Avaya Aura® 7.1 Release Notes

Release 7.1
Issue 3
May 2017

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

Change history

Issue	Date	Description
1	08-May-2017	GA Release of Avaya Aura® 7.1 Release Notes
2	08-May-2017	Modified PLDS ID and Software Files for SMGR
3	09-May-2017	Addition of a couple of recommended patches for Utility Services

Introduction

This document provides late-breaking information to supplement Avaya Aura® 7.1 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							
	7.1	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	X
Avaya Aura® Session Manager	X	X	X	X	NA	X	X	X
Avaya Aura® System Manager	X	X	X	X	NA	X	X	X
Avaya Aura® Presence Services	X	NA	NA	X	NA	NA	X	X
Avaya Aura® Application Enablement Services	X	NA	X	X	NA	NA	NA	X
Avaya Aura® Utility Services	X	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	X	NA	NA	NA	X
Avaya Aura® G430 and G450 Media Gateways	X	X	X	X	NA	NA	X	X
Avaya Aura® WebLM on VMWare	X	X	X	X	NA	X	X	X
Avaya Aura® Device Services*	*	X	NA					
Avaya Aura® Media Server Release 7.8.0 Service Pack Beta 3	X							

* GA in June 2017.

What's new in Avaya Aura®

What's new in Avaya Aura® 7.1

Product	Enhancement	Description
G430/G450	Security	TLS feature enhancements and administration.
G430/G450	Security	Enhanced user login and password administration.
G430/G450	Security	SSH cipher, key exchange algorithm, and MAC administration.
G430/G450	Security	Update versions of OpenSSL, SSH Server, and SSH Client.
G430/G450	Security	Use of SHA2 to provide more secure download of firmware images.
G430/G450	Security	FIPS mode configuration option to assure only NIST approved authentication and encryption algorithms and security policies are used (*FIPs certification currently in progress*).

Compatibility

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

Version	Product	Description
7.1.x.x	Communication Manager G430 and G430 Media Gateways	In Release 7.1, the gateway defaults to using TLS 1.2, PTLS, and unencrypted H.248 communication with Communication Manager. Earlier versions of Communication Manager do not support TLS version 1.2. Refer to the "set link-encryption" gateway CLI command to adjust these settings.

Contacting support

Contact support checklist

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

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

   If you continue to have a problem, contact Avaya Technical Support:
4. Log in to the Avaya Technical Support Web site https://support.avaya.com.

5. Contact Avaya Technical Support at one of the telephone numbers in the Support Directory listings on the Avaya support Web site.

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

Contact support tasks

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

Avaya Aura® Communication Manager

Installation for Avaya Aura® Communication Manager 7.1

Required patches

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

For more details see PCN2061S on the Avaya Technical Support site https://downloads.avaya.com/css/P8/documents/101038688

NOTE: There is a known issue if CM 7.0.x was previously deployed using the vSphere™ client, and SDM on Avaya Aura® System Manager is being used to upgrade from CM 7.0.x to CM 7.1, trust between SDM and CM cannot be established. For this case a CM 7.0.x pre-upgrade patch that allows trust to be established between CM and SDM must be activated on CM 7.0.x prior to using SDM to upgrade to CM 7.1.x. The pre-upgrade patch is available on Avaya Support under CM 7.1.x Downloads.

Backing up and installing Communication Manager

Communication Manager 7.1 software includes certain third party components including Open Source Software. Open Source Software licenses are included in the Avaya Aura® 7.1.

Communication Manager Solution Templates DVD. To view the licenses:

1. Insert the Avaya Aura® 7.1 Communication Manager Solution Templates DVD into the CD/DVD drive of a personal computer.
2. Browse the DVD content to find and open the folder D:\Licenses.
3. Within this folder are subfolders for Branch Gateway, Communication Manager, Installation Wizard, Session Manager, and Utility Services that contain the license text files for each application.
4. Right click the license text file of interest and select Open With -> WordPad. This information is only accessible on the Communication Manager software DVD and is not installed or viewable on the Communication Manager Server.

Troubleshooting the installation

Support for Communication Manager is available through Avaya Technical Support.

If you encounter trouble with Communication Manager:

1. Retry the action. Follow the instructions in written or online documentation carefully.
2. Check the documentation that came with your hardware for maintenance or hardware-related problems.
3. Note the sequence of events that led to the problem and the exact messages displayed. Have the Avaya documentation available.
4. If you continue to have a problem, contact Avaya Technical Support by:
   a. Logging on to the Avaya Technical Support Web site http://www.avaya.com/support
   b. Calling or faxing Avaya Technical Support at one of the telephone numbers in the Support Directory listings on the Avaya support Web site.

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

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

When you request technical support, provide the following information:

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

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

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

- Copies of all logs related to the issue.

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

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

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

Enhanced Access Security Gateway (EASG)

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

What's new in Communication Manager Release 7.1

For more information see ***What's New in Avaya Aura® Release 7.1*** document on Avaya Support site.

Enhancement	Description
New Features	• Compliance with DISA security STIGs • CAC sharing between CM and SM • IPv6 support for Commercial and Federal markets • Command history – ability to define the number of months to maintain command history up to 24 months • Support for network preemption • Support for CM simplex configuration in AWS environment
Operational Improvements	• Updated browser support • Discontinued support of tethereal symbolic link to tshark • Discontinued support for Telnet • Discontinued support of default server identity certificate

Avaya Aura® Session Manager

Installation for Session Manager 7.1.x.x

Backing up the software

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

Installing the Session Manager software

Upgrading

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

Note: the S8510 and S8800 servers are not supported on Session Manager 7.1 and later. Upgrades from prior releases running on those servers must include planning for a Server replacement.

All upgrades to 7.1 must be performed on a system running 7.0.x.x. Once the system is running 7.0.x.x 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 7.1 are from:

   - SM 7.0 and subsequent service packs
   - SM 6.3 and subsequent feature or service packs
   - SM 6.2 and subsequent service packs.
   - SM 6.1 and subsequent service packs
   - SM 6.0 SP1 and subsequent 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 7.1.

2. VMware-based Session Manager

   The supported upgrade paths to Session Manager 7.1 are:

   - SM 6.2 Service Pack 3 and SM 6.2 Service Pack 4
   - 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.

3. Upgrades to Profile 1 Session Manager

   In Session Manager 7.1 the concurrently registered device capacity of SM Profile 1 has been reduced from 2500 devices to 2000 devices. Customers with SM systems that have been administered with more than 2000 devices prior to upgrading to 7.1, must understand usage and if the system requires more than 2000 concurrent registrations, the solution needs to be re-administered to reduce the number of devices prior to the upgrade. In some instances this may include adding an additional SM server, or increasing the footprint (using a higher Profile) on the existing server.

4. Certificate Special Handling

Any pre-6.3 Session Manager using third party identity certificates will need to have those certificates re-administered after upgrading to SM 7.1. Third party trusted certificates will be preserved. No action is required for pre-6.3 SM's using default identity certificates. Refer to Session Manager Administration guide for details on configuring third party certificates.

5. Systems using Avaya Aura Device Services (AADS)

   When upgrading from a 7.0.1.2 system where AADS is being used, a pre-upgrade patch must be applied to SM prior to upgrading to 7.1. The patch can be downloaded from https://plds.avaya.com. The patch name is *Session_Manager_7.0.1.2.03701394.bin*

   Note: During the maintenance window where SMs are being upgraded to 7.1, AADS services will be impacted. Specifically, when upgrading SMs from 7.0.1.2 systems where User Data Storage clustering was enabled, a User Data Storage repair needs to be manually run after the SMs have been upgraded to 7.1. AADS operations may fail until the repair operation is completed. Prior to executing the repair, ensure that the Connect Test and Cluster Status indicators on the User Data Storage status screen are showing success (green). Once the indicators are green, select all SMs in the cluster and run a "Repair" operation. Note that this applies to all SMs, even those that were not yet upgraded to 7.1 in the same maintenance window.

Troubleshooting the installation

Refer to Troubleshooting Avaya Aura® Session Manager.

Restoring software to previous version

Refer to product documentation.

What's new in Session Manager Release 7.1.x.x

Enhanced Access Security Gateway (EASG)

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

What's new in Session Manager Release 7.1

The following table lists enhancements in this release.

Enhancement	Description
New Features	• Security Enhancements (DOD and Commercial), including: o Ability to deprecate usage of TLS 1.0/1.1 o Certificate revocation lists • CAC sharing between CM and SM • IPv6 support for Commercial and Federal markets • Assured Services SIP
Operational Improvements	• Update to RHEL 7 • ESXi 6.5 Support
Ease of Use	• Support VE and AVP upgrades to 7.1 using SDM. • WebLM Upgrade Workflow Simplification eliminates need to re-host licenses during upgrade.

Fixes in Session Manager Release 7.1.x.x

Fixes in Session Manager Release 7.1

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-60005	[RHSA-2016:2079-01] java-1.8.0-openjdk security update	N/A	N/A
ASM-54034	Oracle Java Critical Patch Update (October 2015)	N/A	N/A
ASM-351	[RHSA-2015:0863-01] glibc security and bug fix update	N/A	N/A
ASM-318	[RHSA-2015:0794-01] Moderate: krb5 security update	N/A	N/A
ASM-400	[RHSA-2015:1081-2] Important: kernel security and bug fix update	N/A	N/A
ASM-58918	[RHSA-2016:1664-01] Important: kernel security and bug fix update	N/A	N/A
ASM-58916	[RHSA-2016:1626-01] Moderate: python security update	N/A	N/A
ASM-59501	[RHSA-2016:1944-01] Important: bind security update	N/A	N/A
ASM-60665	[RHSA-2016:2824-01] Moderate: expat security update	N/A	N/A
ASM-60011	[RHSA-2016:2702-01] Important: policycoreutils security update	N/A	N/A
ASM-60765	[RHSA-2016:2972-01] Moderate: vim security update	N/A	N/A
ASM-61591	[RHSA-2017:0063-01] Important: bind security update	N/A	N/A
ASM-61594	[RHSA-2017:0252-01] Moderate: ntp security update	N/A	N/A
ASM-60764	[RHSA-2017:0036] Important: kernel security and bug fix update	N/A	N/A
ASM-60014	[RHSA-2016:2779-01] Moderate: nss and nss-util security update	N/A	N/A
ASM-59502	[RHSA-2016:1940-01] Important: openssl security update	N/A	N/A
ASM-56237	[RHSA-2016:0494-01] Moderate: kernel security, bug fix, and enhancement update	N/A	N/A

Known issues and workarounds in Session Manager 7.1.x.x

Known issues and workarounds in Session Manager Release 7.1

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

ID	Minimum conditions	Visible symptoms	Workaround
N/A	Breeze interop	Breeze 3.3 or later is required if Session Manager 7.1 IPv6 features are to be enabled. Failure to ensure this will result in Breeze nodes becoming unusable.	N/A
N/A	Third party certificates	Any pre-6.3 Session Manager using third party identity certificates will need to have those certificates re-administered after upgrading to SM 7.1. Third party trusted certificates will be preserved. No action is required for pre-6.3 SM's using default identity certificates. Refer to Session Manager Administration guide for details on configuring third party certificates.	N/A

