	Before installing the CVLAN Linux client on a Red Hat Linux ES v5.0 system, a separate installation of the following RPM may be required: openssl097a-0.9.7a-9.el5_4.2.i386.rpm.	This RPM may be available with the Red Hat Linux installation media and is also available for download at http://rpm.pbone.net.
	CallVisor Local Area Network (CVLAN) Client	The CVLAN Linux client, installed on Red Hat Linux ES v5.0 system, may not be able to establish a secure connection to the CVLAN Service when using certificates with SHA2 (e.g., SHA256) signatures. Note: The CVLAN Linux client, installed on Red Hat Linux ES v6.5 system, will be able to establish a secure connection to the CVLAN Service running on AE Services 7.0 server when using certificates with SHA2 (e.g., SHA256) signatures.	Use certificates with SHA1 signatures instead.
		CVLAN Service	
	CVLAN Service	CVLAN Services does not display online. If there are no CVLAN links administered, the CVLAN Service will appear as "OFFLINE" on both the AE	The status will change to "ONLINE" after you administer at least one CVLAN link. This is desirable behavior

ID	Minimum conditions	Visible symptoms	Workaround
		Services summary page and the Status summary page of the AE Services Management Console.	because it stops CVLAN from listening on a port that is not in use and stops that listening port from being reported as a risk on a security audit.
		DLG Service	
	DLG	DLG Service does not display online. If there are no DLG links administered, the DLG Service will appear as "OFFLINE" on both the AE Services summary page and the Status summary page of the AE Services Management Console.	The status will change to "ONLINE" after you administer at least one DLG link. This is desirable behavior because it stops DLG from listening on a port that is not in use and stops that listening port from being reported as a risk on a security audit
		Device, Media and Call Control (DMCC)	
AES-13507	Device, Media and Call Control (DMCC)	When attempting to connect to the AE Services server's IPv6 address using the DMCC Java SDK from Microsoft Windows, the user will see the following error message: "java.net.SocketException: Permission denied: connect"	Oracle is tracking this issue with IPv6 addresses for Java NIO channels on Windows. Currently there is no workaround. This issue will be addressed in a future release of Microsoft Windows.
AES-13492	Device, Media and Call Control (DMCC)	DMCC/TR87 cannot properly track a call made to Vector Directory Numbers (VDNs) or hunt-groups. When a call reaches a VDN and is answered on the far end by an agent or the call reaches a hunt group, Microsoft Office Communicator will create a phantom screen pop and any further transfers will result in new screen pops. This is similar behavior to when a call is alerting on one station and is answered immediately on a different station; DMCC assumes it is a bridged station as there is no differentiation in behavior.	Suppressing bridged call appearances for the station (or VDN) alleviates the issue unless the stations involved are SIP stations.
		High Availability (HA)	
AES-14410	High Availability (HA)	If a restored configuration came from a GRHA enabled AE Server, then after restoring the configuration data, the High Availability page wrongly displays HA to be partially configured.	To fix this issue, after restoring the configuration data go to High Availability page and click on "Remove HA" button before configuring HA again. This issue has been resolved in AE Services release 7.0.1.
AES-14374	High Availability (HA)	Occasionally, the sohd HA arbiter process aborts if the WebLM URL is not configured properly.	There is no need for a workaround as it is restarted automatically by a watchdog.
	High Availability	Once GRHA is configured with one or more virtual IPs, client applications cannot connect to	Check if AE Services has opened all the listen ports on the configured virtual IP address. This can be done by running

ID	Minimum conditions	Visible symptoms	Workaround
	(HA)	AE Services server.	"showHAStatus" command as root on a shell in AE Server Virtual Machine. If the listen ports are not opened on the desired virtual IP address, make sure that on "Networking | AE Services IP (Local IP)" page in the management console the "client connectivity" and the "switch connectivity" are using the desired virtual IP address. If not, select the proper virtual IP from the drop down menu. Restart AE Services via the Service Management Console, whether or not any changes were made. Make sure AE Services has opened the listen ports on the right virtual IP address.
Java Telephony Application Programming Interface (JTAPI)			
AES-13728	Java Telephony Application Programming Interface (JTAPI)	If a JTAPI application is monitoring H.323 stations in a paging group which also contains SIP stations, it does not receive events for the H.323 stations when the stations receive a group call. The expected events are received for the SIP stations	
AES-13960	Java Telephony Application Programming Interface (JTAPI)	JTAPI application monitoring a call does not receive the same sequence of events if a conference is initiated by a third party (either manually or by another CTI application), as opposed to if the application initiates the conference itself.	
Lync 2013 Client			
	Lync 2013 Client	The following are known issues with Lync 2013 client. The cumulative update (CU) 2880474 package for Lync 2013: April 2014 has resolved the Conference and Transfer issues described below. More details can be found by searching the internet for "KB 2941643". The 'redirecting a call' remains an issue after this CU is applied.	
	Lync 2013 Client	Conferencing a call: When a Lync 2013 client is a participant in a conference call, an orphan conversation window (the call before the conference was established) will remain open after the call ends.	The conversation window must be manually closed. Note that when an orphan conversation window remains displayed after a call ends, new calls that are answered by the Lync 2013 client will automatically be placed on hold until the orphan window is closed.
	Lync 2013 Client	Transferring a call: When a Lync 2013 client is transferred to another party, the Lync 2013 client that was transferred (transferred party) will have	Terminate the call from the device. Note that when an orphan conversation window remains displayed after a call

ID	Minimum conditions	Visible symptoms	Workaround
		two conversation windows displayed after the transfer is completed. The transferred party will not be able to end the call using the Lync 2013 user interface. The call must be ended from the device. There are also issues when a Lync 2013 client is transferred to 'an existing conversation' and the (Lync 2013) transferred party is unable to end the call from the user interface.	ends, new calls that are answered by the Lync 2013 client will automatically be placed on hold until the orphan window is closed.
	Lync 2013 Client	Redirecting a call: The Lync clients allow the user to administer mobile, home and 'other' phone numbers. When a Lync client receives a call, the user may redirect the call to one of the administered numbers (in the 'Options' drop down in the alerting window). When a call is redirected to a destination that is a Lync client, the Lync client the call was redirected to will not be able to answer the call from the user interface; the call must be answered by using the device.	
		Microsoft Office Communicator (OC)	
	Microsoft Office Communicator (OC)	The Microsoft Office Communicator (OC) client will not re-establish phone integration automatically when the AE Services server is restarted This is a known issue in Office Communications Server (OCS) 2007 R2 which does not exist in Live Communications Server (LCS) 2005.	The first attempt to make a call from an active OC client after an AE Services restart will fail. Click the "retry" button to re-establish phone integration and to make the call. Call events will not be reported to an active OC client after an AE Services restart. To re-establish phone integration, sign-out of the OC client and then sign-in again.
	Microsoft Office Communicator (OC)	When using Microsoft as the Certificate Authorities (CA), Microsoft recommends using an Enterprise CA. The Enterprise CA template used to create the AE Services certificate must have the Enhanced Key Usage (EKU) field specified appropriately (Server and Client Auth or neither). The LCS/OCS AE Services integration uses Mutual TLS (MTLS) to authenticate server-to-server SIP communication. On an MTLS connection, the server originating a message and the server receiving it exchange certificates from a mutually trusted CA to prove the identity of each server to the other.	The server certificate used for MTLS on both servers must either not specify an EKU or specify an EKU for Server and Client Authorization. When the EKU is not specified the certificate is not restricted to a particular usage. However when the Key Usage field is specified and the EKU is specified as Server and Client Auth, the certificate can only be used by the server for mutual server and client based authentication purposes. If an EKU with only Server Auth is specified, in this scenario, the connecting server certificate will fail authentication and the MTLS connection will not be established.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum conditions	Visible symptoms	Workaround
			The Standalone CA, which may also be used (but is not Microsoft recommended), does not provide configurable templates including some additional features and must adhere to the same certificate generation rules in regards to the EKU field. Note: This statement doesn't preclude administrators from using non-Microsoft CAs (e.g. VeriSign).
		Single Step Transfer Call	
	Single Step Transfer Call	The Single Step Transfer Call service does not work reliably when transferring a call to a mobile device.	
		SIP	
	SIP	When using 3rd party call control to make a call using a Communication Manager TAC (Trunk Access Code), the call will fail on a SIP phone if the Communication Manager does not have a TN2602AP board. Note it is not common practice to use TAC dialing to access trunks.	The Automated Alternative Routing (AAR) and Automated Route Selection (ARS) routing features are recommended methods of accessing trunks.
	SIP	If Communication Manager does not have a TN2602AP board, the media encryption on the SIP endpoint should be disabled. The SIP endpoint transport type must be set to TCP or UDP. If the transport type is set to TLS, the 3rd party call control application may fail during transfer and conference. SIP endpoints (by default) will not respond to out of dialog (OOD) REFER messages from Communication Manager (ASAI third party call control and Communication Manager Call Center features) unless the transport mode is TLS.	There is a parameter in the endpoint configuration file that can be set to allow ASAI 3PCC on SIP endpoints with TCP.
	SIP	Avaya has observed intermittent problems with SIP endpoints in the 6.2 SP4 and prior releases particularly with scenarios that result in Computer Telephony Integration (CTI) requests that occur within a short time span of other CTI requests. It is currently not known when these issues will be completely addressed, but it is anticipated that future endpoint releases will address them fully. As an example, the Single Step Transfer Call service does not work reliably for SIP stations.	

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum conditions	Visible symptoms	Workaround
Telephony Services Application Programming Interface (TSAPI) Linux Client			
	Telephony Services Application Programming Interface (TSAPI) Linux Client	Before installing the TSAPI Linux client (i.e. tsapi-client-linux-7.0.0.rhel5-xxx or tsapi-sdk-linux-7.0.0.rhel5-xxx) on a Red Hat Linux ES v5.0 system, a separate installation of the following RPM may be required: openssl097a-0.9.7a-9.el5_4.2.i386.rpm.	This RPM may be available with your Red Hat Linux installation media, and is also available for download at http://rpm.pbone.net.
	Telephony Services Application Programming Interface (TSAPI) Linux Client	The TSAPI Linux client, installed on Red Hat Linux ES v5.0 system, may not be able to establish a secure connection to the TSAPI Service when using certificates with SHA2 (e.g., SHA256) signatures. Note: The TSAPI Linux client, installed on Red Hat Linux ES v6.5 system, will be able to establish a secure connection to the TSAPI Service running on AE Services 7.0 server when using certificates with SHA2 (e.g., SHA256) signatures.	Use certificates with SHA1 signatures instead
WebLM			
	WebLM	The WebLM session may hang.	Performing one of the following actions on WebLM may hang the session. a. Repeatedly uninstalling and installing licenses b. Repeatedly refreshing the licensing page The current session should be closed and a new session opened.
	WebLM	WebLM Enterprise Model – Using HTTPS: Run the following workaround if all three of the following conditions are true: a. The master WebLM Server, which hosts the Enterprise License File (ELF), is not co-located with another Avaya product such as AE Services or System Manager. b. The local WebLM servers are co-located with AE Services. HTTPS is in use for communication between the master and local WebLM servers (for example, to push an Allocation License File (ALF) to the local WebLM server on AE Services).	The Enterprise Web Licensing WebLM patch, “importCertToWebLm.zip”, is available on PLDS (ID = AES00000520). a. Download importCertToWebLm.zip files to the EWL master WebLM server. b. Unzip the file. c. Follow the directions in the README to install.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum conditions	Visible symptoms	Workaround
	WebLM	WebLM access may be denied in AE Services Software Only Servers. The WebLM server embedded in the AE Services software only server may not be accessible using port 443 when AE Services secure mode is enabled or if the AE Services Apache web server is configured to require a connecting client (browser or application) to provide a client identity certificate.	Either use port 8443 or a WebLM server external to the AE Services software only server.

Known issues and workarounds Application Enablement Services in Release 7.0.1

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

ID	Minimum conditions	Visible symptoms	Workaround
		AE Services Server	
N/A	AE Services Server	In AE Services 7.0.1, the Transport Layer Security (TLS) 1.2 protocol is enabled by default. This may cause older AE Services clients TLS to fail to connect.	To make a more secure connection, Avaya encourages current client applications to use newer (AE Services 7.0) SDKs where TLS 1.2 is supported. If upgrading to newer SDKs is not a viable option, the AE Services administrator can enable TLS1.1 or TSL1.0 protocols via the AE Services web management interface. Note that all three TLS protocol versions can be active at the same time. This will allow a gradual migration of current client applications to move towards a more secure TLS protocol over a period of time.
N/A	AE Services Server	The following log configuration files will not be restored in release 7.0.1 and going forward: 1. dmcc-logging.properties, 2. lcm-logging.properties, 3. hmdc logging properties and 4. tracemask As a result, if any debugging was enabled during the last backup, these files will not be restored. This was implemented for the following reasons: 1. Restoring a system will overwrite the current debug log. 2. Debug flags may change across	N/A

ID	Minimum conditions	Visible symptoms	Workaround
		releases. Debug flags are meant to be temporary and when enabled, they may impact system performance.	
AES-14658	AE Services Server SRTP Encryption	SRTP encryption used by DMCC softphones is different compared to the encryption configured and reported on Communication Manager. Even though SRTP is specified by the AE Server client application, AE Server sends the “AES” media encryption type to Communication Manager instead of SRTP.	Use “AES” media encryption instead of SRTP.
		Device, Media and Call Control (DMCC)	
AES-15077	DMCC Endpoint registration on Communication Manager release 7.0.1	DMCC endpoint registration request fails if “video softphone” is enabled on Communication Manager release 7.0.1.	Disable the “video softphone” flag on Communication Manager release 7.0.1 for the given extension (via “station” form).
		Device, Media and Call Control (DMCC)	
High Availability (HA)			
AES-14861	High Availability	If the Avaya Aura AE Services 7.0 Linux Security Update (LSU) Patch 1 is applied to an AE Services geo-redundant high availability (GRHA) system, the DBService will not come up and the following error is observed when an attempt is made to start the DBService: "GetDBProps.inc, Cannot find postgreSQL.cfg"	The workaround for is to remove GRHA before installing LSU Patch 1. Once the LSU Patch 1 is applied on both AE Services servers, then GRHA can be configured.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Avaya Aura® Utility Services

Installation for Avaya Aura® Utility Services Release 7.0.x.x

Required patches

Service Pack 1 for Utility Services 7.0:- 7.0.0.1.

