Avaya Aura® Release Notes

Release 7.1.x.x

Issue 41

March 2021

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, https://support.avaya.com/LICENSEINFO, UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “**Software**” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “**Designated Processor**” means a single stand-alone computing device. “**Server**” means a Designated Processor that hosts a software application to be accessed by multiple users. “**Instance**” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“**VM**”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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

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

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo/ under the link “Heritage Nortel Products,” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel

Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"**Third Party Components**" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components, to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED

OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of 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

Contents ... 6

Change history ... 20

Introduction ... 22

Product Release Matrix ... 23

What's new in Avaya Aura® ... 24

- Support for the next generation server platform ... 24

Compatibility ... 24

Contacting support ... 24

- Contact support checklist ... 24
- Contact support tasks ... 25

Avaya Aura® Communication Manager ... 26

- Installation for Avaya Aura® Communication Manager 7.1.x.x ... 26
  - Required patches ... 26
  - Backing up and installing Communication Manager ... 26
  - Troubleshooting the installation ... 26
  - Enhanced Access Security Gateway (EASG) ... 27
  - Speculative Execution Vulnerabilities (includes Meltdown and Spectre and also L1TF Vulnerabilities) ... 27
- What's new in Communication Manager Release 7.1.x.x ... 27
  - What's new in Communication Manager Release 7.1.3.8 ... 27
  - What's new in Communication Manager Release 7.1.3.7 ... 28
  - What's new in Communication Manager Release 7.1.3.6 ... 28
  - What's new in Communication Manager Release 7.1.3.5 ... 28
  - What's new in Communication Manager Release 7.1.3.4 ... 28
  - What's new in Communication Manager Release 7.1.3.3 ... 28
  - What's new in Communication Manager Release 7.1.3.2 ... 28
  - What's new in Communication Manager Release 7.1.3.1 ... 28
  - What's new in Communication Manager Release 7.1.3 ... 28
  - What's new in Communication Manager Release 7.1.2 ... 29
  - What's new in Communication Manager Release 7.1.1 ... 29
  - What's new in Communication Manager Release 7.1 ... 29
- Security Service Pack and Kernel Service Pack ... 30
- Required artifacts for Avaya Aura® Communication Manager 7.1.x.x ... 30
  - Required artifacts for Communication Manager Release 7.1.3.8.0 ... 30
  - Required artifacts for Communication Manager Release 7.1.3.7.0 ... 30
- Known issues and workarounds in Communication Manager Release 7.1.x.x ... 30
  - Known issues and workarounds in Communication Manager Release 7.1.3.8 ... 30
  - Known issues and workarounds in Communication Manager Release 7.1.3.7 ... 30
  - Known issues and workarounds in Communication Manager Release 7.1.3.6 ... 30

Known issues and workarounds in Communication Manager Release 7.1.3.5 31
Known issues and workarounds in Communication Manager Release 7.1.3.4 31
Known issues and workarounds in Communication Manager Release 7.1.3.3 31
Known issues and workarounds in Communication Manager Release 7.1.3.2 31
Known issues and workarounds in Communication Manager Release 7.1.3.1 31
Known issues and workarounds in Communication Manager Release 7.1.3 31
Known issues and workarounds in Communication Manager Release 7.1.2 32
Known issues and workarounds in Communication Manager Release 7.1.1 32
Known issues and workarounds in Communication Manager Release 7.1 32
Fixes in Communication Manager Release 7.1.x.x 33
Fixes in Communication Manager Release 7.1.3.8 33
Fixes in Communication Manager Release 7.1.3.7 34
Fixes in Communication Manager Release 7.1.3.6 42
Fixes in Communication Manager Release 7.1.3.5 46
Fixes in Communication Manager Release 7.1.3.4 54
Fixes in Communication Manager Release 7.1.3.3 59
Fixes in Communication Manager Release 7.1.3.2 64
Fixes in Communication Manager Release 7.1.3.1 66
Fixes in Communication Manager Release 7.1.3 70
Fixes in Communication Manager Release 7.1.2 76
Fixes in Communication Manager Release 7.1.1 79
Avaya Aura® Session Manager 87
Installation for Session Manager 7.1.x.x 87
Backing up the software 87
Installing the Session Manager software 87
Upgrading 87
Special Case Upgrade Paths 87
Speculative Execution Vulnerabilities (includes Meltdown and Spectre and also L1TF Vulnerabilities) 88
Troubleshooting the installation 89
Restoring software to previous version 89
What’s new in Session Manager Release 7.1.x.x 89
What’s new in Session Manager Release 7.1.3.8 89
What’s new in Session Manager Release 7.1.3.7 89
What’s new in Session Manager Release 7.1.3.6 89
What’s new in Session Manager Release 7.1.3.5 89
What’s new in Session Manager Release 7.1.3.4 89
What’s new in Session Manager Release 7.1.3.3 90
What’s new in Session Manager Release 7.1.3.2 90
What’s new in Session Manager Release 7.1.3.1 90

What's new in Session Manager Release 7.1.3 90
What's new in Session Manager Release 7.1.2 90
What's new in Session Manager Release 7.1.1 91
What's new in Session Manager Release 7.1 91
Fixes in Session Manager Release 7.1.x.x 93
Fixes in Session Manager Release 7.1.3.8 93
Fixes in Session Manager Release 7.1.3.7 94
Fixes in Session Manager Release 7.1.3.6 96
Fixes in Session Manager Release 7.1.3.5 97
Fixes in Session Manager Release 7.1.3.4 99
Fixes in Session Manager Release 7.1.3.3 100
Fixes in Session Manager Release 7.1.3.2 101
Fixes in Session Manager Release 7.1.3.1 102
Fixes in Session Manager Release 7.1.3 102
Fixes in Session Manager Release 7.1.2 103
Fixes in Session Manager Release 7.1.1 104
Fixes in Session Manager Release 7.1 106
Known issues and workarounds in Session Manager 7.1.x.x.......... 107
Known issues and workarounds in Session Manager Release 7.1.3.8.......... 107
Known issues and workarounds in Session Manager Release 7.1.3.7.......... 107
Known issues and workarounds in Session Manager Release 7.1.3.6.......... 107
Known issues and workarounds in Session Manager Release 7.1.3.5.......... 107
Known issues and workarounds in Session Manager Release 7.1.3.4.......... 108
Known issues and workarounds in Session Manager Release 7.1.3.3.......... 108
Known issues and workarounds in Session Manager Release 7.1.3.2.......... 108
Known issues and workarounds in Session Manager Release 7.1.3.1.......... 108
Known issues and workarounds in Session Manager Release 7.1.3.......... 108
Known issues and workarounds in Session Manager Release 7.1.2.......... 109
Known issues and workarounds in Session Manager Release 7.1.1.......... 109
Known issues and workarounds in Session Manager Release 7.1 110
Avaya Aura® System Manager.......... 111
Installation for System Manager 7.1.3.x 111
Upgrading the System Manager software.......... 111
System Manager upgrade path 111
Troubleshooting the installation 111
Required artifacts for System Manager Release 7.1.x.x 112
Required artifacts for System Manager Release 7.1.3.8 112
Required artifacts for System Manager Release 7.1.3.7 112
Required artifacts for System Manager Release 7.1.3.6 112

Required artifacts for System Manager Release 7.1.3.5 113
Required artifacts for System Manager Release 7.1.3.4 113
Required artifacts for System Manager Release 7.1.3.3 113
Required artifacts for System Manager Release 7.1.3.2 114
Required artifacts for System Manager Release 7.1.3.1 114
Required artifacts for System Manager Release 7.1.3 115
Speculative Execution Vulnerabilities (includes Meltdown and Spectre and also L1TF Vulnerabilities) 115
Required artifacts for System Manager Release 7.1.2 115
Required artifacts for System Manager Release 7.1.1.1 116
Required artifacts for System Manager Release 7.1.1 116
Required artifacts for System Manager Release 7.1 116
Download Data Migration Utility........ 118
Software information........ 118
Must read:........ 118
How to find a License Activation Code (LAC) in PLDS for a product........ 119
What’s new in System Manager Release 7.1.x.x 119
What’s new in System Manager Release 7.1.3.8 119
What’s new in System Manager Release 7.1.3.7 119
What’s new in System Manager Release 7.1.3.6 119
What’s new in System Manager Release 7.1.3.5 120
What’s new in System Manager Release 7.1.3.4 120
What’s new in System Manager Release 7.1.3.3 120
What’s new in System Manager Release 7.1.3.2 120
What’s new in System Manager Release 7.1.3.1 120
What’s new in System Manager Release 7.1.3 120
What’s new in System Manager Release 7.1.2 121
What’s new in System Manager Release 7.1.1.1 121
What’s new in System Manager Release 7.1.1 121
Enhancements delivered to System Manager Release 7.1.x.x 122
Enhancements delivered to System Manager Release 7.1.3.8 122
Enhancements delivered to System Manager Release 7.1.3.7 122
Enhancements delivered to System Manager Release 7.1.3.6 122
Enhancements delivered to System Manager Release 7.1.3.5 122
Enhancements delivered to System Manager Release 7.1.3.4 122
Enhancements delivered to System Manager Release 7.1.3.3 122
Enhancements delivered to System Manager Release 7.1.3.2 122
Enhancements delivered to System Manager Release 7.1.3.1 122
Enhancements delivered to System Manager Release 7.1.3 123
Enhancements delivered to System Manager Release 7.1.2 123

Enhancements delivered to System Manager Release 7.1.1.1 ... 123
Enhancements delivered to System Manager Release 7.1.1 ... 123
Enhancements delivered to System Manager Release 7.1 ... 124
Fixes in System Manager Release 7.1.x.x ... 126
Fixes in System Manager 7.1.3.8 ... 126
Fixes in System Manager 7.1.3.7 ... 128
Fixes in System Manager 7.1.3.6 ... 131
Fixes in System Manager 7.1.3.5 ... 133
Fixes in System Manager 7.1.3.4 ... 136
Fixes in System Manager 7.1.3.3 ... 139
Fixes in System Manager 7.1.3.2 ... 143
Fixes in System Manager 7.1.3.1 ... 145
Fixes in System Manager 7.1.3 ... 147
Fixes in System Manager 7.1.2 ... 149
Fixes in System Manager 7.1.1.1 ... 150
Fixes in System Manager 7.1.1 ... 151
Known issues and workarounds in System Manager 7.1.x.x ... 153
Known issues and workarounds in System Manager on VMware in Release 7.1.3.8 ... 153
Known issues and workarounds in System Manager on VMware in Release 7.1.3.7 ... 155
Known issues and workarounds in System Manager on VMware in Release 7.1.3.6 ... 157
Known issues and workarounds in System Manager on VMware in Release 7.1.3.5 ... 160
Known issues and workarounds in System Manager on VMware in Release 7.1.3.4 ... 161
Known issues and workarounds in System Manager on VMware in Release 7.1.3.3 ... 164
Known issues and workarounds in System Manager on VMware in Release 7.1.3.2 ... 166
Known issues and workarounds in System Manager on VMware in Release 7.1.3.1 ... 168
Known issues and workarounds in System Manager on VMware in Release 7.1.3 ... 170
Known issues and workarounds in System Manager on VMware in Release 7.1.2 ... 172
Known issues and workarounds in System Manager on VMware in Release 7.1.1.1 ... 173
Known issues and workarounds in System Manager on VMware in Release 7.1.1 ... 175
Known issues and workarounds in System Manager on VMware in Release 7.1 ... 176
Solution Deployment Manager Adopter Matrix ... 178
Deployment and Upgrade Guides: ... 182
Avaya Aura® Presence Services ... 183
Installation for Avaya Aura® Presence Services 7.1.x.x ... 183
Required patches for Presence Services 7.1.2.0 ... 183
File list for Presence Services 7.1.2.0 ... 183
Installing the release ... 183
Troubleshooting the installation ... 183
Restoring software to previous version ... 183

Backing up the software ... 183
Migrating to the PS 7.1.2 release from a PS 6.2.X release ... 183
Changes Affecting Migrations to 7.1.2 ... 183
Minimum required versions by Release ... 185
Upgrade References to Presence Services 7.1.2.0 ... 185
Interoperability and requirements/Applicability ... 185
Software Development Kit ... 185
Functionality not supported in Presence Services 7.1.x.x ... 186
What's new in Presence Services 7.1.x.x ... 186
What's new in Presence Services Release 7.1.2 ... 186
What's new in Presence Services Release 7.1 ... 186
Fixes in Presence Services 7.1.x.x ... 187
Fixes in Release 7.1.2 ... 187
Fixes in Release 7.1 ... 188
Known issues and workarounds in Presence Services 7.1.x.x ... 189
Known issues and workarounds in Presence Services Release 7.1.2.0 ... 189
Known issues and workarounds in Release 7.1 ... 191
Avaya Aura® Application Enablement Services ... 193
Installation for Avaya Aura® Application Enablement Services Release 7.1.x.x ... 193
Backing up the AE Services software ... 193
Interoperability and requirements ... 193
Functionality not supported ... 193
Installation for Avaya Aura® Application Enablement Services Release 7.1.x ... 193
Installation of Avaya Aura® Application Enablement Services 7.1.2 ... 194
Installation of Avaya Aura® Application Enablement Services 7.1.3 ... 195
Installation of Avaya Aura® Application Enablement Services 7.1.3.1 ... 196
Installation of Avaya Aura® Application Enablement Services 7.1.3.2 ... 196
Installation of Avaya Aura® Application Enablement Services 7.1.3.3 ... 196
Installation of Avaya Aura® Application Enablement Services 7.1.3.4 ... 196
Installation of Avaya Aura® Application Enablement Services 7.1.3.5 ... 196
Installation of Avaya Aura® Application Enablement Services 7.1.3.6 ... 196
Installation of Avaya Aura® Application Enablement Services 7.1.3.7 ... 197
Installation of Avaya Aura® Application Enablement Services 7.1.3.8 ... 197
Speculative Execution Vulnerabilities (includes Meltdown and Spectre and also L1TF Vulnerabilities) ... 197
Upgrading to AE Services 7.1.x ... 197
AE Services Server Upgrade Instructions ... 197
Restoring AE Services software to previous version ... 198
Installation for Avaya Aura® Application Enablement Services Software Only 7.1 ... 198
Installation steps for Avaya Aura® Application Enablement Services 7.1 Aura® OVA Media ... 199

Installation steps for Avaya Aura® Application Enablement Services 7.1.1 RPM-only Installer 199
Required artifacts for Application Enablement Services Release 7.1.x.x 199
Required artifacts for Application Enablement Services Release 7.1.3.8 199
Required artifacts for Application Enablement Services Release 7.1.3.7 199
Required artifacts for Application Enablement Services Release 7.1.3.6 200
Required artifacts for Application Enablement Services Release 7.1.3.5 200
Required artifacts for Application Enablement Services Release 7.1.3.4 200
Required artifacts for Application Enablement Services Release 7.1.3.3 201
Required artifacts for Application Enablement Services Release 7.1.3.2 201
Required artifacts for Application Enablement Services Release 7.1.3.1 201
Required artifacts for Application Enablement Services Release 7.1.3.1.1 202
Required artifacts for Application Enablement Services Release 7.1.3 202
Required artifacts for Application Enablement Services Release 7.1.3.0.1 203
Required artifacts for Application Enablement Services Release 7.1.3.0.2 203
What’s new in Application Enablement Services 7.1.x.x 203
What’s new in Application Enablement Services 7.1.3.8 203
What’s new in Application Enablement Services 7.1.3.7 204
What’s new in Application Enablement Services 7.1.3.6 204
What’s new in Application Enablement Services 7.1.3.5 204
What’s new in Application Enablement Services 7.1.3.4 204
What’s new in Application Enablement Services 7.1.3.3 204
What’s new in Application Enablement Services 7.1.3.2 204
What’s new in Application Enablement Services 7.1.3.1 204
What’s new in Application Enablement Services 7.1.3 205
What’s new in Application Enablement Services 7.1.2 205
What’s new in Application Enablement Services 7.1.1 206
What’s new in Application Enablement Services 7.1 206
VM Footprint Size and capacity 207
Enhanced Access Security Gateway (EASG)... 207
Issues related to Backup and Restore 207
Upgrading issues related to licenses and the AE Services 7.1 embedded WebLM server... 208
WebLM server compatibility.. 208
Issues related to Enterprise Directory.. 208
Issues related to SNMP 208
Alarm Viewer Change.. 208
Known issues and workarounds in Application Enablement Services 7.1.x.x 209
Known issues and workarounds Application Enablement Services in Release 7.1.3.8 209
Known issues and workarounds Application Enablement Services in Release 7.1.3.7 210
Known issues and workarounds Application Enablement Services in Release 7.1.3.6 211

Known issues and workarounds Application Enablement Services in Release 7.1.3.5 213
Known issues and workarounds Application Enablement Services in Release 7.1.3.4 214
Known issues and workarounds Application Enablement Services in Release 7.1.3.3 214
Known issues and workarounds Application Enablement Services in Release 7.1.3.2 215
Known issues and workarounds Application Enablement Services in Release 7.1.3.1 215
Known issues and workarounds Application Enablement Services in Release 7.1.3 217
Known issues and workarounds Application Enablement Services in Release 7.1.2 219
Known issues and workarounds Application Enablement Services in Release 7.1.1 220
Known issues and workarounds Application Enablement Services in Release 7.1 221
Fixes in Application Enablement Services in Release 7.1.x.x 223
Fixes in Application Enablement Services in Release 7.1.3.8 223
Fixes in Application Enablement Services in Release 7.1.3.7 223
Fixes in Application Enablement Services in Release 7.1.3.6 225
Fixes in Application Enablement Services in Release 7.1.3.5 226
Fixes in Application Enablement Services in Release 7.1.3.4 228
Fixes in Application Enablement Services in Release 7.1.3.3 229
Fixes in Application Enablement Services in Release 7.1.3.2 230
Fixes in Application Enablement Services in Release 7.1.3.0.2 231
Fixes in Application Enablement Services in Release 7.1.3.1 231
Fixes in Application Enablement Services in Release 7.1.3 232
Fixes in Application Enablement Services in Release 7.1.2 234
Fixes in Application Enablement Services in Release 7.1.1 234
Fixes in Application Enablement Services in Release 7.1 234
Avaya Aura® Utility Services 235
Installation for Avaya Aura® Utility Services Release 7.1.x.x 235
Installation for Avaya Aura® Utility Services Release 7.1.3.8 235
Installation for Avaya Aura® Utility Services Release 7.1.3.7 235
Installation for Avaya Aura® Utility Services Release 7.1.3.6 235
Installation for Avaya Aura® Utility Services Release 7.1.3.5 235
Installation for Avaya Aura® Utility Services Release 7.1.3.4 235
Installation for Avaya Aura® Utility Services Release 7.1.3.3 235
Installation for Avaya Aura® Utility Services Release 7.1.3.2 235
Installation for Avaya Aura® Utility Services Release 7.1.3 236
Installation for Avaya Aura® Utility Services Release 7.1.2 236
Installation for Avaya Aura® Utility Services Release 7.1.1 236
Installation for Avaya Aura® Utility Services Release 7.1 236
Enhanced Access Security Gateway (EASG) 236
Speculative Execution Vulnerabilities (includes Meltdown and Spectre and also L1TF Vulnerabilities) 236
How to find License Activation Code (LAC) in PLDS for a product 237

What’s new in Utility Services Release 7.1.x.x ... 237
What’s new in Utility Services Release 7.1.3.8 ... 237
What’s new in Utility Services Release 7.1.3.7 ... 237
What’s new in Utility Services Release 7.1.3.6 ... 237
What’s new in Utility Services Release 7.1.3.5 ... 238
What’s new in Utility Services Release 7.1.3.4 ... 238
What’s new in Utility Services Release 7.1.3.3 ... 238
What’s new in Utility Services Release 7.1.3.2 ... 238
What’s new in Utility Services Release 7.1.3 ... 238
What’s new in Utility Services Release 7.1.2 ... 238
What’s new in Utility Services Release 7.1.1 ... 239
What’s new in Utility Services Release 7.1 ... 239
Fixes in Utility Services in Release 7.1.x.x ... 241
Fixes in Utility Services Release 7.1.3.8 ... 241
Fixes in Utility Services Release 7.1.3.7 ... 242
Fixes in Utility Services Release 7.1.3.6 ... 244
Fixes in Utility Services Release 7.1.3.5 ... 245
Fixes in Utility Services Release 7.1.3.4 ... 247
Fixes in Utility Services Release 7.1.3.3 ... 248
Fixes in Utility Services Release 7.1.3.2 ... 249
Fixes in Utility Services Release 7.1.3 ... 250
Fixes in Utility Services Release 7.1.2 ... 252
Fixes in Utility Services Release 7.1.1 ... 254
Fixes in Utility Services Release 7.1 ... 255
Known issues and workarounds in Utility Services in Release 7.1.x.x ... 255
Known issues and workarounds in Utility Services Release 7.1.3.8 ... 255
Known issues and workarounds in Utility Services Release 7.1.3.7 ... 255
Known issues and workarounds in Utility Services Release 7.1.3.6 ... 256
Known issues and workarounds in Utility Services Release 7.1.3.5 ... 256
Known issues and workarounds in Utility Services Release 7.1.3.4 ... 256
Known issues and workarounds in Utility Services Release 7.1.3.3 ... 257
Known issues and workarounds in Utility Services Release 7.1.3.2 ... 257
Known issues and workarounds in Utility Services Release 7.1.3 ... 257
Known issues and workarounds in Utility Services Release 7.1.2 ... 258
Known issues and workarounds in Utility Services Release 7.1.1 ... 258
Known issues and workarounds in Utility Services Release 7.1 ... 258
Avaya Aura® Communication Manager Messaging ... 259
Installation for Avaya Aura® Communication Manager Messaging 7.0.x.x ... 259
Backing up the software ... 259

Upgrade Paths (from/to System Platform) 259
File list 259
Installing the release 260
Troubleshooting the installation 260
Hardware compatibility 260
Interoperability and requirements 260
What’s new in Avaya Aura® Communication Manager Messaging Release 7.0.x.x 260
What’s new in Communication Manager Messaging 7.0.0.0 260
Fixes in Communication Manager Messaging Release 7.0.x.x 261
Fixes in Communication Manager Messaging 7.0.0.0 261
Fixes in Communication Manager Messaging 7.0.0.1 261
Known issues and workarounds in Communication Manager Messaging Release 7.0.x.x 264
Known issues and workarounds in Communication Manager Messaging Release 7.0.0.1 264
Avaya Aura® Appliance Virtualization Platform 265
Installation for Avaya Aura® Appliance Virtualization Platform Release 7.1.x.x 265
Installation for Avaya Aura® Appliance Virtualization Platform Release 7.1.3.8 265
Installation for Avaya Aura® Appliance Virtualization Platform Release 7.1.3.7 265
Installation for Avaya Aura® Appliance Virtualization Platform Release 7.1.3.6 265
Installation for Avaya Aura® Appliance Virtualization Platform Release 7.1.3.5 265
Installation for Avaya Aura® Appliance Virtualization Platform Release 7.1.3.4 266
Installation for Avaya Aura® Appliance Virtualization Platform Release 7.1.3.3 266
Installation for Avaya Aura® Appliance Virtualization Platform Release 7.1.3.2 266
Installation for Avaya Aura® Appliance Virtualization Platform Release 7.1.3 266
Speculative Execution Vulnerabilities (includes Meltdown and Spectre and also L1TF Vulnerabilities) 266
Installing the release – AVP 7.1.3.x 267
Installation for Avaya Aura® Appliance Virtualization Platform Release 7.1.2 269
Installing the release 269
Restoring software to previous version 271
Installation for Avaya Aura® Appliance Virtualization Platform Release 7.1.0.1 272
Installing the release 272
Restoring software to previous version 272
Installation for Avaya Aura® Appliance Virtualization Platform Release 7.1 272
Enhanced Access Security Gateway (EASG) 272
Installing the release 272
Troubleshooting the installation 273
Restoring software to previous version 273
What’s new in Avaya Aura® Appliance Virtualization Platform Release 7.1.x.x 273
What’s new in Avaya Aura® Appliance Virtualization Platform Release 7.1.3.8 273
What’s new in Avaya Aura® Appliance Virtualization Platform Release 7.1.3.7 273

What’s new in Avaya Aura® Appliance Virtualization Platform Release 7.1.3.6 273
What’s new in Avaya Aura® Appliance Virtualization Platform Release 7.1.3.5 273
What’s new in Avaya Aura® Appliance Virtualization Platform Release 7.1.3.4 273
What’s new in Avaya Aura® Appliance Virtualization Platform Release 7.1.3.3 273
What’s new in Avaya Aura® Appliance Virtualization Platform Release 7.1.3.2 273
What’s new in Avaya Aura® Appliance Virtualization Platform Release 7.1.3 274
What’s new in Avaya Aura® Appliance Virtualization Platform Release 7.1.2 274
What’s new in Avaya Aura® Appliance Virtualization Platform Release 7.1.0.1 274
What’s new in Avaya Aura® Appliance Virtualization Platform Release 7.1.0.0 274
Fixes in Avaya Aura® Appliance Virtualization Platform Releases 7.1.x.x 275
Fixes in Avaya Aura® Appliance Virtualization Platform 7.1.3.8 275
Fixes in Avaya Aura® Appliance Virtualization Platform 7.1.3.7 275
Fixes in Avaya Aura® Appliance Virtualization Platform 7.1.3.6 275
Fixes in Avaya Aura® Appliance Virtualization Platform 7.1.3.5 276
Fixes in Avaya Aura® Appliance Virtualization Platform 7.1.3.4 277
Fixes in Avaya Aura® Appliance Virtualization Platform 7.1.3.3 277
Fixes in Avaya Aura® Appliance Virtualization Platform 7.1.3.2 278
Fixes in Avaya Aura® Appliance Virtualization Platform 7.1.3 278
Fixes in Avaya Aura® Appliance Virtualization Platform 7.1.2 279
Fixes in Avaya Aura® Appliance Virtualization Platform 7.1.0.1 279
Fixes in Avaya Aura® Appliance Virtualization Platform 7.1 279
Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform Release 7.1.x.x 280
Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform 7.1.3.8 280
Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform 7.1.3.7 280
Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform 7.1.3.6 280
Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform 7.1.3.4 280
Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform 7.1.3.3 280
Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform 7.1.3.2 281
Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform 7.1.3 285
Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform 7.1.2 288
Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform 7.1 291
Languages supported 293
Avaya Aura® G430 and G450 Media Gateways 294
Installation for Avaya Aura® G430 and G450 Media Gateways Release 7.1.x.x 294
Required patches 294
Pre-Install Instructions 295
File Download Instructions 295
Backing up the software 296
Installing the release 296

Troubleshooting the installation 297
Restoring software to previous version 297
Meltdown and Spectre Vulnerabilities 297
What’s new in Avaya Aura® G430 and G450 Media Gateways Release 7.1.x.x 298
What’s new in G430 and G450 Media Gateways Release 7.1.3.7 (Builds 39.49.00 and 39.49.30) 298
What’s new in G430 and G450 Media Gateways 7.1.3.6 (Builds 39.40.00 and 39.40.30) 298
What’s new in G430 and G450 Media Gateways Release 7.1.3.5 (Builds 39.34.00 and 39.34.30) 298
What’s new in G430 and G450 Media Gateways Release 7.1.3.4 (Builds 39.27.00 and 39.27.30) 298
What’s new in G430 and G450 Media Gateways Release 7.1.3.2 (Builds 39.16.00 and 39.16.30) 298
What’s new in G430 and G450 Media Gateways Release 7.1.3 (Builds 39.12.00 and 39.12.30) 299
What’s new in G430 and G450 Media Gateways Release 7.1.2 (Builds 39.05.00 and 39.05.30) 299
What’s new in G450 Media Gateways Release 7.1.0.5 (Builds 38.21.03 and 38.21.33) 299
What’s new in G430 and G450 Media Gateways Release 7.1.0.4 (Builds 38.21.02 and 38.21.32) 299
What’s new in G430 and G450 Media Gateways Release 7.1.0.3 (Builds 38.21.01 and 38.21.31) 300
What’s new in G430 and G450 Media Gateways Release 7.1.0.2 (Builds 38.21.00 and 38.21.30) 300
What’s new in G430 and G450 Media Gateways Release 7.1.0.0 (Builds 38.18.00 and 38.18.30) 300
Fixes in G430 and G450 Media Gateways Release 7.1.x.x 304
Fixes in G430 and G450 Media Gateways Release 7.1.3.7 (Builds 39.49.00 and 39.49.30) 304
Fixes in G430 and G450 Media Gateways Release 7.1.3.6 (Builds 39.40.00 and 39.40.30) 304
Fixes in G430 and G450 Media Gateways Release 7.1.3.5 (Builds 39.34.00 and 39.34.30) 304
Fixes in G430 and G450 Media Gateways Release 7.1.3.4 Hotfix (Builds 39.28.00 and 39.28.30) 305
Fixes in G430 and G450 Media Gateways Release 7.1.3.4 (Builds 39.27.00 and 39.27.30) 305
Fixes in G430 and G450 Media Gateways Release 7.1.3.3 (Builds 39.20.00 and 39.20.30) 306
Fixes in G430 and G450 Media Gateways Release 7.1.3.2 (Builds 39.16.00 and 39.16.30) 307
Fixes in G430 and G450 Media Gateways Release 7.1.3 (Builds 39.12.00 and 39.12.30) 307
Fixes in G430 and G450 Media Gateways Release 7.1.0.1 (Builds 38.20.01 and 38.20.31) 308
Fixes in G430 and G450 Media Gateways Release 7.1.0.0 (Builds 38.18.00 and 38.18.30) 308
Known issues and workarounds in G430 and G450 Media Gateways 308
Languages supported 308
Documentation errata 308
Avaya Aura® Media Server 309
Avaya WebLM 310
Installation for Avaya WebLM Release 7.1.x.x 310
Installation for Avaya WebLM Release 7.1.3.8 310
Installation for Avaya WebLM Release 7.1.3.7 310
Installation for Avaya WebLM Release 7.1.3.6 310
Installation for Avaya WebLM Release 7.1.3.5 310
Installation for Avaya WebLM Release 7.1.3.4 310
Installation for Avaya WebLM Release 7.1.3.3 311

Installation for Avaya WebLM Release 7.1.3.2 311
Installation for Avaya WebLM on VMware Release 7.1.3.1 311
Installation for Avaya WebLM Release 7.1.3 311
Speculative Execution Vulnerabilities (includes Meltdown and Spectre and also L1TF Vulnerabilities) 311
Installation for Avaya WebLM Release 7.1.2 312
Installation for Avaya WebLM Release 7.1.1 312
Installing the release 7.1.x 312
Resource allocation and reservation for standalone WebLM on VMware 313
Software information 314
Troubleshooting the installation 314
Contacting support 314
Contact support checklist 314
What’s new in Avaya WebLM for 7.1.x.x 315
What’s new in Avaya WebLM for 7.1.3.8 315
What’s new in Avaya WebLM for 7.1.3.7 315
What’s new in Avaya WebLM for 7.1.3.6 315
What’s new in Avaya WebLM for 7.1.3.5 315
What’s new in Avaya WebLM for 7.1.3.4 315
What’s new in Avaya WebLM for 7.1.3.3 315
What’s new in Avaya WebLM for 7.1.3.2 316
What’s new in Avaya WebLM for 7.1.3.1 316
What’s new in Avaya WebLM for 7.1.3 316
What’s new in Avaya WebLM for 7.1.2 316
What’s new in Avaya WebLM for 7.1.1 316
What’s new in Avaya WebLM for 7.1 316
Fixes in Avaya WebLM on VMware for 7.1.x.x 317
Fixes in Avaya WebLM on VMware for 7.1.3.8 317
Fixes in Avaya WebLM on VMware for 7.1.3.7 318
Fixes in Avaya WebLM on VMware for 7.1.3.6 319
Fixes in Avaya WebLM on VMware for 7.1.3.5 319
Fixes in Avaya WebLM on VMware for 7.1.3.4 320
Fixes in Avaya WebLM on VMware for 7.1.3.3 321
Fixes in Avaya WebLM on VMware for 7.1.3.2 322
Fixes in Avaya WebLM on VMware for 7.1.3.1 322
Fixes in Avaya WebLM on VMware for 7.1.3 322
Fixes in Avaya WebLM on VMware for 7.1.2 322
Fixes in Avaya WebLM on VMware for 7.1.1 323
Fixes in Avaya WebLM on VMware for 7.1 323
Known issues and workarounds in Avaya WebLM on VMware for 7.1.x.x 323

Known issues and workarounds in Avaya WebLM on VMware for 7.1.3.8 ... 323
Known issues and workarounds in Avaya WebLM on VMware for 7.1.3.7 ... 323
Known issues and workarounds in Avaya WebLM on VMware for 7.1.3.6 ... 324
Known issues and workarounds in Avaya WebLM on VMware for 7.1.3.5 ... 324
Known issues and workarounds in Avaya WebLM on VMware for 7.1.3.4 ... 325
Known issues and workarounds in Avaya WebLM on VMware for 7.1.3.3 ... 325
Known issues and workarounds in Avaya WebLM on VMware for 7.1.3.2 ... 325
Known issues and workarounds in Avaya WebLM on VMware for 7.1.3.1 ... 326
Known issues and workarounds in Avaya WebLM on VMware for 7.1.3 ... 326
Known issues and workarounds in Avaya WebLM on VMware for 7.1.2 ... 326
Known issues and workarounds in Avaya WebLM on VMware for 7.1.1 ... 327
Known issues and workarounds in Avaya WebLM on VMware for 7.1 ... 327
Avaya Aura® Device Services ... 328

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
4	11-May-2017	Addition of important note regarding Utility Services Patches.
5	15-May-2017	Addition of Zephyr-52087 to known issues section for Presence.
6	25-May-2017	Modified Session Manager upgrade procedures for AADS customers
7	07-June-2017	Updates for re-spin of Utility Services 7.1 to Build 17.
8	29-June-2017	Updates for Avaya Aura® System Manager Release 7.1
9	11-July-2017	Updates for Avaya Aura® Utility Services
10	14-Aug-2017	Updates for Avaya Aura® Release 7.1.1
11	01-Sept-2017	Updated the Product Release Matrix table
12	07-Sept-2017	Updated the Product Release Matrix table
13	13-Oct-2017	Added information related to Avaya Aura® System Manager Release 7.1.1.1 Service Pack
14	11-Dec-2017	Updates for Avaya Aura® Release 7.1.2
15	05-Jan-2018	Removed Avaya Aura® Media Server information from this document and added reference to the Avaya Aura® Media Server Release 7.8 Release Notes that contains all the required information.
16	07-Jan-2018	Updated the note for the supported version of CMM Release 7.0.0.1 on a new AVP Release 7.1.2 host.
17	16-Jan-2018	Updated the file name, PLDS File ID, and PCN number for Avaya Aura® Communication Manager Kernel Service Pack. Updated the file name and PLDS File ID for Avaya Aura® Appliance Virtualization Platform.
18	16-Feb-2018	Updated the Presence Services release notes section to include an update related to the Presence Services Web UI.
19	30-Apr-2018	Updates for Avaya Aura® Release 7.1.3
20	04-June-2018	Updates for Branch Gateway G430/G450 Release 7.1.0.3 Builds 38.21.01 and 38.21.30
21	06-Aug-2018	Updates for Avaya Aura® Release 7.1.3.1
22	22-Oct-2018	Updates for Avaya Aura® Release 7.1.3.2
23	12-Nov-2018	Updates for Branch Gateway G430/G450 Release 7.1.0.4 Builds 38.21.02 and 38.21.32
24	11-Feb-2019	Updates for Avaya Aura® Release 7.1.3.3
25	14-Feb-2019	Updated the OVA file names for Avaya Aura® Application Enablement Services
26	15-Feb-2019	Updated the info for Avaya Aura® Application Enablement Services. New OVA re-issued for ACP100 series 2200GHz CPU used for profiles 2 and 3.

Issue	Date	Description
27	08-Jul-2019	Updates for Avaya Aura® Release 7.1.3.4
28	14-Aug-2019	Updates for the Fixes in G430 and G450 Media Gateways Release 7.1.3.3 Builds 39.20.00 and 39.20.30
29	9-Sep-2019	Updates for Installation and What's New in G430 and G450 Media Gateways Release 7.1.0.5 Builds 38.21.03 and 38.21.33. Updates for the Fixes in G430 and G450 Media Gateways Release 7.1.3.4 Builds 39.28.00 and 39.28.30.
30	20-Dec-2019	Updates for Avaya Aura® Release 7.1.3.5
31	08-Jan-2020	Removed notes from Avaya Aura® Communication Manager section.
32	16-Jan-2020	Updated for What's new in Application Enablement Services 7.1.3.5.
33	20-Jan-2020	Updated the Kernel Service Pack and Security Service Pack PCN number for CM
34	13-April-2020	Updates for Avaya Aura® Release 7.1.3.6
35	24-June- 2020	Updates for the Fixes in Session Manager Release 7.1.3.6 section.
36	13-July-2020	Updates for the Fixes in Session Manager Release 7.1.3.5 section.
37	26-Aug-2020	Added the System Manager upgrade path section.
38	09-Nov-2020	Updates for Avaya Aura® Release 7.1.3.7.
39	11-Jan-2021	Updates for Avaya Aura® Release 7.1.3.8.
40	13-Jan-2021	Updates for the Fixes in Application Enablement Services in Release 7.1.3.8 section.
41	15-Mar-2021	Updates to the "Installation for Avaya Aura® Appliance Virtualization Platform Release 7.1.3.5" and "Fixes in Avaya Aura® Appliance Virtualization Platform 7.1.3.5" sections.

Introduction

This document provides late-breaking information to supplement Avaya Aura® 7.1.x release software and documentation. For updated documentation, product support notices, and service pack information, go to the Avaya Support site at https://support.avaya.com.

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

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	7.1.3.8.0	7.1.3.7.0	7.1.3.6.0	7.1.3	7.1.2	7.1.1.1	7.1.1	7.1.0.1	7.1
Avaya Aura® Communication Manager	X	X	X	X	X	NA	X	NA	X
Avaya Aura® Session Manager	X	X	X	X	X	NA	X	NA	X
Avaya Aura® System Manager	X	X	X	X	X	X	X	NA	X
Avaya Aura® Presence Services	NA	NA	NA	NA	X	NA	X	NA	X
Avaya Aura® Application Enablement Services	X	X	X	X	X	NA	X	NA	X
Avaya Aura® Utility Services	X	X	X	X	X	NA	X	NA	X
Avaya Aura® Communication Manager Messaging (supported through 7.0.x)	NA	NA	NA	NA	NA	NA	NA	NA	NA
Avaya Aura® Appliance Virtualization Platform	X	X	X	X	X	NA	NA	X	X
Avaya Aura® G430 and G450 Media Gateways	X	X	X	X	X	NA	NA	X	X
Avaya WebLM	X	X	X	X	X	NA	X	NA	X
Avaya Aura® Device Services	NA	NA	NA	NA	NA	NA	NA	NA	X
Avaya Aura® Media Server Release 7.8.0 SP 3	NA	NA	NA	NA	NA	NA	NA	NA	X
Avaya Aura® Media Server Release 7.8.0 SP 5	NA	NA	NA	NA	NA	NA	X	NA	NA
Avaya Aura® Media Server Release 7.8.0 SP 6	X	X	X	X	X	NA	NA	NA	NA
Avaya Aura® Media Server Release 7.8.0 SP 7	X	X	X	X	X	NA	NA	NA	NA
Avaya Aura® Media Server Release 7.8.0 SP 8	X	X	X	X	X	NA	NA	NA	NA
Avaya Aura® Media Server Release 7.8.0 SP 9	X	X	X	X	X	NA	NA	NA	NA
Avaya Aura® Media Server Release 7.8.0 SP 10	X	X	X	X	X	NA	NA	NA	NA

Note:

- Customers can install CMM 7.0.0.1 on a new AVP 7.1.2 Host. The same applies for upgrades of another Avaya Aura VMs on a shared AVP host with CMM 7.0.0.1, they also can upgrade to 7.1.2.
- The Avaya Aura® System Manager release/version must always be greater than or equal to the release/version of the components of the solution (Session Manager, Communication Manager, Application Enablement Services).

What’s new in Avaya Aura®

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

Support for the next generation server platform

Avaya Aura® Release 7.1.3.3 introduces support for the next generation server platform, Avaya Converged Platform (ACP).

This release includes support for ACP 120 and ACP 130 servers.

The following 7.1.x OVAs were reissued to allow for installation on ACP 2.2GHz servers:

- Communication Manager
- Application Enablement Services
- System Manager
- WebLM

Information about Speculative Execution Vulnerabilities including Spectre/Meltdown and L1TF

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

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

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.x.x

Required patches

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

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

For more details on Kernel Service Pack and Security Service Pack see PCN2075Su on the Avaya Technical Support site https://support.avaya.com/css/P8/documents/101043464

Note 1: If System Manager (SMGR) SDM was used to upgrade from CM 7.0 to 7.1.x, reference PSN020355u - Avaya Aura® Communication Manager 7.x, 8.x Kernel and Security Service Pack Installation Failures . The pre-activation patch listed in that PSN is required when applying any 7.1 SSP or KSP if SMGR SDM was used in the upgrade process.

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.

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

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

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

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

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

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

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

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

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

What's new in Communication Manager Release 7.1.3.8

Enhancement	Description
N/A	

What’s new in Communication Manager Release 7.1.3.7

Enhancement	Description
CM-30764	When the race condition of SIP UPDATE and INVITE method in dialog was encountered, the display was not updated correctly. With the new field “Resend Display UPDATE once on Receipt of 481 Response?” on trunk-group is set to ‘Y’ then, CM will send a SIP UPDATE message for 481 response received from far end.
CM-33014	When SA9095 is enabled and the hunt-group algorithm is set to “circ” and there are no members in the hunt group, “Re-hunt on no answer” is configured and no coverage path assigned to hunt, then, the caller should hear a busy tone

What’s new in Communication Manager Release 7.1.3.6

Enhancement	Description
N/A	

What’s new in Communication Manager Release 7.1.3.5

Enhancement	Description
N/A	

What’s new in Communication Manager Release 7.1.3.4

Enhancement	Description
CM-24157	SA8157 enhancement to collect digits from the caller without sending the CONNECT message to PSTN trunk

What’s new in Communication Manager Release 7.1.3.3

Enhancement	Description
CM-23000	MLPP (Multilevel Precedence and Preemption) Call Diversion support for SIP Attendant

What’s new in Communication Manager Release 7.1.3.2

Enhancement	Description
SSP/KSP	In concurrence with the 7.1.3.2 Service Pack there is also a SSP/KSP available

What’s new in Communication Manager Release 7.1.3.1

Enhancement	Description
CM-8811	CM blocks the call origination if called number matches AAR/ARS deny pattern
CM-17729	To enhance security, 1024-bit keys and sha1 hashes are no longer available as options in the CM Certificates Signing Requests (CSR) - CM SMI configuration page

What’s new in Communication Manager Release 7.1.3

For more information see ***What’s New in Avaya Aura® Release 7.1.3*** document on Avaya Support site.

Enhancement	Description
CM-19567	Make delayed EC 500 timeout variable based on client requested timeout value
CM-17505 (SA9135) - Block Mobility Call if Service Link Call is active for H.323	If SA9135 is enabled, then the EC500 call will be blocked for a H.323 station if the station is logged in to telecommuter mode. This way, only one call will ring on the mobile phone and the user can answer that call without any interruption.

What's new in Communication Manager Release 7.1.2

For more information see ***What's New in Avaya Aura® Release 7.1.2*** document on Avaya Support site.

Enhancement	Description
(SA9134) - Send ELIN as SIP Station Number for Home User	• If SA9134 is disabled, then it will continue to send (Emergency Location Identification Number) ELIN from ip-network-map. • If SA9134 is enabled and CM SIP station makes E-911 call, then SIP station number shall be sent as calling party number to PSAP (Public-Safety Answering Point).

What's new in Communication Manager Release 7.1.1

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

Enhancement	Description
Special Application SA9131 SA9132	• A new Special Application "(SA9131) - Intercept Treatment for Calls from SM if Call Routing Missing?" provides the ability to block calls and route to intercept treatment if an invalid number is dialed. • A new Special Application "(SA9132) - Intercept Treatment for Calls from SM if Call Routing Blocked?" provides the ability to block calls and route to intercept treatment if a number is dialed that matches an AAR/ARS deny pattern or is not in the digit analysis table.
Special Application SA9133	This Special Application enables the usage of "tandem-calling-party-num" form for transferred SIP calls.
Operational Improvement	Support for KVM platform

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

Enhancement	Description
	• Discontinued support of tethereal symbolic link to tshark • Discontinued support for Telnet • Discontinued support of default server identity certificate

Security Service Pack and Kernel Service Pack

Communication Manager releases Security Service Packs and Kernel Service Packs aligned with the application release cycle. These are not intended for use by "software-only" customers

For further information on contents and installation procedures for CM 7.1.x, please see PCN2095S

Required artifacts for Avaya Aura® Communication Manager 7.1.x.x

Required artifacts for Communication Manager Release 7.1.3.8.0

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

Download ID	Artifact	Notes
CM000000935	01.0.532.0-26690.tar	CM 7.1.3.8.0 Feature Pack
CM000000936	PLAT-rhel7.2-0100.tar	Security Service Pack #10
CM000000937	KERNEL-3.10.0-1160.6.1.el7.tar	Kernel Service Pack #10

Required artifacts for Communication Manager Release 7.1.3.7.0

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

Download ID	Artifact	Notes
CM000000928	01.0.532.0-26633.tar	CM 7.1.3.7.0 Feature Pack
CM000000933	PLAT-rhel7.2-0090.tar	Security Service Pack #9
CM000000934	KERNEL-3.10.0-1127.19.1.el7.AV1.tar	Kernel Service Pack #9

Known issues and workarounds in Communication Manager Release 7.1.x.x

Known issues and workarounds in Communication Manager Release 7.1.3.8

ID	Minimum conditions	Visible symptoms	Workaround
N/A			

Known issues and workarounds in Communication Manager Release 7.1.3.7

ID	Minimum conditions	Visible symptoms	Workaround
N/A			

Known issues and workarounds in Communication Manager Release 7.1.3.6

ID	Minimum conditions	Visible symptoms	Workaround
N/A			

Known issues and workarounds in Communication Manager Release 7.1.3.5

ID	Minimum conditions	Visible symptoms	Workaround
N/A			

Known issues and workarounds in Communication Manager Release 7.1.3.4

ID	Minimum conditions	Visible symptoms	Workaround
N/A			

Known issues and workarounds in Communication Manager Release 7.1.3.3

ID	Minimum conditions	Visible symptoms	Workaround
N/A			

Known issues and workarounds in Communication Manager Release 7.1.3.2

ID	Minimum conditions	Visible symptoms	Workaround
N/A			

Known issues and workarounds in Communication Manager Release 7.1.3.1

ID	Minimum conditions	Visible symptoms	Workaround
N/A			

Known issues and workarounds in Communication Manager Release 7.1.3

ID	Minimum conditions	Visible symptoms	Workaround
CM-20423	Administer Avaya Media Server (AMS) having 9000 announcement files on Communication Manager (CM)	The “list directory” command became unresponsive, timed out and did not generate any output. Use of the AAMS Element Manager Media Management function also became unresponsive but eventually generated output but only for the first 3000 files. If the AAMS announcement content-group contains more than 3000 files, files not associated with a CM announcement extension or audio-group could not be seen.	There are several CM SAT commands available to display information about announcements. “list announcements” displays all administered announcement extensions and audio-groups. “list int-ann-source” displays valid file presence information for up to 9000 but only for those files which correspond to administered announcement extensions or audio-groups. “list directory” can be used to list all files in an announcement directory for a specific VAL, MG, or AAMS. The files are displayed whether they are associated with an administered announcement extension or not.

ID	Minimum conditions	Visible symptoms	Workaround
CM-20437	FIPs mode turned ON	Sync with SMGR failed	Disable FIPs mode. CM customers with root authority could manually change their SSH server configuration to add diffie-hellman-group14-sha1.

Known issues and workarounds in Communication Manager Release 7.1.2

ID	Minimum conditions	Visible symptoms	Workaround
CM-14121	Communication Manager (CM) configured and integrated with Computer Telephony Integration (CTI) interface supported by AES (Application Enablement Services), VDN, Hunt Group, Agent.	When Communication Manager (CM) endpoints controlled via Application Enablement Services (AES) made a call to a station over SIP trunk and routed the call to an agent via hunt-group, the agent display showed its own number instead of that of the caller.	

Known issues and workarounds in Communication Manager Release 7.1.1

ID	Minimum conditions	Visible symptoms	Workaround
CM-16774	Communication Manager (CM) system with only IPv4 address, activity on CM System Management Interface (SMI) web pages	Communication Manager (CM) System Management Interface (SMI) web pages were not accessible	Execute the following commands from command line interface (CLI) using super user login: stop –s httpd start –s httpd
CM-16892	Inter-Gateway Alternate Routing (IGAR) Avaya Aura® Media Server (AMS)	An outgoing call from a SIP endpoint Network Region (NR) with AMS to H.323 endpoint in another NR observed no talk-path.	After H.323 endpoint hold/unhold the call, talk-path did restore.

Known issues and workarounds in Communication Manager Release 7.1

ID	Minimum conditions	Visible symptoms	Workaround
N/A	CM 7.1.x on VMware® ESXi 6.5 on servers with Broadwell processors	CM VM reboots while starting the Communication manager service	Enhanced vMotion Compatibility (EVC) mode must be disabled.

Fixes in Communication Manager Release 7.1.x.x

Fixes in Communication Manager Release 7.1.3.8

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
CM-30895	Contact Center with POM transferring to a VDN before the call became stable.	Unstable POM transfer to agent did not display the customer's phone number.	6.3.1.0.0
CM-31390	SIP VDN call	SIP call could be stuck after the originator dropped the call if the originator of the call to vector SIP agent did not get 18x response before 200OK.	7.1.3.3.0
CM-33514	SIPCC station with agent logged in, agent in AuxWrk state i.e not available	The call diversion information was not displayed correctly when the call landed on an available agent after being queued for a while listening to announcement.	7.1.3.5.0
CM-35395	Call routing thru a VDN to Experience Portal, then back to CM and delivered to agent	UUI information is missing in the ASAI message after the call is transferred from Experience Portal to CM, and SIP trunking refer messages updated	7.1.3.5.0
CM-35688	ACD, hunt group	A call made to an ACD (automated call distribution) hunt group consistently requeued to the Hunt group and that drove CM (Communication Manager) towards CPU overload	7.1.3.6.0
CM-36086	CM active agent telecommuter service links	Increase max telecommuter service links from 3500 to 5000, thus allowing higher capacity.	7.1.3.1.0
CM-36235	Have ESS setup with thousands of recorded announcements on AMS	Customer is not able to listen to the AMS announcements.	7.1.3.5.0
CM-36280	One X Agents that are not ASAI controlled.	In using One X Agent, Service Link (S/L) is set for as-needed but is acting as if permanent and back to back calls are not ringing the cell phone for each new call, callers are immediately link to the cell on the same S/L.	6.3.1.0.0
CM-36403	Incoming H323 trunk call to H323 station, which is being monitored by ASAI, and this call dropped due to NATO time expires.	No ASAI drop event when call dropped due to no answer time out expires.	7.1.3.5.0
CM-36474	AAFD agents	AAFD user having intermittent login issues.	7.0.1.3.0
CM-36495	Call Center with Externally Controlled Distribution (ECD) through an AES application.	CC Elite occasionally delivered a call to an agent without informing the ECD controller that the agent was available.	7.1.3.1.0

CM-36510	Call Centers without EAS and CMS connected	Call Centers with traditional ACD (not EAS) may encounter reset of the link to CMS after adding or removing an even-digit extension from an ACD hunt group.	7.0.0.0
CM-36574	Call Centers and Oceana customers with SIP agents.	SIP Agents were not moved to AUX after several failed attempts to route multiple Oceana DAC calls to the agent.	6.3.1.0.0
CM-36726	Repeatedly pickup buttons get "stuck" and have to be cleared by Corruption team.	Occasionally, pickup buttons get "stuck" and have to be cleared by Corruption team.	7.1.3.6.0
CM-36749	Call Center with Externally Controlled Distributor and SIP agents.	An Externally Controlled Distributor sometimes received 'resource busy' upon attempt to route a call, only to find that CC Elite later sent a call to the agent.	7.1.3.6.0
CM-36781	EC500, tenancy, with inter-tenant calls blocked	Incoming calls from cell phone fails to EC500 when tenants are used and inter-tenants are blocked from calling each other.	7.1.3.5.0
CM-37560	PNs with a lot of announcements	Potential Cross talk warning occur in logs	7.1.3.3.0

Fixes in Communication Manager Release 7.1.3.7

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
CM-9508	QSIG, CM, LAR (Look ahead routing)	History Info was lost in QSIG to SIP interworking calls involving LAR	6.3.12.0
CM-9955	Incoming call, anonymous, REFER from Avaya Aura Contact Center.	Avaya Aura Contact Center was not able to route the call properly when incoming call has anonymous in From header	6.3.0.0
CM-18825	RONA/Xport station/SIP trunk	RONA (Redirect On No Answer) call that covered through an exported station to a remote coverage path got no History-Info header in the outgoing invite on the SIP trunk. As a result, the call couldn't cover to the right voice mail box	6.3.16.0
CM-21971	Un-administered codec-set, in-dialog OPTIONS message	Customer was experiencing no talk path issue when in-dialog OPTIONS request containing codec set which are not administered on CM.	7.1.2.0.0
CM-24390	SIP, hold	The first call which was held by far-end gets dropped after SM connection was restored	7.1.3.2.0
CM-26003	SIP, Proxy Authentication	SIP call failed with 407 "Proxy Authentication Required" from SM for INVITE from CM	7.1.1.0.0

CM-28731	Any servers 7.1.3.4.0 and later in the 7.1.x load line or 8.1.0.1.1 and later in the 8.1.x load line	In certain conditions, installing a patch could cause the system to issue a crit_os warning while restarting the logging service.	9.0.0.0.0
CM-28837	SIP Direct Media enabled	At times, no talk path observed on service observed calls.	7.1.3.1.0
CM-29382	Tandem calling party number form, modification of existing entries	The tandem calling number form, when they have a particular combination of entries including some with the "any" choice in the CPN Prefix column, could not be changed	7.1.3.3.0
CM-29859	ASAI, DMCC recording, SSC	ACR failed to record a call because DMCC station was reported busy after a CM system warm start.	8.0.1.1.0
CM-31376	ip-codec-set - On page 1, media-encryption is set. For FAX, t.38-G711-fallback is set.	T38 Fax fallback to G711 with encryption failed	7.0.1.3.0
CM-31390	SIP VDN call	SIP call could be stuck after the originator dropped the call if the originator of the call to vector SIP agent did not get 18x response before 200OK.	7.1.3.3.0
CM-31853	Outbound call, CM, ASAI	When 3rd party application requested a snapshot of the outbound call, CM 8.x did not send trunk as second leg.	8.0.1.2.0
CM-31857	SA9095	Hunt group using SA9095 queuing did not work as expected	8.0.1.2.0
CM-31863	SA9124	In ASAI transferred event, both calling and connected number were similar when SA9124 was enabled	7.1.3.3.0
CM-31864	CM, AMS	Calls got stuck in vector queues after interchange	7.1.3.5.0
CM-31877	SIP call is dropped.	In rare circumstances a SIP call may be dropped.	7.0.1.3.0
CM-31911	Monitor SIP station	End user received receive in-correct state of station in response to ASAI status station query.	7.0.0.0
CM-31930	Call pickup, H.323 station	Call continues ringing on H323 station on answering of call by another station using call pickup button	7.1.3.4.0
CM-32137	SIP, transfer, SIPS URI, TCP	Blind transfer failed when CM sends request uri with sips and the far end response with “503 Service Unavailable”, with mixed use of TLS and TCP across the solution.	7.1.1.0.0
CM-32139	Tandem call, VDN, ASAI	In ASAI ALERT message, VDN number was seen instead of actual called party number.	7.1.3.4.0

CM-32837	AMS and recording	Callers hear incorrect ring back tone if the caller and AMS were in different locations	8.1.1.0.0
CM-32993	SIP, transfer, hunt group	When a SIP phone attempted to transfer a hunt group call, transfer failed	7.1.3.5.0
CM-33020	SIP session interval timer	For cancelled SIP-A to SIP-B call, CM sent 422 instead of 487 if SIP-B responded with 422 to the INVITE.	6.2.0.0
CM-33023	3rd Party SIP Endpoint, CM, SM	3rd Party SIP end point was crashing on receiving 422 instead of 487 for canceled call	7.1.3.5.0
CM-33039	H323 1xagent	1X Agent on Citrix Server could be stuck and consistently sent KARRQ (keep alive registration request) with obsolete endpointID without stop, that would cause CM (Communication Manager) overload.	7.1.3.0.0
CM-33062	h323 sig group	CM could experience a segmentation fault and a server interchange when an H323 sig group with "RRQ Required" set to "y".	8.0.1.1.0
CM-33065	ASAI, alerting and connected event, bridge-appearance	Alert and connected events were missing when transfer is completed using the bridge-appearance	8.0.1.1.0
CM-33095	SIP transfer	SIP transfer could fail if the refer-to URI has no user portion in the refer header when the SEMT (SIP Endpoint Managed Transfer) was turned on.	8.0.1.2.0
CM-33185	predictive calling/Dial-er	When Predictive call was made via AES to CM and customer, Customer was not connecting to Agent	8.1.0.2.0
CM-33205	Server duplication	System may crash after the interchange after an upgrade.	8.1.2.0.0
CM-33210	CAG(coverage answer group), pickup group, call coverage	No ASAI Redirected event was sent when call is answered by pickup feature of coverage answer group call	8.1.1.0.0
CM-33214	Coverage path with several out of service stations as coverage points before an in-service coverage point station. Call goes to coverage and is answered by the in-service coverage point station, and then a single step conference is requested via CTI.	Single Step Conference (SSC) can incorrectly fail when coverage path includes stations which are not in-service before an in-service coverage point station answers the call. This can lead to CTI call recording failures after failed routing to coverage points.	7.1.3.5.0
CM-33251	Look Ahead Inter flow between 2 CMs	CTI-Applications was not receiving the delivered/Alert event for a customer call was queued to trunk and vector steps having multiple LAI(Look Ahead Inter flow) failed and connected to final Agent.	7.1.3.2.0

CM-33316	Any system running CM8.1	A listen socket was opened on port 111 for CM and reported as a vulnerability by a security scanner.	8.1.1.0.0
CM-33331	voice mail	When the call went to the voice mail, CM (Communication Manager) could experience a segmentation fault.	7.1.3.4.0
CM-33345	H.323 trunks, 2 CMs	Dropped calls during a H245 messaging race condition	7.1.3.2.0
CM-33364	EC500	When a call was termed to an EC500 trunk, the media resource region was chosen from the principal instead of the EC500 trunk. As a result of this. wrong media codec was chosen for the call.	7.1.3.0.0
CM-33371	CM, AMS, interchange	There was a segmentation fault observed during CM interchange with active AMS SIP sessions	7.1.0.0.0
CM-33386	Endpoint that was both part of a hunt group and part of a multimedia complex.	CM (Communication Manager) could experience a segmentation fault when a call termed to an endpoint that was both part of a hunt group and part of a multimedia complex.	8.0.1.1.0
CM-33397	Avaya Media Server	Avaya Media Server connected to duplicated CM and when the interchange happens, CM was generating core-dump	8.1.3.0.0
CM-33398	ANAT configuration	MCD on interchange when exactly at same time, 420 with sdp-anat not supported is received for a ANAT INV Offer and CM attempts to resend non-ANAT offer.	8.1.3.0.0
CM-33414	3rd party SIP endpoint	Call is dropped.	7.1.3.4.0
CM-33415	Hunt Group, hunt coverage	Hunt coverage call did not follow to Message Adjunct Hunt group.	7.1.3.5.0
CM-33433	SIP, blind transfer, drop event	Missing drop event for the agent on the held leg of the call for an IVR SIP blind transfer to an incorrect / intercepted number	8.1.1.0.0
CM-33514	SIPCC station with agent logged in, agent in Aux Work state i.e not available	The call diversion information was not displayed correctly when the call landed on an available agent after being queued for a while listening to announcement.	7.1.3.5.0
CM-33529	EC500	It was required to have an extend button for the EC500 delayed call to be launched successfully.	7.1.3.5.0
CM-33530	OneX Station	Non-OneX stations show one-X Server Status as trigger or normal, causing misbehavior of calls termed to that station.	7.1.3.3.0

CM-33587	AMS and announcement/music on AMS	Occasionally an inter Gateway connection can lead to a segmentation fault	7.1.3.3.0
CM-33599	SIP station	When a Non-SIP administered set type was put in the off-pbx station form for OPS SIP station registration, proc error 7171 8936 could be seen in /var/log/ecs log file and the call-appr in the expansion module wouldn't function well on the SIP station.	7.1.3.4.0
CM-33606	Mempool Error	Internal software memory error did not capture the corrupted memory	7.1.3.4.0
CM-33653	Telecommuter agent, NICE call recorder	Some telecommuter agent calls were stopped being recorded by NICE	7.1.3.3.0
CM-33734	sip	Double deletion MEMPOOL error for Class Bytes_32 was seen in /var/log/ecs.	7.1.3.4.0
CM-33744	AMS, interchange, CIQAA	After an AMS interchange, CIQAA happened due to corruption of service link	7.1.3.4.0
CM-33752	SIP agent	CM (Communication Manager) would drop the queued hunt call if the sip agent returned 500 error response.	7.1.3.2.0
CM-33777	SNMP users with FIPS enabled.	Cannot remove V3 SNMP users from polling, incoming traps and traps when FIPS enabled.	7.1.3.5.0
CM-33817	Native H.323 phone	CM (Communication Manager) could experience a system restart when the native h.323 station's MWL (message waiting lamp) button was audited through maintenance.	8.0.1.1.0
CM-33833	EC500, FAC, transfer	FAC for transfer from EC500 failed for transfer complete	7.1.3.6.0
CM-33850	one-x server	One-X server call back call could be dropped occasionally.	8.0.1.2.0
CM-33852	SIP Direct Media off	For initial INVITE with hold audio SDP, CM sent 200 with audio port 0 in 200 OK, causing call drop	7.1.3.5.0
CM-33853	Circular hunt group	The first call to a circular hunt group will fail after the system starts up.	7.1.3.2.0
CM-33873	dual reg	For a DUAL registration configured extension, if the administered set type was H323 station type and the h323 station was registered and SIP station not registered, a call to this extension would follow the Coverage Path Point "Logged off/PSA/TTI" rule for coverage.	7.1.3.6.0
CM-33927	SIP, SRTP	Unattended transfer fails for SIP calls with encryption	7.1.3.3.0