Avaya Aura® System Manager

Installation for System Manager 7.1

Required artifacts for System Manager Release 7.1

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

Download ID	Artifact	Notes
SMGR71GA001	Avaya Aura System Manager 7.1 OVA	Verify that the md5sum for the downloaded OVA image matches the number on the Avaya PLDS website. SMGR-7.1.0.0.1125193-e65-50.ova Size: 2.90 GB Md5sum: da29c8fe0e22579823ed6d6ed84fbe67
SMGR71GA002	Avaya Aura System Manager 7.1 High Capacity (Profile 3) OVA	Verify that the md5sum for the downloaded OVA image matches the number on the Avaya PLDS website. SMGR-PROFILE3-7.1.0.0.1125193-e65-50.ova Size: 2.92 GB Md5sum: 4232aaf1cf83e94e78f63447a9a503bb
SMGR71GA004	SDM Client for System Manager 7.1	Verify that the md5sum for the downloaded zip image matches the number on the Avaya PLDS website. Avaya_SDMClient_win64_7.1.0.0.1125684_45.zip Size:227 MB Md5sum: c9e6881f796795d31a0bac8a7cd8b099
SMGR71GA006	System Manager 7.1 Mandatory Patch bin file Post OVA deployment / Data Migration	Verify that the md5sum for the downloaded bin image matches the number on the Avaya PLDS website. System_Manager_R7.1_r710006654_mandatoryPatch.bin Size: 730MB Md5sum: 38d40925fe14e3b070bac629241c8061
SMGR71GA007	System Manager 7.1 GA Patch 1 for Breeze 3.3	Verify that the md5sum for the downloaded Bin image matches the number on the Avaya PLDS website. SystemManagerPatchForBreeze3.3_r710006662.bin Size:91MB Md5sum: 71032939ce7e1dfaae72236314a66bf5
SMGR71AWS01	Avaya Aura System Manager 7.1 Amazon Web Service OVA	Verify that the md5sum for the downloaded OVA image matches the number on the Avaya PLDS website. SMGR-7.1.0.0.1125193-aws-50.ova Size: 2.90 GB Md5sum: 80e45c700f6acf10a994b4f18a3b298f

Download ID	Artifact	Notes
SMGR71AWS02	Avaya Aura System Manager 7.1 Amazon Web Service Profile-3 (High Capacity) OVA	Verify that the md5sum for the downloaded OVA image matches the number on the Avaya PLDS website. SMGR-PROFILE3-7.1.0.0.1125193-aws-50.ova Size: 2.92 GB Md5sum: ad6654b9b75a60c9fdd271f198392b95

Note: To leverage deployment via Service Port using SDM client, get the Solution Deployment Manager client software from Avaya support site. The Solution Deployment Manager 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, 6.3.x and 7.0.x Ensure that you run the data migration utility only on 7.1 release. Refer to the document Upgrading Avaya Aura® System Manager to Release 7.1 for more details.

Download ID	Artifact	Notes
SMGR71GA005	Data Migration utility for System Manager 7.1	datamigration-144.bin Size: 1.79 MB MD5SUM: 20cc18b7594600d5ae50243427ac9170

What's new in System Manager R7.1

This Release Notes document provides information about new features, installation downloads, and the documentation of Avaya Aura® System Manager 7.1 on VMware. This document also contains information about known issues and the possible workarounds.

This document provides information about System Manager 7.1 Release deliverables which includes System Manager 7.1 VMWare OVA, 7.1 Data Migration Utility and Solution Deployment Manager (SOLUTION DEPLOYMENT MANAGER) Client.

Some product changes are documented as Product Support Notice (PSN). The PSN number defines the related document.

Enhancements delivered to System Manager 7.1:

Enhancement	Keywords
• Moved base operating system to RHEL 7.2 • Updated to OpenJDK 1.8.0.Update 121 • Updated the PostgreSQL database version to 9.6	Infrastructure and Serviceability Updates

Enhancement	Keywords
• VMware ESXi Versions 5.5, 6.0 and 6.5. • AVP 7.1 • Browsers Supported: Firefox Versions 48,49,50 and IE 11 • 7.1 System Manager IPv6 Support [Dual stack Network] • EASG login	
Support for installing System Manager 7.1 OVA on the Appliance Virtualization Platform (AVP) that is being introduced in Avaya Aura 7 as part of the Avaya Provided Appliance. System Manager 7.1 OVA installation on AVP 7.0 is not supported.	Avaya Appliance
User management includes following new features: • Login Password Policies • Communication Profile Password Polices • Generate and Email Password • Multitenancy support for User synchronization using LDAP [User can select Tenant information in User Provisioning Rule]. • Support for maximum of 25 concurrent admin logins [Default is 5]. • Bulk import and export of excel and xml for the Equinox communication profile. • User Management web service support for Equinox communication profile.	User Management
Solution Deployment Manager provides a centralized software management solution in System Manager. SDM can support deployments, migrations, upgrades, and updates to the suite of Avaya Aura 7.1 applications. System Manager Solution Deployment Manager will support Migration/Upgrade [VMWare7.0.x to VMWare7.1 Upgrade] for following products. • Session Manager (SM) • Branch Session Manager (BSM) • Application Enablement Service (AES) [Sprint-10] • Utility Services (US) • Communications Manager (CM) • CM Messaging (CMM) • WebLM	Solution Deployment Manager (Solution Deployment Manager)
• Supports same Web Browsers as System Manager 7.1. • Supports Tomcat Server (8.0.18) • AVP Upgrade from 7.0.x to 7.1 Using Solution Deployment Manager Client/Central Solution Deployment Manager. • System Manager Upgrade to 7.1 from 6.x System Platform based System Manager. • System Manager VMWare to VMWare Upgrade support [System Manager 7.0.x to	Solution Deployment Manager Client

Enhancement	Keywords
System Manager 7.1] Same Box Migration. • Configure and push/delete syslog profiles on AVP • Configure and push/delete syslog profiles on System Manager and SM. • AVP Kick start file • Retaining host id while doing System Manager upgrade from 7.0.x to 7.1 release from Solution Deployment Manager client.	
Clients can also use certificate based authentication while invoking the web services.	Secured Web Services
System Manger 7.1 now supports login for User Interface and Command Line Interface using certificate.	Certificate based login for User Interface and SSH
System Manager 7.1 Supports the following Certificate Management features: • Support for Revocation checking. • As a CA support for OCSP and CRL • Global Configuration for TLS version. • Mutual authentication configuration • Support for scheduled CRL download from external CRL distribution point	Certificate Management
• System Manager 7.1 includes support for Syslog forwarding to Remote Syslog server. • Certificate based Syslog forwarding is also supported.	RSyslog Support
System Manager 7.1 introduces the ability to separate management and non-management with OOBM feature over IPv6 address	Out-of-Band Management[OOBM]
System Manger 7.1 now supports Audit log configuration	Audit Log Configuration
System Manager 7.1 includes support for Geo Configuration with IPv6 address.	Geo Configuration over IPv6
Included New Command Line Interface based user creation during System Manager Deployment	New Customer CLI Login

Software information:

Software	Version	Note
Postgres	9.6	Used as a System Manager database. For more information, see: https://www.postgresql.org/docs/9.6/static/index.html
Red Hat	7.2 64 bit	Used as the operating system for the System Manager template
Open JDK	1.8 update 121 64 bit	For Solution Deployment Manager Client, Open JDK 1.8.0-internal
JBoss	6.1	

Software	Version	Note
Internet Explorer	11.x	Earlier versions of Internet explorer are no longer supported.
Firefox	48,49,50	Earlier versions of Firefox are no longer supported.
VMware vCenter Server, vSphere Client, ESXi Host, VMware Web Client	5.5,6.0,6.5	6.5 has some issue from VMware side.

Must read:

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

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

2. Perform the following steps to enable EASG on System Manager 7.1.
   - To enable EASG on SYSTEM MANAGER via Command Line Interface via Cust user type the following command:
     `# EASGManage --enableEASG`
   - To disable the EASG on SYSTEM MANAGER type the following command:
     `# EASGManage –disableEASG`

3. For VMWare to VE System Manager upgrade, remove all the snapshot from old VMWare System Manager otherwise rollback operation will fail.
4. The versions*.xml is published on ftp://ftp.avaya.com/incoming/Up1cku9/tsoweb/SUM/

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

1. Log in to the PLDS at https://plds.avaya.com.
2. From the Assets menu, select View Entitlements.
3. In the Application field, select System Manager.
4. Do one of the following:
   - To search using group ID, in the Group ID field, enter the appropriate group ID.
     Note: All group IDs are numeric without any leading zeros.
   - To search using the SAP order number, click Advanced Search, and in the Sales/Contract # field, enter the SAP order number.
5. Click Search Entitlements.
   The system displays the LAC(s) in the search results.

Troubleshooting the installation

Execute following command from System Manager Command Line Interface 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.

Fixes in System Manager 7.1

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-40445	Elements Management	UCM elements pages takes a very long time to load and cs1k registration also taking a very long time	7.0.1
SMGR-38481	Authorization	Insufficient authorization checks allow privilege escalation for Auditor to become administrator.	7.0.1
SMGR-38480	Authorization	Password sent in clear text for External Identity Repository (LDAP).	7.0.1
SMGR-40356	Alarm Management	AU_IPT00060 Alarm is getting raised in-spite of System Manager able to pool required number connections from communication manager	7.0.1
SMGR-39423	Alarm Management	CPU system monitor is not alarming based on proper messages	7.0.1
SMGR-40193	Web Service Management	System Manager User Management Web service performance improvements.	7.0.1.2
SMGR-39663	Import and Export Management	Bulk delete of users using Excel or XML import terminates without processing other records if the list contains a user which does not exist in System Manager.	7.0.1.2
SMGR-39189	Import and Export Management	Change the temp location where files are stored during bulk import / export operation.	7.0.1.2
SMGR-38971	User Management	The advanced search under the “AND/OR” function does not work with multiple E164 handle values.	7.0.1.2
SMGR-38638	User Management	In following cases, user list does not show in user management page for the logged in user, if logged in user is associated with custom role having permission on users: If logged in user is authenticated against external server, if the User Principal Name value in external server contains upper case characters. While logging into System Manager, if the login name is entered in upper case for locally authenticated users.	6.3.16
SMGR-38071	User	Translation is not happening correctly for First and last name	6.3.17

ID	Minimum Conditions	Visible symptoms	Release introduced
	Management	having Umlaut characters (ä, ö, ü, ß).	
SMGR-39285	Directory Synchronization	User(s) always shows as modified in Sync summary if prefix + is not present in AD for phone number value	7.0.1.1
SMGR-39388	Directory Synchronization	Users get updated after each sync if DSE mapping mandatory attributes gets empty once user gets created in System Manager.	6.3.18
SMGR-39202	Role Management	if accessed from security – roles link present on right pane Roles page opened one is legacy structured page i.e. page is in table format instead of tree structure format.	6.3.18
SMGR-40337	Software Upgrade Management	Sort fields option is not working for Home / Services / Solution Deployment Manager / VM Management -> Virtual machine	7.0.1.2
SMGR-40249	Communication Manager Management	User unable to see available extensions in-spite of availability in some scenarios.	6.3.17
SMGR-40123	Communication Manager Management	Template name size increased to 100 and also size is consistent across new, duplicate and upgrade operations for template.	7.0.1.2
SMGR-39772	Communication Manager Management	User having customer unable to edit station, user gets below error during edit operation: “The endpoint "xxxx" could not be edited. Cause of failure: button no.1 At least 1 call-appearance is required when IP SoftPhone is 'y'."	6.3.12
SMGR-38057	Communication Manager Management	The message lamp extension provided in the template is not taken when using that template to create an extension.	7.0.1
SMGR-39561	Global Search Component	User having custom role unable to view extensions from global search component if user associated multiple roles are having permission on same CM across different extension ranges.	6.3.7
SMGR-37796	Global Search Component	Admin user cannot edit/view/delete a user via global search component if user contains special(Umlaut) German chars in surname/first name/localized display name	7.0.1
SMGR-39532	Report Management	Qualifier value is missing in list history report	7.0.1.2