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

Download ID	Patch	Notes
US000000056	Util_patch_7.0.0.1.0.12.zip	None.

Installation for Avaya Aura® Utility Services Release 7.0.1

Required patches

Feature Pack 1 for Utility Services 7.0:- 7.0.1.

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

Download ID	Patch	Notes
US000000059	Util_patch_7.0.1.0.0.12.zip	None.

Installation for Avaya Aura® Utility Services Release 7.0.1.1

Required patches

Service Pack 1 for Feature Pack 1 for Utility Services 7.0:- 7.0.1.1.

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

Download ID	Patch	Notes
US000000063	util_patch_7.0.1.1.0.01.zip	None.

Installation for Avaya Aura® Utility Services Release 7.0.1.2

Required patches

Service Pack 2 for Feature Pack 1 for Utility Services 7.0:- 7.0.1.2.

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

Download ID	Patch	Notes
US000000064	util_patch_7.0.1.2.0.03.zip	None.

Backing up the software

Refer to Chapter 6: Maintenance in the Deploying Avaya Aura® Utility Services in Virtualized Environment document for full details of the backup process.

Installing the release

Refer to Chapter 6: Maintenance in the Deploying Avaya Aura® Utility Services in Virtualized Environment document for full details of the updating patches and service pack process.

Troubleshooting the installation

Refer the Deploying Avaya Aura® Utility Services in Virtualized Environment document for any additional troubleshooting information

Restoring software to previous version

Refer to Chapter 6: Maintenance in the Deploying Avaya Aura® Utility Services in Virtualized Environment document for full details of the disaster recovery process.

What's new in Utility Services Release 7.0.x.x

What's new in Utility Services Release 7.0.0.0

Utility Services V7.0 offers the vast majority of features and capabilities as the previous release – V6.3 – with the following additions and exceptions:

- Utility Services supports both VMware Enablement (VE) and Avaya Appliance Virtualization Platform (AVP) Deployments. AVP replaces System Platform in Avaya Aura® 7.0.
- Utility Services must be deployed if AVP is being used as the Host. When Utility Services is deployed on AVP, it provides the following features:
    - AVP Alarming and Log Harvesting. Utility Services acts as a proxy for AVP in generating alarm messages. This means that Utility Services needs to be deployed with a valid System Manager IP Address and Enrollment Password for the registration process to complete successfully.
    - Services Port access to AVP and all deployed Virtual Machines. Avaya's System Platform supported an internal routing mechanism that allowed a Services Laptop connected to the System Platform server to be able to connect to any deployed virtual machine. Such a mechanism does not exist in AVP. So Utility Services now supports an internal routing capability that emulates the System Platform feature;
    - Enabling of SSH Access to AVP. Shell access to AVP is strictly controlled and enabled on a limited time window bases. Utility Services enables this feature.
- Based on CentOS V6.6 – the previous release was based on CentOS V5.
- IP Phone Firmware is now no longer included by default.
- Addition of the Auditor Role – this new role on the VMware version emulates the previous Auditor role on the System Platform release. This user is able to browse many features of Utility Services, but is prohibited from making any changes.
- Support for Utility Services specific Authentication File. The previous release of Utility Services supported a generic System Platform authentication file that could be installed on System Platform itself. Utility Services now supports its own authentication file.
- Utility Services now supports a Deployment Mode. Utility Services can be initially deployed in one of three modes – it is not possible to change mode after deployment:
    - Full Functionality. This mode supports all of the standard Utility Services features as well as the AVP Alarming and Log Harvesting, and the Services Port feature. This is also the default deployment mode.
    - Utility Services Only. This mode supports all of the standard Utility Services features, but AVP Alarming and Log Harvesting, and the Services Port feature are disabled. This is designed for deployment on non-AVP hardware and must not be used with AVP.
    - Services Port Only. This mode only supports AVP Alarming and Log Harvesting and the Services Port feature. All of the standard Utility Services features are disabled. This mode also has a minimal set of firewall rules.
- Addition of Out of Band Management (OOBM) Mode. Utility Services support OOBM to allow the Services Port Feature to access deployed Avaya Virtual Machines by either their Public or OOBM IP Address. The OOBM Mode

allows this element to be enabled to disabled – the default being disabled. AVP also supports OOBM and Utility Services Mode should match AVP – i.e. they should both be enabled or disabled.

What’s new in Utility Services Release 7.0.1

The following table lists enhancements in this release.

Enhancement	Description
170661-030	Utility Services VM supports deployment on ESXi6.0.
170661-060	Utility Services supports deployment on CSR3 Servers with AVP.
170661-065	Utility Services supports deployment on CallPilot 1006r server with AVP.
170661-150	Utility Services 7.0.1.0 supports a full out of band management configuration.

Fixes in Utility Services Release 7.0.x.x

Fixes in Utility Services Release 7.0.0.1

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release introduced
SDM-392	GA Deployment	Support for ESXi 6.0 Deployments	7.0.0.0
SDM-626	GA Deployment	Add support for RTSVersion Updates	7.0.0.0
UTILSERV-109	GA Deployment	Update XINETD Configuration for TFTPBOOT	7.0.0.0
UTILSERV-117	GA Deployment	Create New Pre-Upgrade Plug-In	7.0.0.0
UTILSERV-123	GA Deployment	Update to Copyright Year	7.0.0.0
UTILSERV-141	GA Deployment	Attempting to start the DHCP Service from the System Management Interface is not successful	7.0.0.0
SDM-508	Security Updates	Update to OpenJDK 1.8	7.0.0.0
SDM-622	Security Updates	Reduce User Privilege for Java Apps	7.0.0.0
SDM-617	Security Updates	Address Medium Security Notifications	7.0.0.0
UTILSERV-114	Security Updates	LOW: [RHSA-2015:1640-01] Moderate: pam security update	7.0.0.0
UTILSERV-115	Security Updates	LOW: [RHSA-2015:1668-01] Moderate: httpd security update	7.0.0.0
UTILSERV-118	Security Updates	LOW: [RHSA-2015:1699-01] Moderate: nss-softokn security update	7.0.0.0
UTILSERV-122	Security Updates	MEDIUM: [RHSA-2015:1705-01] Important: bind security update	7.0.0.0
UTILSERV-124	Security Updates	LOW: kernel security and bug fix update (RHSA-2015-1623)	7.0.0.0
UTILSERV-125	Security Updates	LOW: [RHSA-2015:1634-01] Moderate: sqlite security update	7.0.0.0
UTILSERV-129	Security Updates	MEDIUM: [RHSA-2015:1840-01] Important: OpenLDAP security update	7.0.0.0
UTILSERV-132	Security Updates	Fix permissions on authentication file	7.0.0.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release introduced
UTILSERV-133	Security Updates	MEDIUM: [RHSA-2015:1459-01] Moderate: ntp security, bug fix, and enhancement update	7.0.0.0
UTILSERV-134	Security Updates	MEDIUM: [RHSA-2015:1482-01] Important: libuser security update	7.0.0.0
UTILSERV-135	Security Updates	MEDIUM: [RHSA-2015:1330-01] Moderate: python security, bug fix, and enhancement update	7.0.0.0
UTILSERV-136	Security Updates	MEDIUM: [RHSA-2015:0863-01] Moderate: glibc security and bug fix update	7.0.0.0
UTILSERV-137	Security Updates	MEDIUM: [RHSA-2015:1081-01] Important: kernel security, bug fix, and enhancement update	7.0.0.0
UTILSERV-139	Security Updates	LOW: [RHSA-2015:1419-01] Low: libxml2 security and bug fix update	7.0.0.0

Fixes in Utility Services Release 7.0.1

The following table lists the fixes in this release over and above the fixes in Release 7.0.0.1.

ID	Minimum Conditions	Visible symptoms	Release introduced
SDM-305	GA Deployment	Implement OOBM for Utility Services	7.0.0.0
SDM-391	GA Deployment	CSR3 Support	7.0.0.0
SDM-392	GA Deployment	ESXi 6.0 Support	7.0.0.0
UTILSERV-190	GA Deployment	Callpilot 1006r Support	7.0.0.0
UTILSERV-117	GA Deployment	Create New Pre-Upgrade Plug-In	7.0.0.0
UTILSERV-119	GA Deployment	Automation of Removal of previous Service Packs when installing newer feature and service packs.	7.0.0.0
UTILSERV-208	GA Deployment	Patch Process does not appear to complete until you press a carriage return	7.0.0.1
UTILSERV-224	GA Deployment	SMGR IP doesn't get updated on Utility services /etc/hosts after NPC	7.0.0.0
UTILSERV-212	GA Deployment	AVP Utility Services SA needs default 'Alarm Throttling' parameter changed	7.0.0.0
UTILSERV-296	GA Deployment	Utility Server reverts to hostname localhost.localdomain after reboot	7.0.0.0
UTILSERV-320	GA Deployment	Network parameters change does not set properly in US	7.0.0.0
UTILSERV-81	Security Updates	Increased SSH algorithm and cipher strength.	7.0.0.0
UTILSERV-145	Security Updates	System password storage hardening	7.0.0.0

ID	Minimum Conditions	Visible symptoms	Release introduced
UTILSERV-154	Security Updates	MEDIUM: [RHSA-2015:1981-01] Critical: nss, nss-util, and nspr security update	7.0.0.0
UTILSERV-158	Security Updates	MEDIUM: [RHSA-2015:1930-01] Important: ntp security update	7.0.0.0
UTILSERV-161	Security Updates	LOW: [RHSA-2015:2081-01] Moderate: postgresql security update	7.0.0.0
UTILSERV-193	Security Updates	LOW: [RHSA-2015:2594-01] Moderate: libpng security update	7.0.0.0
UTILSERV-196	Security Updates	LOW: [RHSA-2015:2617-01] Moderate: openssl security update	7.0.0.0
UTILSERV-198	Security Updates	MEDIUM: [RHSA-2015:2636-01] Important: kernel security and bug fix update	7.0.0.0
UTILSERV-204	Security Updates	LOW: [RHSA-2015:2549-01] Moderate: libxml2 security update	7.0.0.0
UTILSERV-210	Security Updates	LOW: [RHSA-2016:0008-01] Moderate: openssl security update	7.0.0.0
UTILSERV-211	Security Updates	LOW: [RHSA-2016:0007-01] Moderate: nss security update	7.0.0.0
UTILSERV-245	Security Updates	MEDIUM: [RHSA-2016:0175-01] Critical: glibc security and bug fix update	7.0.0.0
UTILSERV-216	Security Updates	MEDIUM: [RHSA-2016:0050-01] Important: java-1.8.0-openjdk security update	7.0.0.0
UTILSERV-219	Security Updates	MEDIUM: [RHSA-2016:0063-01] Important: ntp security update	7.0.0.0
UTILSERV-223	Security Updates	LOW: [RHSA-2016:0073-01] Moderate: bind security update	7.0.0.0
UTILSERV-242	Security Updates	Security Scan - libXfont Update	7.0.0.0
UTILSERV-243	Security Updates	Security Scan - freetype Update	7.0.0.0
UTILSERV-251	Security Updates	LOW: Apache Tomcat Directory disclosure (CVE-2015-5345)	7.0.0.0
UTILSERV-254	Security Updates	MEDIUM: Apache Tomcat Limited Directory Traversal (CVE-2015-5174)	7.0.0.0
UTILSERV-256	Security Updates	LOW: Apache Tomcat Security Manager Bypass (CVE-2016-0714)	7.0.0.0
UTILSERV-258	Security Updates	MEDIUM: Apache Tomcat Security Manager bypass (CVE-2016-0706)	7.0.0.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release introduced
UTILSERV-263	Security Updates	MEDIUM: [RHSA-2016:0301-01] Important: openssl security update	7.0.0.0
UTILSERV-267	Security Updates	MEDIUM: [RHSA-2016:0347-01] Important: postgresql security update	7.0.0.0
UTILSERV-295	Security Updates	MEDIUM: [RHSA-2016:0370-01] Critical: nss-util security update	7.0.0.0
UTILSERV-305	Security Updates	LOW: [RHSA-2016:0466-01] Moderate: openssh security update	7.0.0.0
UTILSERV-307	Security Updates	LOW: [RHSA-2016:0493-01] Moderate: krb5 security update	7.0.0.0
UTILSERV-308	Security Updates	MEDIUM: [RHSA-2016:0494-01] Moderate: kernel security, bug fix, and enhancement update	7.0.0.0
UTILSERV-309	Security Updates	MEDIUM: [RHSA-2016:0459-01] Important: bind security update	7.0.0.0
UTILSERV-310	Security Updates	LOW: [RHSA-2016:0514-01] Important: java-1.8.0-openjdk security update	7.0.0.0

Fixes in Utility Services Release 7.0.1.1

The following table lists the fixes in Release 7.0.1.1. These fixes apply over and above the fixes in Release 7.0.1.0.

ID	Minimum Conditions	Visible symptoms	Release introduced
UTILSERV-323	Security Updates	MEDIUM: [RHSA-2016:0591-01] Moderate: nss, nss-util, and nspr security, bug fix, and enhancement update	7.0.0.0
UTILSERV-323	Security Updates	LOW:[RHSA-2016:0372-1] Important: openssl098e security update	7.0.0.0
UTILSERV-326	Security Updates	MEDIUM: [RHSA-2016:0651-01] Critical: java-1.8.0-openjdk security update	7.0.0.0
UTILSERV-340	Security Updates	MEDIUM: [RHSA-2016:0715-01] Moderate: kernel security, bug fix, and enhancement update	7.0.0.0
UTILSERV-341	Security Updates	MEDIUM: [RHSA-2016:0996-01] Important: openssl security update	7.0.0.0
UTILSERV-343	Security Updates	LOW: [RHSA-2016:0741-01] Moderate: openssh security, bug fix, and enhancement update	7.0.0.0
UTILSERV-344	Security Updates	LOW: [RHSA-2016:0855-01] Moderate: kernel security, bug fix, and enhancement update	7.0.0.0
UTILSERV-345	Security Updates	LOW: [RHSA-2016:0780-01] Moderate: ntp security and bug fix update	7.0.0.0
UTILSERV-346	Security	LOW: [RHSA-2016:0760-01] Moderate: file security, bug fix, and	7.0.0.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release introduced
	Updates	enhancement update	
UTILSERV-357	Security Updates	MEDIUM: [RHSA-2016:1141-01] Moderate: ntp security update	7.0.0.0

Fixes in Utility Services Release 7.0.1.2

The following table lists the fixes in Release 7.0.1.2. These fixes apply over and above the fixes in Release 7.0.1.1.