CM-33940	Duplicate a DS1FD station type.	The SAT "duplicate station" command hangs and causes system reset when duplicating a DS1FD set type.	7.1.3.0.0
CM-33943	SIP call	SIP station call failed with 400 Bad Request since CM (Communication Manager) put invalid (0xff) in the "From" header of the outgoing Invite message to the SIP station intermittently.	8.1.0.1.1
CM-34056	Cisco CSM, CM, AES, IVR, DS1FD	Cisco's CSM restarted when the call scenario to CM involved multiple transfers and conferences.	7.1.3.0.0
CM-34079	EC500, ACD, hunt group	IP station port was corrupted after failed EC500 call on ACD hunt group agent. IP phone becomes unusable and the agent stops getting calls. It requires a CM reboot to fix this.	7.1.3.2.0
CM-34104	Call transfer, AAM, coverage	Incoming AEP call to station that is transferred to another station, results in the caller being relayed the generic greeting when the call covered to voicemail	7.1.3.5.0
CM-34105	System Manager	International characters can be truncated when using System Manager Native Names feature.	8.1.2.0.0
CM-34131	bridge-appearance, transfer	When transfer to a VDN is attempted from bridge appearance then EVNT_ALERT was not sent when agent logged in	7.1.3.7.0
CM-34144	AMS, announcement	Delay in playing an announcement from AMS	7.0.0.1.0
CM-34177	iOS app, SIP direct media, EC500	When iOS app which is in background, answers incoming call using INVITE replaces, sometimes it resulted in no audio	8.0.0.1.2
CM-34205	SIPCC agent	Busy/Release a SIPCC phone could potentially drop a SIP trunk call owned by other SIP station.	7.1.3.5.0
CM-34236	pick up group	CM (Communication Manager) could experience a segmentation fault after a warm restart due to an internal pick up group audit.	7.1.3.0.0
CM-34296	SIP, multiple inter CM calls	Sometimes CM denied conference involving two SIP stations and one SIP trunk.	8.1.3.0.0
CM-34425	Station Service State query	Response to "Station status query" had service state as unknown	7.1.3.5.0
CM-34436	Voicemail, inter PBX call, X port	Call routing did not cover to voicemail when call originated on different PBX	7.1.3.2.0

CM-34437	AAM system with SNMP.	The snmpinctrapconfig command fails in Voice Messaging Stand Alone mode.	7.1.3.3.0
CM-34440	J179 SIP station, pickup, hunt group	J179 SIP popup did not work when call routed through hunt group to pickup group.	7.1.3.2.0
CM-34467	MOH, SIP direct media, incoming trunk call	ISG unhold event was not received when incoming trunk call to hunt and hold/resume from agent	8.1.2.0.0
CM-34505	Contact Center, Circular hunt group	Sometimes circular hunt group calls resulted in an internal software loop leading to reset of CM.	7.1.3.6.0
CM-34522	CM, station service state, SIP reachability	When a device force re-registers and if NOTIFY with terminated state comes later, CM sets the registered state as unregistered	7.1.3.7.0
CM-34523	H323 phone	An H323 phone's TCP socket could be stuck after a Duplicate CM (Communication Manager) server interchange.	7.1.3.4.0
CM-34646	SIP, H.323 trunks	Sometimes SIP/H.323 calls resulted in CM interchange	7.1.3.2.0
CM-34653	sip agent	The call was returned to the skill after AAFD (Avaya Agent For Desktop) responded 380 with "Line Appearance In Use" to the incoming Invite. The direct agent call that got 380 response with "Line Appearance In use" should be redirected to the agent's coverage path or "Redirect on IP/OPTIM Failure" VDN if agent coverage path is not configured.	7.1.3.3.0
CM-34676	R2MFC, call coverage	Call from a R2MFC trunk on a Port Network to a station which then cover-all to another R2MFC trunk did not have a Talk Path after answer.	8.1.1.0.0
CM-34697	Announcement, recording	When customer tried to change the source location for announcement, object already in use was displayed and when trying to rerecord the announcement, denial event 1052 was generated	7.1.3.6.0
CM-34993	Incoming trunk call, two VDNs, hunt group, coverage answer group, CTI monitoring	ASAI alert event contained the VDN number in CALLED PARTY information instead of hunt group extension, when the call was routed through multiple VDNs and covered via Coverage-Answer-Group.	7.1.3.6.0
CM-35035	RONA calls, route to external number	Some RONA call failed to route to external number	7.1.3.4.0

CM-35040	Call Center with SIP agents on a 7.1 release of 96x1SIPCC or other newer SIP phones that allow the agent to 'transfer now' using a plain REFER.	Call Centers with SIP agents on stations that perform blind REFER may notice some calls transferred by those agents are not correctly tracked on CMS. The original SIP agent stations did not support a blind (plain) REFER.	7.1.3.2.0
CM-35055	Capability negotiation	CM didn't send 200 OK to in dialog OPTIONS when the negotiated SDP is encrypted causing call failures	8.1.2.0.0
CM-35075	Multiple ISDN trunks with Path replacement enabled	When the path replacement triggered CM was not sending the disconnect event to CTI-Application	7.1.3.5.0
CM-35100	SIP station, coverage	Principal SIP station gave audible ring even when call was ringing on the coverage point.	6.3.118.0
CM-35129	One X Agent, service link	In using One X Agent, Service Link (S/L) is set for as-needed but was acting as if permanent, and back to back calls were not ringing cell phone for each new call, and callers were immediately linked to the cell on the same S/L.	7.1.3.3.0
CM-35166	AAEP, blind transfer	Intermittently, blind transfer from AAEP to agent caused no talk path	7.1.3.7.0
CM-35275	CTI, recording	One of the calls was not recorded when an internal software data structure array boundary condition was met	8.0.1.2.0
CM-35366	CM interchange, warm restart, H.323 stations/trunks	Sometimes H.323 calls resulted in CM interchange	7.1.3.4.0
CM-35431	ASAI, bridge appearance	Drop/disconnect event was not received when bridge-appearance dropped	7.1.3.6.0
CM-35557	SIP station, Logged off/PSA/TTI, coverage path	Logged off SIP station with Logged off/PSA/TTI? was disabled for coverage path, and caller received ring back instead of busy tone.	7.1.3.6.0
CM-35621	Announcement, re-recording	When trying to rerecord the announcement, denial event 1052 was generated	7.1.3.6.0
CM-35687	PRI trunks	Sometimes CM reported a segmentation fault when processing calls over PRI trunks	8.1.2.0.0
CM-35688	ACD, hunt group	A call made to an ACD (automated call distribution) hunt group consistently requeued to the Hunt group and that drove CM (Communication Manager) towards CPU overload	7.1.3.6.0
CM-35756	Empirix h323 stations	Empirix phone couldn't make calls after the TCP link was down and it recovered back.	7.1.3.6.0

CM-35810	unlock_time is set to 0	System will report that the login was not locked (even though it is) when the unlock_time is set to 0.	7.1.2.0.0
CM-35843	CC Elite Call Center with Externally Controlled Distribution (ECD) special application 9137 activated. SA9137 is only used for integration with the ECD EBP product.	CC Elite customer with Externally Controlled Distribution (ECD) SA9137 activated, and agents that placed outgoing calls may have delays in delivery of calls to ECD enabled skills.	7.1.3.6.0
CM-35877	Calling-party number conversion, tandem calls	CM sat "CALLING PARTY NUMBER CONVERSION FOR TANDEM CALLS" form lost entries when "all" used in "delete" field sometimes.	8.1.1.0.0
CM-35979	Elite with CMS release 18 or higher connected.	When an agent has more than 80 skills erroneous information is sent to CMS, sometimes causing the link to bounce.	7.1.3.0.0
CM-35991	High volume of DSP resources in a network region.	CM SAT 'list measurements ip dsp-resource hourly' command displayed incorrect data that overflows the 'DSP Usage' field when high volume of DSP resources was used for an IP network region.	7.1.3.5.0
CM-36009	CC Elite with special application SA9137 activated for Externally controlled distribution (ECD)	False agent available messages were being sent to the ECD EBP product. This fix only applies to customers with SA9137 and ECD EBP deployed.	7.1.3.6.0
CM-36126	Domain controlled SIP endpoint, Enhanced Call Forward	No CTI notification was sent for ECF (Enhanced Call Forward) invocation via button by SIP endpoints	7.1.3.4.0
CM-36199	Call appearance, EC500, IX workplace	Sometimes call appearance hangs after making EC500 call with IX Workplace	7.1.3.5.0
CM-36231	Unregistered SIP hunt-group user, EC500 enabled.	Unregistered SIP hunt-group user did not ring with EC500 enabled	8.1.2.0.0

Fixes in Communication Manager Release 7.1.3.6

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
CM-15861	AAM (Avaya Aura Messaging) 7.0	Restore backup from Server (Maintenance)>Data Backup/Restore screen did not result in a prompt to stop messaging before restoring, causing restore to fail	7.0.1.2.0
CM-23752	Incoming SIP call	Call drop when initial invite has no-media lines and re-invite is received with media lines	7.1.0.0.0
CM-25454	AMS (Avaya Aura Media Server), SIP endpoint, Announcement	User was not able to stop announcement recording if announcement length was 10 secs or more	7.1.3.1.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-28278	Coverage of Calls Redirected Off Net (CCRON), SIP Direct Media, call forward	Call forward off net failed in certain scenarios, if CCRON was enabled	6.3.0.0
CM-28431	Equinox SIP endpoint	Equinox transferred call could fail if the transfer target phone had LNCC (limited number of concurrent calls) feature turned on.	7.1.3.3.0
CM-28929	Enhanced call forward, AES	Enhanced call forward notification was not sent to AES (Application Enablement Services) /AES clients (in turn)	7.1.3.2.0
CM-29230	Call Center with SIP trunks.	While processing a SIP REFER without Replaces, in some cases CM incorrectly sends a trunk IDLE to CMS, resulting in CMS ignoring a call.	7.1.3.1.0
CM-29543	SIP AACC (Avaya Aura Contact Center) call	SIP trunk call could be stuck if the outgoing reinvite from CM (Communication Manager) got the BYE before the 200OK response to the reinvite.	7.1.3.2.0
CM-29272	Messaging, call coverage, numbering format	Calling user heard generic greeting instead of personalized mailbox greeting if messaging system was connected to CM (Communication Manager) directly instead of via SM.	6.3.16.0
CM-30031	Call Center with SIP Trunks using lookahead-routing (LAR) and SIP blind REFER.	CMS (call management server) ignored a call after an Experience Portal or other SIP adjunct redirected the call via SIP BLIND REFER out over a routing pattern which encountered certain types of routing failures.	7.1.3.3.0
CM-30100	More than 1024 files for backup	Backup failed if security set files exceeded count of 1024	7.1.3.2.0
CM-30403	SA8475 enabled	CM (Communication Manager) interchange if SA8475 was enabled and calls were passive monitored	7.0.0.0.0
CM-30478	SIP call with no tag in the From header	Communication Manager (CM) could experience a server interchange due to a memory issue caused by an invite SIP message that had no tag in the From header.	4.0.0.0.0
CM-30580	ASAI, monitoring, VDN	Incorrect VDN (vector directory number) information in ASAI (Adjunct Switch Application Interface) messages and CDR (call detail recording) for incoming calls to an agent	7.1.3.4.0
CM-30652	SIP INVITE, From URI having port number	Incoming SIP call was dropped by the far end if CM did not respond with port number in 180 Ringing and incoming SIP	7.1.3.2.0

ID	Minimum Conditions	Visible symptoms	Release found in
		INVITE had the port number in From URI	
CM-30653	Automatic wakeup, check out	Automatic wakeup was still active after room was checked out.	7.1.3.1.0
CM-30775	ASAI client, SIP station, blind transfer	Blind transfer failed if transfer was completed even before target party started ringing	7.1.0.0.0
CM-30883	ASAI, CTI link administration, negotiated ASAI link version	Sometimes ACR fails to record a call in spite of recording being enabled	7.1.3.4.0
CM-30919	NetSNMP with trunks.	If snmpwalk is used on avCmStatusTrunkRangeTable, due to an internal memory leak, SNMP traps/alarming were not performing as expected	7.0.0.0.0
CM-30920	Call center, Media resources, Afiniti	Calls queued while agents were available	6.3.119.0
CM-30936	SIP endpoint	The SIP endpoint's transfer button would no longer work if the SIP end point cancelled the 1st transfer attempt in the case that the field "Restrict Second Call Consult?" on the COR (class of restriction) form was set.	6.3.2.0.0
CM-31016	CM, ASAI monitored station	Under some conditions involving ASAI messaging, CM did a restart	7.0.0.0
CM-31121	SIP Hold/Unhold Notification, Network Call Redirection	Customer may experience call drop issue during transfer of a SIP call	4.0.0.0.0
CM-31134	TCP sig group, SRTP attributes in unhold INVITE	Unhold failed if unhold INVITE contained crypto attributes and insecure transport	7.1.3.2.0
CM-31135	AAR, ARS, locations	CM uses per-location ARS or AAR entry to route a call to a voice mail system, even though the all-location ARS or AAR entry was a better match	7.1.3.3.0
CM-31303	AMS	In rare circumstances the user hears no ringback on call and CPU occupancy spikes	7.1.2.0.0
CM-31326	Agents with messages.	Message Waiting Indicator audit does not audit ACD logical-agent extensions and MWI lights on agent phones may not light after reboot or upgrade.	7.1.3.2.0
CM-31334	SIP, Transfer, Conference	Failed transfer when in conference involving SIP phones, conf target initiates a blind transfer and before 180 is received from transferee, conference host completes conference.	7.1.1.0.0
CM-31371	Call Center, non-optim stations	Call work codes may not operate properly with non-optim sets on-hook	6.2.0.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-31392	CM, AMS	Calls failed due to exhaustion of AMS licenses	7.1.3.3.0
CM-31393	AMS voip license limit, CM, SIP, incorrect response code	Due to AMS voip channel license limit being hit, CM sends incorrect response code because of which SM could not route the call and the call fails.	7.1.3.3.0
CM-31409	Blast conference	CM reset sometimes during blast conference	4.0.0.0.0
CM-31472	Agent, Consultative transfer	Call dropped by CM when agent did a consultative transfer.	7.1.3.0.0
CM-31476	SIP trunk call, transfer, unstaffed agent, coverage, Single Step Conference	Call dropped when recorded agent transferred the call to an unstaffed agent	4.0.0.0.0
CM-31619	Call pickup, TSAPI user on a call	Not able to pickup the call from pick-group using 3PCC (3rd party call control) if user was already on another call	7.0.0.0.0
CM-31677	CM, hunt group traffic	The SAT command "list measurements hunt-group" sometimes displayed incorrect hunt-group number if the "Total Usage" data for that group exceeded 10,000.	7.1.3.3.0
CM-31689	CTI in use with SIP trunk with UUI Treatment set to 'service-provider'.	ASAI does not send UUI when received over a trunk with UUI Treatment set to 'service-provider'.	7.1.3.5.0
CM-31699	Multi-tenant system, incoming trunk call, LDN, SIP attendant	Incoming trunk call to a LDN (Listed Directory Number), did not route to an attendant, if it was Equinox Based Attendant group	7.1.3.5.0
CM-31704	Criteria for Logged Off/PSA/TTI Stations? Y	Call did not follow coverage path on logged off SIP station	7.1.3.4.0
CM-31726	SIP agent, ASAI	SIP agent can't cancel a call in progress via ASAI third party selective drop	7.1.3.5.0
CM-31840	MDA	Segmentation fault encountered during certain off-PBX call scenarios,	7.1.3.4.0
CM-31878	CM, G450 connected	G450 faults not alarmed on CM server	7.1.3.4.0
CM-31902	SIP INVITE, Av-Global-Session-ID header	Customer may experience system reset if incoming SIP call is received with an empty Av-Global-Session-ID header	6.3.16.0.0
CM-31974	Shared control registered for an H.323 station of 96x1 type	A segmentation fault or mempool error was seen when trying to delete an H.323 station which has a corresponding shared control station registered	6.0.0.0
CM-32812	VOA, auto-answer, call is transferred from another agent to VDN.	VOA playback aborted and auto-answer fails when call is transferred from another agent to VDN	7.1.3.5.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-32836	9650 set, shared control	Segmentation fault was observed in calls when phone was in shared controlled mode	7.0.1.3.0
CM-32951	Incoming SIP trunk call	One way talkpath if SIP trunk sends initial INVITE with sendonly followed by sendrecv REINV and call is termed to a H.323 station.	6.0.0.0
CM-32956	aut-msg-wt buttons assigned to stations	Sometimes save translation failed to complete and eventually errors out.	4.0.0.0.0
CM-32997	LSP, server ID 1	Customer could not add a lsp "survivable-processor" using "Server ID" set to 1 from the SAT.	7.1.3.4.0
CM-33015	Drop button, ACR extension, recording	Drop button on phone did not work when ACR extension was added for recording.	7.0.1.3.0

Fixes in Communication Manager Release 7.1.3.5

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
CM-10028	Telecommuter call	CM did a restart	6.3.9.1
CM-12585	Incoming call over FIPN trunk (SA8506 enabled) The calling party number must be mapped to a station in the off-pbx station-mapping form.	A call forwarded from Altura through FIPN trunk to a message center switch would get generic greeting if calling party is mapped in EC500	7.0.0.2.0
CM-16983	Breeze, Communication Manager	Call remains active on trunk user even after Communication Manager user dropped the call, when Breeze application was attempting to establish a 2-party call.	6.3.12.0
CM-18330	CM SMI	Missing HTTP Strict-Transport-Security-Header on Web help pages	7.1.0.0.0
CM-19015	Communication manager, external caller, voice mail.	Voicemail recorded by an external caller was incorrectly identified as of internal caller.	6.3.16.0
CM-20083	VDN, vector route-to with no coverage, unregistered SIP station, vector processing	Call to a VDN with vector route-to with no coverage to an unregistered SIP station failed to continue with vector processing	7.1.2.0.0
CM-21102	SIP station, H.323 telecommuter attendant	SIP station direct media call to H323 telecommuter attendant failed	7.0.1.1.1
CM-21403	Call classification, TN744 HW11	Denial event 2399 when ofcom call classification is attempted on a TN744 HW11 board	7.1.1.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-21432	Call center with SIP agents	RONAs are appearing on CMS report more than normal since SIP phones have been installed	6.3.117.0
CM-21799	WebLM server	CM did not come up since License Server took up 100% CPU when WebLM server was partially reachable	8.0.0.0.0
CM-22549	H323 softphone using SIP service link in telecommuter mode with media encryption	Softphone in telecommuter mode using permanent SIP service link will see service link drop when softphone drops a call	7.1.3.0.0
CM-22946	Communication Manager with small memory config, trunk call to vector with collect step	Segmentation fault observed when an incoming call was routed to a VDN with collect steps in the vector.	7.0.1.3.0
CM-22985	System Management Interface (SMI) and user operations	The secure log showed password in clear text when a new user was added, or an existing user password was changed using System Management Interface	7.1.3.1.0
CM-23053	Outgoing call via an analog (e.g., CO) trunk group and insert a pause character via the route pattern (e.g., to wait for far-end dial tone)	Call dropped when a call was made over an analog (e.g., CO) trunk group, with pause character added in the route pattern	7.1.2.0.0
CM-23362	Access endpoint, SOSM	The SOSM attribute of the Access Endpoint appeared to be un-checked when a passive monitor is added creating a security issue in SOSM feature.	7.1.3.0.0
CM-23510	Media Gateways in same NR having VOA announcement configured, VDN and pickup group	VOA was not played to the user when a call was picked up by pickup member and also resulting in no talkpath	7.1.2.0.0
CM-23659	CM, AMS, announcement	No denial event was logged when AMS announcement ports are out of service	7.1.2.0.0
CM-23903	SIP station	Communication Manager (CM) could experience a system segmentation fault if the termination to a SIP station returned BUSY.	7.1.3.0.0
CM-23921	EC500, call-forwarding over SIP	Via header which is used by SM to identify location of call originator was incorrect, leading to improper per location bandwidth calculation	7.1.3.1.0
CM-24016	SIP trunk, H.323 station, hair-pinning enabled	DTMF does not work with in-band or RTP-payload DTMF mode on hair-pinned calls	7.1.3.0.0
CM-24018	SIP trunk, vectors, announcement	Some incoming SIP trunk calls routed over vectors were dropped due to error response to SIP request	7.1.3.0.0
CM-24562	One-X agent, SIP service link. Agent without password administered, Direct media enabled.	Agent hears DTMF tones if they use password while logging in	7.1.1.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-24766	3 CMs, QSIIG H.323 trunk	50% of time QSIG path-replacement fails when multiple transfers are initiated. No end user visible impact.	7.1.2.0.0
CM-24845	CM, principal with Busy Indicator button, EC500 enabled on principal. SA9106 enabled	Place a call to the principal station which then rings on the EC500 station. Answer the call on the EC500 station. The BI lamp would be lit. Now drop the call and the BI lamp would not be turned off.	7.0.1.3.0
CM-25032	SIP trunk and announcement	Call transferring into Vector over SIP Trunk does not hear music.	6.3.118.0
CM-25117	AMS announcement and SIP trunk	AMS announcement will restart and play over from beginning	7.1.3.0.0
CM-25181	B179 Phone	Hold failed when attempted from B179 phone	7.1.1.0.0
CM-25387	E-911 call and SIP station	Wrong ELIN for E-911 call if ELIN is part of P-Location header.	7.0.1.3.0
CM-25441	Modifications to web access mask, SMI	If Web Access Mask is changed, and then the system is upgraded, or backup/restore operation is performed, the user is unable to access SMI pages after restore	7.1.3.2.0
CM-25597	G650 gateways connected to a flaky network.	False alarms raised against the IPSI maintenance board during network instability	7.1.1.0.0
CM-25829	SIP station with call-fwd button	J169 SIP client could not cancel the call-fwd if the call-fwd button was pushed and only ARS/AAR FAC code was put in.	7.1.1.0.0
CM-27266	Coverage Answer Group members part of the Pickup Group. Call termed on CAG group	Members of the pickup group will not get Enhanced Call Pickup alert if CAG members are part of the Pickup group and call Termed on CAG group.	7.1.0.0.0
CM-27320	SIP trunk call, SAC enabled, Voice Mail, DM enabled	A covered call was not being forwarded if SIP Direct Media was enabled	7.0.1.2.0
CM-27395	SIP station	When the field "Criteria for Logged Off/PSA/TTI Stations?" was off, the 302 redirected call to the logged off SIP station will not go to the coverage path even if the "Coverage After Forwarding?" was turned on. "chained call-forwarding" had to be turned on to make the call to cover to the coverage point.	7.1.3.1.0
CM-27466	Multiple pickup groups	Intermittently other pickup group members were getting pickup group notifications for the group to which they did not belong	7.1.2.0.0
CM-27469	A SIP trunk, SIP station, call transfer, AES	AES restarted when it received a hold event from CM for SIP transfer scenario	7.1.0.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
		where the SIP REFER method was used for transferring the call	
CM-27516	16xx set type	"disable ip-reg-tti old xxxx" command did not work for 16xx set type although 16xx set type is TTI un-named	7.1.3.0.0
CM-27648	NA	UDP sockets can be closed by sending zero-length packets.	7.1.2.0.0
CM-27673	Enable caller disconnect tone	Sometimes CMS_IDLE event is not sent in an SIP-agent call to CMS.	7.1.2.0.0
CM-27695	SIP station, coverage, Voice mail	Voicemail played a generic greeting instead of the prompt to leave a message for the called extension if "Coverage Answer Group" was the first coverage point followed by SIP MM as the second point in the coverage path	7.1.3.3.0
CM-27697	H323 station	Denial event 1941 always had ip address 0 in Data 2	7.1.1.0.0
CM-27752	AMS link down	Customer does not see CM alarm when AMS link was down, and the only warning was seen which did not alarm out	7.1.3.3.0
CM-27845	TTI enabled	Multiple ports are unable to be assigned to stations. Data conflict detected, please cancel and try again error seen on SAT. Softphones could not login.	7.1.3.2.0
CM-28028	Signaling group, DPT not enabled, typical ip-network-map configuration	DPT was not triggered from SIP station in a survivable mode	7.0.1.3.0
CM-28074	Incoming INVITE with "History-Info" headers but no "histinfo" tag in "Supported:" header.	The "History-Info" headers were not tandem'ed in the outgoing INVITE from the incoming INVITE if "Supported:" header did not have "histinfo" tag.	7.1.3.3.0
CM-28107	Auto callback, SIP	Auto-cback showed up in phone display as a national call only. The phone display only displayed the national phone number as like 0069910xxxxx instead of the full international number 0004969910xxxxx even if the number is available in the sip methods	6.3.118.0
CM-28119	Call Center	During vector processing, if DTMF tones were received, it caused no talk path on the call.	7.1.1.0.0
CM-28138	Logging Levels field logging enabled	The commandhistory file can have entries for vdn form field changes that did not occur.	7.1.3.2.0
CM-28178	Survivability servers and Avaya Aura Media Servers	In an installation with the Main server and one or more survivable servers served by Avaya Aura Media Servers (AAMS), the Main may go out of service (i.e., refuse	7.1.3.3.0

ID	Minimum Conditions	Visible symptoms	Release found in
		registrations and service to endpoints) if certain AAMS are out of service and others go out of service temporarily and come back into service.	
CM-28203	SIP traffic	Communication Manager could experience a segmentation fault during SIP traffic.	7.1.1.0.0
CM-28207	Avaya Experience Portal softphone ept registered to CM and SIP RFC2833 trunks	Avaya Experience portal stations configured on CM cannot detect DTMF input from SIP trunks using RFC2833	7.1.3.3.0
CM-28246	Incoming SIP trunk call to an agent	Incorrect CDR value for disconnect information field for incoming SIP trunk call to an agent	7.1.3.2.0
CM-28283	CM and hunt group	Calls were not routed to agent or hunt group members when a stale entry existed in off-pbx-station records, i.e. no call appearance was used, but still, an entry existed in change off pbx station	7.1.0.0.0
CM-28287	Coverage answer group, TEAM buttons monitoring the CAG SIP station members.	CM was getting strange resets, system message buffer exhaustion messages	7.1.3.1.0
CM-28429	A SIP trunk, transfer and across GW connections	Inter Gateway Connection was held by the call even after shuffling	7.1.3.1.0
CM-28544	Hold on the SBCE is set to RFC2543. MOH Disabled	No talk path in remote worker case when a bridge appearance bridged on after principal held the call and resumed after a bridge on	7.1.3.2.0
CM-28596	H.323 agent	One-x H.323 agent was not put on-hook after the caller dropped the call before the announcement finished to play to the agent	7.1.3.1.0
CM-28700	SIP station, Send All Calls button configured for the SIP station	Third-party feature activation failed on SIP station if the preferred handle configured for the third-party extension on SMGR had a different extension than the extension configured on CM.	7.1.3.1.0
CM-28792	SIP trunk call	SIP trunk member was active on a call with call record forever if the far end sent a BYE instead of a final response to CM's outgoing INVITE	7.1.3.2.0
CM-28794	Non-privileged administrator	When a non-privileged admin user logs in, they are prompted for their password a second time, then receive and error indicating that they are not allowed to run the 'customer_root_account' command.	7.1.3.3.0
CM-28811	SIP trunk call, VDN and vector having typical steps, G729 codec, "Prefer G711 for announcement" flag on change	Announcement on AMS did not get played when "prefer G711 for an announcement" was enabled	6.3.0.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
	system-parameters ip-options		
CM-28812	Auto callback	Canceling auto-callback failed when call routed from CM to SM to CM	6.3.118.0
CM-28813	IP trunks, AEP 7434ND administered stations, TN2602 media processor	Avaya Experience Portal IVR function may fail to detect customer entered digits	7.1.3.2.0
CM-28840	QSIG CAS (centralized attendant group)	Occasionally QSIG CAS calls dropped when seg fault happens	7.1.0.0.0
CM-28841	SIP phone, non AST-2 phone, equinox and call recorded	When an equinox client has recorder ports, and it merged the call in adhoc conference way, then the recorder stopped getting RTP stream	7.1.3.2.0
CM-28867	CM, call transfer to agent, ringing call	CTI-application did not receive the connect event when the transferred call was answered	7.1.3.3.0
CM-28935	AMS and administration to customize "busy-verify" tone	When using AMS, administrative customizing of busy-verify tone, will not affect warning tone, when they both should have the same tone content.	7.1.1.0.0
CM-28987	CC Elite SIPCC 9611G agents using Service Observing.	When activating service observing on a SIPCC phone, the COR of the station is checked, not the COR of the agent.	7.1.3.1.0
CM-28992	one-x H.323 agent	If the user switched PC (Personal Computer) login account where one-x agent was running and registered the one-x agent to the same CM (Communication Manager) from the new account, CM treated it as recovery phone, CM would only have one instance of the registration record, but PC has two instances of one-x agent running. That could cause unexpected flooding KARRQ msg from the obsolete registration object on PC which drove CM overload.	7.1.1.0.0
CM-29001	Softphone Agents in telecommuter mode, non-shuffable SIP trunk, permanent mode service links, NCR (Network Call Redirection) enabled	Agents in telecommuter mode, using non-shuffable SIP trunk, permanent mode service links, with NCR (Network Call Redirection) enabled experienced no talk-path during calls	7.1.3.2.0
CM-29029	ISDN-PRI trunk	Remote Automatic Callback activation occasionally failed	7.1.3.3.0
CM-29227	CM Multiple AMS/MG Music on hold Service observing	When call was put on hold the Music on hold is not played.	7.1.3.3.0
CM-29228	List trace command	Unassigned numbers looping between ASM and CM, and list trace command did not capture the appropriate information needed to troubleshoot the root cause	7.1.3.3.0

ID	Minimum Conditions	Visible symptoms	Release found in
		quickly	
CM-29253	SA9137 enabled in system, issue skill threshold status query.	ACR completely stops recording when CTI link is version 7	7.1.3.4.0
CM-29296	Call-pickup group	Call answered by call-pickup button was not getting recorded via DMCC	7.1.3.2.0
CM-29300	Single step conference	SIP station couldn't finish the transfer if the SSC (single step conference) was involved in the transferred call.	7.1.3.0.0
CM-29307	SIP, NCR	CM did reset/interchange due to NCR REFER-491 loop	7.1.2.0.0
CM-29319	BRI stations and trunks	CM did a warm restart when an internal data structure was exhausted	7.1.2.0.0
CM-29321	SA9095 enabled and SIP stations in the hunt group	Coverage to hunt group caused an internal call to remain stuck	7.1.2.0.0
CM-29340	SEMT, SIP stations	SEMT (SIP Endpoint Managed Transfer) could fail if the transferred SIP station had preferred handle configured differently from the CM (Communication Manager) administered extension	7.1.3.4.0
CM-29451	System Manager and CM	System Manager was not controlled the Signaling Group "Network Call Transfer" field correctly when in "Cut Through" mode	6.0.0.0
CM-29491	SIP agent in a call center	When a SIP REFER without Replaces tandem out through a routing pattern with a busy trunk group, CMS stopped tracking the call.	7.1.3.3.0
CM-29571	Enable SO on the SIP phone.	Call drops when SIP trunk call transferred to a SIP station which was service observed.	7.1.3.4.0
CM-29577	IP-codec-set, prefer G.711A for music enabled	With Prefer G.711A for music enabled, announcement is not heard if it is configured on AMS.	6.3.0.0.0
CM-29651	Unregistered SIP station, hunt group	SIP Phones which are unregistered are not deactivated at hunt groups resulting in inaccurate routing of hunt group calls	7.1.3.4.0
CM-29745	SIP call	In a SIP-SIP call, if 183 was received with PAI header having an extension longer than 22 characters, CM sometimes did a software restart	6.3.0.0.0
CM-29777	AAMS, SRTP encryption, H323 station or softphone	SRTP encrypted call using AMS and H323 station, will lose talkpath if call is up for greater than approx. 17 minutes and then the user does hold/unhold.	7.1.3.3.0
CM-29842	1) H.323/DCP attendant as the first coverage point of the called station.	H.323/DCP attendant initiated call transfer to voice-mail had incorrect "Hist-	7.1.3.3.0

ID	Minimum Conditions	Visible symptoms	Release found in
	2) Voice mail as the second coverage point.	Info".	
CM-29861	SIP station, media encryption, ISDN trunk	Equinox transfer failed on ISDN trunk call when IP audio was encrypted	7.1.3.4.0
CM-29946	Outbound FAX call, list trace command	Tracing an outbound fax call using the list trace station command outputs the wrong tone data	7.1.3.4.0
CM-29952	Multiple duplicated CMs sharing a common AAMS	Music on hold may be prematurely terminated	7.1.3.4.0
CM-29974	AES with a version less than 8.1 SP1 (AES 8.1.1) in use. CTI adjunct issues agent login audit query	An Agent Login Audit query issued by a CTI application failed and received an abort generated by AES with a cause value of CS0/100 (Invalid IE)	7.1.3.4.0
CM-29984	An unprivileged administrator using SMI	Unprivileged users were asked to change the password every time they logged in to the SMI	7.1.3.4.0
CM-29993	Avaya Aura Conferencing	The SIP call to AAC (Avaya Aura Conference) could be dropped if the AAC long duration audit feature was used.	7.1.3.0.0
CM-30024	Agent, call coverage, un-registered state	A direct agent call to a logged-off agent with coverage path administered didn't get cover. Instead the caller heard busy tone.	8.0.1.1.0
CM-30028	AMS media server, IP trunk, H323 station	Noise on call	7.1.3.1.0
CM-30030	EC500, DTMF	When blind transfer was done from SIP station, no XFER event was sent to CMS for measured trunks if Fast connect on orig was set to true.	8.0.1.1.0
CM-30055	1) EC500 call over SIP/H.323/PRI trunk. 2) CDR configured	Call Detail Recording was not being generated for EC500 leg after the call was dropped.	8.0.1.1.0
CM-30085	CDR, call transfer	CDR report is not getting generated for 2nd leg in case of call transfer	7.1.3.4.0
CM-30216	SIP station, call forward	On a SIP station, already set Call-Forward button does not get updated when new call forward is set using FAC	7.1.3.4.0
CM-30228	CM and AAM	CM was not sending correct number to AAM after "clear amw all" command	8.0.1.1.0
CM-30263	Auto-icom button	Pressing the Auto-ICOM button on a phone gives a busy tone	7.0.1.3.0
CM-30352	Station with active 'ringer-off' button. Try removing from SAT	A station with a lit 'ringer-off' button could not be removed by an administrator using the 'remove station' command. Error "Object in use, try again later' would be displayed.	8.0.1.1.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-30353	Call Center, Vectoring, Music, Tenant Partitioning.	wrong announcement was played on vector step "wait hearing music" when Vector Directory Number (VDN)call was redirected another VDN.	7.1.0.0.0
CM-30369	SIP transfer from Experience Portal with Interactive Voice Response.	When Experience Portal IVR (Interactive Voice Response) tried to transfer a call to an extension using '#' + digits, it could fail if the SEMT (SIP Endpoint Managed Transfer) was turned on.	7.1.3.4.0
CM-30428	SIP, 480 response with corrupt warning header	CM may experience reset	8.1.0.2.0
CM-30430	Multiple CM connected by SIP trunks Prefer G711 MOH enabled Hold/Unhold Notifications enabled	No Music on HOLD and 1 way talkpath	7.1.3.4.0

Fixes in Communication Manager Release 7.1.3.4

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
CM-7871	HTTP	Unnecessary HTTP methods disabled CEC 172968-190-P1	7.1.2.0.0, 7.0.0.0
CM-16017	Agent Display, Call Recording	Agent sets lose caller ANI when recorded by Verint	6.3.13.0
CM-16686	Call-forward over QSIG trunk/SIP trunk, team button	Team button did not alert if Call gets forwarded on QSIG trunk, forwarded-to party is logged off and EC500 is configured with disabled state.	6.3.17.0
CM-16687	Call-forward over QSIG trunk/SIP trunk - "Diversion by Reroute? y", team button	Team button didn't alert if call is routed back to same CM over QSIG trunk and forwarded-to party which is Out-of-Service	6.3.17.0
CM-17432	CDR, R2MFC Trunk	CM generated CDR as answered call for an outgoing call via R2MFC trunk and dropped before call answered	6.3.15.0
CM-18377	SIP Trunk call, Experience Portal (EP) or Voice Portal (VP)	Incoming SIP trunk call to Experience Portal (EP) or Voice Portal (VP) dropped around 15 seconds after call is transferred	6.3.17.0
CM-21023	CM	Occasionally, CM did warm reload	8.0.0.0.0, 6.3.12.0
CM-21075	SIP agent reachability or Domain Controlled SIP station reachability is enabled.	SIP Agent logged out before the maximum polling attempts for SIP agents were exhausted	7.1.3.0.0
CM-21123	SIP, CTI (ASAI)	Incorrect information about held participants shared across application when call is between two extension across CMs	7.1.3.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-21424	Avaya Aura Contact Center with two SIP agents and one caller (9620, H175 or Equinox).	Transfer event was not sent in consult mode when SIP hard phone presses transfer/conference	8.0.0.0.0, 6.3.0.0
CM-21900	Backup	BACKUP completed successfully but with Warnings for os backupset	7.1.3.0.0
CM-22058	SIP Station	Occasionally an agent did hear a beep on a call, a bridge button appeared on the station and station locked up.	7.0.1.3.0
CM-23056	Service Observe, Conference	Service Observe (SO) tone suppressed when conferencing SO station too soon	6.3.118.0
CM-23350	Analog/DECT phone present in pickup group as LAST member.	Pickup group members did not receive the accurate enhanced pickup display update.	7.1.2.0.0
CM-23609	VDN, IP (H.323) Stations	The call dropped from AAEP due to missing UUI information. The UUI information did not get pass to AES and AAEP as CM fails to build and send ALERT and CONNECTED event to AES putting UUI information.	7.1.3.1.0
CM-23712	Bandwidth management Option: shared-SM	Announcements in an audio group across regions could not be played	7.1.3.1.0
CM-23753	EC500 enabled station over ISDN/PRI trunk.	EC500 mobile connected over ISDN/PRI trunk would able to see the caller's name even when the incoming SIP trunk call had CPN restriction.	7.1.2.0.0
CM-23851	SIPCC Agent, AAAD desktop	CMS Reports ignored the conference call involving SIPCC agent using AAAD as a moderator	7.1.3.0.0
CM-23960	SA8967 is enabled. "Mask CLI/Name for internal/QSIG/ISDN Calls?" enabled on cor form. H.323 stations connected over a direct SIP trunk between two CMs.	When the caller conferences the call on its own CM, other members of the conference were able to see the identity of the called party on the trunk side.	6.3.118.0, 6.3.115.1
CM-24005	VAL Announcement	VAL-PT Alarms seen after maintenance	7.1.0.0.0, 6.3.111.0
CM-24017	Video Call, Call Recording	The Video call did not establish when call recording is enabled	7.1.3.0.0
CM-24032	Hunt group with one member. The agent must be video enabled RONA	Video enabled softphone agent cannot answer same call coming out of queue if the same agent did not answer the 1st time	7.1.3.0.0
CM-24150	(SA8734) - Enhanced Extension Display enabled. Multinational and Multi Locations enabled. Country Code was set on locations form.	Call log entry of a SIP station was incorrect when station busy on all call-appearances.	7.1.3.0.0
CM-24168	SIPCC agent, COR not enabled for DAC call	While a SIPCC agent is on an outbound call, an incoming call is delivered to the agent by Experience Portal as a DAC when the agent COR does not allow DAC. CMS ignored the call	7.1.3.1.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-24246	SIP, VDN, AES	More than one party on call and call is blind transferred to a SIP trunk via VDN, CM did not send the alert event to AES	7.1.2.0.0
CM-24260	Call Recording, ASAI	Outgoing calls from agents did not record intermittently	7.1.3.0.0
CM-24460	Voice Recorder, Attendant	CM experienced reset when ASC Voice Recorder tries to register as shared control to an Attendant	7.1.3.1.0
CM-24479	Call Coverage	Call to VDN/vector with route-to number with coverage failed to cover	7.1.3.1.0
CM-24502	Enable SA8481	An alternate Caller Line Identification (CLI) on the called device for a call over SIP trunk did not get displayed	6.3.118.0
CM-24515	Audit	Call record audit blocked from dropping stuck call.	7.1.3.2.0
CM-24548	Call Coverage	Unregistered SIP station with no bridges or EC500 failed to immediately cover to VM.	7.1.3.2.0
CM-24735	Call Recording, Path Replacement	Call recording was getting terminated after path replacement	7.1.3.2.0
CM-24767	Attendant	ASAI Connect Event was not received by CTI Application when attendant user made a call	8.0.1.0.0
CM-24770	Call Center with SIP-connected messaging adjunct	Agent calls out to voicemail which transfers to station with immediate coverage back to voicemail. CMS ignores the next call over that SIP trunk port	7.1.3.0.0
CM-24780	send-nn	EC500 Call failed when send-nn button mapped to VDN	7.1.3.2.0
CM-24897	Network Call Redirection (NCR), VDN, SIP Trunk	Occasionally, calls did not clear	7.1.3.0.0
CM-24899	ISDN Trunk, VDN	The display on the calling station was changed when the call made to a VDN over an ISDN trunk played an announcement as a part of the vector step	7.1.3.1.0
CM-24975	Direct Agent Call	The Call Handing Preference, Service objective information not sent to CMS for DAC calls sent to agent	8.0.0.1.2, 7.1.2.0.0
CM-25004	One-X CTI	Calls generated from One-X CTI application get half ring	7.1.2.0.0
CM-25028	Bridge Appearances	Few SIP bridged appearances did not ring in	7.1.3.2.0
CM-25029	Direct Media, Music-on-hold	When call was put on hold on SIP station, the remote party over the SIP trunk did not hear the music on hold	7.1.3.1.0
CM-25043	Call Center, CTI	CM sent wrong party information in response to ASAI party query request for a transferred call ringing on agent	7.1.3.2.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-25133	LSP	During call reconstruction CM LSP rebooted for every few minutes while in active mode	7.0.1.3.0
CM-25134	VDN with Voice Mail	VDN number was displayed on the voice mail box instead of the caller's number when the caller was connected to the VDN over an ISDN trunk	7.1.3.2.0
CM-25150	Field "Provide Forced Local Ringback for EC500" is disabled and "Cellular Voice Mail Detection: timed for 5 seconds" in off-pbx-telephone configuration-set form	The caller did not hear ring back when EC500 VM answers the call.	7.1.2.0.0
CM-25182	EC500	EC500 call dropped when a conferencing in an announcement.	6.3.118.0
CM-25200	IVR, Call Transfer	IVR could not able to perform transfer after receiving the call because CM sent called party information (VDN extension) with wrong type of number (NPI_TOA)	7.1.2.0.0
CM-25218	96x1 SIPCC phone	Q-Stats/VuStats feature button push failed on 9611SIPCC phone if the preferred handle was administered differently on System Manager than CM extension	7.1.3.2.0
CM-25234	VDN, SIP Call	A call routed through collect step in vector failed to collect digits and hung at the collect step	7.1.3.1.0
CM-25237	Call Center Agent	Most idle agent did not receive calls for up to 30 minutes. If the agent logs out and back in agent starts to receive calls again	7.1.2.0.0
CM-25262	SEMT (SIP Endpoint Managed Transfer, Call Forwarding	The transferred call dropped if the transfer target had call forward enabled and the call forward destination was the transferrer extension	7.1.3.2.0
CM-25300	QSIG Trunk, Call Forward	Call forward did not work if call arrives from QSIG trunk	8.0.1.1.0, 7.0.1.3.0
CM-25378	SIP Service Link, Agent	Sometimes the call transfer failed for an agent with SIP service link	7.1.2.0.0
CM-25410	Privileged administrator command line access	Unauthorized root privileges could be obtained using sudo a privileged administrator	7.1.3.2.0
CM-25463	SIP Station, Post Major Network Outage	Occasionally, SIP stations could not register or able to make SIP calls	7.1.3.2.0
CM-25488	SIP Station	CM reset when the SIP messages contains Invalid Reason header	7.1.3.4.0, 7.1.3.2.0
CM-25527	Pickup Group	SIP phone gets alerted for another pickup-group where that SIP station is not a member	7.1.3.2.0
CM-25594	Vector VDN, Auto Answer, Call Recording	No Connected event sent for an incoming trunk calls that get transferred to a SIP agent which is in auto ans mode	7.1.3.1.0
CM-25613	Hyperactive H.323 station	CM could experience heap corruption and reset if the H.323 station went into hyperactivity and	7.1.3.1.0

ID	Minimum Conditions	Visible symptoms	Release found in
		consistently sent CM a huge amount of data in a short period time.	
CM-25859	MDA	Equinox MDA (Multiple Device Access) SIP client displayed missed call log instead of incoming call log if the incoming call to the MDA extension was answered by the other MDA device.	7.1.3.2.0
CM-25871	Enabled (SA9108) - Local Time Support for CDRs	CDR printed incorrect local-time-to and local-time-from upon CDR link recovery	7.1.3.2.0, 7.1.3.1.0
CM-25912	Call Coverage, Call Forward, EC500	Trunk call did not cover if call cover is configured to same destination as call forward destination with EC500 enabled	7.1.3.3.0
CM-25925	(SA8702) - CDR Enhancements for Network? y UNIVERSAL CALL ID Create Universal Call ID (UCID)? y UCID Network Node ID: 341 Copy UCID for Station Conference/Transfer? Y	Corrupt CDR records with strange binary characters in the UCID field	7.0.1.3.0
CM-25927	Stub Network Region, Fax	Fax mode set to fax relay when fax server in stub network region	7.1.3.1.0
CM-26019	CTI, Announcement	In the conference call, missed Disconnect Event for announcement drop	7.1.3.0.0
CM-26032	SMI	Deep Secure to filter web traffic found incorrect syntax in SMI	7.1.3.1.0
CM-26068	CM, SM	CM sent 403 response to SIP INVITE instead of 50x	7.1.3.1.0
CM-26074	Group Page	If any SIP phone is unavailable and part of a group page, confirmation tone is delayed 6-8 seconds.	7.1.3.2.0
CM-26183	Missed Call Log	The missed call log for SIP phone showed incoming trunk name instead of far end caller for a "covered-all" call	7.1.3.1.0
CM-26298	CTI	CTI links failed with CM sending a zero window at TCP level to AES	7.1.2.0.0
CM-26382	Call Center with Timed After Call Work	Sometimes an auto-in agent that dropped from a call due to a network transfer could not receive ACD calls before another work mode change	7.1.3.2.0
CM-26386	Equinox	Equinox could not make or receive calls because the call appearances got stuck	7.1.3.4.0, 7.1.3.1.0
CM-26760	SIP station	If the field "Restrict Second Call Consult?" was turned on in the COR form, The SIP station couldn't make the second consult call if it cancelled the first consult call attempt.	7.1.3.2.0
CM-26851	Uniform Dial Plan	Lots of Denial Event 2400 UDP: too many conversions were generated	7.1.3.2.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-27010	Attendant	Connect Event was not received by CTI-application when attendant user made a call termed to a SIP station	7.1.3.3.0
CM-27056	ASAI	In rare instances CM did reset	7.1.3.2.0
CM-27181	Station activating call forwarding and an audit updating its lamps at the same time	Occasionally CM servers did warm interchange due to system message buffer exhaustion	7.1.3.1.0
CM-27250	Call Forward	Call Forward Override by Team Button not working if coverage criteria all outside is set	7.1.3.3.0
CM-27391	AAR/ARS	Adding AAR/ARS call type in dialplan analysis table allowed even if "ARS/AAR Dialing without FAC?" is disabled	7.1.3.0.0
CM-27407	One-X Attendant	One-X Attendant when transferring call to external number did not send Calling Party Number	7.1.3.3.0
CM-27470	VDN, ASAI	Incorrect called party number (VDN number instead of original dialed number sent in ASAI notification	7.1.3.3.0
CM-27500	Enter trunk number as 4 in "Trunk Selection" field of the "change off-pbx-telephone station-mapping" form	Unable to set high numbered TGs into the off-pbx station-mapping form with error message generated as Error encountered, can't complete request; check errors before retrying	7.1.3.2.0
CM-27524	CTI	CM sent wrong connected number info in domain control disconnect event report	7.1.2.0.0
CM-27544	Conference	Conference using bridged-appearance failed when call is answered from a VDN	7.1.3.1.0
CM-27689	MWI	CM sent bogus NOTIFY which contains both message-waiting yes and no	7.1.3.2.0
CM-27751	CM with AMS	AMS remained stuck in pending-lock state and became unusable	7.0.1.2.0
CM-28276	Unregistered SIP Stations as members in a hunt group	SIP Phones which are unregistered are not deactivated at hunt groups	7.1.2.0.0

Fixes in Communication Manager Release 7.1.3.3

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
CM-14982	Media Gateway configured for Clock Synchronization Over IP (CSoIP) with no external TDM clock source	"Status ip-synchronization oos-members" screen incorrectly shows a slave member is out of service	7.0.1.2.0
CM-20190	CLIENT ROOM turned on in COS SA8744 turned on	If the special application (SA) 8744 was turned on, a call to a station with "Client Room" enabled for its COS could potentially cause CM (Communication	7.1.2.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
		Manager) a segmentation fault when the call covered to a coverage point	
CM-20947	Conference call	CM did system reset in a rare instance CMC	7.0.1.3.0
CM-20978	Configure send-nn button and press it before launching a call from a station monitored by ASAI	Call recording fails via AES if monitored calling party presses send-nn button before placing call	7.0.0.0
CM-21314	SIP station	The page call would fail if SIP station made the page call through the autodial button	6.3.17.0
CM-21332	Outgoing trunk call. Call is answered and the connect event changed the NPI-TOA.	CTI-application sends wrong NPI-TOA in connect event impacting 3rd party applications consuming that event	7.1.2.0.0
CM-21387	Communication Manager 7.1.x or 8.0.x.	Under rare conditions, if a new user was added from the SMI and the "Force password change on next login" option was selected, the password change at first login fails with the message "Authentication token manipulation error, old password is not correct"	7.1.2.0.0
CM-21393	Converse step configured in a VDN vector and stations being monitored	Transfer operation does not result in drop indication impacting 3rd party applications.	7.0.1.3.0
CM-21434	ESS	Interchange of duplicated ESS or loss of service for simplex ESS	6.3.15.1
CM-21751	Announcements	Reset or interchange of duplicated CM.	7.1.1.0.0
CM-21853	SOSM (SA8475)	Monitoring with SOSM (SA8475) failed for IP and digital stations while redial or autodial feature used	7.1.1.0.0
CM-21856	EC500, Direct Media Enabled	CM failed to launch EC500 call leg	7.1.2.0.0
CM-21944	SA9135 is enabled H.323 station logged in telecommuter mode IP-Agent logged into the H.323 station One-X CES mapping configured for the H.323 station	OneX CES callback calls were blocked when the call was made for an IP-Agent logged into a H.323 station in telecommuter mode	7.1.3.0.0
CM-22015	"Enable Criteria for Logged Off/PSA/TTI Stations? y on system-parameters coverage-forwarding form H.323 station A with team button configured for H.323 station B. H.323 station B has EC500 configured but disabled. H.323 station B has Enhanced call forwarding (No reply) enabled to H.323 station C."	Enhanced call forwarding failed when call was made using team button speed dial to a logged-out station	6.3.18.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-22382	Enable shuffling Change SIP headers associated with display while sending SDP answer to CM	One way talk path issue may be observed	7.1.0.0.0
CM-22561	Incoming ISDN call to OneX-C station with CES integration	A missed call was observed in logs for an established call when an incoming ISDN call was made to Avaya one-x communicator with CES (Customer Enhancement service) Integration	7.1.2.0.0
CM-22569	Configure personal-co line group button on two stations and make a direct connection of their media gateways	Softkeys on station do not appear when taking a personal-CO line off hold from another station where it was answered	6.3.18.0
CM-22576	Redirections managed by endpoint locally, where server is aware about redirection feature activated for endpoint	Segmentation fault was seen on CM when the endpoints managed the call redirection and had a NULL contact for the destination.	7.1.2.0.0
CM-22599	SOSM application running a multi-party call	Under rare circumstances a reset occurred when running SOSM feature	7.1.1.0.0
CM-22670	SIP stations	Communication Manager (CM) could experience a memory leak if the far end does not respond	7.1.3.0.0
CM-22721	H.323 station with buttons administered	When any personalized button label on CM H.323 endpoint was changed to blank, the button was removed from the phone display	8.1.0.0.0, 8.0.0.0.0, 7.1.3.0.0
CM-22774	Incoming and outgoing numbering format were international and 'tandem calling party number' conversion table did not have an entry for 'insert'	Tandem Calling Party Number table entry was not prefixing outgoing digits with '+', if incoming and outgoing numbering format were of type 'international'	6.3.12.0
CM-22863	SA9114 (Expand Public Numbers to International for ASAI?) is enabled. On location-parameters form, International and country code configured with at-least 3 digits	Missing "CALLING PARTY NUMBER" in ASAI "Alert" event leading to display issues	7.1.3.0.0
CM-22969	CDR, VDN, Agent Call Transfer	CDR did not generate for an agent in case call is blind transferred to another agent or VDN	7.1.2.0.0
CM-22979	SIP stations	Barge tone was played continuously if the SIP station bridged in an EC500 call.	7.1.3.0.0
CM-23134	Monitor VDN and do predictive calling from the VDN	ASAI message for incoming call, contained default trunk number (#####) and the called number as the VDN instead of correct calling party number in case of predictive calling.	7.1.3.0.0
CM-23145	System with heavy traffic loaded and/or having a high number of measured	Hourly measurements not coming out at the top of the hour, but at random times within the hour	8.0.0.1.0

ID	Minimum Conditions	Visible symptoms	Release found in
	trunks.	Every 13th hourly measurement is missing Hourly measurements cover 65 minutes instead of 60 minutes, thus skewing the numbers (e.g., call counts are 8.3% too high)	
CM-23148	Conference, Station Display	An incorrect CLI display at the end station added to the conference	7.1.3.0.0
CM-23149	SIP transfer	Network-region was retrieved from signaling group instead of the ip-network-map form resulting in a failed call	7.1.2.0.0, 6.3.18.0
CM-23166	calltype analysis configured	User dialed from call log containing ARS/AAR code was shown on event orig went to cti-applications	7.1.3.0.0, 6.3.113.0
CM-23188	Operator Transfer Call	Call dropped when call is transferred by attendant during the redirect tone	7.1.3.0.0
CM-23335	RONA	RONA did not work properly, RONA call directed to VDN to agent went to cover immediately	7.1.1.0.0
CM-23363	Team Button Monitoring station had COR enabled, to pick up incoming call at monitoring station by going off-hook	Team Button monitoring station was not able to pick up the incoming call at monitored station, by going off-hook	7.1.3.1.0
CM-23400	SNMP enabled	Occasional segmentation fault when SNMP is starting	7.1.3.1.0, 7.1.2.0.0
CM-23500	Conference, Station Display	An incorrect CLI display at the end station added to the conference	7.1.3.0.0
CM-23537	Enhanced Pickup Group	Enhanced pickup group members did not alert	7.1.3.1.0
CM-23579	Call Park	Parked Calls are getting disconnected when recording station disconnects	7.0.1.3.0
CM-23595	A certification chain that contains more than 6 certificates which is allowed limit	TLS connections could not be established due to certificate errors	7.1.3.1.0
CM-23661	Domain control of a station, with a CTI selective drop request where the domain control is for a call that does not exist at that station	Calls are not recording, CM responding with error 98 to 3rd party selective drop	7.1.2.0.0
CM-23678	Signal button	Signal button got denial treatment when signaling an analog station	7.1.3.0.0
CM-23687	Hold, Misoperation Alerting	The call dropped when trunk call put on hold and SSC party drops with Misoperation Alerting enabled	7.1.2.0.0
CM-23742	Tenant form page 4, entry for tenant 230	At the SAT, the title of field for tenant 230 on the Tenant form page 4 is incorrectly displayed as 220	7.1.3.1.0
CM-23744	Incoming SIP trunk call with request uri of sips was tandem out another sip trunk	SIP call failed when CM did not convert	7.1.3.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
	TLS and Media Encryption is enabled and Enforce SIPS URI for SRTP is disabled on both trunks	the request URI from SIPS to SIP	
CM-23779	VDN with converse step Transfer with converse step destination	Incoming call to VDN, which will run over the converse-on step to IVR, which intern transfer back to another VDN caused no drop event to cti-application for IVR drop	8.1.0.0.0, 7.1.2.0.0
CM-23786	SIP signaling group configured	Possible Server interchanges when SAT Signaling Group field "Peer Detection Enabled" set to 'n' on SIP signaling group	7.0.1.3.0
CM-23816	Conference, Station Display	An incorrect CLI display at the end station added to the conference.	7.1.3.0.0
CM-23902	Agent State	Agents noticed they could not change states anymore from Aux to Auto-In, After Call or another Aux	7.1.0.0.0
CM-23947	Attendant, Voice Mail, Coverage	Attendant extended call to virtual station that covers to remote Voice Mail (VM) sometimes fails to complete.	7.1.2.0.0
CM-23950	Service Observe (SO)	Service observe did not drop after transfer, call continued to be monitored erroneously	7.1.2.0.0
CM-23990	TN2602 Media processor, IP stations, ip-codec-set has G726 as selected codec.	Using G726 codec without encryption with the TN2602 medpro will result in no talkpath	7.1.1.0.0
CM-23995	EC500, SIP, Display	For an incoming call user's own extension is displayed as CPN on his One-X mapped mobile	7.1.3.0.0
CM-24153	1.IP softphone agents in telecommuter mode 2. permanent SIP service links 3. codec incompatibility between caller and SIP SL far-end	Agents using telecommuter permanent SIP service links fail to get audio	7.1.3.0.0
CM-24161	Outgoing SIP trunk call, called number has PAI with Privacy ID	CM did not send calling number towards AES intermittently	7.1.3.1.0
CM-24193	SIP trunk, Direct-media enabled, and call must shuffle to TDM before terming to destination	CM reset	7.1.3.2.0
CM-24308	ASAI, Service Observe (SO), SIP, H.323	ASAI message flow for SIP versus H.323 SO of a SIP station was different For SIP SO, there was an alerting (extra message) followed by a connect. The difference in messaging caused Oceana to mishandle the call.	7.1.3.0.0
CM-24310	IPV6 procr ip-interface	An error message was seen instead of data at the SAT interface when executing a "list ip-interface all" command	7.1.3.1.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-24480	SIP station using a route-pattern that is the same as a SIP trunk-group	SIP trunk-group could not be removed due to false positive usage by a SIP station that is using a routing pattern in the "SIP Trunk" field with the same number	7.1.3.2.0
CM-24510	CM License, SMGR WebLM	SMGR 8.0 WebLM did not show license status for CM	7.1.2.0.0

Fixes in Communication Manager Release 7.1.3.2

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
CM-17702	Configure WebLM Server with IP address having 58 octets.	Communication Manager was not able to connect to WebLM having IP address with 58 octets	8.0.0.0.0, 7.1.0.0.0
CM-18777	Voice Mail, CDR	CDR did not generate for direct or transferred calls to Voice Mail	6.3.12.0
CM-20891	Vector Directory Number (VDN), E-911, Announcement	Emergency Location Identification Number (ELIN) to Public Switch Telephone Network (PSTN) did go wrong for SIP E-911 calls routed through VDN with Announcement	7.0.1.3.0
CM-20941	SIPCC, Service Observer	SIPCC Service Observer could not go to listen/talk mode from listen/only mode	7.1.2.0.0
CM-21113	CM, AMS	Media capacity for out-of-service AMS servers showed up as 50 channels instead of 0 on measurement reports	7.0.1.3.0
CM-21140	H.323 Trunk, Tandem Call	CM failed to tandem call if an incoming CPN contains '+' from ISDN/H.323 trunk	6.3.9.0
CM-21325	CM, WebLM	CM Web server did not check WebLM URL parameters, allowing invalid characters to be processed	7.1.2.0.0
CM-21364	CM, H.248 Media Gateway	CM did system restart	7.1.1.0.0
CM-21451	CM, Port network with medpro board, Multiple Network Regions	An announcement from a remote PN could not be listened	6.3.13.0
CM-21875	SIP, User to User Information (UUI)	An agent failed to get a proper screen pop regarding the outside caller due to improper UUI passed between CM	7.1.2.0.0
CM-21915	Monitored Station, Bridge Appearance, AES	CM did not send drop event to AES for principle station, if call is unhold by bridged station	7.0.1.2.0
CM-22017	CM with port network, TN2602, H323 trunks, non-CM far-end.	CM IP trunk calls might stay anchored on Media Processor (TN2602) rather than being hairpinned on TN2602	7.1.2.0.0
CM-22176	Do not administer ip-network-map and administer "CPN, ANI for Dissociated Sets:" field on change system-parameter	ELIN from "CPN, ANI for Dissociated Sets:" field did not go correctly	6.3.16.0

ID	Minimum Conditions	Visible symptoms	Release found in
	features form.		
CM-22429	SIP Endpoint Managed Transfer (SEMT) Enabled	CTI wrong or missing messages caused reporting malfunctions at TSAPI applications. For example, CIE could not count answered calls correctly.	7.1.2.0.0
CM-22447	Monitor VDN, CTI Application	Delivered Event to CTI-application sent wrong calling and called parties in case of predictive make call request from cti-application.	7.1.2.0.0
CM-22540	Communication Manager (CM) Release 7.0 (or later) Call Management System (CMS) Release R18 (or later)	CMS Link restarted when the Tenant Number is changed from CM Admin for an Externally Measured Skill while Agents are Logged in to the Skill.	7.1.2.0.0
CM-22558	CM, AMS	Announcements on AMS with "&" in the name did not play. for example: AC&ME_Greeting2	7.1.1.0.0
CM-22559	Bridged Appearance	Bridged Appearance showed active/busy preventing calls to main number.	7.0.1.2.0
CM-22570	CDR, IVR	CDR did not generate for call transferred to VDN by IVR	7.0.1.3.0
CM-22594	CM, Contact Center	Best Service Routing (BSR) polling did not work	7.1.3.0.0
CM-22668	Call Transfer, External SIP trunk and Internal H.323 (IP) trunk	External number not displayed when the transfer is completed	7.1.3.0.0
CM-22683	VDN, VOA	High runner count of cm processing error (7169) during VDN VOA call.	7.0.1.3.0
CM-22729	Equinox, Vector	Vector prompt timeout did not work when using Equinox	6.3.16.0
CM-22824	CM with PN with medpros, SIP trunk using RFC2833 for DTMF transmission.	Entering digits for a remote system such as a conference bridge with password access might fail due to failure of DTMF digits to be recognized by the conference bridge	7.1.2.0.0
CM-22843	Call Recording	FTC (Facility Test Circuit) calls did not get recorded using Single Step Conferencing	7.0.1.3.0
CM-22853	Port Network with Analog & IPSI boards	TN2793 boards generating FATAL errors because IPSI too fast for TN2793 board resulted in '(msgRetrans) no ack to AA' errors.	7.1.3.0.0
CM-22928	CMS	When an Agent with Stroke Count Buttons administered presses the 'stroke-cnt Code: 8' Button, CM reported it as a 'stroke-cnt Code: 3' Button press to CMS.	7.1.1.0.0
CM-22986	Re-hunt on No answer	Re-hunt On No Answer did not ring back on all hunt group members	7.0.1.3.0
CM-23016	Attendant Group	Denial event 1536 in queue when calling attendant group and it goes to idle state.	7.1.3.1.0
CM-23046	Run 'list trace tac' and MST call trace for same trunk group.	MST`s call trace filter unexpected messages collected	7.1.3.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-23047	One-X Agent, UUI	The UUI displayed is truncated when the Agent presses the 'uui-info' button.	7.1.2.0.0
CM-23086	SIP Trunk, VDN/Vector Calls	SIP trunk call to VDN/vector that loops doing route-to that fails with LAI is limited to DEFAULT_MAX_FORWARDS (70) attempts before the call is dropped.	7.1.3.0.0