Known issues and workarounds in System Manager on VMWare in Release 7.1

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

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-40680	SDM Client	Solution Deployment Manager-Client: Upgrade and Deployment fails as SMGR allows keeping VM name more than 80 characters (during fresh deploy and upgrade).	Rename the vm name
SMGR-40660	Solution Deployment Manager Client	Upgrade failed on one System Manager, if upgrade started concurrently on 2 or more systems from same Solution Deployment Manager-Client and same system.	Do the System Manager upgrade in an hour gap.
SMGR-40659	Solution Deployment Manager Client	During upgrade if auto-commit of patch fails, then user is unable to commit the patch again manually.	
SMGR-40716	Solution Deployment Manager Client	Upgrade stops responding at backup process.	
CM-15872	SMGR - Software Upgrade Management	Solution Deployment Manager SUM: CM R7.0.1.2 trust failed from System Manager R7.1 S11 P27 Solution Deployment Manager-SUM if it is deployed from vSphere client.	
SMGR-40239	SMGR - Software Upgrade Management	Browse for VM –Management not supported on IE11 on System Manager-Solution Deployment Manager.	User the supported Firefox browser for this use case.
SMGR-40389	System Manager - Software Upgrade Management	Generate AVP Kickstart File feature not supported on IE11 on System Manager-Solution Deployment Manager.	User the supported Firefox browser for this use case.
SMGR-40684	Software Upgrade Management	Ability to start 2 upgrades simultaneously, with same ova URL.	Do the use the “URL” option. Either use URL option once and Upgrade the second system after that (using any option); or use s/w library option for triggering simultaneous Upgrades of 2 System Manager's to the same version.

ID	Minimum conditions	Visible symptoms	Workaround
SDM-1267	Solution Deployment Manager Client	After installing patch on System Manager, using Solution Deployment Manager client, the status is not updating, and hence the user is unable to commit or rollback	User should click on 'Update VM' (this button is to install new Patch). 'Update VM' gets the latest patch State and if the patch is not committed will show commit/rollback option. User can then perform necessary action
SMGR-40602	User Management	Time zone value associated with user (identity page) not getting populated properly after DST change.	Restart JBoss service
SMGR-39710	User Management	Updating users through “Home / Users / User Management / Manage Users -> More Actions - > Bulk edit users” does not update Session Manager Profile data in some scenarios.	Changing single value is not getting updated so if user want to update Secondary Session Manager only in this case, they need to select multiple entries i.e. Primary (they need to explicitly select SM value instead of “use existing value” in dropdown, if needed they can keep the old value) and secondary server (new value) so that secondary Session Manager entry gets updated after operation.
SMGR-40508	Directory Synchronization	Apostrophe in the data-source name will cause issues later.	Do not provide Apostrophe in the data-source name.
SMGR-40390	Software Deployment Management	Company ID under user settings (Home / Services / Solution Deployment Manager / User Settings) gets blank from after the upgrade.	Provide value for Company ID under user settings (Home / Services / Solution Deployment Manager / User Settings) and save the value.
SMGR-39977	Report Management	Report settings in configurations (Home / Services / Configurations / Settings / Reports / Configuration) are reverted back to default after System Manager Upgrade.	After upgrade, change the values as present prior to upgrade.

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-39711	Backup and Restore	After Restore earlier scheduled backup job is getting disabled.	Enable the scheduled backup.
SMGR-4071	Rsyslog	Rsyslog and IPV6: incorrect GUI message displayed (failed to push) while pushing messages to rsyslog server.	
SMGR-40718	Rsyslog	Incorrect GUI message displayed (failed to delete) while deleting messages from rsyslog server.	

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

Solution Deployment Manager Adopter Matrix	**Adopting Product (System Manager Release 7.1)**												
System Manager Solution Deployment Manager - 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
	[Other than System Manager hosting AVP]												
Automated Migrations R7.x to R7.1 (analysis and pre-upgrade checks) [Target Platform: AVP / customer VMWare]	Y	Y	Y	Y	n/a [Covered as Firmware Updates]	Y	Y	Y	N (Breeze Upgrade Supported from Breeze 3.3 Onwards)	N	Y	Y	N
Automated Migrations R6.x to R7.0/7.1 (analysis and pre-upgrade checks)	n/a	N	Y1	Y	n/a [Covered as Firmware Updates]	Y	Y	Y	N	N	N	N	N
Automated Migrations R6.x to 7.0.0.x/ 7.0.x/7.1	n/a	N	Y[1]	Y	n/a [Covered	Y	Y	Y	N	N	N	N	N

Solution Deployment Manager Adopter Matrix	**Adopting Product (System Manager Release 7.1)**												
System Manager Solution Deployment Manager - 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
[Source Platform: System Platform]			[Bare Metal which is not on SP]		as Firmware Updates]								
[Target Platform: AVP / customer VMWare]													
Automated Migrations R6.x to 7.0.x/7.1			Y[1]										
[Source Platform: System Platform]	n/a	N	[Bare Metal which is not on SP]	Y	n/a [Covered as Firmware Updates]	Y	Y	Y	N	N	N	N	N
[Target Platform: AVP / customer VMWare]													
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
Solution Deployment Manager RBAC	n/a	Y	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Solution Deployment Manager Adopter Matrix	Adopting Product (System Manager Release 7.1)												
System Manager Solution Deployment Manager - 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
Available													
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

VMWare: Virtualized Environment

The following section provides **Solution Deployment Manager Client feature** information.

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

Deployment and Upgrade Guides:

Products	Deployment and Upgrade Guides
Appliance Virtualization Platform	Migrating and Installing Appliance Virtualization Platform (Release 7.1)
Session Manager	Deploying Avaya Aura® Session Manager (Release 7.1) Upgrading Avaya Aura® Session Manager (Release 7.1)
Communication Manager	Deploying Avaya Aura® Communication Manager (Release 7.1) Upgrading Avaya Aura® Communication Manager (Release 7.1)
CM Adjuncts (MM, TN Boards, Gateways)	Deploying and Upgrading G430 Branch Gateways (Release 7.1) Deploying and Upgrading G450 Branch Gateways (Release 7.1)
Branch Session Manager	Deploying Avaya Aura® Branch Session Manager (Release 7.1)
Utility Services	Deploying Avaya Aura® Utility Services (Release 7.1)
CM Messaging	Deploying Avaya Aura® Communication Manager Messaging (Release 7.1)
Breeze (w/ Presence Snap-in)	Deploying Avaya Breeze™ (Release 3.1) Quick start guide for Deploying Avaya Breeze™ 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 7.1)
Avaya Aura Solution using Solution Deployment Manager and Solution Deployment Manager Client	
Avaya Aura® System Manager Solution Deployment Manager Job-Aid	
Deploying Avaya Aura® applications for deploying Aura applications using System Manager Solution Deployment Manager (Solution Deployment Manager) and Solution Deployment Manager – Client (Solution Deployment Manager-Client)	
Upgrading Avaya Aura® applications to Release 7.1 for upgrading Aura applications using Solution Deployment Manager (Solution Deployment Manager)	
Upgrading Avaya Aura® applications to Release 7.1 for upgrading Aura applications using the Solution Deployment Manager Client	

Avaya Aura® Presence Services

Installation for Avaya Aura® Presence Services 7.1.x.x

Required patches for Presence Services 7.1.0.0

Patches in 7.1 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 7.1.0.0

Filename	Modification time stamp	File size	Version number
PresenceServices-Bundle-7.1.0.0.451.zip **(PLDS ID PS070100000)**		165 MB	PresenceServices-7.1.0.0.584.svar

Installing the release

Refer to chapters 5and 6 of the customer documentation for instructions related to the deployment of the PS 7.1.0.0 release.

Troubleshooting the installation

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

Restoring software to previous version

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

Backing up the software

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

Migrating to the PS 7.1 release from a PS 6.2.X release

Changes Affecting Migrations to 7.1

Avaya Aura® Presence Services 7.X introduces significant changes that affect migrations to PS 7.1:

- **For instructions on how to perform the migration, refer to the documentation bundled with the Migration tool found in PLDS**
- 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 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 Engagement Development Platform. If migrating users from pre-PS 7.0.0.0 to PS 7.1.0.0, the Presence Profile for those users must be updated.
- 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 7.1. Applications must use the Presence Services 7.1 compatible LPS client. This includes:
    - Avaya one-X Client Enablement Services
    - Avaya one-X Attendant
- All presence-related configuration on Avaya Aura® System Manager will be migrated automatically when System Manager is upgraded to release 7.1 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 7.1.
- The migration script must be run as part of the migration of existing PS 6.2.X users to PS 7.1. The migration script can be downloaded from the Avaya Support site (PLDS ID = PS070000001).

  In order to run Presence Services 7.1.0.0, migrations should be performed using the following method:

  - Presence Services 7.1 Snap-in on Breeze 3.3:

Download and install the Avaya Aura Presence Services 7.1.0.0 Software (PS-7.1.0.0.584.svar) on a Breeze 3.3 Core cluster.

Note: At the time general availability of Presence Services 7.1.0.0 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 7.1.0.0 deployments.

Migrations to release 7.1.0.0 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)
Avaya Aura® Presence Services 6.2 Service Pack 7	PS-6.2.7.6-58 + any additional patch(es)

Upgrade References to Presence Services 7.1.0.0

Upgrade Quick Reference	Download	Prerequisite Downloads
Presence Services Customer Documentation	PresenceServices-Bundle-7.1.0.0.451.zip (PLDS ID: PS070100000)	**Breeze 3.3 Platform OVA – PS 7.1 is only compatible with Breeze 3.3 and newer platform loads.**

Interoperability and requirements/Applicability

Presence Services 7.1 is compatible with the following applications.

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

The following table lists the compatibility changes in this release.

Application	Certified version	Minimum supported version	Mandatory/Optional
Avaya Breeze Platform	3.3	3.3	M
Avaya Aura® System Manager	7.1.0.0	7.1.0.0	M
Avaya Aura® Session Manager	7.1.0.0	7.1.0.0	M
Avaya Aura® Communication Manager	7.1.0.0	7.0.0.0	O
Avaya Appliance Virtualization Platform	7.1.0.0	7.0.0.0	O
Avaya Aura® Application Enablement Services	7.1.0.0	7.0.0.0	O
Avaya Multimedia Messaging	3.0.0.0	3.0.0.0	O
Avaya one-X® Client Enablement Services	6.2.5 + Patch 3	6.2.5 + Patch 3	O

Application	Certified version	Minimum supported version	Mandatory/Optional
IBM® Domino®	9.0.1	8.5.3	O
Microsoft Lync®	Lync 2013	Lync 2010	O
Microsoft Exchange	Exchange 2013	Exchange 2010 SP1	O
Microsoft Skype for Business	6.0.9319.0	6.0.9319.0	O
Avaya Session Border Controller for Enterprise	7.1.0.1-07-12030	7.1.0.1-07-12030	O

Software Development Kit

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

SDK File name	SDK Version	Presence Services Compatibility
PresenceServices-LPS-SDK-7.1.0.0.556.zip	7.1	PS 7.1 and PS 7.0.1
PresenceServices-LPS-SDK-7.0.1.0.855.zip	7.0.1	PS 7.1 and PS 7.0.1

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

Functionality not supported in Presence Services 7.1.x.x

Avaya Multimedia Messaging (AMM 2.1) XMPP federation is not supported in Presence services 7.X. AMM 3.0 supports REST-based integration and is fully compatible with Presence services 7.0.1 and above.