ID	Minimum Conditions	Visible symptoms	Release introduced
UTILSERV-376	Security Updates	MEDIUM: [RHSA-2016:1406-01] Important: kernel security and bug fix update.	7.0.0.0
UTILSERV-399	Security Updates	LOW: [RHSA-2016:1664-01] Important: kernel security and bug fix update.	7.0.0.0
UTILSERV-413	Security Updates	LOW: [RHSA-2016:2006-01] Important: kernel security and bug fix update.	7.0.0.0
UTILSERV-367	Security Updates	PSST: update php packages per RHSA-2015-1218.	7.0.0.0
UTILSERV-391	Security Updates	LOW: [RHSA-2016:1609-01] Moderate: php security update.	7.0.0.0
UTILSERV-378	Security Updates	LOW: [RHSA-2016:1421-01] Important: httpd security update.	7.0.0.0
UTILSERV-389	Security Updates	LOW: [RHSA-2016:1421-01] Important: httpd security update.	7.0.0.0
UTILSERV-371	Security Updates	MEDIUM: [RHSA-2016:1292-01] Important: libxml2 security update.	7.0.0.0
UTILSERV-390	Security Updates	LOW: [RHSA-2016:1458-01] Critical: java-1.8.0-openjdk security update.	7.0.0.0
UTILSERV-392	Security Updates	LOW: [RHSA-2016:1626-01] Moderate: python security update.	7.0.0.0
UTILSERV-397	GA Deployment	Settings Editor Fails with Permissions Issue.	7.0.0.0
UTILSERV-408	Security Updates	HIGH Priority: [RHSA-2016:1940-01] Important: openssl security update.	7.0.0.0
UTILSERV-409	Security Updates	LOW: [RHSA-2016:1944-01] Important: bind security update.	7.0.0.0
UTILSERV-412	GA Deployment	Fix Permissions Issues on remote.log file.	7.0.0.0
UTILSERV-417	Security Updates	Ensure Tomcat Examples and Docs Folders are Removed.	7.0.0.0

ID	Minimum Conditions	Visible symptoms	Release introduced
UTILSERV-419	Security Updates	LOW: [RHSA-2016:2093-01] Important: bind security update.	7.0.0.0
UTILSERV-420	Security Updates	LOW: [RHSA-2016:2079-01] Critical: java-1.8.0-openjdk security update.	7.0.0.0
UTILSERV-422	Security Updates	LOW: [RHSA-2016:2099-01] Important: bind security update.	7.0.0.0

Known issues and workarounds in Utility Services Release 7.0.x.x

Known issues and workarounds in Utility Services Release 7.0.0.0

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

ID	Minimum conditions	Visible symptoms	Workaround
		Firefox cannot access the MyPhone and MyPhoneAdmin web pages	Firefox has support for some weak ciphers enabled, although it will prohibit access to web sites with these ciphers. It is however, easy to remove support for these weak ciphers as detailed below: Open a new Firefox session with “about:config” – there is a warning that this is not recommended unless you know exactly what you are doing. Scroll down to the entries labelled “security.ssl3.dhe_rsa_aes_128.sha” and “security.ssl3.dhe_rsa_aes_256.sha”. Both entries will have a default of “true” – change both to “false” by double clicking the entry. The entry will be bold if it has changed from the default. The effect is immediate and does not require the browser to be restarted.
UTILSERV-45		Internet Explorer 9 cannot access the Utility Services Web Pages	Update the security configuration in advanced options of the browser to DISABLE SSL and ENABLE TLS support. Note that later versions of Microsoft® Internet Explorer do not need to be modified.
		Firefox 39 does not support uploading of large files to Utility Services.	The exact failure here is still a mystery, but this late release of Firefox seems to have problems with files for more than about 100MB. The recommended workaround is to use Internet Explorer.
		Utility Services currently only supports a single NTP server, although the dialogue box appears to support multiple IP Addresses.	There is no workaround at this time.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum conditions	Visible symptoms	Workaround
		Utility Services supports multiple DNS Server IP Addresses, but these should be separate by a space rather than a comma.	The dialogue box for DNS Server IP Addresses states that multiple values should be separated by a comma. This does not work correctly, so use a space instead.
UTILSERV-88		Utility Services has an absolute maximum file size of around 800MB for file uploads. This can cause a problem when trying to restore a very large backup file.	If possible, select “exclude firmware” when generating a backup file. This greatly speeds up the process and will generate a much smaller backup file. If this is not possible, then a large backup file can be manually restored as follows: Firstly, the backup file needs to be transferred to the /tmp directory - this can be achieved using something like WinSCP with the administrative credentials. Secondly, open a secure shell session to Utility Services using the administrative credentials. Now type "/opt/avaya/common_services/backup –r <filename>. Note that the path should NOT be specified for the filename.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

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

Avaya Aura Appliance Virtualization Platform 7.0.1	File name	PLDS File ID	PCN/PSN
AVP 7.0.1.0.0.5	avaya-avp-7.0.1.0.0.5.zip	AVP00000008	Not applicable.

VMware vSphere (for VE installations)	File name	PLDS File ID	PCN/PSN
ESXi 5.0, 5.1, 5.5, or 6.0	Not applicable.	Not applicable.	Not applicable.

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.x Kernel Service Pack	KERNEL-2.6.32-573.18.1.el6.AV2.tar	CMM70000007	PCN2028S
Avaya Aura® Communication Manager 7.0.x Security Service Pack 2	PLAT-rhel6.5-0030.tar	CM000000627	PCN2008Su
Avaya Aura® Communication Manager 7.0.1 Service Pack 0	00.0.441.0-23012.tar	CMM70000009	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

What’s new in Communication Manager Messaging 7.0.0.1

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 subsequent to 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	Minimum Conditions	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 logfiles	
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.	

ID	Minimum Conditions	Visible symptoms	Release found in
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	
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 take into account 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	

ID	Minimum Conditions	Visible symptoms	Release found in
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	
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.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Avaya Appliance Virtualization Platform

Installation for Avaya Appliance Virtualization Platform Release 7.0.x.x

Appliance Virtualization Platform (AVP) service pack 7.0.1.2 will be released at a later date. Until that time, please use the AVP 7.0.1 GA Feature Pack.

Required patches

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

Download ID	Patch	Notes
AVP00000008	Avaya Appliance Virtualization Platform 7.0.1 Feature Pack	
AVP00000006	Avaya Appliance Virtualization Platform 7.0 Kick Start Generator	Use this Kick Start generator for new AVP 7.0 installations.
AVP00000009	Avaya Appliance Virtualization Platform 7.0.0.0 rollback bundle	Use this bundle to roll back to AVP 7.0.0.0 after installing AVP 7.0.1. See "Restoring software to previous version from AVP Release 7.0.1" section below.

File list

Filename	Modification time stamp	File size	Version number
avaya-avp-7.0.1.0.0.5.zip	4/25/2016 9:24:08 AM	384,299,358 bytes	7.0.1.0.0.5
AVP-installation-file-generator-V1-7c.xlsm	12/14/2015 4:29:33 PM	98,304 bytes	V1-7c
avaya-avp-7.0.0.0.0.21.iso	4/25/2016 3:31:59 PM	366,252,610 bytes	7.0.0.0.0.21

Installing the release

This release is an upgrade bundle to be applied onto an existing AVP 7.0.0.0 or later installation. It will not be necessary to reinstall guest VMs.

This AVP Service Pack can be applied using the Avaya Aura® System Manager Solution Deployment Manager or the Avaya Aura® Solution Deployment Manager Client.

- Stop all guest VMs
- Select the AVP host from the **Hosts** tab of the **VM Management** page
- Click the **Update** button
- Enter the full path name to the Service Pack file or Feature Pack file
- Click the **Update Host** button
- See System Manager documentation for more details

Alternatively, this AVP Service Pack can be installed from the AVP ESXi Command Line:

- Copy the file to the local data store on the AVP host /vmfs/volumes/server-local-disk

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

- Using Solution Deployment Manager, stop all running Virtual Machines before placing the host in maintenance mode
- From a root prompt enter:

  ```
  vim-cmd hostsvc/maintenance_mode_enter
  esxcli software vib install -d /vmfs/volumes/server-local-disk/avaya-avp-7.0.1.0.0.5.zip --no-sig-check -f
  reboot
  ```
- After reboot enter:

  ```
  vim-cmd hostsvc/maintenance_mode_exit
  /sbin/vmware-autostart.sh start
  ```
- Restart guest Virtual Machines
- Verify the AVP software release and ESXi version

Restoring software to previous version from AVP Release 7.0.1

Download the AVP 7.0.0.1 patch or the AVP 7.0.0.0 rollback bundle from PLDS.

Copy the above AVP 7.0.0.1 patch or the AVP 7.0.0.0 rollback bundle to /vmfs/volumes/server-local-disk

Before restoring software to the previous version, make sure all Virtual Machines on this host are gracefully shut down. Run the following commands:

```
/opt/avaya/bin/rollback_bootbank.sh /vmfs/volumes/server-local-disk/<patch or rollback bundle name>
/opt/avaya/bin/avpshutdown.sh -r
```

After a rollback and subsequent reboot, be sure the system is not in maintenance mode and all VMs have started. If necessary, maintenance mode can be disabled and VMs started by running the following commands:

```
esxcli system maintenanceMode set --enable false
/sbin/vmware-autostart.sh start
```

Restoring software to previous version from AVP Release 7.0.0.1

Before restoring software to the previous version, make sure all Virtual Machines on this host are gracefully shut down. Run the following commands:

```
/opt/avaya/bin/rollback_bootbank.sh
/opt/avaya/bin/avpshutdown.sh -r
```

After a rollback and subsequent reboot, be sure the system is not in maintenance mode and all VMs have started. If necessary, maintenance mode can be disabled and VMs started by running the following commands:

```
esxcli system maintenanceMode set --enable false
/sbin/vmware-autostart.sh start
```

Fixes in Avaya Appliance Virtualization Platform Release 7.0.x.x

Fixes in Avaya Appliance Virtualization Platform 7.0.0.1

The following table lists the fixes in this release.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release introduced
AVP-192	Avaya Aura® Utility Services 7.0 hostname and IP address is not correctly entered in the customer's DNS and Utility Services reboots	If Avaya Aura® Utility Services 7.0 IP address and hostname is not correctly entered in the customer's DNS and Utility Services reboots, Avaya Appliance Virtualization Platform (AVP) alarming will fail.	US 7.0
AVP-223	Initial installation of AVP 7.0 on a server with 64 GB or more of memory	The first boot script does not complete after installation of Avaya Appliance Virtualization Platform 7.0 on a server with 64 GB or more of memory.	AVP-installation-file-generator-V1-7.xlsm
AVP-236	Avaya Appliance Virtualization Platform 7.0	Avaya Appliance Virtualization Platform had certain vulnerabilities described in the following Avaya Security Advisory. To see the document, go to http://support.avaya.com and search for the ASA number. • ASA-2015-443 (VMware vCenter and ESXi updates address critical security issues VMSA-2015-0007)	AVP 7.0

Fixes in Avaya Appliance Virtualization Platform 7.0.1

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release introduced
AVP-189	Avaya Appliance Virtualization Platform 7.0 or 7.0.0.1	Under rare conditions, the End User License Agreement (EULA) acceptance prompt is not shown during the Avaya Appliance Virtualization Platform (AVP) 7.0 installation. Avaya Aura® System Manager Solution Deployment Manager will show that the AVP is not licensed.	AVP 7.0
AVP-340	Avaya Appliance Virtualization Platform 7.0 or 7.0.0.1	Avaya Aura® Appliance Virtualization Platform had certain vulnerabilities described in the following Avaya Security Advisory. To see the document, go to http://support.avaya.com and search for the ASA number. • ASA-2016-087 VMware product updates address a critical glibc security vulnerability (VMSA-2016-0002)	AVP 7.0

Known issues and workarounds in Avaya Appliance Virtualization Platform Release 7.0.x.x

Known issues and workarounds in Avaya Appliance Virtualization Platform 7.0.0.0

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

ID	Minimum conditions	Visible symptoms	Workaround

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum conditions	Visible symptoms	Workaround
AVP-157	Initial installation of Avaya Appliance Virtualization Platform 7.0	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-163	Avaya Appliance Virtualization Platform 7.0 on Avaya S8300D server	On an Avaya S8300D server, the OK TO REMOVE LED does not turn on after issuing Shutdown Server if the server has gone through a soft reboot.	After issuing a Shutdown Server or pressing the SHUTDOWN button, wait about 5 minutes and try pinging AVP IP address from a network connected PC. The S8300 server can be pulled out from the Media Gateway, or powered off when it no longer responds to the pings.
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 by logging into the AVP via an SSH client. If virtual machine deployments are

ID	Minimum conditions	Visible symptoms	Workaround
			attempted prior to accepting the EULA, 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 Utility Services VM.
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 a Utility Services VM with AVP. Utility Services provides key alarming and security functions to the AVP host and is mandatory to deploy.