Fixes in Communication Manager Release 7.1.3.1

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
CM-14121	Communication Manager (CM) configured and integrated with Computer Telephony Integration (CTI) interface supported by AES (Application Enablement Services), VDN, Hunt Group, Agent.	When Communication Manager (CM) endpoints controlled via Application Enablement Services (AES) made a call to a station over SIP trunk and routed the call to an agent via hunt-group, the agent display showed its own number instead of that of the caller.	6.3.15.1
CM-15539	SIP Call Transfer with Video enabled CM setup, Encryption, Avaya Aura Contact Center (AACC) Agents, 96x1 Endpoint	Transfer Call from AACC Agent to 96x1 SIP endpoint is dropped	7.1.1.0.0, 7.0.0.0
CM-15962	Multiple trunks configured	CM did reset while parsing some SIP headers	6.3.11.1
CM-15988	ESS (Enterprise Survivable Server) with SIP signaling groups	SM is unable to establish a socket to the ESS to send OPTIONs request	6.3.115.1
CM-16419	CM Trunks, Avaya Media Server (AMS in different network regions	Dual-tone multi-frequency (DTMF) did not recognize in the call	7.0.1.2.0
CM-16473	Use IGAR with SIP stations	No talk paths or delayed talk path experience with IGAR involved calls	6.3.16.0
CM-16499	When the station with Bridge Call appearance configured had CES enabled	Bridge appearance did not ring audibly if the station was CES (Client Enablement Server) mapping.	6.3.15.1
CM-17102	Transfer, Display	Agent call transfer, trunk group name displayed instead of calling party number	6.3.16.0
CM-17847	SIP Trunk, Call Transfer	An outgoing call over a SIP trunk might drop for some blind transfer call scenarios	7.1.0.0.0, 7.0.1.3.0, 6.3.17.0
CM-18918	1. Enable special application SA8900 2. Configure feature button "call-scrn" on station form sta-A 3. Duplicate station sta-A	On CM SAT terminal "duplicate station <sta_Num>" command failed with error _ "Error encountered, can't complete request; check errors before retrying"_ when SA8900 was enabled and station had "call-scrn" button administered.	7.0.1.3.0
CM-19317	DUAL stack (IPv4 and v6) SIP entity in the call	Communication Manager (CM) could experience a warm restart due to a segmentation fault when dual stack (IPV4	7.1.1.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
		and V6) SIP entity was involved in the call.	
CM-19318	VDN, Hunt Group, Unregistered SIP Station	Call to VDN with vector route-to no coverage a hunt group with an unregistered SIP station fails to continue vector processing.	7.1.1.0.0
CM-19559	Criteria for Logged Off/PSA/TTI Stations? N, No EC500, Coverage path configured, SIP Stations	Caller did not hear ring back on a call to station which has bridge appearance on another station.	7.1.2.0.0
CM-19576	Trunks with QSIG-MWI TSCs configured with 5-digit length. MWI - Number of Digits Per Voice Mail Subscriber: 11	Communication Manager Restart due to bad config - when maximum number of DCS voicemail number greater than configured MWI length	7.1.0.0.0
CM-19774	AAMS with over 900 announcements	The command "list directory source media-server" may fail to show any output.	7.0.1.2.0
CM-19792	Agents logged in on SIPCC stations that initiate Service Observing	Call to the station of a SIPCC Service Observer drops if the observer has an agent logged-in who is administered for auto-answer ACD or administered for auto-answer STATION and the station is administered for auto-answer ACD	7.0.1.3.0
CM-19810	DCS trunk call to Agent. Agent transfers the call to another Agent.	No ASAI events to cti-application via AES.	7.1.1.0.0, 7.0.0.0
CM-19853	SIP Call	CM did reset while parsing some SIP headers	7.1.1.0.0
CM-19869	Reboot on the Avaya S8300D Server running as a Local Survivable Server.	Local Survivable Processor does not register with the main server after a reboot.	7.1.1.0.0
CM-19886	Port Networks with AAMS and High traffic	Occasional Failed calls. Possible system restarts.	7.1.3.0.0, 7.0.1.3.0
CM-19887	Port Networks with AAMS	Missing announcement or Music-on-hold. Possible system restarts.	7.0.1.1.1
CM-19970	IP DECT station which is bridge to another station	IP DECT could not place outbound calls for a few minutes until audit triggered to resolve the stuck state of the station.	7.1.2.0.0
CM-20102	Upgrading from CM R6.x to CM R7.y or CM R7.0.x to CM R7.1.y will result in any Agent Skills administered in the range 61 to 120 being lost (i.e. Those administered on Page 3 of 'change agent-loginID' form).	Upgrading from CM R6.x to CM R7.y or CM R7.0.x to CM R7.1.y will result in any Agent Skills administered in the range 61 to 120 being lost (i.e. Those administered on Page 3 of 'change agent-loginID' form).	7.0.1.3.0
CM-20153	Audio group with multiple media-gateways and the 1st media gateway in the group is disabled.	If an announcement source that is part of an audio group is disabled and this is the 1st member of the audio group, then all calls to the announcement will fail.	7.0.1.2.0
CM-20238	The "list usage extension" SAT command does not show extensions used as station extensions	The "list usage extension" SAT command does not show extensions used as station extensions	7.0.1.3.0
CM-20248		CM did restart	7.1.1.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-20280	Loudspeaker paging	Paging loudspeaker may emit a popping sound when the station hangs up.	7.1.1.0.0
CM-20342	Intercom Call to a busy SIP Station (with no available call appearance)	Intercom Group feature did not work on SIP phones. Even after the call is dropped, intercom button remained stuck in a ringing state.	7.0.1.3.0
CM-20355	1) SIP station trying to activate enhanced call forward for toll restricted destination. 2) Toll restricted number configured in "change toll" form on CM. 3) "Calling Party Restriction:" set to "all-toll" in Class of Restriction (COR) form of calling party on CM.	SIP phones could activate Enhanced Call Forward to a toll restricted destination number.	6.2.0.0
CM-20418	TN-A calls STN-B. STN-B covers to STN-C. STN-D is part of pkup-group answers the call. Later from 3rd party cti-application tries to hold the call at STN-D. hold operation fails.	Not able hold the call from 3rd party cti-application if the call was picked up using pickup feature on a redirected call	7.0.1.3.0
CM-20431	SIP Station, VDN	CM sent BYE instead BUSY for a call to VDN that routes to a busy SIP station.	7.0.1.3.0
CM-20447	SIP Avaya Onex-Communicator logged in as other phone mode	When SIP Avaya OneX-Communicator was logged using other phone mode, the other phone was not receiving calling line identification as per public/private numbering configuration	7.1.1.0.0
CM-20473	Transfer call using SIP stations or trunks.	Intermittently, 3rd Party CTI Application detected an "off-hook" event from CM	7.0.1.3.0
CM-20474	CM with a PN or MG sourced announcement	When using the Announcement Feature Access Code, announcements may not be heard	8.0.0.0.0, 7.1.2.0.0
CM-20578	SIP trunk group assigned to SIP station has Measured set to something other than 'none'.	Digital phone calls a SIP phone that is bridged to another SIP phone, bridged appearance could not be picked up.	7.1.2.0.0
CM-20878	Enable Fast Connect at Orig from off-pbx configuration-set for station and configure SIP station with ACB.	Call appearance is stuck when Fast connect is enabled and station has ACB (auto callback) button (bad config).	7.0.1.3.0
CM-20882	Incoming H.323 trunk call with a CPN to a station that is forwarded to another station shows 'Unknown' instead of the CPN. CPN/ANI/ICLID Replacement for Unavailable Calls: Unknown on System Features page 9. Replace Unavailable Numbers? y on trunk group form page 3.	Forwarded call shows unknown instead of CLI of the original caller	7.1.2.0.0
CM-20906	SIP Trunk, Service Observe, Agent, Verint Call Recording	Transferred Call missed ASAI event to stop recording hence silence recorded until agent received a new call	6.3.117.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-21030	AACM, DMCC recorder, AAMS	DMCC recorder calls may fail	7.1.1.0.0
CM-21105	Call-Park feature, IP shuffling disabled	One-way talk path experienced in the SIP call park scenario	7.1.2.0.0, 7.1.1.0.0
CM-21136	Service Observe	Service observer did not drop when observed party transfers a call.	6.3.117.0
CM-21190	Register 2 SIP endpoint. Enable DM Add 3 party in the call (conference, bridge or any other feature.)	CM did system reset	7.0.1.2.0
CM-21216	Administer Survivable Processor form through SMGR using cut-through mode and make type simplex or duplex ESS	In SMGR cut through mode and GEDI mode of ASA, the "Server ID" field on the Survivable Processor form was not displayed properly.	7.0.1.0.0
CM-21294	More than 4 SIP stations in a Coverage Answer Group (CAG)	List trace station and tac commands failed to record all SIP station terminations in a cover answer group.	6.3.17.0
CM-21303	CTI	Predictive Make Call was not working. cti-application gets the Timeout error message	8.0.0.0.0
CM-21346	Make call using FTC (Facility Test Circuit) FAC and attempt to service observe the station.	Service observe of calls failed with denial event 1679.	7.0.1.3.0
CM-21413	Busy out a CTI link with more than 50 ASAI controlled agents logged in.	After busying out a CTI link, CM did warm reset and hung.	7.1.2.0.0
CM-21537	MOH on or shuffling off.	No talk path in an Avaya phone to Cisco call over SIP trunk after Cisco phone did hold unhold.	7.1.2.0.0
CM-21539	One-X Attendant, Call Transfer	One-X attendant could not able to transfer call to virtual station that covers to SIP station	6.3.17.0
CM-21565	SIP Domain	CM did an interchange multiple time	7.1.2.0.0
CM-21698	Group Page more than 8 members, VDN	Call to group-page with more than 8 members via VDN/vector failed.	6.3.16.0
CM-21711	SIP stations configured with pick-groups and enhanced call pickup alerting enabled on the change system parameters feature form.	Randomly, enhanced call-pickup alert notification was received by members not being a part of the called pickup-group.	7.1.2.0.0
CM-21749	Unregistered SIP Station, Criteria for Logged Off/PSA/TTI Stations? set to Yes	When SIP user is not registered and no coverage path for the station, caller kept hearing ring back.	7.1.2.0.0
CM-21797	Copy ASAI UUI During Conference/Transfer. change system feature Enter UUI while making call.	UUI is not carried by ASAI events generated because of transfer and conference when SIP endpoints are involved.	7.0.1.3.0
CM-21980	LDN, Attendant	For LDN call coming from an attendant, an TSAPI event received only when the call was connected, not while it was ringing	7.1.2.0.0
CM-22055	Fax over SIP trunk using G.711 pass-through mode	A call did not transition to XOIP (Fax over IP) type	7.0.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-22081		Occasionally, CM did reset	8.0.0.0.0

Fixes in Communication Manager Release 7.1.3

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
	Infrastructure	CM 7.1.3 includes the Red Hat updates to support mitigation of the Meltdown/Spectre vulnerabilities. However, this has the potential to affect performance – so there is now a small script that allows the setting of kernel options to control how these vulnerabilities are handled. The effect of running the kernel configuration script is both immediate and will persist across reboots. The script should be called from the CLI using the admin user and is called kernel_opts.sh. It has the argument "status" to display the current status of the kernel options, "enable" to enable all flags to provide maximum protection, and "disable" to disable all flags to provide maximum performance.	
CM-11120	SIP phone on a communication Manager	Occasionally, a call appearance on the SIP phone stayed stuck with bridging icon even when there were no active calls.	6.3.9.1
CM-13156	CM, Port Network (PN)	Occasionally it is possible to exhaust all timeslots in a port network. All calls involving that port network will fail.	6.2.7.0
CM-14213	CM, WebLM	Temporarily statuslicense shows license timeout error.	6.3.14.0
CM-15629	A SIP integrated voice messaging system; calling party not configured in private/public numbering	A caller received the wrong voice message greeting if a call was transferred to a SIP integrated voice messaging system when the calling party wasn't configured in private or public numbering on CM.	6.3.14.0
CM-16080	SIP trunk's far end network region location number is larger than 255	Call to a SIP trunk with location larger than 255 could fail and H.323 endpoint might experience unregistration	7.0.1.1.1
CM-16180	Voice Mail routing configuration through aar locations table	Direct call to Voice Mail did not work.	6.3.16.0
CM-16290	1) SIP station with call-fwd and third party cfwd-enh administered 2) Third party cfwd-enh set to self.	Call was forwarded incorrectly	7.0.1.1.0
CM-16468	Avaya Aura Communication Manager (AACM) with Application Enablement Services (AES) server being used to	Communication Manager went into reset because H.323 stations were being used with ASAI SIP Domain controlled station	7.0.1.2.0

ID	Minimum Conditions	Visible symptoms	Release found in
	monitor H.323 stations (being used as Dual-registration SIP stations) and 'Enable Reachability for Domain Control SIP Stations?' set to 'y' on CM	reachability feature (an unsupported configuration).	
CM-16470	Call from an Analog station to a non-disconnect supervision CO trunk (Disconnect Supervision - Out? n) transferred to a SIP station	A call appearance on the SIP phone was stuck in ringing state	6.3.16.0
CM-16540	Incoming Call Handling Treatment (ICHT) is configured	ICHT on ISDN-PRI trunks did not work when called from a cell phone associated with a OneX Mobile station	7.0.1.2.0, 6.3.16.0
CM-16649	Call to a B179 phone which sends x-nat parameter (unknown attribute) in SDP	No talkpath on a call from SBC to B179 phone which sent unknown session attribute in SDP	7.0.1.3.0
CM-16652	SIP Call	In some rare circumstances CM did reset	6.3.14.0
CM-16688	AAMS media resources	Possible missing or misdialed digits	7.0.1.2.0
CM-16917	CM, LAR configurations, no-hold-conference feature	Look Ahead Routing (LAR) did not trigger while no-hold-conference was in-progress	6.3.14.0
CM-16943	Call forward, SIP & QSIG trunk	The call forwarded terminating station did not display any forwarding information.	6.3.12.0
CM-17013	SIP Endpoint as Group Page member	Non-compliant SIP History-Info header caused parsing error	6.3.14.0
CM-17093	CM with AMS announcements on multiple AMS servers	AMS announcements won't play	7.0.1.2.0
CM-17225	Avaya H323 stations and an Avaya Media Server	Calls involving H323 stations anchored at the Avaya Media Server can randomly produce DTMF tones. This is dependent on the voice characteristics of the user at the H323 station	7.0.1.2.0
CM-17258	SIP phone with bridged call appearances	Occasionally the bridged call appearance could not make an outgoing call.	6.3.14.0
CM-17388	CTI agents transferring calls with 'Station Tone Forward Disconnect' configured to 'busy'.	Agents were getting busy tone and remaining on calls when transferring via a CTI application if 'Station Tone Forward Disconnect' was configured to 'busy'.	6.3.13.0
CM-17392	IP phone in shared control mode, call transfer	If user tried to transfer a call which has not been connected yet and unholds the first call, it fails.	7.0.1.0.0
CM-17421	CM, AES, EC500 mapping, 3PCC call from a logged off station	Call dropped	6.3.12.0
CM-17424	Call routed to an agent Direct agent (DAC) Skill via a vector step where the DAC was not measured.	When the Direct Agent Skill was not measured, routing to an agent-loginID from a vector resulted in an incorrectly formatted message to CMS.	7.0.1.2.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-17505	Same mobile number mapped for OneX and telecommuting number.	Two calls ring on the same station	6.3.16.0
CM-17512	H.323 station with TTS an TLS in a duplicated processor Ethernet configuration	After a server interchange a H.323 station could be in a stuck state, requiring a reboot to recover.	7.0.1.3.0
CM-17613	CTI agent application; the CTI applications sends two answer messages within 200 milliseconds or less.	If CM received two answer messages from CTI application less than 200 milliseconds apart, a response was not sent for the second answer message causing timeout errors on the CTI applications.	6.3.15.1
CM-17614	H323 telecommuter	A call cannot be answered on a telecommuter phone if the answer came 60 seconds after ringing started.	7.0.1.3.0, 6.3.16.0
CM-17619	Call Center CM 7, using Add/Remove Agent Skills via FAC	Changing agent skills using the Add and Remove Skill FACs had occasional delay in sending updates to CMS. Thus, CMS was showing the agent in the OTHER state for minutes after the state change.	7.0.1.3.0, 6.3.4.0
CM-17731	NATed H323 user	The H323 station behind the Network Translated Device (NAT) couldn't get dial tone if the user tried to go off-hook the first time after registration.	6.3.8.0
CM-17743	Calabrio voice recording solution in an AMS configuration	During call recording with a Calabrio voice recorder the recorder may be dropped after 5 minutes.	7.1.0.0.0
CM-17756	Corrupted data in CM 7 with ACD call delivery to agents and CMS connected	Improved software reliability to avoid possible data corruptions	7.0.1.2.0
CM-17773	CM, AES, CTI Application	cti-application received the wrong npi_toa (Number Plan Identifier - Type of Address) on incoming trunk call to Agent/station.	6.3.15.1
CM-17775	CM, AES, incoming r2mfc trunk,	CTI application failed to process alert event.	7.0.1.3.0
CM-17827	SIP tandem calls	The system may restart due to a memory leak	7.0.1.2.0
CM-17828	Service Observing warning tone configured on an IP station that has a bridged appearance of another IP station.	When an IP phone/station made an outgoing call, Service Observing (SO) warning tone was heard in the conversation when another IP phone/station had SO warning tone enabled and had a bridged appearance of the calling station.	6.3.12.0
CM-17867	Call Center with measured SIP trunks using ASAI/CTI	For some types of outgoing SIP trunk failures, an extraneous, delayed trunk IDLE message was sent to CMS causing CMS to stop tracking the next call on that	6.3.16.0

ID	Minimum Conditions	Visible symptoms	Release found in
		same measured trunk	
CM-18000	Signaling groups configured.	In one instance a system reset occurred when signaling groups were used.	6.3.16.0
CM-18001	A system logging a new error	In one instance a system reset occurred due to a corrupted linked list when a new system error was logged.	6.3.15.0
CM-18009	more than 255 network regions	An H.323 phone registers to CM in a stub Network Region and gets an incorrect Alternate Gatekeeper List.	6.3.14.0
CM-18010	CTI application, Virtual Directory Number (VDN)	CTI applications did not to get events from Communication Manager	7.0.1.3.0
CM-18011	Communication Manager with G650 Media Gateway	In rare instance a reset system 1 occurred on a system with a G650 Media Gateway.	6.3.10.0
CM-18110	LSP, BSM	The BSM's asset IP gets deleted from LSP's server role SMI page each time the server is rebooted.	7.1.1.0.0
CM-18195	Stations with more than 2 button modules	Stations with more than 48 custom button labels will lose the labels that exceed 48 buttons. Generally, this happens only on stations with more than 2 button modules.	7.0.1.2.0
CM-18196	CDR records in use; a leading "+" in the CPN for an incoming call over ISDN	Null characters appeared in Call Detail Recording (CDR) records when a Calling Party Number contained a leading "+" in the incoming ISDN SETUP message.	6.3.15.0
CM-18198	Direct Media turned ON, encryption administered on CM	No talk path observed	7.0.1.2.0
CM-18206	CM 6.3 or later, vectoring with queue-to skill step and VDN return destination	A 'queue-to skill' vector command in the VDN Return Vector step will result in the call being queued at Low Priority regardless of the priority (top, high, medium, low) specified in the command	6.3.11.1
CM-18232	Running call traffic on CM when CM software internally encounters a UID of zero	CM ECS logs filled with process errors (proc_err) 7171 with sequence number of 6054 and 6055 when CM internally encountered a UID of zero. The only impact was ECS logs rolling over more quickly than usual.	7.0.1.0.0
CM-18244	Monitored station is cleared when it takes over another station and TTI is enabled	CTI events/messages were not provided to CTI applications when a monitored station took over a station that was registered to another extension when Terminal Translation Initialization (TTI) was enabled.	7.0.1.3.0
CM-18331	Phones/stations going off hook	An enhancement to add a debug setting that prints all station off hook activity in the CM ECS logs.	7.0.1.2.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-18361	Change the ARS ANALYSIS form or AAR ANALYSIS form and submit.	Customer would see "Error encountered, can't complete request" error message when changing the ARS ANALYSIS form or AAR ANALYSIS form	7.1.1.0.0
CM-18421	An analog music source on a PN or an MG, Stations listening to the analog music must be anchored on an AMS	Music on hold may remain on the call after unholding the call.	7.0.1.3.0
CM-18427	SEMT turned ON, adhoc conference which moves to AAC	AAC adhoc conference does not work for local stations	7.1.1.0.0
CM-18428	SIP stations/agents configured as non-ACD group or skill members	No ‘list trace hunt-group’ System Access Terminal (SAT) command output was provided for calls terminating to a SIP station that was a member of a non-ACD (Automatic Call Distribution) group or skill.	7.1.0.0.0
CM-18433	H.323 Station	Communication Manager could experience a warm restart when an H323 station registers	6.3.16.0
CM-18477	Vectors and vector variables configured, orphaned data records	In one instance a system reset occurred when vectors and variables were configured in a system due to an audit that encountered orphaned data records.	6.3.11.0
CM-18554	The "ISDN" trunk form with the "NCA-TSC Trunk Member" field is set to an out of range value of zero instead of blank or a numeric value between 1-255	Customer could not submit an "ISDN" trunk form because the "NCA-TSC Trunk Member" field is set to an out of range value of zero instead of blank or a numeric value between 1-255.	7.0.1.3.0
CM-18682	CTI application inter CM call, r2mfc trunk	CTI application failed to handle alert event	7.0.1.3.0
CM-18747	Call Transfer	Intermittent one-way audio in transfer when held party is ACME SBC.	7.1.1.0.0
CM-18795	Unregistered SIP Station	Hunt group call couldn't term to the next available agent if one SIP agent was not registered and the field "Criteria for Logged Off/PSA/TTI Stations" was set to "y" on "system-parameters coverage-forwarding" form	7.1.1.0.0
CM-18797	CTI application, Virtual Directory Number (VDN), SIP trunk, Call transfer	CTI applications did not to get events from Communication Manager	7.1.3.0.0, 7.0.1.3.0
CM-18812	SA9095 enabled on the "system-parameters special-applications" System Access Terminal (SAT) form; SIP phone/station members unregistered	Special Application SA9095 "Hunt Group Modifications" did not work with SIP phone/station members when they were unregistered.	7.0.1.2.0
CM-18824	Using the "list trace station" SAT command on a phone/station with an internal UID of two.	The "list trace station" System Access Terminal (SAT) command run on a phone/station with an internal UID of two would only provide output of denial event	7.1.1.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
		2287.	
CM-18825	RONA, Xport station, SIP trunk	RONA (Redirect On No Answer) call that covered through an X-ported station to a remote coverage path couldn't cover to the right voice mail box.	6.3.17.0, 6.3.16.0
CM-18839	3rd Party call control tool, use cstaMakePredictiveCall, ISDN-PRI trunk, Trunk Hunt is set as cyclical, End OCM After Answer (msec): xx on location-parameters form	Customer Call was not answered by predictive call.	7.0.1.2.0
CM-18896	SIP call-center agent with a vu-display button above 9	The system may reset if the site has a SIP call-center agent with a vu-display button above button number 9 or a format number above 9	7.1.1.0.0, 7.1.0.0.0
CM-18940	Using the "list trace hunt-group" SAT command; logged off SIP stations	The "list trace hunt-group" System Access Terminal (SAT) command output didn't provide failed call terminations for logged off SIP stations.	7.1.1.0.0
CM-18941	"IP Network Map" form "Emergency Location" field extension	"IP Network Map" form "Emergency Location" field extension	6.3.12.0
CM-18942	The system must be configured for and LSP and the optional LSP Media Gateway Serial Number field on the Server Role SMI Page needs to be administered	The contents of in the Optional LSP Media Gateway Serial Number field on the Server Role SMI Page can now be deleted once it has been added.	7.1.0.0.0
CM-18949	Execute enable or disable nr-registration with non-numeric values. For instance, "disable nr-registration 3-120"	Customer can enter non-numeric values at SAT when executing a "disable nr-registration" or "enable nr-registration" command and the command displays that it has successfully completed. However, it has only operated on the first digits entered.	6.3.15.1
CM-18950	Incoming Trunk Call	On SOSM configuration the event incoming trunk call was having call ID 0x0.	7.1.1.0.0
CM-18955	X-ported DCP station	Calls made to x-ported logged off DCP stations resulted in a busy tone instead of ring back.	6.3.15.0
CM-18997	H323 Station, In-band H23 trunk, Port Network	End to end signaling produced a continuous tone	7.1.1.0.0
CM-19285	Incoming SIP trunk with wrong UUI with UUI Treatment is set to "service-provider" and tandem over to ISDN/H.323 trunk with UUI Treatment is set to "shared".	CM did reset	6.3.16.0
CM-19309	RONA for SIP Agent	CM did reset	7.0.1.3.0
CM-19532	Music source on a PN or MG, The Listener is on an AMS, Inter-region connectivity uses IGAR with	No MG/PN sourced Music source when listener in served by an AMS and the regions are inter-connected by	7.0.1.3.0

ID	Minimum Conditions	Visible symptoms	Release found in
	IP trunks	IGAR using IP trunks.	
CM-19566	SIP agent	When an incoming call to the VDN queued to two skills, if the SIP agent in the 2nd skill answered the call, and if this SIP agent tried to put the call on hold first and then pushed the conference button to do the conference, the conference could fail	7.0.1.2.0
CM-19626	Multi-tenant configuration with music on hold configured	When user in a tenant held the call, wrong music source was played	6.3.16.0
CM-19774	AMS with lots of announcements	The command "list directory source media-server" may fail to show any output.	7.0.1.2.0

Fixes in Communication Manager Release 7.1.2

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
CM-2359	All configurations	The System Management Interface (SMI) was vulnerable to the Slowloris denial of service attacks.	6.0.0.0
CM-11028	Send all Calls (SAC), Call-forwarding activated	The call went into a loop between two stations.	6.3.8.0
CM-15135	TSAPI monitored shared control station, Server Interchange	One way talk path was observed when server interchange happened while TSAPI monitored shared control station was in active talk path.	7.0.1.2.0
CM-15289	SIP station, Call-pickup group, "Enhanced Call Pickup Alerting" field set to "y", "Caller ANI during pickup alert?" set to "n"	The call-pickup group members displayed calling party number and name.	7.0.1.2.0
CM-15501	Call Center using Timed After Call Work and the option "After call transfer or Held Call Drops" set to 'n'.	The option for Timed ACW after transferred call dropped worked differently depending on which direction the ACD call was transferred, and whether the agent was on a SIP station or a non-SIP station.	6.3.16.0
CM-15898	SIP Calls	CM did restart when CM received BYE message formatted badly as "U" string in request URI.	7.0.1.1.1
CM-15978	Administered with Agent/Caller Disconnect Tones and Music on Transferred trunk calls.	A hung call could occur on a system with music on transferred trunk calls, when an incoming SIP ACD call answered by an agent is transferred to a SIP station that does not answer and has no coverage path.	6.3.14.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-16039	One-X Agent	Occasionally, H323 one-x Agent could not register to Communication Manager (CM) when operated in Time-To-Service Mode.	7.0.1.2.0
CM-16123	CM with AMS	Administration of the location-parameters tone loss plan has no effect on AMS generated tones.	7.0.1.2.0
CM-16126	H323 softphone with SIP service link. Auto-hold AMS multiple CMs	Occasionally a call would drop when taken off hold.	7.0.1.2.0
CM-16188	CMs connected with SIP Trunk, Service Observing, and Initial IP-IP Direct Media? set to 'Y', outgoing direct media enabled	SIP call dropped.	6.3.13.0
CM-16239	Coverage Answer Group, Call Transfer, CM restart	No call recording happened after 2 days of CM restart.	7.0.1.3.0
CM-16251	H.323 trunk group and CM configured to transmit a large number of DTMF digits when the far end answers.	A system reset could occur when CM attempted to transmit more than 32 digits via end-to-end DTMF signaling over an H.323 trunk group.	6.3.116.0
CM-16275	SIP station had "rpxxx" configured on "SIP Trunk" field on stations form, and call forwarding was enabled on the SIP phone.	No call log was recorded on SIP phone when call forwarded.	7.0.1.2.0
CM-16278	SIP Trunk, IVR, SA9124 - AACC Connected Information Enhancement.	Connected number in ASAI transfer message incorrect.	6.3.16.0
CM-16327	SIP call	Occasionally an incoming SIP call drops after being transferred by an agent.	7.0.1.2.0
CM-16367	IP trunks	Occasionally a telecommuter agent call is dropped.	7.0.1.2.0
CM-16390	SIP & H.323 Trunk Groups, set the field "Supplementary Service Protocol" as "b".	Cannot delete the SIP trunk group.	6.3.15.1
CM-16441	IP Station, Off-net coverage	Soft buttons except bridge button on IP (H.323) station disappeared when a call traversing through off-net was answered.	7.0.1.2.0
CM-16501	H.323 stations with vu-display configuration	Topline display on H.323 phone gets cleared when endpoint goes off-hook and on-hook.	7.0.1.2.0, 6.3.16.0
CM-16507	Call Center with CMS, IQ, or Oceanalytics connected. Call Center agents defined with a mix of measured and unmeasured skills where their first logged-in skill is unmeasured.	If an agent's first skill is unmeasured, when ASAI logs the agent in, the AUX message indicating the agent's work mode did not get sent to CMS so the CMS reporting of the time the agent spent in AUX is not totally accurate.	6.3.16.0
CM-16517	SIP, ASAI	Occasionally an ASAI event received the	6.3.16.0

ID	Minimum Conditions	Visible symptoms	Release found in
		incorrect cause value resulting in a dropped call.	
CM-16560	TSAPI, AES, CTI, call transfer.	Call transfer on 3rd party cti-application failed.	7.0.1.3.0
CM-16571	Call forward, ISDN PRI trunk	Random digits displayed on the station when incoming SETUP received without calling party number.	6.3.116.0
CM-16577	Server with stations and agents administered.	System restarts seen in the logs and processor interchanges due to segmentation faults.	6.3.14.0
CM-16647	CM >= 7.1, large number of entries on ars analysis form.	EECCR error was seen on "change ars analysis location xx" form.	7.1.1.0.0
CM-16660	VDN, Dialer, outbound trunk call	Erroneous call pop-up at agent screen was seen.	6.3.15.1
CM-16690	File containing CM6.X backups restored to CM7.1 load.	After restoring of data from CM 6.3 load on CM 7.1, command history file stopped getting updates breaking SMGR.	7.1.0.0.0, 7.0.1.3.0
CM-16712	AES connected to CM	While a call was alerting at a monitored H.323 or DCP agent's station, the call type reported to AES application was always "unknown".	7.1.1.0.0
CM-16724	Call Center using Multiple Call Handling	When an agent was on a call and had ACW pending they could not receive a Multiple Call Handling (MCH) call.	6.3.16.0
CM-16744	Auto-hold disabled, "Station Tone Forward Disconnect" is set as either "intercept" or "busy", two separate calls to dual registration phone.	The call appearance was seen stuck on SIP phone.	7.0.1.3.0
CM-16774	CM configured with only IPv4	Occasionally, the CM System Management Interface (SMI) becomes unusable.	8.0.0.0.0, 7.1.0.0.0
CM-16783	Call Center where agents can conference to VDN/Vector	One-X agent completing a conference to a VDN/vector is incorrectly put in ACW.	6.3.16.0
CM-16861	Customer must have more than 999 announcements administered.	Customer is blocked from adding 1000th announcement or more when doing "add announcement".	6.3.17.0
CM-16915	A system reset could occur when CM attempted to transmit more than 32 digits via end-to-end DTMF signaling over an H.323 trunk group.	In a configuration with coverage answer groups having 60 or more members being team monitored by 10 users and ASAI monitored, CM would possibly interchange and/or reset.	6.3.16.0
CM-16955	SIP bridge	The principal station locked up after its first call appearance joined a bridge call and the bridge phone conferenced the first line to the second line.	6.3.16.0
CM-17068	Communication Manager with at least 15 agents being logged out at the same time.	Doing a Forced Agent Logout by Clock	6.3.15.1

ID	Minimum Conditions	Visible symptoms	Release found in
	These agents must have average > 40 skills each.	Time causes system reset.	
CM-17073	Call Center with a SIP-connected adjunct using REFER without Replaces to route calls out of the CM.	CMS Reporting ignored calls that went through a REFER without Replaces and were answered off-site prior to completing the transfer processing.	6.3.16.0
CM-17342	H323 Agents, AMS, Network Transfer	Occasionally, not all digits get signaled to the PSTN hence network transfer calls failed.	7.1.0.0.0
CM-17733	Hunt Group Busy Position button on SIP	On rare occasions, Communication Manager could experience a system warm restart if Hunt Group Busy Position button was used on a SIP client.	7.0.1.2.0
CM-17778	Installation of Kernel Service Pack on an S8300D server.	Occasionally, installation of a Kernel Service Pack failed on an S8300D server due to a timeout.	7.1.0.0.0
CM-17812	ESS/LSP with no C-LAN board.	An installation or upgrade on an LSP or ESS might fail.	6.3.17.0
CM-17847	SIP Trunk, Call Transfer	An outgoing call over a SIP trunk might drop for some blind transfer call scenarios.	7.1.0.0.0, 7.0.1.3.0, 6.3.17.0
CM-18186	GW sourced announcement with additional GWs or AMSs.	Occasionally an announcement or Music-on-hold stopped in mid-play.	7.1.1.0.0

Fixes in Communication Manager Release 7.1.1

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
CM-3296	This issue occurred when SIP station had Send All Calls activated and "Maintain SBA at principal" was set to "y" on "change system-parameters coverage-forwarding" form.	For a SIP station with Send all Calls activated, Simulated Bridge Appearance for covered calls was not maintained on endpoint.	6.3.9.0
CM-9621	Hunt Group, Terminating Extension Group (TEG), Coverage Answer Group (CAG), H.323 IP Endpoints, Bridge Appearance.	When principle station (as a member of Hunt Group/TEG/CAG) was on active call and at the same time its bridged station attempted to originate a new call, then on principle station soft buttons such as conference, transfer, hold disappeared and only bridge button appears on the screen.	7.0.0.3.0
CM-14531	This problem occurred only when the dialed number contained + immediately following a #. The H.323 trunk had "overlap/overlap" configured on the "Digit handling (in/out) field on the "change trunk group form" on SAT.	If the number dialed had # followed by + over an H.323 trunk, the system underwent a restart.	6.3.113.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-14705	Communication Manager (CM) with agents having 'Timed after call work' (TACW) configured.	For a call that landed on an agent, via a vector with the converse-on step, who had TACW configured, when the caller disconnected the call before the agent could, Communication Manager failed to change the agent's mode to TACW.	7.0.1.2.0
CM-14771	Communication Manager (CM) configured with Call vectoring and H.248 media gateways, Application Enablement Services (AES) server, Computer Telephony Integration (CTI) applications.	CM dropped calls while executing the 'adjunct route' vector step.	6.3.15.1
CM-14870	This issue occurred when - 1. Outgoing call was made from an Avaya one-X Communicator SIP/H.323 soft phone/H.323 desk phone to an extension with "911" in the string of dialed numbers. 2. On System Access Terminal (SAT), “Location-Based Call Type Analysis?" was set to "y” on "change dial plan parameters" form. Use of enbloc dialing (logdial feature not used).	Call is routed out to an incorrect extension (911 EMERGENCY in this case), if dialed number contains a routable extension (911 in this case) after the short extension, when “Location-Based Call Type Analysis?" is set to "y" on "change dial plan parameters" form.	6.3.15.1, 6.3.15.0
CM-15093	Communication Manager (CM) with trunks, attendant, virtual stations with SIP Modular Messaging (MM) in their coverage path.	When the attendant transferred an incoming trunk call to a virtual station whose coverage was set to 'All', the caller over the trunk received a generic greeting from the SIP MM.	6.3.16.0
CM-15188	Communication Manager (CM) with SIP trunks and Application Enablement Services (AES) server integration.	CM incorrectly sent a user not responding message to AES applications for SIP trunk calls which failed to reach the user because of network problems.	6.3.14.0
CM-15189	Communication Manager (6.3.0.0 or above).	The customer was able to enter and submit a value out of the permissible range (1-2000) for the "change route-pattern" form on the System Access Terminal (SAT).	6.3.15.0, 6.3.0.0
CM-15242	Multiple locations short dialing A local station having short dial code same as initial dialing digits of EC500 destination.	EC500 call was getting termed to a local station when the call met with a glare on first attempt.	6.3.15.1
CM-15319	SIP Calls	TCM variable NumSipRingingCalls on Avaya Communication Manager was showing count as number of transactions instead of number of SIP calls in ringing state.	6.3.15.1
CM-15388	An H.323 IP AnnexLP station shuffled (Direct IP-IP) call.	On shuffled (Direct IP-IP) calls involving an H.323 IP AnnexLP station, the DTMF tone for the first digit dialed from the station after the call was established was longer than the DTMF tone provided for subsequent dialed	6.3.14.0

ID	Minimum Conditions	Visible symptoms	Release found in
		digits.	
CM-15434	Incoming 200 OK response with Authentication-Info header	Call dropped as ACM (Avaya Communication Manager) wrongly modified Authentication-Info header of incoming 200 OK response by inserting a semicolon before sending it out to Avaya Session Manager (ASM).	7.0.1.2.0
CM-15435	Communication Manager (CM 6.3.0.0 or above) configured with a Media Gateway Communication Server 1000(CS1K)	The call was dropped during a very specific capability negotiation SIP signaling between CS1K and Gateway via CM. This happened when an ongoing call was redirected to a gateway for joining a conference.	6.3.15.1
CM-15469	A station on CM calling MSUM (Microsoft UM voicemail). The station does not have a mailbox in MSUM	Call dropped by MSUM (Microsoft UM voicemail) with a 403 "Forbidden" due to invalid History-Info header in INVITE coming from Avaya Communication Manager (ACM).	6.3.14.0
CM-15486	Communication Manager (CM) and Application Enablement Services (AES) server.	AES applications reported incorrect called party number for transferred calls.	7.0.0.3.1
CM-15490	One-X Agent in Telecommuter mode.	Occasionally, a One-X Agent in telecommuter mode was unable to answer the incoming call.	7.0.1.2.0
CM-15521	Communication Manager (CM) with CLAN boards.	During a network outage between CM and CLAN boards, the 'status socket-usage' command on CM administration terminal 'sat' displayed incorrect values.	6.3.6.0
CM-15542	Communication Manager (CM) provisioned with SIP trunks and Application Enablement Services (AES) server.	AES applications monitoring calls to SIP trunks did not get a call answer notification.	7.0.1.2.0
CM-15559	Communication Manager (CM) provisioned with PSTN SIP trunks, SIP agents and Application Enablement Services (AES) server.	When applications on AES server made outbound calls over SIP trunks, the calls could not be transferred to SIP agents at a later stage.	7.0.1.2.0
CM-15581	SIP	ACM (Avaya Communication Manager) experienced a restart owing to a memory leak situation.	6.3.13.0
CM-15618	1. Enable SA8886 (ISDN Incoming Calling Party Number Conversion?) on the "change system-parameters special-applications" form on System Access Terminal (SAT). 2. "change calling-party-num-conv" form administered. 3. Incoming call on a Basic Rate Interface (BRI) trunk.	When SA8886 was enabled on CM, incoming trunk calls were denied by Communication Manager intermittently.	7.0.1.2.0
CM-15619	Call Management System (CMS) connected to Communication Manager (CM) configured with	CMS stopped tracking a call if a 'reverse transfer' was completed after a service	6.3.14.0

ID	Minimum Conditions	Visible symptoms	Release found in
	Automatic Call Distribution (ACD) and service observers.	observer joined the active ACD call.	
CM-15674	SIP stations that have bridged appearances of other stations.	A warm interchange occurred on one occasion in a duplicated server pair where SIP stations with bridged appearances were being used.	6.3.14.0
CM-15676	This occurred only when a new SIP station was added using System Manager (SMGR)/Avaya Site Administration (ASA).	The "Phone Number" field on the "off-pbx-telephone station-mapping" form would revert to its original value if changed using SMGR or ASA when the newly entered extension matched a previously administered extension for another station.	6.3.15.1
CM-15682	9404, 9408, 1408 and 1416 set types.	The SAT "Terminal Parameters" form, page 2 included DCP set types that do not support download of terminal parameters. Those were 9404, 9408, 1408 and 1416 set types.	6.2.4.0
CM-15686	Call Management System (CMS) connected to Communication Manager (CM) with R2MFC trunks.	CMS server was unable to track some calls over R2MFC trunks causing the CMS-CM link to go down.	7.0.1.2.0, 6.3.1.0
CM-15690	Communication Manager (CM) with endpoints using Call Park feature, Application Enablement Services (AES) server and Computer Telephony Integration (CTI) applications.	When a parked call between parties A and B was picked up by C, the call connected event to the CTI application had C as the calling party B as the called party.	7.0.1.2.0
CM-15720	This issue occurred when the SIP endpoint was administered with a third-party call-forward button for a hunt-group.	The status of call-forward button lamp was incorrect every time the SIP station registered. This happened only when the button was a third-party call-forward for a hunt group.	7.0.1.2.0
CM-15735	1. Communication Manager (CM 7.0.0.0.0 above) system with Avaya Media Server (AMS) connected to a CM (6.3.0.0.0 or above) system over a H.323 trunk. 2. Codec used on both CMs is G.726 administered on "change ip-codec-set" form.	The call made over the H.323 trunk was dropped.	7.1.0.0.0
CM-15745	Two Communication Manager (CM) servers connected using R2MFC trunk, Application Enablement Services (AES) server and Computer Telephony Integration (CTI) applications.	When a call was placed from one of the CMs to second on the R2MFC trunk, the CTI application connected to the second CM did not get the called party number information.	7.0.1.2.0
CM-15746	Team Button feature, QSIG Trunk, "Criteria for Logged Off/PSA/TTI Stations?" is enabled on "system-parameters coverage-forwarding"	Team-button did not ring for an incoming call on QSIG trunk forwarded to the monitored station which was unregistered at that time.	6.3.3.0
CM-15747	LAR (Look Ahead Routing) First trunk on route-pattern responds	Caller heard intercept tone instead of busy	7.0.1.1.0

ID	Minimum Conditions	Visible symptoms	Release found in
	with 404 User Not Found Second trunk responds with User busy.	tone.	
CM-15749	SIP call ACM (Avaya Communication Manager) receives 500 Server Internal Error: Destination Unreachable for session refresh UPDATE message.	The SIP call got dropped after 500 Server Internal Error: Destination Unreachable response was received by ACM (Avaya Communication Manager) for its session refresh UPDATE message.	7.0.1.2.0
CM-15788	Alternate Network Address Types (ANAT) enabled on "system-parameter ip-options" and "ip-network-region" form.	The call got dropped on answer after an un-attended transfer to SIP trunk when ANAT was enabled.	7.1.0.0.0
CM-15835	Call Management System (CMS), IQ, WAE or Oceanalytics collector connected to Communication Manager (CM).	The 'busyout mis' command on CM administration screen 'sat' did not work when trying to busy a specific processor channel.	7.1.0.0.0
CM-15960	Field 'Prefer use of G.711 by IP Endpoints Listening to Music' and 'Prefer use of G.711 by IP Endpoints Listening to Announcements' set to 'y' on system-parameters ip-options form on ACM (Avaya Communication Manager) Multiple network regions Multiple Gateways Conference.	Intermittently, no talk path at one of the IP endpoints in the conference across SIP trunks.	6.3.16.0, 6.3.12.0
CM-15963	Communication Manager (CM) ESS server running in Duplex mode.	The standby server from the duplex ESS server pair went into a reboot once a day when configuration files were pushed from the main server to the ESS servers.	6.3.16.0, 6.3.15.0, 6.3.14.0
CM-16014	Communication Manager (CM) with endpoints using Whisper page feature, Application Enablement Services (AES) server and Computer Telephony Integration (CTI) applications.	While in the middle of a call, if one of the parties received a whisper page call from an endpoint controlled by a CTI application and the call was dropped by the called party, the CTI application did not drop the call.	7.0.1.2.0
CM-16015	This issue occurred when Latin-script based Unicode language was configured on SIP phones as well as Communication Manager.	Conference display on SIP phones was not consistent when any one of the Latin-script based Unicode language was used.	7.0.1.2.0, 6.3.4.0
CM-16028	This issue occurred when the SIP endpoint was administered with a third-party call-forward button for a hunt-group with number 415 or greater.	SIP station could not activate the call-forward for the hunt group if the hunt group number was 415 or greater.	7.0.1.2.0
CM-16029	Alternate Network Address Types (ANAT) enabled on "system-parameter ip-options" and "ip-network-region" form ANAT disabled on ASBC (Avaya	Hold-Unhold on a call between ANAT SIP user on ACM (Avaya Communication Manager) and remote worker across ASBC (Avaya Session Border Controller) resulted in no talk path.	7.1.0.0.0

ID	Minimum Conditions	Visible symptoms	Release found in
	Session Border Controller).		
CM-16034	This occurred when - 1. SIP stations logged in with Equinox and EC500 enabled. 2. Connection to Equinox lost due to network issues, and call terminated on EC500 device.	Users could see their own extension number for calls received on EC500 devices. This happened when user logged in with Equinox on their mobile devices and had EC500 enabled.	6.3.15.1
CM-16047	Call Management System (CMS), Communication Manager (CM) with agents having a conference button on their stations.	If an agent used the conference button to initiate a conference, entered insufficient digits, used the button again to complete the conference and then entered the remaining digits, the CMS was unable to track the call.	6.3.115.0
CM-16050	Executing "almclear " command	Segmentation fault when trying to clear a list of server alarms and comma separated list as follows. almclear -n 6, 5	6.3.11.1
CM-16051	Two ACMs (Avaya Communication Manager) Alternate Network Address Types (ANAT) enabled on both ACMs Field 'Initial IP-IP Direct Media' set to 'y' on signaling group form on both ACMs Conference across ACMs.	Hold on a conference call across two ACMs (Avaya Communication Manager) resulted in call drop.	7.1.0.0.0
CM-16052	Equinox Client LAR (Look Ahead Routing) configured on route-pattern on ACM (Avaya Communication Manager) Field 'Initial IP-IP Direct Media' set to 'y' on signaling group form.	Call from an Equinox client got dropped when call was routed to a route-pattern where first couple of trunks responded with 403 Forbidden and last trunk responded with "480 SIPS Not Allowed" response.	6.3.15.1
CM-16059	This issue occurred when multiple Avaya Media Servers (AMS) were connected via Inter-Gateway Connectivity (IGC) and music on source is hosted on AMS for multiple listeners.	Not all users present on the call were able to hear an announcement on AMS for a call over SIP trunk.	7.0.1.2.0
CM-16064	Communication Manager (CM) with agents and Vector Directory Numbers (VDNs), Application Enablement Services (AES) server, Computer Telephony Integration (CTI) applications, and CallVisor (CVLAN) applications.	If an agent placed a call to a monitored VDN which was transferred to another VDN by 'adjunct route' vector step, CVLAN CTI applications received error messages from the CM via AES because of which they closed their connection to the AES and other CTI applications did not receive a correct call redirection message.	7.0.1.2.0
CM-16079	1. SIP stations utilizing team button. 2. Complex routing patterns on the monitoring and monitored stations.	Team button did not provide a status change indication on some SIP phones when there were complex routing patterns for the monitoring and monitored stations.	7.0.1.2.0

ID	Minimum Conditions	Visible symptoms	Release found in
CM-16125	The "Calling Party Number Conversion for Tandem calls" table accessed by "change tandem-calling-party-number" with a mixture of "any" and numeric length fields, on System Access Terminal (SAT).	Customer could not remove or change some entries on the SAT "change tandem-calling-party-num” form if there was a "Length" of any before them and their length was numeric.	7.0.1.2.0
CM-16154	Communication Manager (CM), Application Enablement Services (AES) server, Computer Telephony Integration (CTI) applications, and SIP agents.	CTI applications stopped receiving messages from CM.	7.0.1.2.0
CM-16181	Communication Manager (CM) using NTP for time synchronization.	When CM used NTP for time synchronization, the time on the server was different from the actual time and on a CM duplex server configuration it resulted in loss of memory shadowing.	8.0.0.0.0, 7.1.0.0.0
CM-16265	Alternate Network Address Types (ANAT) enabled on "system-parameter ip-options" and "ip-network-region" form Field 'Direct IP-IP Audio Connections' set to 'n' on "signaling-group" form.	Hold on a call between an IPv6 SIP user on ACM (Avaya Communication Manager) and remote worker across ASBC (Avaya Session Border Controller) resulted in no talk-path.	7.1.1.0.0
CM-16277	1. Configure SIP stations using the "rpxxx" option rather than "aar". 2. Configure the trunk groups in the route pattern pointed to by "rpxxx" to point to two or more Session Managers (e.g., primary and secondary).	When a station is configured using the "rpxxx" option introduced in CM7.0, CM traverses that route pattern in the inverse order when deciding where to send feature button update signaling. This can cause SIP station feature buttons not to go on or off correctly in some configurations.	7.0.1.2.0
CM-16332	Avaya one-X Agent with telecommuter mode enabled Auto-answer enabled on "change station" form on System Access Terminal (SAT).	When an incoming call for Avaya One-X Agent was answered by telecommuter, the call could not be answered on the Avaya One-X Agent Client.	7.0.1.3.0
CM-16440	Alternate Network Address Types (ANAT) enabled on "system-parameter ip-options" and "ip-network-region" form Field 'Initial IP-IP Direct Media' set to 'y' on "signaling-group" form.	An ANAT enabled end-point could not make call to an IPv4 end-point.	7.1.1.0.0
CM-16458	Avaya Media Server (AMS) H.323 trunk	Call forward over an H.323 trunk, to a remote station failed.	7.1.0.0.0
CM-16502	Multiple network regions Field 'Initial IP-IP Direct Media' set to 'y' on signaling group form on ACM (Avaya Communication Manager).	A SIP user on ACM (Avaya Communication Manager) was not able to call another SIP user on ACM when bandwidth available could still sustain one call.	7.1.0.0.0
CM-16516	Communication Manager (CM) with SIP trunks, Application Enablement	CM incorrectly sent a user not responding message to CTI applications for SIP trunk calls	6.3.16.0

ID	Minimum Conditions	Visible symptoms	Release found in
	Services (AES) server, Computer Telephony Integration (CTI) applications.	which failed to reach the user because of network problems.	
CM-16645	Communication Manager (CM) Application Enablement Services (AES) server Adjunct/Switch Application Interface (ASAI) Avaya Contact Recorder (ACR) Avaya Aura Agent Desktop (AAD)	Occasionally various symptoms were observed as follows: • ACR stopped recording calls • AAAD did not receive calls • Agent pop-up screen did not show incoming number correctly • User Application did not get call control buttons properly	7.1.0.0.0

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.x require the deployment of the 7.1 OVA. Once deployed, 7.1.x can 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.x are from:

   - SM 7.0 and subsequent feature or 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.x are:

   - SM 6.2 Service Pack 3 and SM 6.2 Service Pack 4
   - SM 6.3.2 and subsequent feature or service packs
   - SM 7.0 and subsequent feature or service packs

3. AWS-based Session Manager

   - SM 7.0.1 and subsequent service packs

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

4. Upgrades to Profile 1 Session Manager

   Starting with 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.x, 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.

5. 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.

6. 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 must be applied to every 7.0.1.2 SM in the system *prior* to upgrading the first SM 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.

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

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

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

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

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

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

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

Important note regarding S8300D upgrading to 7.1.3

The introduction of Spectre and Meltdown fixes with 7.1.3 has an impact on S8300D scalability performance. A Survivable Remote configuration (CM LSP and BSM) with the Spectre and Meltdown fixes enabled can only now support 200 users with up to 500 BHCC traffic.

Since these fixes are enabled by default, consider whether configuration changes are to plan a 7.1.3 upgrade.

The following options should be considered if higher capacity is required from the S8300D:

- Disabling the Spectre and Meltdown fixes on the S8300Ds – this will allow the S8300D to deliver the same level of capacity as with 7.1.2 and before.

or

- if disabling the fixes on the S8300D is not a viable option for you/your customer, plan to upgrade the embedded server to the latest S8300E model.

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

What's new in Session Manager Release 7.1.3.8

The following table lists enhancements in this release.

Enhancement	Description
ASM-83220	Diffie-helman-group1-sha1 key exchange algorithm has been removed from SSH. This change may cause connections from older SSH clients to be rejected. The best way to resolve failed connections is by updating to a newer SSH client that supports newer options.

What's new in Session Manager Release 7.1.3.7

The following table lists enhancements in this release.

Enhancement	Description
None	

What's new in Session Manager Release 7.1.3.6

The following table lists enhancements in this release.

Enhancement	Description
None	

What's new in Session Manager Release 7.1.3.5

The following table lists enhancements in this release.

Enhancement	Description
None	

What's new in Session Manager Release 7.1.3.4

The following table lists enhancements in this release.

Enhancement	Description
Security Service Pack (SSP)	Starting with Session Manager 7.1.3.4, Avaya will publish a Security Service Pack (SSP) in addition to the normal dot release artifacts. The SSP will include all available, and applicable, updates for Redhat Security Advisories (RHSA) published prior to the time of the building of the related software release. This SSP will be available on the 7.1.3.4 General Availability (GA) date for download via PLDS per normal procedures. Note that the 7.1.3.4 ISO itself will include the entire contents of the 7.1.3.4 SSP. If the ISO is used, there is no need to also install the SSP. Also note that the 7.1.3.4 SSP can be applied to any Session Manager release between 7.1.0.0 and 7.1.3.3, and it will install all RHSA fixes relevant to the underlying release. Going forward, information regarding future 7.1 SSPs will be provided in updates to PCN 2104S.

What's new in Session Manager Release 7.1.3.3

The following table lists enhancements in this release.

Enhancement	Description
None	

What's new in Session Manager Release 7.1.3.2

The following table lists enhancements in this release.

Enhancement	Description
None	

What's new in Session Manager Release 7.1.3.1

The following table lists enhancements in this release.

Enhancement	Description
None	

What's new in Session Manager Release 7.1.3

The following table lists enhancements in this release.

Enhancement	Description
UCID in CDR records	Session Manager Call Detail Records now capture portions of the User-to-User header, which contains the UCID value. The XML based CDRs are enhanced to support this field.
Security - AIDE	Session Manager now allows administrators to selectively enable or disable Advanced Intrusion Detection Environment (AIDE). By default, AIDE is disabled.

What's new in Session Manager Release 7.1.2

The following table lists enhancements in this release.

Enhancement	Description

Enhancement	Description
Export of User Registration Entries	A new button is available on the 7.1.2 User Registration page that allows the export of all registration data in XML or CSV format.
Customer Root Account	On upgrade to 7.1.2 and later loads, an option will be available to activate a customer root account as part of the upgrade activity.
Additional Security Hardening	Session Manager 7.1.2 supports a new security mode called "Hardened Profile" which activates FIPS level security.

What's new in Session Manager Release 7.1.1

The following table lists enhancements in this release.

Enhancement	Description
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.
Emergency Calling Application Sequence	In the release 7.1.1, administrators can enable application for emergency calls. Administrators can assign emergency calling application sequences to a user. For more information, see Administering Avaya Aura® Session Manager. In the release 7.1.1, a new tab for regular expression pattern rules is introduced on the Implicit User Rule Editor page. This tab enables the administration of application sequences for emergency calling using regular expression-based pattern rules. For more information, see *Administering Avaya Aura® Session Manager*.
Access to SIP phone registration data via the System Manager API	The System Manager Web services interface provides programmatic access to the Session Manager dashboard and user registration data for querying registration status and initiating various actions, including phone reboot. The System Manager Web Services API enforces the same level of data integrity as the GUI and import interfaces.
KVM	Session Manager 7.1.1 supports Kernel-based Virtual Machine (KVM) hypervisor as an additional deployment option.
Backup and Restore of Pluggable Adaptations	Pluggable adaptation modules will no longer require a re-install after upgrade from 7.1.1 to later loads. The modules will be automatically backed up and restored as part of the System Manager upgrade process.
Regular Expression Pattern Rule	In the release 7.1.1, a new tab for regular expression pattern rules is introduced on the Implicit User Rule Editor page. This tab enables the administration of application sequences for emergency calling using regular expression-based pattern rules. For more information, see *Administering Avaya Aura® Session Manager*.

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: ○ Ability to deprecate usage of TLS 1.0/1.1 ○ 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 7.1.3.8

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-82912	Administrator changes the extension number of a user that has an associated BSM.	The edit operation times out and displays a message complaining of an internal error.	7.1.3.6
ASM-82998	Failover to secondary System Manager	Session Manager continues to attempt to contact failed System Manager	8.1.3.0
ASM-80502	Remote users accessing Session Managers via an Avaya SBC	The Session Manager is not able to return VMON parameters based on the location derived from the IP address of the Avaya SBC	7.0.1.0
ASM-82668	Cassandra duplicate entries	Cassandra connection test fails	7.1.3.6
ASM-82906	TraceSM usage	TraceSM showed change in codec even when there was no actual codec change in call.	8.1.0.0
ASM-82975	TLS usage	Added capability to change the cipher string that is used for SIP & HTTP connections.	8.1.2.0
ASM-83224	Log harvester usage	Running the collection profile results in failure and not all logs are collected.	7.1.3.3
ASM-82599	[RHSA-2020:3908] Moderate: cpio security update	N/A	7.1.3.7
ASM-83196	[RHSA-2020:5083] Moderate: microcode_ctl	N/A	7.1.3.7
ASM-82603	[RHSA-2020:4011] Moderate: e2fsprogs security and bug fix update	N/A	7.1.3.7
ASM-82605	[RHSA-2020:3861] Low: glibc security, bug fix, and enhancement update	N/A	7.1.3.7
ASM-82607	[RHSA-2020:4007] Low: systemd security and bug fix update	N/A	7.1.3.7
ASM-82584	[RHSA-2020:3952] Moderate: expat security update	N/A	7.1.3.7
ASM-82919	[RHSA-2020:4276] Important: kernel security update	N/A	7.1.3.7
ASM-83193	[RHSA-2020:5002] Moderate: curl	N/A	7.1.3.7
ASM-83194	[RHSA-2020:5009] Moderate: python	N/A	7.1.3.7
ASM-82606	[RHSA-2020:3978] Moderate: glib2 and ibus security and bug fix update	N/A	7.1.3.7

ASM-82597	[RHSA-2020:3996] Moderate: libxml2 security and bug fix update	N/A	7.1.3.7
ASM-82612	[RHSA-2020:4032] Moderate: dbus security update	N/A	7.1.3.7
ASM-82613	[RHSA-2020:3848] Low: libmspack security update	N/A	7.1.3.7
ASM-83190	[RHSA-2020:4907] Important: freetype security update	N/A	7.1.3.7
ASM-83195	[RHSA-2020:5011] Moderate: bind	N/A	7.1.3.7
ASM-82585	[RHSA-2020:4026] Moderate: mariadb security and bug fix update	N/A	7.1.3.7
ASM-82611	[RHSA-2020:3915] Moderate: libssh2 security update	N/A	7.1.3.7
ASM-82610	[RHSA-2020:3911] Moderate: python security update	N/A	7.1.3.7
ASM-82602	[RHSA-2020:3916] Moderate: curl security update	N/A	7.1.3.7
ASM-82951	[RHSA-2020:4350] Moderate: java-1.8.0-openjdk security and bug fix update	N/A	7.1.3.7
ASM-83189	[RHSA-2020:5023] Moderate: kernel security and bug fix update	N/A	7.1.3.7

Fixes in Session Manager Release 7.1.3.7

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-78557	High usage of the Cassandra database on Session Manager.	Stale endpoint data on the SMGR SIP Registration page.	8.0.1.0
ASM-78383	Out-of-dialog REFER gets NOTIFY before 202 response.	Session Manager memory leak	8.0.1.2
ASM-80076	Attempting to use UDP with no UDP entity link administered	SIP header Parsing error in WebSphere log and error indication not properly returned	7.1.3.2
ASM-81094	Scheduled User Data Storage backups	Scheduled backups periodically may fail	8.1.3.0
ASM-79245	An egress adaptation is configured to adapt To/From headers. The far end entity modifies only the display name portion of the header values when it responds to the INVITE or sends a new request on the session towards the Session Manager.	The To/From headers in the 200 OK response and in subsequent requests on the session from the far end entity are not restored back to original values when sending the message back to the originating entity.	8.0.1.0

ASM-79738	Branch Session Manager with links to the main Communication Manager.	When links to the main Communication Manager are updated or removed on the Branch Session Manager, the changes do not get translated to the links to LSP.	7.1.3.2
ASM-80701	Setting CDR record format to XML and having calls active longer than the CDR Service interval	CDR records will have the port number rather than the dialed number.	7.1.3.3
ASM-80437	Mixture of UDP and TCP entity links.	SIP reINVITE is not retransmitted as mandated by RFC 3261.	7.1.0.0
ASM-81488	SIP request arrives at Session Manager with Max-Forwards set to 6.	SIP request receives 500 response rather than 483 response.	7.1.3.0
ASM-80636	Have the user registrations page up and leave it up in System Manager.	Registration details will indicate no registration even for devices that are actively registered.	7.1.3.3
ASM-80097	[RHSA-2020:1047] Moderate: wireshark	N/A	7.1.3.6
ASM-80100	[RHSA-2020:1190] Moderate: libxml2	N/A	7.1.3.6
ASM-80056	[RHSA-2020:0834] Important: kernel	N/A	7.1.3.6
ASM-81318	[RHSA-2020:2664] Important: kernel	N/A	7.1.3.6
ASM-80106	[RHSA-2020:1113] Moderate: bash	N/A	7.1.3.6
ASM-80641	[RHSA-2020:2082] Important: kernel	N/A	7.1.3.6
ASM-80105	[RHSA-2020:1061] Moderate: bind	N/A	7.1.3.6
ASM-80098	[RHSA-2020:1181] Low: unzip	N/A	7.1.3.6
ASM-80102	[RHSA-2020:1022] Low: file	N/A	7.1.3.6
ASM-80101	[RHSA-2020:1138] Low: gettext	N/A	7.1.3.6
ASM-80099	[RHSA-2020:1135] Low: polkit	N/A	7.1.3.6
ASM-81317	[RHSA-2020:2663] Moderate: ntp security update	N/A	7.1.3.6
ASM-80500	[RHSA-2020:1512] Important: java-1.8.0-openjdk security update	N/A	7.1.3.6
ASM-80089	[RHSA-2020:1011] Moderate: expat security update	N/A	7.1.3.6
ASM-80975	[RHSA-2020:2344] Important: bind security update	N/A	7.1.3.6
ASM-80051	[RHSA-2020:0897] Important: icu security update	N/A	7.1.3.6
ASM-81503	[RHSA-2020:2894] Important: dbus security update	N/A	7.1.3.6
ASM-80088	[RHSA-2020:1131] Moderate: python security update	N/A	7.1.3.6
ASM-81557	[RHSA-2020:2968] Important: java-1.8.0-openjdk security update	N/A	7.1.3.6

ASM-80085	[RHSA-2020:1100] Moderate: mariadb security and bug fix update	N/A	7.1.3.6
ASM-80096	[RHSA-2020:1000] Moderate: rsyslog security, bug fix, and enhancement update	N/A	7.1.3.6
ASM-81862	[RHSA-2020:3217] Moderate: grub2 security and bug fix update	N/A	7.1.3.6
ASM-80090	[RHSA-2020:1016] Moderate: kernel security, bug fix, and enhancement update	N/A	7.1.3.6
ASM-80084	[RHSA-2020:1021] Moderate: GNOME security, bug fix, and enhancement update	N/A	7.1.3.6
ASM-80087	[RHSA-2020:1020] Low: curl security and bug fix update	N/A	7.1.3.6
ASM-81868	[RHSA-2020:3220] Important: kernel security and bug fix update	N/A	7.1.3.6
ASM-81087	[RHSA-2020:2432] Moderate: microcode_ctl security, bug fix and enhancement update	N/A	7.1.3.6

Fixes in Session Manager Release 7.1.3.6

The following table lists the fixes in this release.