What's new in Presence Services 7.1.x.x

What's new in Presence Services Release 7.1

The following table lists enhancements in this release:

Enhancement	Description
Support for federation with Microsoft Skype for Business	PS 7.1 now supports federation with on premise Microsoft Skype for Business for both Presence and Instant Messaging. This feature is applicable to both Inter and Intra enterprise solutions. (Note that federation with cloud based Microsoft Skype for Business is not supported).
Rest interface for Web clients	The PS 7.1 release introduces a new REST based interface which will allow customers to develop their own web clients which can interface with PS. Customer developed Web clients will be able to Get, Set, and Subscribe for presence as well as Send and Receive IMs.
Instant Message and Presence federation with Nextplane	PS 7.1 now supports federation with Nextplane for both Presence and Instant Messaging. Federation with Nextplane opens up a lot of different options for interacting with external enterprises,
Support for IM broadcasts via the new REST interface	As part of the new Rest interface PS 7.1 a new broadcast function was added which allows users to broadcast IMs to all other users on the system. The ability for a given user to broadcast IMs to all other system user users (or a subset of users) is enabled via a service attribute which the system administrator must set. The default is disabled.

Enhancement	Description
Option to allow the exchange of Presence and IMs between tenants when ITCC is enabled.	In previous releases of PS if the Inter Tenant Communication Control feature was enabled the exchange of Presence and IMs between users with different tenant IDs was blocked. In PS 7.1 a system attribute was added which allows the system administrator to allow the exchange of Presence and IMs between users with different tenant IDs when the ITCC feature is enabled.
Option to allow administrators to set user roster limits on a per user basis.	In previous releases of PS the system administrator was only able to set roster limits on a system wide basis. In release 7.1 the system administrator is able to set roster limits on a per user basis.
Enabling ITCC support in SYSTEM MANAGER for Presence Services Elements	Supports Presence Services Communication Profiles with User Provisioning Rules when ITCC is enabled. Supports selecting Presence Services elements in ITCC management.

Fixes in Presence Services 7.1.x.x

Fixes in Release 7.1

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 7.1.0.0 release:

ID	Minimum conditions	Visible symptoms	Release found in
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.	7.0.0.0
PSNG-3807	A network outage (ex. cable disconnect) occurs.	At times Presence Service will not recover from a network connection interruption	7.0.0.0
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,	7.0.0.0
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	7.0.0.0

ID	Minimum conditions	Visible symptoms	Release found in
		to provide service.	
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 and 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.	7.0.0.0
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.	7.0.0.0
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".	7.0.0.0
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.	7.0.0.0
PSNG-1184	PS on Breeze Element Manager Provisioning - Breeze 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.	7.0.0.0

Known issues and workarounds in Presence Services 7.1.x.x

Known issues and workarounds in Release 7.1

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

ID	Minimum conditions	Visible symptoms	Workaround
PSNG-4101	PS federated with Avaya Multimedia Messaging (AMM)	AMM inter-op doesn't work with PS REST APIs, the PS LPS, or the PSConnector. It currently works only for XMPP IM clients.	There is no work-around for this issue. This issue will be addressed in a subsequent release of the PS software.
PSNG-4085	PS REST interface used	When using the REST interface on PS you should not use ON_A_CALL as a manual state. The ON_A_CALL can be used as a manual presence state in the REST API due to the JSON schema definition, but it is actually not a valid manual state from PS availability-calculate perspective, and therefore should not be used in this way. ON_A_CALL can only be used as a video/phone-channel state	There is no work-around for this issue.
PSNG-4079	Delete a PS element in SMGR it reports an error	When attempting to delete a PS element in SMGR it reports the error that "unable to delete an element that is assigned to a user", however the element is only assigned to a UPR.	The work around is to manually remove the PS element from UPR. This issue will be addressed in a subsequent release of the PS software.
PSNG-4069	presGSql core dumps selecting too many objects	When viewing some objects in the presGSql tool, it may core dump as there are too many objects to list.	There is no work-around for this issue. This issue will be addressed in a subsequent release of the PS software.
PSNG-2630	Avaya Aura is federated with Microsoft Lync	There is no message notification when Lync sends chat message to 1XC in DND state,	There is no work-around for this issue.
PSNG-1379	Clear Logs in the EDP EM for Presence Services does not clear logs	The “Clear Logs” button on the EDP EM does not have any effect on the ps.log file.	There is no workaround for this issue.
Note		After an Avaya contact is removed from a XMPP federated client, presence does not render if the Avaya contact is re-added to the federated user.	Use either of the two solutions: 1. Toggle the favorite flag for the federated user in the Avaya client 2. Logout and log back in to the Avaya client

Avaya Aura® Application Enablement Services

Installation for Avaya Aura® Application Enablement Services Release 7.1.x.x

Backing up the AE Services software

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

1. Log into the AE Services Management Console using a browser.
2. From the main menu, select Maintenance | Server Data | Backup. AE Services backs up the database, and displays the Database Backup screen, that displays the following message: The backup file can be downloaded from Here.
3. Click the "Here" link. A file download dialog box is displayed, that allows you to either open or save the backup file (named as: serverName_rSoftwareVersion_mvapdbddmmyyyy.tar.gz, where ddmmyyyy is a date stamp).
4. Click Save, and download the backup file to a safe location that the upgrade will not affect. For example, save the file to your local computer or another computer used for storing backups

Interoperability and requirements

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

Installation for Avaya Aura® Application Enablement Services Release 7.1

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:

- Migrating and Installing Avaya Appliance Virtualization Platform
- Release Notes for Avaya Appliance Virtualization Platform Release 7.1
- Deploying Avaya Aura® Utility Services in Virtualized Environment
- Release Notes for Avaya Aura® Utility Services Release 7.1
- Deploying Avaya Aura® applications Release 7.1
- Upgrading and Migrating Avaya Aura® applications Release 7.1

Note: For Communication Manager 7.1, AE Services 7.0.1 or later is required for DMCC first-party call control (1PCC) applications. DMCC 1PCC station registrations will fail when using Communication Manager 7.1 with AE Services 7.0 or earlier versions. When upgrading to Avaya Aura 7.1, it is recommended to upgrade AE Services server before upgrading Communication Manager.

In AE Services 7.1, 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 or earlier) that are using TLS to fail to establish a secure socket connection to the AE Services 7.1 server. In order to achieve a more secure client/server socket connection, we encourage current client applications to use an AE Services 7.0 or later SDK where the TLS 1.2 protocol is supported. Note, the initial released AE Services 7.0 Windows TSAPI client (tsapi-client-win32) did not initially support TLS 1.2 and has been updated to support TLS 1.2. All the latest versions of the AE Services 7.1

SDKs support TLS 1.2. If upgrading to AE Services 7.1 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 7.1 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 7.1, any customer application relying on the old, Avaya provided server certificate for TLS will not be able to connect to the AE Services 7.1 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 7.1 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 7.1 Administration and Maintenance document

  *** See the OpenSSL section in the AE Services 7.1 Administration and Maintenance document.

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

Upgrading to AE Services 7.1

AE Services Server Upgrade Instructions

Note: For an AE Service 7.0.1 VMware offer upgrade to AE Service 7.1 VMware offer using SDM, see Chapter 7 in the document "Deploying Avaya Aura® Application Enablement Services in Virtualized Environment"

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

- Using the AE Services patch process, install the pre-upgrade patch on your existing AE Services server.

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

  AES7_PreUpgradePatch addresses the following issues:

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

4. Using the AE Services Management Console web page, note the configuration values for the following items on the specified web pages:
   - External LDAP checkbox setting on “Security > PAM > PAM Password Manager”
   - PAM MOTD checkbox setting on “Security > PAM > PAM MOTD”
   - Session Timeout values on “Security > Session Timeouts”
   - Product ID value on “Utilities > Product ID”
5. Take a backup of the AE Services server data. Refer to the topic “Backing up the AE Services software”
6. Download the backup file to a safe location that the upgrade will not affect.
7. Note the AE Services server hostname and IP address, and shutdown system.
8. Install AE Services 7.1. See below sections for each platform.
9. Use the AE Services 7.1 Management Console web page “Maintenance > Server Data > Restore” to restore previously backup data.

   Note: When using the AE Services 7.1 Management Console to perform a restore, the “Restart Services Confirmation” page may be displayed again after the restore completes. In order to determine if a restore failed and is still pending, select the Restore link again (i.e. Maintenance > Server Data > Restore). If a Browser textbox is displayed the restore has completed. If the message “A database restore is pending” is displayed, the restore failed to complete.

10. Using the AE Services 7.1 Management Console, verify and update the values recorded in step 4 on the AE Services 7.1 server.

Restoring AE Services software to previous version

Use the AE Services 7.1 Management Console web page “Maintenance > Server Data > Restore” to restore any backup data.

Note: If the backup is from AE Services version 6.3.3 SP3 or earlier, verify the pre-upgrade patch, "AES7_PreUpgradePatch.bin", in Step 3 in the topic “Upgrading to AE Services 7.1” was executed before the previous backup was taken.

Note: When using the AE Services 7.1 Management Console to perform a restore, the “Restart Services Confirmation” page may be displayed again after the restore completes. In order to determine if a restore failed and is still pending, select the Restore link again (i.e. Maintenance > Server Data > Restore). If a Browser

textbox is displayed the restore has completed. If the message “A database restore is pending” is displayed, the restore failed to complete.

Installation for Avaya Aura® Application Enablement Services Software Only 7.1

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

Install Avaya Aura® Application Enablement Services Software Only 7.1 (swonly-7.1.0.0.0.17-20170418.iso).

Installation steps for Avaya Aura® Application Enablement Services 7.1 Aura® OVA Media

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

Install Avaya Aura® AE Services 7.1 Aura® OVA Media (AES-7.1.0.0.0.17.20170418-e51-00.ova)

Functionality not supported

- AE Services 7.1 does not support the “Bundled” and “System Platform” offers. Customers upgrading to AE Services 7.1 must switch to the “Software-Only” offer or “VMware” (AE Services on AVP) offer.
- In AE Services 7.1, the Machine Preserving High Availability (MPHA) (aka VSST) feature is not available.

What’s new in Application Enablement Services 7.1.x.x

What’s new in Application Enablement Services 7.1

The following table lists enhancements in this release.