Known issues and workarounds in Avaya Appliance Virtualization Platform 7.0.0.1

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 Appliance Virtualization Platform 7.0	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.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum conditions	Visible symptoms	Workaround
AVP-163	Avaya Appliance Virtualization Platform 7.0 on Avaya S8300D server	On an Avaya S8300D server, the OK TO REMOVE LED does not turn on after issuing Shutdown Server if the server has gone through a soft reboot.	After issuing a Shutdown Server or pressing the SHUTDOWN button, wait about 5 minutes and try pinging AVP IP address from a network connected PC. The S8300 server can be pulled out from the Media Gateway, or powered off when it no longer responds to the pings.
AVP-189	Avaya Appliance Virtualization Platform 7.0	Under rare conditions, the End User License Agreement (EULA) acceptance prompt is not shown during the Avaya Appliance Virtualization Platform (AVP) 7.0 installation. Avaya Aura® System Manager Solution Deployment Manager will show that the AVP is not licensed.	Log in to the AVP host via SSH and run the command /opt/avaya/bin/show_eula.sh
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 by logging into the AVP via an SSH client. If virtual machine deployments are attempted prior to accepting the EULA, 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 Utility Services VM.
General issues			If the system is to be set with Out of Band Management, the AVP host should be

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum conditions	Visible symptoms	Workaround
and workarounds			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 a Utility Services VM with AVP. Utility Services provides key alarming and security functions to the AVP host and is mandatory to deploy.

Known issues and workarounds in Avaya Appliance Virtualization Platform 7.0.1

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 Appliance Virtualization Platform 7.0	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-346	Avaya Appliance Virtualization Platform on Avaya S8300D server	Performing a server shutdown on the Avaya S8300D causes the server to shut down for a brief period of time, and then restart and applications come back online.	Enable ssh to the AVP. Log in to the AVP via ssh and issue the following command before powering down the media gateway or removing the S8300D server from the media gateway: esxcli system maintenanceMode set -e true

ID	Minimum conditions	Visible symptoms	Workaround
AVP-347	Avaya Appliance Virtualization Platform on Dell R630 server	The MegaCLI maintenance commands to query the Dell R630 servers for RAID and disk status do not work.	
AVP-389	Avaya Appliance Virtualization Platform on any Avaya common server.	Server hardware alarms, such as power supply or disk alarms may be delayed by up to 3 hrs.	
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 by logging into the AVP via an SSH client. If virtual machine deployments are attempted prior to accepting the EULA, 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 Utility Services VM.
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

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum conditions	Visible symptoms	Workaround
			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 a Utility Services VM with AVP. Utility Services provides key alarming and security functions to the AVP host and is mandatory to deploy.
General issues and workarounds			Out of Band Management setting should only be used if required. If you do not have a separate management network and IP address range do not activate this setting on AVP.

Languages supported

Languages supported in this release:

- *English*

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Avaya Aura® G430 & G450 Media Gateways

Installation for Avaya Aura® G430 & G450 Media Gateways Release 7.0.x.x

Required patches

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

Note: 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.

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 of 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 version 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

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 as long as 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 particular 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.

Installing the release

Pre Install Instructions

-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

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

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

File Download Instructions

Before attempting a download, read the section in the Installation documentation titled "Upgrading / Downloading Software / Firmware".

What's new in Avaya Aura® G430 & G450 Media Gateways Release 7.0.x.x

What's new in G430 & G450 Media Gateways Release 7.0.0.0, Build 37.19.0

The following table lists enhancements in this release:

Enhancement	Description
hw140170	G430, G450 AES-256 media encryption support for voice, data, video. AES-256 is managed in the "Media Encryption" field of Communication Manager's ip-codec-set form.
CMG4xx-234	G430, G450 Encrypted SRTCP bearer control channel support. Encrypted SRTCP is managed in the "Encrypted SRTCP" field of the Communication Manager's ip-codec-set form.
CMG4xx-304	G430, G450 Online Certificate Status Protocol (OCSP) support has been added as an alternative certificate validation technique to Certificate Revocation Lists (CRLs). The following certificate-option commands have been added to support X.509 Certificate validation using OCSP: set ocsp-validation [yes | no] - Enables or disabled OSCP certificate validation. set ocsp-local-url [url] - Sets the URL to be used when validating a certificate using OCSP (default is no url). set ocsp-url-precedence [certificate | local] - Sets whether the certificate URL or the local URL should be used first whenever a certificate is validated using OCSP (default is certificate). Also, the "show certificate-options" command has been updated to display the setting of the above OCSP options.
CMG4xx-265	G430, G450 Greenwich Mean Time (GMT) Timezone offset awareness added to provide greater accuracy when validating certificate expiration.
hw140178	G430, G450 SHA-2 signed certificates supported for firmware images downloaded to the gateway.
CMG4xx-251	G430, G450 Out Of Band Management Interface support added for VLAN and Fast-ethernet. OOB management includes the addition of the following new CLI commands: oob-interface - Configures the interface as an Out of Band Management interface. no oob-interface - Removes the out-of band management interface. show oob-interface - Displays the out-of-band management interface. set non-oob access <disable|enable> - Disables and enables management access to the in-band network connection. Also, the "show interface" command has been updated to include information for OOB for VLAN and Fast-ethernet.
hw140126	G430, G450 Gateway login password policy has been enhanced. The date and time of the last login and the number of login failures is now displayed on the console every time a user logs onto the gateway. In addition, the following new CLI commands have been added: login authentication password-no-change-interval <hours> - set the number of hours before a password can be changed again (default 24). login authentication passwords-don't-reuse command <n-passwords> - set the number of

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Enhancement	Description
	previous passwords that cannot be reused (default 1).
CMG4xx-338	G430, G450 TLS upgraded to include support of TLS version 1.2. SSLv2 andSSLv3 are no longer supported.
CMG4xx-233	G430, G450 OpenSSL upgraded to version 1.0.1L

What’s new in G430 & G450 Media Gateways Release 7.0.0.2, Build 37.21.30 (Russia only)

The following table lists enhancements in this release:

Enhancement	Description
CMG4xx-430	G430, G450 A separate firmware build with VPN disabled was created (Build 37.21.30 – for Russia only).

What’s new in G430 & G450 Media Gateways Release 7.0.1.0, Build 37.38.0

Enhancement	Description
	Two new CLI Commands are introduced: - set allow-unencrypted: System administrator can use this command to allow or disallow media encryption requests from Communication Manager. - set link-encryption: System administrator can use this command to specify what TLS versions will be offered by the gateway when connecting to a server.
	OPUS Codec - The MP120 and MP160 VOIP modules are now capable of supporting the Opus codec in narrowband mode.
	FIPS-mode support - FIPS-mode is a feature that is currently not supported in Release 7.0.1 for use by our customers since it is pending FIPS certification by a 3rd-party at this time. It is targeted to be available in a post 7.0.1 release after achieving FIPS certification.

What’s new in G430 & G450 Media Gateways Release 7.0.1.0, Build 37.38.30 (Russia only)

Enhancement	Description
New CLI commands	Two new CLI Commands are introduced: - set allow-unencrypted: System administrator can use this command to allow or disallow media encryption requests from Communication Manager. - set link-encryption: System administrator can use this command to specify what TLS versions will be offered by the gateway when connecting to a server.
OPUS Codec support	OPUS Codec - The MP120 and MP160 VOIP modules are now capable of supporting the Opus codec in narrowband mode.
FIPS-mode support	FIPS-mode support - FIPS-mode is a feature that is currently not supported in Release 7.0.1 since it is pending FIPS certification by a 3rd-party at this time. FIPS-mode is not intended for use by our

Enhancement	Description
	customers in Russia nor will it provide any additional encryption capabilities.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Fixes in Avaya Aura® G430 & G450 Media Gateways Release 7.0.x.x

Fixes in G430 & G450 Media Gateways 7.0.0.0, Build 37.19.0

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
		G430, G450 The "set fips enabled" CLI command is not supported in this release.	
		G430 Show voip-parameters" and "show voip-dsp" do not display the following warning when registered to SLS: Note: The gateway is registered with a Communication Manager version which limits DSP resources to 120 channels.	
		G450 Show voip-parameters" and "show voip-dsp" do not display the following warning when registered to SLS: "Note: The gateway is registered with a Communication Manager version which limits DSP resources to 240 channels.	

Fixes in G430 & G450 Media Gateways 7.0.0.1, Build 37.20.0

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release found in
PSN020223u		G430, G450 Media Gateways that were running firmware prior to the release of 36.9.0 and then were upgraded (36.9.0 to 36.15.0 or 37.19.0) can experience minor corruption. Such corruption causes a failure when attempting to download TLS certificates or can prompt the media gateway to restart. Media Gateways shipped from the factory that have 36.9.0 firmware or higher preinstalled are not affected. Media Gateways that have had a NVRAM INIT reset performed while running 36.9.0 or higher firmware are also not affected.	7.0.0.0

Fixes in G430 & G450 Media Gateways 7.0.0.2, Builds 37.21.0 and 37.21.30 (Russia Only)

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
CMG4xx-428	G450 with MM340 installed	G450 G450 Media Gateway with MM 340 installed reboots whenever the “show controllers” CLI command is invoked.	6.3.5

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
CMG4xx-429	Use of EmWeb Application	G430, G450 The following error is generated whenever the Trap Manager Table is accessed using the EmWeb application: "(1.3.6.1.2.1.10.32.4.1.0: null) SNMP Error: No Such Name"	6.3.0
CMG4xx-435		G430, G450 SRTCP packets will be discarded whenever a G450/G430 Media Gateway interacts with a product other than a G450/G430 Media Gateway.	7.0.0.0
CMG4xx-450		G430, G450 In-band digits from a SIP trunk are sometimes not detected by the gateway's tone detectors.	6.3.0
CMG4xx-464		G430, G450 Using and MP-80 or MP-20 with AES256 and Fax or Modem traffic can lead to a DSP core going out of service, thereby reducing the number of available VoIP channels	7.0.0.0

Fixes in G430 & G450 Media Gateways 7.0.1.1, Build 37.39.0, Build 37.39.30 (Russia Only)

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
CMG4xx-474, CMG4xx-622	Overloaded Call Traffic condition using Announcements	G430, G450 Fixed a very rare condition where the system would reset when an announcement is to be applied but no timeslots and/or DSP channels are available.	6.3.13
CMG4xx-625	Interchange on a PEDup Server configured with Dual IP Stack	G430, G450 An interchange on a PEDup server using Dual IP stacks (i.e. both IPv4 and IPv6) take takes longer than usual to reregister (approximately 7 seconds). In addition, entries were continuously and very frequently logged in the event log after the interchange occurred.	7.0.1
CMG4xx-639	MP-160 or MP-120 DSPs	G430, G450 Receipt of a Flash telephony event within an RFC2833 packet could cause an MP-160 or MP-120 DSP Core to go out of service. This problem does not occur in the MP-80, MP-25, and MP-10 DSPs.	6.3.12
CMG4xx-646	MP-160 or MP-120 DSPs	G430, G450 Additional diagnostic information is collected in the event that an MP-160 or MP-120 DSP core goes out of service.	6.3.14
CMG4xx-652	MP-160 or MP-120 DSPs	G430, G450 Additional diagnostic information is collected in the event that SRTP authentication fails on a received RTP packet.	6.3.1

Fixes in G430 & G450 Media Gateways 7.0.1.2, Build 37.41.0, Build 37.41.30 (Russia Only)

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
CMG4xx-695	OOB Interface	G430, G450 Unable to ping the Out of Band interface within the same subnet when the next hop gateway is defined in a static route that includes that subnet is unreachable.	7.0.1.0
CMG4xx-722	All DSPs	G430, G450 DSP made more tolerant of RTCP encryption mismatches and/or malformed data that could otherwise result in DSP core failures.	6.3.12
CMG4xx-699	PE-Dup Server configured with Dual IP Stack	G430, G450 In a PE-Dup environment that is configured to use both IPv4 and IPv6, the gateway would not always switch to the alternate IP version when re-registering with CM. This would only occur if "set link-encryption h248reg unencrypted yes" is set on the gateway and CM link-encryption is set to "any", "tls-only" or "ptls-only".	7.0.1.0
CMG4xx-736	PE-Dup Server	G430, G450 In a PE-Dup environment, a customer's gateways experienced a reset during an upgrade to Release 37.39.10.	7.0.1.0
CMG4xx-667	Spanning Tree disabled	G450 Spanning tree BPDU frames were briefly being sent out during G450 startup even when spanning-tree was disabled.	7.0.1.0

Known issues and workarounds in Avaya Aura® G430 & G450 Media Gateways Release 7.0.x.x

Known issues and workarounds in G430 & G450 Media Gateways Releases 7.0.0.1, 7.0.0.2, 7.0.1.0, 7.0.1.1, and 7.0.1.2 Builds 37.19.0 thru 37.41.0 Builds 37.21.30, 37.38.30, 37.39.30, and 37.41.30 (Russia Only)

The following table lists the known issues, symptoms, and workarounds in these releases:

ID	Minimum conditions	Visible symptoms	Workaround
None		G430, G450 This Branch Gateway version doesn't 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.

Avaya Aura® Media Server

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

The Avaya Aura® Media Server delivers advanced multimedia processing features to a broad range of products and applications. Utilizing the latest open standards for media control and media processing, the highly scalable software based solution deploys on standard server hardware. It is comprised of the following components:

- Media Server Software
- System Layer (appliance only).

Installation for Avaya Aura® Media Server Release 7.7.x.x

Required patches

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

Download ID	Patch	Notes
N/A		

File list for Media Server Release 7.7.0.236 SP1

Filename	File size	Version Number	Notes
MediaServer_Update_7.7.0.236_2015.07.24.iso	335,650,816	7.7.0.236	Appliance installs.
MediaServer_7.7.0.236_2015.07.24.bin	335,273,825	7.7.0.236	Non-appliance installs

File list for System Layer 7.7.0.11 SP1 (Appliance Only)

Filename	File size	Version Number	Notes
MediaServer_System_Update_7.7.0.11_2015.07.13.iso	498,702,336	7.7.0.11	Appliance installs.

File list for Media Server Release 7.7.0.281 SP2

Filename	File size	Version Number	Notes
MediaServer_Update_7.7.0.281_2015.11.20.iso	337,838,080	7.7.0.281	Appliance installs.
MediaServer_7.7.0.281_2015.11.20.bin	337,458,257	7.7.0.281	Non-appliance installs

File list for System Layer 7.7.0.14 SP2 (Appliance Only)

Filename	File size	Version number	Notes
MediaServer_System_Update_7.7.0.14_2015.10.26.iso	498,595,840	7.7.0.14	Appliance installs.