NOTE: As of June 23, 2020, Release 7.1.3.6 has been re-issued as version 713606 to include the first 2 defects in the following table.

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-79245	Adaptation of From and/or To header in initial request of dialog.	If callee UA modifies only the display name portion of the From and/or To header, or omits display name that was originally there in a request response or new request, then restoration of the From and/or To header towards the caller UA will not take place. The restoration logic will now ignore changes in display name and only check to see if callee UA modified the From and/or To header URI.	8.0.1.0
ASM-80898	None	Security vulnerability found in 7.1.3.6 version 713604	7.1.3.6
ASM-78037	A call routed by Session Manager is unanswered for 3 hours.	Session Manager drops the unanswered call after three hours.	7.1.3.1
ASM-78544	Change of domain name after installation of Session Manager	Alarms and SNMP traps not being sent for Session Manager	8.1.0.0
ASM-79440	Dial pattern administration	Use of the filter to search for dial patterns results in an error	7.1.3.3
ASM-77861	N/A	[RHSA-2019:3834] Important: kernel security update	7.1.3.5

ASM-77872	N/A	[RHSA-2019:3872] Important: kernel security update	7.1.3.5
ASM-78323	N/A	[RHSA-2019:3979] Important: kernel security and bug fix update	7.1.3.5
ASM-78322	N/A	[RHSA-2019:4190] Important: nss, nss-softokn, nss-util security update	7.1.3.5
ASM-79378	N/A	[RHSA-2020:0196] Important: java	7.1.3.5
ASM-79379	N/A	[RHSA-2020:0227] Important: sqlite	7.1.3.5
ASM-79376	N/A	[RHSA-2020:0374] Important: kernel	7.1.3.5
ASM-79605	N/A	[RHSA-2020:0540] Important: sudo security update	7.1.3.5

Fixes in Session Manager Release 7.1.3.5

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-76174	Mutual authentication set as “optional” and the occurrence of certificate errors on TLS links.	Spontaneous TLS connection failures	7.1.3.4
ASM-75851	A large amount of log files and CDR files.	High CPU usage and multiple instances of the process log_file_permissions.sh.	7.1.3.2
ASM-77666	Accessing the Session Manager Element Manager Maintenance Test screen multiple times from multiple login sessions.	System Manager could eventually run out of swap space and crash.	7.1.3.4
ASM-77844	Certificate Revocation List (CRL)) validation set to best effort or mandatory, with no System Manager CRLs available.	Session Manager network connections dropped and restarted.	7.1.0.0
ASM-76138	None	Error responses from PPM service providing excess information.	7.1.3.0
ASM-76943	AWS deployment	sm-report command fails	7.1.3.4
ASM-76132	Syslog based SIP tracing enabled	Syslog based SIP tracer configuration does not function properly	7.1.3.2
ASM-77121	Configure location groups or device settings groups via GUI at Home / Elements / Session Manager / Device and Location Configuration.	RTCP server info is not provided to SIP endpoints during registration	7.1.3.5
ASM-77853	Contact added where login name is same as email handle.	Login name is stored as SIP handle and hence contact is not dialable.	7.1.3.3
ASM-77359	Incorrect UCID format received from SIP entity	CDR records may be missing information or in certain cases, calls may fail.	7.1.3.1
ASM-76126	[RHSA-2019:1294] bind security update	N/A	7.1.3.4

ASM-76150	[RHSA-2019:1481] kernel security update	N/A	7.1.3.4
ASM-76337	[RHSA-2019:1619] vim security update	N/A	7.1.3.4
ASM-76581	[RHSA-2019:1815] java-1.8.0-openjdk security update	N/A	7.1.3.4
ASM-76920	[RHSA-2019:1873] kernel	N/A	7.1.3.4
ASM-76795	[RHSA-2019:1880] curl security and bug fix update	N/A	7.1.3.4
ASM-76598	[RHSA-2019:1884] libssh2 security update	N/A	7.1.3.4
ASM-76921	[RHSA-2019:2029] kernel	N/A	7.1.3.4
ASM-76934	[RHSA-2019:2030] python	N/A	7.1.3.4
ASM-76922	[RHSA-2019:2033] patch	N/A	7.1.3.4
ASM-76740	[RHSA-2019:2046] polkit security and bug fix update	N/A	7.1.3.4
ASM-76923	[RHSA-2019:2047] libcgroup	N/A	7.1.3.4
ASM-76735	[RHSA-2019:2049] libmspack security update	N/A	7.1.3.4
ASM-76924	[RHSA-2019:2052] libjpeg	N/A	7.1.3.4
ASM-76925	[RHSA-2019:2057] bind	N/A	7.1.3.4
ASM-76926	[RHSA-2019:2060] dhclient	N/A	7.1.3.4
ASM-76927	[RHSA-2019:2091] systemd	N/A	7.1.3.4
ASM-76928	[RHSA-2019:2110] rsyslog	N/A	7.1.3.4
ASM-76929	[RHSA-2019:2118] glibc	N/A	7.1.3.4
ASM-76885	[RHSA-2019:2136] libssh2 security, bug fix, and enhancement update	N/A	7.1.3.4
ASM-76930	[RHSA-2019:2143] openssh	N/A	7.1.3.4
ASM-76931	[RHSA-2019:2159] unzip	N/A	7.1.3.4
ASM-76741	[RHSA-2019:2169] linux-firmware security, bug fix, and enhancement update	N/A	7.1.3.4
ASM-76886	[RHSA-2019:2181] curl security and bug fix update	N/A	7.1.3.4
ASM-76737	[RHSA-2019:2189] procps-ng security and bug fix update	N/A	7.1.3.4
ASM-76739	[RHSA-2019:2197] elfutils security, bug fix, and enhancement update	N/A	7.1.3.4
ASM-76932	[RHSA-2019:2237] nspr	N/A	7.1.3.4
ASM-76933	[RHSA-2019:2304] openssl	N/A	7.1.3.4
ASM-76738	[RHSA-2019:2327] mariadb security and bug fix update	N/A	7.1.3.4

ASM-77124	[RHSA-2019:2600] kernel security and bug fix update	N/A	7.1.3.4
ASM-77352	[RHSA-2019:2829] kernel security update	N/A	7.1.3.4
ASM-77396	[RHSA-2019:2964] patch security update	N/A	7.1.3.4
ASM-77593	[RHSA-2019:3055] kernel security and bug fix update	N/A	7.1.3.4
ASM-77693	[RHSA-2019:3128] java-1.8.0-openjdk security update	N/A	7.1.3.4
ASM-77688	[RHSA-2019:3197] sudo security update	N/A	7.1.3.4
ASM-76915	[RHSA-2019-2075] binutils security and bug fix update	N/A	7.1.3.4
ASM-76914	[RHSA-2019-2077] Low: ntp security, bug fix, and enhancement update	N/A	7.1.3.4
ASM-76225	[RHSA-2019:1587] python (tcp)	N/A	7.1.3.4
ASM-76434	[RHBA-2019:1703] tzdata enhancement update	N/A	7.1.3.4

Fixes in Session Manager Release 7.1.3.4

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-74365	Call Detail Recording (CDR) enabled and restarted from command line	CDR files grow unbounded leading to possible disk exhaustion and system impacts.	7.1.3.2
ASM-75825	High alarming rates	Alarm failures and Serviceability Agent stops responding	7.1.3.0
ASM-72976	N/A	Various TraceSM improvements	7.1.0.0
ASM-72072	Administration issue resulting SIP routing loops	BSM goes out of service due to failure to detect and break looping SIP invite.	7.1.2.0
ASM-75626	[RHSA-2019:0818-01] Important: kernel security and bug fix update	N/A	7.1.3.3
ASM-74971	[RHSA-2019:0512-01] Important: kernel security, bug fix, and enhancement update	N/A	7.1.3.3
ASM-75386	[RHSA-2019:0775] Important: java security update	N/A	7.1.3.3
ASM-75288	[RHSA-2019:0679-01] Important: libssh2 security update	N/A	7.1.3.3
ASM-75167	[RHSA-2019:0435-01] Moderate: java-1.8.0-openjdk security update	N/A	7.1.3.3

ASM-75310	[RHSA-2019:0710] Important python security update	N/A	7.1.3.3
ASM-74712	(RHSA-2019:0163) (tcp) kernel	N/A	7.1.3.3
ASM-74713	(RHSA-2019:0230) (tcp) polkit	N/A	7.1.3.3
ASM-74714	(RHSA-2019:0368) (tcp) systemd	N/A	7.1.3.3
ASM-74711	(RHSA-2019:0194) (tcp) bind	N/A	7.1.3.3
ASM-74160	RHSA-2019:0109 Perl Security Update	N/A	7.1.3.3
ASM-74078	[RHSA-2019:0049] Important: systemd update	N/A	7.1.3.3
ASM-75377	(RHSA-2019:0679) (tcp) libssh2	N/A	7.1.3.3
ASM-75818	(RHSA-2019:1168) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout) (tcp) kernel	N/A	7.1.3.3
ASM-75817	(RHSA-2019:1228) (tcp) wget	N/A	7.1.3.3

Fixes in Session Manager Release 7.1.3.3

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-71636	Branch Session Manager (BSM) on S8300D server	BSM eth0 interface does not come up in rare cases and BSM is out of service until reboot	7.1.3.0
ASM-71601	Call Detail Recording (CDR) usage in presence of a corrupted record.	CDR Processing stops permanently when a parsing error occurs.	7.1.3.0
ASM-69662	Use of J1xx phone models aliased as 96x1	Administrator changes of buttons, labels, etc do not appear on J100 series phones	7.1.3.0
ASM-71635	[RHSA-2018:2570-01] Important: bind security update	N/A	7.1.3.2
ASM-73060	RHEL 7 : glibc (RHSA-2018:3092) (tcp)	N/A	7.1.3.2
ASM-73025	[RHSA-2018:3059-01] Low: X.org X11 security, bug fix, and enhancement update	N/A	7.1.3.2
ASM-72398	[RHSA-2018:2768-01] Moderate: nss security update	N/A	7.1.3.2
ASM-70881	RHEL 7 : python (RHSA-2018:2123) (tcp)	N/A	7.1.3.2
ASM-70883	RHEL 7 : gnupg2 (RHSA-2018:2181) (tcp)	N/A	7.1.3.2
ASM-73050	RHEL 7 : kernel (RHSA-2018:3083) (tcp)	N/A	7.1.3.2
ASM-72360	[RHSA-2018:2748-01] Important: kernel security and bug fix update	N/A	7.1.3.2

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-71554	RHEL 7 : yum-utils (RHSA-2018:2285) CVE-2018-10897	N/A	7.1.3.2
ASM-71581	[RHSA-2018:2384] Important kernel update	N/A	7.1.3.2
ASM-72990	[RHSA-2018:3157-01] Moderate: curl and nss-pem security and bug fix update	N/A	7.1.3.2
ASM-73054	RHEL 7 : GNOME (RHSA-2018:3140) (tcp)	N/A	7.1.3.2
ASM-72789	Java Security Update (RHSA-2018:2942)	N/A	7.1.3.2

Fixes in Session Manager Release 7.1.3.2

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-66343	IPv6 route header showing up in SIP messages when IPv6 disabled	Some external SIP devices may be unable to parse the SIP message correctly, even though the V6 header can be safely ignored. This will cause SIP signaling failures.	7.1.0.0
ASM-69675	Incorrect SIP firewall rule loading	SIP Manipulators being lost on secmod restart/reboot	7.1.2.0
ASM-70860	Sm-report tool usage resulting in failures	Running sm-report causes Websphere javacores and possible system outages	7.1.0.0
ASM-71155	ETH0 network interface sometimes does not come up after S8300D reboot.	Session Manager dashboard shows “no connection” to the BSM and the BSM cannot be accessed via SSH. The BSM is completely out of service.	7.1.0.0
ASM-72091	SM to SM connections failing due to missing CN field in Root CA.	TLS connection failures	7.1.3.1
ASM-70965	Resource starvation on the S8300D	S8300D BSM generating excessive CPU and memory alarms	7.1.0.0
ASM-70882	kernel (RHSA-2018:1965) (Spectre) (tcp)	N/A	7.1.3.0
ASM-70881	python (RHSA-2018:2123) (tcp)	N/A	7.1.3.0
ASM-70883	gnupg2 (RHSA-2018:2181) (tcp)	N/A	7.1.3.0
ASM-71554	yum-utils (RHSA-2018:2285) CVE-2018-10897	N/A	7.1.3.0
ASM-71551	[RHSA-2018:2242-01] Moderate: java-1.8.0-openjdk security and bug fix update	N/A	7.1.3.0

ASM-71580	[RHSA-2018:2349] Moderate: mariadb-libs update	N/A	7.1.3.0
ASM-71581	[RHSA-2018:2384] Important kernel update	N/A	7.1.3.0
ASM-70861	tzdata Linux RPM updated to tzdata-2018e	N/A	7.1.3.0

Fixes in Session Manager Release 7.1.3.1

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-69014	Changing the SAL-Agent certificate from System Manager	The old certificate is still used until the SAL-Agent is restarted. Serviceability administration and retrieving logs might not be possible until SAL-Agent is restarted.	6.1.3
ASM-70265	None	TLS 1.0/1.1 ports were available though not in use	7.1.0.0
ASM-69675	Use of SIP manipulator	SIP manipulator not properly activated after restart/reboot	7.1.0.0
ASM-69676	Unknown – Timing issue	The traceSM command does not capture any messages.	7.1.2.0
ASM-64731	Systems with large numbers of dial pattern and large numbers of defined locations	Slow response times on GUI actions and import performance	7.0.0.0
ASM-69981	7.1 System Manager managing pre-6.3.12 Session Managers.	Data Redundancy Tests will fail on the SM. CAC issues resulting in call failures. SMs may go into Deny New Service state occasionally.	7.1.0.0
ASM-70260	[RHSA-2018:1319-01] Important: kernel security and bug fix update	N/A	N/A
ASM-69446	[RHSA-2018:0395-01] Important: kernel security and bug fix update	N/A	N/A
ASM-70271	[RHSA-2018:1453] RHEL 7: dhcp (tcp)	N/A	N/A
ASM-70259	[RHSA-2018:1318-01] Important: kernel security, bug fix, and enhancement update	N/A	N/A
ASM-70270	[RHSA-2018:1700] RHEL 7: procps-ng (tcp)	N/A	N/A
ASM-69933	[RHSA-2018:1191-01] Critical: java-1.8.0-openjdk security update	N/A	N/A

Fixes in Session Manager Release 7.1.3

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-66819	Use of remote NFS shares to store performance data.	NFS share would fail to mount.	SM 7.1
ASM-65686	Use of the Registration Status screen for viewing third party or non-AST device information	The IP Address doesn't appear on the main display but does appear when the user clicks Show Detail.	SM 7.1
ASM-66743	Viewing Session Manager Dashboard and filtering the display on the Version column	An error appeared instead of filtering the column on entered version string	SM 7.0.1.2
ASM-66457	Equinox conference when all parties are remote (PSTN-based)	Conference fails when customers try to join the conference	SM 7.1
ASM-67735	A system heavily loaded with administrator activity, or under heavy traffic.	High CPU usage from JBoss which could negatively impact the system functionality	SM 7.0.1.2
ASM-467	Contacts that are added on one endpoint type then updated or deleted on a different type.	For update, the operation may fail with invalid contact. For delete, the contact may not get deleted.	SM 7.0.1.1
ASM-67618	RHSA-2018:0007-01: Important: kernel security update	Contains fixes for Spectre/Meltdown vulnerability	N/A
ASM-67616	RHSA-2018:0012-01: Important: microcode_ctl security update	N/A	N/A
ASM-66686	RHSA-2017:2930: Kernel	N/A	N/A
ASM-66685	RHSA-2017:3075: wget	N/A	N/A
ASM-67611	RHSA-2017:3315-01: Important: kernel security and bug fix update	N/A	N/A
ASM-67610	RHSA-2017:3263-01: Moderate: curl security update	N/A	N/A
ASM-68037	RHSA-2018:0102: bind	N/A	N/A
ASM-68038	RHSA-2018:0095: java-1.8.0-openjdk	N/A	N/A
ASM-66684	RHSA-2017:2998: java-1.8.0-openjdk	N/A	N/A

Fixes in Session Manager Release 7.1.2

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-57972	Red Hat Update for boost (RHSA-2013:0668)	N/A	N/A
ASM-57971	Red Hat Update for MySQL (RHSA-2014:0164)	N/A	N/A
ASM-58021	[RHSA-2016:1292-01] Important: libxml2 security update	N/A	N/A
ASM-58518	[RHSA-2016:0591-01] Moderate: nss, nss-util, and nspr security, bug fix, and	N/A	N/A

ID	Minimum Conditions	Visible symptoms	Release found in
	enhancement update		
ASM-59501	[RHSA-2016:1944-01] Important: bind security 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-57694	[RHSA-2016:0760-01] Moderate: file security, bug fix, and enhancement update	N/A	N/A
ASM-59502	[RHSA-2016:1940-01] Important: openssl security update	N/A	N/A
ASM-64054	Unreachable DNS server	Call completion delays up to 10 seconds	7.1
ASM-65876	Use of Team button on SIP stations assigned to a survivable server (BSM)	In some cases, data replication will fail to the associated BSM.	7.0
ASM-64815	SIP entities administered with FQDNs and Session Manager running 7.1.	Entity links out of service when the links involved contain SIP entities administered with FQDNs.	7.1
ASM-64055	One or more DNS servers administered.	Entering “none” when prompted for DNS servers in SMnetSetup does not remove the DNS server.	7.1
ASM-62560	Administered FQDN on Local Host Name Resolution page in a different case format than what is administered under SIP Entity	Session Manager is unable to perform case insensitive LHNR FQDN lookups to proper IP Address, which results in Entity Links out of service.	7.1
ASM-64190	SIP endpoint remains logged in for over 90 days prior to log off.	User customized setting on the endpoint may be lost upon next login.	6.3.8

Fixes in Session Manager Release 7.1.1

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms	Release found in
ASM-64157	[RHSA-2017:1680-01] bind security update	N/A	N/A
ASM-64156	[RHSA-2017:1574-01] sudo security update	N/A	N/A
ASM-64158	[RHSA-2017:1481-01] glibc security update	N/A	N/A
ASM-62279	[RHSA-2017:0286-01] Moderate: openssl security update	N/A	N/A
ASM-63493	[RHSA-2017:1365-03] Important: nss security and bug fix update	N/A	N/A
ASM-63415	[RHSA-2016:2872]: Moderate: sudo	N/A	N/A

ID	Minimum Conditions	Visible symptoms	Release found in
	security update		
ASM-63416	[RHSA-2017:1108-01] Moderate: java-1.8.0-openjdk security and bug fix update	N/A	N/A
ASM-63421	[RHSA-2017:1095] Important: bind security update	N/A	N/A
ASM-62873	[RHSA-2017:1100-01] Critical: nss and nss-util security update	N/A	N/A
ASM-64128	[RHSA-2017:0725-01] kernel security and bug fix update	N/A	N/A
ASM-62874	[RHSA-2017:0933-01] Important: kernel security, bug fix, and enhancement update	N/A	N/A
ASM-63491	[RHSA-2017:1308-01] Important: kernel security, bug fix, and enhancement update	N/A	N/A
ASM-63412	[RHSA-2017:0907] Moderate: util-linux security and bug fix update	N/A	N/A
ASM-63413	[RHSA-2016:2597] Moderate: firewalld security, bug fix, and enhancement update	N/A	N/A
ASM-60501	Equinox clients and Avaya Aura Device Services (AADS)	Cassandra commit logs don’t get cleaned up and start accumulating and occupying disk space. After some time, data partition gets full.	7.1
ASM-61724	System Manager Geo-Redundancy	After creating and enabling a GEO configuration, none of the SMs and BSMs was pointing to the primary SMGR, resulting in a failure to properly initialize.	7.1
ASM-61184	Malformed SIP message handling	Previously, when a third-party endpoint sent a malformed REGISTER request to Session Manager, other SIP messages may have been lost, potentially causing call failures. Now, the malformed REGISTER request is rejected, and other requests are not impacted.	7.0.1.1
ASM-62227	CDR adjuncts	CDR adjuncts were not able to remove the CDR files after retrieving them. CDR adjuncts now can remove the file.	7.0.1.1
ASM-63009	3rd party identity certificates	3rd party identity certificates are lost on upgrades to SM 7.1. 3rd party identity certificates are now preserved through upgrade when applying 7.1.1 or later loads.	7.1
ASM-57981	Equinox clients and Avaya Aura Device Services (AADS)	In certain cases, when a request to add or update a contact arrived at the wrong node in a cluster, or when the contact had greater than 4 associated phone numbers, the	7.0.1.2

ID	Minimum Conditions	Visible symptoms	Release found in
		request would fail.	
ASM-62169	FQDN administration	Using SMnetSetup to change the hostname from a short hostname (no domain) to a FQDN resulted in WebSphere failing to start. Although it is recommended that Session Manager be administered with a FQDN, SMnetSetup now handles changing from a short hostname to a FQDN.	7.0
ASM-62560	Local Host Name Resolution (LHNR) administration.	Inconsistent case usage on FQDNs administered on the LHNR page could result in failed address resolution and Entity links down. Now LHNR entries are handled in a case-insensitive manner.	7.1

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 7.1.3.8

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

ID	Minimum conditions	Visible symptoms	Workaround
ASM-67319	Use of Emergency checkbox on dialpattern	Unchecking of Emergency checkbox on dialpattern does not result in reload of affected endpoints	Select the affected devices on the Session Manager -> Registration Summary page and initiate a “reload config” operation.
ASM-83776	Location bandwidth exceeded	Alarm description incorrectly displays event ID instead of Location name	None

Known issues and workarounds in Session Manager Release 7.1.3.7

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

ID	Minimum conditions	Visible symptoms	Workaround
ASM-67319	Use of Emergency checkbox on dialpattern	Unchecking of Emergency checkbox on dialpattern does not result in reload of affected endpoints	Select the affected devices on the Session Manager -> Registration Summary page and initiate a “reload config” operation.

Known issues and workarounds in Session Manager Release 7.1.3.6

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

ID	Minimum conditions	Visible symptoms	Workaround
ASM-67319	Use of Emergency checkbox on dialpattern	Unchecking of Emergency checkbox on dialpattern does not result in reload of affected endpoints	Select the affected devices on the Session Manager -> Registration Summary page and initiate a “reload config” operation.

Known issues and workarounds in Session Manager Release 7.1.3.5

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

ID	Minimum conditions	Visible symptoms	Workaround
ASM-67319	Use of Emergency checkbox on dialpattern	Unchecking of Emergency checkbox on dialpattern does not result in reload of affected endpoints	Select the affected devices on the Session Manager -> Registration Summary page and initiate a “reload config” operation.

Known issues and workarounds in Session Manager Release 7.1.3.4

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

ID	Minimum conditions	Visible symptoms	Workaround
ASM-67319	Use of Emergency checkbox on dialpattern	Unchecking of Emergency checkbox on dialpattern does not result in reload of affected endpoints	Select the affected devices on the Session Manager -> Registration Summary page and initiate a “reload config” operation.

Known issues and workarounds in Session Manager Release 7.1.3.3

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

ID	Minimum conditions	Visible symptoms	Workaround
ASM-67319	Use of Emergency checkbox on dialpattern	Unchecking of Emergency checkbox on dialpattern does not result in reload of affected endpoints	Select the affected devices on the Session Manager -> Registration Summary page and initiate a “reload config” operation.

Known issues and workarounds in Session Manager Release 7.1.3.2

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

ID	Minimum conditions	Visible symptoms	Workaround
ASM-67319	Use of Emergency checkbox on dialpattern	Unchecking of Emergency checkbox on dialpattern does not result in reload of affected endpoints	Select the affected devices on the Session Manager -> Registration Summary page and initiate a “reload config” operation.

Known issues and workarounds in Session Manager Release 7.1.3.1

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

ID	Minimum conditions	Visible symptoms	Workaround
ASM-67319	Use of Emergency checkbox on dialpattern	Unchecking of Emergency checkbox on dialpattern does not result in reload of affected endpoints	Select the affected devices on the Session Manager -> Registration Summary page and initiate a “reload config” operation.

Known issues and workarounds in Session Manager Release 7.1.3

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

ID	Minimum conditions	Visible symptoms	Workaround
ASM-67319	Use of Emergency checkbox on dialpattern	Unchecking of Emergency checkbox on dialpattern does not result in reload of affected endpoints	Select the affected devices on the Session Manager -> Registration Summary page and initiate a “reload config” operation.
ASM-66343	IPv6 route header showing up in SIP messages when IPv6 disabled	Some external SIP devices may be unable to parse the SIP message correctly, even though the V6 header can be safely ignored. This will cause SIP signaling failures.	Contact Support – PSN005101
ASM-68390	Changing the name of a Data Storage Cluster	When the name of a Data Storage cluster is changed via the System Manager GUI, the name change is not detected by Cassandra.	Execute a “restart mgmt.” command on the SM command line.

Known issues and workarounds in Session Manager Release 7.1.2

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

ID	Minimum conditions	Visible symptoms	Workaround
ASM-66343	IPv6 route header showing up in SIP messages when IPv6 disabled	Some external SIP devices may be unable to parse the SIP message correctly, even though the V6 header can be safely ignored. This will cause SIP signaling failures.	Contact Support – PSN005101
ASM-62675	Removal of Session Manager from a Cassandra clustered system	After decommissioning a previously installed Session Manager instance, User Data Store errors may start being seen, and subsequent upgrade problems may arise if the earlier Session Manager instance is not manually removed from the Session Manager Cassandra Cluster.	PSN005086 - Avaya Aura® Session Manager v7x User Data Store Errors for decommissioned SM

Known issues and workarounds in Session Manager Release 7.1.1

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

ID	Minimum conditions	Visible symptoms	Workaround
ASM-482	Use of SIP performance graphs after	The SIP performance graphs may show an incorrect value at the time of restart indicating a very high volume of calls during that period.	Exclude the affected time period from

ID	Minimum conditions	Visible symptoms	Workaround
	ASSET restarts		the graphing interval.
N/A	AADS	Avaya Aura Device Services (AADS) versions prior to 7.1 will not interoperate with Session Manager 7.1.1.	AADS should be upgraded to 7.1 prior to SM upgrade to 7.1.1

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 7.1.3.x

Backing up the software

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

Installing the System Manager software

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

Upgrading the System Manager software

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

System Manager upgrade path

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

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

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

Troubleshooting the installation

Execute following command from System Manager Command Line Interface with customer 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.

Required artifacts for System Manager Release 7.1.x.x

Required artifacts for System Manager Release 7.1.3.8

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

Download ID	Artifact	Notes
SMGR7138GA1	System Manager 7.1.3.8 Release 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_7.1.3.8_r713812157.bin Size: 1408 MB MD5sum: 493b4ee5bc88210712af13b20f57c3e5
SMGR7138GA2	SDM Client for System Manager 7.1.3.8	Verify that the md5sum for the downloaded bin image matches the number on the Avaya PLDS website. Avaya_SDMClient_win64_7.1.3.8.0035922_48.zip Size: 229 MB MD5sum: d1ecb35b8dc8d867c53fbb9ac0878cbd

Required artifacts for System Manager Release 7.1.3.7

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

Download ID	Artifact	Notes
SMGR7137GA1	System Manager 7.1.3.7 Release 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_7.1.3.7_r713711864.bin Size: 1.4 GB MD5sum: e52e1911f922301b8f8f0d027f062b54
SMGR7137GA3	SDM Client for System Manager 7.1.3.7	Verify that the md5sum for the downloaded bin image matches the number on the Avaya PLDS website. Avaya_SDMClient_win64_7.1.3.7.0035487_38.zip Size: 229 MB MD5sum: 2274cf2efb9a6059829f5bbf7eb05141

Required artifacts for System Manager Release 7.1.3.6

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

Download ID	Artifact	Notes
SMGR7136GA1	System Manager 7.1.3.6 Release 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_7.1.3.6_r713611194.bin Size: 1370 MB MD5sum: d07102957da328c0eeda342e6387944f

Download ID	Artifact	Notes
SMGR7136GA3	SDM Client for System Manager 7.1.3.6	Verify that the md5sum for the downloaded bin image matches the number on the Avaya PLDS website. Avaya_SDMClient_win64_7.1.3.6.0034633_26.zip Size: 229 MB MD5sum: 0fa461ee176fadf206c9706b07e8574f

Required artifacts for System Manager Release 7.1.3.5

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

Download ID	Artifact	Notes
SMGR7135GA1	System Manager 7.1.3.5 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_7.1.3.5_r713510693.bin Size: 1368 MB MD5sum: 61da15806ee7d73f912723d03974bfdb
SMGR7135GA3	SDM Client for System Manager 7.1.3.5	Verify that the md5sum for the downloaded bin image matches the number on the Avaya PLDS website. Avaya_SDMClient_win64_7.1.3.5.0033955_13.zip Size: 229 MB MD5sum: 16386f70f48164f7b11661c3a2ba4844

Required artifacts for System Manager Release 7.1.3.4

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

Download ID	Artifact	Notes
SMGR7134GA1	System Manager 7.1.3.4 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_7.1.3.4_r713409912.bin Size: 1234 MB MD5sum: 7bc480f2f346035d6650946b71cc36b9
SMGR7134GA3	SDM Client for System Manager 7.1.3.4	Verify that the md5sum for the downloaded bin image matches the number on the Avaya PLDS website. Avaya_SDMClient_win64_7.1.3.4.0033316_17.zip Size: 229 MB MD5sum: 61af9d3adb5ff969a72766a7a298171d

Required artifacts for System Manager Release 7.1.3.3

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

Download ID	Artifact	Notes

Download ID	Artifact	Notes
SMGR7133GA1	System Manager 7.1.3.3 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_7.1.3.3_r713309127.bin Size: 1212 MB MD5sum: 5839c1ffcf2fce64d27f66bc041ac554
SMGR7133GA3	SDM Client for System Manager 7.1.3.3	Verify that the md5sum for the downloaded bin image matches the number on the Avaya PLDS website. Avaya_SDMClient_win64_7.1.3.3.0032501_9.zip Size: 229 MB MD5sum: 4b74ed00ab048114b40820c78272fe56

Required artifacts for System Manager Release 7.1.3.2

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

Download ID	Artifact	Notes
SMGR7132GA1	System Manager 7.1.3.2 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_7.1.3.2_r713208362.bin Size: 1203 MB MD5sum: 398aa00f9effcaf2697ff9444040276f
SMGR7132GA2	SDM Client for System Manager 7.1.3.2	Verify that the md5sum for the downloaded bin image matches the number on the Avaya PLDS website. Avaya_SDMClient_win64_7.1.3.2.0031821_5.zip Size:229 MB MD5sum: 935fb8fdb7a6fd1fa0e534533c69a3b0

Required artifacts for System Manager Release 7.1.3.1

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

Download ID	Artifact	Notes
SMGR7131GA1	System Manager 7.1.3.1 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_7.1.3.1_r713108157.bin Size: 1191 MB MD5sum: 3cade30f7af5079335959c8ed6e264dd
SMGR7131GA2	SDM Client for System Manager 7.1.3.1	Verify that the md5sum for the downloaded bin image matches the number on the Avaya PLDS website. Avaya_SDMClient_win64_7.1.3.1.0031570_3.zip Size:229 MB MD5sum: 82c7cb16c4772e5c58fb262309224b39

Required artifacts for System Manager Release 7.1.3

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

Download ID	Artifact	Notes
SMGR713GA01	System Manager 7.1.3 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_7.1.3.0_r713007763.bin Size: 1107 MB MD5sum: d5bbdffc8a6c1ba049505cfc59dc8d2c
SMGR713GA02	SDM Client for System Manager 7.1.3	Verify that the md5sum for the downloaded bin image matches the number on the Avaya PLDS website. Avaya_SDMClient_win64_7.1.3.0.0330162_32.zip Size: 229 MB MD5sum: 7c96d5524e81c27e6d103d6b53431066

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

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

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

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

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

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

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

Required artifacts for System Manager Release 7.1.2

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

Download ID	Artifact	Notes
SMGR712GA01	System Manager 7.1.2 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_7.1.2.0_r712007353.bin Size: 1123 MB MD5sum: 20d1fd7a4661895f8ffd40b8e607ac1c
SMGR712GA02	SDM Client for System Manager 7.1.2	Verify that the md5sum for the downloaded bin image matches the number on the Avaya PLDS website. Avaya_SDMClient_win64_7.1.2.0.0528621_26.zip

Download ID	Artifact	Notes
		Size: 227 MB MD5sum: 32c89bff5bdd811d57c5c3bc4712791b

Required artifacts for System Manager Release 7.1.1.1

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

Download ID	Artifact	Notes
SMGR7111GA1	System Manager 7.1.1.1 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_7.1.1.1_r711107109.bin Size: 1.2 GB Md5sum: aad9bff4cf0cd6b72642c5a702673dc4

Required artifacts for System Manager Release 7.1.1

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

Download ID	Artifact	Notes
SMGR711GA01	System Manager 7.1.1 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_7.1.1.0_r711006931.bin Size: 988 MB Md5sum: c30d7e0785700b46874bb35be2220ac6
SMGR711GA02	SDM Client for System Manager 7.1.1	Verify that the md5sum for the downloaded bin image matches the number on the Avaya PLDS website. Avaya_SDMClient_win64_7.1.1.0.0426596_43.zip Size: 226 MB Md5sum: 60c34dac757d07c2148eb2659fb42117
SMGR711KVM1	System Manager KVM OVA 7.1GA OVA Profile-2	Verify that the md5sum for the downloaded bin image matches the number on the Avaya PLDS website. SMGR-7.1.0.0.1125193-kvm-52.ova Size: 2.93 GB Md5sum: 9f0a81eb6f670af0fa5421a9124e9306
SMGR711KVM2	System Manager KVM OVA 7.1GA OVA Profile-3	Verify that the md5sum for the downloaded bin image matches the number on the Avaya PLDS website. SMGR-PROFILE3-7.1.0.0.1125193-kvm-52.ova Size 2.93 GB Md5sum: fe98c50258a104392aef48c5d7087fc1

Required artifacts for System Manager Release 7.1

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

Download ID	Artifact	Notes

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-e65-54.ova Size: 2971 MB Md5sum: e909788930da189b4cca0b1ca6bc376e
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-e65-54.ova Size: 2997 MB Md5sum: e646aec6fc53c9e96162ba4cdd876dd7
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
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 deployment and upgrade procedure, see deployment and upgrade documents on the Avaya Support website.

Note: The data migration utility is required only if you are upgrading from System Manager 6.0.x, 6.1.x, 6.2.x, 6.3.x 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 7.1.3 for more details.

Download ID	Artifact	Notes
SMGR71GA012	Data Migration utility for System Manager 7.1.x release. Refer **PSN004802u** for more details	Verify that the md5sum for the downloaded OVA image matches the number on the Avaya PLDS website. File Name: datamigration-147.bin Size: 2.4 MB Md5sum: d379a78740804b6e497cc2fbf26a4b13

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 242 64 bit	For Solution Deployment Manager Client, Open JDK Open JDK 1.8.0-internal
JBoss	6.1	
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	5.5,6.0,6.5,6.7	Earlier versions of VMware are no longer supported.

Must read:

1. For Release 7.1.1 GA Installation:
   - Fresh: Deploy 7.1 GA OVA + Apply 7.1.1 GA Patch bin
   - Upgrade: Deploy 7.1 GA OVA + 7.1.1 Data Migration Bin + 7.1.1 GA Patch bin.
   - Production SMGR 7.1 GA Customers: Apply 7.1.1 GA Bin on existing SMGR 7.1 Load.

2. To verify that the System Manager installation is ready for patch deployment, do one of the following:
   - On the web browser, type https://<Fully Qualified Domain Name>/SMGR and ensure that the system displays the System Manager 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`.

3. Perform the following steps to enable EASG on System Manager 7.1.1:
   - To enable EASG on SYSTEM MANAGER via Command Line Interface via Cust user type the following command:
     ```
     # EASGManage --enableEASG
     ```
   - To disable the EASG on SYSTEM MANAGER type the following command:
     ```
     # EASGManage –disableEASG
     ```
4. For VMware to VE System Manager Upgrade, remove all the snapshot from old VMware System Manager otherwise rollback operation will fail.
5. The versions*.xml is published on PLDS. To download latest versions.xml file for SUM, search on PLDS using Download PUB ID “SMGRSUM0001” only. Do not use version or product on PLDS in the search criteria.
6. System Manager Login banner no longer supports html characters.

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.

What’s new in System Manager Release 7.1.x.x

What’s new in System Manager Release 7.1.3.8

The following table lists enhancements in this release.

Enhancement	Description
N/A	N/A

What’s new in System Manager Release 7.1.3.7

The following table lists enhancements in this release.

Enhancement	Description
N/A	N/A

What’s new in System Manager Release 7.1.3.6

The following table lists enhancements in this release.

Enhancement	Description

Enhancement	Description
N/A	N/A

What’s new in System Manager Release 7.1.3.5

The following table lists enhancements in this release.

Enhancement	Description
N/A	N/A

What’s new in System Manager Release 7.1.3.4

The following table lists enhancements in this release.

Enhancement	Description
N/A	N/A

What’s new in System Manager Release 7.1.3.3

The following table lists enhancements in this release.

Enhancement	Description
N/A	N/A

What’s new in System Manager Release 7.1.3.2

The following table lists enhancements in this release.

Enhancement	Description
N/A	N/A

What’s new in System Manager Release 7.1.3.1

The following table lists enhancements in this release.

Enhancement	Description
N/A	N/A

What’s new in System Manager Release 7.1.3

The following table lists enhancements in this release.

Enhancement	Description
Customer customization for Security Profiles	Support for customization of some of the parameters in the Security Profiles
Virtual Machine Application Reports	Enables customer or partner administrators looking to expand an Avaya Aura 7 solution, to easily run a report via the SMGR CLI to gather a single view of an existing Avaya Aura 7 Solution deployment.
VM Snapshot Management on AVP	Enabled listing/deletion of VM snapshots on AVP hosts
Bulk Import/Export support extended in CM Element Manager	Bulk Import/Export using Excel datasheets is now supported for End Points, Coverage Paths and Hunt Groups.

What’s new in System Manager Release 7.1.2

The following table lists enhancements in this release.

Enhancement	Description
AVP License enforcement	From SMGR release 7.1.2 onwards enforcement of AVP Licenses is supported by System Manager.
AVP Remote Deployment for S8300 D/E LSP migrations (CM R5.2.1 & R6.x to CM R7.1.2)	SDM orchestrates and automates the migration of Communication Manager (R5.2.1 & R6.x) LSPs to Release 7.1.2. This includes Remote Deployment of AVP to target platform.
Bulk Provisioning File support for bulk upgrade/migration (AVP and CM parameters)	Software Deployment Manager now supports Excel file import for configuration of AVP and CM parameters for Bulk upgrade/migration.
Support for EASG for Web login	EASG based login is now supported for Avaya support technicians to login to the System Manager web console.
Export the “delta” of changes in User Management	System Manager now supports the feature to export the “delta” of users (“Added/Updated/Deleted”) for a specified period of time. Delta period could be “One Day” or “One Week” or “One Month”.
Performance improvements in Bulk Export of Users	Improvement in the time required to export user data in User Management.
Enhanced Editor support for Trunk Group	Trunk Group provisioning is now supported using Enhanced editor to achieve Communication Manager connection optimization.
Bulk Import/Export support for Vector Directory Number	Bulk Import/Export using Excel datasheets is now supported for Vector Directory Number.

What’s new in System Manager Release 7.1.1.1

The following table lists enhancements in this release.

Enhancement	Description
N/A	N/A

What’s new in System Manager Release 7.1.1

The following table lists enhancements in this release.

Enhancement	Description
KVM/Open stack Support	System Manager 7.1 is now available as OVA for Kernel-Based Virtual Machine (KVM) Hypervisors – for example, Red Hat Enterprise Linux 7. Although this OVA is being released as V7.1 (in line with the release string for the VMware and AWS OVA’s), it should be upgraded to 7.1.1 by applying Feature Service Pack 7.1.1 as soon as possible after installation.
Enhanced Editor support for Hunt Group	From SMGR release 7.1.1 onwards Hunt Group provisioning is supported using Enhanced editor to achieve CM connection optimization
Emergency Call Sequence added in Session Manager User Provisioning Rule and Bulk Editor.	
Map VMware Platform Services Controller [PSC] with vCenter in SDM	To Support PSC server for Mapping vCenter in SDM

This Release Notes document provides information about new features, installation downloads, and the documentation of Avaya Aura® System Manager 7.1.2 on VMware and KVM. This document also contains information about known issues and the possible workarounds.

This document provides information about System Manager 7.1.2 Release deliverables which includes System Manager 7.1.2 VMware OVA and KVM 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 Release 7.1.x.x

Enhancements delivered to System Manager Release 7.1.3.8

Enhancement	Keywords
N/A	N/A

Enhancements delivered to System Manager Release 7.1.3.7

Enhancement	Keywords
N/A	N/A

Enhancements delivered to System Manager Release 7.1.3.6

Enhancement	Keywords
N/A	N/A

Enhancements delivered to System Manager Release 7.1.3.5

Enhancement	Keywords
N/A	N/A

Enhancements delivered to System Manager Release 7.1.3.4

Enhancement	Keywords
N/A	N/A

Enhancements delivered to System Manager Release 7.1.3.3

Enhancement	Keywords
N/A	N/A

Enhancements delivered to System Manager Release 7.1.3.2

Enhancement	Keywords
N/A	N/A

Enhancements delivered to System Manager Release 7.1.3.1

Enhancement	Keywords
N/A	N/A

Enhancements delivered to System Manager Release 7.1.3

Enhancement	Keywords
• Virtual Machine Application Reports • Support for listing/deletion of VM snapshots on AVP hosts	SDM
• Updated to OpenJDK 1.8.0 Update 161 • VMware ESXi Versions 5.5, 6.0, 6.5 and 6.7. • AVP 7.1.3 • Enabling Customer customization for Security Profiles	Infrastructure and Serviceability Updates
• Added feature for Bulk Import/Export using Excel datasheets for Endpoints, Coverage Paths and Hunt Groups • Support for administration of alphanumeric handles for Aura users to support SIP URI based addressing and dialing • Support for administration of SIP Attendant Console	Communication Manager Management

Enhancements delivered to System Manager Release 7.1.2

Enhancement	Keywords
• Improvements to Update/Upgrade Management for AVP • Support for AVP License enforcement • AVP Remote Deployment for S8300 D/E LSP migrations (CM R5.2.1 & R6.x to CM R7.1.2) • Bulk Provisioning File (Excel) support to import configuration parameters for bulk upgrade/migration (AVP and CM parameters) • AVP upgrades integrated into SDM functions like Software Library, Analyze, Preupgrade checks, Logging	SDM
• Support for EASG for Web login • Updated to OpenJDK 1.8.0 Update 131	Infrastructure and Serviceability Updates
• Added feature to export the “delta” of users (“Added/Updated/Deleted”) for a specified period of time • Improvement in time required to export users.	UPM
• Enhanced Editor support for Trunk Group • Added feature for Bulk Import/Export using Excel datasheets for Vector Directory Number	Communication Manager Management

Enhancements delivered to System Manager Release 7.1.1.1

Enhancement	Keywords
N/A	

Enhancements delivered to System Manager Release 7.1.1

Enhancement	Keywords
KVM/Open stack Support	Platform
Enhanced Editor support for Hunt Group	CM EM
Emergency Call Sequence added in Session Manager User Provisioning Rule and Bulk	UPM

Enhancement	Keywords
Editor.	
Map VMware Platform Services Controller [PSC] with vCenter in SDM	SDM

Enhancements delivered to System Manager Release 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 • 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 • From System Manager Release 7.1, the root user account is disabled. • From System Manager release 7.1 "admin" user is no longer available on the command line • You must log in with the administrator privilege account that you create during deployment or upgrade of System Manager. You can use the same account for performing various operations like restarting service, reboot, shutdown etc. on System Manager. Refer section “System Manager command line interface operations” in Admin guide for various commands to perform operations on System Manager. • The System Manager system that has security hardening enabled, displays the login warning banner message. • Security profiles to enable hardened security modes refer admin guide for more details: - Standard Grade Hardening - Commercial Grade Hardening - Military Grade Hardening	Infrastructure and Serviceability Updates
• Support for Session Properties and Inactive Account Deactivation Policy. Refer admin guide for more details. • Administrators must change their System Manger Web Console Password post upgrade to 7.1 Release since the passwords are getting re-hashed using more secure sha2 based algorithms.	Authentication
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	User Management

Enhancement	Keywords
• 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. • When synchronized with Enterprise Directory, the roles, rights, and restrictions for administrators are automatically configured for the correct role and inherit the capability of roles. Refer admin guide for more details. You can map the userRoles attribute to one of the following: • Groups in LDAP. For example, in Active Directory, the attribute memberOf contains the fully qualified group name, such as CN=DnsAdmin,CN=Users,DC=avaya,DC=com. The system searches for DnsAdmin role name. • Other LDAP attribute: System searches for the exact name with the value in LDAP attribute that matches with the role in System Manager.	
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) • 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 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.	Solution Deployment Manager Client

Enhancement	Keywords
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. • Generate the license file by using the host ID of Primary System Manager which has the “Geo Redundancy” feature present in it and install the same on Primary System Manger prior to Geographic Redundancy Configuration. Configuring / Enabling geo redundancy feature will fail if you do not have the “Geo Redundancy” feature in the System Manager License file.	Geographic Redundancy
Included New Command Line Interface based user creation during System Manager Deployment	New Customer CLI Login
• For generating the new license file, the value of System Manager Host ID is now 14 characters. • Licenses installed on System Manager 7.0.x release for Avaya elements with 12 digits Host ID will work post upgrade of System Manager 7.0.x to 7.1, if upgrade is done using Solution Deployment Manager Client. • System Manager now requires a license. After installing System Manager 7.1 note down the 14-digit host ID and generate a license file for System Manager and install it. If you plan on using Geo redundancy feature, make sure the license file has the Geo Redundancy feature in it. If a System Manager License file is not installed, then a “System Manager Licenser Error” pop-up will be displayed every time you login to the System Manager Web interface. • On Fresh install of System Manager Port 52233 will be secured using System Manager CA signed certificates. Upgraded system will retain the default Sip CA certificates for backward compatibility. If admin need to revert to the default SIP CA certificates on port 52233 on a fresh install of System Manager, use the command “toggleWeblmOldcert” for the same. Refer the admin guide for details.	License Management

Fixes in System Manager Release 7.1.x.x

Fixes in System Manager 7.1.3.8

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-58745	Security Updates	(RHSA-2020:4041) Moderate: openldap security update	
SMGR-58769	Security Updates	(RHSA-2020:3911) Moderate: python security update	
SMGR-58771	Security Updates	(RHSA-2020:3908) Moderate: cpio security update	
SMGR-58731	Security Updates	(RHSA-2020:4908) Important: libX11 security update	
SMGR-58755	Security Updates	(RHSA-2020:4005) Moderate: libxslt security update	
SMGR-58727	Security Updates	(RHSA-2020:5009) Moderate: python security update	
SMGR-58737	Security Updates	(RHSA-2020:4276) Important: kernel security update	
SMGR-58773	Security Updates	(RHSA-2020:3901) Low: libpng security update	
SMGR-58781	Security Updates	(RHSA-2020:3848) Low: libmspack security update	
SMGR-58717	Security Updates	(RHSA-2020:5566) Important: openssl security update	
SMGR-58741	Security Updates	(RHSA-2020:4072) Moderate: libcroco security update	
SMGR-58733	Security Updates	(RHSA-2020:4907) Important: freetype security update	
SMGR-58729	Security Updates	(RHSA-2020:5002) Moderate: curl security update	
SMGR-58763	Security Updates	(RHSA-2020:3952) Moderate: expat security update	
SMGR-58765	Security Updates	(RHSA-2020:3916) Moderate: curl security update	
SMGR-58747	Security Updates	(RHSA-2020:4032) Moderate: dbus security update	
SMGR-58767	Security Updates	(RHSA-2020:3915) Moderate: libssh2 security update	
SMGR-58735	Security Updates	(RHSA-2020:4350) Moderate: java-1.8.0-openjdk security and bug fix update	
SMGR-58725	Security Updates	(RHSA-2020:5011) Moderate: bind security and bug fix update	
SMGR-58757	Security Updates	(RHSA-2020:4003) Moderate: NetworkManager security and bug fix update	
SMGR-58759	Security Updates	(RHSA-2020:3996) Moderate: libxml2 security and bug fix update	
SMGR-58739	Security Updates	(RHSA-2020:4076) Moderate: nss and nspr security, bug fix, and enhancement update	
SMGR-58743	Security Updates	(RHSA-2020:4060) Important: kernel security, bug fix, and enhancement update	
SMGR-58721	Security Updates	(RHSA-2020:5083) Moderate: microcode_ctl security, bug fix, and enhancement update	
SMGR-58775	Security Updates	(RHSA-2020:3878) Low: dnsmasq security and bug fix update	
SMGR-58753	Security Updates	(RHSA-2020:4007) Low: systemd security and bug fix update	
SMGR-58761	Security Updates	(RHSA-2020:3978) Moderate: glib2 and ibus security and bug fix update	
SMGR-58749	Security Updates	(RHSA-2020:4026) Moderate: mariadb security and bug fix update	

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-58779	Security Updates	(RHSA-2020:3861) Low: glibc security, bug fix, and enhancement update	
SMGR-58777	Security Updates	(RHSA-2020:3864) Moderate: cups security and bug fix update	
SMGR-58751	Security Updates	(RHSA-2020:4011) Moderate: e2fsprogs security and bug fix update	
SMGR-58723	Security Updates	(RHSA-2020:4011) Moderate: e2fsprogs security and bug fix update	
SMGR-58719	Security Updates	(RHSA-2020:5437) Important: kernel security and bug fix update	
SMGR-58385	User Management	Preferred handle doesn't get updated if user has two sip handles and administrator try to update it with second one.	
SMGR-55372	Communication Manager Management	AD sync to remove user fails because the station is part of hunt group on tenant management enabled system.	
SMGR-57981	Communication Manager Management	INIT sync resets "Dual Registration" and "Calculate Route Pattern" fields on CM communication profile.	
SMGR-58354	Communication Manager Management	When user tries to associate existing H323 station with existing user on System Manager and enables dual registration, System Manager tries to add incorrect station number to the off-pbx station-mapping form.	
SMGR-58285	Communication Manager Management	Importing multiple Service Hours Table into System Manager does not populate Start/End Time for week.	
SMGR-57999	Communication Manager Management	Same CM extension can be assigned to multiple users through AD sync.	
SMGR-57953	Communication Manager Management	List registered station report in System Manager does not show all endpoints that are registered.	
SMGR-58194	Software Deployment Manager	SDM iso file space is not freed after it was deleted.	

Fixes in System Manager 7.1.3.7

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-57187	Security Updates	ksh (RHSA-2020:0568) (tcp)	N/A
SMGR-54966	Security Updates	(RHSA-2020:1020) Low: curl security and bug fix update	N/A
SMGR-54914	Security Updates	(RHSA-2020:1113) Moderate: bash security update	N/A
SMGR-57366	Security Updates	(RHSA-2020:2663) Moderate: ntp security update	N/A
SMGR-57364	Security Updates	(RHSA-2020:2894) Important: dbus security update	N/A
SMGR-54986	Security Updates	(RHSA-2020:1138) Low: gettext security and bug fix update	N/A

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-54990	Security Updates	(RHSA-2020:1000) Moderate: rsyslog security, bug fix, and enhancement update	N/A
SMGR-54926	Security Updates	(RHSA-2020:1176) Low: avahi security update	N/A
SMGR-57378	Security Updates	(RHSA-2020:3217) Moderate: grub2 security and bug fix update	N/A
SMGR-54978	Security Updates	(RHSA-2020:1135) Low: polkit security and bug fix update	N/A
SMGR-57374	Security Updates	(RHSA-2020:2968) Important: java-1.8.0-openjdk security update	N/A
SMGR-55448	Security Updates	(RHSA-2020:2082) Important: kernel security and bug fix update	N/A
SMGR-54958	Security Updates	(RHSA-2020:1047) Moderate: wireshark security and bug fix update	N/A
SMGR-54918	Security Updates	(RHSA-2020:1512) Important: java-1.8.0-openjdk security update	N/A
SMGR-54982	Security Updates	(RHSA-2020:1061) Moderate: bind security and bug fix update	N/A
SMGR-54922	Security Updates	(RHSA-2020:1022) Low: file security update	N/A
SMGR-54970	Security Updates	(RHSA-2020:1080) Moderate: evolution security and bug fix update	N/A
SMGR-54974	Security Updates	(RHSA-2020:1050) Moderate: cups security and bug fix update	N/A
SMGR-54910	Security Updates	(RHSA-2020:1011) Moderate: expat security update	N/A
SMGR-57370	Security Updates	(RHSA-2020:3220) Important: kernel security and bug fix update	N/A
SMGR-57360	Security Updates	(RHSA-2020:2432) Moderate: microcode_ctl security, bug fix and enhancement update	N/A
SMGR-57356	Security Updates	(RHSA-2020:2664) Important: kernel security and bug fix update	N/A
SMGR-54934	Security Updates	(RHSA-2020:1016) Moderate: kernel security, bu	N/A
SMGR-54950	Security Updates	(RHSA-2020:1021) Moderate: GNOME security, bug fix, and enhancement update	N/A
SMGR-54896	Security Updates	(RHSA-2020:1131) Moderate: python security update	N/A
SMGR-54946	Security Updates	(RHSA-2020:1100) Moderate: mariadb security and bug fix update	N/A
SMGR-54942	Security Updates	(RHSA-2020:0897) Important: icu security update	N/A
SMGR-54900	Security Updates	(RHSA-2020:1181) Low: unzip security update	N/A
SMGR-57387	Security Updates	(RHSA-2020:2344) Important: bind security update	N/A
SMGR-54545	Infrastructure Management	ON SMGR Local FTP Server cannot be enabled which is required for media module upgrade using SDM.	
SMGR-55642	Infrastructure Management	Postgresql Time Based SQL Injection Security fixes.	

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-54619	User Management	User updates fails with error STACOMMPROFILE0009.	
SMGR-54448 SMGR-49268 SMGR-54566	User Management	Issues with user create/update when user first, last and login name contains special characters and administrator does not receive proper error message on failure.	
SMGR-55543	User Management	Issues with Duplicate user operation.	
SMGR-53888	User Management	Export failures logs show wrong failures	
SMGR-57434	User Management	Unable to create new users through WebService API after upgrade to 7.1.3.6.	
SMGR-54446	Software Upgrade Management	Empty parent field for Media Modules due to failed extension pack.	
SMGR-48963	Software Upgrade Management	Not able downloaded files from PLDS if Authentication base proxy server is used under user setting.	
SMGR-54453	Licensing Management	Remove AJP port 8009 from configurations.	
SMGR-57778	Licensing Management	Vulnerability within the Avaya Web License Manager (WebLM) allows an authenticated user to read arbitrary files.	
SMGR-56325	Communication Manager Management	Endpoints with blank Location field cannot be searched through Advanced search option on Manage endpoint page.	
SMGR-55938	Communication Manager Management	All locations in NRP of System Manager Routing > Locations screen shows all locations are shared bandwidth control, but all locations when viewed in NRP show an error.	
SMGR-52636	Communication Manager Management	Custom user can view/edit/delete CM data like endpoints, VDN from different CM for which custom user does not have permissions.	
SMGR-54732	Communication Manager Management	When user tries to associate existing H323 station with existing user on SMGR and enables dual registration, SMGR tries to add incorrect station number to the off-pbx station-mapping form.	
SMGR-55152	Communication Manager Management	Inventory -> Synchronization page : Scheduling INIT sync weekly for Saturday fails.	
SMGR-55155	Communication Manager Management	Import an endpoint with name change then user gets error as “Duplicate Button 17 error”.	
SMGR-55439	Communication Manager Management	Incremental sync fails after duplicate station	
SMGR-55435	Communication Manager Management	Blank agent name when tilde(~) is used in "Endpoint Display Name" while configuring user.	
SMGR-56659	Communication Manager Management	Bulk endpoint export failing for combined Communication Managers.	
SMGR-56841	Infrastructure Management	privilege escalation possible for script sudocommonscript.bin.	

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-56299	Infrastructure Management	Sensitive files can be viewed by using Software upgrade management scripts for CLI Cust users.	
SMGR-55256	Trust Management	System Manager stops working properly if default tls outbound truststore contains more than 250 trusted CA certificates in it.	
SMGR-55125	Global Search Component	Global search shows less results than filtered table search	

Fixes in System Manager 7.1.3.6

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-53854	Security Updates	ksh (RHSA-2020:0568)	N/A
SMGR-51750	Security Updates	(RHSA-2019:4326) Important: fribidi security update	N/A
SMGR-50879	Security Updates	(RHSA-2019:3872) Important: kernel security update	N/A
SMGR-53775	Security Updates	(RHSA-2020:0630) Important: ppp security update	N/A
SMGR-51339	Security Updates	(RHSA-2019:3976) Low: tcpdump security update	N/A
SMGR-50859	Security Updates	(RHSA-2019:3834) Important: kernel security update	N/A
SMGR-51283	Security Updates	(RHSA-2019:3979) Important: kernel security and bug fix update	N/A
SMGR-53774	Security Updates	(RHSA-2020:0374) Important: kernel security and bug fix update	N/A
SMGR-53773	Security Updates	(RHSA-2020:0196) Important: java-1.8.0-openjdk security update	N/A
SMGR-53772	Security Updates	(RHSA-2020:0227) Important: sqlite security update	N/A
SMGR-53771	Security Updates	(RHSA-2020:0540) Important: sudo security update	N/A
SMGR-51333	Security Updates	(RHSA-2019:4190) Important: nss, nss-softokn, nss-util security update	N/A
SMGR-53846	Security Updates	ruby (RHSA-2020:0663)	N/A
SMGR-50097	Bulk Import and Export Management	Failures are marked on "Export All Users" without logging with reason and user(s) details.	
SMGR-53410	Communication Manager Management	Agent Editor does not open from user management page.	
SMGR-53793 SMGR-50525	Communication Manager Management	Failure in commit activity when uncheck "Allow H.323 and SIP Endpoint Dual Registration" for a user with EC500.	
SMGR-52334	Communication Manager Management	Holiday table import and export issues	
SMGR-51993	Communication Manager Management	Memory leak observed when reports are executed to get data from Communication Manager	

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-52898	Communication Manager Management	"Security Code:" field is not getting updated for import operation from Manage endpoint page.	
SMGR-52891	Communication Manager Management	"SIP Trunk" field doesn't accept value in range rp6xx for SIP endpoint templates.	
SMGR-52892	Communication Manager Management	Hunt group cannot be exported if hunt group members are not added in sequence.	
SMGR-51312	Communication Manager Management	Export user fails if speakerphone field is set as "grp-listen".	
SMGR-50647	Communication Manager Management	Thread leak in component managing Communication Manager.	
SMGR-46856	Communication Manager Management	Missing data module feature when custom template is chosen via User Management.	
SMGR-53104	Communication Manager Management	Add "MWI Served User Type" to template for agents.	
SMGR-49316	Global Search Component	Global search feature does not show group membership data.	
SMGR-50626	Inventory Management	Display issues with Inventory -> Manage elements page	
SMGR-50116	Infrastructure	IPFQDN change corrupts network files causing database startup issue.	
SMGR-50992	Infrastructure	Sensitive files can be viewed by command line interface custom accounts using Software upgrade components.	
SMGR-50884	Infrastructure	/var/log/Avaya/systemmonitor_service_affects.log and spiritagent_service_affects.log files are not rotating and filling up disk space.	
SMGR-50242	Infrastructure	Disk Space usage alarm(s) missing for System Manager disk partitions.	
SMGR-53299	Software Upgrade Management	Upgrade resume failure for Session Manager via SDM embedded in System Manager.	
SMGR-50700	Software Upgrade Management	After re-establish connection or VM refresh from VM manager page for Communication Manager ,Current version is not proper in upgrade management page.	
SMGR-48454	Software Upgrade Management	System Manager Local FTP Server cannot be enabled which is required for media module upgrade using Software Upgrade Management.	
SMGR-48287	Software Upgrade Management	Migrating from CM 6.3.x on VSP to CM 7.1 on AVP does not work if remote software library used to provide the AVP ISO file.	
SMGR-53550	Software Upgrade Management	Issues noticed while performing upgrade of two Utility Servers on different AVP hosts at the same time from System Manager.	
SMGR-47752	SDM Client	AVP Patch from 7.1.3 to 7.1.3.2 failure through SDM client.	

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-49620	Role Management	Unable to parse comma (“ , “) in role description field, while creating new or updating existing role.	
SMSG-1173 SMSG-153 SMSG-1331	Messaging Server Management	Messaging Element Manager fixes.	