Feature	Description
RedHat 7	AE Services is now based on RedHat Enterprise Linux 7.2 64-bit
OVA Signing	The AE Services 7.1 Open Virtualization Archive (OVA) is supplied as a signed image.
EASG	Enhanced ASG is now used in AE Services 7.1. Disabling EASG is possible with configuration change.
VMware ESXi 6.5	AE Services 7.1 supports VMware ESXi 6.5.
TSAPI client for MS Windows 10 and Windows Server 2016 standard edition	TSAPI applications which were built in previous MS Windows version can run on MS Windows 10 and Windows Server 2016 standard edition. Note that TSAPI application is supported in binary compatible mode in MS Windows 10 and Windows Server 2016 standard edition. Compiling TSAPI application in MS Windows 10 or Windows Server 2016 standard edition is not supported yet and will be supported in later release.
Increase ASAI notification	Increase ASAI Notifications from 32K to 50K in CM 7.1. This enhancement would be limited only in CM 7.1 so that CM 7.1 can support up to 50K ASAI event notification and handle 50K domain control association. However, the limit on AE Services is the same as before and it would be limited to 32K per CM. Even though one AE Services server is limited to 32K per CM, it is possible to support 50K when multiple AE Services servers are connect to a CM. Also when multiple CMs are connected to one AE Services server, One AE Services server can support more than 32K. The 32K limitation is for

Feature	Description
	single AE Services server per CM."
Increase Active Control Association	Increase domain control association from 32K to 50K in CM 7.1. This enhancement would be limited only in CM 7.1 so that CM 7.1 can support up to 50K ASAI event notification and handle 50K domain control association. However, the limit on AE Service server is the same as before and it would be limited to 32K per CM. Even though one AE Services is limited to 32K per CM, it is possible to support 50K when multiple AE Services servers are connect to a CM. Also when multiple CMs are connected to one AE Service server, one AE Services server can support more than 32K. The 32K limitation is for single AE Services server per CM."
VM foot print increase	AE Services 7.1 requires more memory and 2 G additional memory is required for all foot prints. See foot print sizes in the section "VM foot print sizes"
License Preservation and AE Services upgrade from System Manager SDM.	AE Services 7.0.1 can be upgraded to AE Services 7.1 using SDM. In this case, the license file is preserved.

VM Foot Print Size and capacity

Note: The requirements for RAM and HDD have been increased in AE Services server 7.1.

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

Enhanced Access Security Gateway (EASG)

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

Changes and Issues

Issues related to Backup and Restore

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

- External LDAP checkbox setting on “Security > PAM > PAM Password Manager”
- PAM MOTD checkbox setting on “Security > PAM > PAM MOTD”
- Session Timeout values on “Security > Session Timeouts”
- Product ID value on “Utilities > Product ID”

Upgrading issues related to licenses and the AE Services 7.1 embedded WebLM server

- An AE Services 7.0.1 VMware offer type upgrade to an AE Services 7.1 VMware offer type will require the customer to obtain a new license file as the WebLM HostID will change. However, if SDM and AVP are used to perform the upgrade, the AE Services embedded WebLM HostID will be preserved and a new license will not be required.
- For an AE Services 7.0.1 SW Only upgrade to AE Services 7.1 SW Only, a new license is not required and will be restored using the AE Services 7.0.1 SW Only backup data. This only works when the AE Services 7.0.1 SW Only platform is not deployed in a virtual environment, the same bare metal server is used and a backup of the server is taken before the upgrade process starts.
- When upgrading from AE Services 7.0.1 to AE Services 7.1, some customers using the AE Services embedded WebLM server may have to obtain a new license file. For this scenario, customers must use the new WebLM 7.1 HostID as displayed on the WebLM server web page. The previous WebLM HostID in PLDS will not be able to be reused.
- If a customer wants to increase the number of licenses for an AE Services 7.1 server after an upgrade, where the license was preserved, the customer will be required to obtain a new license based on the new HostID of the embedded WebLM
- If the AE Services server is in a GRHA configuration, GRHA must be disabled and then the active and standby AE Services server must be upgraded. Before enabling GRHA, the administrator must log into WebLM on both AE Services servers to obtain the WebLM HostID of each server. These two HostIDs will be required to obtain the new AE Services license file.
- PLDS cannot generate an AE Services 7.1 server GRHA associated license file with two HostIDs where one HostID is based on the WebLM 7.0.1 format and the other is based on the WebLM 7.1 format. Both HostIDs must use the WebLM 7.1 format.

WebLM server compatibility

In addition to the embedded WebLM 7.1 server, the AE Services server incorporates and uses the WebLM 7.1 client components. The WebLM server supports N-1 backward compatibility with its client component. This means the WebLM 7.1 server can support connectivity to WebLM 6.x clients. Note the WebLM 6.x clients are used in the AE Services 6.x release. The WebLM server does not support forward compatibility. This means the AE Services 7.x WebLM client will not work with the WebLM 6.x server.

Issues related to Enterprise Directory

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

Issues related to SNMP

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

Alarm Viewer Change

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

Known issues and workarounds in Application Enablement Services 7.1.x.x

Known issues and workarounds Application Enablement Services in Release 7.1

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

ID	Visible symptoms	Workaround
AES-16100	Redirect media doesn't work with media encryption "strp-xxx" and "none"	Do not use media encryption "strp-xxx" and "none"
AES-16028	SMS: List public unknown-numbering always fails when number of records are large	
AES-14892	DMCC extension registration rejected	Use "pin-eke" instead of "challenge" on Communication Manager on "ip-network-region" form for "H323 Security profile" field.
AES-15077	DMCC endpoints cannot register to CM7.0.1 if video is enabled on CM	Disable "video softphone" flag on communication manager for the given extension (via "station" form)
AES-16272	Cannot Establish Trust on a VMWare Based AE Services from SMGR SDM	For AE Services 7.1, in order to reestablish the trust relationship between SDM 7.1 and an AE Services 7.1 VM, the "7.0" or "other" option on the SDM Graphical user Interface need to be selected.
AES-16009	Hostname is not taken by AE Services even after running netconfig	run command : "hostnamectl set-hostname name" to set the hostname
AES-15984	HMDC Reporting : Current snapshot data report cannot be saved as a csv file	
AES-16137	Virtual IP address is not shown on HA page even when its configured and accessible	Make a note for Virtual IP address

Avaya Aura® Utility Services

Installation for Avaya Aura® Utility Services Release 7.1

Download ID	Patch	Notes
US000000070	US-7.1.0.0.0.16-e55-373_OVF10.ova	This OVA can be used for both new installs and upgrades from previous releases of Utility Services.
US000000072	util_patch_7.1.0.0.1.01.zip	Utility Services Patch 7.1.0.0.1 provides a fix to allow the DHCP Daemon to start up correctly after an upgrade from V6.3/7.0.x. It is not necessary to apply this to a new install. This patch corrects an issue with the DHCPD Configuration file when it is installed - removing the patch has no effect.
US000000073	util_patch_7.1.0.0.2.01.zip	Utility Services Patch 7.1.0.0.2 provides a fix to allow the state of the Enhanced Access Security Gateway (EASG) to be preserved after a reboot with a partial environment file. This patch is recommended for all new installs and is immediate in effect - removing the patch has no effect.

Enhanced Access Security Gateway (EASG)

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

Refer to the **Migrating and Installing Avaya Appliance Virtualization Platform Release 7.1** document for instructions on enabling and disabling EASG, and for instructions on installing the EASG site certificates.

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

Licensing is new to Utility Services 7.1 and requires a License Activation Code from PLDS. There are many ways to find a LAC in PLDS so you can activate the available entitlements associated to it.

1. Login to https://plds.avaya.com
2. Access the Assets menu and select View Entitlements.
3. From this screen you can search for entitlements using the sold-to, FL, ship-to or end user for foreign train ID. These IDs are known as a group ID in PLDS.

Searching using the Group ID in PLDS:

1. To search for a LAC using the Group ID first select the Assets menu option and select View Entitlements.
2. Enter the Group ID in the Group ID field (Note that all group IDs are numeric and do not have leading zeros).
3. Select the System Manager Application and click the **Search Entitlements** button.

The LAC(s) will be displayed in the search results.

Searching using the SAP order number in PLDS:

1. To search for a LAC using the SAP Order number first select the Assets menu option and select View Entitlements.
2. On the View Entitlements screen select Advanced Search next to the search Entitlements button.
3. Select the Application and enter the SAP Order number in the Sales/Contract # field.
4. Click the **Search Entitlements** button.

   The LAC(s) will be displayed in the search results.

What's new in Utility Services Release 7.1.x

What's new in Utility Services Release 7.1

The following table lists enhancements in this release.

Enhancement	Description
RedHat 7	Utility Services is now based on RedHat Enterprise Linux 7 64-bit.
TLS 1.2	Utility Services now supports TLS 1.2 for both Apache and Tomcat access by default – however, both TLS 1.0 and 1.1 can be enabled if necessary.
IPv6	Utility Services now supports IPv6 – this is optional at initial deployment and also subsequently. Note that IPv4 configuration is mandatory.
SHA256 Firmware	Avaya are now publishing IP Phone Firmware signed with SHA256. Utility Services now supports this as default, but retains the ability to support older SHA1 and unsigned packages.
Third Party Certificates	Utility Services now fully supports Third Party Certificates. Certificate Signing Request (CSR) certificates can be generated as well as supporting PKCS#12 bundles.
Enhanced Access Security Gateway (EASG)	EASG provides a secure method for Avaya services personnel to access the Avaya Aura® Application remotely and onsite. Access is under the control of the customer and can be enabled or disabled at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck.
OVA Signing	The Utility Services Open Virtualization Archive (OVA) is supplied as a signed image.
Update Signing	Utility Services now supports signed Updates.
HTTP Disabled	HTTPS is now the default mode of connecting to Utility Services – however, HTTP can be enabled if required.
Multiple Account Handling	Utility Services now has a single Administrative Account at initial deployment. Additional Administrative and Auditor Accounts can be created.
LDAP Authentication	Utility Services now supports an external LDAP server for account authentication. This supports both administrative and auditor accounts.
Security	Utility Services now offers a fourth mode of deployment – Hardened Mode Services Port

Enhancement	Description
Hardening	Only – which has been designed to be JITC Compliant.
Amazon Web Services	Utility Services will be available for import into Amazon Web Services to allow customers to create their own AMI Image. This will allow Utility Services to be deployed as a virtual machine on Amazon's Cloud.
WebLM Licensing	Utility Services will require a WebLM License when used in a VMWare Deployment. Deployment on AVP will be covered by the license required for AVP itself.

The following items have been deprecated in Utility Services 7.1 as a result of increased system security.

Feature	Description
Remote CDR Database Access	Utility Services has always offered remote access to the CDR Data stored in a PostgreSQL Database via the standard port 5432. The PUSH Database was also available via the same mechanism. This feature is being deprecated in Utility Services 7.1 and remote access will no longer be possible.
Phone Firmware Manager	The Phone Firmware Manager feature is being deprecated in Utility Services 7.1. This means that it will no longer be possible to schedule H.323 Phone Firmware updates. Support for IP Phone Firmware (both H.323 and SIP) as well as configuration files is unaffected by this change.

The following commands have been modified to support a hypervisor independent architecture. The majority has identical syntax but have their name changed from "vami_xxx" to "ovf_xxx".