File list for Media Server Release 7.7.0.292 SP3

Filename	File size	Version Number	Notes
MediaServer_Update_7.7.0.292_2015.12.25.iso	337,833,984	7.7.0.292	Appliance installs.
MediaServer_7.7.0.292_2015.12.25.bin	337,453,745	7.7.0.292	Non-appliance installs

File list for System Layer 7.7.0.15 SP3 (Appliance Only)

Filename	File size	Version number	Notes
MediaServer_System_Update_7.7.0.15_2015.12.14.iso	498,597,888	7.7.0.15	Appliance installs.

File list for Media Server Release 7.7.0.334 FP1

Filename	File size	Version Number	Notes
MediaServer_Update_7.7.0.334_2016.04.13.iso	339,099,648	7.7.0.324	Appliance installs.
MediaServer_7.7.0.334_2016.04.13.bin	338,715,489	7.7.0.324	Non-appliance installs

File list for System Layer 7.7.0.19 FP1 (Appliance Only)

Filename	File size	Version number	Notes
MediaServer_System_Update_7.7.0.19_2016.04.07.iso	504,066,048	7.7.0.19	Appliance installs.

File list for Media Server Release 7.7.0.359 FP1 SP1

Filename	File size	Version Number	Notes
MediaServer_Update_7.7.0.359_2016.07.20.iso	339,634,176	7.7.0.359	Appliance installs
MediaServer_7.7.0. 359_2016.07.20.bin	339,250,587	7.7.0.359	Non-appliance installs

File list for System Layer 7.7.0.20 FP1 SP1 (Appliance Only)

Filename	File size	Version number	Notes
MediaServer_System_Update_7.7.0.20_2016.06.22.iso	504,066,048	7.7.0.20	Appliance installs.

File list for Media Server Release 7.7.0.375 FP1 SP2

Filename	File size	Version Number	Notes
MediaServer_Update_7.7.0.375_2016.11.10.iso	325,824,512	7.7.0.375	Appliance installs
MediaServer_7.7.0.375_2016.11.10.bin	325,439,404	7.7.0.375	Non-appliance installs

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

File list for System Layer 7.7.0.21 FP1 SP2 (Appliance Only)

Filename	File size	Version number	Notes
MediaServer_System_Update_7.7.0.21_2016.11.03.iso	135,233,536	7.7.0.21	Appliance installs.

Backing up the software

For appliance installations, refer to procedures documented in *Deploying and Updating Avaya Aura® Media Server Appliance FP1.*

https://downloads.avaya.com/css/P8/documents/101013582

For non-appliance installations, refer to procedures documented in *Implementing and Administering Avaya Aura® Media Server.*

https://downloads.avaya.com/css/P8/documents/101013586

Installing the release

For appliance installations, refer to procedures documented in *Deploying and Updating Avaya Aura® Media Server Appliance FP1*.

https://downloads.avaya.com/css/P8/documents/101023789

For non-appliance installations, refer to procedures documented in *Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS.*

https://downloads.avaya.com/css/P8/documents/101013584

When upgrading from Avaya Aura® Media Server 7.7 Feature Pack 1 (Media Server 7.7.0.334 and System Layer 7.7.0.19) to a more recent 7.7 version use the new, easier to use software update procedure from the Avaya Aura® MS Element Manager console. See Deploying and Updating Avaya Aura® Media Server Appliance FP1 for the new update procedure. See *Deploying and Updating Avaya Aura® Media Server Appliance* FP1 for the new update procedure.

When upgrading from versions prior to 7.7 Feature Pack 1 note the following:

- The procedures for upgrading have changed to accommodate the transition to a simplified one button update. See Updating to FP1 in *Deploying and Updating Avaya Aura® Media Server Appliance* FP1 for the detailed transition procedure. The transition procedure to FP1 is summarized as follows:
  - Upload both 7.7 Feature Pack 1 updates (Media Server and System Layer) before executing any further commands.
  - A new command "installUpdate" will be available after the system layer update is uploaded. Previous CLI commands used to update the media server are deprecated and will refer to this command if they are run.
  - Open a new Linux® shell or simply login to a new SSH session and execute the installUpdate command to perform the upgrade. The system reports the installUpdate command as not found if a new Linux® shell is not used.
  - After the upgrade completes, Avaya Aura® Media Server provides a new, easier to use software update procedure using the Avaya Aura® MS Element Manager. See *Deploying and Updating Avaya Aura® Media Server Appliance* FP1 for the new update procedure.
- SHOUTcast and RSS configuration will be removed during the upgrade process. If these music streaming features are utilized, you must configure them again using the new music streaming provisioning interface available on the Avaya Aura® MS Element Manager.
- TLSv1.2 is enabled by default for most interfaces.

- When connecting to AAMS Element Manager ensure that the web browser has TLSv1.2 enabled.
- Ensure any other endpoints that communicate with AAMS using protocols like SIP TLS have TLSv1.2 support enabled.

Troubleshooting the installation

For appliance installations, refer to procedures documented in *Deploying and Updating Avaya Aura® Media Server Appliance FP1.*

https://downloads.avaya.com/css/P8/documents/101023789

For non-appliance installations, refer to procedures documented in *Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS.*

https://downloads.avaya.com/css/P8/documents/101013584

Restoring software to previous version

For appliance installations refer to procedures documented in *Deploying and Updating Avaya Aura® Media Server Appliance FP1.*

https://downloads.avaya.com/css/P8/documents/101023789

For non-appliance installs refer to procedures documented in Implementing and Administering Avaya Aura® Media Server.

https://downloads.avaya.com/css/P8/documents/101013586

What's new in Avaya Aura® Media Server Release 7.7.x.x

What's new in Media Server Release 7.7.0.236 (SP1)

The following table lists enhancements in this release.

Enhancement	Description
N/A	

What’s new in System Layer Release 7.7.0.11 (SP1)

The following table lists enhancements in this release.

Enhancement	Description
N/A	

What’s new in Media Server Release 7.7.0.281 (SP2)

The following table lists enhancements in this release.

Enhancement	Description
N/A	

What’s new in System Layer Release 7.7.0.14 (SP2)

The following table lists enhancements in this release.

Enhancement	Description
N/A	

What’s new in Media Server Release 7.7.0.292 (SP3)

The following table lists enhancements in this release.

Enhancement	Description
N/A	

What’s new in System Layer Release 7.7.0.15 (SP3)

The following table lists enhancements in this release.

Enhancement	Description
N/A	

What’s new in Media Server Release 7.7.0.334 (FP1)

The following table lists enhancements in this release.

Enhancement	Description
AMS-2230	Enable TLSv1.2 as default protocol for all TLS connections.

What’s new in System Layer Release 7.7.0.19 (FP1)

The following table lists enhancements in this release.

Enhancement	Description
N/A	

What’s new in Media Server Release 7.7.0.359 (FP1 SP1)

The following table lists enhancements in this release.

Enhancement	Description
N/A	

What’s new in System Layer Release 7.7.0.20 (FP1 SP1)

The following table lists enhancements in this release.

Enhancement	Description
N/A	

What’s new in Media Server Release 7.7.0.375 (FP1 SP2)

The following table lists enhancements in this release.

Enhancement	Description
AMS-3263	**AAMS installer enhancements to simplify building Amazon AMI**

What’s new in System Layer Release 7.7.0.21 (FP1 SP2)

The following table lists enhancements in this release.

Enhancement	Description
N/A	

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 *Avaya Aura® Media Server*, 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:

1. Log in to the Avaya Technical Support Web site https://support.avaya.com.
2. 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.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Contact support tasks

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

- Media Server log capture with trace logs included
- Network packet capture on the Media Server

Fixes in Avaya Aura® Media Server Release 7.7.x.x

Fixes in Media Server Release 7.7.0.236 (SP1)

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
AMS-1821	Select deployments where applications utilize DTMF generation.	Missing marker bit for outbound RFC2833/4733 packets could cause DTMF interop issues with some devices. DTMF collection and DTMF relay features are not impacted by this issue.	7.7.0

Fixes in System Layer Release 7.7.0.11 (SP1)

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
N/A			

Fixes in Media Server Release 7.7.0.281 (SP2)

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
AMS-1756	Appliance deployments with no DNS server in the network.	FQDN can't resolve to an IP address and customer account doesn't have access to modify the /etc/hosts file.	7.7.0

Fixes in System Layer Release 7.7.0.14 (SP2)

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
AMS-1756	Appliance deployments with no DNS server in the network.	FQDN can't resolve to an IP address and customer account doesn't have access to modify the /etc/hosts file.	7.7.0
AMS-2032	All appliance deployments.	Incorrect OS is displayed in vSphere client.	7.7.0

Fixes in Media Server Release 7.7.0.292 (SP3)

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
AMS-2250	Appliance enrolled with a SMGR not using default certificates.	Enrollment test connection fails.	7.7.0

Fixes in System Layer Release 7.7.0.15 (SP3)

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
N/A			

Fixes in Media Server Release 7.7.0.334 (FP1)

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
AMS-2662	All deployments.	SIP or H323 Service Observer loses talk path after VOA.	7.7.0
AMS-2671	All deployments.	Component is not restarted after abnormal exit.	7.7.0
AMS-2625	All deployments EM use SMGR for authentication.	EM sign out doesn’t work properly.	7.7.0
AMS-2579	HA deployments.	System Monitor crashes when the HA state is locked.	7.7.0
AMS-2526	All deployments with SMGR enrolment.	Test connection with SMGR fails during enrollment.	7.7.0
AMS-2497	All deployments.	EM Login attempt fails if browser left open on login page for too long.	7.7.0
AMS-1992	All deployments.	Unable to delete certificates from AAMS certificate management key store.	7.7.0
AMS-2377	All deployments with HTTP proxy server configured for streaming and proxy server is unreachable.	Stream Source component restarts.	7.7.0
AMS-2252	All deployments with SMGR enrollment and SMGR default CA cert not used.	Test connection with SMGR fails during enrollment.	7.7.0
AMS-2254	All deployments.	EM unable to import multiple trust certificate using a single PEM file.	7.7.0
AMS-2335	All deployments.	Red text appears in EM Account Management Policies page.	7.7.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Fixes in System Layer Release 7.7.0.19 (FP1)

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
AMS-2679	Appliance deployments with no domain configured.	Installation of system layer update fails.	7.7.0
AMS-2681	All appliance deployments.	RHEL RPM security update (April, 2016)	7.7.0
AMS-2484	All appliance deployments.	Unable to view information about the configured authentication file.	7.7.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Fixes in Media Server Release 7.7.0.359 (FP1 SP1)

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
AMS-3016	German dial tone	Fix for MSML tone generation timing issue	7.7.0
AMS-2969	All deployments	Fix for timer rollover at 497 days of continuous runtime	7.7.0
AMS-2956	All deployments	Security enhancement to prevent clickjacking in Element Manager	7.7.0
AMS-2881	All deployments	Upgrade OpenSSL to version 1.0.1t	7.7.0
AMS-2890	All deployments	Certificate import may fail after certificates are deleted.	7.7.0
AMS-2886	Application Software Only Installs.	AMS installation fails if there is not enough free disk space. Add better indication of failure reason.	7.7.0

Fixes in System Layer Release 7.7.0.20 (FP1 SP1)

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
AMS-2918	All deployments	Updated end user licensing agreement	7.7.0

Fixes in Media Server Release 7.7.0.375 (FP1 SP2)

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
AMS-3369	All deployments	MySQL Oracle Critical Patch Update Oct 2016.	7.6
AMS-3352	All deployments	Security fixes for Element Manager web application	7.7
AMS-3232	Deployments that use OPUS codec.	OPUS -> G722 transcode fails because of miscalculation of OPUS frame size overhead	7.8
AMS-3130	Deployments using tone generation.	Some iterated MSML tones were experiencing phase issues when mixed causing audible distortion. MSML tonegen XML was not being interpreted correctly for all types of iterated tones.	7.7
AMS-3195	All deployments	Cluster MeetMe participants sometimes cannot join a conference if they were waiting on hold on a node different than the one the Chairperson joins on to start the conference	7.6
AMS-3058	All deployments	Upgrade OpenJDK to version 8u102	7.7
AMS-3160	All deployments	MySQL startup race condition fix	7.8
AMS-3067	Deployments with SNMP Agent enabled	SNMP Agent may crash when there are multiple simultaneous SNMP requests	7.7

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
AMS-3061	Deployments using tone generation	German dial tone sounds odd when AAMS plays it, sounds fine with G700	7.7
AMS-3037	Deployments using conferences	Update for a=activetalker:1 support	7.6

Fixes in System Layer Release 7.7.0.21 (FP1 SP2)

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
AMS-2246	All appliance deployments	Password required for single user mode	7.6
AMS-3119	All appliance deployments	File permissions (password, shadow and group) are not properly set	7.8
AMS-3255	All appliance deployments	RHEL RPM security update	7.7

Known issues and workarounds in Avaya Aura® Media Server Release 7.7.x.x

Known issues and workarounds in Media Server Release 7.7.0.236 (SP1)

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

ID	Minimum conditions	Visible symptoms	Workaround
N/A			

Known issues and workarounds in System Layer Release 7.7.0.11 (SP1)

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

ID	Minimum conditions	Visible symptoms	Workaround
N/A			

Known issues and workarounds in Media Server Release 7.7.0.281 (SP2)

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

ID	Minimum conditions	Visible symptoms	Workaround
N/A			

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Known issues and workarounds in System Layer Release 7.7.0.14 (SP2)

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

ID	Minimum conditions	Visible symptoms	Workaround
N/A			

Known issues and workarounds in Media Server Release 7.7.0.292 (SP3)

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

ID	Minimum conditions	Visible symptoms	Workaround
N/A			

Known issues and workarounds in System Layer Release 7.7.0.15 (SP3)

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

ID	Minimum conditions	Visible symptoms	Workaround
N/A			

Known issues and workarounds in Media Server Release 7.7.0.334 (FP1)

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

ID	Minimum conditions	Visible symptoms	Workaround
N/A			

Known issues and workarounds in System Layer Release 7.7.0.19 (FP1)

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

ID	Minimum conditions	Visible symptoms	Workaround
N/A			

Known issues and workarounds in Media Server Release 7.7.0.359 (FP1 SP1)