Fixes in System Manager 7.1.3.5

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-50876	Security Updates	kernel (RHSA-2019:3872)	N/A
SMGR-50587	Security Updates	java-1.8.0-openjdk (RHSA-2019:1815)	N/A
SMGR-50586	Security Updates	python-urllib3 (RHSA-2019:2272)	N/A
SMGR-50596	Security Updates	vim (RHSA-2019:1619	N/A
SMGR-50584	Security Updates	dhcp (RHSA-2019:2060)	N/A
SMGR-50597	Security Updates	openssl (RHSA-2019:2304)	N/A
SMGR-50585	Security Updates	glibc (RHSA-2019:2118)	N/A
SMGR-50589	Security Updates	curl (RHSA-2019:2181)	N/A
SMGR-50595	Security Updates	polkit (RHSA-2019:2046)	N/A
SMGR-50594	Security Updates	python-requests (RHSA-2019:2035)	N/A
SMGR-50603	Security Updates	kernel (RHSA-2018:2748)	N/A
SMGR-50598	Security Updates	nss, nss-softokn, nss-util, and nspr (RHSA-2019:2237)	N/A
SMGR-50592	Security Updates	bind (RHSA-2019:2057) (tcp)	N/A
SMGR-50590	Security Updates	ntp (RHSA-2019:2077)	N/A
SMGR-50591	Security Updates	mariadb (RHSA-2019:2327)	N/A
SMGR-50602	Security Updates	libssh2 (RHSA-2019:2136)	N/A
SMGR-50593	Security Updates	unzip (RHSA-2019:2159)	N/A
SMGR-50599	Security Updates	ruby (RHSA-2019:2028)	N/A
SMGR-50600	Security Updates	python (RHSA-2019:2030)	N/A
SMGR-50601	Security Updates	binutils (RHSA-2019:2075)	N/A
SMGR-50605	Security Updates	openssh (RHSA-2019:2143)	N/A
SMGR-50604	Security Updates	kernel (RHSA-2019:2829)	N/A
SMGR-50609	Security Updates	elfutils (RHSA-2019:2197)	N/A
SMGR-50608	Security Updates	libmspack (RHSA-2019:2049)	N/A
SMGR-50610	Security Updates	procps-ng (RHSA-2019:2189)	N/A
SMGR-50611	Security Updates	systemd (RHSA-2019:2091)	N/A
SMGR-50614	Security Updates	sssd (RHSA-2019:2177)	N/A
SMGR-50606	Security Updates	libcgroup (RHSA-2019:2047)	N/A

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-50613	Security Updates	Xorg (RHSA-2019:2079)	N/A
SMGR-50607	Security Updates	libjpeg-turbo (RHSA-2019:2052)	N/A
SMGR-50612	Security Updates	pango (RHSA-2019:2571)	N/A
SMGR-50378	Security Updates	(RHSA-2019:2053) Moderate: libtiff security update	N/A
SMGR-49659	Infrastructure	HTTP Thread Usage Monitor is not calculating the http thread percentage properly causing unnecessary Major/Minor Alarms on System Manager	
SMGR-49792	Infrastructure	System Manager is returning unacceptable data in the XML when we do a GET User through the API.	
SMGR-50714	Infrastructure	Non admin users having read/write access to the files in SearchConfig and REPORTS directory	
SMGR-48645	Infrastructure	Audit.log file does not get auto rotate if System Manager deployed in Military mode	
SMGR-50143	Infrastructure	System Manager stops working properly if default outbound truststore contains more than 250 trusted CA certs in it.	
SMGR-50348	Infrastructure	Some of the Session Manager Element Manager file permissions had write permissions for non-admins users.	
SMGR-50660 SMGR-45610	Infrastructure	On System manager where Non admin users having read/write access to the files.	
SMGR-49861	Infrastructure	/var/log/Avaya/postgres/postgres.log file not rotating and filling up disk space.	
SMGR-50007	Infrastructure	No cron job to cleanup DRS dump files from $AVAYA_LOG/drs/errordump directory.	
SMGR-47841	Infrastructure	Provide proper Audit logs for Security Configuration changes done from System Manager Web console.	
SMGR-49724	Role Management	Custom user sees Blank pages when clicks on session manager dashboard or user registrations page if role permission mappings for Session Manager are created under group.	
SMGR-50203	Role Management	If a user's id/full name or role name/description has a space at the beginning or at the end, then if you try to create/edit such a user/role the operation will fail with error "Invalid request received. Please contact your system administrator"	
SMGR-50821	User Management	Allow duplicate operation on user for logged in user having role permissions to manage users under group.	
SMGR-50809	User Management	Directory Sync fails where UPR has mapped officelinx mailbox field with active directory attribute like ipPhone.	
SMGR-50983	Alarming	Secondary server logs being sent to primary server once secondary server activated instead of secondary server.	

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-49245	Global Search Management	Group membership data is not populated properly in Global search if multiple endpoints are viewed/edited one after another.	
SMGR-49967	Geo Redundancy Management	GEO configuration fails due to database configuration files corruption in case of space usage issue associated with swlibrary partition.	
SMGR-50152	Communication Manager Management	list usage service-hours-table option is not available.	
SMGR-49677	Communication Manager Management	Less than sign is not displayed in Element Cut-through pages.	
SMGR-49661	Communication Manager Management	Display issue on Service Hours Tables on System Manager 7.1.3.4.	
SMGR-49156	Communication Manager Management	Cannot add more ip-network-map entries if ip-network-map already has >=500 entries.	
SMGR-47952	Communication Manager Management	Export All Endpoints causes system to go out of memory.	
SMGR-49709	Communication Manager Management	Duplicate station entries when paging on Manage Endpoints.	
SMGR-47156	Communication Manager Management	Delete station job gets stuck in running mode.	
SMGR-50866	Communication Manager Management	Unable to remove users that are added to many hunt groups.	
SMGR-50902	Communication Manager Management	Thread leak caused by Communication Manager Management component.	
SMGR-49027	Communication Manager Management	When adding user with WCBRI station, clicking on Commit gives error Data Extension is Mandatory.	
SMGR-49788	Communication Manager Management	"Identity for Calling Party Display" value on Communication Manager SIP trunk form is not saved properly in System Manager.	
SMGR-49994	Communication Manager Management	Notify sync may not work due to firewall reject rule associated with 9000 port in System Manager 7.1.3.4 release.	
SMGR-47777	Communication Manager Management	EndpointDisplayName missing ASCII validation.	
SMGR-48555	Communication Manager Management	In Exported list of user’s ‘Attendant’ header missing in CM Endpoint Profile.	
SMGR-49863	Report Management	Graph is not showing proper percentage.	
SMGR-50169 SMGR-50321	Report Management	System Manager generated reports have data missing in headers.	
SMGR-49368	Report Management	Reports for commands (list route-pattern, list audio-group, list configuration firmware-versions, list configuration media-gateway, list ip-codec-set) are failed to generate.	

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-50223	Software Upgrade Management	Refresh Families and Analyze operation fails due to change in PLDS certificate	
SMGR-49847	Software Upgrade Management	Gateway discovery does not work with SNMPv3.	
SMGR -50250	Software Upgrade Management	Migrating from CM 6.3.x on VSP to CM 7.1 on AVP does not work if remote software library used to provide the AVP ISO file	
SMGR-48408	Software Upgrade Management	For G450 MG, MP160 board subtype shows as 'other'	
SMGR-49315	Software Upgrade Management	File upload to external FTP server using alternate source or /swlibrary/staging/sync does not work.	
SMGR-48743	Software Upgrade Management	Avaya Aura messaging element should not get added to System Manager inventory through SDM after trust re-establishment.	
SMGR-49868	Software Upgrade Management	Not able download files from plds if Authentication base proxy server is used under user setting.	
SMGR-50128	Software Upgrade Management	Refresh Element shows successful even when it failed.	

Fixes in System Manager 7.1.3.4

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-48473	Security Updates	(RHSA-2019:0194) bind security update	N/A
SMGR-48470	Security Updates	(RHSA-2019:0230) polkit security update	N/A
SMGR-49274	Security Updates	(RHSA-2019:0775) Important: java-1.8.0-openjdk security update	N/A
SMGR-48464	Security Updates	(RHSA-2019:0109) perl security update	N/A
SMGR-49294	Security Updates	(RHSA-2019:1235) Important: ruby security update	N/A
SMGR-49286	Security Updates	(RHSA-2019:1228) Important: wget security update	N/A
SMGR-48528	Security Updates	(RHSA-2019:0435) Moderate: java-1.8.0-openjdk security update	N/A
SMGR-48593	Security Updates	(RHSA-2019:0710) Important: python security update	N/A
SMGR-48521	Security Updates	[RHSA-2019:0483) Moderate: openssl security and bug fix update	N/A
SMGR-48478	Security Updates	(RHSA-2019:0679) Important: libssh2 security update	N/A
SMGR-48514	Security Updates	(RHSA-2019:2019:0512) Important: kernel security, bug fix, and enhancement update	N/A
SMGR-49309	Security Updates	(RHSA-2019:1481) Important: kernel security update	N/A
SMGR-49300	Security Updates	(RHSA-2019:1168) Important: kernel security update	N/A

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-48468	Security Updates	(RHSA-2019:0163) kernel security, bug fix, and enhancement update	N/A
SMGR-48508	Security Updates	(RHSA-2019:0368) Important: systemd security update	N/A
SMGR-48504	Security Updates	(RHSA-2019-0201) systemd security update	N/A
SMGR-48462	Security Updates	(RHSA-2019:0049) systemd security update	N/A
SMGR-47572	Infrastructure	full-vacuum-reindex-cron-job.sh cron job is running but not performing vacuum on database.	7.1.x
SMGR-48330	Infrastructure	Unable to deploy change VFQDN if vFQDN provided value has "-U" in it.	N/A
SMGR-48302	Infrastructure	Firewall Changes to support ED application.	N/A
SMGR-49021	Infrastructure	Full path disclosure vulnerability associated with search config component.	N/A
SMGR-48663	Infrastructure	Thread leak in Trust Management Component causing System Manager Crash.	7.1.x
SMGR-47841	Infrastructure	Provide proper Audit logs for Security Configuration changes.	7.1.x
SMGR-39711	Backup and Restore Management	After Restore earlier scheduled backup job is getting disabled.	7.0.x
SMGR-46591	Alarming Management	Cannot assign target profile to a Serviceability Agent while the target profile already has a notification profile linked.	7.1.2.0
SMGR-44450	Geographic Redundancy Management	GEO reconfiguration fails during Clean Up phase if Discovery Profile has entries associated with System Manager Element Type.	7.1.x
SMGR-46939	Geographic Redundancy Management	GEO configuration fails in rare scenario and secondary system goes into bad state.	7.1.x
SMGR-44755	Geographic Redundancy Management	GEO- Redundancy Enable Replication resulted in full /var on both primary and secondary.	7.1.x
SMGR-47633	Geographic Redundancy Management	Provide log rotation for log file /var/log/Avaya/mgmt/geo/csync2.log	7.1.x
SMGR-47592	Geographic Redundancy Management	Unable to configure Geo when the 3rd party CA cert that customer is using does not have a CN value in it.	7.1.x
SMGR-43554	Inventory Management	Unable to delete messaging element entry from manage elements page.	7.0.x
SMGR-48161	Inventory Management	When a CM is deleted from System Manager UI, it does not log IP address of machine from where System Manager UI is accessed.	7.1.x
SMGR-48347	WebService Management	UPM Error code issue when webservice is used for user creation which is not administered in CM dial plan	7.1.3.1

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-49459	User Management	While create/edit of user or role gets error "Invalid request received. Please contact your system administrator" if a field value has space at beginning or end.	7.1.x
SMGR-48316	User Management	Communication Address/SIP handle should not be case sensitive.	7.1.x
SMGR-48198	Self Provisioning	Self provisioning login should not be to be case sensitive.	7.1.x
SMGR-48138	Self Provisioning	Self provisioning to reset password sometime add space (" ") in automatically generated password.	7.1.x
SMGR-48604	User Provisioning Rule	User cannot edit Messaging profile when editing a User Provisioning Rule from View User Provisioning Rule page.	7.1.x
SMGR-46344	Communication Manager Management	Configuring CM with notify sync from System Manager deployed in Geographic Redundancy can stop syslog service on Communication Manager from working.	7.0.x
SMGR-48053	Communication Manager Management	"Global Endpoint Change" deletes station Name when "Endpoint Display Name:" contains "~" character.	7.1.3.1
SMGR-48044	CommuUser (on Manager Management	User (any user other than super user) cannot delete announcement backup manually from CLI.	7.1.x
SMGR-48034	Communication Manager Management	list extension-type report puts COR and COS field values in wrong place.	7.1.1.1
SMGR-48421	Communication Manager Management	Few specific feature-access-codes are not listed in the System Manager	7.1.x
SMGR-48434	Communication Manager Management	Edit VDN operation fails for custom user (having permission with extension range) if VOA extension contains "-" and "."	7.1.x
SMGR-48725	Communication Manager Management	Vector Directory Number page needs to have correct label for table column "IPTCM_VDN_Destination_Number"	7.1.3.x
SMGR-48677	Communication Manager Management	Station delete fails with foreign key constraint error for table on table "ipt_abbrdial_pers"	7.1.3.1
SMGR-47813	Communication Manager Management	Multiple issues when "data module" is enabled on WCBRI station.	7.1.3.1
SMGR-49052	Communication Manager Management	Downloading the Excel template from the manage endpoints page and using it to delete stations does not work.	7.1.3.1
SMGR-47823	Communication Manager Management	Option to set setType to "ALIAS Set Type" ends in error (Not able to read station template from DB)	7.1.3.1
SMGR-47955	Communication Manager Management	Same extension gets assigned to multiple users	7.1.3.2
SMGR-48320	Communication Manager Management	Usage of cssecurestore filling up the cssecurestore table to the extent that it causes Geo Redundancy workflow to fail.	7.1.3.2

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-47849	Report Management	"list monitored-station" report generation is failing	7.1.x
SMGR-48489	Report Management	Custom user cannot generate report when he has multiple ranges defined under endpoint, VDN, Vector etc.	7.1.3.3
SMGR-48540	Report Management	Setdata report taken in SMGR has incorrect column alignments.	7.1.3.0
SMGR-48417	Report Management	"Creation Time" does not show date and time in AM/PM in report generation and history pages.	7.1.x
SMGR-48535	Report Management	Display vector report generation fails for PDF format.	7.1.x
SMGR-48438	Report Management	list registered-ip-stations report shows displays incorrect data under columns.	7.1.x
SMGR-48623	Report Management	Report generation in pdf format fails for forms containing "&".	7.1.x
SMGR-48545	Report Management	When multiple reports are run concurrently, some of the runs produce zero size (empty) reports.	7.1.x
SMGR-48329	Report Management	Incorrect report is generated when pagination/order settings are changed.	7.1.x
SMGR-49112	Report Management	Report generation fails for custom role when report (such as display/status) which requires Qualifier Value.	7.1.x
SMGR-49134	Report Management	“list registered-ip-stations” and “list usage hunt-group” created by custom account does not populate data.	7.1.x
SMGR-46784	SDM Client	Trust establishment fails from SDM client for Military mode enabled on System Manager.	7.1.3.2
SMGR-48068	SDM Client	Unable to use SDM Client for upgrading vCenter based System Manager.	7.1.3.2
SMGR-48425	Software Upgrade Management	After clicking "Migrate with AVP install" checkbox new tab is not displayed while migrating from SP to AVP	N/A
SMGR-48862	Software Upgrade Management	AVP custom patches should not be displayed in download management as its not supported.	7.1.3.1
SMGR-47708	Software Upgrade Management	If Upgrade management jobs like analyze, pre-upgrade check are deleted from scheduler page, it does not clean the respective entries from SDM pages.	7.1.3.0
SMGR-47975	Software Upgrade Management	While updating Session Manager 7.1.3.1 to 7.1.3.2, Update configuration page does not show service pack 7.1.3.2 if Session Manager 8.0 OVA is downloaded in software library.	7.1.3.2
SMGR-48049	Software Upgrade Management	Refresh Families and analyze fails as invalid company ID for freshly deployed System Manager 7.1.3.3 release	7.1.3.3
SMGR-48147	VM Management	Refresh Host gets stuck after changing host password through SDM.	7.1.3.2

Fixes in System Manager 7.1.3.3

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-47762	Security Updates	java-1.8.0-openjdk (RHSA-2018:2942)	N/A
SMGR-47235 SMGR-47764	Security Updates	(RHSA-2018:3050) Moderate: gnutls security, bug fix, and enhancement update	N/A
SMGR-46921 SMGR-47753	Security Updates	(RHSA-2018:2768) Moderate: nss security update	N/A
SMGR-47319 SMGR-47760	Security Updates	(RHSA-2018:3249) Low: setup security and bug fix update	N/A
SMGR-47232 SMGR-47754	Security Updates	(RHSA-2018:3032) Low: binutils security, bug fix, and enhancement update	N/A
SMGR-47236 SMGR-47767	Security Updates	(RHSA-2018:3041) Moderate: python security and bug fix update	N/A
SMGR-47402 SMGR-47757	Security Updates	(RHSA-2018:3221) Moderate: openssl security, bug fix, and enhancement update	N/A
SMGR-47273 SMGR-47759	Security Updates	(RHSA-2018:3157) Moderate: curl and nss-pem security and bug fix update	N/A
SMGR-47240 SMGR-47772	Security Updates	(RHSA-2018:3107) Moderate: wpa_supplicant security and bug fix update	N/A
SMGR-47413 SMGR-47756	Security Updates	(RHSA-2018:3327) Low: libmspack security update	N/A
SMGR-46920 SMGR-47761	Security Updates	(RHSA-2018:2748) Important: kernel security and bug fix update	N/A
SMGR-47407 SMGR-47773	Security Updates	(RHSA-2018:3071) Low: krb5 security, bug fix, and enhancement update	N/A
SMGR-47428	Security Updates	(RHSA-2018:3083) Important: kernel security, bug fix, and enhancement update	N/A
SMGR-47420 SMGR-47763	Security Updates	(RHSA-2018:3059) Low: X.org X11 security, bug fix, and enhancement update	N/A
SMGR-47230	Security Updates	(RHSA-2018:2942) Critical: java-1.8.0-openjdk security update	N/A
SMGR-47233 SMGR-47758	Security Updates	(RHSA-2018:3052) Moderate: wget security and bug fix update	N/A
SMGR-47237 SMGR-47755	Security Updates	(RHSA-2018:3158) Low: sssd security, bug fix, and enhancement update	N/A
SMGR-47545 SMGR-47770	Security Updates	(RHSA-2018:3651) Moderate: kernel security, bug fix, and enhancement update	N/A
SMGR-47540 SMGR-47765	Security Updates	(RHSA-2018:3092) Moderate: glibc security, bug fix, and enhancement update	N/A

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-47771	Security Updates	Network Manager (RHSA-2018:3665) update	N/A
SMGR-47766	Security Updates	GNOME (RHSA-2018:3140) update	N/A
SMGR-47769	Security Updates	ruby (RHSA-2018:3738) update	N/A
SMGR-46729	Security	Cross site scripting vulnerability in System Manager	N/A
SMGR-45420	Web Service Management	umapi lookup with start Index and offset does not work as expected.	7.1
SMGR-46896	Web Service Management	Preferred Handle attribute to "None" when name changes for user is performed.	7.1
SMGR-34021	Export and Import Management	Unable to delete user export job from export list if it's already deleted from scheduler.	6.3.x
SMGR-46919	Log Viewer Management	Multiple logs generated with Event ID "IAMAT008E" when user other than default admin user view the log viewer page.	7.1
SMGR-41270	Alarming Management	System Manager do not validate Authentication Password while changing it from default under TrapListener Configuration Parameters page.	7.0.x
SMGR-46876	User Management	Exception: null is displayed during creation SMGR user with Messaging profile using UPR	7.1.3.0
SMGR-45884	Directory Synchronization Management	If the same attribute from AD is mapped to login name and other Email and value of the attribute is in mixed case or upper case, then after each sync user shows as modified.	7.1.2.0
SMGR-41634	Self Provisioning	Self provisioning does not work after providing windows user id if external authentication is configured.	7.1
SMGR-45076	Self Provisioning	User cannot change password for AAM 7.1 Messaging by self-provisioning.	7.1.2.0
SMGR-45095	Self Provisioning	System Manager does not validate AAM7.1 password rule from self provisioning.	7.1.2.0
SMGR-46344	Infrastructure	Notify Sync does not work in case of Geo Redundancy if both System Manager servers are configured on Communication Manager to receive notifications.	7.0.x
SMGR-43365	Infrastructure	"changeIPFQDN" does not work properly if executed with "SEARCH" and "DNS" options.	7.1
SMGR-47060	Infrastructure	/tmp folder does not have the sticky bit set.	7.1
SMGR-46812	Infrastructure	"changeIPFQDN" command execution corrupts the VFQDN entry in hosts file in some scenarios.	7.1
SMGR-46365	Infrastructure	System Manager deployed in security mode is not able to do "re-establish trust" with the servers deployed in the environment.	7.1.3.1
SMGR-45703	Infrastructure	"changeVFQDN" execution fails to update VFQDN in certain scenarios.	7.1.x
SMGR-46676	Infrastructure	Web console access EASG account enables FIPS mode at the JVM level which causes Pre-upgrade check in Software upgrade management to fail.	7.1

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-46640	Communication Manager Management	Addition of Extension to coverage answer-group failed with Cause: "Maximum no. of extensions for the group exceeded".	7.0.1.3
SMGR-46686	Communication Manager Management	Custom users cannot utilize the Import/Export feature on Hunt group form.	7.1.3
SMGR-46723	Communication Manager Management	Custom users cannot use the Import/Export feature on VDN form.	7.1.3
SMGR-44451	Communication Manager Management	Default template list is mismatching with selected CM version.	7.1
SMGR-47155	Communication Manager Management	After selecting VDN record buttons(view/edit/delete) are not getting enabled.	7.1.3.2
SMGR-46561	Communication Manager Management	Support of mailbox and virtual set type in the Element Cut-through.	N/A
SMGR-47490	Communication Manager Management	Announcement backup fails to get audio files when local scp server is set.	7.1.2.0
SMGR-46856	Communication Manager Management	Data module feature is missing when custom template is chosen via user management -> Communication Manager Profile.	7.1.3.0
SMGR-46782	Communication Manager Management	Failed to add hunt group, if user associated with custom role has all permissions and it has endpoint and hunt extension ranges defined.	7.1.3.0
SMGR-46515	Communication Manager Management	Backup All Announcement job shows success even though it is unable to download all announcement file.	7.0.1.3
SMGR-46930	Communication Manager Management	Extension lookup very slow on VND and hunt group pages causing system slowness.	7.1.3.0
SMGR-46502	Communication Manager Management	Stack Overflow Error when user provides Number Range for various attributes in a custom role.	7.1.0.0
SMGR-47312	Communication Manager Management	Delete station job gets stuck in running mode.	7.1.2.0
SMGR-47845	Communication Manager Management	Communication Manager IP gets interchanged on System Manager -> Communication Manager pages causing interchanged Communication Manager to disappear for logged in user having custom role mapped with Communication Manager active IP address.	7.1.3.2
SMGR-46875	Report Management	Issues with report definition for duplex Communication Manager when Communication Manager interchange happens.	7.1.3.1

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-46783	Report Management	"list measurements ip dsp-resource" report does not match column headings and values.	7.1.3.0
SMGR-47538	Report Management	Two report jobs for two different Communication Manage scheduled for same time, one completes successfully but other creates empty file.	7.1.3.0
SMGR-47175	Software Upgrade Management	System Platform Based LSP upgrade from 6.3.x to 7.1.x not working in System Manager 7.1.3.2.	7.1.3.2
SMGR-47515	Software Upgrade Management	Refresh Element job does not finish when elements of different types are selected.	7.1.3.2
SMGR-46818	Software Upgrade Management	System Platform upgrade using System Manager fails while trying to clean the previous backup from System Platform.	7.1.2.0
SMGR-46757	Software Upgrade Management	If admin select multiple hosts and perform Set Login Banner operation, it works only for one host and for other hosts it gets stuck.	7.1.2.0
SMGR-46794	Discovery Management	Gateway Discovery using discovery profile doesn't work for G430 version 39.12.0.	7.1.3.1
SMGR-46742	Software Upgrade Management	Cannot upload file with .fdl extension to software library using My Computer option.	7.1.3.1
SMGR-47833	Software Upgrade Management	Unable to discover TN Boards in 7.1.3.2 when a Communication Manager is added or updated.	7.1.3.2

Fixes in System Manager 7.1.3.2

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-46469	Security Updates	(RHSA-2018:2384) kernel update	N/A
SMGR-46472	Security Updates	(RHSA-2018:2570) bind update	N/A
SMGR-46471	Security Updates	(RHSA-2018:2439) mariadb security and bug fix update	N/A
SMGR-46138	Security Updates	(RHSA-2018:2181) gnupg2 update	N/A
SMGR-46473	Security Updates	(RHSA-2018:2242) java-1.8.0-openjdk	N/A
SMGR-46474	Security Updates	(RHSA-2018:2613) Samba update	N/A
SMGR-46537	Infrastructure	editHosts command does not allow to add record having first character as digit in the FQDN	7.1
SMGR-46401	Infrastructure	tzdata Linux RPM updated to tzdata-2018e	N/A
SMGR-46327	Infrastructure	JBoss service not come up due if System Manager is configured with Communication Manager and if CRL is expired on System.	7.1.x
SMGR-46336	Infrastructure	Database transactions are getting stuck in some scenarios	7.0.x
SMGR-45124	Infrastructure	Unable to change password from password change page if user id has space at beginning or end	7.1.x

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-46646	User Export	Unable to delete user export job from export list if job record is already deleted from scheduler	6.3
SMGR-46466	Directory Synchronization	Directory synchronization fails to add new user when we have a mapping for "Microsoft Exchange Handle" along with a mapping for "email"	7.1.3.2
SMGR-46613	User Management	cannot change the domain of e164 handle using bulk edit operation	7.0.1.2
SMGR-46608	User Management	Option " Auto Generate Communication Profile Password" selection does not update existing communication password for users using bulk edit user operation.	7.1.3.0
SMGR-46146	User Management	Duplicate of existing user fails with an error “Cause of failure: SIP URI '' is not added as a SIP handle”	7.1.3.1
SMGR-46232	Alarm Management	Alarming is not working properly	7.1.3.0
SMGR-45926	Communication Manager Management	Using IE browser, changes are not getting committed after EDIT/ADD hunt group from Home / Elements / Communication Manager / Groups / Hunt Group	7.1.3.2
SMGR-46592	Communication Manager Management	Unable to configure COR value higher than 250 for Communication Manager 5.2.1 using System Manager Endpoint Editor.	6.3.x
SMGR-46606	Communication Manager Management	Broadcast announcement throws error "Special Character Not Allowed in Audio File"	7.1.3.1
SMGR-45675	Communication Manager Management	Ring setting for each brdg-appr button not seen for an existing station when viewing or editing it via System Manager UI even though entry present on communication Manager and System Manager database.	7.0.x
SMGR-46412	Communication Manager Management	Add Buttons fields on End Point report for CSV format	7.1.x
SMGR-46516	Report Management	Unable to delete reports by user associated custom role	7.1
SMGR-46086	SDM client	Provide validation during deployment to prevent System Manager being deployed with invalid Command line User Name details.	7.1.3
SMGR-45959	Software Upgrade Management	SDM support for G430/G450 Gateway upgrades to release 38.21.x and above	7.1.3.2
SMGR-46263	Software Upgrade Management	Company ID under user settings gets empty after upgrade.	7.0.x
SMGR-46637	Software Upgrade Management	Analyze and Refresh Families activities not working due to change in PLDS certificate.	N/A
SMGR-46119	Software Upgrade Management	Null pointer exception while performing pre-upgrade check.	7.1.3.0
SMGR-46281	Software Upgrade Management	After performing refresh elements & analyze operation on CM 7.0 entry, SDM shows un-entitled symbol even if customer is entitled for CM 7.1 and Update/Upgrade option is disabled.	7.1.3.0

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-46340	Inventory Management	After upgrading System Manager 7.1.3 GA to 7.1.3.1, Communication Manager Entitled Upgrade version in Upgrade Management shows N/A even - though the user is entitled for a valid Communication Manager version.	7.1.3.1
SMGR-46303	Inventory Management	Device type entries are missing in the System Manager 7.1 upgraded from release 6.3.4	6.3.4
SMGR-46270	Inventory Management	Alternate IP address is not updating if discovery failed during editing Communication Manager duplex entry in inventory.	7.0.x
SMGR-46220	Inventory Management	SDM shows incorrect Entitled Update Version.	7.1.3.0

Fixes in System Manager 7.1.3.1

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-45378	Security Updates	(RHSA-2018:0483) dhcp security update	N/A
SMGR-45436	Security Updates	(RHSA-2018:1062) Kernel update	N/A
SMGR-45435	Security Updates	(RHSA-2018:0805) glibc update	N/A
SMGR-45294	Security Updates	(RHSA-2018:0378) ruby security update	N/A
SMGR-46017	Security Updates	[RHSA-2018:1191-01] Critical: java-1.8.0-openjdk security update	N/A
SMGR-46058	Security Updates	(RHSA-2018:1649) Important: java-1.8.0-openjdk security update	N/A
SMGR-46060	Security Updates	(RHSA-2018:1629) Important: kernel security update	N/A
SMGR-46067	Security Updates	RHSA-2018:1700) Important: procps-ng security update	N/A
SMGR-45441	Infrastructure	Commands serviceJBossRESTART, serviceJBossSTART, serviceJBossSTATUS and serviceJBossSTOP are not working in 7.1.3 release	7..1.3
SMGR-45703	Infrastructure	ChangeVFQDN fails to update VFQDN in some scenarios	7.1
SMGR-45586	Infrastructure	External authentication configuration fails and next access to External authentication page will throw system error.	7.1
SMGR-45588	Infrastructure	Do not allow to configure external server configuration with invalid values in external authentication.	7.1
SMGR-45869	Infrastructure	Allow Administrative users to have '.' in user id.	7.1
SMGR-45327	Directory Synchronization	Allow System Manager to set null value (remove value) for AD attribute in bi-direction Synchronization.	All
SMGR-45622	Geo Redundancy Management	Authentication on secondary server does not work if Data Store Access certificate is installed with 3rd party issuer and if that certificate CN is in reverse order.	7.1
SMGR-45766	Role Management	Unable to store value in range field if custom role is created under communication manager admin.	7.1.3

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-45060	Trust Management	Unable to change the CRL distribution points inside the default certificate profiles and Cloned Profiles.	7.1
SMGR-45058	Trust Management	Unable to load certificate when the ExtendedKeyUsages in the certificate has certain values (values in OID format).	7.1
SMGR-45698	Logging Management	System Manager JBoss service go down due to file “dbFailureBackup.txt” growth.	All
SMGR-44680	Web Services	Auto Logout/Login fields are not defined for Agent in XML schema to update from Web-Services.	All
SMGR-45431	Communication Manager Management	Number for autodial button does not get saved after commit.	7.1
SMGR-45801	Communication Manager Management	While changing the vector via element cut-through output does not shows the hash character (#).	7.1
SMGR-45799	Communication Manager Management	Support duplication option for VDN.	7.1
SMGR-45818	Communication Manager Management	Broadcast Announcement Job status show successful even if it failed or partially completed.	7.1
SMGR-45814	Communication Manager Management	Backup Announcement Job status show successful even if it failed or partially completed.	7.1
SMGR-46042	Communication Manager Management	Notify Sync is not working for change agent-ID with auto option.	7.1
SMGR-46051	Communication Manager Management	Uploading announcements via System Manager using special character in filename / announcement name introduces inconsistencies and issues between Communication Manager and Avaya Media Server.	7.1
SMGR-46057	Communication Manager Management	Audit report shows discrepancy when location.locationidex=null on Communication Manager and location.locationidex=0 on System Manager.	7.1
SMGR-45803	Communication Manager Management	Number of favorites calculated incorrectly when a contact is added as a favorite on 96x0 and 96x1 phones.	7.1
SMGR-45909	User Management	Null Exception on UI when user check the Dual Registration box for H323 user on CM profile section	7.1.3
SMGR-45928	User Management	System does not send mail for user's communication password change in some scenarios.	7.1
SMGR-46025	User Management	Error “Invalid Email Address” if email address domain part contains digit for user.	7.1
SMGR-43407	Report Management	Export of Reports from System Manager to a SFTP-Server is not working.	7.1
SMGR-33607	Report Management	Report for 'display alarms' does not gets created.	7.1
SMGR-45885	Report Management	Report for “Display error” for Communication Manager is blank	7.1
SMGR-45807	Report Management	For detailed VDN report, Name and Destination number fields do not show proper data.	7.1
SMGR-45948	Report Management	On System Manager list vdn reports show skewed output.	7.1

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-46001	Report Management	In detailed report when all fields are selected report runs as empty for VDN.	7.1
SMGR-45202	Software Upgrade Management	Refresh Job get stuck if SNMP values are not proper for gateway	7.1
SMGR-46015	Software Upgrade Management	Clear text password in upgrade logs.	7.1
SMGR-44958	Software Upgrade Management	Unable to unmanage the hosts from VCenter.	7.1
SMGR-46045	Inventory Management	Clear text password in inventory logs.	7.1

Fixes in System Manager 7.1.3

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-44959	Infrastructure	System Manager 7.1.3 includes the Red Hat updates to support mitigation of the Meltdown/Spectre vulnerabilities. However, this has the potential to affect performance – so there is now a small script that allows the setting of kernel options to control how these vulnerabilities are handled. The effect of running the kernel configuration script is both immediate and will persist across reboots. The script is called kernel_opts.sh and should be executed from the System Manager command line interface using the customer's command line user. It has the argument “status” to display the current status of the kernel options, “enable” to enable all flags to provide maximum protection, and “disable” to disable all flags to provide maximum performance.	
SMGR-43351	Infrastructure	Creating new CA from UI restricted to 3 years validity instead of 10 years	
SMGR-44288	Infrastructure	SMGR Web UI is not available after SMGR powered down for over 7 days	
SMGR-43139	Infrastructure	Application server HTTP Header reveals software version details	
SMGR-44678	Infrastructure	Memory leak issue in OpenJDK 8u144 causes JBoss application server to terminate	
SMGR-43579	Infrastructure	"changeVFQDN" does not update /etc/hosts file with new VFQDN value, which further causes issue with GEO configuration or Data Replication Issue.	
SMGR-41117	Infrastructure	Invalid alarm “Default ASG Auth file found on System Manager alarm” getting generated	7.1.0.0
SMGR-44337	Infrastructure	SMGR goes into unusable state after upgrade to SMGR 7.1.2 due to /tmp partition getting full	

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-43331	Communication Manager Management	Announcement files are not getting pushed by SCP to CF enabled gateway	
SMGR-44448	Communication Manager Management	Add/Edit agent is not allowed if "Business Advocate" field is disabled even though it is not always required	
SMGR-43527	Communication Manager Management	Communication Manager details not getting removed completely on deleting from Inventory if that Communication Manager had notification sync enabled and it is unreachable during removal	
SMGR-43074	Communication Manager Management	Communication Manager initial synchronization is failing at hunt-group with error "EJB_EXCEPTION : Removing a detached instance"	
SMGR-44869	Communication Manager Management	Communication Manager initial synchronization is fails at "service-hours-table". Also "change service-hours-table" command from element cut-through does not work.	
SMGR-43827	Communication Manager Management	The existing EC500 entries in off-pbx-telephone station are getting deleted on Communication Manager when adding a check mark to “Allow H.323 and SIP Endpoint Dual Registration” on an existing users' CM Endpoint Profile	
SMGR-43744	Communication Manager Management	Re-Calculate route pattern fails if there are large number of users	
SMGR-43743	Communication Manager Management	Error thrown when user provides values in Range for custom role	
SMGR-43189	Communication Manager Management	Detailed Reports page not working in CM Element Manager	
SMGR-44522	Communication Manager Management	Detailed Reports not getting generated properly	
SMGR-43745	Communication Manager Management	Editing of existing report does not work properly	
SMGR-44377	Communication Manager Management	SMGR going "out of memory" due to memory leak in Reports Output Panel	
SMGR-44170	Solution Deployment Manager	Unable to add / discover hosts under VM Management using vCenter if the hosts have a lot of datastores configured	
SMGR-44588	Solution Deployment Manager	Refresh Element fails for Duplex ESS Communication Manager with encryption enabled. This is blocking upgrade.	
SMGR-41580	User Management	Subject Common Name -CN" gets removed if other options from left panel are selected on Provision User Certificate Authentication page.	
SMGR-41841	User Management	Error thrown while adding Administrative user having a comma character in Full Name	
SMGR-43081	User Management	admin user loses System Administrator role while doing certain operations	

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-41621	End User Self Provisioning	After Certificate based authentication fails for End User Self Provisioning, the fall back option for authentication does not work with normal login credentials	
SMGR-43352	User Management	Change Presence/IM Domain using "Bulk Edit Users" does not update xmpp handle in other users which are Associated contacts	
SMGR-38071	User Management	Translation is not happening correctly for First and last name having Umlaut characters (ä, ö, ü, ß)	
SMGR-44774	License Management	SMGR still shows no license installed after installing license file having certain values	

Fixes in System Manager 7.1.2

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-39423	Infrastructure	System Monitor CPU usage parameter is not generating alarms based on proper messages for high CPU usage	
SMGR-43355	Infrastructure	Bug in JDK causes Out of memory issue for JBoss	
SMGR-43330	Infrastructure	CS1k registration fails with System Manager 7.1 as during registration system property file gets corrupted	
SMGR-41626	Infrastructure	Disk Usage alarm is missing for database (/var/lib/pgsql) partition	
SMGR-41674	Infrastructure	IP Address/FQDN and DNS change is not getting reflected for all elements in the Manage Elements page	
SMGR-40251	Infrastructure	Upload of customized image for header is not working for JPG format	
SMGR-26896	Infrastructure	Potential RMI Vulnerability. This has been addressed by upgrading Apache Commons Collection library and enforcing strict 2-way SSL authentication over various RMI ports.	
SMGR-40508	Directory Synchronization	Datasoucre name accepts special characters, this further cause’s error.	
SMGR-41487	Directory Synchronization	CS1000 extension assigned to a user is not getting synced to Active Directory through bi-directional sync mapping	
SMGR-40602	User Management	Timezone value in user identity page not getting populated properly after DST change	
SMGR-43206	User Management	Creation of user with Communication Manager profile takes minimum 50 seconds in certain configuration	
SMGR-41620	User Self Provisioning	User self-provisioning does not work with personal certificate if certificate attributes values are in upper case/mixed case and mapped to user name in System Manager	

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-41841	User Administration	New administrator user cannot be created if comma character is present in Full Name	
SMGR-41909	License Management	C++ WebLM client (7.1.x) is unable to connect to WebLM server	
SMGR-41667	Trust Management	CA certificate without CN cannot be imported into System Manager trust store	
SMGR-41675	Communication Manager Management	Communication Manager synchronization is failing with error message saying element is not managed by System Manager after System Manager IP address change	
SMGR-41896	Communication Manager Management	Button values for SIP Endpoints cannot be edited using endpoint editor feature from User Management page	
SMGR-41917	Communication Manager Management	Media Server elements are not shown in Broadcasting Announcements page	
SMGR-43216	Communication Manager Management	Calendar feature is not working while scheduling a job in Communication Manager Element Manager	
SMGR-41386	Report Management	Report with list vdn does not show skill data properly	
SMGR-43189	Report Management Manager	Detailed Reports page is not working	
SMGR-41902	Report Management	"list agent-loginID" report does not show skill data	

Fixes in System Manager 7.1.1.1

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release introduced
MX-4772	Meeting Exchange Element Manager	Meeting Exchange allRouteTo configuration is missing from System Manager.	
AMS-4319	AMS Element Manager	Fix the UI display issue for Edit Application Assignment. User can only see 15 AAMS clusters for application assignment if the total number of AAMS clusters is greater than 15.	
SMSG-960	Messaging Element Manager	Error occurs when Messaging tab and Templates tab are opening concurrently, and the Admin is selecting Template in Edit Subscriber page.	
SMSG-1017	Messaging Element Manager	When the Admin adds a new user with Messaging profile without touching Messaging Editor, Site Prefix is added to mailbox number in the PBX Extension field.	
SMGR-41693	Trust Management	Scalability related improvement in EJBCA.	
SMGR-41903	User Self Previsioning Management	User self-provisioning does not work with personal certificate if certificate attribute mapped to user name in System Manager values are in upper case/mixed case.	

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-41897	Security Updates	Security updates with openjdk.	
SMGR-41674	Infrastructure	System Manager IP/FQDN change along with Gateway change does not work properly.	
SMGR-41683,	Communication Manager Management	After IP change on System Manager, issue with managing Communication Manager from System Manager. Managing CM fails with error as “CM "Name" is not being managed by this System Manager server and could not be synched. Try using the other Geo-Redundant System Manager server or enable management from this System Manager server”.	
CS1000SMGR-345	CS1K Element Manager	Patch Manager shows as "ready to install" patches which are not applicable to selected platform.	
CS1000SMGR-334	CS1K Element Manager	Cannot edit a custom SNMP profile associated with CS1K system.	
CS1000SMGR-335	CS1K Element Manager	Got System Error message during assigning a custom SNMP profile to a CS1K system.	

Fixes in System Manager 7.1.1

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-41293	User Interface	Unable to add user preference from custom user login.	
SMGR-40706	Inventory Management	Not able to bulk export the CS1K element along with other elements like CM, SM through SMGR CLI	
SMGR-39790	Inventory Management	Modify sqls for ipv6 paired node ipfqdn change	
SMGR-41352	Infrastructure	Root account is accessible in SMGR 7.1.1 using "sudo runuser" command	
SMGR-41489	VM Management	Unable to see Map vCenter page after update	
SMGR-41418	VM Management	Unable to Add vCenter in SDM vm management using local admin	
SMGR-41406	VM Management	Deployment + Patching failing in SMGR using URL option	
SMGR-41143	VM Management	Unable to Upgrade 7.0.x to Upgrade to 7.1.x as trust is failing in 7.1.1 SDM Client	
SMGR-41140	VM Management	Trust Establishment Fails on SMGR 7.1.1 for AES	
SMGR-41139	VM Management	Block warning popup during SMGR deployment if patch is not given for product version 7.0 and below	

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-40985	VM Management	Version shows 7.1 only even if we deploy 7.1GA OVA + 7.1.1 patch and Blank FQDN for SMGR in latest SDM Client	
SMGR-41180	Licensing Management	Primary host ID of the SMGR should start with “V” letter under Licensing Server properties.	
SMGR-41171	VM Management	Upgrade of System Manager getting stuck in OVA Parse of SDM Client	
SMGR-41256	Software Upgrade Management	User is unable to commit an upgrade.	
SMGR-41153	Software Upgrade Management	Upgrade Management > Analyze is stuck for AES VM from System Manger 7.1.1	
SMGR-41445	VM Management	After upgrade failed, all other operations are blocked from SDM Client.	**7.1.1**
SMGR-41431	VM Management	System Manage upgrade fail through SDM client from 7013 to 711.	
SMGR-41290	Communication Manager Management	On upgraded system R7.0.1.3 to R7.1.1, failed to add/edit hunt groups with old RBAC and custom user.	
SMGR-41287	Communication Manager Management	Help link of hunt group does not redirect to the correct page.	
SMGR-41283	Communication Manager Management	Announcement file path is prefixed with filename path while uploading.	
SMGR-41254	Communication Manager Management	NCM cannot be launched for the selected Communication Manager while creating hunt group	
SMGR-41188	Communication Manager Management	Argument type mismatch error message displayed during Add and edit of hunt group with ACD on (if supervisor extension is edited and/or then kept null).	
SMGR-41187	Communication Manager Management	Incorrect error message displays in scheduler log during delete or edit operation for hunt group.	
SMGR-40987	Communication Manager Management	Coverage path validation is showing java exception	
SMGR-40982	Communication Manager Management	Scheduled hunt group job is failing.	
SMGR-40980	Communication Manager Management	Extension range and Group Number Range operations are not working for Hunt Group operations	
SMGR-40929	SMGR:Security:TM	Getting internal error when trying enrollment password page	
SMGR-41506	VM Management	SDM Upgrade Management VM greensm01 appears twice.	
SMGR-41364	VM Management	SDM Client Patch Commit takes too long to complete.	
SMGR-41158	VM Management	Issue with Host certificate, hence all SDM Operation blocked!!	**7.1.1**
SMGR-40984	VM Management	Status detail page is not coming for failed operation.	**7.1.1**
SMGR-40983	VM Management	Patch Rollback operation failed on latest SDM Client	**7.1.1**

ID	Minimum Conditions	Visible symptoms	Release introduced
SMGR-41477	Software Upgrade Management	“Flexi Foot print” field is being mapped with “SMGR_DEFAULT_LOCAL” data storage path	
SMGR-41469	Software Upgrade Management	Patch-Install Commit fails when we upgrade SM to 7.1.1.0.711003 from SMGR SDM.	**7.1.1**
SMGR-41444	Software Upgrade Management	SDM-Client - On Primary System Manager update got failed but Commit and Rollback options are disabled on SDM-Client.	
SMGR-41417	Software Upgrade Management	Unable to complete upgrade+patch for WebLM element.	
SMGR-41367	Software Upgrade Management	Pre-populate Data for Utility Server does not populate all the data.	
SMGR-41316	Software Upgrade Management	Cannot upgrade standalone WebLM server from 7.1.0.0.11.25605 to 7.1.1.0.036745.	
SMGR-41073	Software Upgrade Management	Session Manager upgrade failed from 7.1 to 7.1.1 patch via System Manager SDM.	
SMGR-40926	Software Upgrade Management	Unable to apply SM FP1 patch vis SMGR SDM	**7.1.1**
SMGR-41174	Infrastructure	Existing System Configuration needs to be removed from System Manager KVM OVA.	**7.1.1**
SMGR-41302	Backup and Restore Management	Backup Restore is failing on OOBM Enabled System Manager.	
SMGR-41222	Backup and Restore Management	Backup Restore is failing from SFTP Server	
SMGR-41196	Backup and Restore Management	Upgrade of System Manager is failing from 7.0.1.3 OOBM Enabled to 7.1.1.	
SMGR-41499	Infrastructure	SMGR-KVM: Unable to login after system instance reboots for Profile-3 on KVM.	**7.1.1**
SMGR-41467	Infrastructure	SMGR-KVM: System time changes after reboot.	**7.1.1**
SMGR-41464	Infrastructure	Backup is failing on DOD Mode Machine for KVM setup.	**7.1.1**
SMGR-41223	Infrastructure	SMGR-KVM: Backup space does not work while configuring System Manager network configurations parameters through virt-manager on KVM hypervisor	**7.1.1**
SMGR-41173	Infrastructure	SMGR-KVM: Unable to deploy KVM OVA with an IPv6 DNS address.	
SMGR-41141	Infrastructure	[SIDT]7.1.1 Issue with reboot SMGR after DOD conversion	7.1.1

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

Known issues and workarounds in System Manager on VMware in Release 7.1.3.8

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
SMGR-40715	Infrastructure	• SSL handshake fails on JMX port connection if revocation checking set to OCSP. • Access to Configure Identity/Trusted Certificates page throws error, if accessed from Home / Services / Inventory / Manage Elements. System Manager Backup fails.	Revert to OCSP settings back to default settings in Home / Services / Security / Configuration / Security Configuration (Revocation Configuration section.)
SMGR-46901	Infrastructure	Click on User Management View/Edit button takes 2 to 3 minutes load to page if User has Communication profile and syslog is loaded to root logger.	Remove Syslog appender from root logger.
SMGR-49359	Infrastructure	jboss_service_affects.log do not get roll over.	Manually remove the contents from file.
SMGR-48200 SMGR-33574	Backup and Restore Management	User cannot take System Manager backup on HDI (Hitachi Data Ingestor) Linux appliance remote server and Windows base SFTP server (WS_FTP server).	
SMGR-53497	User Management	User's Distinguished Name is not getting updated in System Manager database via LDAP sync if user is moved from one OU to another OU under same data store	Delete user in AD and execute Sync. Recreate user again in AD and then execute Sync again.
SMGR-39653	Data Replication Service	Data replication stuck in read for repair if element FQDN length greater than 50 characters	Set the node FQDN value to less than 50 characters
SMGR-46088	Geo Graphic Redundancy	Cannot login to secondary server UI using EASG after secondary server is activated.	User another user credentials.
SMGR-44830	Geo Graphic Redundancy	GEO configuration will fail if we set (Maximum Sessions Per User: 1) in session properties	Set Maximum Sessions Per User to 5 (default value) and then perform GEO configuration.
SMGR-46363	Trust Management	Replacing a PEM certificate using a third-party certificate which is signed using Elliptical Curve signing algorithm results in the certificate to get corrupted and removed from the Managed Id certificates User interface.	Use different algorithm to sign certificate.
SMGR-25823	Scheduler Management	Scheduled jobs created by a user with "administrative" privileges will start to fail once the scheduled user gets deleted from the system.	Delete the existing jobs and recreate new jobs.
SMGR-45856	User Management	Latin transcription of "First Name" and "Last Name" in the Identity Tab of User are not happening properly for Russian name with the Cyrillic alphabet.	Manually update Latin transcription value for the First Name" and "Last Name" in the Identity Tab of User and save user.
SMGR-41380	Software Deployment Manager	Deployment using SDM Client fails if you enter "0.0.0.0" in the field for DNS.	Use valid DNS or Use DNS values as "127.0.0.1"
SMGR-43249	User Interface	Last logged Time is not shown properly when login is done using Certificate based authentication.	
SMGR-44904	License	Enterprise WebLM configuration, "Usage by WebLM"	

ID	Minimum conditions	Visible symptoms	Workaround
	Management	does not show the local PC time zone.	
SMGR-48582	License Management	WebLM fails to generate hosts ID when system language is set to local language like de_DE.UTF-8 i.e. Germany (other than English).	
SMGR-46448	License Management	Centralized License links does not work after upgrading System Manager with centralized licensing from 7.0.x to 7.1.x release.	
SMGR-43445	Communication Manager Management	Shortcut keys provided for certain Tabs on the Communication Manager Management pages are not working.	
SMGR-45752	Communication Manager Management	Announcement backup works only for MD5 and DES combination.	
SMGR-47826	Communication Manager Management	User cannot update preferred handle of Communication Manager communication profile using bulk edit option.	
SMGR-45913	Role Management	User gets system error while updating existing role having permissions for group once group is renamed.	First remove the permissions associated with old group from role and update the role by assigning the required permissions.
SMGR-49195	Global Search Component	Global Search with Russian Language doesn't work as expected.	

Known issues and workarounds in System Manager on VMware in Release 7.1.3.7

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

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-40715	Infrastructure	• SSL handshake fails on JMX port connection if revocation checking set to OCSP. • Access to Configure Identity/Trusted Certificates page throws error, if accessed from Home / Services / Inventory / Manage Elements. System Manager Backup fails.	Revert to OCSP settings back to default settings in Home / Services / Security / Configuration / Security Configuration (Revocation Configuration section.)
SMGR-46901	Infrastructure	Click on User Management View/Edit button takes 2 to 3 minutes load to page if User has Communication profile and syslog is loaded to root logger.	Remove Syslog appender from root logger.
SMGR-49359	Infrastructure	jboss_service_affects.log do not get roll over.	Manually remove the contents from file.
SMGR-48200 SMGR-33574	Backup and Restore Management	User cannot take System Manager backup on HDI (Hitachi Data Ingestor) Linux appliance remote server and Windows base SFTP server (WS_FTP server).	
SMGR-53497	User Management	User's Distinguished Name is not getting updated in System Manager database via LDAP sync if user is moved from one OU to another OU under same data	Delete user in AD and execute Sync. Recreate user again in AD

ID	Minimum conditions	Visible symptoms	Workaround
		store	and then execute Sync again.
SMGR-39653	Data Replication Service	Data replication stuck in read for repair if element FQDN length greater than 50 characters	Set the node FQDN value to less than 50 characters
SMGR-46088	Geo Graphic Redundancy	Cannot login to secondary server UI using EASG after secondary server is activated.	User another user credentials.
SMGR-44830	Geo Graphic Redundancy	GEO configuration will fail if we set (Maximum Sessions Per User: 1) in session properties	Set Maximum Sessions Per User to 5 (default value) and then perform GEO configuration.
SMGR-46363	Trust Management	Replacing a PEM certificate using a third-party certificate which is signed using Elliptical Curve signing algorithm results in the certificate to get corrupted and removed from the Managed Id certificates User interface.	Use different algorithm to sign certificate.
SMGR-25823	Scheduler Management	Scheduled jobs created by a user with "administrative" privileges will start to fail once the scheduled user gets deleted from the system.	Delete the existing jobs and recreate new jobs.
SMGR-45856	User Management	Latin transcription of "First Name" and "Last Name" in the Identity Tab of User are not happening properly for Russian name with the Cyrillic alphabet.	Manually update Latin transcription value for the First Name" and "Last Name" in the Identity Tab of User and save user.
SMGR-41380	Software Deployment Manager	Deployment using SDM Client fails if you enter "0.0.0.0" in the field for DNS.	Use valid DNS or Use DNS values as “127.0.0.1”
SMGR-43249	User Interface	Last logged Time is not shown properly when login is done using Certificate based authentication.	
SMGR-44904	License Management	Enterprise WebLM configuration, "Usage by WebLM" does not show the local PC time zone.	
SMGR-48582	License Management	WebLM fails to generate hosts ID when system language is set to local language like de_DE.UTF-8 i.e. Germany (other than English).	
SMGR-46448	License Management	Centralized License links does not work after upgrading System Manager with centralized licensing from 7.0.x to 7.1.x release.	
SMGR-43445	Communication Manager Management	Shortcut keys provided for certain Tabs on the Communication Manager Management pages are not working.	
SMGR-45752	Communication Manager Management	Announcement backup works only for MD5 and DES combination.	
SMGR-47826	Communication Manager Management	User cannot update preferred handle of Communication Manager communication profile using bulk edit option.	
SMGR-45913	Role	User gets system error while updating existing role having	First remove the

ID	Minimum conditions	Visible symptoms	Workaround
	Management	permissions for group once group is renamed.	permissions associated with old group from role and update the role by assigning the required permissions.
SMGR-57785	Communication Manager Management	INIT sync resets "Dual Registration" and "Calculate Route Pattern" fields on Communication Manager communication profile.	
SMGR-57615	Communication Manager Management	List registered station report in System Manager does not show all endpoints that are registered, only one of the soft phone extensions in AES instead of all 3.	
SMGR-55372	Communication Manager Management	AD sync to remove user fails if the station is part of hunt group on tenant management enabled system.	
SMGR-49195	Global Search Component	Global Search with Russian Language doesn't work as expected.	

Known issues and workarounds in System Manager on VMware in Release 7.1.3.6

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

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-40715	Infrastructure	• SSL handshake fails on JMX port connection if revocation checking set to OCSP. • Access to Configure Identity/Trusted Certificates page throws error, if accessed from Home / Services / Inventory / Manage Elements. System Manager Backup fails.	Revert to OCSP settings back to default settings in Home / Services / Security / Configuration / Security Configuration (Revocation Configuration section.)
SMGR-46901	Infrastructure	Click on User Management View/Edit button takes 2 to 3 minutes load to page if User has Communication profile and syslog is loaded to root logger.	Remove Syslog appender from root logger.
SMGR-49359	Infrastructure	jboss_service_affects.log do not get roll over.	Manually remove the contents from file.
SMGR-48200 SMGR-33574	Backup and Restore Management	User cannot take System Manager backup on HDI (Hitachi Data Ingestor) Linux appliance remote server and Windows base SFTP server (WS_FTP server).	
SMGR-53767	User Management	If user is associated with Communication Profile and tenant management is enabled on system then user update fails with error STACOMMPROFILE0009 when there is change in user’s First Name, Last Name or Display Name value.	
SMGR-53497	User Management	User’s Distinguished Name is not getting updated in System Manager database via LDAP sync if user is moved from one OU to another OU under same data store	Delete user in AD and execute Sync. Recreate user again in AD and then execute Sync again.

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-39653	Data Replication Service	Data replication stuck in read for repair if element FQDN length greater than 50 characters	Set the node FQDN value to less than 50 characters
SMGR-46088	Geo Graphic Redundancy	Cannot login to secondary server UI using EASG after secondary server is activated.	User another user credentials.
SMGR-44830	Geo Graphic Redundancy	GEO configuration will fail if we set (Maximum Sessions Per User: 1) in session properties	Set Maximum Sessions Per User to 5 (default value) and then perform GEO configuration.
SMGR-46363	Trust Management	Replacing a PEM certificate using a third-party certificate which is signed using Elliptical Curve signing algorithm results in the certificate to get corrupted and removed from the Managed Id certificates User interface.	Use different algorithm to sign certificate.
SMGR-25823	Scheduler Management	Scheduled jobs created by a user with "administrative" privileges will start to fail once the scheduled user gets deleted from the system.	Delete the existing jobs and recreate new jobs.
SMGR-45856	User Management	Latin transcription of "First Name" and "Last Name" in the Identity Tab of User are not happening properly for Russian name with the Cyrillic alphabet.	Manually update Latin transcription value for the First Name" and "Last Name" in the Identity Tab of User and save user.
SMGR-41380	Software Deployment Manager	Deployment using SDM Client fails if you enter "0.0.0.0" in the field for DNS.	Use valid DNS or Use DNS values as “127.0.0.1”
SMGR-53555	Software Deployment Manager	Data store values are not showing during Pre-upgrade Configuration page for IE Browser.	User other browser like Firefox.
SMGR-43249	User Interface	Last logged Time is not shown properly when login is done using Certificate based authentication.	
SMGR-44904	License Management	Enterprise WebLM configuration, "Usage by WebLM" does not show the local PC time zone.	
SMGR-48582	License Management	WebLM fails to generate hosts ID when system language is set to local language like de_DE.UTF-8 i.e. Germany (other than English).	
SMGR-46448	License Management	Centralized License links does not work after upgrading System Manager with centralized licensing from 7.0.x to 7.1.x release.	
SMGR-43445	Communication Manager Management	Shortcut keys provided for certain Tabs on the Communication Manager Management pages are not working.	
SMGR-45752	Communication Manager Management	Announcement backup works only for MD5 and DES combination.	
SMGR-47826	Communication Manager Management	User cannot update preferred handle of Communication Manager communication profile using bulk edit option.	

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-45913	Role Management	User gets system error while updating existing role having permissions for group once group is renamed.	First remove the permissions associated with old group from role and update the role by assigning the required permissions.
SMGR-49195	Global Search Component	Global Search with Russian Language doesn't work as expected.	
SMGR-54062	Licensing Management	Remove AJP port 8009 from configurations.	

Known issues and workarounds in System Manager on VMware in Release 7.1.3.5

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

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-40715	Infrastructure	• SSL handshake fails on JMX port connection if revocation checking set to OCSP. • Access to Configure Identity/Trusted Certificates page throws error, if accessed from Home / Services / Inventory / Manage Elements. System Manager Backup fails.	Revert to OCSP settings back to default settings in Home / Services / Security / Configuration / Security Configuration (Revocation Configuration section.)
SMGR-46901	Infrastructure	Click on User Management View/Edit button takes 2 to 3 minutes load to page if User has Communication profile and syslog is loaded to root logger.	Remove Syslog appender from root logger.
SMGR-49359	Infrastructure	jboss_service_affects.log do not get roll over.	Manually remove the contents from file.
SMGR-50884	Infrastructure	/var/log/Avaya/systemmonitor_service_affects.log and spiritagent_service_affects.log file not rotating and filling up disk space.	
SMGR-51064	Infrastructure	IPFQDN change corrupts network files causing database startup issue.	
SMGR-50097	Export and Import Management	Failures are marked on "Export All Users", but no logging for failed users.	
SMGR-49620	Role Management	Unable to parse comma (“ , “) in role description field, while creating new or updating the role.	Remove comma in role description field before role create/update operation.
SMGR-48200 SMGR-33574	Backup and Restore Management	User cannot take System Manager backup on HDI (Hitachi Data Ingestor) Linux appliance remote server and Windows base SFTP server (WS_FTP server).	
SMGR-39653	Data Replication Service	Data replication stuck in read for repair if element FQDN length greater than 50 characters	Set the node FQDN value to less than 50 characters
SMGR-46088	Geo Graphic Redundancy	Cannot login to secondary server UI using EASG after secondary server is activated.	User other user credentials.
SMGR-44830	Geo Graphic Redundancy	GEO configuration will fail if we set (Maximum Sessions Per User: 1) in session properties	Set Maximum Sessions Per User to 5 (default value) and then perform GEO configuration.
SMGR-46363	Trust Management	Replacing a PEM certificate using a third-party certificate which is signed using Elliptical Curve signing algorithm results in the certificate to get corrupted and removed from the Managed Id certificates User interface.	Use different algorithm to sign certificate.
SMGR-25823	Scheduler Management	Scheduled jobs created by a user with "administrative" privileges will start to fail once the scheduled user gets deleted from the system.	Delete the existing jobs and recreate new jobs.
SMGR-45856	User	Latin transcription of "First Name" and "Last Name" in the Identity Tab of User are not happening properly for	Manually update Latin transcription value for the

ID	Minimum conditions	Visible symptoms	Workaround
	Management	Russian name with the Cyrillic alphabet.	First Name" and "Last Name" in the Identity Tab of User and save user.
SMGR-41380	Software Deployment Manager	Deployment using SDM Client fails if you enter "0.0.0.0" in the field for DNS.	Use valid DNS or Use DNS values as “127.0.0.1”
SMGR-43249	User Interface	Last logged Time is not shown properly when login is done using Certificate based authentication.	
SMGR-44904	License Management	Enterprise WebLM configuration, "Usage by WebLM" does not show the local PC time zone.	
SMGR-48582	License Management	WebLM fails to generate hosts ID when system language is set to local language like de_DE.UTF-8 i.e. Germany (other than English).	
SMGR-46448	License Management	Centralized License links does not work after upgrading System Manager with centralized licensing from 7.0.x to 7.1.x release.	
SMGR-43445	Communication Manager Management	Shortcut keys provided for certain Tabs on the Communication Manager Management pages are not working.	
SMGR-45752	Communication Manager Management	Announcement backup works only for MD5 and DES combination.	
SMGR-47826	Communication Manager Management	User cannot update preferred handle of Communication Manager communication profile using bulk edit option.	
SMGR-45913	Role Management	User gets system error while updating existing role having permissions for group once group is renamed.	First remove the permissions associated with old group from role and update the role by assigning the required permissions.
SMGR-49195	Global Search Component	Global Search with Russian Language doesn't work as expected.	