Feature	7.0.x Command	7.1.x Command
OOBM Enable/Disable	sudo /opt/avaya/common_services/vami_set_oobm OOBM_Enabled	sudo /opt/avaya/common_services/ovf_set_oobm OOBM_Enabled.
	sudo /opt/avaya/common_services/vami_set_oobm OOBM_Disabled	sudo /opt/avaya/common_services/ovf_set_oobm OOBM_Disabled
OOBM Static Route Add/Display/Remove	/opt/avaya/common_services/vami_set_static –a <route> <netmask> <via>	/opt/avaya/common_services/ovf_set_static –a <route> <netmask> <via>
	/opt/avaya/common_services/vami_set_static –d	/opt/avaya/common_services/ovf_set_static –d
	/opt/avaya/common_services/vami_set_static –r	/opt/avaya/common_services/ovf_set_static –r
Change IP	/opt/avaya/common_services/VMware_conf.sh	/opt/avaya/common_services/Initial_conf.sh
SMGR Enrollment Pwd	/opt/avaya/common_services/vami_set_spirit	/opt/avaya/common_services/ovf_set_spirit
Above spirit command is usually run after "Set_SMGR" command		
Auth File	/opt/avaya/common_services/vami_set_asg	N/A – See EASG in Deploying Avaya Aura Utility Services

Fixes in Utility Services Release 7.1.x.x

Fixes in Utility Services Release 7.1

The following table lists the fixes in Release 7.1. These fixes apply over and above the fixes in Release 7.1.1.

ID	Minimum Conditions	Visible symptoms	Found in Release
UTILSERV-66	Initial Install	HTTP access to web pages for administration purposes	7.0.0.0
UTILSERV-82	Initial Install	Reference to external URLs must be removed	7.0.0.0
UTILSERV-84	Initial Install	Tomcat manager application is enabled by default.	7.0.0.0
UTILSERV-85	Initial install	Tomcat version information is revealed	7.0.0.0
UTILSERV-95	Initial Install	Web Pages are susceptible to BEAST vulnerability.	7.0.0.0
UTILSERV-96	Initial Install	Disable cryptographically weak RC4 cipher suites	7.0.0.0
UTILSERV-97	Initial install	Use of HTTPS is not enforced for web pages	7.0.0.0
UTILSERV-248	Initial Install	Disable insecure services (tftp and http) by default	7.0.0.0
UTILSERV-427	Initial Install	Apache Tomcat JK ISAPI Connector buffer overflow (CVE-2016-6808).	7.0.0.0
UTILSERV-449	Initial Install	Apache Tomcat Remote Code Execution (CVE-2016-8735)	7.0.0.0
UTILSERV-452	Initial Install	Apache Tomcat Information Disclosure (CVE-2016-6816)	7.0.0.0
UTILSERV-588	Initial Install	Weak Cipher Suites enabled by default	7.0.0.0
UTILSERV-611	Initial Install	Missing Security Related Headers	7.0.0.0
UTILSERV-612	Initial Install	Server Information Disclosure	7.0.0.0

Known issues and workarounds in Utility Services Release 7.1.x.x

Known issues and workarounds in Utility Services Release 7.1

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

ID	Minimum conditions	Visible symptoms	Workaround
UTILSERV-613	UPDATED 96x1 H323 Phone is failed to back up the local device settings to Utility Services	Backup/Restore of IP Phones works correctly when using HTTPS (the default), but fails when using HTTP.	Use HTTPS to support backup/restore of IP Phones. The use of a secure protocol when communicating with the IP Phones is normally recommended. HTTP is supported, but requires enablement by the Administrator.
UTILSERV-600	Deployed using SDM Client and then attempt to establish trust with System Manager SDM	After successful deployment with SDM Client, it is possible that the attempt to establish trust with System Manager SDM	Reboot the Utility Services Virtual machine after deploying with SDM Client and before attempting to establish trust with System Manager SDM.

ID	Minimum conditions	Visible symptoms	Workaround
		fails.	
UTILSERV-631	The Product ID in WebLG and PLDS is NOT the same – this means that ONLY PLDS Licenses will work with this release.	A WebLG generated license will NOT work with Build 16.	Use a PLDS license for Build 16.
UTILSERV-640	Need to reboot Utility Services after upgrading US 7.0 to US 7.1 build 15 to apply the static route again	The Static Route for the OOBM network is preserved on an upgrade but is not active.	Reboot Utility Services when convenient to enable the Static Route for the OOBM Network.

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

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	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	

ID	Visible symptoms	Release found in
	NumericAddress is the same as the MailboxNumber.	
MSG-21899	Resent messages generate corrupt mb inbox counts if there is an active login for the subscriber - this can cause an incorrect MWI state.	
MSG-21948	SipAgent could core-dump during an MWI operation	
MSG-21961	Unencrypted insecure SMTP login mechanisms allowed	
MSG-21999	Multi-page fax failing	
MSG-22000	SMTP: Remove support for anonymous SSL/TLS ciphers	
MSG-22027	syslog messages could be lost if too many come from one process in too short a time period	
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	

ID	Visible symptoms	Release found in
MSG-22513	LDAP FE UTP commands do not work (they hang)	
MSG-22521	SipAgent should support TLSv1.2	
MSG-22529	AAM incorrectly using SIPS URI for all outgoing SIP calls when the transport is TLS	
MSG-22546	Anonymous Authentication advertised for SMTP	
MSG-22568	Enhance SMTP configuration options: Allow removal of port 25 from corporate LAN	
MSG-22600	Message Delivery fails to local subscriber from remote reply-able ELA list for message initiated by a local subscriber due to authentication required for messages sent by local subscribers	
MSG-22633	Modify default slapd log level to match openlap recommendations	
MSG-22683	SipAgent could consume 100% CPU on shutdown of messaging relying on watchdog to kill the process	
MSG-22689	cornerstone authmon process could consume ~100% CPU if rsyslog service is restarted	
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

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

Avaya Appliance Virtualization Platform

Installation for Avaya Appliance Virtualization Platform Release 7.1.x.x

File list

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

Download ID	Filename	File size	Notes
AVP00000011	avaya-avp-7.1.0.0.0.9.iso	755 MB	Use this ISO file for new AVP 7.1 installations. This ISO also contains the avaya-avp-7.1.0.0.0.9.zip upgrade bundle.
AVP00000012	avaya-avp-7.1.0.0.0.9.zip	372 MB	Use this ZIP file for upgrade from AVP 7.0.x or 7.1.0.0.x.

Enhanced Access Security Gateway (EASG)

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

Refer to the **Migrating and Installing Avaya Appliance Virtualization Platform Release 7.1** document for instructions on enabling and disabling EASG, and for instructions on installing the EASG site certificates.

Installing the release

This release can be used as a new install of AVP 7.1.0.0 or as an upgrade to an existing AVP 7.0.0.0 or later installation. For an upgrade, it will not be necessary to reinstall the guest VMs.

Refer to the **Migrating and Installing Avaya Appliance Virtualization Platform Release 7.1** document for instructions on new installs and upgrades of AVP.

Troubleshooting the installation

Refer to Chapter 11: Troubleshooting in the **Migrating and Installing Avaya Appliance Virtualization Platform Release 7.1** document.

Restoring software to previous version

Copy the previous patch to the system's local disk (/vmfs/volumes/server-local-disk).

Issue the following command (example using AVP 7.0.1.0.0.5 service pack):

```
/opt/avaya/bin/rollback_bootbank.sh /vmfs/volumes/server-local-disk/avaya-avp-7.0.1.0.0.5.zip
/opt/avaya/bin/avpshutdown.sh -r
```

Note: The full pathname to the rollback patch is required. You cannot use a relative path.

What's new in Avaya Appliance Virtualization Platform Release 7.1.x.x

What's new in Release 7.1.0.0

The following table lists enhancements in this release.

Enhancement	Description
IPv4 / IPv6 dual stack support	AVP will support IPv4 and IPv6 dual stack. IPv4 is mandatory. IPv6 is optional.
VIB Signing	The vSphere Installation Bundles (VIBs) included in AVP 7.1 will be signed with VMware certificate.
Third party certificate support	Third party certificates can be loaded through Solution Deployment Manager (SDM).
TLS 1.0 and 1.1 are disabled by default	TLS 1.0 and 1.1 can be enabled on the AVP host by issuing the following command from an SSH session: esxcli system settings advanced set -o /UserVars/ESXiRhttpproxyDisabledProtocols -s "sslv3"
AVP embedded host client replaces vSphere Client	vSphere Client can no longer connect to the AVP host because TLS 1.0 and 1.1 have been disabled by default. The embedded host client can be accessed at https://<IP of AVP host>/ui
Enhanced Access Security Gateway (EASG)	EASG provides a secure method for Avaya services personnel to access the Avaya Aura® Appliance Virtualization Platform remotely and onsite. Access is under the control of the customer and can be enabled or disabled at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck.
AVP Kickstart Generator in Avaya SDM Client	AVP Kickstart Generator is now part of the Avaya SDM Client. The AVP Kickstart Generator based on the Excel Spreadsheet is no longer supported.
AVP 'root' account is disabled on new installations	The 'admin' user replaces 'root' as the superuser for the system on fresh installation of AVP 7.1. On upgrades from AVP 7.0.x to AVP 7.1, 'root' continues to be the superuser for the system.

Fixes in Avaya Appliance Virtualization Platform Release 7.1.x.x

Fixes in Avaya Appliance Virtualization Platform 7.1

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Found in Release
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.	7.0.1.0
AVP-389	Avaya Appliance Virtualization Platform on any Avaya common	Server hardware alarms, such as power supply or disk alarms may be delayed by up	7.0.1.0

ID	Minimum Conditions	Visible symptoms	Found in Release
	server. Avaya Aura® adds support for HP DL360PG8 and Dell R630 in Avaya Virtual Deployment configurations.	to 3 hrs.	

Known issues and workarounds in Avaya Appliance Virtualization Platform Release 7.1.x.x

Known issues and workarounds in Avaya Appliance Virtualization Platform 7.1

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
AVP-410	AVP 7.0.1 or 7.1 with duplicate IP address in the	Cannot change the IP address of the AVP if there is a duplicate IP address on the subnet.	Follow the directions in the VMware Knowledge Base https://kb.vmware.com/selfservice/m

ID	Minimum conditions	Visible symptoms	Workaround
	subnet		icrosites/search.do?language=en_US&cmd=displayKC&externalId=1020647
AVP-429	AVP 7.1	Cannot administer IPv6 address using the firstboot.sh script during an attended installation.	Use the kickstart generator and use the USB key to install AVP 7.1 with an IPv6 address.
AVP-446	AVP 7.1	Cannot deploy VMs on AVP 7.1 via the embedded host client.	Use the System Manager SDM or the SDM Client to deploy VMs.
AVP-466	Enabling OOBM via CLI command on AVP 7.1	Enabling Out-of-Band Management (OOBM) via the CLI command '/opt/avaya/bin/set_oobm enable' may display the following error message although the command was successful: "Error performing operation: Sysinfo error on operation returned status: Bad parameter. See the VMkernel log for detailed error information"	
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

ID	Minimum conditions	Visible symptoms	Workaround
			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 or via SDM.
General issues and workarounds			If the system is to be set with Out of Band Management, the AVP host should be installed with Out of Band Management on or should be set to use Out of Band Management before VMs are deployed. When Out of Band Management is enabled on the host, all VMs must be set up to use Out of Band Management.
General issues and workarounds			It is always required to deploy a Utility Services VM with AVP. Utility Services provides key alarming and security functions to the AVP host and is mandatory to deploy.