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

ID	Minimum conditions	Visible symptoms	Workaround
N/A			

Known issues and workarounds in System Layer Release 7.7.0.20 (FP1 SP1)

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

ID	Minimum conditions	Visible symptoms	Workaround
N/A			

Known issues and workarounds in Media Server Release 7.7.0.375 (FP1 SP2)

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

ID	Minimum conditions	Visible symptoms	Workaround
N/A			

Known issues and workarounds in System Layer Release 7.7.0.21 (FP1 SP2)

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

ID	Minimum conditions	Visible symptoms	Workaround
AMS-3519	**OVA deployed without configuring DNS server**	Installation of system update fails and system layer event logs indicate “Error obtaining DNS servers”	Use netSetup to configure DNS server prior to installing update

Languages supported

- *English*

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Avaya Aura® WebLM on VMWare

Installation for Avaya Aura® WebLM on VMWare Release 7.0.x.x

Required patches for Avaya Aura® WebLM on VMWare for 7.0.0.0

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

Download ID	Patch	Notes
SMGR70GA004	WebLM-7.0.0.9-16703-e55-19.ova	WebLM 7.0.0.0 OVA software. Size: 649 MB MD5SUM: 091f695381199a23e2c493fed16852e

Required patches for Avaya Aura® WebLM on VMWare for 7.0.0.1

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

Download ID	Patch	Notes
SMGR7001003	WebLM_7.0.0.1_r70014205.bin	WebLM 7.0.0.1 software. WebLM 7.0.0.1 can be installed only on WebLM Release 7.0.0.0. Size: 194 MB MD5SUM: 56429ca9edc732948610db4bb1682e55

Required patches for Avaya Aura® WebLM on VMWare for 7.0.0.2

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

Download ID	Patch	Notes
SMGR7002002	WebLM_7.0.0.2_r70024453.bin	WebLM 7.0.0.2 software. WebLM 7.0.0.2 can be installed only on WebLM Release 7.0.0.0 or 7.0.0.1. Size: 212 MB MD5SUM: 5a263cc06d71fb1ca0015a5a766c1191

Required patches for Avaya Aura® WebLM on VMWare for 7.0.1

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

Download ID	Patch	Notes
SMGR7010003	**WebLM_7.0.1.0_r701064822.bin**	WebLM 7.0.1 software. WebLM 7.0.1 can be installed only on WebLM Release 7.0.0.0 or 7.0.0.1 or 7.0.0.2. **Size**: 285 MB

Download ID	Patch	Notes
		MD5SUM: bf940aa02d1e641c2117cf173a8be1a1

Required patches for Avaya Aura® WebLM on VMWare for 7.0.1.1

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

Download ID	Patch	Notes
SMGR7011003	**WebLM_7.0.1.1_r701105241.bin**	WebLM 7.0.1.1 software. WebLM 7.0.1.1 can be installed only on WebLM Release 7.0.0.0 or 7.0.0.1 or 7.0.0.2 or 7.0.1.0 release. **Size**: 285 MB **MD5SUM**: 37cdd75ed382393dac1d794bd4c549d5

Required patches for Avaya Aura® WebLM on VMWare for 7.0.1.2

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

Download ID	Patch	Notes
SMGR7012003	**WebLM_7.0.1.2_r701205894.bin**	WebLM 7.0.1.2 software. WebLM 7.0.1.2 can be installed only on WebLM Release 7.0.0.0 or 7.0.0.1 or 7.0.0.2 or 7.0.1.0 or WebLM 7.0.1.1 release. **Size**: 284 MB **MD5SUM**: 5769c2eabfffde48f798f3778ddfe031

Backing up the software

1. **Perform VMWare snapshot of the WebLM VM**
   A snapshot preserves the state and data of a virtual machine at a specific point in time. Snapshots consume large amounts of data resources, increase CPU loads on the host, and affect performance and service.
   Note: Verify that the patch installation or upgrade is successful, and ensure that the virtual application is functional. You can then delete the snapshot.

2. **Log in to the WebLM CLI interface as the ‘admin’ user and perform a Backup as mentioned below:**
   Backup can be performed in the following two ways –
   Option 1: Provide the backup location as a parameter.
   - WebLMBackup <backup_location>
   - In this case the backup of WebLM would be taken at the specified location.

   Option 2: If a backup location is not given as a parameter.
   - WebLMBackup
   - In this case the backup of WebLM would be taken at the default location specified in conf. properties.

Installing the release 7.0.0.0

Important Notes

1. Characters required in the hostname

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

WebLM hostnames must include only letters, numbers, and hyphens (-) and not underscores. For example, WebLM_62 is an invalid host name.

2. Log in to the standalone WebLM on VMware

   The login credentials for CLI login is admin/admin. After the first CLI login, you must change the password.

   When you gain access to the Web interface, use the default username admin and the default password weblmadmin. After you log in using the default credentials, the system prompts you to change the password. After you change the default password, the system redirects you to the login page to log in with the changed credentials.

3. 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.

4. Restoring WebLM Backup

   Ensure that the Tomcat is restarted after the WebLM restore functionality.

5. 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 changes, 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.

3. 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	Profile S8300E
vCPUs	1	1	1
CPU reservation	2290 MHz	2290 MHz	1950 MHz
Memory	1 GB	2 GB	2 GB
Memory reservation	1 GB	2 GB	2 GB
Storage reservation	30 GB	30 GB	35 GB
Shared NIC	1	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.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

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.

In the navigation pane, right-click the WebLM VM and select the Power On option from the context menu.

Software information

Software	Version
CentOS	6.5 64-bit
OpenJDK	1.8 update 77 64-bit
Apache Tomcat	8.0.18
VMware vCenter Server, vSphere Client, ESXi Host	5.0, 5.1, 5.5, 6.0
Microsoft® Internet Explorer	9.x, 10.x, and 11.x
Mozilla® Firefox	40, 41, 42

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

Upgrading to Avaya Aura® WebLM on VMWare for 7.0.0.1

Patch install will not work with ASG login's init/inads and craft user. You must login as admin user to perform patch installation.

1. Log in to the WebLM CLI interface as the 'admin' user.
2. Copy the patch installer file to the WebLM server.
3. Verify md5sum of the bin file with the value from PLDS.
4. Run the following Service Pack:

   #WebLMPatchdeploy

5. When the system prompts for the location of the patch file, provide the correct location of the patch and click Enter.

   Wait for the system to execute the patch installer and display the installer prompt.

6. Perform the following to verify the service pack installation:
   a. Log into the WebLM web console.
   b. Click the About link on the home/landing page. Verify that About page contains as below:

      Web License Manager (WebLM v7.0)

      Build Number – 7.0.0.1.X.XXXX

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Note: If the patch installation or upgrade is successful and the virtual application is functional, you can delete the snapshot.

7. After you upgrade the system to service pack 7.0.0.1, **reboot** the WebLM from CLI to get the updated kernel running in memory.

Upgrading to Avaya Aura® WebLM on VMWare for 7.0.0.2

Patch install will not work with ASG login's init/inads and craft user. You must login as admin user to perform patch installation.

1. Log in to the WebLM CLI interface as the 'admin' user.
2. Copy the patch installer file to the WebLM server.
3. Verify md5sum of the bin file with the value from PLDS.
4. Run the following Service Pack:

   #WebLMPatchdeploy
5. When the system prompts for the location of the patch file, provide the correct location of the patch and click Enter.

   Wait for the system to execute the patch installer and display the installer prompt.
6. Perform the following to verify the service pack installation:
   a. Log into the WebLM web console.
   b. Click the About link on the home/landing page. Verify that About page contains as below:

   Web License Manager (WebLM v7.0)

   Build Number – 7.0.0.2.X.XXXX

   Note: If the patch installation or upgrade is successful and the virtual application is functional, you can delete the snapshot.
7. After you upgrade the system to service pack 7.0.0.2, **reboot** the WebLM from CLI to get the updated kernel running in memory.

Upgrading to Avaya Aura® WebLM on VMWare for 7.0.1

Patch install will not work with ASG login's init/inads and craft user. You must login as admin user to perform patch installation.

1. Log in to the WebLM CLI interface as the 'admin' user.
2. Copy the patch installer file to the WebLM server.
3. Verify md5sum of the bin file with the value from PLDS.
4. Run the following Feature Pack:

   #WebLMPatchdeploy
5. When the system prompts for the location of the patch file, provide the correct location of the patch and click Enter.
6. Wait for the system to execute the patch installer and display the installer prompt.
7. Perform the following to verify the feature pack installation:

a. Log into the WebLM web console.

b. Click the About link on the home/landing page. Verify that About page contains as below:

   Web License Manager (WebLM v7.0.1)

   Build Number – **7.0.1.**X.XXXX

   Note: If the patch installation or upgrade is successful and the virtual application is functional, you can delete the snapshot.

8. After you upgrade the system to feature pack 7.0.1, reboot the WebLM from CLI to get the updated kernel running in memory.

Upgrading to Avaya Aura® WebLM on VMWare for 7.0.1.1

Patch install will not work with ASG login's init/inads and craft user. You must login as admin user to perform patch installation.

1. Log in to the WebLM CLI interface as the 'admin' user.
2. Copy the patch installer file to the WebLM server.
3. Verify md5sum of the bin file with the value from PLDS.
4. Run the following Service Pack:

   ```
   #WebLMPatchdeploy
   ```

5. When the system prompts for the location of the patch file, provide the correct location of the patch and click Enter.

   Wait for the system to execute the patch installer and display the installer prompt.

6. Perform the following to verify the service pack installation:
   a. Log into the WebLM web console.
   b. Click the About link on the home/landing page. Verify that About page contains as below:

      Web License Manager (WebLM v7.0)

      Build Number – 7.0.1.1.X.XXXX

   Note: If the patch installation or upgrade is successful and the virtual application is functional, you can delete the snapshot.

7. After you upgrade the system to service pack 7.0.1.1, **reboot** the WebLM from CLI to get the updated kernel running in memory.

Upgrading to Avaya Aura® WebLM on VMWare for 7.0.1.2

Patch install will not work with ASG login's init/inads and craft user. You must login as admin user to perform patch installation.

1. Log in to the WebLM CLI interface as the 'admin' user.
2. Copy the patch installer file to the WebLM server.
3. Verify md5sum of the bin file with the value from PLDS.
4. Run the following Service Pack:

   ```
   #WebLMPatchdeploy
   ```

5. When the system prompts for the location of the patch file, provide the correct location of the patch and click Enter.

   Wait for the system to execute the patch installer and display the installer prompt.

6. Perform the following to verify the service pack installation:
    a. Log into the WebLM web console.
    b. Click the About link on the home/landing page. Verify that About page contains as below:

       Web License Manager (WebLM v7.0)

       Build Number – 7.0.1.2.X.XXXX

    Note: If the patch installation or upgrade is successful and the virtual application is functional, you can delete the snapshot.
7. After you upgrade the system to service pack 7.0.1.2, **reboot** the WebLM from CLI to get the updated kernel running in memory.

Troubleshooting the installation

Collect logs 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.
- Installation log files are available at **/opt/Avaya/install_logs**
- The WebLM Tomcat server log files are available at **$CATALINA_HOME/logs**. You can gain access to the CLI using **admin** as the user name and gain access to the log file.

Additional WebLM logs at **$CATALINA_HOME/webapps/WebLM/data/log**

Restoring software to previous version

If the Service Pack installation fails, use the VM snapshot manager to revert to a snapshot taken prior to patch installation.

Contacting support

Contact support checklist

Avaya Technical Support provides support for WebLM 7.0.x on VMware.

For any problems with WebLM 7.0.x on VMware, 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.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

- Installation log files are available at **/opt/Avaya/install_logs**
- The WebLM Tomcat server log files are available at **$CATALINA_HOME/logs**. You can gain access to the CLI using admin as the user name and then gain access to the log file.
- Additional WebLM logs at **$CATALINA_HOME/webapps/WebLM/data/log**.

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.

What's new in Avaya Aura® WebLM on VMWare Release 7.0.x.x

What's new in Avaya Aura® WebLM on VMWare for 7.0.0.0

The following table lists enhancements in this release.

Enhancement	Description
WebLM migrated from Oracle JDK to OpenJDK 1.7 update 79 64-bit.	Infrastructure Updates
Support for CentOS 6.5 and Apache Tomcat 8.0.18.	EULA
Support for display and logging of EULA Acceptance.	Avaya Appliance
Support for installing WebLM 7.0 OVA on the Appliance Virtualization Platform (AVP) that is being introduced in Avaya Aura 7 as part of the Avaya Provided Appliance.	Hosted Cloud Deployment

What's new in Avaya Aura® WebLM on VMWare for 7.0.1

The following table lists enhancements in this release.