Known issues and workarounds in System Manager on VMware in Release 7.1.3.4

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

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-40715	Infrastructure	• SSL handshake fails on JMX port connection if revocation checking set to OCSP. • Access to Configure Identity/Trusted Certificates page throws error, if accessed from Home / Services / Inventory / Manage Elements. System Manager Backup fails.	Revert to OCSP settings back to default settings in Home / Services / Security / Configuration / Security Configuration (Revocation Configuration section.)
SMGR-41360	Infrastructure	In System Manager 7.1.x.x and Solution Deployment	Do not use special

ID	Minimum conditions	Visible symptoms	Workaround
		Manager Client 7.1.x.x, while deploying OVA if CLI / UI password of VM includes few special characters such as ',>, <, &,", = then the password will not be set properly for VM after post deployment.	characters mentioned in list during deployment. Once deployment successfully completed then reset the password as per requirement.
SMGR-46901	Infrastructure	Click on User Management View/Edit button takes 2 to 3 minutes load to page if User has Communication profile and syslog is loaded to root logger.	Remove Syslog appender from root logger.
SMGR-49359	Infrastructure	jboss_service_affects.log do not get roll over.	Manually remove the contents from file.
SMGR-49029	Infrastructure	HTTP Thread Usage Monitor is not calculating the http thread percentage properly causing unnecessary Major/Minor Alarms on System Manager.	
SMGR-48645	Infrastructure	Audit.log file does not get auto rotate if System Manager deployed in Military mode.	Manual empty file and restart audit service.
SMGR-48200 SMGR-33574	Backup and Restore Management	User cannot take System Manager backup on HDI (Hitachi Data Ingestor) Linux appliance remote server and Windows base SFTP server (WS_FTP server).	
SMGR-39653	Data Replication Service	Data replication stuck in read for repair if element FQDN length greater than 50 characters	Set the node FQDN value to less than 50 characters
SMGR-46088	Geo Graphic Redundancy	Cannot login to secondary server UI using EASG after secondary server is activated.	User other user credentials.
SMGR-44830	Geo Graphic Redundancy	GEO configuration will fail if we set (Maximum Sessions Per User: 1) in session properties	Set Maximum Sessions Per User to 5 (default value) and then perform GEO configuration.
SMGR-46363	Trust Management	Replacing a pem certificate using a third-party certificate which is signed using Elliptical Curve signing algorithm results in the certificate to get corrupted and removed from the Managed Id certificates User interface.	Use different algorithm to sign certificate.
SMGR-25823	Scheduler Management	Scheduled jobs created by a user with "administrative" privileges will start to fail once the scheduled user gets deleted from the system.	Delete the existing jobs and recreate new jobs.
SMGR-45074	User Management	Additional sip handle gets created for user through user management web services (using replace option) or from UI import (partial/replace options).	Remove additional SIP handle from user.
SMGR-45856	User Management	Latin transcription of "First Name" and "Last Name" in the Identity Tab of User are not happening properly for Russian name with the Cyrillic alphabet.	Manually update Latin transcription value for the First Name" and "Last Name" in the Identity Tab of User and save user.
SMGR-41380	Software Deployment Manager	Deployment using SDM Client fails if you enter "0.0.0.0" in the field for DNS.	Use valid DNS or Use DNS values as “127.0.0.1”

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-43122	Software Deployment Manager	If Session Manager is added with its FQDN in Inventory and subsequently the Host of that Session Manager is added in VM Management and certain edit operations are done, then relationship between Host and VM breaks subsequently.	
SMGR-43249	User Interface	Last logged Time is not shown properly when login is done using Certificate based authentication.	
SMGR-44904	License Management	Enterprise WebLM configuration, "Usage by WebLM" does not show the local PC time zone.	
SMGR-43445	Communicatio n Manager Management	Shortcut keys provided for certain Tabs on the Communication Manager Management pages are not working.	
SMGR-45752	Communicatio n Manager Management	Announcement backup works only for MD5 and DES combination.	
SMGR-47826	Communicatio n Manager Management	User cannot update preferred handle of Communication Manager communication profile using bulk edit option.	
SMGR-49156	Communicatio n Manager Management	Cannot add more ip-network-map entries if ip-network-map already has >=500 entries.	Use Element Cut through to update ip-network-map.
SMGR-48555	Communicatio n Manager Management	In Exported list of user's 'Attendant' header missing in CM Endpoint Profile.	
SMGR-47952	Communicatio n Manager Management	Export All Endpoints causes system to go out of memory.	Please export 500 endpoints at a time.
SMGR-45913	Role Management	User gets system error while updating existing role having permissions for group once group is renamed.	First remove the permissions associated with old group from role and update the role by assigning the required permissions.
SMGR-48617	Role Management	Custom user sees Blank pages when clicks on session manager dashboard or user registrations page if role permission mappings for Session Manager are created under group.	Add role Session Manager Mappings in role without group association.
SMGR-46415	License Management	If System Manager with centralized license is upgraded from 7.0.x to 7.1.x using SDM client, it allows installation of new centralized license with same Centralized Licensing ID.	
SMGR-49316	Global Search Component	Global search feature does not show group membership associated with station.	
SMGR-49245	Global Search Component	Group membership data is not populated properly if multiple endpoints are viewed/edited one after another and updated through Global search component.	

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-49195	Global Search Component	Global Search with Russian Language doesn't work as expected.	
SMGR-49315	Software Upgrade Management	File upload to external FTP server using alternate source or /swlibrary/staging/sync does not work.	
SMGR-49253	Software Upgrade Management	Gateway discovery does not work with SNMPv3	

Known issues and workarounds in System Manager on VMware in Release 7.1.3.3

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

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-39711	Infrastructure	After performing a restore the previously scheduled backup job is getting disabled	Enable the backup job after restore.
SMGR-40715	Infrastructure	• SSL handshake fails on JMX port connection if revocation checking set to OCSP. • Access to Configure Identity/Trusted Certificates page throws error, if accessed from Home / Services / Inventory / Manage Elements. System Manager Backup fails.	Revert to OCSP settings back to default settings in Home / Services / Security / Configuration / Security Configuration (Revocation Configuration section.)
SMGR-41360	Infrastructure	In System Manager 7.1.x.x and Solution Deployment Manager Client 7.1.x.x, while deploying OVA if CLI / UI password of VM includes few special characters such as ',>, <, &,", = then the password will not be set properly for VM after post deployment.	Do not use special characters mentioned in list during deployment. Once deployment successfully completed then reset the password as per requirement.
SMGR-47633	Infrastructure	No log rotation for /var/log/Avaya/mgmt/geo/csync2.log.	Manually clean the file.
SMGR-46901	Infrastructure	Click on User Management View/Edit button takes 2 to 3 minutes load to page if User has Communication profile and syslog is loaded to root logger.	Remove Syslog appender from root logger.
SMGR-39653	Data Replication Service	Data replication stuck in read for repair if element FQDN length greater than 50 characters	Set the node FQDN value to less than 50 characters
SMGR-46591	Serviceability Agent Management	Cannot assign target profile to a Serviceability Agent while the target profile already has a notification profile linked	Unassign the notification profile, Link the target profile to new agent and then reassign the notification profile back again.
SMGR-46088	Geo Graphic Redundancy	Cannot login to secondary server UI using EASG after secondary server is activated.	User other user credentials.
SMGR-44830	Geo Graphic Redundancy	GEO configuration will fail if we set (Maximum Sessions Per User: 1) in session properties	Set Maximum Sessions Per User to 5 (default value) and then perform

ID	Minimum conditions	Visible symptoms	Workaround
			GEO configuration.
SMGR-46363	Trust Management	Replacing a pem certificate using a third-party certificate which is signed using Elliptical Curve signing algorithm results in the certificate to get corrupted and removed from the Managed Id certificates User interface.	Use different algorithm to sign certificate.
SMGR-25823	Scheduler Management	Scheduled jobs created by a user with "administrative" privileges will start to fail once the scheduled user gets deleted from the system.	Delete the existing jobs and recreate new jobs.
SMGR-45074	User Management	Additional sip handle gets created for user through user management web services (using replace option) or from UI import (partial/replace options).	Remove additional SIP handle from user.
SMGR-45856	User Management	Latin transcription of "First Name" and "Last Name" in the Identity Tab of User are not happening properly for Russian name with the Cyrillic alphabet.	Manually update Latin transcription value for the First Name" and "Last Name" in the Identity Tab of User and save user.
SMGR-41380	Software Deployment Manager	Deployment using SDM Client fails if you enter "0.0.0.0" in the field for DNS.	Use valid DNS or Use DNS values as “127.0.0.1”
SMGR-43122	Software Deployment Manager	If Session Manager is added with its FQDN in Inventory and subsequently the Host of that Session Manager is added in VM Management and certain edit operations are done, then relationship between Host and VM breaks subsequently.	
SMGR-43249	User Interface	Last logged Time is not shown properly when login is done using Certificate based authentication.	
SMGR-46088	User Interface	User cannot login to Secondary System Manager Web console UI using EASG after Secondary server is activated.	
SMGR-44904	License Management	Enterprise WebLM configuration, "Usage by WebLM" does not show the local PC time zone.	
SMGR-43445	Communication Manager Management	Shortcut keys provided for certain Tabs on the Communication Manager Management pages are not working.	
SMGR-45752	Communication Manager Management	Announcement backup works only for MD5 and DES combination.	
SMGR-47826	Communication Manager Management	User cannot update preferred handle of Communication Manager communication profile using bulk edit option.	
SMGR-47813	Communication Manager Management	Issues noticed in webservice API when "data module" is enabled on station.	
SMGR-45913	Role Management	User gets system error while updating existing role having permissions for group once group is renamed.	First remove the permissions associated with old group from role and update the role by

ID	Minimum conditions	Visible symptoms	Workaround
			assigning the required permissions.
SMGR-47849	Report Management	"list monitored-station" report generation is failing.	

Known issues and workarounds in System Manager on VMware in Release 7.1.3.2

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

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-39711	Infrastructure	After performing a restore the previously scheduled backup job is getting disabled	Enable the backup job after restore.
SMGR-40715	Infrastructure	• SSL handshake fails on JMX port connection if revocation checking set to OCSP. • Access to Configure Identity/Trusted Certificates page throws error, if accessed from Home / Services / Inventory / Manage Elements. • System Manager Backup fails.	Revert to OCSP settings back to default settings in Home / Services / Security / Configuration / Security Configuration (Revocation Configuration section.)
SMGR-41360	Infrastructure	In System Manager 7.1.x.x and Solution Deployment Manager Client 7.1.x.x, while deploying OVA if CLI / UI password of VM includes few special characters such as ',>, <, &,", = then the password will not be set properly for VM after post deployment.	Do not use special characters mentioned in list during deployment. Once deployment successfully completed then reset the password as per requirement.
SMGR-43365	Infrastructure	The changeIPFQDN utility is not working properly when used to modify Default Search List and DNS Server entries in a certain manner.	While executing ChangeIPFQDN command with -SEARCH option, don't use -DNS option.
SMGR-39653	Data Replication Service	Data replication stuck in read for repair if element FQDN length greater than 50 characters	Set the node FQDN value to less than 50 characters
SMGR-46591	Serviceability Agent Management	Cannot assign target profile to a Serviceability Agent while the target profile already has a notification profile linked	Unassign the notification profile, Link the target profile to new agent and then reassign the notification profile back again.
SMGR-28093	Geo Graphic Redundancy	On Primary dashboard, in notification section following message is shown, if GEO reconfiguration is performed from Secondary server after Secondary server activate/de-activate activities. "Restore Data to start synchronization between primary and secondary SMGR"	Please contact Avaya Support Team
SMGR-46088	Geo Graphic Redundancy	Cannot login to secondary server UI using EASG after secondary server is activated.	User other user credentials.

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-44830	Geo Graphic Redundancy	GEO configuration will fail if we set (Maximum Sessions Per User: 1) in session properties	Set Maximum Sessions Per User to 5 (default value) and then perform GEO configuration.
SMGR-46363	Trust Management	Replacing a pem certificate using a third-party certificate which is signed using Elliptical Curve signing algorithm results in the certificate to get corrupted and removed from the Managed Id certificates User interface.	Use different algorithm to sign certificate.
SMGR-25823	Scheduler Management	Scheduled jobs created by a user with "administrative" privileges will start to fail once the scheduled user gets deleted from the system.	Delete the existing jobs and recreate new jobs.
SMGR-45074	User Management	Additional sip handle gets created for user through user management web services (using replace option) or from UI import (partial/replace options).	Remove additional SIP handle from user.
SMGR-45856	User Management	Latin transcription of "First Name" and "Last Name" in the Identity Tab of User are not happening properly for Russian name with the Cyrillic alphabet	Manually update Latin transcription value for the First Name" and "Last Name" in the Identity Tab of User and save user.
SMGR-41634	User Self Provisioning	User self-provisioning does not work after providing windows user id if external authentication is configured on System Manager	
SMGR-45884	Directory Synchronization	If the same attribute from AD is mapped to login name and otherEmail and value of the attribute is in mixed case or upper case, then after each sync user shows as Modified.	Map different attributes or update the value in AD to lower case.
SMGR-41380	Software Deployment Manager	Deployment using SDM Client fails if you enter "0.0.0.0" in the field for DNS	Use valid DNS or Use DNS values as “127.0.0.1”
SMGR-43122	Software Deployment Manager	If Session Manager is added with its FQDN in Inventory and subsequently the Host of that Session Manager is added in VM Management and certain edit operations are done, then relationship between Host and VM breaks subsequently	
SMGR-46365	Software Deployment Manager	System Manager deployed in military mode is not able to establish “trust” with the servers deployed in the environment.	
SMGR-43249	User Interface	Last logged Time is not shown properly when login is done using Certificate based authentication.	
SMGR-46088	User Interface	User cannot login to Secondary System Manager Web console UI using EASG after Secondary server is activated.	
SMGR-44904	License Management	Enterprise WebLM configuration, "Usage by WebLM" does not show the local PC time zone.	
SMGR-43445	Communication Manager Management	Shortcut keys provided for certain Tabs on the Communication Manager Management pages are not working.	

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-45752	Communication Manager Management	Announcement backup works only for MD5 and DES combination.	
SMGR-46686	Communication Manager Management	Users with custom role cannot utilize the Import/Export feature on Hunt group form.	
SMGR-46640	Communication Manager Management	Addition of Extension to coverage answer-group failed with Cause: "Maximum no. of extensions for the group exceeded"	
SMGR-45913	Role Management	User gets system error while updating existing role having permissions for group once group is renamed.	First remove the permissions associated with old group from role and update the role by assigning the required permissions.

Known issues and workarounds in System Manager on VMware in Release 7.1.3.1

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

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-39711	Infrastructure	After performing a restore the previously scheduled backup job is getting disabled	Enable the backup job after restore.
SMGR-46090	Infrastructure	editHosts command doesn't allow first character as digit in the FQDN	Add host to hosts file using root user credentials.
SMGR-40569	Infrastructure	Device type entries are missing for Media Gateways when System Manager is upgraded from release 6.3.4 to 7.1 so refresh element operation is not working properly.	
SMGR-40715	Infrastructure	• SSL handshake fails on JMX port connection if revocation checking set to OCSP. • Access to Configure Identity/Trusted Certificates page throws error, if accessed from Home / Services / Inventory / Manage Elements. • System Manager Backup fails.	Revert to OCSP settings back to default settings in Home / Services / Security / Configuration / Security Configuration (Revocation Configuration section.)
SMGR-41360	Infrastructure	In System Manager 7.1.x.x and Solution Deployment Manager Client 7.1.x.x, while deploying OVA if CLI / UI password of VM includes few special characters such as ',>, <, &,", = then the password will not be set properly for VM after post deployment.	Do not use special characters mentioned in list during deployment. Once deployment successfully completed then reset the password as per requirement.
SMGR-43365	Infrastructure	The changeIPFQDN utility is not working properly when used to modify Default Search List and DNS Server entries in a certain manner.	
SMGR-45124	Infrastructure	Unable to change password from passwordChange page if user id has space at beginning or end	Remove space from user id value and perform change password again.

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-39653	Data Replication Service	Data replication stuck in read for repair if element FQDN length greater than 50 characters	Set the node FQDN value to less than 50 characters
SMGR-28093	Geo Graphic Redundancy	On Primary dashboard, in notification section following message is shown, if GEO reconfiguration is performed from Secondary server after Secondary server activate/de-activate activities. "Restore Data to start synchronization between primary and secondary SMGR"	Please contact Avaya Support Team
SMGR-46088	Geo Graphic Redundancy	Cannot login to secondary server UI using EASG after secondary server is activated.	User other user credentials.
SMGR-44830	Geo Graphic Redundancy	GEO configuration will fail if we set (Maximum Sessions Per User: 1) in session properties	Set Maximum Sessions Per User to 5 (default value) and then perform GEO configuration.
SMGR-25823	Scheduler Management	Scheduled jobs created by a user with "administrative" privileges will start to fail once the scheduled user gets deleted from the system.	Delete the existing jobs and recreate new jobs.
SMGR-46008	User Management	Option " Auto Generate Communication Profile Password" selection does not generate communication password for user in bulk edit user option.	Manually provide communication password
SMGR-45874	User Management	Cannot change the domain of e164 handle using bulk edit operation.	
SMGR-45074	User Management	Additional sip handle gets created for user through user management web services (using replace option) or from UI import (partial/replace options).	Remove additional SIP handle from user.
SMGR-45856	User Management	Latin transcription of "First Name" and "Last Name" in the Identity Tab of User are not happening properly for Russian name with the Cyrillic alphabet	Manually update Latin transcription value for the First Name" and "Last Name" in the Identity Tab of User and save user.
SMGR-41634	User Self Provisioning	User self-provisioning does not work after providing windows user id if external authentication is configured on System Manager	
SMGR-45884	Directory Synchronizatio n	If the same attribute from AD is mapped to login name and otherEmail and value of the attribute is in mixed case or upper case, then after each sync user shows as Modified.	Map different attributes or update the value in AD to lower case.
SMGR-41380	Software Deployment Manager	Deployment using SDM Client fails if you enter "0.0.0.0" in the field for DNS	Use valid DNS or Use DNS values as “127.0.0.1”
SMGR-43122	Software Deployment Manager	If Session Manager is added with its FQDN in Inventory and subsequently the Host of that Session Manager is added in VM Management and certain edit operations are done, then relationship between Host and VM breaks subsequently	

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-31321	Software Deployment Manager	Upgrades not working if software library with HTTP protocol is on a Linux system	
SMGR-40390	Software Deployment Manager	Company ID under user setting for upgrade management get blank from after the upgrade in some scenarios.	Configure Company ID under user setting for upgrade management and continue upgrade management activities.
SMGR-43249	User Interface	Last logged Time is not shown properly when login is done using Certificate based authentication.	
SMGR-44904	License Management	Enterprise WebLM configuration, "Usage by WebLM" does not show the local PC time zone.	
SMGR-43445	Communication Manager Management	Shortcut keys provided for certain Tabs on the Communication Manager Management pages are not working.	
SMGR-45926	Communication Manager Management	Using IE, changes are not getting committed after Edit/Add hunt group from Home / Elements / Communication Manager / Groups / Hunt Group page	User Firefox to perform these activities.
SMGR-45752	Communication Manager Management	Announcement backup works only for MD5 and DES combination.	
SMGR-46021	Report Management	Unable to create and delete reports using custom role.	Use user having system admin role to perform the activity.
SMGR-45490	Routing Management	Adaptation filter option is not working properly in some scenarios.	
SMGR-45913	Role Management	User gets system error while updating existing role having permissions for group once group is renamed.	First remove the permissions associated with old group from role and update the role by assigning the required permissions.
SMGR-45020	Data Migration	Upgrade of System Manger to 7.1 fails in certain scenarios due to updating VFQDN value from backup on system if installed system has different VFQDM value.	User the VFQDN value of existing system during 7.1 installation and perform upgrade again.

Known issues and workarounds in System Manager on VMware in Release 7.1.3

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

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-39711	Infrastructure	After performing a restore the previously scheduled backup job is getting disabled	Enable the backup job after restore.
SMGR-40569	Infrastructure	Device type entries are missing for Media Gateways when System Manager is upgraded from release 6.3.4 to 7.1 so	

ID	Minimum conditions	Visible symptoms	Workaround
		refresh element operation is not working properly.	
SMGR-40715	Infrastructure	• SSL handshake fails on JMX port connection if revocation checking set to OCSP. • Access to Configure Identity/Trusted Certificates page throws error, if accessed from Home / Services / Inventory / Manage Elements. • System Manager Backup fails.	Revert to OCSP settings back to default settings in Home / Services / Security / Configuration / Security Configuration (Revocation Configuration section.)
SMGR-41360	Infrastructure	In System Manager 7.1.x.x and Solution Deployment Manager Client 7.1.x.x, while deploying OVA if CLI / UI password of VM includes few special characters such as ',>, <, &,", = then the password will not be set properly for VM after post deployment.	Do not use special characters mentioned in list during deployment. Once deployment successfully completed then reset the password as per requirement.
SMGR-43365	Infrastructure	The changeIPFQDN utility is not working properly when used to modify Default Search List and DNS Server entries in a certain manner.	
SMGR-39653	Data Replication Service	Data replication stuck in read for repair if element FQDN length greater than 50 characters	Set the node FQDN value to less than 50 characters
SMGR-28093	Geo Graphic Redundancy	On Primary dashboard, in notification section following message is shown, if GEO reconfiguration is performed from Secondary server after Secondary server activate/de-activate activities. "Restore Data to start synchronization between primary and secondary SMGR"	Please contact Avaya Support Team
SMGR-25823	Scheduler Management	Scheduled jobs created by a user with "administrative" privileges will start to fail once the scheduled user gets deleted from the system.	Delete the existing jobs and recreate new jobs.
SMGR-41634	User Self Provisioning	User self-provisioning does not work after providing windows user id if external authentication is configured on System Manager	
SMGR-41380	Software Deployment Manager	Deployment using SDM Client fails if you enter "0.0.0.0" in the field for DNS	Use valid DNS or Use DNS values as “127.0.0.1”
SMGR-43122	Software Deployment Manager	If Session Manager is added with its FQDN in Inventory and subsequently the Host of that Session Manager is added in VM Management and certain edit operations are done, then relationship between Host and VM breaks subsequently	
SMGR-31321	Software Deployment Manager	Upgrades not working if software library with HTTP protocol is on a Linux system	
SMGR-43168	Data Migration Utility	Data Migration Utility does not check if patch (Service Pack or Feature Pack) is already installed on top 7.1 OVA.	

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-43249	User Interface	Last logged Time is not shown properly when login is done using Certificate based authentication.	
SMGR-43407	Report Management	Export of Reports from System Manager to a SFTP Server is not working.	
SMGR-43445	Communication Manager Management	Shortcut keys provided for certain Tabs on the Communication Manager Management pages are not working	

Known issues and workarounds in System Manager on VMware in Release 7.1.2

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

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-39711	Infrastructure	After performing a restore the previously scheduled backup job is getting disabled	Enable the backup job after restore.
SMGR-40569	Infrastructure	Device type entries are missing for Media Gateways when System Manager is upgraded from release 6.3.4 to 7.1 so refresh element operation is not working properly.	
SMGR-40715	Infrastructure	• SSL handshake fails on JMX port connection if revocation checking set to OCSP. • Access to Configure Identity/Trusted Certificates page throws error, if accessed from Home / Services / Inventory / Manage Elements. • System Manager Backup fails.	Revert to OCSP settings back to default settings in Home / Services / Security / Configuration / Security Configuration (Revocation Configuration section.)
SMGR-41360	Infrastructure	In System Manager 7.1.x.x and Solution Deployment Manager Client 7.1.x.x, while deploying OVA if CLI / UI password of VM includes few special characters such as ',>, <, &,'', = then the password will not be set properly for VM after post deployment.	Do not use special characters mentioned in list during deployment. Once deployment successfully completed then reset the password as per requirement.
SMGR-43365	Infrastructure	The changeIPFQDN utility is not working properly when used to modify Default Search List and DNS Server entries in a certain manner.	
SMGR-43579	Infrastructure	"changeVFQDN" does not update /etc/hosts file with new VFQDN value, which further causes issue with GEO configuration or Data Replication Issue.	Update new VFQDN value in /etc/hosts and reboot system.
SMGR-41117	Alarm Management	Invalid alarm “Default ASG Auth file found on System Manager alarm” getting generated	
SMGR-39653	Data Replication Service	Data replication stuck in read for repair if element FQDN length greater than 50 characters	Set the node FQDN value to less than 50 characters
SMGR-28093	Geo Graphic Redundancy	On Primary dashboard, in notification section following message is shown, if GEO reconfiguration is performed from Secondary server after Secondary server activate/de-activate activities.	Please contact Avaya Support Team

ID	Minimum conditions	Visible symptoms	Workaround
		"Restore Data to start synchronization between primary and secondary SMGR"	
SMGR-25823	Scheduler Management	Scheduled jobs created by a user with "administrative" privileges will start to fail once the scheduled user gets deleted from the system.	Delete the existing jobs and recreate new jobs.
SMGR-41580	User Management	"Subject Common Name -CN" gets removed if other options from left panel are selected on Provision User Certificate Authentication page.	
SMGR-43352	User Management	Change in Presence/IM Domain using "Bulk Edit Users" does not update xmpp handle in associated user's Contact Address.	Change the Presence/IM Domain for user from Manage Users.
SMGR-41621	User Self Provisioning	After Certification authentication fails for self-provisioning then fall back option does not work with normal login credentials	
SMGR-41634	User Self Provisioning	User self-provisioning does not work after providing windows user id if external authentication is configured on System Manager	
SMGR-41380	Software Deployment Manager	Deployment using SDM Client fails if you enter "0.0.0.0" in the field for DNS	Use valid DNS or Use DNS values as “127.0.0.1”
SMGR-43122	Software Deployment Manager	If Session Manager is added with its FQDN in Inventory and subsequently the Host of that Session Manager is added in VM Management and certain edit operations are done, then relationship between Host and VM breaks subsequently	
SMGR-31321	Software Deployment Manager	Upgrades not working if software library with HTTP protocol is on a Linux system	
SMGR-43168	Data Migration Utility	Data Migration Utility does not check if patch (Service Pack or Feature Pack) is already installed on top 7.1 OVA.	
SMGR-43249	User Interface	Last logged Time is not shown properly when login is done using Certificate based authentication.	
SMGR-43351	Certificate Management	Validity is set to 3 years if new CA is created from Certificate Management.	Create CA from command line interface using command “CreateCA”.
SMGR-43407	Report Management	Export of Reports from System Manager to a SFTP Server is not working.	
SMGR-43445	Communication Manager Management	Shortcut keys provided for certain Tabs on the Communication Manager Management pages are not working	

Known issues and workarounds in System Manager on VMware in Release 7.1.1.1

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

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-41490	User Management	User created with UPR does not get Presence handle even if presence domain is assigned in UPR.	
SMGR-41050	Software Upgrade Management	SMGR patch state shows pending even if it got committed	
SMGR-41432	SMGR:GR:UI	Contacts tab taking more than 2 Mins to display contacts if user has more than 20 contacts.	
SMGR-41559	Software Upgrade Management	On WebLM, if user-initiated trust establishment job, then Refresh Element job is getting performed automatically after trust.	
SMGR-41505	Software Upgrade Management	SDM missing vCenter VM's.	
SMGR-41485	Software Upgrade Management	While patch update is in progress, the Current Action Status column appears blank.	
SMGR-41192	Software Upgrade Management	Upgrade failed from R7.0.1.3 to R7.1.1 during commit, due to less hard disk space.	
SMGR-41275	Infrastructure	Not able to view Security link with user assigned with custom role in MUDG enabled SMGR	
SMGR-41565	Software Upgrade Management	Last Action status missing information	
SMGR-41564	Software Upgrade Management	Session Manager patch rollback fails.	
SMGR-41560	Software Upgrade Management	Analyze job performed for element, but in the GUI, it shows Refresh Element job completed successfully after refresh.	
SMGR-41557	Software Upgrade Management	WebLM upgrade failed from R7.0.1.3 to R7.1.1.	
SMGR-41486	Software Upgrade Management	On R7.1.1 SMGR SDM-SUM: CM Refresh Element job failed if it is upgraded from R7.0.1.3 to R7.1.1 and then performed Rollback operation.	
SMGR-41463	Software Upgrade Management	SMGR CLI login doesn't work while updating patch through SDM Client	
SMGR-41340	Alarming Management	Alarm Purging is not working	
SMGR-41307	Backup and Restore Management	CM licenses not restored on backup and restore operation	
SMGR-41453	Infrastructure	java.security.AccessControlException: access denied on	

ID	Minimum conditions	Visible symptoms	Workaround
		Bulk Edit User with Breeze Profile	
SMGR-41433	License Management	Nutanix KVM 7.1.1 Avaya Utility server failed to retrieve license from SMGR WebLM	
SMGR-41323	License Management	WebLM library generating core dump	
SMGR-41212	SDM:ClientInfrastructure	Avaya logo and product name (excluding version number) is missing in the login page of SMGR and product name from SDM Client.	
SMGR-40831	User Interface	Feature Pack line shall be on new line in About page	

Known issues and workarounds in System Manager on VMware in Release 7.1.1

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

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-41490	User Management	User created with UPR does not get Presence handle even if presence domain is assigned in UPR.	
SMGR-41050	Software Upgrade Management	SMGR patch state shows pending even if it got committed	
SMGR-41432	SMGR:GR:UI	Contacts tab taking more than 2 Mins to display contacts if user has more than 20 contacts.	
SMGR-41559	Software Upgrade Management	On WebLM, if user-initiated trust establishment job, then Refresh Element job is getting performed automatically after trust.	
SMGR-41505	Software Upgrade Management	SDM missing vCenter VM’s.	
SMGR-41485	Software Upgrade Management	While patch update is in progress, the Current Action Status column appears blank.	
SMGR-41192	Software Upgrade Management	Upgrade failed from R7.0.1.3 to R7.1.1 during commit, due to less hard disk space.	
SMGR-41275	Infrastructure	Not able to view Security link with user assigned with custom role in MUDG enabled SMGR	
SMGR-41565	Software Upgrade Management	Last Action status missing information	
SMGR-41564	Software Upgrade Management	Session Manager patch rollback fails.	
SMGR-41560	Software Upgrade Management	Analyze job performed for element, but in the GUI, it shows Refresh Element job completed successfully after refresh.	
SMGR-41557	Software Upgrade Management	WebLM upgrade failed from R7.0.1.3 to R7.1.1.	
SMGR-41486	Software Upgrade	On R7.1.1 SMGR SDM-SUM: CM Refresh	

ID	Minimum conditions	Visible symptoms	Workaround
	Management	Element job failed if it is upgraded from R7.0.1.3 to R7.1.1 and then performed Rollback operation.	
SMGR-41463	Software Upgrade Management	SMGR CLI login doesn't work while updating patch through SDM Client	
SMGR-41340	Alarming Management	Alarm Purging is not working	
SMGR-41307	Backup and Restore Management	CM licenses not restored on backup and restore operation	
SMGR-41453	Infrastructure	java.security.AccessControlException: access denied on Bulk Edit User with Breeze Profile	
SMGR-41433	License Management	Nutanix KVM 7.1.1 Avaya Utility server failed to retrieve license from SMGR WebLM	
SMGR-41323	License Management	WebLM library generating core dump	
SMGR-41212	SDM:ClientInfrastructure	Avaya logo and product name (excluding version number) is missing in the login page of SMGR and product name from SDM Client.	
SMGR-40831	User Interface	Feature Pack line shall be on new line in About page	

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
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-40602	User Management	Time zone value associated with user (identity page) not getting populated properly after DST change.	Restart JBoss service

ID	Minimum conditions	Visible symptoms	Workaround
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-39711	Backup and Restore	After Restore earlier scheduled backup job is getting disabled.	Enable the scheduled backup.
SMGR-40715	Security Management	Accessing Home / Services / Inventory / Manage Elements/System Manager -> Configure Identity Certificates or / Configure Trusted Certificates page throws error	➢ Go to Home / Services / Security / Configuration / Security Configuration ➢ Refer section “Revocation Configuration” ➢ Set the settings back to default values i.e. set “Revocation Type” to “BOTH” and “Revocation Type Preference” to “OCSP”.
SMGR-41419	Installation /Upgrade	Upgrade to System manager 7.1 with new FQDN will fail if older system manager release has third-party certificate installed	If earlier System Manager release has 3rd party certificates installed, then upgrade to System Manger 7.1 should be done with same network parameters (IP Address/FQDN and VFQDN) of earlier system manager release.

Solution Deployment Manager Adopter Matrix

Solution Deployment Manager Adopter Matrix	Adopting Product (System Manager Release 7.1.3)												
System Manager Solution Deployment Manager - Centralized	Appliance Virtualization Platform	System Manager	Session Manager	Communication Manager	CM Adjuncts (MM, TN Boards, Gateways)	Branch Session Manager	Utility Services	CM Messaging	Breeze	Secure Access Gateway	WebLM	Application Enablement Services	Avaya Aura®
Functionality									(w/ Presence Snap-in)				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
OVA Deployment R 7.1R (Configuration and Footprint)	n/a	N	Y	Y	n/a	Y	Y	n/a	n/a	n/a	n/a	n/a	n/a
Patching Deployment (hotfixes)	Y [Other than AVP hosting System Manager]	N	Y	Y	n/a	Y	Y	Y	N	N	N	Y	N
Custom Patching Deployment	n/a	N	Y	Y	n/a	Y	Y	Y	N	N	Y [7.0.1 onwards]	Y	N
Service/Feature Pack Deployment	Y [Other than AVP hosting System Manager]	N	Y	Y	n/a	Y	Y	Y	N	N	N	Y	N

Solution Deployment Manager Adopter Matrix	**Adopting Product (System Manager Release 7.1.3)**												
System Manager Solution Deployment Manager - Centralized	Appliance Virtualization Platform	System Manager	Session Manager	Communication Manager	CM Adjuncts (MM, TN Boards, Gateways)	Branch Session Manager	Utility Services	CM Messaging	Breeze	Secure Access Gateway	WebLM	Application Enablement Services	Avaya Aura®
Functionality									(w/ Presence Snap-in)				Media Server
Automated Migrations R7.x to R7.1 (analysis and pre-upgrade checks) [Target Platform: AVP / customer VMware]	Y [Other than AVP hosting System Manager]	Y	Y	Y	n/a [Covered as Firmware Updates]	Y	Y	Y	N (Breeze Upgrade Supported from Breeze 3.3 Onwards)	N	Y	Y	N
Automated Migrations R6.x to R7.0/7.1 (analysis and pre-upgrade checks)	n/a	N	Y[1]	Y	n/a [Covered as Firmware Updates]	Y	Y	Y	N	N	N	N	N
Automated Migrations R6.x to 7.0.0.x/ 7.0.x/7.1 [Source Platform: System Platform] [Target Platform: AVP / customer VMware]	n/a	N [Only using SDM Client]	Y[1] [Bare Metal which is not on SP]	Y	n/a [Covered as Firmware Updates]	Y	Y	Y	N	N	N	N	N

Solution Deployment Manager Adopter Matrix	**Adopting Product (System Manager Release 7.1.3)**												
System Manager Solution Deployment Manager - Centralized									Breeze				Avaya Aura®
Functionality	Appliance Virtualization Platform	System Manager	Session Manager	Communication Manager	CM Adjuncts (MM, TN Boards, Gateways)	Branch Session Manager	Utility Services	CM Messaging	(w/ Presence Snap-in)	Secure Access Gateway	WebLM	Application Enablement Services	Media Server
Automated Migrations R6.x to 7.0.x/7.1 [Source Platform: System Platform] [Target Platform: AVP / customer VMware]	n/a	N	Y[1] [Bare Metal which is not on SP]	Y	n/a [Covered as Firmware Updates]	Y	Y	Y	N	N	N	N	N
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 Available	n/a	Y	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Create Software Library	n/a	Y	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Solution Deployment Manager Adopter Matrix	**Adopting Product (System Manager Release 7.1.3)**												
System Manager Solution Deployment Manager - Centralized	Appliance Virtualization Platform	System Manager	Session Manager	Communication Manager	CM Adjuncts (MM, TN Boards, Gateways)	Branch Session Manager	Utility Services	CM Messaging	Breeze	Secure Access Gateway	WebLM	Application Enablement Services	Avaya Aura®
Functionality									(w/ Presence Snap-in)				Media Server
Support for changing VM Flexible Footprint	n/a	Y [Only using SDM Client]	Y	Y	n/a	Y	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

Deployment and Upgrade Guides:

Products	**Deployment and Upgrade Guides**
Appliance Virtualization Platform	Migrating and Installing Appliance Virtualization Platform
Session Manager	Deploying Avaya Aura® Session Manager Upgrading Avaya Aura® Session Manager
Communication Manager	Deploying Avaya Aura® Communication Manager Upgrading Avaya Aura® Communication Manager
CM Adjuncts (MM, TN Boards, Gateways)	Deploying and Upgrading G430 Branch Gateways Deploying and Upgrading G450 Branch Gateways
Branch Session Manager	Deploying Avaya Aura® Branch Session Manager
Utility Services	Deploying Avaya Aura® Utility Services
CM Messaging	Deploying Avaya Aura® Communication Manager Messaging
Breeze (w/ Presence Snap-in)	Deploying Avaya Breeze$^{\text{TM}}$ (Release 3.1) Quick start guide for Deploying Avaya Breeze$^{\text{TM}}$ snap-ins (Release 3.1)
Secure Access Gateway	Deploying Secure Access Link Gateway using Avaya Aura® System Manager in the VMware Virtualized Environment (Release 2.5)
Application Enablement Services	Deploying Avaya Aura® Application Enablement Services in Virtualized Environment

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.x for upgrading Aura applications using Solution Deployment Manager (Solution Deployment Manager)
Upgrading Avaya Aura® applications to Release 7.1.x 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 7.1.2.0

Patches in 7.1.x are cumulative. Only the latest supported cumulative update of a Generally Available release will be available for download from the Avaya Support/PLDS website.

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

It is important that any GA patches available at a later date be applied as part of all 7.1.x deployments.

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

Presence Services 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 7.1.2.0

Filename	Modification time stamp	File size	Version number
PresenceServices-Bundle-7.1.2.0.285.zip **(PLDS ID PS070102000)**		166 MB	PresenceServices-7.1.2.0.214.svar

Installing the release

Refer to chapters 5 and 6 of the customer documentation for instructions related to the deployment of the PS 7.1.2.0 release.

Troubleshooting the installation

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

Restoring software to previous version

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 7.1.2 release from a PS 6.2.X release

Changes Affecting Migrations to 7.1.2

Avaya Aura® Presence Services 7.X introduces significant changes that affect migrations to PS 7.1.2:

- **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 to enable presence for a user.
- 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 7.1.2.0, 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 7.1.2. Applications must use the Presence Services 7.1.2 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 7.1.2 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 that the administrator’s 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 7.1.2. The migration script can be downloaded from the Avaya Support site (PLDS ID = PS070000001).

  To run Presence Services 7.1.2.0, migrations should be performed using the following method:

  - Presence Services 7.1.2 Snap-in on Breeze 3.4:

  Download and install the Avaya Aura Presence Services 7.1.2.0 Software (PS-7.1.2.0.214.svar) on a Breeze 3.4 Core cluster.

  Note: At the time general availability of Presence Services 7.1.2.0 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 7.1.2.0 deployments.

  Migrations to release 7.1.2.0 are supported from the following releases only:

Minimum required versions by Release

Release	Minimum Required Version
Avaya Aura® Presence Services 7.0	PresenceServices-7.0.0.0.1395.svar + any additional patch(es)
Avaya Aura® Presence Services 7.0 Service Pack 1	PresenceServices-7.0.0.1.1528.svar + any additional patch(es)
Avaya Aura® Presence Services 7.0 Feature Pack 1	PresenceServices-7.0.1.0.871.svar + any additional patch(es)
Avaya Aura® Presence Services 7.1	PresenceServices-7.1.0.0.614.svar + any additional patch(es)

Upgrade References to Presence Services 7.1.2.0

Upgrade Quick Reference	Download	Prerequisite Downloads
Presence Services Customer Documentation	PresenceServices-Bundle-7.1.2.0.285.zip (PLDS ID: PS070102000)	**Breeze 3.4 Platform OVA – PS 7.1.2 is only compatible with Breeze 3.3.1.1 or Breeze 3.4 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	3.4	3.3.1.1	M
Avaya Aura® System Manager	7.1.2.0 and 7.1.3.0	7.1.2.0	M
Avaya Aura® Session Manager	7.1.2.0 and 7.1.3.0	7.1.2.0	M
Avaya Aura® Communication Manager	7.1.2.0 and 7.1.3.0	7.1.0.0	O
Avaya Appliance Virtualization Platform	7.1.2.0 and 7.1.3.0	7.1.0.0	O
Avaya Aura® Application Enablement Services	7.1.2.0 and 7.1.3.0	7.1.0.0	O
Avaya Multimedia Messaging	3.3.0.0	3.3.0.0	O
Avaya one-X® Client Enablement Services	6.2.5 + Patch 3	6.2.5 + Patch 3	O
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-7.1.2.0.182.zip	7.1.2	PS 7.1.2, PS 7.1.0 and PS 7.0.1
PresenceServices-LPS-SDK-7.1.0.0.556.zip	7.1.0	PS 7.1 and PS 7.0.1

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

Functionality not supported in Presence Services 7.1.x.x

Avaya Multimedia Messaging (AMM 2.1) XMPP federation is not supported in Presence services 7.X. AMM 3.X 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 7.1.2

The following table lists enhancements in this release:

Enhancement	Description
PS Connector support for a privileged user	This feature provides an override mechanism for Access Control List (ACL) enabled solutions. This feature introduces the concept of a privileged user (attribute set by system administrator). A privileged user can see other users' presence states without their explicit permission even if the ACL feature is enabled. This capability is only accessible through the PS connector's JAVA API. For compliance purposes this feature is not available via the PS REST, SIP and XMPP interfaces.
REST API support for Self-Identity	This feature updates the PS REST API to include specifying identity using the "self" keyword. This feature was implemented to make the PS REST API simpler to use and saves the clients from having to look up all the details normally included in messages sent to PS. This feature is only applicable to developers creating web client software using the PS REST API.
Zang Federation: Capability to send an SMS via the PS REST APIs	This feature allows Aura users exchange Instant Messages (as a SMS) to any mobile number. A Zang number can be associated with an Aura User's profile and allows the two-way exchange of messages between mobile users and Aura users. The Zang number should be provisioned as a communication address in user's communication profile on SMGR as a handle of type="Other SIP" with the Zang number as "handle" and "zang.io" as the domain. This feature is also available via the PS REST API.
PS support for KVM deployments	It is now possible to deploy PS/Breeze on KVM (Kernel-based Virtual Machine).
PS support for JITC compliance	It is now possible to deploy PS/Breeze in a hardened secure mode which meets the JITC (Joint Interoperability Test Command) security standards. This feature is intended for deployments in the government space and several PS features have been disabled when PS is deployed in JITC mode (REST I/F and XMPP client I/F are disabled). PS 7.1.2 must be deployed using Breeze 3.4.0.1 to enable JITC mode.

What's new in Presence Services Release 7.1

The following table lists enhancements in this release:

Enhancement	Description
Support for federation	PS 7.1 now supports federation with on premise Microsoft Skype for Business

Enhancement	Description
with 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 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.
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 can 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 7.1.2

The following issues have been resolved in cumulative updates to the 7.1.2 release:

ID	Minimum conditions	Visible symptoms	Release found in
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.	7.1.0
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 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	7.1.0
PSNG-4079	Delete a PS element in SMGR it reports an	When attempting to delete a PS element in SMGR it reports the error that "unable to delete an element	7.1.0

ID	Minimum conditions	Visible symptoms	Release found in
	error	that is assigned to a user", however the element is only assigned to a UPR.	
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.	7.1.0

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 to provide service.	7.0.0.0
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,	7.0.0.0

ID	Minimum conditions	Visible symptoms	Release found in
		and watchers do not see the updated state. This only happens with the first change. All subsequent changes by User A are reflected properly. Additionally, this only happens with the first change by any of the users on the system. As soon as a single user makes a change all subsequent changes by all other users work properly.	
PSNG-1452	When the IP Address has changed in a EDP Cluster the Admin must resubmit the associated Presence Element in the Manage Elements page	When the EDP Cluster IP address changes the PS on CE Manage Element must be resubmitted. The Admin will see text in red on the Manage Element edit page for that element that indicates the IP address is "updated".	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 Presence Services Release 7.1.2.0

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

ID	Minimum conditions	Visible symptoms	Workaround
Zephyr-58971	The PS/Breeze application is deployed in JITC/Hardened mode.	High Availability DB fails to startup after importing 3rd party certs and enabling FIPS mode	There is no work-around for this issue. This problem is fixed in Breeze 3.4.0.1 which will be delivered in April 2018. This problem will not occur if PS 7.1.2 is deployed on Breeze 3.4.0.1
PSNG-4154	Avaya Aura is federated with Microsoft Lync	Lync/S4B federation: Hybrid user: Aura user can't send IM to MS device of hybrid user (Avaya phone on desktop and MS messaging client)	There is no work-around for this issue. This problem is fixed in PS 8.0.0.0.
PSNG-4137	Avaya Aura is federated with Microsoft Lync	Lync/S4B federation: Hybrid user: Aura manual states removed by MS automatic states.	There is no work-around for this issue. This problem is fixed in PS 8.0.0.0.
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-	Clear Logs in the EDP EM for	The “Clear Logs” button on the EDP EM does not have any effect	There is no workaround for this

ID	Minimum conditions	Visible symptoms	Workaround
1379	Presence Services does not clear logs	on the ps.log file.	issue.
Note		After an Avaya contact is removed from a XMPP federated client, presence does not render if the Avaya contact is re-added to the federated user.	Use either of the two solutions: 1. Toggle the favorite flag for the federated user in the Avaya client 2. Logout and log back in to the Avaya client

Note: The Presence Services Admin Web GUI, as shown below, is disabled by default in PS 7.1.2.

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

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
ZEPHYR-52087	Breeze 3.2 deployed with System Manager 7.1	The Encryption algorithm for the password stored on the cluster database backup configuration page changed between R3.2.x and R3.3.x of Avaya Breeze ™. Backup operations will no longer work on 3.2.x Breeze nodes post Avaya Aura ® System Manager upgrade to Release 7.1.	If the data stored within the Breeze cluster database for R3.2.x is to be retained, the cluster database backup operation must be performed prior to upgrade of the Avaya Aura ® System Manager to Release 7.1. See “Backing up a Cluster”, Chapter 3 in Administering Avaya Breeze™ for information on how to complete this operation.
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 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.

ID	Minimum conditions	Visible symptoms	Workaround
PSNG-2630	Avaya Aura is federated with Microsoft Lync	There is no message notification when Lync sends chat message to 1XC in DND state,	There is no work-around for this issue.
PSNG-1379	Clear Logs in the EDP EM for Presence Services does not clear logs	The “Clear Logs” button on the EDP EM does not have any effect on the ps.log file.	There is no workaround for this issue.
Note		After an Avaya contact is removed from a XMPP federated client, presence does not render if the Avaya contact is re-added to the federated user.	Use either of the two solutions: 1. Toggle the favorite flag for the federated user in the Avaya client. 2. Logout and log back in to the Avaya client.

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.

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.

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

Refer to the Deploying Avaya Aura® Application Enablement Services in Virtualized Environment or Deploying Avaya Aura® Application Enablement Services in a Software-Only Environment 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, 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. 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.

Installation of Avaya Aura® Application Enablement Services 7.1.2

Important Note: Avaya Aura® Application Enablement Services 7.1.2 requires a patch to be applied to the system after fresh installations as well as upgrades. Please refer to PSN020332u for complete patch installation details.

PLDS Product ID	Download Title and Description
AES00000608	Avaya Aura® Application Enablement Services Software Only 7.1.2 Description: Avaya Aura® Application Enablement Services Software Only 7.1.2 File Name: swonly-7.1.2.0.0.3-20171109.iso File Size: 360.34 MB (368,986 KB) MD5 Checksum: d9c0afc33a9b7796d11b58fe33526e49

PLDS Product ID	Download Title and Description
AES00000609	Avaya Aura® AE Services 7.1.2 Aura® OVA Media Description: Avaya Aura® Application Enablement Services 7.1.2 Aura® OVA Media File Name: AES-7.1.2.0.0.3.20171110-e55-00.ova File Size: 1,682.37 MB (1,722,750 KB) MD5 Checksum: a728dacaf716381daaf616540b8dc433
AES00000610	Avaya Aura® Application Enablement Services 7.1.2 KVM Support Description: Avaya Aura® Application Enablement Services 7.1.2 KVM Support File Name: AES-7.1.2.0.0.3.20171110-kvm-001.ova File Size: 1,676.9 MB (1,717,150 KB) MD5 Checksum: 47818c691f20476908c27e3530f42c05
AES00000612	Avaya Aura® Application Enablement Services 7.1.2 RPM-only Installer To install the Avaya Aura® Application Enablement Services 7.1.2 RPM-only Installer, the following installation order needs to be followed (depending on starting with 7.1 or 7.1.1): Starting from AE Services 7.1: Before performing an upgrade or update, a backup of the AE Services data should be performed. 1. Avaya Aura® AE Services 7.1 Aura® Bundled Media VMware Template OVA or Avaya Aura® AE Services Software Only 7.1 is installed. 2. Avaya Aura® AE Services 7.1 Linux Security Update Patch 1. 3. Avaya Aura® AE Services 7.1.1 RPM-only Installer. 4. Avaya Aura® AE Services 7.1.1 Linux Security Update Patch 1. Starting from AE Services 7.1.1: Before performing an upgrade or update, a backup of the AE Services data should be performed. 1. Avaya Aura® AE Services 7.1.1 Aura® VMware Template OVA or Avaya Aura® AE Services Software Only 7.1.1 or Avaya Aura® AE Services KVM OVA 7.1.1 is installed 2. Avaya Aura® AE Services 7.1.1 Linux Security Update Patch 1 File Name: aesvcs-7.1.2.0.0.3-featurepack.bin File Size: 150.92 MB (154,538.2 KB) MD5 Checksum: 908b250423e129d67ff779e2a95272e1

Installation of Avaya Aura® Application Enablement Services 7.1.3

Important Notes:

- **Upgrade from an older AES version to AES 7.1.3 through the RPM-only installer is not supported**

AES 7.1.3 is available in the three offers mentioned in the table below. All installations of AES 7.1.3 need to be fresh deployments. The AE Services 7.1.3 restore tool (i.e., Maintenance > Server Data > Restore) should be applied to restore data from an older version of AES to AES 7.1.3.

- **After installing AES 7.1.3 you must install the following updates:**
  - **AES 7.1.3 Linux Security Update Patch 1**
  - **AES 7.1.3.0.1 Super Patch**

- **The following updates are available and should be applied on AES 7.1.3 that has been previously updated with AES 7.1.3 Linux Security Update Patch 1 and AES 7.1.3.0.1 Super Patch. The order of application of these patches should be maintained.**
  - **AES 7.1.3 Linux Security Update Patch 2**
  - **AES 7.1.3.0.2 Super Patch**

Installation of Avaya Aura® Application Enablement Services 7.1.3.1

AES 7.1.3.1 is available as a binary file and needs to be installed over AES 7.1.3

- **After installing AES 7.1.3.1 you must install the following update:**
    - **AES 7.1.3.1.1 Super Patch**

Installation of Avaya Aura® Application Enablement Services 7.1.3.2

- AES 7.1.3.2 is available as a binary file and needs to be installed over AES 7.1.3 OR over AES 7.1.3.1.
    - **Before installing AES 7.1.3.2 you must install LSU 3:**

      Avaya Aura® AE Services 7.1.3 Linux Security Update Patch 3
      File Name: 713_LSUPatch3.bin

Installation of Avaya Aura® Application Enablement Services 7.1.3.3

- AES 7.1.3.3 is available as a binary file and needs to be installed over AES 7.1.3 OR over AES 7.1.3.1.or over AES 7.1.3.2

Installation of Avaya Aura® Application Enablement Services 7.1.3.4

- AES 7.1.3.4 is available as a binary file and needs to be installed over any of the following releases
    - AES 7.1.3
    - AES 7.1.3.1
    - AES 7.1.3.2
    - AES 7.1.3.3

- AES 7.1.3 LSU 5 is available as a binary file and can be installed over AES 7.1.3.4

Installation of Avaya Aura® Application Enablement Services 7.1.3.5

- AES 7.1.3.5 is available as a binary file and needs to be installed over any of the following releases
    - AES 7.1.3
    - AES 7.1.3.1
    - AES 7.1.3.2
    - AES 7.1.3.3
    - AES 7.1.3.4

Installation of Avaya Aura® Application Enablement Services 7.1.3.6

- AES 7.1.3.6 is available as a binary file and needs to be installed over any of the following releases
    - AES 7.1.3
    - AES 7.1.3.5

CRITICAL NOTE : Application of Linux Security Updates (LSU 1 – 7) MUST be done prior to updating to 7.1.3.6. due to a dependency on the updated php rpm in 7.1.3.6. Existing LSUs have an older version of this php rpm and will downgrade the php rpm version if applied after 7.1.3.6.

If an LSU is inadvertently applied after 7.1.3.6, leave the LSU installed, uninstall 7.1.3.6 and reinstall 7.1.3.6 to recover to the latest php rpm version.

Avaya Aura® AE Services 7.1.3 Linux Security Update Patch 8 (LSU 8) with additional security mitigation will be available with a target GA of early May 2020. It will not have the same restrictions as earlier LSUs with respect to order of application.

PSN020334u - Avaya Aura® Application Enablement (AE) Services 7.1.x Linux Security Updates will be updated when LSU 8 is available.

Installation of Avaya Aura® Application Enablement Services 7.1.3.7

- AES 7.1.3.7 is available as a binary file and needs to be installed over any of the following releases
  - AES 7.1.3
  - AES 7.1.3.5
  - AES 7.1.3.6

Installation of Avaya Aura® Application Enablement Services 7.1.3.8

- AES 7.1.3.8 is available as a binary file and needs to be installed over any of the following releases
  - AES 7.1.3
  - AES 7.1.3.6
  - AES 7.1.3.7

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

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

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

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

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

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

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

Upgrading to AE Services 7.1.x

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. 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. 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)

Installation steps for Avaya Aura® Application Enablement Services 7.1.1 RPM-only Installer

To install the Avaya Aura® Application Enablement Services 7.1.1 RPM-only Installer, the following installation order needs to be followed:

Note: Before performing an upgrade or update, a backup of the AE Services data should be performed.

1. Avaya Aura® AE Services 7.1 Aura® Bundled Media VMware Template OVA or Avaya Aura® AE Services Software Only 7.1 is installed
2. Avaya Aura® AE Services 7.1 Linux Security Update Patch 1
3. Avaya Aura® AE Services 7.1.1 RPM-only Installer

   File Name: aesvcs-7.1.1.0.0.5-featurepack.bin using PLDS ID AES00000593

   File Size: 150.62 MB (154,239.68 KB)

   MD5 Checksum: 6888d6e680f3e62bc9d2006fffff612e

Required artifacts for Application Enablement Services Release 7.1.x.x

Required artifacts for Application Enablement Services Release 7.1.3.8

The following section provides Application Enablement Services downloading information

PLDS Product ID	Download Title and Description
AES00000849	Avaya Aura® Application Enablement Services 7.1.3.8 Service Pack File Name: aesvcs-7.1.3.8.0.3-servicepack.bin File Size: 185.81 MB (190276.05 KB) MD5 Checksum: d0994b77c896ab00a1732d9849f05df2 Refer to PCN2066S for details.
AES00000850	Avaya Aura® AE Services 7.1.3 Linux Security Update Patch 10 Refer to PSN020334u for details. File Name: 713_LSUPatch10.bin File Size: 344.62 MB (352899.77 KB) MD5 Checksum: 5f3fc3d6f60251e0fe5d661028102f19

Required artifacts for Application Enablement Services Release 7.1.3.7

The following section provides Application Enablement Services downloading information

PLDS Product ID	Download Title and Description

AES00000846	Avaya Aura® Application Enablement Services 7.1.3.7 Service Pack File Name: aesvcs-7.1.3.7.0.4-servicepack.bin File Size: 185.7 MB (190,157 KB) MD5 Checksum: 79555f345101068004f718a74bfb030c Refer to PCN2066S for details.
AES00000847	Avaya Aura® AE Services 7.1.3 Linux Security Update Patch 9 Refer to PSN020334u for details. File Name: 713_LSUPatch9.bin File Size: 341.49 MB (349,687 KB) MD5 Checksum: 596b4635f85be218a6a8708f6eb04eb2

Required artifacts for Application Enablement Services Release 7.1.3.6

The following section provides Application Enablement Services downloading information

PLDS Product ID	Download Title and Description
AES00000817	Avaya Aura® Application Enablement Services 7.1.3.6 Service Pack File Name: aesvcs-7.1.3.6.0.3-servicepack.bin File Size: 180.28 MB (184,601.9 KB) MD5 Checksum: 689ab7f8224dbc39bdae1f56e4d7a6f3 Refer to PCN2066S for details.

Required artifacts for Application Enablement Services Release 7.1.3.5

The following section provides Application Enablement Services downloading information.

PLDS Product ID	Download Title and Description
AES00000793	Avaya Aura® Application Enablement Services 7.1.3.5 Service Pack File Name: aesvcs-7.1.3.5.0.4-servicepack.bin File Size: 163.33 MB (167,251.9 KB) MD5 Checksum: de8b1a3afbce8fb1ac81cddae62843df Refer to PCN2066S for details.
AES00000791	Avaya Aura® AE Services 7.1.3 Linux Security Update Patch 7 Refer to PSN020334u for details. File Name: 713_LSUPatch7.bin File Size: 314.76 MB (322,323.85 KB) MD5 Checksum: 77242ad2edaf79d17df899dc2b98d0fa

Required artifacts for Application Enablement Services Release 7.1.3.4

The following section provides Application Enablement Services downloading information.

PLDS Product ID	Download Title and Description
AES00000759	Avaya Aura® Application Enablement Services 7.1.3.4 Service Pack

PLDS Product ID	Download Title and Description
	File Name: aesvcs-7.1.3.4.0.6-servicepack.bin File Size: 163.32 MB (167238.79 KB) MD5 Checksum: e5c3b60f7630efae33784c0c0a8c558c Refer to PCN2066S for details.
AES00000760	Avaya Aura® AE Services 7.1.3 Linux Security Update Patch 5 File Name: 713_LSUPatch5.bin File Size: 319.37 MB (327031.11 KB) MD5 Checksum: 7ac5acddc21f55c13ece0f7850987cfb Refer to PSN020334u for details.

Required artifacts for Application Enablement Services Release 7.1.3.3

The following section provides Application Enablement Services downloading information.

PLDS Product ID	Download Title and Description
AES00000725	Avaya Aura® Application Enablement Services 7.1.3.3 Service Pack File Name: aesvcs-7.1.3.3.0.2-servicepack.bin File Size: 154.42 MB (158,131.53 KB) MD5 Checksum: dd6c8ee3ca2c4d322cf5ddc3604eba76

Required artifacts for Application Enablement Services Release 7.1.3.2

The following section provides Application Enablement Services downloading information.

PLDS Product ID	Download Title and Description
AES00000697	Avaya Aura® Application Enablement Services 7.1.3.2 Service Pack File Name: aesvcs-7.1.3.2.0.2-servicepack.bin File Size: 154.41 MB (158,115.85 KB) MD5 Checksum: db364bb35f2c4a0a74d505ebc65053ef
AES00000696	Avaya Aura® AE Services 7.1.3 Linux Security Update Patch 3 File Name: 713_LSUPatch3.bin File Size: 248.24 MB (254,200.88KB) MD5 Checksum: 940bb89d29d0a3eca6fe9b6fb8a65b3d

Required artifacts for Application Enablement Services Release 7.1.3.1

The following section provides Application Enablement Services downloading information.

PLDS Product ID	Download Title and Description
AES00000688	Avaya Aura® Application Enablement Services 7.1.3.1 Service Pack Installer.

PLDS Product ID	Download Title and Description
	File Name: aesvcs-7.1.3.1.0.6-servicepack.bin File Size: 154.4 MB (158103.5 KB) MD5 Checksum: 38205615ba72023a13db2c3928a01b0e

Required artifacts for Application Enablement Services Release 7.1.3.1.1

The following section provides Application Enablement Services downloading information.

PLDS Product ID	Patch Download Title and Description	Description
AES00000689	Avaya Aura® Application Enablement Services 7.1.3.1.1 Super Patch File Name: aesvcs-7.1.3.1.1-superpatch.bin File Size: 6.64 MB (6799.37KB) MD5 Checksum: 0f8b5e4f2a879323ce156d796aa7f598	This Superpatch contains fixes for some vulnerabilities present in AES 7.1.3.1

Required artifacts for Application Enablement Services Release 7.1.3

The following section provides Application Enablement Services downloading information.

PLDS Product ID	Download Title and Description
AES00000637	Avaya Aura® Application Enablement Services Software Only 7.1.3 Description: Avaya Aura® Application Enablement Services Software Only 7.1.3 File Name: swonly-7.1.3.0.0.7-20180301.iso File Size: 368.94 MB (377,796 KB) MD5 Checksum: f314214388117b9a231da6cd2e53b4a0
AES00000638	Avaya Aura® AE Services 7.1.3 Aura® OVA Media Description: Avaya Aura® Application Enablement Services 7.1.3 Aura® OVA Media File Name: 7.1.3.0.0.7.20181127-e55-02.ova * File Size: 2,118.08 MB (2,168,910 KB) MD5 Checksum: 2c5af455be7597e05c6f123b083d8f26 *New OVA re-issued to support the ACP 100 Series 2200GHz CPUs used in Profile 2 and 3 of the server.
AES00000639	Avaya Aura® Application Enablement Services 7.1.3 KVM Support Description: Avaya Aura® Application Enablement Services 7.1.3 KVM Support File Name: AES-7.1.3.0.0.7.20181127-kvm-002.ova * File Size: 2,098.19 MB (2,148,550 KB) MD5 Checksum: 93d53122b83b5ac8722eeda202fdc3d6 *New OVA re-issued to support the ACP 100 Series 2200GHz CPUs used in Profile 2 and 3 of the server.

Required artifacts for Application Enablement Services Release 7.1.3.0.1

The following section provides Application Enablement Services downloading information.

PLDS Product ID	Patch Download Title and Description	Description
AES00000660	Avaya Aura® AE Services 7.1.3.0.1 Super Patch File Name: aesvcs-7.1.3.0.1-superpatch.bin File Size: 110.79 MB (113452.4 KB) MD5 Checksum: cd4dcb3958644b48aa0378f0c5193f6c	This Superpatch contains fixes for some vulnerabilities present in AES 7.1.3. For more details see PSN020351u.
AES00000640	Avaya Aura® AE Services 7.1.3 Linux Security Update Patch 1 File Name: 713_LSUPatch1.bin File Size: 113.93 MB (116,662.22 KB) MD5 Checksum: 75ef1e1e2a50ce73bf9be9182d65716d	AES 7.1.3 LSU 1 includes the Red Hat updates to support mitigation of the Meltdown/Spectre vulnerabilities. However, this has the potential to affect performance – so there is now a small script that allows the setting of kernel options to control how these vulnerabilities are handled. The effect of running the kernel configuration script is both immediate and will persist across reboots. The script should be called from the CLI using the admin user and is called kernel_opts.sh. It has the argument "status" to display the current status of the kernel options, "enable" to enable all flags to provide maximum protection, and "disable" to disable all flags to provide maximum performance.

Required artifacts for Application Enablement Services Release 7.1.3.0.2

The following section provides Application Enablement Services downloading information.

PLDS Product ID	Patch Download Title and Description	Description
AES00000694	Avaya Aura® AE Services 7.1.3.0.2 Super Patch File Name: aesvcs-7.1.3.0.2-superpatch.bin File Size: 62.37 MB (63,862.16 KB) MD5 Checksum: 6a569f280da463aa33fe6535ec056e94	This Superpatch contains fixes for some vulnerabilities present in AES 7.1.3. For more details see PSN020351u.
AES00000695	Avaya Aura® AE Services 7.1.3 Linux Security Update Patch 2 File Name: 713_LSUPatch2.bin File Size: 116.47 MB (119,270.12 KB) MD5 Checksum: 67fa2237188990596e7e03a8653d1d04	Refer to PSN020334u for details.

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

What's new in Application Enablement Services 7.1.3.8

The following table lists enhancements in this release.

Feature	Description

Feature	Description
RPM Upgrade	Tomcat RPM is been upgraded

What’s new in Application Enablement Services 7.1.3.7

The following table lists enhancements in this release.