Languages supported

Languages supported in this release:

- English

Avaya Aura® G430 and G450 Media Gateways

Installation for Avaya Aura® G430 and G450 Media Gateways Release 7.1.x.x

Required patches

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

Important: Gateways using an earlier release MUST upgrade to a 7.0.x,x Release (Builds 37.x.y) prior to installing Release 7.1.x.x (Builds 38.x.y).

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 series and Communication Manager releases. This means the latest version within the GW Firmware Series are recommended with the following Communication Manager software releases:

Gateway Firmware Series	Communication Manager Release
33.xx.xx	6.3
34.xx.xx	6.3.2
35.xx.xx	6.3.5
36.xx.xx	6.3.6
37.xx.xx	7.0.0
38.xx.xx	7.1.0.0

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.

Pre-Install Instructions

The following is required for installation:

- Avaya Communication Manager Release 6.3.6 or later should be used since earlier versions are no longer supported.
- Browser access to the Customer Support Web site (http://support.avaya.com), or another way to get the Target File
- SCP, FTP or TFTP applications on your PC or Local Computer or a USB drive formatted FAT32 file system.
- G430 or G450 Media Gateways hardware version 1 or greater
- Inads, dadmin, craft or a customer login that has been enabled for system maintenance.

File Download Instructions

Before attempting to download the latest firmware, read the "Upgrading the Branch Gateway Firmware" section in the following documents:

- Deploying and Upgrading Avaya G430 Branch Gateway.
- Deploying and Upgrading Avaya G450 Branch Gateway.

.

Note: To ensure a successful download, from the system access terminal (SAT) or ASA, issue the command 'busyout board v#' before issuing 'copy tftp' command. Upon completion, from the SAT or ASA issue the command 'release board v#'.

Backing up the software

For information about G430 and G450 Gateway backup and restore, Refer to the "Backup and Restore" section in the following documents:

- Deploying and Upgrading Avaya G430 Branch Gateway.
- Deploying and Upgrading Avaya G450 Branch Gateway.

Installing the release

Important: Gateways using an earlier release MUST upgrade to a 7.0.x.x Release (Builds 37.x.y) prior to installing Release 7.1.x.x (Builds 38.x.y).

Note: In Release 7.1 the gateway defaults to using TLS 1.2, PTLS, and unencrypted H.248 communication with CM. Refer to the "set link-encryption" command to adjust these settings.

For information about installing G430 and G450 Gateway firmware, Refer to the “Installing the Branch Gateway” section in the following documents:

- Deploying and Upgrading Avaya G430 Branch Gateway.
- Deploying and Upgrading Avaya G450 Branch Gateway.

Troubleshooting the installation

For information about troubleshooting G430 and G450 Gateway issues, Refer to the “Troubleshooting” section in the following documents:

- *Deploying and Upgrading Avaya G430 Branch Gateway.*
- *Deploying and Upgrading Avaya G450 Branch Gateway.*

Restoring software to previous version

For information about G430 and G450 Gateway backup and restore, Refer to the “Backup and Restore” section in the following documents:

- Deploying and Upgrading Avaya G430 Branch Gateway.
- Deploying and Upgrading Avaya G450 Branch Gateway.

What’s new in Avaya Aura® G430 and G450 Media Gateways Release 7.1.x.x

What’s new in G430 and G450 Media Gateways Release 7.1.0.0, Builds 38.18.00 and 38.18.30

The following table lists enhancements in this release.

Enhancement	Description
Security	TLS feature enhancements and administration for • TLS versions used for H.248 registration and SLA monitor. • Subject Alternate Name Certificate Validation. • Mandatory Revocation Checking for CRLs and OCSP. A new CLI command has been introduced for Subject Alternate Name validation of TLS certificates: **set validate-alternate-name <yes | no>** - Sets whether Subject Alternate Name validation should be performed. In addition, the following TLS certificate option commands have been enhanced: **show certificate-options** - Show the administered certificate options. **set crl-http-validation** <none | best-effort | mandatory>

Enhancement	Description
	- Set Certificate Revocation List validation. **set ocsp-validation** < none | best-effort | mandatory> - Set OCSP revocation validation. Also the following link-encryption commands have been enhanced: **show link-encryption** - Show which link encryption is allowed **set link-encryption h248reg** {protocol} <yes | no> - Set link encryption options for H.248 Registration with Communication Manager where {protocol} = < all | tls | tls1.2 | tls1.1 | tls1.0 | ptls | unencrypted > **Note: PTLS cannot be enabled while in FIPS mode.** **set link-encryption sla** {protocol} <yes | no> - Set link encryption options for SLA Monitor Agent where {protocol} = < all | tls | tls1.2 | tls1.1 | tls1.0 >
Security	Enhanced user login and password administration including: • Notification Messages for failed logins. • Forced password change on first login. The following new CLI commands have been introduced: **login authentication change-password-on-first-login** - Require that the user change password upon first login. **no login authentication change-password-on-first-login** - Do not require that the user change password upon first login. **banner failed-login** - Set the banner message to be displayed when login failure occurs. **show banner failed-login** - Show the banner message to be displayed when login failure occurs. In addition, this CLI command has been enhanced to include the new authentication options: **show login authentication** - Show login authentication options.
Security	The following new CLI commands have been introduced for the administration of SSH ciphers, key exchange algorithms, and MAC options for the SSH server and SSH client: **show ssh-server-configuration**

Enhancement	Description
	- Show the SSH server configuration. **show ssh-client-configuration** - Show the SSH client configuration. **ssh-server-configuration** - Enter the SSH server configuration CLI context. **ssh-client-configuration** - Enter the SSH client configuration CLI context. The following commands apply within the **ssh-server-configuration** or the **ssh-client-configuration** CLI command contexts: **set ciphers** <default | all | {cipher} [{cipher}...] > - Set the list of allowed SSH ciphers where {cipher} = < aes256-ctr | aes128-ctr | aes256-cbc | aes128-cbc | 3des-cbc > **set kex-algorithms** <default | all | {kex} [{kex}...]> - Set the list of allowed SSH Key Exchange (KEX) algorithms where {kex} = < diffie-hellman-group14-sha1 | diffie-hellman-group-exchange-sha1 | diffie-hellman-group-exchange-sha256 > **set macs** <default | all | {mac} [{mac}...]> - Set the list of allowed SSH Message Authentication Code (MAC) algorithms where {mac} = < hmac-sha1 | hmac-sha2-256 | hmac-sha2-512 | hmac-sha1-96 > **show ciphers** - Show the administered list of allowed SSH ciphers. **show kex-algorithms** - Show the administered list of allowed SSH KEX algorithms. **show macs** - Show the administered list of allowed SSH MAC algorithms.
Security	Updated versions of OpenSSL, SSH Server, and SSH Client. OpenSSL has been updated to Version 1.02h-fips. OpenSSH has been updated to Version 7.2p2. In addition, the following CLI command has been modified to display the versions of OpenSSH and OpenSSL currently being used.

Enhancement	Description
	show ip ssh - Show the OpenSSL and OpenSSH versions implemented in the gateway.
Security	Use of SHA2 to provide more secure download of firmware images.
Security	FIPS mode configuration option to assure only NIST approved authentication and encryption algorithms and security policies are used (*FIPs certification currently in progress*). The following new CLI commands have been introduced for FIPS mode: **set fips-mode** <enable | disable> - Set whether FIPS mode is enabled or disabled. **show fips-mode** - Show the state of FIPS mode.

Fixes in G430 and G450 Media Gateways Release 7.1.x.x

Fixes in G430 and G450 Media Gateways Release 7.1.0.0

Builds 38.18.00 and 38.18.30

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

Known issues and workarounds in G430 and G450 Media Gateways Release 7.1.x.x

Known issues and workarounds in G430 and G450 Media Gateways Release 7.1.0.0

Builds 38.18.00 and 38.18.30

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

ID	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.

Languages supported

- English

Documentation errata

- None

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)

What's new in Avaya Aura® Media Server

What's new in Avaya Aura® Media Server 7.8.0

The following table lists enhancements in this release.

Enhancement	Description
EASG	Enhanced Access Security Gateway (ESG) and replaces ASG.
SNMPv3	Support for SNMPv3 was added.
Deployment Profile 5 and 6	Introduce new virtual appliance deployment profiles 5 and 6, which support 16vCPU 16 GB memory.

What's new in 7.8.0 Service Pack Beta 3

The following table lists enhancements in this release.

Enhancement	Description
Dell R230	New server option for small bare metal appliances.
IPv6	Support for IPv6 SIP signaling was added. IPv6 media is supported for audio only.
ESXi 6.5	Support for ESXi 6.5 was added.

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 software for maintenance or software-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.

- Media Server log capture with trace logs included
- Network packet capture on the Media Server
- Screen shots for Element Manager issues
- Debug log (ams_debug.log) for SMGR Media Server element issues

Installation for Avaya Aura® Media Server 7.8

New Installation File List

Download ID	Filename	Notes
MSR000000056	MediaServer_7.8.0.309_A5_2017.04.12_OVF10.ova	AAMS virtual appliance (OVA) for new deployments or deployments that require ESXi 6.5. After initial deployment ensure that the latest System Layer and Media Server update is applied.
MSR000000053	MediaServer_7.8.0.312_2017.04.24.bin	AAMS software only installer (PVI) for new deployments where customer is supplying the hardware and Linux OS.

Required patches

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

Download ID	Patch	Notes
MSR000000054	Media Server 7.8.0.312	AAMS update for Media Server software that needs to be applied to all 7.7 or 7.8 deployments.
MSR000000055	System Layer 7.8.0.6	AAMS update for System Layer software that needs to be applied to all 7.7 or 7.8 appliance deployments. This update is not required for the virtual appliance deployments using 7.8.309 A5.

Patch File list (Appliance Only)

Filename	File size	Version
MediaServer_Update_7.8.0.312_2017.04.24.iso	363,528,192	7.8.0.312
MediaServer_System_Update_7.8.0.6_2017.03.27.iso	529,430,528	7.8.0.6

Patch File list (Non-Appliance Only)

Filename	File size	Version
MediaServer_7.8.0.312_2017.04.24.bin	363,198,583	7.8.0.312

ESXi/vCenter 6.5 Limitations

Deploying OVA's to an ESXi 6.5 host using the desktop vSphere Client is not supported by VMware and the vSphere Web Client or Host Client must be used instead. It is recommended that you use vSphere Web Client (https://FQDN-or-IP-Address-of-VC/vsphere–client) when deploying new OVA's since there are known issues with the Host Client (https://FQDN-or-IP-Address-of-ESXi-host/UI).

The following issues exist when using the Host Client to deploy OVA:

- During deployment you are not prompted for the VM profile and default to profile 1 (4 vCPU, 4.5 GB memory and 50 GB vDisk). To work around this you will need to manually edit the VM Virtual Hardware settings before powering the VM on.
- Properties specified when deploying OVA are ignored and they must be re-entered during the first boot process. Drop-down lists are not provided and property defaults are not populated.