Enhancement	Description
Platform Upgrade	OpenJDK upgraded to 1.8 update 77

Fixes in Avaya Aura® WebLM on VMWare Release 7.0.x.x

Fixes in Avaya Aura® WebLM on VMWare for 7.0.0.0

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
SMGR-985		The WebLM login and change password pages disabled the autocomplete HTML Attribute for the Password field.	
SMGR-986		The **About** link opens on a new browser tab when you expand the WebLM navigation tree.	
SMGR-27343		Cleanup of uninstalled license file. What is the issue?	
SMGR-28962		License peak usages get reset at the end of a month in some cases. This issue is a customer issue.	
SMGR-31581		IPO does not go into WebLM error mode after decreasing the number of available licenses on the	

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release found in
		WebLM server by changing the order on OSC.	
SMGR-24634; SMGR-24635; SMGR-32435		Security Enhancements	

Fixes in Avaya Aura® WebLM on VMWare for 7.0.0.1

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
SMGR-34575	Infrastructure	In keeping with NIST guidelines and industry best practices, Avaya is rotating the security keys associated with remote maintenance access through the Avaya Security Gateway (ASG).	7.0.0.0
SMGR-34417	Security Updates	Oracle Java Critical Patch Update (October 2015)	7.0.0.0
SMGR-34208	Security Updates	[RHSA-2015:1920-01] Critical: java-1.7.0-openjdk security update (RHSA-2015-1920)	7.0.0.0
SMGR-34003	Security Updates	[RHSA-2015:0863-01] Moderate: glibc security and bug fix update (RHSA-2015-0863)	7.0.0.0
SMGR-33995	Security Updates	[RHSA-2015:1330-01] Moderate: python security, bug fix, and enhancement update	7.0.0.0
SMGR-33957	Security Updates	[RHSA-2015:1457-01] Moderate: gnutls security and bug fix update (RHSA-2015-1457)	7.0.0.0
SMGR-33953	Security Updates	[RHSA-2015:1471-01] Important: bind security update (RHSA-2015-1471)	7.0.0.0
SMGR-33943	Security Updates	[RHSA-2015:1081-01] Important: kernel security, bug fix, and enhancement update (RHSA-2015-1081) (RHSA-2015-1272)	7.0.0.0
SMGR-33912	Security Updates	[RHSA-2015:1185-01] Moderate: nss security update (RHSA-2015-1185)	7.0.0.0
SMGR-33907	Security Updates	[RHSA-2015:1419-01] Low: libxml2 security and bug fix update (RHSA-2015-1419)	7.0.0.0
SMGR-33948	Security Updates	[RHSA-2015:1482-01] Important: libuser security update (RHSA-2015-1482)	7.0.0.0
SMGR-34011	Security Updates	[RHSA-2015:1459-01] Moderate: ntp security, bug fix, and enhancement update	7.0.0.0
SMGR-33601	Security Updates	[RHSA-2015:1640-01] Moderate: pam security update	7.0.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
SMGR-33608	Security Updates	[RHSA-2015:1699-01] Moderate: nss-softokn security update	7.0.0.0
SMGR-33606	Security Updates	[RHSA-2015:1708-01] Important: libXfont security update	7.0.0.0
SMGR-33604	Security Updates	[RHSA-2015-1623] kernel security and bug fix update	7.0.0.0
SMGR-33603	Security Updates	[RHSA-2015:1634-01] Moderate: sqlite security update	7.0.0.0
SMGR-34427	Security Updates	Java Security Provider changes for Elliptic Curve cryptography	7.0.0.0
SMGR-34898	Infrastructure	Update for Turkey 2015 DST changes	N/A

Fixes in Avaya Aura® WebLM on VMWare for 7.0.0.2

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
SMGR-33907	Security Updates	[RHSA-2015:1419-01] Low: libxml2 security and bug fix update	7.0.0.0
SMGR-33837	Security Updates	[RHSA-2015:1330-01] Moderate: python security, bug fix, and enhancement update	7.0.0.0

Fixes in Avaya Aura® WebLM on VMWare for 7.0.1

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-33906	Security Updates	[RHSA-2015-1419] libxml2 security and bug fix update	7.0.0.0
SMGR-33912	Security Updates	[RHSA-2015-1185] nss security update	7.0.0.0
SMGR-33942	Security Updates	[RHSA-2015-1081][RHSA-2015-1272] kernel security, bug fix, and enhancement update	7.0.0.0
SMGR-33947	Security Updates	[RHSA-2015-1482] libuser security update	7.0.0.0
SMGR-33952	Security Updates	[RHSA-2015-1471] bind security update	7.0.0.0
SMGR-33956	Security Updates	[RHSA-2015-1457]gnutls security and bug fix update	7.0.0.0
SMGR-33994	Security Updates	[RHSA-2015:1330-01]security, bug fix, and enhancement update	7.0.0.0

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-34002	Security Updates	[RHSA-2015-0863] glibc security and bug fix update	7.0.0.0
SMGR-34010	Security Updates	[RHSA-2015:1459-01] ntp security, bug fix, and enhancement update	7.0.0.0
SMGR-33906	Security Updates	[RHSA-2015-1419] libxml2 security and bug fix update	7.0.0.0
SMGR-34899	DST	Turkey DST Changes	7.0.0.0
SMGR-35490	Security Updates	Removed WebLM version display to unauthenticated connection	7.0.0.0

Fixes in Avaya Aura® WebLM on VMWare for 7.0.1.1

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
SMGR-36378	Security Updates	(CEEA-2016:0463) CentOS 6 tzdata Enhancement Update	7.0.1.0
SMGR-36457	Security Updates	(CESA-2016:0459) [RHSA-2016:0459-01] Important: bind security update	6.3.17
SMGR-36971	Security Updates	[RHSA-2016:0760-01] Moderate: file security, bug fix, and enhancement update	7.0.0.0
SMGR-37061	Security Updates	CESA-2016:0996) [RHSA-2016:0996-01] Important: openssl security update	7.0.0.0
SMGR-37050	Security Updates	(CESA-2016:0591) [RHSA-2016:0591-01] Moderate: nss, nss-util, and nspr security, bug fix, and enhancement update	7.0.0.0
SMGR-37332	Security Updates	[RHSA-2016:1141-01] Moderate: ntp security update	7.0.0.0
SMGR-37104	Security Updates	(CESA-2016:0855) [RHSA-2016:0855-01] Moderate: kernel security, bug fix, and enhancement update	7.0.0.0
SMGR-37462	Security Updates	(CEBA-2016:1266) CentOS 6 tzdata 2016e BugFix Update	7.0.0.0
SMGR-36729	Security Updates	Oracle Java SE Critical Patch Update for April 2016	6.3.17
SMGR-37451	Security Updates	Disable CBC mode cipher	7.0.0.0
SMGR-37541	Infrastructure	Tomcat access logs on server fill up disk to 100%.	6.3.14

Fixes in Avaya Aura® WebLM on VMWare for 7.0.1.2

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
SMGR-38937	Security Updates	[RHSA-2016:2141-01] Important: bind security update	7.0.1.1
SMGR-38916	Security Updates	[CESA-2016:2105] [RHSA-2016:2105-01] Important: kernel security update	7.0.1.1
SMGR-38912	Security Updates	[CESA-2016:1940] [RHSA-2016:1940-01] Important: openssl security update	7.0.1.1
SMGR-37765	Security Updates	Oracle Java SE Critical Patch Update for Oct 2016	7.0.1.1
SMGR-37658	Security Updates	(CESA-2016:1406) Important CentOS 6 kernel Security Update	7.0.1.0
SMGR-37654	Security Updates	(CEEA-2016:1388) CentOS 6 tzdata 2016f Enhancement Update	7.0.1.0
SMGR-37586	Security Updates	(CESA-2016:1292) [RHSA-2016:1292-01] Important: libxml2 security update	7.0.0.0
SMGR-37097	Security Updates	(CESA-2016:0073) [RHSA-2016:0073-01] Moderate: bind security update	7.0.0.1

Known issues and workarounds in Avaya Aura® WebLM on VMWare Release 7.0.x.x

Known issues and workarounds in Avaya Aura® WebLM on VMWare for 7.0.0.0

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

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-25348		WebLM does not have a Web UI to configure SNMP alarms or agent for SNMP V2c or V3 for VPFM to pick up and report on.	Workaround is unavailable.
SMGR-26801		Navigation menu does not get minimized.	Workaround is unavailable.

Known issues and workarounds in Avaya Aura® WebLM on VMWare for 7.0.0.1

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

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-25348	Alarm Management	Does not have a Web User Interface to configure SNMP alarms or agent for SNMP V2c or V3 for VPFM to pick up and report on.	No workaround
SMGR-26801	User Interface	Navigation menu is not getting minimized.	No workaround

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Known issues and workarounds in Avaya Aura® WebLM on VMWare for 7.0.0.2

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

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-25348	Alarm Management	Does not have a Web User Interface to configure SNMP alarms or agent for SNMP V2c or V3 for VPFM to pick up and report on.	No workaround
SMGR-26801	User Interface	Navigation menu is not getting minimized.	No workaround

Known issues and workarounds in Avaya Aura® WebLM on VMWare for 7.0.1

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

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-25348	Alarm Management	Does not have a Web User Interface to configure SNMP alarms or agent for SNMP V2c or V3 for VPFM to pick up and report on.	No workaround
SMGR-26801	User Interface	Navigation menu is not getting minimized.	No workaround

Known issues and workarounds in Avaya Aura® WebLM on VMWare for 7.0.1.1

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

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-25348	Alarm Management	Does not have a Web User Interface to configure SNMP alarms or agent for SNMP V2c or V3 for VPFM to pick up and report on.	No workaround
SMGR-26801	User Interface	Navigation menu is not getting minimized.	No workaround

Known issues and workarounds in Avaya Aura® WebLM on VMWare for 7.0.1.2

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

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-25348	Alarm Management	Does not have a Web User Interface to configure SNMP alarms or agent for SNMP V2c or V3 for VPFM to pick up and report on.	No workaround
SMGR-26801	User Interface	Navigation menu is not getting minimized.	No workaround

Solution Deployment Manager (SDM)

Solution Deployment Manager is a centralized software management solution in System Manager that provides deployments, upgrades, migrations, and updates to Avaya Aura® 7.0 and later applications. Solution Deployment Manager supports the operations on customer Virtualized Environment and Avaya Aura® Virtualized Appliance model.

From 7.0, Avaya Aura® System Manager also provides a standalone version of Solution Deployment Manager, the Solution Deployment Manager client.

With Solution Deployment Manager (SDM), you can perform the following operations in Customer provided Virtualized Environment and Avaya Aura® Virtualized Appliance models:

- Deploy Avaya Aura® applications.
- Upgrade and migrate Avaya Aura® applications.
- Download Avaya Aura® applications.
- Install service packs, feature packs, and software patches for the following Avaya Aura® applications.
- Support vCenter operations for hosts and Virtual Machines (VMs). For more details on SDM features, see ***Administering Avaya Aura® System Manager for Release 7.0.1.***

The deploy process from Solution Deployment Manager involves the following key tasks:

- Download the necessary software components.
- Add Location.
- Add host.
- Deploy 7.0.0 OVA.

The upgrade process from Solution Deployment Manager involves the following key tasks:

- Discover the Avaya Aura® applications.
- Execute Analyze.
- Refresh applications and associated devices, and download the necessary software components.
- Run the pre-upgrade check to ensure successful upgrade environment.
- Upgrade Avaya Aura® applications.
- Install software patch, service pack, or feature pack on the Avaya Aura® applications. This step is not mandatory.

The patching process (Hotfixes, Service Pack, and Feature Pack) after 7.0.0 OVA deployment from Solution Deployment Manager involves the following key tasks:

- Execute Analyze.
- Run the preupgrade check to ensure successful upgrade environment.
- Install software patch, service pack, or feature pack on the Avaya Aura® applications.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Note: For custom patching, Execute Analyze and Preupgrade check are optional. Select the element, Select the custom patch and Schedule the custom patching job.

Note:
In Release 7.0 and later, Solution Deployment Manager does not support migration of Virtualized Environment-based 6.x applications to 7.x in customer Virtualized Environment. Use vSphere Client to migrate to customer's Virtualized Environment.

Avaya Aura Solution using SDM and SDM Client:

For more information about the setup of the Solution Deployment Manager functionality that is part of System Manager 7.x and later, see:

- ***Avaya Aura® System Manager Solution Deployment Manager Job-Aid***
- ***Deploying Avaya Aura® applications*** for deploying Aura applications using System Manager Solution Deployment Manager (SDM) and Solution Deployment Manager – Client (SDM-Client)
- ***Upgrading Avaya Aura® applications to Release 7.0.1*** for upgrading Aura applications using Solution Deployment Manager (SDM)
- ***Upgrading Avaya Aura® applications to Release 7.0.1*** for upgrading Aura applications using the Solution Deployment Manager Client

The following section provides **Solution Deployment Manager Feature** information.

SDM Adopter Matrix	Adopting Product (System Manager Release 7.0.1)												
SMGR SDM - Centralized Functionality	Appliance Virtualization Platform	System Manager	Session Manager	Communication Manager	CM Adjuncts (MM, TN Boards, Gateways)	Branch Session Manager	Utility Services	CM Messaging	Breeze (w/ Presence Snap-in)	Secure Access Gateway	WebLM	Application Enablement Services	Avaya Aura® Media Server
OVA Deployment R 7.0.0 (Configuration & Footprint)	N	N	Y	Y	n/a	Y	Y	Y	Y	Y	Y	Y	Y
Patching Deployment (hotfixes)	Y [Other than SMGR hosting AVP]	N	Y	Y	n/a	Y	Y	Y	N	N	N	N	N
Custom Patching Deployment	n/a	N	Y	Y	n/a	Y	Y	Y	N	N	Y [7.0.1 onwards]	N	N
Service Pack Deployment	Y [Other than SMGR hosting AVP]	N	Y	Y	n/a	Y	Y	Y	N	N	N	N	N
Feature Pack Deployment	Y [Other than SMGR hosting AVP]	N	Y	Y	n/a	Y	Y	Y	N	N	N	N	N
Automated Migrations R6.x to R7.0 (analysis & pre-upgrade checks) [Source Platform: System Platform] [Target Platform: AVP / customer VE]	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 R6.x to 7.0.0.1 / 7.0.0.2/7.0.0.x [Source Platform: System Platform] [Target Platform: AVP / customer VE]	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 R6.x to 7.0.1 [Source Platform: System Platform] [Target Platform: AVP / customer VE]	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	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
SDM 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
Support for changing VM Flexible Footprint	n/a	Y	Y	Y	n/a	Y	Y	Y	Y	Y	Y	Y	Y
Change Network Parameters	Y	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

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

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

AVP: Appliance Virtualization Platform

VE: Virtualized Environment

The following section provides **Solution Deployment Manager Client feature** information.