Feature	Description
N/A	N/A

What’s new in Application Enablement Services 7.1.3.6

The following table lists enhancements in this release.

Feature	Description
RPM Upgrades	PHP and Tomcat RPMS have been upgraded

What’s new in Application Enablement Services 7.1.3.5

The following table lists enhancements in this release.

Feature	Description
Single Step Transfer support on Avaya Media Server	The “Single Step Transfer” feature has been enhanced to accommodate network delays between CM and media resources (AES-18557)

What’s new in Application Enablement Services 7.1.3.4

The following table lists enhancements in this release.

Feature	Description
N/A	N/A

What’s new in Application Enablement Services 7.1.3.3

The following table lists enhancements in this release.

Feature	Description
N/A	N/A

What’s new in Application Enablement Services 7.1.3.2

The following table lists enhancements in this release.

Feature	Description
SSP/KSP	In concurrence with the 7.1.3.2 Service Pack there is also a SSP/KSP available

What’s new in Application Enablement Services 7.1.3.1

The following table lists enhancements in this release.

Feature	Description
N/A	N/A

What’s new in Application Enablement Services 7.1.3

The following table lists **enhancements in this release.**

Feature	Description
Compliance to DISA security STIGs to achieve JITC certification for AES	Compliance to DISA security STIGs by addressing open Cat I, Cat II and Cat III as identified by the product level self-assessments PIV/CAC support has been included to complete support of Multi Factor Authentication Embedded WebLM has been upgraded and validated to be FIPS compliant.
Support of JITC testing cycle for SIP based Aura (UCCP) to achieve certification and APL for AES	Support of JITC testing cycle for SIP based Aura (UCCP) to achieve certification and APL. AES will be compliant with relevant STIGS and UCR2013 components
Support for vSphere 6.7	Support for running AES in VE with vSphere 6.7
Enabling Customer Customization for Security Profile	Provide support and ability for customers to cherry pick the preferred security profile from a given suite of security profiles. Each Security feature can be enabled or disabled by the customer. The features include FIPS, TLS1.2, TLS1.0/1.1 on/off, extra Auditing, SElinux

Note: The enhancements related to the DISA Security STIGs and JITC certification are not available on the Software-Only offer of AE Services 7.1.3

What’s new in Application Enablement Services 7.1.2

The **following table lists enhancements in this release.**

Feature	Description
Agent Pending States	An Agent would be available but could have pressed an Aux or ACW button. The Pending state reminds the Agent when the call is completed that he/she will be placed in the Aux or ACW state as applicable. The Call Center client will be able to see the pending states on a User Interface.
ASL enable Officelinx	Officelinx is now an Avaya application and will be treated as a "trusted" application by AES to ensure the DMCC and/or TSAPI licenses it needs for deployment and operation are made available via the AES Application Specific Licensing (ASL) capability.
ASL enable ACAL	ACAL (Avaya Cloud Application Link) runs on Aura and syncs messages from Avaya Aura Messaging to cloud apps. AES is needed for CTI control. As an Avaya application ACAL will be ASL enabled to ensure it receives the basic TSAPI and DMCC licenses it needs as well as Agent Events. The ACAL client is a desktop call control client and is used to monitor devices.
ASL enable EP&T Breeze Snap-in	The EP&T Breeze Snap-in will be treated as a “trusted” application by AES to ensure the DMCC and/or TSAPI licenses it needs for deployment and operation are made available via the AES Application Specific Licensing (ASL) capability.
ASL support for CRA Breeze Snap-in	The EP&T CRA (CRM Routing Adaptor) Breeze Snap-in will be treated as a “trusted” application by AES to ensure the DMCC and/or TSAPI licenses it needs for deployment and operation are made available via the AES Application Specific Licensing (ASL) capability. The snap-in provides phantom call services to the EP&T CRM Routing Adaptor and will require Basic and Advanced TSAPI, DMCC and Agent Events.

What’s new in Application Enablement Services 7.1.1

The following table lists en**hancements in this release.**

Feature	Description
KVM (Kernel based Virtual Machine) Support	AES 7.1.1 is available on the KVM platform.
Support Supervisor Observe/Barge	Oceana Workspace Supervisor Desktop can perform Observe/Barge operations on the voice channel. This feature is available only with Avaya Aura Communication Manager 7.1.1.
Channel Type identification over ASAI for OCEANA	Distinction between a voice and a video channel that is now available on AES will provide solution level support for video calls. This feature is available only with Avaya Aura Communication Manager 7.1.1.

What’s new in Application Enablement Services 7.1

The following table lists enhancements in this release.

Feature	Description
Red Hat 7	AE Services is now based on Red Hat 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 connected 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 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 connected 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.”

Feature	Description
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 Footprint 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	20K BHCC	1K	9K BHCC	1K MPS
		10K	6K BHCC			
Medium	2 CPU 4 GB RAM 30 GB HDD	2.5K	50K BHCC	2.4K	18K BHCC	1K MPS
		12K	12K BHCC			
Large	4 CPU 6 GB RAM 30 GB HDD	5K	100K BHCC	8K	36K BHCC	2K MPS
		20K	24K BHCC			

Enhanced Access Security Gateway (EASG)

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

Changes and Issues

Issues related to Backup and Restore

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

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

Upgrading issues related to licenses and the AE Services 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 7.1.3.8

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

ID	Visible symptoms	Workaround
AES-23496	Unable to login into OAM, OAM recovers only after tomcat restart.	Restart tomcat service
AES-21271	Re-initialize tripwire database after installation of Service Patch or Super Patch	Manually Re-initialize tripwire database as per admin guide.
AES-23210	jtapi dmcc errors for event queue are being generated, Socket w/ Oceana CallServerConnector is closed, Service Unavailable	
AES-23757	State of calling party is cs_none after transfer event having one of the merge extension as hunt group	Placing explicit VDN monitor using Call Via Device API before the call gets routed to VDN.
AES-14792	WebLM server points to external webLM server even after the feature pack upgrade to AES 7.0.1.	
AES-21028	AES OAM not accessible from 8443 port if OAM connectivity is not set to ANY in AES SW Only 7.1.3.6	
AES-15702	Error in dmcc-dotnet-sdk-7-0\Visual Studio\VB Snippets\Events\ThirdPartyCallControlEvents.snippet	
AES-17260	MIB browser not able to connect AES Snmp server when SeLinux is Enable	Disable SecureMode
AES-17635	The "mvap.sh" command doesn't shows correct number for DMCC licenses acquired	
AES-16002	sroot user is not displayed on OAM -> User management.	
AES-23869	After uninstalling AES 7.1.3.8, SMS rpm is not downgraded.	Use the following steps: cd /var/disk/rpms ls | grep aesvcs-sms From swversion get the release id Run the command with corresponding rpm from the ls command rpm -U --oldpackage --force aesvcs-sms-<release-id>-0.noarch.rpm --nodeps Ignore the warnings.

Known issues and workarounds Application Enablement Services in Release 7.1.3.7

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

ID	Visible symptoms	Workaround
AES-19711	asai_trace couldn't decode larger ASAI messages	
AES-22399	Ethernet interfaces states on HA status page was shown as down where they were not.	
AES-21271	Re-initialize tripwire database after installation of Service Patch or Super Patch	Manually Re-initialize tripwire database as per admin guide.
AES-17077	SMSXML wsdl import failure using https	Enable http port from OAM
AES-15422	sohctl -lh replication failover command does not drop last two error entries	
AES-23256	CSTA_MONITOR_CALL failure with cause RESOURCE_LIMITATION_REJECTION	
AES-21028	AES OAM not accessible from 8443 port if OAM connectivity is not set to ANY in AES SW Only 7.1.3.6	
AES-16140	Reset log are missing service name	
AES-15951	If we disable eth0 (IPV4, IPV6 Entries) interface from OAM > Network Configure > and restart, then we will see only IPV4 and not IPV6. There is no possibility to bring eth0-IPV6 in the OAM > Network Configure Page.	1. Login to AES via SSH. 2. Switch to root user. 3. Open file /etc/sysctl.conf 4. Check for below flag value at the end of file. net.ipv6.conf.eth0.disable_ipv6 5. If value is set to 1 then make it 0 and save 6. If the flag is not present then append the end of file with below line net.ipv6.conf.eth0.disable_ipv6=0 7. Reboot the system and log in to OAM. You should be able to see the IPV6 interface in the table.
AES-20999	After upgrading to AES 7.1.3.6, starting of subagent2 service errors are seen.	
AES-15702	Error in dmcc-dotnet-sdk-7-0\Visual Studio\VB Snippets\Events\ThirdPartyCallControlEvents.snippet	

AES-22083	sohd process generated core when weblm server was rebooted	
AES-19377	TSAPI & DMCC Links restarts on Active AES server when standby AES is powered On.	
AES-17260	MIB browser not able to connect AES Snmp server when SeLinux is Enable	Disable SecureMode
AES-23210	jtapi dmcc errors for event queue are being generated; Socket w/ Oceana CallServerConnector is closed; Service Unavailable	
AES-16100	Redirect media doesn't work with media encryption "srtp-xxx" & "none"	Use only single value in encryption list when value is of type srtp-xxxx.
AES-16002	sroot user is not displayed on OAM -> User management.	
AES-14792	WebLM server points to external WebLM server even after the feature pack upgrade to AES 7.0.1.	

Known issues and workarounds Application Enablement Services in Release 7.1.3.6

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

ID	Visible symptoms	Workaround
AES-21028	AES OAM not accessible from 8443 port if OAM connectivity is not set to ANY in AES SW Only 7.1.3.6	
AES-21045	S/w only should not be installed if interface name is not "eth0"	
AES-21026	OAM not launching after upgrading 7.1.3.5 S/w only AES to 7.13.6	In /etc/hosts file make sure that hostname for IPV6 localhost is localhost6
AES-20988	7.1.3.6 - SMS Test app not working.	
AES-20871	Receiving error "Could not extract an x500 distinguished name" when attempting to renew third-party certificate with AES generated CSR	Remove the " NEW" text from AES generated CSR. Make sure that the whitespace before NEW should also be removed
AES-20789	OAM page gives 404 Request not found error for software only system	Execute the following steps: 1) Stop Tomcat 2) export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/mvap/lib 3) echo $LD_LIBRARY_PATH (Confirm the output is /opt/coreservices/dss/lib::/opt/mvap/lib) 4) ln -s /usr/share/tomcat5 /usr/share/tomcat

ID	Visible symptoms	Workaround
		5) Delete aesvcs from Tomcat webapp directory (under /var/lib/tomcat/webapps). 6) Delete aesvcs directory from tomcat directory (/var/cache/tomcat/work/Catalina/localhost/aesvcs). Start tomcat service
AES-19406	SNMP subagent is in hung state. TSAPI/DLG/CVLAN/Switch page summary shows blank table.	Restart snmpd, subagent1 and subagent2
AES-17864	Unnecessary kernel martian source logs were being written to alarm.log resulting in low retention of useful logging data	
AES-21035	The CTI application doesn't have the required information in snapshot query response in case of predictive call. The DeviceID for calling party is Dynamic Device when Agent call is ringing but changes to VDN when answered the call.	
AES-20883	The CTI application doesn't have the required information in snapshot query response in case of predictive call. The information for calling party shows connection state as None and DeviceID as Dynamic Device	
AES-17707	In SOAP import, the http import fails due to http port being disabled on newer AES versions	
AES-21016	"SPIRITAgent_1_0_supportedproducts_orig.xml" file is empty after 7.1.3.6 installation	
AES-20980	"Tomcat user not found" warnings are seen while installing 7.1.3.6	
AES-20755	Incorrect error message was printed on OAM at Security -> Security Database -> Worktops	
AES-20773	In snapshot query post the alerting message, AES sends the local connection state for called party as None	
AES-20723	Error seen while accessing the TSAPI service status page on OAM	
AES-20104	If assigning a used virtual IP on an HA system the system may be not accessible through this virtual IP	Verify VIP is unused before assigning to HA system
AES-20103	AES in already configured GRHA setup allows itself to get GRHA configured with another standalone AES	Do not take database backup while system is in HA
AES-19377	TSAPI & DMCC Links restarts on Active AES server when standby AES is powered On	
AES-19226	Aesvcs service does not automatically start after removing GRHA	Manually restart services
AES-17260	MIB browser is not able to connect to the AES SNMP server when SeLinux is Enabled	Disable SecureMode
AES-18984	Intermittently, only INFO and ERROR messages get logged in the /var/avaya/aes/dmcc-trace.log file even when the logging level is set to FINEST.	Use Java Appender instead of SyslogAppender in /opt/mvap/conf/dmcc-

ID	Visible symptoms	Workaround
		logging.properties file. Follow steps in mentioned PSN to apply the workaround: https://downloads.avaya.com/css/P8/documents/101064097

Known issues and workarounds Application Enablement Services in Release 7.1.3.5

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

ID	Visible symptoms	Workaround
AES-19406	SNMP issue due to hung subagent1 and subagent2	Restart SNMP, subagent1 and subagent2
AES-19383	JTAPI Null pointer exception while processing CSTA held event	
AES-19291	SWonly installation showing incorrect information on "Networking Page".	
AES-19238	AES Secondary OAM after failover is not reachable through virtual IP	
AES-19012	User still had group permissions though the group had been removed from user.	
AES-19392	Kernel update required for RHSA-2019:3834	Fix available in 7.1.3 LSU 7
AES-19369	[RHSA-2019:3197] Important: sudo security update	Fix available in 7.1.3 LSU 7
AES-19363	Update OpenJDK RPMs for AES per RHSA-2019-3128	Fix available in 7.1.3 LSU 7
AES-19302	httpd service does not start automatically after reboot	
AES-15750	AES 6.3.3 SP6 - Incorrect days shown in Clearing grace period message.	
AES-19226	After removing GRHA, AE services didn't start automatically on now separated two individual AES servers.	
AES-19020	Spirit Agent CPU spike on AES	
AES-14374	sohd exits on SIG_ABRT raised in weblm client library	
AES-19556	DMCC log level "INFO" & "WARNING" are dumping "FINE" logs	
AES-18984	DMCC logs reduce from Finest to Info	

Known issues and workarounds Application Enablement Services in Release 7.1.3.4

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

ID	Visible symptoms	Workaround
AES-18420	In a GRHA setup, when a service pack is installed on primary AES server via SDM, the patch is not installed on the secondary server	Install the service on the primary server via the command line interface.
AES-15383	DMCC process gets restarted with Out of Memory error.	TR87 client with invalid certificates tries to connect to AES continuously.
AES-18434	The Active Link status displays incorrect information on the OAM page, AE Services -> CVLAN Client	Correct Active Link Status information is displayed on Status->Status and Control-> CVLAN Service Summary
AES-18431	A call answered by a Coverage Answer Group User on Communication Manager gets disconnected.	

Known issues and workarounds Application Enablement Services in Release 7.1.3.3

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

ID	Visible symptoms	Workaround
AES-17850	Cannot view alarm viewer page due to large trapVarbinds.log.1 file	
AES-18071	SMS socket gets closed intermittently on time out.	
AES-18035	mvap.log shows incorrect libg3pd.so file version for 7.1.3	
AES-18033	Cannot redirect to External WebLM by clicking on WebLM server access on OAM	Reload the page manually.
AES-17985	DMCC .Net J-script is not supported in modern browsers(Firefox, Chrome).	DMCC .Net J-script is only supported in IE 6 on windows OS.
AES-17984	The result for skill extension query using JTAPI API getLoggedOnAgents() yields wrong result. It returns the agent information which was removed from skill recently which causes client application to assume that agent still belongs to the same skill.	For the 2nd getLoggedOnAgents() query attempt, use different JTAPI provider
AES-17781	JTAPI doesn’t reflect immediate changes to SDB unless the app is restarted.	Restart the application to get the latest changes.
AES-17701	TLS version 1.0 and 1.1 is not disabled on SOHD port 9041	Use TLS 1.2 version for GRHA
AES-17635	The "mvap.sh" command doesn't show correct number for DMCC licenses acquired	
AES-17332	DMCC Application stops receiving events after Service Provider is restarted.	Shutdown JVM and restart application.
AES-17260	MIB browser is not able to connect with AES/SNMP server when secure mode and selinux is enabled	Disable SeLinux and connect with MIB browser

ID	Visible symptoms	Workaround
AES-17064	JTAPI exerciser, release 7.1.1 onwards may not output all the Call listener events/data that are present in older releases' call listener output.	Use call observer instead of call listener as a workaround to see the detailed events/data.
AES-16983	When re-configuring GRHA setup, OAM is showing an error Creating and exchanging ssh keys failed.	When reconfiguring HA, make sure to remove entry for remote host from /root/.ssh/known_hosts file on Active Server

Known issues and workarounds Application Enablement Services in Release 7.1.3.2

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

ID	Visible symptoms	Workaround
AES-17738	Listed log files (sssd_ldap_domain.log, sssd.log, sssd_nss.log, maillog, cron) have no rotation configured, hence the file sizes may grow to a very large size.	Manually empty the older and large sized log files.
AES-17707	SOAP wsdl import fails because http port is disabled by default.	Replace http://AES_IP with https://AES_IP.
AES-17696/AES-16068	CM UTF8 native name improperly handled by OSSICM/SMS.	
AES-17635	Mvap.sh will show incorrect number for 'DMCC license required' field.	
AES-17439	"ANI_Reqd" field in AAR Analysis table cannot be modified.	
AES-17386	User cannot login to OAM after a backup from 7.0.x is restored on 7.1.x system using the password from the 7.0.x system.	Before configuring GRHA, new linux users that are created on the primary server must be created on the secondary server as well.
AES-17347	Mvap.sh does not return expected data during license query.	
AES-17338	SNMP query for TSAPI License Table (AVAESTSAPILICENSETABLE_OID) does not return SNMP OIDs.	
AES-16984	DMCC threads does not get killed even after DMCC client issues Stop/Disconnect for ServiceProvider.	
AES-16833	Observe tone keep playing after observed agent complete transfer.	
AES-17569	If AES is in secure mode, then we need to disable Secure mode to install patch.	After installing 7.1.3.2, users can install patches without disabling secure mode.

Known issues and workarounds Application Enablement Services in Release 7.1.3.1

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

ID	Visible symptoms	Workaround
AES-17097	WebLM IP address changes after removal of GRHA	
AES-17439	"ANI_Reqd" field in AAR Analysis table cannot be	

ID	Visible symptoms	Workaround
	modified	
AES-17134	"IPServices" Model does not return any response when Field specific request is sent using the SMS service	
AES-16068	Utility Services MyPhone user cannot log in due to CM UTF8 native name improperly handled by OSSICM/SMS	The user's native language name should not contain D0 in byte position 18 on the Communication Manager
AES-17386	AES 7.1 restore does not restore Linux password (/etc/shadow)	
AES-17287	The field "HA Status" goes missing on the top right-hand corner of the OAM after modifications are made to Security-> PAM->Pam Limits	
AES-17064	JTAPI Exerciser does not output all Call Listener events/data	
AES-14927	Incorrect number of ACD Address logged on and off events	
AES-14924	TerminalLoggedOffEvent not generated via removeAgent	
AES-17415	AES 8.0.0.0.4: Unable to populate OCI trunk info and OCI trunk group in Delivered and Establish event of consultation call	
AES-17527	Allow Secure Mode users to use a "." in the username	
AES-17526	remote logging not working in secure mode	Manually add the following data to mvap.conf :
AES-17523	Commented SSLVerifyDepth Value causes "Certificate Chain Too Long" error	Modify the file "/etc/https/conf.d/ssl.conf" to add the entry "SSLVerifyDepth 10". This allows for multiple chain certificate
AES-17454	SNMP Trap receiver not properly configured in AES restore	Manually reconfigure SNMP trap receiver
AES-17434	"Error talking to MBean service" while creating TSAPI or CVLAN link.	
AES-17385	AEP up/down SNMP trap with wrong OID	
AES-17347	mvap.sh does not returns expected result	
AES-17338	SNMP query for TSAPI License Table (AVAESTSAPILICENSETABLE_OID) does not return SNMP OIDs.	
AES-17297	When the AES is in Secure Mode, restarting any service through the OAM, displays the following error "Error talking to MBean Service"	Restart the service through the CLI
AES-17260	MIB browser not able to connect AES SNMP server when SeLinux is Enable	
AES-16982	Deletion of the SNMP v2 trap from OAM deleted this trap from the Database but not from configureNMS. This causes the corresponding alarms to be generated even when not set in the Database	

ID	Visible symptoms	Workaround
AES-17495	For 16XX phones, DMCC client fails with an error NoSuchMethodException when display update action is performed	
AES-17399	External LDAP authentication does not work after switching to secure mode.	
AES-17562	Tomcat localhost_access_log is not automatically cleaned up	Manually delete older /var/log/tomcat/localhost_access_log
AES-17550	Restoring older backup on 7.1.x breaks OAM login	Applicable when restoring from AES 4.x which contains deprecated pam_stack.so. The file /etc/pam.d/oam_login_service should be manually edited to contain only the following entries: #%PAM-1.0 auth include system-auth auth required pam_nologin.so account include system-auth password include system-auth session include system-auth session optional pam_lastlog.so
AES-17306	The value of the field “Time to Begin Audit Each Day” in Security -> Audit -> Login Audit is reset to “00” whenever a double-digit number is entered.	

Known issues and workarounds Application Enablement Services in Release 7.1.3

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

ID	Visible symptoms	Workaround
AES-17097	WebLM IP address changed after removal of GRHA	
AES-17223	DLG service license mode shows "N/A" and cause as "UNKNOWN".	
AES-16068	CFD: Utility Services MyPhone user cannot log in due to CM UTF8 native name improperly handled by OSSICM/SMS	Modify user’s native language name not to have D0 in byte position 18 on CM
AES-16575	JTAPI SDK Client did not properly handle TSAPI FailedEvent	
AES-14927	Incorrect number of ACD Address logged on and off events	

ID	**Visible symptoms**	**Workaround**
AES-14924	TerminalLoggedOffEvent not generated via removeAgent	
AES-17064	JTAPI Exerciser doesn't output all Call Listener events/data	
AES-14892	DMCC extension registration rejected	Clear out /var/log/wtmp
AES-15383	DMCC leaks memory when TR87 client with invalid certs try to connect to AES continuously.	
AES-17332	Not getting DMCC Call Control events from JAVA SDK after an application shuts down and restarts the Service Provider.	
AES-16974	ASL drives GRHA large license.	
AES-16971	After interchange, AES is converting hostname to lowercase instead of taking the actual hostname	Manually change the hostname in /etc/hosts and /etc/hostname
AES-16807	Tripwire configuration needs to be reviewed as critical alarms are generated by addition / modification of some files.	
AES-17245	The alarm.log file gets updated along with ossicm.log for every SMS request/response	
AES-16982	UI and CLI/DB not in sync when change is removed through UI for v2 traps	
AES-17260	MIB browser not able to connect AES SNMP server when SeLinux is Enable	
AES-17289	AES 7.1.3 Build 6 - Cannot create home folder for User in Secondary AES	Use CLI on Secondary server to manually create the user
AES-16983	AES 7.1.2 - Not able to re-configure GRHA setup	When you need to reconfigure HA, make sure you remove entry for remote host from /root/.ssh/known_hosts file on Active Server.
AES-17232	Cannot create CSR if using complex password	Use password with simple characters
AES-17253	After disabling aesvcsSecuremode HA page shows incorrect NIC status	
AES-17288	AES 7.1.3 Build 6 - Secondary AES > Account Management Issues	
AES-16712	DMCC not accepting connection after 4 abnormal disconnect	
AES-15919	ECC traffic experiences high recovery times and loss of subscriptions following CM resets	
AES-17059	DMCC use duplicate crossRefID	
AES-16553	AES: /var/log/wtmp file size impacting login response times	Clear the /var/log/wtmp file manually.
AES-17283	7.1.3 "List All Users" page giving exception after restoring the backup file	
AES-14676	No MediaStart events or RTP when a terminal is registered with a long list of codecs and encryption	

ID	Visible symptoms	Workaround
	types	
AES-16021	AES 7.1 build 13: "JVM exited unexpectedly" error in dmcc-wrapper.log	
AES-16150	sohd fills up logs if certificate is invalid	

Known issues and workarounds Application Enablement Services in Release 7.1.2

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

ID	Visible symptoms	Workaround
AES-14892	Occasionally, a DMCC extension will fail to register and registration will be successful after multiple attempts.	
AES-14924	The event "TerminalLoggedOffEvent" is not generated via removeAgent.	
AES-14927	Logging on and off generated incorrect number of events for listeners of ACD Address.	
AES-15383	DMCC leaks memory when a TR87 client with invalid certificates tries to connect to AES continuously.	
AES-15625	For outbound PC dialer calls, delays in establishing single step conferences causes queueing of requests in AAWFOS as well as loss of call recordings.	
AES-15629	Crash files observed for AES 7.1 build 8 (AsaiMonitor & TRANSMonitor).	
AES-15795	There is a possibility of an “out of memory” condition or thread leak.	
AES-15919	ECC traffic experiences high recovery times and loss of subscriptions following CM resets.	
AES-16021	AES 7.1 build 13: "JVM exited unexpectedly" error in dmcc-wrapper.log.	
AES-16068	Occasionally, attempts to log in to the MyPhone interface of the Utility Services VM using extension and station security code details failed.	Modify the native language name such that byte position 18 does not contain D0.
AES-16099	Occasionally, when DN (Direct Number) calls are made to an agent and the caller performs a hold/unhold operation, the ACR recording is segmented and contains duplicated Caller Numbers.	
AES-16150	Occasionally, installation of incorrect certificates on both Geo-Redundancy High availability servers causes TLS connections to fail "SOHD" (State of Health daemon) to stop functioning.	
AES-16324	In a Call Center Elite environment, for an external call made to an agent, the destination address in CTI events displays the Agent extension instead of the Agent ID.	Use an H.323 Agent
AES-16361	When using a physical set to transfer/conference CDN to an agent, dynamic number in the list of Parties that are being recorded recording and a 1 second extra recording is being generated.	
AES-16439	Not able receive alarms on OAM and Trap receiver.	Manually change hostname in /etc/hostname and /etc/hosts
AES-16552	Not all Call Control monitors receive MonitorStop	

ID	Visible symptoms	Workaround
	events when TSAPI service stops.	
AES-16575	JTAPI SDK Clients do not handle the TSAPI FailedEvent correctly.	
AES-16604	TSAPI clients incorrectly receive a “DUPLICATE INVOCATION REJECTION” error.	
AES-16712	The DMCC service stops accepting connections after 4 abnormal disconnects.	
AES-16807	Critical and Major alarms are generated by addition or modification of some files after a Tripwire Integrity check.	
AES-16926	OAM is not accessible	Manually start httpd service
AES-16944	Not able receive alarms on OAM and Trap receiver.	Need to change hostname manually in /etc/hostname and /etc/hosts
AES-16971	AES and CM connection will go down after interchange if mismatched (i.e. mismatch in the letter casing of the hostname) hostname entry exists in CM and AES.	Manually change hostname in /etc/hostname and /etc/hosts
AES-16974	In GRHA systems, AE Services incorrectly include ASL client Applications in the license usage.	
AES-16975	On a "clean" CM without the "Proceed With Logoff" prompt, it is observed that when the AES SMS invokes a Release, the OSSI connection between the AES and CM will not disconnect immediately. This eventually causes all OSSI sessions to get consumed. SMS will not be able to establish a new OSSI request and the following error will be seen in the SMS test page: ‘Fault: Connection Failed: All available connections are in use. Try again later.’	Manually kill the ossicm process on AES and then establish a new connection.
AES-16982	SNMP v2 version number not visible after deleting SNMP v2 trap destination from OAM.	
AES-16983	When re-configuring GRHA setup, OAM throws the following error: “Creating and exchanging ssh keys failed”.	Remove entry for the remote host from the file /root/.ssh/known_hosts file on the Active Server.
AES-17042	Modifications made to OAM-> Security-> PAM->MOTD (Message of the day) causes corruption and inconsistent behavior on OAM	
AES-17035	DMCC applications using ASL might not be able to connect to AE Services after an application or DMCC service restart.	Refer to PSN020332u to install a patch that will resolve this issue

Known issues and workarounds Application Enablement Services in Release 7.1.1

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

ID	Visible symptoms	Workaround
AES-16099	Occasionally, when DN (Direct Number) calls are made to an agent and the caller performs a hold/unhold operation, the ACR recording is segmented and contains duplicated Caller Numbers.	
AES-15230	The DMCC service summary page sorts the sessions in alphabetical order per page instead of sorting all	

ID	**Visible symptoms**	**Workaround**
	existing sessions.	
AES-16068	Occasionally, attempts to log in to the MyPhone interface of the Utility Services VM using extension and station security code details failed.	Modify the native language name such that byte position 18 does not contain D0.
AES-13960	When the conference controller is a hard phone or in a different JVM as the conferenced party, the conferenced party does not receive termination events for the old call. When the conferenced party is in the same JVM as the conference controller, the conferenced party receives the correct events.	
AES-16324	In a Call Center Elite environment, for an external call made to an agent, the destination address in CTI events displays the Agent extension instead of the Agent ID.	Use an H.323 Agent
AES-16435	Restarting the AES, after modifying the connectivity variables on the "AE Service IP (Local IP)" through OAM, failed to preserve the changes made.	
AES-16288	GetDeviceList will return an empty list for the "Away Worktop" level when TCP Naming format is set to FQDN for the TSAPI CTI link.	Set TCP Naming format to the IP address for the TSAPI CTI link.
AES-16479	In Geo-Redundancy High Availability mode, in a configuration where both AES servers are configured with the same hostname but in different cases (i.e., lowercase and uppercase) then after an interchange takes place, the hostname on the new active AES gets modified causing the connectivity with Communication Manager to fail.	
AES-16238	While making changes through the OAM, the following rules are not followed: "No. of times user is prompted for new password (retry)", "Number of characters in new password that must be different from old password (difok)" and "Number of previous passwords that cannot be reused". **Note:** For modifying login or adding a new login, user must be part of the securityadmin group.	These field validations are successful if the password change or addition of a new login is attempted through the Command Line Interface. **Note:** The root user can change passwords irrespective of these rules.
AES-16281	In an AES configuration that includes recording systems, such as Verint, a call clearing indication by TSAPI application does not get recognized by the recorder causing the recorder to remain on the call indefinitely.	
AES-16239	A Single Step Transfer from a monitored station on Communication Manager to an unmonitored station results in an empty "Transferred To" field in the CTI Transferred event.	
AES-16385	For large values of UUI, DMCC applications receive incorrect UUI.	
AES-16150	Occasionally, installation of incorrect certificates on both Geo-Redundancy High availability servers causes TLS connections to fail "SOHD" (State of Health daemon) to stop functioning.	

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 the numbers 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, 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 it is configured and accessible.	Make a note for Virtual IP address.

Fixes in Application Enablement Services in Release 7.1.x.x

Fixes in Application Enablement Services in Release 7.1.3.8

The following table lists the fixes in this release:

ID	Minimum Config	Customer Visible Symptom
AES-20720	AES 7.1.3.6, CM 7.1.3	Application call recording stopped working due to the application stopped receiving CSTA events.
AES-23256	AES 7.1.3.6 and above, CM 7.1.3	Call monitoring failed with cause value RESOURCE_LIMITATION_REJECTION.
AES-23590	AES 8.0.1, CM 8.0.1	Customer got “technical difficulty experienced” message played on the IVR because the call was not fully established on AES connector side.

Fixes in Application Enablement Services in Release 7.1.3.7

The following table lists the fixes in this release:

ID	Minimum Config	Customer Visible Symptom
AES-22559	AES-7.1.3	In IPAddressUsageModel in SMS, while trying to access XML schema, Group Number Field was named as "01A00" While in the non XML schema it was correctly mentioned
AES-22099	AES 7.1.3.4 in GRHA	Virtual IP was not visible on HA Status page
AES-21414	AES 8.1.3 or AES 7.1.3.6	Exception was raised when list vector command was run using SMS SOAP service
AES-21240	AES 7.1.3.6	On uninstallation of FP, the php rpms were reverted back to the GA version of 7.1.3 irrespective of the previous version of FP installed on the system
AES-21050	7.1.3.2 AES with incorrectly configured JavaManager.properties	Attempting to access OAM->Status->Status and Control->TSAPI Service Summary->TSAPI Service Status when JavaManager.properties was incorrectly configured caused a UI Exception to be raised
AES-21046	AES 8.0 or above JTAPI SDK 8.0 or above	getRegisteredEndpoints query from JTAPI for AES 8 and above was not being executed
AES-20988	AES 7.1.3.6	SMS Web test application was inaccessible
AES-20981	AES 7.1.3.6	SMS RPM warnings were being generated and seen in updatelog
AES-19083	AES 7.1.3	Cross site scripting occurred if the SMS page was accessed as below https://<AES_IP>/sms/ModelSchema.php?model=<Some script>
AES-20871	AES 7.1.3	If the certificate contains the characters "END" then CSR for renewing the certificate is generated wrong thus failing the renewal request

AES-22747	AES 7.1.3.6 and above, CM 7.1.3	When transferred event has 1 merge extension and is same as calling_num, In this case transfer controlling device/calling_num will be removed causing call record to get deleted if there are no more parties left while processing next event/conf. This results in conf (for take control requests) not send to client causing stale invokeID and later duplicate invocation rejection.
AES-21860	AES 7.1.3, CM 7.1.3	Local/Embedded WebLM rejected the license request saying "Too many licenses" which caused TSAPI to enter into LICENSE_ERROR mode.
AES-21645	AES 7.1.3.6, SMGR 7.1.3, CM 7.1.3	OAM pages (AE Services & Status) were stuck and TSAPI stopped processing CSTA traffic when WebLM was not reachable.
AES-21309	AES 7.1.3.4	TSAPI service crashed which resulted in termination of all active client connections.
AES-21218	AES 7.1.3.6, SMGR 7.1.3, CM 7.1.3	OAM pages (AE Services & Status) were stuck and TSAPI stopped processing CSTA traffic when WebLM was not reachable
AES-21190	AES 7.1.3	No alarms were generated when the TSAPI service stopped processing the CSTA requests as a result of a broken connection between TSAPI service and the WebLM server.
AES-21035	AES 7.1.3.2.0.2-0	The CSTA snapshot query response for predictive call scenarios returned incorrect data to the CTI application. The local Connection Info State for the Calling device was displayed as 'None' instead of 'Connected' when Agent call was in ringing mode. Also, the DeviceID for calling party changed to VDN from Dynamic Device when state changed from ringing to answered.
AES-20883	AES 7.1.3.2.0.2-0	The CSTA snapshot query response for predictive call scenarios returned incorrect data to the CTI application. The information for calling party displayed connection state as 'None' and DeviceID as 'Dynamic Device' when the Agent was in Alert State.
AES-21026	Upgrade from AES 7.1.3.5 to AES 7.1.3.6	OAM did not launch after upgrading 7.1.3.5 S/w only AES to 7.1.3.6 Note: This was fixed as a part of documentation.
AES-20755	AES-7.1.3.5 or AES-8.1.2	When an incorrect file was uploaded on OAM under Security -> Security Database -> Worktops, wrong error message was displayed.
AES-22913	AES 7.1.x with reserved licensing for DMCC configured.	Extra DMCC licenses were consumed from WebLM when reserved licensing was enabled.
AES-22362	AES 7.1.3.x	AES stopped responding to TSAPI/DMCC messages when a ClamAV (clamscan) was in progress.
AES-22342	Profile 1 AES 7.1.3.x and above	Executing snmp queries or using the mvap.sh info caused high CPU usage on AES.

AES-20104	AES 7.1.3	An IP address, which was already in use by some other system, was accepted on the High Availability configuration page as a Virtual IP.
AES-20103	3 AES 7.1.x and above, out of which 2 AES are already configured for GRHA.	When an AES IP, which was already in GRHA running/configured state with other AES, was given as the secondary AES in a new GRHA configuration on a third server, broke the initial GRHA configuration.
AES-20773	AES 7.0 with CTI application	AES sent local connection state for called party as None in Snapshot query post Delivered event.
AES-22175	AES 7.0 and above	Weak key exchange algorithm (diffie-hellman-group1-sha1) was supported on AES
AES-21933	AES 7.1.3.6	swversion command was showing the older PHP rpm version in case an upgrade happens for PHP.
AES-19226	AES 7.1.3 or 8.1.3 systems should be available in GRHA mode.	After removing GRHA on AES 7.1.3 or 8.1.3, aesvcs service was not coming up on standby AES.
AES-21237	TSAPI CTI application connected to AES.	TSAPI crashed with signal 11, Segmentation fault
AES-18984	AES DMCC 7.1.3	Intermittently, only 'INFO' and 'ERROR' level messages were getting logged in the /var/avaya/aes/dmcc-trace.log file even when the logging level was set to 'FINEST'.

Fixes in Application Enablement Services in Release 7.1.3.6

The following table lists the fixes in this release:

ID	Minimum Config	Customer Visible Symptom
AES-19605	AES-7.1.3.4 and later	Under the conditions mentioned below, the NMS server even though configured on the system and visible on the OAM, was not reflected in the snmpd.conf file: On 7.1.3.4 1. When SNMP version 2c was used 2. When SNMP version 3 was used and Authentication and Privacy protocols were not provided On 8.0 and above 1. When SNMP version 3 was used and Authentication and Privacy protocols were not provided
AES-19287	AES 6.3.3 onwards	The alarms.log files were being rotated twice per day instead of once resulting in retention of 5 days instead of 10
AES-19558	CM 6.3.119.0, AES 7.1.3.4 and CM Special Application SA 9137 is enabled	In ECD configuration only, in rare cases calls remained in queue with available agents. Only applicable if CM Special Application SA 9137 is enabled. Reference PSN020412u Required patch for CM 7.1.3.2 and 7.1.3.3 for systems implementing SA 9137
AES-19710	AES 7.1.3.5, CM 7.1.3.5	In ECD Configuration only, when ECD Activate and Deactivate Skill Responses were sent from the CM, any other application request, such as Make Call, Answer Call failed with the error "DUPLICATE_INVOCATION_REJECTION"

AES-20756	Config requirement for SNMP version 3	Trap are not being sent to NMS server for SNMP version 3, due to improper configuration
AES-20767	AES 7.1.3.5	Tomcat Vulnerability corresponding to the configured Apache JServ Protocol (AJP) port was seen on tomcat versions below 8.5.51
AES-19031	AES 7.1.3.4 AES 8.1.1	Entire path of the AES page was been send to the external site as referer that is: https://135.27.162.26/aesvcs/view/aboutAes/aboutAes.xhtml
AES-18999	AES 7.1.3.5, AES 8.1.1	File of any type could be uploaded on the AES
AES-18983	AES 7.1.3	DMCC logs were not being compressed resulting in /var/log filling quickly
AES-14892	DMCC registrations on AES 7.0.1 onwards	Intermittently, DMCC registration failed
AES-19682	AES 7.1.3.0.0	AES listened to unknown IP Address 135.9.172.122 on port number 8180
AES-19378	AES upgraded from 7.1.3.3 to 7.1.3.5 or from 8.0.1.0.x to 8.0.1.0.y, where y > x, and then reverted to the original service pack	GRHA status would get corrupted when uninstalling AES 7.1.3.5 and reverting to 7.1.3.3 and when upgrading from AES 8.0.1.0.x to 8.0.1.0.y, where y > x, and then reverting to 8.0.1.0.x. On OAM, HA status at top of page showed running, but Status on HA page showed stopped and the "start" button was available on HA page.
AES-19066	AES 7.1.3.5 and later	On a system that connects to SMGR WebLM for licenses, during high traffic, delays were observed in APIs that use licenses. This issue is also present with standalone WebLM if it is in a different network than the AES. Embedded WebLM in AES and Reserved Licensing on any configuration do not have this issue
AES-19556	AES 7.0.1 and later	FINE messages would get logged in the /var/log/avaya/aes/dmcc-trace.log file even when the dmcc trace log level was set to WARNING

Fixes in Application Enablement Services in Release 7.1.3.5

The following table lists the fixes in this release:

ID	Minimum Config	Customer Visible Symptom
AES-18819	AES-7.1.3.5	The customer could see wrong permitted values (1-10000) ms for ECD timer. However the correct values were (100-10000)
AES-18589	7.1.3	Information, such as userid, common name, surname, etc, did not get written to the oam-audit.log during the process of adding a user through the OAM.
AES-18499	7.1.3	Restoring the backup, previously taken on an HA system, on a newly deployed AES server incorrectly copied the HA configuration of the older AES system onto the new AES system.

ID	Minimum Config	Customer Visible Symptom
AES-14927	AES 7.0	Multiple Logged on Events were being generated for a single object
AES-19558	CM 6.3.119.0 AES 7.1.3.4	CMS reports showed that calls remained in queue when agents were available (CIQAA)
AES-19025	AES 7.1.3.4, CM 7.1.3.4	"ConnectionClear" events were not received for the Call Monitors placed on calls. In addition, "MonitorStop" events were not received after call drop for Call Monitor requests.
AES-18945	AES 8.1.1 CM 7.1.3.4	Predictive Call failed because "ECD Route Select" message on "ECD Route Request" was not generated resulting in "ECD Route End" (ECD timeout) from CM.
AES-18769	AES 7.1.3.1, CM 7.1.3.4	A TSRV process restart on AES caused all clients to get disconnected.
AES-18235	AES 7.0.1 onwards	Unnecessary cron entries were being logged in /var/log/wtmp
AES-19312	AES 7.1.3.5 upgraded from AES 7.1.3.4	After uninstallation of 7.1.3.5 which was installed over 7.1.3.4, AES OAM was not accessible.
AES-18942	AES 7.1.x with GRHA running	In an AES GRHA setup, when the standby was not reachable, patch installation or uninstallation proceeded without any error resulting in software version mismatch between the servers.
AES-18899	AES 7.1.3.3 and SGMR 7.1.x.	When an SMGR that is used for licensing on AES is rebooted, the TSAPI (tsrv) process showed a CPU spike of 100 percent resulting in high CPU usage, which caused the TSAPI clients connected to AES to disconnect.
AES-18672	AES 7.1.x	Customer could not login to OAM with user configured in LDAP Active Directory when "User ID Attribute Name" was changed from "uid" to "samAccountName" on the "Enterprise Directory" page of OAM.
AES-17434	A CVLAN link on AES 8.0	Attempts to toggle the status of the CVLAN from AES OAM -> Status -> Status and Control -> CVLAN Service Summary failed with the error,"Error talking to MBean Server."

ID	Minimum Config	Customer Visible Symptom
AES-19303	Upgrade to 7.1.3.4 from 7.1.3.2/7.1.3.3	GRHA did not start properly.
AES-18434	7.1.3.3 system	The ASAI Link Version on "AE Services ---> CVLAN ---> CVLAN links" tab was seen as "UNKNOWN," whereas the same was seen correctly as a numeral in the "Status ---> Status and Control ---> CVLAN Service Summary" tab.
AES-18431	AES 6.3.3.10	Singe Step Conference Fails when the call is answered by Coverage Answer Group user
AES-18711	AES 6.3.3. N/A after AES release 8.1	When accessing web server, the security related headers are either not present or not set to acceptable usage as per the following guideline: https://www.owasp.org/index.php/List_of_useful_HTTP_headers

Fixes in Application Enablement Services in Release 7.1.3.4

The following table lists the fixes in this release:

ID	Minimum Config	Customer Visible Symptom
AES-18104	7.1.3.3	TWS logs failed to get generated due to wrong port redirection of logs
AES-18088	7.1.3.4 LSU 4	Updating “slapd” to the latest version caused it to remain in the "update" stage
AES-18071	7.1.3.1.1	Multiple SMS requests caused an SMS timeout. This was not experienced for single SMS requests
AES-17850	AES 7.1.3.1.1	Customer could not view the alarm viewer page because of the large size of the trapVarbinds.log.1 file
AES-18094	AES 7.1.2	The Monitor Call event failed with the DUPLICATE_INVOCATION_REJECTION error after the limit of 40000 Monitored calls was reached. .
AES-18502	AES 7.1.3.3	1. From AE Service Management Console main menu, Select Networking -> TCP Settings. 2. On the TCP Settings page, select: TSAPI Routing Application Configuration (6) 3. Select Apply Changes. 4. Confirmation page will be loaded, Select Apply 5. The previous page is re-loaded with the default value
AES-18012	AES 6.3.3 or later.	AES 1 did not relinquish control of the snapshot device call on station 1 on which 3PTC was invoked. As a result, when AES 2 invoked ClearCall, it failed to take control of the call and resulted in an "Outstanding Request Limit Exceeded" message.

ID	Minimum Config	Customer Visible Symptom
AES-18331	AES 7.1.x	A restore on the system incorrectly replaced the existing logging levels, that were set on the system prior to the restore, to the logging levels obtained from the backup file. This resulted in failure in generation of log files.
AES-18320	AES 7.1	The enterprise directory page on OAM did not apply changes nor did it display any error if the FQDN entry of the active directory was missing in the /etc/hosts file on AES. On restoring of backup data on AES, if the entry of the Active directory was not present in /etc/hosts, it generated an error for invalid FQDN which persisted even after adding the host entry in /etc/hosts
AES-18314	AES 7.1.3	Tomcat Version on AES 7.1.3 was 7.0.54
AES-18252	AES 7.1.3 (SWONLY offer)	After a database restore, users were unable to log in to the AES system.
AES-18110	AES 7.1.3.x	The setSELinux utility displayed incorrect status of SELinux
AES-18419	AES DMCC stations configured to use H.323 Security Profile as "pin-eke"	DMCC application stopped receiving events from the DMCC service after 5 days of high traffic when the H.323 Security profile was configured as "pin-eke" on ip-network-region form on CM
AES-18246	SMS logging set to Verbose and SMS Log Destination set to syslog from AES OAM.	/var/log/avaya/aes/ossicm.log file is not generated
AES-18101	CM extension is monitored	Private Data was missing from the delivered event when ChannelType was sent from CM.
AES-17701	AES 7.1.3	When AES was configured to use only TLS 1.2, while negotiating the TLS version, "sohd" tried to connect with versions 1.0 and 1.1. This failed and then eventually sohd connected to TLS 1.2

Fixes in Application Enablement Services in Release 7.1.3.3

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms
AES-17997	AES 7.1.x	Log Entry in /var/log/httpd/mod_jk.log. “init_jk::mod_jk.c (3591): mod_jk/1.2.46 initialized”
AES-17995	AES 7.1.3	The potentially vulnerable HTTP ‘DELETE’ and ‘OPTIONS’ method requests could be sent
AES-17965	AES 7.1.x	Cookies on AES do not have the 'HttpOnly' flag set
AES-17873	AES 7.1.x	The AE services fail to start as the softlink /usr/java/default doesn’t point to the latest OpenJDK version.
AES-17870	AES 7.1.3	AES didn't send "Connection Clear" event to CTI application for service observer dropping off the call to observed party for the 2nd time.
AES-17864	AES 7.1.3	Huge amount of kernel martian logs were generated in alarm.log
AES-17860	AES 7.1.x	The “avayadefaultsal” entry on SNMP Trap Receivers page could not be

ID	Minimum Conditions	Visible symptoms
		deleted.
AES-17834	AES 6.3.3	DLG Service License Mode and cause is shown as N/A on OAM under AE Services Page for DLG
AES-17754	AES 6.3.3	HMDC report showed incorrect values for TSAPI fields: “avAesTsapiClientCallMonitors”, “avAesTsapiClientDeviceMonitors”, “avAesTsapiClientRegisteredRoutes”, “avAesTsapiClientVdnMonitors”
AES-17738	AES 7.x	Listed log files (sssd_ldap_domain.log, sssd.log, sssd_nss.log, maillog, cron) grew to a very large size.
AES-17707	AES 7.x	Import of smsxml wsdl on SoapUI using https, resulted in an error of ‘Error loading http://<ip>/smsxml/xsd/models/ModelChoices.xsd:java.io.IOException: Attempted read from closed menu’.
AES-17579	AES 7.0.1	In a single step transfer scenario, when the transfer was completed the extension of the party that transferred the call was sent in the "Established" event" instead of the party that was being transferred.
AES-17439	AES 7.1.2	When using AES SMS, the "ANI_Reqd" field in the AAR Analysis table/model could not be modified with "change" operation
AES-17347	AES 7.1.1	Running 'mvap.sh info' will showed unexpected exceptions output.
AES-17338	AES 7.1	Snmpwalk on AES did not show information for TsapiLicense
AES-17097	AES 7.1.1	Removal of GRHA would result in removal of license on secondary AES and in an incorrect WebLM server IP address.

Fixes in Application Enablement Services in Release 7.1.3.2

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms
AES-17793	AES 7.1.3.1	Changing TLS setting via OAM was resulting in the error message “Error running TLS configuration script”.
AES-17684	AES 7.1.2	sohd service would go in restart loop if it was killed or restarted externally.
AES-17677	AES 6.3.3.9	While transferring monitor objects across sessions, all monitors which did not have deviceid associated with them (e.g. Session Mgmt Monitor Objects) and did not belong to transfer monitor object, the request sessions were also getting transferred.
AES-17633	AES 7.1.2 and above	While administering Ports under Management Console->Networking->Ports (e.g. Disabling/Enabling port 4722 for DMCC encryption) error message was getting thrown: ‘Exception occurred while trying to save SMS Proxy Ports to the configuration file. Either the file could not be found or you do not have write permissions. SMS changes have not been saved!'
AES-17562	AES 7.1.x onwards	There was an increase in the disk usage when the tomcat localhost_access.log file was being rapidly filled up and was not being cleaned up.
AES-17551	AES 7.1.2	Incorrect display of Security Database data after import on OAM. Mismatch in the number of records shown.
AES-17550	AES 7.1	When restoring a backup from releases older than 7.1 on a 7.1.x system, OAM was only accessible using the default 'custpw' password and only 3 tabs remained visible on OAM. Also, OAM became

ID	Minimum Conditions	Visible symptoms
		inaccessible for 'craft' user.
AES-17460	AES 7.1.3 onwards	The pages on OAM that had auto refresh enabled (High Availability, Status -> Status and Control pages) redirected to crossSiteError page and logged out the user from the active session.
AES-17454	AES 7.1	On OAM user could see SNMP trap receiver configured properly, but user was unable to send alarm on trap receiver.
AES-17352	AES 6.3.3	This is the CSRF vulnerability that allowed a user to perform unintended operations on OAM while the user is authenticated on OAM.
AES-17351	AES-7.1	Failover did not work when FQDN was entered on the Network Configuration Page on OAM.
AES-17287	AES-7.1.3	HA Status field was missing on the confirmation page during submission of Security ->PAM-> PAM Limits
AES-16982	AES 7.1	On OAM, version of trap receiver was not being displayed.
AES-17097	AES 6.3.3	After removal of HA or stopping HA, WebLM IP was getting set to a random IP because of incorrect backup file.

Fixes in Application Enablement Services in Release 7.1.3.0.2

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms
AES-17527	AES 7.1.3	Username that contained a period, ".", was not allowed for OAM logins
AES-17526	AES 7.1.3	In secure mode while using or changing the rsyslog configuration through the OAM, the data was not written onto the server causing failure to send logs to the remote server
AES-17523	AES 7.1.3	Client certificate that was created with more than two root certificates failed to be read by the server
AES-17455	AES 7.1.3	PAM issue messages were not displayed if configured through OAM.
AES-17410	AES 7.0.1	When modifying account via OAM, two of the password policy rules did not work: 'maxrepeat' and 'Number of previous passwords that cannot be reused'. Note: All password rules are applicable when modifying account via CLI.

Fixes in Application Enablement Services in Release 7.1.3.1

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms
AES-17463	AES with DMCC service used.	CSTA Delivered and CSTA Established event private data did not populate all required fields like trunkGroup, trunkMember and acdGroup information.
AES-17455	AES 7.1.3	PAM issue messages were not displayed if configured through OAM.
AES-17410	AES 7.0.1 onwards.	When modifying account via OAM, two of the password policy rules don't work: 'maxrepeat' and 'Number of previous passwords that cannot be

ID	Minimum Conditions	Visible symptoms
		reused'. Note: All password rules are applicable when modifying account via CLI.
AES-17406	AES 7.1.3	Uppercase hostname was converted to lowercase when installed on VMware and KVM
AES-17405	AES 7.0.1 onwards.	ossicm.log file never rotated
AES-17402	configure AES in secure mode and use embedded webLM.	In secure mode, license could not be acquired for embedded webLM.
AES-17394	AES 7.1.3	Clicking on any tab within the Security tab on OAM would open the tab just above the one that was selected
AES-17389	AES 7.1.3	The “Apply Changes” process on the PAM password manager page on OAM did not return any result
AES-17346	AES 7.1.2 and above and GRHA setup.	GeoHA Virtual IP configured in Client connectivity (AE Service IP - Local IP) did not get synchronized with the standby server
AES-17262	AES 7.1.3	After installation on KVM, post install configuration process required user to input two times to proceed. It took 5 seconds longer to display the next settings
AES-15539	AES 7.0.1 with libssh2-1.2.x library	SMS services stopped working after some time. OSSICM process became non-responsive

Fixes in Application Enablement Services in Release 7.1.3

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms
	Infrastructure	AES 7.1.3 includes the Red Hat updates to support mitigation of the Meltdown/Spectre vulnerabilities. However, this has the potential to affect performance – so there is now a small script that allows the setting of kernel options to control how these vulnerabilities are handled. The effect of running the kernel configuration script is both immediate and will persist across reboots. The script should be called from the CLI using the admin user and is called kernel_opts.sh. It has the argument “status” to display the current status of the kernel options, “enable” to enable all flags to provide maximum protection, and “disable” to disable all flags to provide maximum performance.
AES-16239	AES 7.0.1 and above	TransferredTo field was missing in CSTA transferred event in case of single step transfer call.
AES-16288	AES 6.3.3 and above	GetDeviceList returns empty for “away work top” if the TCP naming format is FQDN.
AES-16532	AES 7.0.1 and above	TSAPI service would restart resulting in a service outage.

ID	Minimum Conditions	Visible symptoms
AES-16942	AES 7.1.2	DB operation failed and provided undesired results when queried.
AES-16716	AES 7.1	TWS WSDL could not be retrieved when accessing https://<AESIP>/axis/services/TelephonyService?wsdl , throwing AXIS errors
AES-16975	AES 6.3.3 and above configured with a CM that did not have alarms enabled i.e. upon logoff from sat, CM did not prompt for user input.	On a CM with alarms or busyout station, the SAT logoff generates a "Proceed With Logoff" prompt. On a "clean" CM without the "Proceed With Logoff" prompt, it was observed that when the AES SMS application invoked a Release, the connection between the AES and CM did not disconnect immediately.
AES-17108	AES 6.x with CM 6.x	When an ampersand character was provided in the field values on CM, SMS was not able to parse the string and hence returned a truncated or empty result.
AES-16926	AES 7.1.2 GRHA	Any change made to the Session Timeout fields on the AES Management Console (OAM) caused the HTTPD service to fail. A Manual restart of httpd was required
AES-17330	AES 7.1.1 and above	On the Management Console (OAM) no changes could be made to the PAM Password Manager fields
AES-16435	AES 6.3.3 and above	Switch connectivity IP would get reset after a Linux restart if eth0 and eth1 IPs were configured in the system.
AES-16028	SMS Client SDK AES version 6.3.3 and above.	AES SMS service to retrieve public unknown number failed when the count was greater than 5000.
AES-17100	AES 7.1.1 and above	The full menu, that is normally available to the "cust" user, was not displayed on the management console (OAM). In addition, when a user tried to login as “cust” on the CLI console, the login failed and the error “too many logins for cust” was displayed.
AES-16998	AgentTerminal configured with Terminal Listener.	JTAPI Client did not send a TERMINALLOGGEDOFFEVENT for TSAgent over the Terminal Listener to the application when the application logged off the agent successfully.
AES-17105	AES 7.1.2	During an unsupervised transfer, CTI application did not receive the agent state change event
AES-16729	AES-7.1.1 and above	TSAPI Established Event was not being received by the monitor on a SIP station when the call was unpark using call unpark button.
AES-16827	AES 7.1 and above	After configuring SNMP Agent, SNMP trap receiver and OAM alarm status did not receive any alarms
AES-17043	AES 7.1 and above	A change of OAM IP address in Local IP caused the file permissions of server.xml to change which in turn caused the OAM to become inaccessible on the Primary server
AES-17003	AES 7.1 and above	When AES was deployed with the FQDN as the hostname during OVA deployment, alarming failed to

ID	Minimum Conditions	Visible symptoms
		work
AES-16385	Register Event in DMCC with userData containing non-ascii characters.	While monitoring for events in DMCC, user provided userData would get corrupted in case of user-data contains the ascii characters greater than 7F.
AES-16937	Compatible AES and CM and an SMS application that can access (Change, Display) VectorVariables model in CM.	Access (change, display) to the VDN_Assig_3 and VDN_Assig_2 fields of the VectorVariables Model through an SMS application failed
AES-16578	SWOnly 7.1 and 7.1.1 AES.	In a SWOnly environment, when the security database was imported from the maintenance page in OAM, the imported users did not get displayed in security database -> list all CTI users page.
AES-16806	AES 7.1.1 and above.	Older alarms were not purged. All the alarms until date were visible on the OAM.
AES-16802	SWOnly installation of AES 7.1.2	HTPD service failed causing the OAM to become inaccessible

Fixes in Application Enablement Services in Release 7.1.2

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible symptoms
AES-16729	AES 7.0.1 configured with CM to use the call-park button	Incorrect information was generated when a call that was parked using the "call-park" button was subsequently unparked; The event "New_Call" was seen instead of "Park" as is expected.
AES-16288	AES 6.3.3.8 and above	GetDeviceList returned an empty list for the "Away Worktop" level when TCP Naming format was set to FQDN for the TSAPI CTI link.
AES-16716	AES 7.1 and above	TWS WSDL could not be retrieved when accessing https://<AES-IP>/axis/services/TelephonyService?wsdl; Reported AXIS errors
AES-16435	AES 6.3.3.8 and above	Switch Connectivity IP was being reset after a system restart if both eth0 and eth1 were configured in the system.
AES-16553	AES 7.0.1 and above	Log rotation failed for the file /var/log/wtmp
AES-16573	AES 7.1 and above	Occasionally, the system would generate a multiple core files caused by the SOHD service
AES-16281	AES 6.3.3.7 and above	CTI application did not receive the correct connection state of the party dropping off the call.

Fixes in Application Enablement Services in Release 7.1.1

N/A

Fixes in Application Enablement Services in Release 7.1

N/A

Avaya Aura® Utility Services

Installation for Avaya Aura® Utility Services Release 7.1.x.x

Installation for Avaya Aura® Utility Services Release 7.1.3.8

Download ID	Patch	Notes
US000000097	util_patch_7.1.3.8.0.05.zip	This patch can be applied to the VMware, AWS, and KVM version of Utility Services 7.1.

Installation for Avaya Aura® Utility Services Release 7.1.3.7

Download ID	Patch	Notes
US000000096	util_patch_7.1.3.7.0.03.zip	This patch can be applied to the VMware, AWS, and KVM version of Utility Services 7.1.

Installation for Avaya Aura® Utility Services Release 7.1.3.6

Download ID	Patch	Notes
US000000095	util_patch_7.1.3.6.0.03.zip	This patch can be applied to the VMware, AWS, and KVM version of Utility Services 7.1.

Installation for Avaya Aura® Utility Services Release 7.1.3.5

Download ID	Patch	Notes
US000000094	util_patch_7.1.3.5.0.02.zip	This patch can be applied to the VMware, AWS, and KVM version of Utility Services 7.1.

Installation for Avaya Aura® Utility Services Release 7.1.3.4

Download ID	Patch	Notes
US000000093	util_patch_7.1.3.4.0.05.zip	This patch can be applied to the VMware, AWS, and KVM version of Utility Services 7.1.

Installation for Avaya Aura® Utility Services Release 7.1.3.3

Download ID	Patch	Notes
US000000092	util_patch_7.1.3.3.0.03.zip	This patch can be applied to the VMware, AWS, and KVM version of Utility Services 7.1.

Installation for Avaya Aura® Utility Services Release 7.1.3.2

Download ID	Patch	Notes
US000000091	util_patch_7.1.3.2.0.01.zip	This patch can be applied to the VMware, AWS, and KVM version of Utility Services 7.1.

Installation for Avaya Aura® Utility Services Release 7.1.3

Download ID	Patch	Notes
US000000087	util_patch_7.1.3.0.0.05.zip	This patch can be applied to the VMware, AWS, and KVM version of Utility Services 7.1.

Installation for Avaya Aura® Utility Services Release 7.1.2

Download ID	Patch	Notes
US000000084	util_patch_7.1.2.0.0.07.zip	This patch can be applied to the VMware, AWS, and KVM version of Utility Services 7.1.

Installation for Avaya Aura® Utility Services Release 7.1.1

Download ID	Patch	Notes
US000000079	util_patch_7.1.1.0.0.01.zip	This patch can be applied to the VMware, AWS, and KVM version of Utility Services 7.1.

Installation for Avaya Aura® Utility Services Release 7.1

Download ID	Patch	Notes
US000000077	US-7.1.0.0.0.18-e55-3_OVF10.ova	You can use the OVA for both new installs and upgrades from previous releases of Utility Services.

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.

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

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

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

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

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

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

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

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 Utility Services 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.x

What’s new in Utility Services Release 7.1.3.8

The following table lists enhancements in this release.

Enhancement	Description
UTILSERV-542	SMS rpm from AES for AES-16068 where UTF8 native name improperly handled

What’s new in Utility Services Release 7.1.3.7

The following table lists enhancements in this release.

Enhancement	Description
None	

What’s new in Utility Services Release 7.1.3.6

The following table lists enhancements in this release.

Enhancement	Description
None	

What’s new in Utility Services Release 7.1.3.5

The following table lists enhancements in this release.

Enhancement	Description
None	

What’s new in Utility Services Release 7.1.3.4

The following table lists enhancements in this release.

Enhancement	Description
None	

What’s new in Utility Services Release 7.1.3.3

The following table lists enhancements in this release.

Enhancement	Description
UTILSERV-935	tzdata Linux RPM updated to tzdata-2018g

What’s new in Utility Services Release 7.1.3.2

The following table lists enhancements in this release.

Enhancement	Description
UTILSERV-935	tzdata Linux RPM updated to tzdata-2018e

What’s new in Utility Services Release 7.1.3

The following table lists enhancements in this release.

Enhancement	Description
Support for vSphere 6.7	Utility Services 7.1 now fully supports deployment using VMware vSphere 6.7 elements – including ESXi 6.7 and vCenter 6.7.
Kernel Configuration	Utility Services 7.1 includes the Red Hat updates to support mitigation of the Meltdown/Spectre vulnerabilities. However, this can affect performance – so there is now a small script that allows the setting of kernel options to control how these vulnerabilities are handled. The effect of running the kernel configuration script is both immediate and will persist across reboots. The script should be called from the CLI using the admin user and is called kernel_opts.sh. It has the argument “status” to display the current status of the kernel options, “enable” to enable all flags to provide maximum protection, and “disable” to disable all flags to provide maximum performance.

What’s new in Utility Services Release 7.1.2

The following table lists enhancements in this release.