Backing up the software

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

https://downloads.avaya.com/css/P8/documents/101033404

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

https://downloads.avaya.com/css/P8/documents/101033402

7.7 to 7.8 Upgrade Considerations

Before you upgrade from 7.7 to 7.8 the following should be considered:

- WebLM 7.0.x or higher (standalone or SMGR)
- System Manager (SMGR) 7.1 now limits the number of simultaneous sessions and the default is 5. So if you have multiple AAMS enrolled with SMGR that use the same System Manager administrative account and you exceed this limit you may experience issues. To avoid this multiple System Manager

administrative accounts should be created and AAMS servers should be updated (Home » Security » System Manager » Advanced Settings) to limit the number of AAMS servers using each account.

- If WebLM is deployed standalone, AAMS will be unable to establish a connection to it over TLS. This is due to differences in the enabled TLS ciphers on each server. It is recommended that you update the WebLM server to use one of the ciphers enabled on AAMS, which are listed the cluster service profile (Home » System Configuration » Network Settings » Advanced Settings » TLS Ciphers).

Enhanced Access Security Gateway (EASG)

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

On the AAMS appliance EASG is disabled by default. Customers that are upgrading an existing 7.7 appliance to 7.8 or deploying a new 7.8 appliance for the first time are encouraged to enable EASG. After upgrading you can enable EASG using the following command:

```
EASGManage --enableEASG
```

Refer to documentation for all EASG related commands.

Installing the release

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

https://downloads.avaya.com/css/P8/documents/101033404

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/101033406

When upgrading a 7.7 or 7.8 appliance the following procedure should be used:

- Backup the system
- Upload both system layer and media sever updates
- Place system in pending lock (one node at a time)
- Click “Install Updates” in Element Manager to initiate update install
- Once installation complete place system in an unlocked state

When upgrading an appliance from versions prior to 7.7 Feature Pack 1 the procedures for upgrading have changed to accommodate the transition to a simplified one button update. The transition procedure is summarized as follows:

- Upload both 7.8 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* for the new update procedure.

Troubleshooting the installation

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

https://downloads.avaya.com/css/P8/documents/101033404

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/101033406

Restoring software to previous version

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

https://downloads.avaya.com/css/P8/documents/101033404

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

https://downloads.avaya.com/css/P8/documents/101033402

Functionality not supported

N/A

Fixes in Avaya Aura® Media Server 7.8.x

Fixes in System Layer for 7.8.0 Service Pack 3

The following table lists the fixes in this release.

ID	Minimum conditions	Visible symptoms	Found in Release
AMS-3986	All deployments	MSML interpreter crashes during traffic.	7.8 GA

ID	Minimum conditions	Visible symptoms	Found in Release
AMS-3951	All deployments	Unable to clear Session Detail Record in Logging Settings	7.8 GA
AMS-3939	All deployments	Disk fills up when enabling System Diagnostic Mode.	7.8 GA
AMS-3774 AMS-3748 AMS-3720	All appliance deployments	OS Security updates	7.8 GA
AMS-3719	Virtual appliance deployed using vCenter host	System layer update fails to apply since DNS server is not configured.	7.8 GA
AMS-3719	All appliance deployments	Removed weak SSH ciphers CBC and arcfour	7.8 GA

Fixes in Media Server for 7.8.0 Service Pack 3

The following table lists the fixes in this release.

ID	Minimum conditions	Visible symptoms	Release Introduced
AMS-3947	All deployments with WebRTC sessions	Memory leak of the ConfMP component	7.8 GA
AMS-3846	All deployments with WebRTC sessions	FNTMP component crashes if ICE connectivity check fails	7.8 GA
AMS-3908	All deployments with secure connections	Connection setup memory leak of components using TLS	7.8 GA
AMS-3808	All deployments enrolling with SMGR using certificates by 3rd party CA	Unable to login to element manager after enrollment completes. The end user may not see a SMGR login page or the SMGR login will fail. Also other applications may fail to connect using secure connections due to TLS handshake failure.	7.8 GA
AMS-3906	All deployments	MSML interpreter stops processing new requests and media server is not responsive.	7.8 GA
AMS-3914	All deployments with an AAMS cluster or master Content Store configured	Content Store data may not be replicated.	7.8 GA
AMS-3787	All deployments	Element Manager certificates signed by SMGR contain incorrect Subject Alternative Names and do not match specified values.	7.8 GA
AMS-3833	All deployments	Unable to view enrolled AAMS in SMGR due to specifying special characters in server name.	7.8 GA

ID	Minimum conditions	Visible symptoms	Release Introduced
AMS-3839	All deployments using ECDHE ciphers	Small memory leak exists when using ECDHE ciphers	7.8 GA
AMS-3810	All deployments using video	Operational Measurements for H264-SVC are incorrect	7.8 GA

Known issues and workarounds in Avaya Aura® Media Server

Known issues and workarounds in 7.8.0 Service Pack 3

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

ID	Minimum conditions	Visible symptoms	Workaround
AMS-3989	Deploy OVA using vSphere Web Client and ESXi 6.5.	OVA properties are listed in alphabetical order instead of order specified by the OVA.	None
AMS-3987	Deploy OVA using Host Client and ESXi 6.5.	During deployment you are not prompted for the VM profile and default to profile 1 (4 vCPU, 4.5 GB vMemory and 50 GB vDisk).	Manually edit the VM Virtual Hardware settings before you power on VM or use vSphere Web Client to deploy OVA.
AMS-3942	Deploy OVA using Host Client and ESXi 6.5.	Properties specified when deploying an OVA are ignored	Specify the properties during the first boot or use vSphere Web Client to deploy OVA.
AMS-3988	Deploy OVA using Host Client and ESXi 6.5.	Drop-down lists are not provided and property defaults are not populated when specifying OVA properties.	Manually enter the properties or use vSphere Web Client to deploy OVA.

Languages supported

List the languages supported in this release.

- English

Documentation errata

Document number	Title	Description
N/A		

Avaya Aura® WebLM

Installation for Avaya Aura® WebLM on VMWare Release 7.1

Download ID	Artifacts	Notes
SMGR71GA003	WebLM OVA	WebLM-7.1.0.0.11-25605-e65-19.ova Size: 942 MB MD5SUM: 608206db759b4d0d2d72c0850811e4da

Installing the release 7.1

Important Notes

1. Characters required in the hostname

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

2. Cloning WebLM on VMware

   A user cannot change the IP of a WebLM OVA system that is cloned to another host. To change the IP, rename the ifcfg-eth0 file to ifcfg-eth0.old. Create the file (ifcfg-eth0). Add the MAC address of the newly cloned VM into the ifcfg-eth0 file with correct network configuration and restart the network service.

3. Restoring WebLM Backup

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

4. Rehost of licenses

   - In VE deployments, host ID of the WebLM server is a function of IP address and UUID of the system. So, if either 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.

Resource allocation and reservation for standalone WebLM on VMware

VMware resource	Profile 1 Values that can support up to 5000 license requests (Default)	Profile 2 Values that can support more than 5000 license requests
vCPUs	1	1
CPU reservation	2290 MHz	2290 MHz
Memory	1 GB	2 GB
Memory reservation	1 GB	2 GB
Storage reservation	30 GB	30 GB
Shared NIC	1	1

WebLM requires more memory to scale to more than 5000 license requests at any point of time.

To update the memory for WebLM on VMware:

1. Log in to your VMware VSphere Client, and turn off the WebLM virtual machine.
2. If WebLM VM is not visible in the navigation pane, then navigate to Home > Inventory > Hosts and Clusters.
3. Right-click the WebLM VM in the navigation pane.
4. Select the Edit Settings option from the available context menu.
5. In the Edit Settings or Virtual Machine Properties dialog box, select the Memory option on the Hardware tab.
6. Specify 2048 in the text field and MB in the drop-down box.
7. In the Hardware tab, type 2 in the CPU option.
8. Click OK.
9. In the navigation pane, right-click the WebLM VM and select the Power On option from the context menu.

Software information

Software	Version
RedHat	7.2
OpenJDK	Openjdk version "1.8.0_121" 64-bit
Apache Tomcat	8.0.18
Internet Explorer	9.x, 10.x and 11.x
Firefox	45,46,47

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

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 Command Line Interface using **admin** as the user name and gain access to the log file.

Additional WebLM logs at **$CATALINA_HOME/webapps/WebLM/data/log**

Contacting support

Contact support checklist

Avaya Technical Support provides support for WebLM 7.1/

For any problems with WebLM 7.1, you can:

1. Retry the action. Carefully follow the instructions in the printed or online documentation.
2. See the documentation that is shipped with your hardware for maintenance or hardware-related problems.
3. Note the sequence of events that led to the problem and the messages that the system displays. See the troubleshooting section of the Avaya product documentation.

If you continue to have problems, contact Avaya Technical Support by logging in to the Avaya Support website at

http://support.avaya.com.

Before contacting Avaya Technical Support, keep the following information handy:

- Problem description.
- Detailed steps to reproduce the problem, if any.
- The release version in which the issue occurs.

Note: To know the release version and build number, log in to WebLM and click **About** on the user interface. If WebLM Console is inaccessible, you can log in to the WebLM SSH interface and run the **swversion command** to get the WebLM version.

- The status of the WebLM software. If the software is an upgrade, then the release from which the software is upgraded.
- Installation log files are available at **/opt/Avaya/install_logs**
- The WebLM Tomcat server log files are available at **$CATALINA_HOME/logs**. You can gain access to the Command Line Interface using admin as the user name and then gain access to the log file.
- Additional WebLM logs at **$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 for 7.1

The following table lists enhancements in this release.

Enhancement	Description
Infrastructure	New column introduced as 'Acquirer ID' in 'Acquired Licenses' details section Moved to openjdk version "1.8.0_121" Server version: Apache Tomcat/8.0.18 WebLM Host ID Suffix System Manager WebLM/WebLM war WebLM License File Host ID Validation WebLM ova License File Host ID Validation WebLM SHA256 Digital Signature Support System Manager WebLM/WebLM war License File Digital Signature Validation WebLM Block Install of License File with SHA1 Digital Signature WebLM ova License File Digital Signature Validation WebLM License File Signing Move Standalone WebLM to Red Hat Enterprise Linux 7.x IPV6 support [Dual stack support] Custom Command line interface user creation during OVA deployment. (No default CLI admin user.) WebLM User Interface admin user password need to set during OVA deployment. (No default UI password for admin user)

Fixes in Avaya Aura® WebLM on VMWare for 7.1

The following table lists the fixes in this release:

ID	Description
SMGR-32763	Missing Cross-Frame Scripting Defense
SMGR-36503	System Manager Licenses page is not launching displaying "Shortcuts Help for Weblm Home"
SMGR-36096	After the OSS upgrade is complete, in the WebLM, the "Date of Installation" for license files is updated to the date of the OSS upgrade

Known issues and workarounds in Avaya Aura® WebLM on VMWare for 7.1

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

ID	Visible symptoms	Workaround
SMGR-25348	There is no Web UI on WebLM to configure SNMP alarms/agent for either SNMP V2c or V3 for VPFM to pick up and report on.	No workaround available

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

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

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 in Avaya Aura Device Services

What's new in Release 7.1

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 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

Enhancement	Description
	• Avaya Equinox™ for Mac • Avaya Equinox™ for Windows.
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 in Avaya Aura Device Services

Fixes in Release 7.1

Known issues and workarounds

Known issues and workarounds in Release 7.1

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

ID	Minimum conditions	Visible symptoms	Workaround

Languages supported

- English