SDM Adopter Matrix	Adopting Product (System Manager Release 7.0.1)												
SDM Client Functionality	Appliance Virtualization Platform	System Manager	Session Manager	Communication Manager	CM Adjuncts (MM, TN Boards, Gateways)	Branch Session Manager	Utility Server	CM Messaging	Breeze (w/ Presence Snap-in)	Secure Access Gateway	WebLM	Application Enablement Services	Avaya Aura ® Media Server
OVA Deployment R7.0.0 (Configuration & Footprint)	N	Y	Y	Y	n/a	Y	Y	Y	Y	Y	Y	Y	Y
Patching Deployment	Y	Y	N	N	N	N	N	N	N	N	N	N	N
Service Packs Deployment	Y	Y	N	N	N	N	N	N	N	N	N	N	N
Feature Packs Deployment	Y	Y	N	N	N	N	N	N	N	N	N	N	N
Automated Migrations R6.x to R7.0 [Source Platform: System Platform] [Target Platform: AVP / VE]	n/a	Y	N	N	N	N	N	N	N	N	N	N	N
Automated Migrations R6.x to R7.0.0.1 / R7.0.0.2 [Source Platform: System Platform] [Target Platform: AVP / VE]	n/a	Y	N	N	N	N	N	N	N	N	N	N	N
Automated Migrations R6.x to R7.0.1 [Source Platform: System Platform] [Target Platform: AVP / VE]	n/a	Y	N	N	N	N	N	N	N	N	N	N	N
Virtual Machine Management (start, stop, reset, status, dashboard)	Y	Y	Y	Y	n/a	Y	Y	Y	Y	Y	Y	Y	Y
Support for changing VM Flexible Footprint	n/a	Y	Y	Y	n/a	Y	Y	Y	Y	Y	Y	Y	Y
Change Network Parameters	Y	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Deployment through Service Ports	n/a	Y	Y	Y	n/a	Y	Y	Y	Y	Y	Y	Y	Y
Support for Static routing	n/a	Y	Y	Y	n/a	Y	Y	Y	Y	Y	Y	Y	Y

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

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Deployment and Upgrade Guides:

Products	**Deployment and Upgrade Guides**
Appliance Virtualization Platform	Migrating and Installing Appliance Virtualization Platform (Release 7.0.1)
Session Manager	Deploying Avaya Aura® Session Manager (Release 7.0.1) Upgrading Avaya Aura® Session Manager (Release 7.0.1)
Communication Manager	Deploying Avaya Aura® Communication Manager (Release 7.0.1) Upgrading Avaya Aura® Communication Manager (Release 7.0.1)
CM Adjuncts (MM, TN Boards, Gateways)	Deploying and Upgrading G430 Branch Gateways (Release 7.0.1) Deploying and Upgrading G450 Branch Gateways (Release 7.0.1)
Branch Session Manager	Deploying Avaya Aura® Branch Session Manager (Release 7.0.1)
Utility Services	Deploying Avaya Aura® Utility Services (Release 7.0.1)
CM Messaging	Deploying Avaya Aura® Communication Manager Messaging (Release 7.0.1)
Breeze (w/ Presence Snap-in)	Deploying Avaya Breeze^{TM} (Release 3.1) Quick start guide for Deploying Avaya Breeze^{TM} snap-ins (Release 3.1)
Secure Access Gateway	Deploying Secure Access Link Gateway using Avaya Aura® System Manager in the VMware Virtualized Environment (Release 2.5
Application Enablement Services	Deploying Avaya Aura® Application Enablement Services in Virtualized Environment (Release 7.0.1)
System Manager	Deploying Avaya Aura® System Manager 7.0.1 (Release 7.0.1) Upgrading Avaya Aura® System Manager to 7.0.1 (Release 7.0.1)

Avaya Aura Solution using SDM and SDM Client
Avaya Aura® System Manager Solution Deployment Manager Job-Aid
Deploying Avaya Aura® applications for deploying Aura applications using System Manager Solution Deployment Manager (SDM) and Solution Deployment Manager – Client (SDM-Client)
Upgrading Avaya Aura® applications to Release 7.0.1 for upgrading Aura applications using Solution Deployment Manager (SDM)
Upgrading Avaya Aura® applications to Release 7.0.1 for upgrading Aura applications using the Solution Deployment Manager Client

Avaya Aura® Device Services

Avaya Aura® Device Services provides a set of services to Avaya Equinox™ 3.0. Avaya Aura® Device Services is co-resident with Session Manager 7.0.1 and is delivered as a separate OVA.

Installation

Required patches

Download ID	Patch	Notes
TBD	aads-7.0.1.0.3345-patch-1-v2.tgz	Fixes for • AADS auto configuration fails if SMGR uses OtherEmail handle mapped to ActiveDir mail address. • AADS incorrectly sets IM handle in PPM update request. • Presence does not work for search results when email address is being used in search query. • Existing PPM contacts do not show up when AADS is enabled. • Picture service fails for contacts who are not AADS users.
TBD	aads-7.0.1.0.3345-patch-2-v2.tgz	Fixes for • E164 Contact Presentation Problem for Multiple Phone Numbers of the same type. • Websocket subscriptions case sensitive. • ADD contacts service fixes for primary phone number.
TBD	aads-7.0.1.0.3345-patch-3.tgz	Fixes for • AADS replication fails and some nodes remain in continual "repairing" state after upgrade to 3345 load. • Issue with handling the data. Multiple COMM profiles on System Manager, for ‘add’, ‘update’, and ‘delete’ contact.
TBD	aads-7.0.1.0.3345-patch-4.tgz	Fixes for • AADS returns 2 primary phone numbers for a contact (multiple LDAP or 2 Avaya SIP numbers). • AutoConfig service couldn’t work due to Inability to create DRS cache.

After the patch has been applied to all AADS node(s) and services are started, perform a DRS repair on the node(s) from the following path: SMGR->Services->Replication GUI.

File list for Avaya Aura® Device Services

Filename	Modification time stamp	File size	Version number
aads-7.0.1.0.3345_OVF10.ova		1423569920 bytes	
aads-7.0.1.0.3345.bin		593988884 bytes	

Backing up the software

Refer to the Backup and Restore System Information section of the Deploying Avaya Aura® Device Services guide.

Installing the release

Refer to the Deploying AADS OVA section of the Deploying Avaya Aura® Device Services guide.

Troubleshooting the installation

Refer to the Trouble shooting and Maintenance section of the Deploying Avaya Aura® Device Services guide.

Restoring software to previous version

Refer to the Backup and Restore System Information section of the Deploying Avaya Aura® Device Services guide.

What's new

What's new in Release 7.0.1

Avaya Aura® Device Services provides a set of services to Avaya Equinox™ 3.0. Avaya Aura® Device Services is co-resident with Session Manager 7.0.1 and is delivered as a separate OVA.

The following table lists enhancements in this release.

Enhancement	Description
Notification	The Notification service provides a common infrastructure that allows a client or endpoint to subscribe to receive events from a number of service resources using a single connection.
Dynamic Configuration	The Dynamic Configuration service provides discovery of configuration settings to UC Clients. You can customize these settings on a global, group, individual, or platform basis. The Dynamic Configuration service uses the automatic configuration feature of Avaya Equinox™ 3.0 to facilitate the configuration details to the UC clients. This helps the user to avoid manual configuration of their client. To log in to the client, the user needs to enter their credentials, such as, email address or Windows user id, along with their enterprise credentials. The Dynamic Configuration service is supported on the following Avaya Equinox™ 3.0 devices: • Avaya Equinox™ for Android • Avaya Equinox™ for iOS • Avaya Equinox™ for Mac • Avaya Equinox™ for Windows.

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

Enhancement	Description
Contact	To use the Contact service, a user must be a provisioned user on LDAP Server. Using the contact service: • Manage the contact detail from any device. • Add, update, and delete a contact. • Perform an enterprise search of existing sources of contacts, such as, System Manager, multiple LDAPs, single LDAP multiple domains, and local only. Avaya Aura® Device Services supports directory search of up to 300 contacts. • Set and retrieve information, such as, preferred names, picture, and preferences.
Web Deployment	The Web Deployment service publishes and deploys the UC client updates to the devices of the end users. The Web Deployment service is supported on the following devices of the Avaya Equinox™ 3.0: • Avaya Equinox™ for Mac • Avaya Equinox™ for Windows

Fixes

Not Applicable as 7.0.1 is the first release.

Fixes in Release 7.0.1

Not Applicable as 7.0.1 is the first release.

Known issues and workarounds

Known issues and workarounds in Release 7.0.1

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

ID	Minimum conditions	Visible symptoms	Workaround
None	**AADS Services should be Up and Running**	Sometimes when you delete a contact and add back immediately, contacts add operation fails.	There should be 3 minute delay between deleting a user from your contacts and adding the same user back to your contacts list. This is a system limitation.
ACS-3449	**AADS Services should be Up and Running**	DELETE session request doesn't remove old user credentials after re-connecting to AADS with new user	Need to clear sessions and cookies from browser, if logging in as new user.
ACS-3843	**AADS Services should be Up and Running**	Avaya Aura AADS services web GUI about section doesn't show correct version of	Can get the patch information using command line argument sudo /opt/Avaya/DeviceServices/7.0.1.0.3345/CAS/7.0.1.0.3345/patches2/patchmgt.sh --query

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum conditions	Visible symptoms	Workaround
		AADS +Patch	

ACS-3846		Software update via AADS web deployment fails.	Workaround: The following steps need be performed by the System Administrator.
			
			1: Create a file called webdeployment-patch-8442.sh . The contents of the file are mentioned below.
			
			{code}
			#!/bin/sh
			
			# verify that user has root permissions
			if [! "$UID" = 0]; then
			    echo "The script must be executed with root permissions, either as root or using sudo"
			    exit 1
			fi
			
			installdir=\`service AADSService echovar INSTALL_DIR\`
			nginxdir=\`service AADSService echovar NGINX_DIR\`
			nginxdir="${nginxdir}/conf"
			
			patch="
			 server {
			        listen 8442;
			        ssl_certificate ${installdir}/nginx/certs/nginx.crt;
			        ssl_certificate_key ${installdir}/nginx/certs/nginx.key;
			
			        ssl_client_certificate ${installdir}/nginx/certs/auth_ca.crt;
			
			        add_header X-Served-By \$server_name always;
			
			        include secure-headers.conf;
			
			        ssl_verify_client off;
			        # We will send static sparkle.xml (generated by Web Deployment sparkle appcast audit) on GET https://&lt;aads_server&gt;:8442/acs/resources/webdeployment request.
			        # In this way we will avoid authorization which is not supported by clients (client Sparkle library).
			        # Nginx can serve static content (directly) very efficiently when the static files are on the same server as Nginx.
			        # So, we don't really need any load-balancing or explicit caching here.
			        location /acs/resources/webdeployment {
			            default_type application/rss+xml;
			            # remove Last-Modified header which prevents from sending 304 Not Modified response
			            add_header Last-Modified \"\";

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum conditions	Visible symptoms	Workaround

			alias /opt/Avaya/DeviceServices/ClientInstallers/sparkle.xml;
			    }
			
			    # Allow downloads on 8442 port as well
			    location ~* ^/acs/resources/webdeployment/downloads {
			        tcp_nopush on;
			        tcp_nodelay on;
			        alias /opt/Avaya/DeviceServices/ClientInstallers/\$basename;
			    }
			  }
			"
			
			echo "${patch}" > ${nginxdir}/acs-nginx-webdeployment-8442.conf
			chown ucapp:ucgrp ${nginxdir}/acs-nginx-webdeployment-8442.conf
			chmod 750 ${nginxdir}/acs-nginx-webdeployment-8442.conf
			
			grep acs-nginx-webdeployment-8442.conf ${nginxdir}/nginx.conf
			if [$? != 0]; then
			  echo "acs-nginx-webdeployment-8442.conf will be added now"
			  cat ${nginxdir}/nginx.conf \| sed '$s/\}/include\ acs-nginx-webdeployment-8442.conf;\n\}/g' > ${nginxdir}/nginx.conf.new
			  mv ${nginxdir}/nginx.conf ${nginxdir}/nginx.conf.orig
			  mv ${nginxdir}/nginx.conf.new ${nginxdir}/nginx.conf
			else
			  echo "acs-nginx-webdeployment-8442.conf already added"
			fi
			
			iptables -L -n | grep 8442
			if [$? != 0]; then
			  echo "iptables rule will be added now"
			  iptables -I INPUT -p tcp --dport 8442 -j ACCEPT
			  iptables-save
			else
			  echo "iptables rule already exists"
			fi
			
			service AADSNginx reload
			{code}
			
			2: Copy the file to the admin home directory.
			
			3: Execute the script using the command such as:
			chmod 777 <admin_home_directory>/webdeployment-patch-8442.sh
			
			4: Apply the patch under sudo permission such as:
			sudo <admin_home_directory>/webdeployment-patch-8442.sh
			
			5: Change Download URL Port to 8442 on AADS Admin GUI in Appcast. For example: https://&lt;AADS FQDN/IP

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

ID	Minimum conditions	Visible symptoms	Workaround
			Address>:8442/acs/resources/webdeployment/downloads/Avaya Equinox Setup 3.0.0.136.msi 6: Change "APPCAST" URL in Dynamic Configurations to Port 8442. For Example: https://&lt;AADS FQDN/IP Address>:8442/acs/resources/webdeployment
		LDAP configuration disappeared in case AADS server was upgraded from build 3151 to 3284	At this point 2 possible causes of keyspaces being lost on SM upgrade: 1. During an upgrade from 7.0.x to an interim load of 7.0.1.2 (either 1153 or 1287 loads) a bug was frequently encountered that resulted in a 7.0.x backup file remaining on the system instead of being deleted. A subsequent upgrade would encounter this out-of-date file, and it would interrupt the successful restore of Cassandra data on that upgrade. The recommended workaround is to check for the out-of-date backup file prior to beginning the SM upgrade. If the file exists, delete it. The filename is /var/avaya/cassandra/upgrade/callLogs.zip 2. In rare cases, usually under heavy traffic, the Cassandra backup operation invoked during SM upgrade fails. This should not occur if the system is properly put into Deny New Service mode prior to beginning the upgrade. However, we are planning to protect against this with ASM-60387.
ACS-3761		Equinox Windows 3.0 doesn't upgrade when there are more than 2 build on AADS's Web Deployment	Equinox Windows keep only 1 build on AADS Web Deployment
ASM-60399	Active use of Equinox clients (configured for AADS) in conjunction with some users having been deleted from the SMGR database and left in the “soft-deleted” state	. Any Equinox client users that have a soft deleted user on their contact list are no longer able to make updates to their contact lists	Ensure the soft-deleted users are permanently deleted. Subsequently run an audit of User Data Storage on each SM.

Languages supported

- *English*

Copyright 2015-2017 Avaya, Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.