Enhancement	Description
Commercial	Utility Services 7.1 now supports Commercial Hardening Options. This allows the

Enhancement	Description
Hardening	administrator to enable FIPS mode – please note that a reboot of the virtual machine is required for all the FIPS elements to be activated. There is also a new script to allow the Serviceability Agent to support Third Party Certificates. Commercial Hardening is fully documented in the “Accessing and Managing Utility Services” guide.
Extended SSH Timeout	The login grace timer for Secure Shell access has been extended from 30s to 120s in line with requests from the field.
Multiple Static Routes	The ability to add a static route to the OOBM network has been extended from a single entry to multiple entries with a new script – ovf_set_multi_static. This is identical in syntax to the current single-entry script, with the exception that the delete option now includes an index to identify which route should be deleted. This is fully documented in the “Accessing and Managing Utility Services” guide.

What’s new in Utility Services Release 7.1.1

The following table lists enhancements in this release.

Enhancement	Description
KVM Support	Utility Services 7.1 is now available as OVA for Kernel-Based Virtual Machine (KVM) Hypervisors – for example, Red Hat Enterprise Linux 7. Although this OVA is being released as V7.1 (in line with the release string for the VMware and AWS OVA’s), it should be upgraded to 7.1.1 by applying Feature Service Pack 7.1.1 as soon as possible after installation. Release 7.1.1 contains important security remediation as detailed later in these Release Notes.

What’s new in Utility Services Release 7.1

The following table lists enhancements in this release.

Enhancement	Description
Red Hat 7	Utility Services is now based on Red Hat 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 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.

Enhancement	Description
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 Hardening	Utility Services now offers a fourth mode of deployment – Hardened Mode Services Port 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 because 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.
Enhanced Services Directory (ESD)	The Directory Application Feature can continue to be used in Utility Services 7.1 but is subject to the contents of PSN027052u – a summary of which is given below. It is also not possible to use Third Party Certificates with ESD using the "esdtlscert" script that is referenced in some documents. "PSN027052u – Avaya Aura® Utility Services End of Bug Fix Support for Directory Application Feature However, if a software issue is found, there is no longer the ability to provide software fixes or enhancements specific to the Directory Application Feature. Users should begin to investigate other solutions such as Avaya Equinox™, Avaya Aura® System Manager and Avaya Aura® Presence Services that will support LDAP integration with directory service providers; for example, Active Directory."

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>

Feature	7.0.x Command	7.1.x Command
	/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 in Release 7.1.x.x

Fixes in Utility Services Release 7.1.3.8

The following table lists the fixes in Release 7.1.3.8. These fixes apply over and above the fixes in Release 7.1.3.

ID	Minimum Conditions	Visible symptoms	Found in Release
UTILSERV-1193	Utility Services 7.1.x	RHSA-2020:5437-01 important: kernel security and bug fix update	7.1.3.7
UTILSERV-1190	Utility Services 7.1.x	138851 - Apache Tomcat 7.0.x lt 7.0.105 WebSocket DoS (tcp)	7.1.3.7
UTILSERV-1189	Utility Services 7.1.x	142009 - RHEL 7 : java-1.8.0-openjdk (RHSA-2020:4350) (tcp)	7.1.3.7
UTILSERV-1187	Utility Services 7.1.x	143079 - RHEL 7 : hunspell (RHSA-2020:3971) (tcp)	7.1.3.7
UTILSERV-1185	Utility Services 7.1.x	142709 - RHEL 7 : kernel (RHSA-2020:5023) (tcp)	7.1.3.7
UTILSERV-1184	Utility Services 7.1.x	142699 - RHEL 7 : python (RHSA-2020:5009) (tcp)	7.1.3.7
UTILSERV-1183	Utility Services 7.1.x	142715 - RHEL 7 : microcode_ctl (RHSA-2020:5083) (tcp)	7.1.3.7
UTILSERV-1181	Utility Services 7.1.x	143068 - RHEL 7 : cups (RHSA-2020:3864) (tcp)	7.1.3.7
UTILSERV-1180	Utility Services 7.1.x	142454 - RHEL 7 : libX11 (RHSA-2020:4908) (tcp)	7.1.3.7
UTILSERV-1177	Utility Services 7.1.x	142906 - RHEL 7 : bind (RHSA-2020:5011) (tcp)	7.1.3.7
UTILSERV-1176	Utility Services 7.1.x	142705 - RHEL 7 : curl (RHSA-2020:5002) (tcp)	7.1.3.7
UTILSERV-1174	Utility Services 7.1.x	143078 - RHEL 7 : dnsmasq (RHSA-2020:3878) (tcp)	7.1.3.7
UTILSERV-1171	Utility Services 7.1.x	142457 - RHEL 7 : freetype (RHSA-2020:4907) (tcp)	7.1.3.7
UTILSERV-1169	Utility Services 7.1.x	143072 - RHEL 7 : openldap (RHSA-2020:4041) (tcp)	7.1.3.7
UTILSERV-1166	Utility Services 7.1.x	[RHSA-2020:4276] Important: kernel security update	7.1.3.7
UTILSERV-1165	Utility Services 7.1.x	RHSA-2020-4005 libxslt security update	7.1.3.7

ID	Minimum Conditions	Visible symptoms	Found in Release
UTILSERV-1163	Utility Services 7.1.x	RHSA-2020-3901 libpng security update	7.1.3.7
UTILSERV-1151	Utility Services 7.1.x	138374 - Red Hat curl local file overwrites (CVE-2020-8177) (tcp)	7.1.3.7
UTILSERV-1133	Utility Services 7.1.x	137313 - RHEL 7 : microcode_ctl (RHSA-2020:2432) (tcp)	7.1.3.7
UTILSERV-1108	Utility Services 7.1.x	Security issue with sms_test.php	7.1.3.5
UTILSERV-542	Utility Services 7.1.x	SMS rpm from AES for AES-16068 where UTF8 native name improperly handled	7.1.3.0

Fixes in Utility Services Release 7.1.3.7

The following table lists the fixes in Release 7.1.3.7. These fixes apply over and above the fixes in Release 7.1.3.

ID	Minimum Conditions	Visible symptoms	Found in Release
UTILSERV-1072	Utility Services 7.1.x	RHSA-2020:1000 Moderate/Sec. rsyslog-8.24.0-52.el7.x86_64	7.1.3.6
UTILSERV-1073	Utility Services 7.1.x	RHSA-2020:1011 Moderate/Sec. expat-2.1.0-11.el7.x86_64	7.1.3.6
UTILSERV-1074	Utility Services 7.1.x	RHSA-2020:1016 Moderate/Sec. kernel-3.10.0-1127.el7.x86_64	7.1.3.6
UTILSERV-1075	Utility Services 7.1.x	RHSA-2020:1020 Low/Sec. curl-7.29.0-57.el7.x86_64	7.1.3.6
UTILSERV-1076	Utility Services 7.1.x	RHSA-2020:1021 Moderate/Sec. gsettings-desktop-schemas-3.28.0-3.el7.x86_64	7.1.3.6
UTILSERV-1077	Utility Services 7.1.x	RHSA-2020:1022 Low/Sec. file-5.11-36.el7.x86_64	7.1.3.6
UTILSERV-1078	Utility Services 7.1.x	RHSA-2020:1050 Moderate/Sec. cups-libs-1:1.6.3-43.el7.x86_64	7.1.3.6
UTILSERV-1079	Utility Services 7.1.x	RHSA-2020:1061 Moderate/Sec. bind-32:9.11.4-16.P2.el7.x86_64	7.1.3.6
UTILSERV-1080	Utility Services 7.1.x	RHSA-2020:1080 Moderate/Sec. atk-2.28.1-2.el7.x86_64	7.1.3.6
UTILSERV-1081	Utility Services 7.1.x	RHSA-2020:1100 Moderate/Sec. mariadb-libs-1:5.5.65-1.el7.x86_64	7.1.3.6
UTILSERV-1082	Utility Services 7.1.x	RHSA-2020:1112 Moderate/Sec. php-5.4.16-48.el7.x86_64	7.1.3.6
UTILSERV-1083	Utility Services 7.1.x	RHSA-2020:1113 Moderate/Sec. bash-4.2.46-34.el7.x86_64	7.1.3.6
UTILSERV-1084	Utility Services 7.1.x	RHSA-2020:1121 Moderate/Sec. httpd-2.4.6-93.el7.x86_64	7.1.3.6
UTILSERV-1085	Utility Services 7.1.x	RHSA-2020:1131 Moderate/Sec. python-2.7.5-88.el7.x86_64	7.1.3.6
UTILSERV-1086	Utility Services 7.1.x	RHSA-2020:1135 Low/Sec. polkit-0.112-26.el7.x86_64	7.1.3.6

ID	Minimum Conditions	Visible symptoms	Found in Release
UTILSERV-1087	Utility Services 7.1.x	RHSA-2020:1138 Low/Sec. gettext-0.19.8.1-3.el7.x86_64	7.1.3.6
UTILSERV-1088	Utility Services 7.1.x	RHSA-2020:1176 Low/Sec. avahi-libs-0.6.31-20.el7.x86_64	7.1.3.6
UTILSERV-1089	Utility Services 7.1.x	RHSA-2020:1180 Moderate/Sec. emacs-filesystem-1:24.3-23.el7.noarch	7.1.3.6
UTILSERV-1090	Utility Services 7.1.x	RHSA-2020:1181 Low/Sec. unzip-6.0-21.el7.x86_64	7.1.3.6
UTILSERV-1091	Utility Services 7.1.x	RHSA-2020:1190 Moderate/Sec. libxml2-2.9.1-6.el7.4.x86_64	7.1.3.6
UTILSERV-1092	Utility Services 7.1.x	RHSA-2020:1512 Important/Sec. java-1.8.0-openjdk-1:1.8.0.252.b09-2.el7_8.x86_64	7.1.3.6
UTILSERV-1093	Utility Services 7.1.x	sshd supports weak key exchange algorithms	7.1.3.6
UTILSERV-1094	Utility Services 7.1.x	Apache Tomcat Remote Code Execution via session persistence (CVE-2020-9484)	7.1.3.6
UTILSERV-1097	Utility Services 7.1.x	Need update for RHSA-2020-2344 bind security update Reference ASA-2020-079	7.1.3.3
UTILSERV-1098	Utility Services 7.1.x	Need update for RHSA-2020-2082 reference ASA-2020-075 kernel update and bug fixes	7.1.3
UTILSERV-1099	Utility Services 7.1.x	XSS vulnerability (cross site scripting)	7.1.3.6
UTILSERV-1100	Utility Services 7.1.x	RHEL 7 : microcode_ctl (RHSA-2020:2432)	7.1.3.6
UTILSERV-1101	Utility Services 7.1.x	RHEL 7 : dbus (RHSA-2020:2894)	7.1.3.6
UTILSERV-1102	Utility Services 7.1.x	RHEL 7 : unbound (RHSA-2020:2642)	7.1.3.6
UTILSERV-1103	Utility Services 7.1.x	RHEL 7 : ntp (RHSA-2020:2663)	7.1.3.6
UTILSERV-1104	Utility Services 7.1.x	RHEL 7 : kernel (RHSA-2020:2664)	7.1.3.6
UTILSERV-1105	Utility Services 7.1.x	RHEL 7 : grub2 (RHSA-2020:3217)	7.1.3.6
UTILSERV-1106	Utility Services 7.1.x	need to remove weak ciphers	7.1.3.6
UTILSERV-1107	Utility Services 7.1.x	Important: WebSocket DoS Vulnerability CVE-2020-13935	7.1.3.6
UTILSERV-1109	Utility Services 7.1.x	UtilServ should disable ssh AllowTCPForwarding CVE-2004-1653	7.1.3.6
UTILSERV-1112	Utility Services 7.1.x	HSTS Missing From HTTPS Server	7.1.3.6
UTILSERV-1116	Utility Services 7.1.x	RHEL 7 : grub2 (RHSA-2020:3276)	7.1.3.6
UTILSERV-1117	Utility Services 7.1.x	RHEL 7 : avahi (RHSA-2020:1176)	7.1.3.6
UTILSERV-1118	Utility Services 7.1.x	RHEL 7 : curl (RHSA-2020:3916)	7.1.3.6
UTILSERV-1119	Utility Services 7.1.x	RHEL 7 : NetworkManager (RHSA-2020:4003)	7.1.3.6

ID	Minimum Conditions	Visible symptoms	Found in Release
UTILSERV-1121	Utility Services 7.1.x	RHEL 7 : java-1.8.0-openjdk (RHSA-2020:2968)	7.1.3.6
UTILSERV-1122	Utility Services 7.1.x	RHEL 7 : unzip (RHSA-2020:1181)	7.1.3.6
UTILSERV-1123	Utility Services 7.1.x	RHEL 7 : httpd (RHSA-2020:3958)	7.1.3.6
UTILSERV-1124	Utility Services 7.1.x	RHEL 7 : rsyslog (RHSA-2020:1000)	7.1.3.6
UTILSERV-1125	Utility Services 7.1.x	RHEL 7 : expat (RHSA-2020:3952)	7.1.3.6
UTILSERV-1126	Utility Services 7.1.x	RHEL 7 : file (RHSA-2020:1022)	7.1.3.6
UTILSERV-1127	Utility Services 7.1.x	RHEL 7 : libcroco (RHSA-2020:4072)	7.1.3.6
UTILSERV-1129	Utility Services 7.1.x	RHEL 7 : gettext (RHSA-2020:1138)	7.1.3.6
UTILSERV-1130	Utility Services 7.1.x	RHEL 7 : systemd (RHSA-2020:4007)	7.1.3.6
UTILSERV-1131	Utility Services 7.1.x	RHEL 7 : grub2 (RHSA-2020:3217)	7.1.3.6
UTILSERV-1132	Utility Services 7.1.x	RHEL 7 : glibc (RHSA-2020:3861)	7.1.3.6
UTILSERV-1134	Utility Services 7.1.x	RHEL 7 : nss and nspr (RHSA-2020:4076)	7.1.3.6
UTILSERV-1135	Utility Services 7.1.x	RHEL 7 : python (RHSA-2020:1131)	7.1.3.6
UTILSERV-1136	Utility Services 7.1.x	RHEL 7 : php (RHSA-2020:1112)	7.1.3.6
UTILSERV-1137	Utility Services 7.1.x	RHEL 7 : ImageMagick (RHSA-2020:1180)	7.1.3.6
UTILSERV-1138	Utility Services 7.1.x	RHEL 7 : glib2 and ibus (RHSA-2020:3978)	7.1.3.6
UTILSERV-1139	Utility Services 7.1.x	RHEL 7 : cups (RHSA-2020:1050)	7.1.3.6
UTILSERV-1140	Utility Services 7.1.x	RHEL 7 : libtiff (RHSA-2020:3902)	7.1.3.6
UTILSERV-1141	Utility Services 7.1.x	RHEL 7 : evolution (RHSA-2020:1080)	7.1.3.6
UTILSERV-1142	Utility Services 7.1.x	RHEL 7 : mariadb (RHSA-2020:4026)	7.1.3.6
UTILSERV-1143	Utility Services 7.1.x	RHEL 7 : ntp (RHSA-2020:2663)	7.1.3.6
UTILSERV-1144	Utility Services 7.1.x	RHEL 7 : cpio (RHSA-2020:3908)	7.1.3.6
UTILSERV-1145	Utility Services 7.1.x	RHEL 7 : dbus (RHSA-2020:4032)	7.1.3.6
UTILSERV-1146	Utility Services 7.1.x	RHEL 7 : polkit (RHSA-2020:1135)	7.1.3.6
UTILSERV-1147	Utility Services 7.1.x	RHEL 7 : kernel (RHSA-2020:4060)	7.1.3.6
UTILSERV-1148	Utility Services 7.1.x	RHEL 7 : kernel (RHSA-2020:2832)	7.1.3.6
UTILSERV-1149	Utility Services 7.1.x	RHEL 7 : bind (RHSA-2020:2344)	7.1.3.6
UTILSERV-1150	Utility Services 7.1.x	RHEL 7 : GNOME (RHSA-2020:1021)	7.1.3.6
UTILSERV-1152	Utility Services 7.1.x	RHEL 7 : bash (RHSA-2020:1113)	7.1.3.6
UTILSERV-1153	Utility Services 7.1.x	RHEL 7 : e2fsprogs (RHSA-2020:4011)	7.1.3.6
UTILSERV-1154	Utility Services 7.1.x	RHEL 7 : libssh2 (RHSA-2020:3915)	7.1.3.6

Fixes in Utility Services Release 7.1.3.6

The following table lists the fixes in Release 7.1.3.6. These fixes apply over and above the fixes in Release 7.1.3.

ID	Minimum Conditions	Visible symptoms	Found in Release
UTILSERV-1048	Utility Services 7.1.x	RHSA-2019-2600: kernel security and bug fix update	7.1.3.5
UTILSERV-1052	Utility Services 7.1.x	RHSA-2019:3834: Important: kernel security update	7.1.3.5
UTILSERV-1053	Utility Services 7.1.x	RHSA-2019:3872: Important: kernel security update	7.1.3.5
UTILSERV-1054	Utility Services 7.1.x	RHSA-2019:3976: Low: tcpdump security update	7.1.3.5
UTILSERV-1055	Utility Services 7.1.x	RHSA-2019:4190: Important: nss, nss-softokn, nss-util security update	7.1.3.5
UTILSERV-1056	Utility Services 7.1.x	RHSA-2019:3979: Important: kernel security and bug fix update	7.1.3.5
UTILSERV-1057	Utility Services 7.1.x	Tomcat Moderate: Local Privilege Escalation CVE-2019-12418 , CVE-2019-17563 and CVE-2019-0221	7.1.3.5
UTILSERV-1058	Utility Services 7.1.x	RHSA-2019:4254-01: Moderate: freetype security update	7.1.3.5
UTILSERV-1060	Utility Services 7.1.x	RHSA-2020:0374 :kernel update	7.1.3.5
UTILSERV-1062	Utility Services 7.1.x	RHSA-2020:0227: sqlite update	7.1.3.5
UTILSERV-1068	Utility Services 7.1.x	High: AJP Request Injection and potential Remote Code Execution CVE-2020-1938 HTTP Request Smuggling CVE-2020-1935 CVE-2019-17569	7.1.3.5
UTILSERV-1069	Utility Services 7.1.x	RHSA-2020:0834: Important/Sec. kernel-3.10.0-1062.18.1.el7.x86_64	7.1.3.5
UTILSERV-1070	Utility Services 7.1.x	RHSA-2020:0897: Important/Sec. libicu-50.2-4.el7_7.x86_64	7.1.3.5
UTILSERV-1071	Utility Services 7.1.x	RHSA-2020:0630: Important/Sec. ppp-2.4.5-34.el7_7.x86_64	7.1.3.5

Fixes in Utility Services Release 7.1.3.5

The following table lists the fixes in Release 7.1.3.5. These fixes apply over and above the fixes in Release 7.1.3.

ID	Minimum Conditions	Visible symptoms	Found in Release
UTILSERV-1051	Utility Services 7.1.x	Security updates: RHSA-2019:3286 Critical/Sec. php-5.4.16-46.1.el7_7.x86_64 RHSA-2019:3197 Important/Sec. sudo-1.8.23-4.el7_7.1.x86_64 RHSA-2019:3128 Important/Sec. java-1.8.0-openjdk-1:1.8.0.232.b09-0.el7_7.x86_64 RHSA-2019:3055 Important/Sec. kernel-3.10.0-1062.4.1.el7.x86_64 RHSA-2019:2896 Low/Sec. redhat-release-server-7.4-18.el7_4.6.x86_64 RHSA-2019:2829 Important/Sec. kernel-3.10.0-1062.1.2.el7.x86_64 RHSA-2019:2571 Important/Sec. pango-1.42.4-4.el7_7.x86_64 RHSA-2019:2343 Moderate/Sec. httpd-2.4.6-90.el7.x86_64	7.1.3.4

ID	Minimum Conditions	Visible symptoms	Found in Release
		RHSA-2019:2327 Moderate/Sec. mariadb-libs-1:5.5.64-1.el7.x86_64 RHSA-2019:2304 Moderate/Sec. openssl-1:1.0.2k-19.el7.x86_64 RHSA-2019:2272 Moderate/Sec. python-urllib3-1.10.2-7.el7.noarch RHSA-2019:2237 Moderate/Sec. nspr-4.21.0-1.el7.x86_64 RHSA-2019:2197 Low/Sec. elfutils-0.176-2.el7.x86_64 RHSA-2019:2189 Moderate/Sec. procps-ng-3.3.10-26.el7.x86_64 RHSA-2019:2181 Low/Sec. curl-7.29.0-54.el7.x86_64 RHSA-2019:2177 Moderate/Sec. libsss_idmap-1.16.4-21.el7.x86_64 RHSA-2019:2169 Important/Sec. linux-firmware-20190429-72.gitddde598.el7.noarch RHSA-2019:2162 Low/Sec. blktrace-1.0.5-9.el7.x86_64 RHSA-2019:2159 Low/Sec. unzip-6.0-20.el7.x86_64 RHSA-2019:2143 Low/Sec. openssh-7.4p1-21.el7.x86_64 RHSA-2019:2136 Moderate/Sec. libssh2-1.8.0-3.el7.i686 RHSA-2019:2118 Moderate/Sec. glibc-2.17-292.el7.i686 RHSA-2019:2110 Moderate/Sec. rsyslog-8.24.0-38.el7.x86_64 RHSA-2019:2091 Moderate/Sec. libgudev1-219-67.el7.x86_64 RHSA-2019:2079 Moderate/Sec. libX11-1.6.7-2.el7.x86_64 RHSA-2019:2077 Low/Sec. ntp-4.2.6p5-29.el7.x86_64 RHSA-2019:2075 Moderate/Sec. binutils-2.27-41.base.el7.x86_64 RHSA-2019:2060 Moderate/Sec. dhclient-12:4.2.5-77.el7.x86_64 RHSA-2019:2057 Moderate/Sec. bind-32:9.11.4-9.P2.el7.x86_64 RHSA-2019:2053 Moderate/Sec. libtiff-4.0.3-32.el7.x86_64 RHSA-2019:2052 Moderate/Sec. libjpeg-turbo-1.2.90-8.el7.x86_64 RHSA-2019:2049 Moderate/Sec. libmspack-0.5-0.7.alpha.el7.x86_64 RHSA-2019:2047 Moderate/Sec. libcgroup-0.41-21.el7.x86_64 RHSA-2019:2046 Moderate/Sec. polkit-0.112-22.el7.x86_64 RHSA-2019:2035 Low/Sec. python-requests-2.6.0-5.el7.noarch RHSA-2019:2030 Moderate/Sec. python-2.7.5-86.el7.x86_64 RHSA-2019:1947 Important/Sec. vim-common-2:7.4.160-2.el7_4.1.x86_64 RHSA-2019:1884 Moderate/Sec. libssh2-1.4.3-12.el7_6.3.i686 RHSA-2019:1815 Moderate/Sec. java-1.8.0-openjdk-1:1.8.0.222.b10-0.el7_6.x86_64	
UTILSERV-1050	Utility Services 7.1.x	[RHSA-2019:3197] Important: sudo security update	7.1.3.4
UTILSERV-1049	Utility Services 7.1.x	[RHSA-2019:3055] Important: kernel security and bug fix update	7.1.3.4

ID	Minimum Conditions	Visible symptoms	Found in Release
UTILSERV-1043	Utility Services 7.1.x	Custom login banner was not shown on web login home page	7.1.3
UTILSERV-1029	Utility Services 7.1.x	[RHSA-2019-1815] OpenJDK: security issue	7.1.3.4
UTILSERV-1027	Utility Services 7.1.x	[RHSA-2019:1619] RHEL 7 / 8 : vim (RHSA-2019:1619) (tcp)	7.1.3.4
UTILSERV-1026	Utility Services 7.1.x	[RHSA-2019:1587] Important/Sec. python.x86_64	7.1.3.4

Fixes in Utility Services Release 7.1.3.4

The following table lists the fixes in Release 7.1.3.4. These fixes apply over and above the fixes in Release 7.1.3.

ID	Minimum Conditions	Visible symptoms	Found in Release
UTILSERV-1025	Initial install	[CVE-2019-0221] Apache Tomcat XSS in SSI printenv	7.1.3
UTILSERV-1024	Initial Install	[RHSA-2019:1228-01] Important: wget security update	7.1.3
UTILSERV-1023	Initial Install	[RHSA-2019:1481] Kernel update for RHEL7	7.1.3
UTILSERV-1021	Initial Install	[RHSA-2019:1294] [MEDIUM] RHEL 7 : bind update	7.1.3
UTILSERV-1020	Initial Install	[RHSA-2019:1168] [HIGH] RHEL 7 : kernel update	7.1.3
UTILSERV-1016	Initial Install	Security vulnerability apache banner reveals information	7.1.3
UTILSERV-1014	Initial Install	[RHSA-2018-0849] gcc security, bug fix, and enhancement update	7.1.3
UTILSERV-1013	Initial Install	[RHSA-2018:0094] update kernel (linux firmware) for RHEL7	7.1.3
UTILSERV-1012	Initial Install	[RHSA-2018:0093] 106088 - RHEL 6 / 7 : microcode_ctl (Spectre) (tcp)	7.1.3
UTILSERV-1011	Initial Install	[RHSA-2019:0818] Update kernel for RHEL7	7.1.3
UTILSERV-1010	Initial Install	SSHD configuration enhanced to support ciphers prescribed by NIST	7.1.3
UTILSERV-1009	Initial Install	[RHSA-2019:0818-01] Important: kernel security and bug fix update	7.1.3
UTILSERV-1008	Initial Install	[RHSA-2019:0485-01] Moderate: tomcat security update	7.1.3
UTILSERV-1007	Initial Install	[RHSA-2019:0679-01] Important: libssh2 security update	7.1.3
UTILSERV-1006	Initial Install	[RHSA-2019:0710-01] Important: python security update	7.1.3
UTILSERV-1005	Initial Install	[RHSA-2019:0483-01] Moderate: openssl security and bug fix update	7.1.3
UTILSERV-1004	Initial Install	[RHSA-2019:0512-01] Important: kernel security, bug fix, and enhancement update	7.1.3
UTILSERV-1003	Initial Install	[RHSA-2019:0201] [LOW] RHEL 7 : systemd update	7.1.3

ID	Minimum Conditions	Visible symptoms	Found in Release
UTILSERV-1002	Initial Install	[RHSA-2019:0368] [MEDIUM] RHEL 7 : systemd update	7.1.3
UTILSERV-1001	Initial Install	[RHSA-2019:0230] [Medium] - RHEL 7 : polkit update	7.1.3
UTILSERV-1000	Initial Install	[RHSA-2019:0163] [MEDIUM] RHEL 7 : kernel update	7.1.3
UTILSERV-999	Initial Install	[RHSA-2019:0435] [MEDIUM] RHEL 7 : java-1.8.0-openjdk update	7.1.3
UTILSERV-998	Initial Install	[RHSA-2019:0049] [HIGH] RHEL 7 : systemd update	7.1.3
UTILSERV-997	Initial Install	[RHSA-2019:0194] [MEDIUM] RHEL 7 : bind update	7.1.3
UTILSERV-996	Initial Install	[RHSA-2019:0109] [HIGH] RHEL 7 : perl update	7.1.3
UTILSERV-995	Initial Install	Unwanted wireless packages observed on the system	7.1.3
UTILSERV-994	Initial Install	Privileged escalation possible with sudoers	7.1.3
UTILSERV-973	Initial Install	Admin web page upload files allowed for remote command execution	7.1.3

Fixes in Utility Services Release 7.1.3.3

The following table lists the fixes in Release 7.1.3.3. These fixes apply over and above the fixes in Release 7.1.2.

ID	Minimum Conditions	Visible symptoms	Found in Release
UTILSERV-982	Initial Install	108988 - RHEL 7 : gcc (RHSA-2018:0849) (tcp)	7.1.3
UTILSERV-981	Initial Install	111802 - RHEL 7 : mariadb (RHSA-2018:2439) (tcp)	7.1.3
UTILSERV-979	Initial Install	119172 - RHEL 7 : NetworkManager (RHSA-2018:3665) (tcp)	7.1.3
UTILSERV-978	Initial Install	118726 - RHEL 7 : GNOME (RHSA-2018:3140) (tcp)	7.1.3
UTILSERV-977	Initial Install	112104 - RHEL 7 : postgresql (RHSA-2018:2557) (tcp)	7.1.3
UTILSERV-965	Initial Install	118186 - RHEL 7 : java-1.8.0-openjdk (RHSA-2018:2942) (tcp)	7.1.3.2
UTILSERV-964	Initial Install	118525 - RHEL 7 : kernel (RHSA-2018:3083) (tcp)	7.1.3.2
UTILSERV-963	Initial Install	118539 - RHEL 7 : jasper (RHSA-2018:3253) (tcp)	7.1.3.2
UTILSERV-962	Initial Install	118527 - RHEL 7 : glibc (RHSA-2018:3092) (tcp)	7.1.3.2
UTILSERV-961	Initial Install	118516 - RHEL 7 : gnutls (RHSA-2018:3050) (tcp)	7.1.3.2
UTILSERV-960	Initial Install	118515 - RHEL 7 : python (RHSA-2018:3041) (tcp)	7.1.3.2
UTILSERV-959	Initial Install	118533 - RHEL 7 : sssd (RHSA-2018:3158) (tcp)	7.1.3.2
UTILSERV-958	Initial Install	118532 - RHEL 7 : curl and nss-pem (RHSA-2018:3157) (tcp)	7.1.3.2
UTILSERV-957	Initial Install	118538 - RHEL 7 : setup (RHSA-2018:3249) (tcp)	7.1.3.2
UTILSERV-956	Initial Install	118514 - RHEL 7 : binutils (RHSA-2018:3032) (tcp)	7.1.3.2
UTILSERV-955	Initial Install	118517 - RHEL 7 : wget (RHSA-2018:3052) (tcp)	7.1.3.2
UTILSERV-954	Initial Install	118534 - RHEL 7 : openssl (RHSA-2018:3221) (tcp)	7.1.3.2
UTILSERV-953	Initial Install	118523 - RHEL 7 : krb5 (RHSA-2018:3071) (tcp)	7.1.3.2
UTILSERV-952	Initial Install	118529 - RHEL 7 : wpa_supplicant (RHSA-2018:3107) (tcp)	7.1.3.2

ID	Minimum Conditions	Visible symptoms	Found in Release
UTILSERV-951	Initial Install	118541 - RHEL 7 : libmspack (RHSA-2018:3327) (tcp)	7.1.3.2
UTILSERV-950	Initial Install	118520 - RHEL 7 : X.org X11 (RHSA-2018:3059) (tcp)	7.1.3.2
UTILSERV-949	Initial Install	118540 - RHEL 7 : fuse (RHSA-2018:3324) (tcp)	7.1.3.2
UTILSERV-972	Initial Install	Update OpenJDK RPMs per RHSA-2018:2943	7.1
UTILSERV-947	Initial Install	On the certificate signing request web page (CSR), the CN of the RDN was being shown as the hostname instead of an option to show hostname or FQDN.	7.1.0.0.1
UTILSERV-946	Initial Install	Important: Apache Tomcat: Information Disclosure (CVE-2018-8037)	7.1.3
UTILSERV-971	Initial Install	Apache Tomcat - Medium: Open Redirect (CVE-2018-11784)	7.1.3.2
UTILSERV-931	Initial Install	Medium : Apache Tomcat - Security Constraint Bypass (CVE-2018-8034)	7.1.3.2
UTILSERV-930	Initial Install	Medium: Apache Tomcat - Denial of Service (CVE-2018-1336)	7.1.3.2
UTILSERV-944	Initial Install	Utility Services had a security bug where it would incorrectly allow user privilege escalation.	7.1.3
UTILSERV-969	Initial Install	L1TF new kernel options support in Utility Services.	7.1.3
UTILSERV-943	Initial Install	[RHSA-2018:2748-01] Important: kernel security and bug fix update	7.1.3.2

Fixes in Utility Services Release 7.1.3.2

The following table lists the fixes in Release 7.1.3.2. These fixes apply over and above the fixes in Release 7.1.2.

ID	Minimum Conditions	Visible symptoms	Found in Release
UTILSERV-936	Initial Install	[RHSA-2018:2123-01] Moderate: python security update	7.1
UTILSERV-935	Initial Install	tzdata Linux RPM updated to tzdata-2018e	7.1
UTILSERV-934	Initial Install	[RHSA-2018:2571-01] Important: bind security update	7.1
UTILSERV-933	Initial Install	Important: [RHSA-2018:2285] yum-utils security update	7.1
UTILSERV-932	Initial Install	Important: [RHSA-2018:2387] L1TF - L1 Terminal Fault Attack - CVE-2018-3620 & CVE-2018-3646	7.1
UTILSERV-929	Initial Install	[RHSA-2018:2242-01] Moderate: java-1.8.0-openjdk security and bug fix update	7.1
UTILSERV-928	Initial Install	[RHSA-2018:2181-01] Important: gnupg2 security update	7.1
UTILSERV-926	Initial Install	passwords stored in clear text	7.1
UTILSERV-924	Initial Install	Update add_spirit_certs support for non-FIPS mode	7.1
UTILSERV-922	Initial Install	[RHSA-2018:1852-01] Moderate: kernel security update	7.1
UTILSERV-916	Initial Install	Fix PHP Timezone	7.1
UTILSERV-915	Initial Install	[RHSA-2018:1629-01] Important: kernel security update	7.1
UTILSERV-913	Initial Install	[RHSA-2018:1700-01] Important: procps-ng security update	7.1
UTILSERV-912	Initial Install	[RHSA-2018:1649-01] Important: java-1.8.0-openjdk security	7.1

ID	Minimum Conditions	Visible symptoms	Found in Release
		update	
UTILSERV-910	Initial Install	[RHSA-2018:1453-01] Critical: dhcp security update	7.1
UTILSERV-907	Initial Install	[RHSA-2018:1318-01] Important: kernel security, bug fix, and enhancement update	7.1
UTILSERV-906	Initial Install	[RHSA-2018:1191-01] Critical: java-1.8.0-openjdk security update	7.1
UTILSERV-905	Initial Install	Apache Tomcat Security constraint annotations applied too late (CVE-2018-1305)	7.1
UTILSERV-900	Initial Install	[RHSA-2018:0805-01] Moderate: glibc security, bug fix, and enhancement update	7.1
UTILSERV-899	Initial Install	[RHSA-2018:0855-01] Moderate: ntp security, bug fix, and enhancement update	7.1
UTILSERV-898	Initial Install	[RHSA-2018:0998-01] Moderate: openssl security and bug fix update	7.1
UTILSERV-897	Initial Install	[RHSA-2018:0849-01] Low: gcc security, bug fix, and enhancement update	7.1
UTILSERV-896	Initial Install	[RHSA-2018:1062-01] Important: kernel security, bug fix, and enhancement update	7.1
UTILSERV-895	Initial Install	RHSA-2018:0666-01] Moderate: krb5 security, bug fix, and enhancement update	7.1
UTILSERV-894	Initial Install	[RHSA-2018:0980-01] Low: openssh security, bug fix, and enhancement update	7.1
UTILSERV-893	Initial Install	[RHSA-2018:0913-01] Low: policycoreutils security, bug fix, and enhancement update	7.1

Fixes in Utility Services Release 7.1.3

The following table lists the fixes in Release 7.1.3. These fixes apply over and above the fixes in Release 7.1.2.

ID	Minimum Conditions	Visible symptoms	Found in Release
UTILSERV-600	Initial Install	Trust establishment failed on Utility services 7.1.0.0.0.12 on SDM client	7.1
UTILSERV-619	Initial Install	The DHCP Service displays wrong status with audit account	7.1
UTILSERV-705	Initial Install	Support for vSphere 6.7	7.1
UTILSERV-768	Initial Install	ZAP:High Path Traversal	7.1
UTILSERV-769	Initial Install	ZAP:High SQL Injection	7.1
UTILSERV-770	Initial Install	ZAP:High Cross Site Scripting (Reflected)	7.1
UTILSERV-771	Initial Install	ZAP:Medium Directory Browsing	7.1
UTILSERV-773	Initial Install	ZAP:Medium X-Frame-Options Header Not Set	7.1
UTILSERV-774	Initial Install	ZAP:Medium Format String Error	7.1
UTILSERV-777	Initial Install	CRITICAL: [RHSA-2017:2836-01] Critical: dnsmasq security update	7.1

ID	Minimum Conditions	Visible symptoms	Found in Release
UTILSERV-778	Initial Install	Customer banner on Utility services shows invalid output when seen via SSH session	7.1
UTILSERV-780	Initial Install	RHEL 7 : wpa_supplicant (RHSA-2017:2907) (KRACK) (tcp)	7.1
UTILSERV-783	Initial Install	RHEL 7 : emacs (RHSA-2017:2771) (tcp)	7.1
UTILSERV-784	Initial Install	RHEL 7 : bind (RHSA-2017:2533) (tcp)	7.1
UTILSERV-786	Initial Install	RHEL 7 : httpd (RHSA-2017:2882) (Optionsbleed) (tcp)	7.1
UTILSERV-787	Initial Install	RHEL 6 / 7 : nss (RHSA-2017:2832) (tcp)	7.1
UTILSERV-818	Initial Install	RHEL 6 / 7 : java-1.8.0-openjdk (RHSA-2017:2998) (tcp)	7.1
UTILSERV-825	Initial Install	Correct Root Certificate Display & Fix Windows Format Files	7.1
UTILSERV-826	Initial Install	Allow Access Control script, Configure_SSH_ACL.sh, to run in "Services Port Only" mode	7.1
UTILSERV-829	Initial Install	HIGH Priority: [RHSA-2017:3075-01] Important: wget security update	7.1
UTILSERV-834	Initial Install	104568 - RHEL 7 : php (RHSA-2017:3221) (tcp)	7.1
UTILSERV-842	Initial Install	MEDIUM: [RHSA-2017:3263-01] Moderate: curl security update	7.1
UTILSERV-846	Initial Install	HIGH: [RHSA-2017:3269-01] Important: procmail security update	7.1
UTILSERV-847	Initial Install	HIGH Priority: [RHSA-2017:3270-01] Important: apr security update	7.1
UTILSERV-848	Initial Install	MEDIUM: [RHSA-2017:3315-01] Important: kernel security and bug fix update	7.1
UTILSERV-849	Initial Install	849 If AIDE is enabled, need to run AIDE update after applying updates and / or performing a restore	7.1
UTILSERV-850	Initial Install	MEDIUM: [RHSA-2017:3379-01] Moderate: sssd security and bug fix update	7.1
UTILSERV-851	Initial Install	MEDIUM: [RHSA-2017:3402-01] Moderate: postgresql security update	7.1
UTILSERV-852	Initial Install	Update Initial_conf.sh to update the entries in /etc/hosts	7.1
UTILSERV-854	Initial Install	HIGH: [RHSA-2018:0007-01] Important: kernel security update	7.1
UTILSERV-855	Initial Install	HIGH: [RHSA-2018:0012-01] Important: microcode_ctl security update	7.1
UTILSERV-856	Initial Install	HIGH: [RHSA-2018:0014-01] Important: linux-firmware security update	7.1
UTILSERV-861	Initial Install	HIGH Priority: [RHSA-2018:0095-01] Important: java-1.8.0-openjdk security update	7.1
UTILSERV-862	Initial Install	HIGH Priority: [RHSA-2018:0102-01] Important: bind security update	7.1
UTILSERV-868	Initial Install	106332 - RHEL 7 : dhcp (RHSA-2018:0158) (tcp)	7.1
UTILSERV-869	Initial Install	106330 - RHEL 7 : kernel (RHSA-2018:0151) (Meltdown) (Spectre) (tcp)	7.1
UTILSERV-875	Initial Install	MEDIUM: [RHSA-2018:0260-01] Moderate: systemd security update	7.1

ID	Minimum Conditions	Visible symptoms	Found in Release
UTILSERV-877	Initial Install	Addition of Kernel Configuration Script	7.1
UTILSERV-882	Initial Install	[RHSA-2018:0483-01] Important: dhcp security update	7.1
UTILSERV-884	Initial Install	Fix Test Alarms for All Users	7.1
UTILSERV-885	Initial Install	[RHSA-2018:0395-01] Important: kernel security and bug fix update	7.1
UTILSERV-886	Initial Install	[RHSA-2018:0406-01] Moderate: php security update	7.1
UTILSERV-888	Initial Install	Improvements To Configure_SSH_ACL.sh Script	7.1
UTILSERV-890	Initial Install	Restore of 7.1.3 backup can fail	7.1
UTILSERV-901	Initial Install	Fix to swversion permissions issues	7.1

Fixes in Utility Services Release 7.1.2

The following table lists the fixes in Release 7.1.2. These fixes apply over and above the fixes in Release 7.1.1.

ID	Minimum Conditions	Visible symptoms	Found in Release
UTILSERV-619	Initial Install	The DHCP Service displays wrong status with audit account	7.1
UTILSERV-639	Upgrade from 7.0.	The mode of Utility Services is blank after upgrading US from 7.0 to 7.1 build 15	7.1
UTILSERV-659	Initial Install	[RHSA-2017:1208-01] Important: jasper security update	7.1
UTILSERV-661	Initial Install	[RHSA-2017:1262-01] Important: rpcbind security update	7.1
UTILSERV-663	Initial Install	[RHSA-2017:1263-01] Important: libtirpc security update	7.1
UTILSERV-667	Initial Install	[RHSA-2017:1308-01] Important: kernel security, bug fix, and enhancement update	7.1
UTILSERV-669	Initial Install	[RHSA-2017:1382-01] Important: sudo security update	7.1
UTILSERV-682	Initial Install	Apache Tomcat Security Constraint Bypass (CVE-2017-5664)	7.1
UTILSERV-683	Initial Install	[RHSA-2017:1481-01] Important: glibc security update	7.1
UTILSERV-684	Initial Install	[RHSA-2017:1484-01] Important: kernel security update	7.1
UTILSERV-671	Initial Install	[RHSA-2017:1365-03] Important: nss security and bug fix update	7.1
UTILSERV-688	Initial Install	Update tmclient.jar for Spirit Agent	7.1
UTILSERV-691	Initial Install	[RHSA-2017:1574-01] Moderate: sudo security update	7.1
UTILSERV-692	Initial Install	[RHSA-2017:1615-01] Important: kernel security and bug fix update	7.1
UTILSERV-709	Initial Install	[RHSA-2017:1680-01] Important: bind security and bug fix update	7.1
UTILSERV-551	Initial Install	ZAP: Cookie No HttpOnly Flag	7.1
UTILSERV-646	Initial Install	Cannot add the second remote syslog server	7.1
UTILSERV-629	Initial Install	The error message is shown when running the command Add_RSYSLOG.sh on US with FIPS mode enabled	7.1
UTILSERV-685	Initial Install	Addition Commercial FIPS Script	7.1
UTILSERV-677	Initial Install	Create new ovf_set_multi_static script	7.1

ID	Minimum Conditions	Visible symptoms	Found in Release
UTILSERV-712	Initial Install	[RHSA-2017:1789-01] Critical: java-1.8.0-openjdk security update	7.1
UTILSERV-719	Initial Install	Alarms raised in AVP7.1 server are not propagated to Utility Services	7.1
UTILSERV-720	Initial Install	[RHSA-2017:1842-01] Important: kernel security, bug fix, and enhancement update	7.1
UTILSERV-721	Initial Install	[RHSA-2017:1931-01] Moderate: bash security and bug fix update	7.1
UTILSERV-722	Initial Install	[RHSA-2017:1852-01] Moderate: openldap security, bug fix, and enhancement update	7.1
UTILSERV-723	Initial Install	[RHSA-2017:2029-01] Moderate: openssh security, bug fix, and enhancement update	7.1
UTILSERV-724	Initial Install	[RHSA-2017:1868-01] Moderate: python security and bug fix update	7.1
UTILSERV-725	Initial Install	[RHSA-2017:2192-01] Moderate: mariadb security and bug fix update	7.1
UTILSERV-726	Initial Install	[RHSA-2017:1916-01] Moderate: glibc security, bug fix, and enhancement update	7.1
UTILSERV-727	Initial Install	[RHSA-2017:2016-01] Moderate: curl security, bug fix, and enhancement update	7.1
UTILSERV-728	Initial Install	[RHSA-2017:1860-01] Moderate: libtasn1 security, bug fix, and enhancement update	7.1
UTILSERV-729	Initial Install	[RHSA-2017:1865-01] Moderate: X.org X11 libraries security, bug fix and enhancement update	7.1
UTILSERV-730	Initial Install	[RHSA-2017:1871-01] Moderate: tcpdump security, bug fix, and enhancement update	7.1
UTILSERV-731	Initial Install	[RHSA-2017:2292-01] Moderate: gnutls security, bug fix, and enhancement update	7.1
UTILSERV-732	Initial Install	[RHSA-2017:2299-01] Moderate: NetworkManager and libnl3 security, bug fix and enhancement update	7.1
UTILSERV-733	Initial Install	[RHSA-2017:2285-01] Moderate: authconfig security, bug fix, and enhancement update	7.1
UTILSERV-697	Initial Install	Add Missing SUDO entry for Local Pre-Populate Plug-In	7.1
UTILSERV-710	Initial Install	Extend SSH Timeout	7.1
UTILSERV-711	Initial Install	TFTP server cannot be started	7.1
UTILSERV-735	Initial Install	[RHSA-2017:1983-01] Moderate: PostgreSQL security and enhancement update	7.1
UTILSERV-736	Initial Install	[RHSA-2017:2459-01] Important: libsoup security update	7.1
UTILSERV-737	Initial Install	Apache Tomcat Cache Poisoning (CVE-2017-7674)	7.1
UTILSERV-739	Initial Install	[RHSA-2017:2473-01] Important: kernel security and bug fix update	7.1
UTILSERV-740	Initial Install	[RHSA-2017:1574-01] Moderate: sudo security update	7.1
UTILSERV-741	Initial Install	[RHSA-2017:2479-01] Important: httpd security update	7.1

ID	Minimum Conditions	Visible symptoms	Found in Release
UTILSERV-742	Initial Install	Cannot access MyPhone admin page with admin login and password with special characters	7.1
UTILSERV-745	Initial Install	Database Autostart Buttons and Status are not working	7.1
UTILSERV-707	Initial Install	Addition of Hardening Mode configuration files to backup/restore	7.1
UTILSERV-613	Initial Install	96x1 H323 Phone is failed to back up the local device settings to Utility Services	7.1
UTILSERV-748	Initial Install	Serviceability Agent Configuration Updates for Hardened Mode	7.1
UTILSERV-747	Initial Install	Addition of 3rd Party Certificate Support for Tomcat	7.1
UTILSERV-717	Initial Install	Serviceability Agent configuration needs to be updated when FIPS Mode enabled	7.1
UTILSERV-749	Initial Install	Allow Common OS setLoginBanner.sh script to be run with root privileges	7.1
UTILSERV-716	Initial Install	Update the Serviceability Agent Configuration for AVP license alarms for Avaya Aura® Utility Services	7.1
UTILSERV-734	Initial Install	Provide script to import 3rd party certificate and create keystores for Serviceability Agent	7.1
UTILSERV-763	Initial Install	Allow admin users to generate security reports for AIDE and auditd.	7.1
UTILSERV-764	Initial Install	Fix Apache Permissions after Update	7.1
UTILSERV-831	Initial Install	Issue while enabling FIPS mode in Utility Services 7.1.2.0.0.04	7.1
UTILSERV-839	Initial Install	Need to Disable chronyd for NTPD to Auto Start	7.1
UTILSERV-840	Initial Install	AVP licensing alarms not picked up by the Serviceability Agent	7.1
UTILSERV-841	Initial Install	Fix Logrotate Rules for Remote.log	7.1
UTILSERV-843	Initial Install	Add Sudo for Configure NMS Script	7.1
UTILSERV-844	Initial Install	Utility services patching failed via SMGR SDM on US commercial setup	7.1
UTILSERV-845	Initial Install	Issues / changes for the add_spirit_certs script	7.1

Fixes in Utility Services Release 7.1.1

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

ID	Minimum Conditions	Visible symptoms	Found in Release
UTILSERV-661	Initial Install	[RHSA-2017:1262-01] Important: rpcbind security update	7.1
UTILSERV-663	Initial Install	[RHSA-2017:1263-01] Important: libtirpc security update	7.1
UTILSERV-691	Initial Install	[RHSA-2017:1574-01] Moderate: sudo security update	7.1
UTILSERV-692	Initial Install	[RHSA-2017:1615-01] Important: kernel security and bug fix update	7.1

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 in Release 7.1.x.x

Known issues and workarounds in Utility Services Release 7.1.3.8

ID	Minimum conditions	Visible symptoms	Workaround
UTILSERV-1115	Utility Services 7.1.3	69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits (tcp)	Need to delete the stale /etc/pki/certs/Utility_Services.pem file using root account
UTILSERV-1114	Utility Services 7.1.3	35291 - SSL Certificate Signed Using Weak Hashing Algorithm (tcp)	Need to delete the stale /etc/pki/certs/Utility_Services.pem file using root account
UTILSERV-1113	Utility Services 7.1.3	15901 - SSL Certificate Expiry (tcp)	Need to delete the stale /etc/pki/certs/Utility_Services.pem file using root account

Known issues and workarounds in Utility Services Release 7.1.3.7

ID	Minimum conditions	Visible symptoms	Workaround
UTILSERV-1065	Utility Services 7.1.3	Configuration or Integration steps required for sending CDR reports via Emails	None
UTILSERV-1108	Utility Services 7.1.3	Security issue with sms_test.php	None

ID	Minimum conditions	Visible symptoms	Workaround
UTILSERV-1155	Utility Services 7.1.3	TenableIO PCI issue : Patch and Upgrade	None
UTILSERV-1156	Utility Services 7.1.3	TenableIO PCI issue : Access Control	None
UTILSERV-1157	Utility Services 7.1.3	TenableIO PCI issue : Configuration	None

Known issues and workarounds in Utility Services Release 7.1.3.6

ID	Minimum conditions	Visible symptoms	Workaround
UTILSERV-369	Utility Services 7.1.3	When clicking on country in IP Phones settings editor, the info is incorrect.	

Known issues and workarounds in Utility Services Release 7.1.3.5

ID	Minimum conditions	Visible symptoms	Workaround
UTILSERV-975	Utility Services 7.1.3	Backup script for Utility Services would give error if run from the command line interface.	None.
UTILSERV-369	Utility Services 7.1.3	When clicking on country in IP Phones settings editor, the info is incorrect.	
UTILSERV-710	Utility Services 7.x	During installation or deployment of Utility Services, when more than one DNS servers are configured but none of them are reachable, all attempts to ssh to Utility Services after deployment will fail. This includes trying to access Utility Services from the services port.	If this issue is encountered, the workaround provided in PSN027055U can be applied.

Known issues and workarounds in Utility Services Release 7.1.3.4

ID	Minimum conditions	Visible symptoms	Workaround
UTILSERV-975	Utility Services 7.1.3	Backup script for Utility Services would give error if run from the command line interface.	None.
UTILSERV-369	Utility Services 7.1.3	When clicking on country in IP Phones settings editor, the info is incorrect.	

ID	Minimum conditions	Visible symptoms	Workaround
UTILSERV-710	Utility Services 7.x	During installation or deployment of Utility Services, when more than one DNS servers are configured but none of them are reachable, all attempts to ssh to Utility Services after deployment will fail. This includes trying to access Utility Services from the services port.	If this issue is encountered, the workaround provided in PSN027055U can be applied.

Known issues and workarounds in Utility Services Release 7.1.3.3

ID	Minimum conditions	Visible symptoms	Workaround
UTILSERV-975	Utility Services 7.1.3	Backup script for Utility Services would give error if run from the command line interface.	None.

Known issues and workarounds in Utility Services Release 7.1.3.2

ID	Minimum conditions	Visible symptoms	Workaround
None	Update is applied on any previous setup.	The UTILSERV VM does not auto reboot after the updates are installed or updated. Need a manual reboot process to apply new kernel patches.	A manual reboot required to Utility Service VM from SDM Client apps.

Known issues and workarounds in Utility Services Release 7.1.3

ID	Minimum conditions	Visible symptoms	Workaround
UTILSERV-878	Add a new local user via the CLI, but the new user has not logged onto the CLI and set their password.	If the new user attempts to access the Web GUI before they have set their password, the Web GUI will display a message asking the user to change their password – but does not offer a means to achieve this.	Ask the new local user to set their password at the CLI before attempting to use the Web GUI for the first time.
None	Restore a backup with a different Secure Linux mode can cause the Utility Services Virtual Machine to reboot.	If the Web GUI is used to restore a backup with a different Secure Linux mode and a reboot is required to fully implement the changed	This is completely normal operation and no workaround is required – it is simply a warning that the implementation of a Secure Linux mode change may require a reboot.

ID	Minimum conditions	Visible symptoms	Workaround
		mode, then the Web GUI can appear to hang.	
None	Uploading files with Firefox may lead to the files being corrupted or Firefox itself crashing or freezing.	The Firefox Web Browser can corrupt files on upload and can also freeze or crash during the upload.	This is an intermittent issue that is not well understood. However, no similar issues have been observed when using Internet Explorer.

Known issues and workarounds in Utility Services Release 7.1.2

N/A

Known issues and workarounds in Utility Services Release 7.1.1

N/A

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 fails.	Reboot the Utility Services Virtual machine after deploying with SDM Client and before attempting to establish trust with System Manager SDM.
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

Download ID	Filename	File size	Notes
AVP00000017	avaya-avp-7.1.2.0.0.09.iso	418 MB	Use this ISO file for new AVP 7.1.2 installations. This ISO also contains the upgrade-avaya-avp-7.1.2.0.0.09.zip upgrade bundle.
AVP00000018	upgrade-avaya-avp-7.1.2.0.0.09.zip	198 MB	Use this ZIP file for upgrade from AVP 7.0.x.

Note: Customers can install CMM 7.0.0.1 on a new AVP 7.1.2 Host. The same applies for upgrades of other Avaya Aura VMs on a shared AVP host with CMM 7.0.0.1, they also can upgrade to 7.1.2.

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

Installing the release

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

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

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

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

Then complete the initial configuration and administration by following:

- Administering Avaya Aura® Communication Manager Messaging guide.

Troubleshooting the installation

Hardware compatibility

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

Interoperability and requirements

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

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

What’s new in Communication Manager Messaging 7.0.0.0

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

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

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

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

Fixes in Communication Manager Messaging Release 7.0.x.x

Fixes in Communication Manager Messaging 7.0.0.0

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

Fixes in Communication Manager Messaging 7.0.0.1

The following table lists the fixes in this release.

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

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

ID	Visible symptoms	Release found in
	error if 3rd party adds any mailbox w/out an email address.	
MSG-22753	Banner page uses the term Federal, when the product is no longer Federal-only	
MSG-22767	Remove possibility for file-descriptor link in libmime_lib.so	
MSG-22815	abs_web_cache incorrectly assumes an average of 180 bytes/subscriber which causes unnecessary rebuilds of that cache.	
MSG-22850	Call is dropped when Call-Answer-Disclaimer and Call-Answer-Disable features are both enabled, a subscriber has the 'disclaimer' Call-Answer permission type, and they attempt to use Call-Answer-Disable.	
MSG-22851	When the green-feature: 'Call Answer Disclaimer' is enabled, the 'Permission Type' label: 'disclaimer' label is blank on the COS SMI form and the Custom COS section of the Subscriber SMI form.	
MSG-22898	Limits form: Label for 'Maximum List Entries' is wrong.	

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

Known issues and workarounds in Communication Manager Messaging Release 7.0.0.1

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

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

Avaya Aura® Appliance Virtualization Platform

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

Installation for Avaya Aura® Appliance Virtualization Platform Release 7.1.3.8

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

Download ID	Filename	File size	Notes
AVP00000074	avaya-avp-7.1.3.8.0.03.iso	511 MB	Use this ISO file for new AVP 7.1.3.8 installations. This ISO also contains the upgrade-avaya-avp-upgrade-avaya-avp-7.1.3.8.0.03.zip upgrade bundle
AVP00000075	upgrade-avaya-avp-7.1.3.8.0.03.zip	214 MB	Use this ZIP file for upgrade from AVP 7.0.x or 7.1.x.

Installation for Avaya Aura® Appliance Virtualization Platform Release 7.1.3.7

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

Download ID	Filename	File size	Notes
AVP00000071	avaya-avp-7.1.3.7.0.04.iso	511 MB	Use this ISO file for new AVP 7.1.3.7 installations. This ISO also contains the upgrade-avaya-avp-upgrade-avaya-avp-7.1.3.7.0.04.zip upgrade bundle
AVP00000072	upgrade-avaya-avp-7.1.3.7.0.04.zip	214 MB	Use this ZIP file for upgrade from AVP 7.0.x or 7.1.x.

Installation for Avaya Aura® Appliance Virtualization Platform Release 7.1.3.6

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

Download ID	Filename	File size	Notes
AVP00000061	avaya-avp-7.1.3.6.0.02.iso	511 MB	Use this ISO file for new AVP 7.1.3.6 installations. This ISO also contains the upgrade-avaya-avp-upgrade-avaya-avp-7.1.3.6.0.02.zip upgrade bundle
AVP00000062	upgrade-avaya-avp-7.1.3.6.0.02.zip	214 MB	Use this ZIP file for upgrade from AVP 7.0.x or 7.1.x.

Installation for Avaya Aura® Appliance Virtualization Platform Release 7.1.3.5

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

Download ID	Filename	File size	Notes
AVP00000054	avaya-avp-7.1.3.5.1.08.iso	511 MB	Use this ISO file for new AVP 7.1.3.5 installations. This ISO also contains the upgrade-avaya-avp-7.1.3.5.0.08.zip upgrade bundle
AVP00000055	upgrade-avaya-avp-7.1.3.5.1.08.zip	213 MB	Use this ZIP file for upgrade from AVP 7.0.x or 7.1.x.
~~AVP00000052~~	~~avaya-avp-7.1.3.5.0.08.iso~~	~~511 MB~~	~~Use this ISO file for new AVP 7.1.3.5 installations. This ISO also contains the upgrade-avaya-avp-7.1.3.5.0.08.zip upgrade bundle~~
~~AVP00000053~~	~~upgrade-avaya-avp-7.1.3.5.0.08.zip~~	~~213 MB~~	~~Use this ZIP file for upgrade from AVP 7.0.x or 7.1.x.~~

Installation for Avaya Aura® Appliance Virtualization Platform Release 7.1.3.4

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

Download ID	Filename	File size	Notes
AVP00000044	avaya-avp-7.1.3.4.0.04.iso	511 MB	Use this ISO file for new AVP 7.1.3.4 installations. This ISO also contains the upgrade-avaya-avp-7.1.3.4.0.04.zip upgrade bundle
AVP00000045	upgrade-avaya-avp-7.1.3.4.0.04.zip	213 MB	Use this ZIP file for upgrade from AVP 7.0.x or 7.1.x.

Installation for Avaya Aura® Appliance Virtualization Platform Release 7.1.3.3

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

Download ID	Filename	File size	Notes
AVP00000035	avaya-avp-7.1.3.3.0.02.iso	509 MB	Use this ISO file for new AVP 7.1.3.3 installations. This ISO also contains the upgrade-avaya-avp-7.1.3.3.0.02.zip upgrade bundle.
AVP00000036	upgrade-avaya-avp-7.1.3.3.0.02.zip	212 MB	Use this ZIP file for upgrade from AVP 7.0.x or 7.1.x.

Installation for Avaya Aura® Appliance Virtualization Platform Release 7.1.3.2

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

Download ID	Filename	File size	Notes
AVP00000030	avaya-avp-7.1.3.2.0.04.iso	509 MB	Use this ISO file for new AVP 7.1.3.2 installations. This ISO also contains the upgrade-avaya-avp-7.1.3.2.0.04.zip upgrade bundle.
AVP00000031	upgrade-avaya-avp-7.1.3.2.0.04.zip	212 MB	Use this ZIP file for upgrade from AVP 7.0.x or 7.1.x.

Installation for Avaya Aura® Appliance Virtualization Platform Release 7.1.3

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

Download ID	Filename	File size	Notes
AVP00000022	avaya-avp-7.1.3.0.0.04.iso	421 MB	Use this ISO file for new AVP 7.1.3 installations. This ISO also contains the upgrade-avaya-avp-7.1.3.0.0.04.zip upgrade bundle.
AVP00000023	upgrade-avaya-avp-7.1.3.0.0.04.zip	200 MB	Use this ZIP file for upgrade from AVP 7.0.x or 7.1.x.

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

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

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

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

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

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

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

Installing the release – AVP 7.1.3.x

This release can be used as a new install of AVP 7.1.3.x or as an upgrade to an existing AVP 7.0.x or 7.1.x installation. For an upgrade, it will not be necessary to reinstall the guest VMs.

Please note that VMware ESXi 6.0 hypervisor on AVP 7.1.3.x uses about 1 GB of more memory than ESXi 5.5 did on AVP 7.0 – 7.1.0.1. If you're using Avaya Aura® System Manager Solution Deployment Manager 7.1.3.x or SDM Client 7.1.3.x to perform the upgrade to AVP 7.1.3.x, SDM will check for available memory on the server before continuing with the upgrade. If there is insufficient memory available on the server, SDM will display a message to either upgrade the memory on the common server or upgrade to a later generation of the common server with more memory before upgrading to AVP 7.1.3.x. The memory check is not required for dedicated System Manager System on 12GB Common Server R1. The AVP 7.1.3.x upgrade will automatically reduce the System Manager's memory reservation for these systems as part of the upgrade process. Similarly, memory check is not required on the S8300D and S8300E servers.

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

Memory check when upgrading from AVP 7.0 – 7.1.0.1 to AVP 7.1.3.x:

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

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

- Look for an output similar to the following:

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

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

- Note the value displayed underneath the "availResv" column and ensure that this value is > 1126 MB.

- If this value is < 1126 MB, then before being able to upgrade to AVP 7.1.3.x, either the memory of the server must be upgraded, or the server must be upgraded to a later generation with more memory.

Memory check when upgrading from System Platform 6.x to AVP 7.1.3.x:

Using System Platform Web console:

- Logon to System Platform Web console as user admin.
- Navigate to Server Management → System Information → Memory
- Note the Available value displayed and ensure that this is > 3700 MB. If < 3700MB, then before being able to upgrade to AVP 7.1.3.x, either the memory of the server must be upgraded, or the server must be upgraded to a later generation with more memory.

Using Dom0 Command Line Interface:

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

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

- Note the free_memory value displayed and ensure that this is > 3700MB.
- If < 3700MB, then before being able to upgrade to AVP 7.1.3.x, either the memory of the server must be upgraded, or the server must be upgraded to a later generation.

If the memory check shows that extra memory is needed before upgrading to AVP 7.1.3.x, please refer to **PSN027060u Avaya Appliance Virtualization Platform Release 7.1.3 Memory Upgrade Instructions** for details on the memory kit and instructions on upgrading the server memory.

Note: The memory check is not required for dedicated System Manager systems on 12GB Common Server R1. The AVP 7.1.3.x upgrade will automatically reduce the System Manager's memory reservation for these systems as part of the upgrade process. Memory check is also not required on the S8300D and S8300E servers.

Refer to the **Migrating and Installing Avaya Appliance Virtualization Platform Release 7.1.3** document for instructions on new installs and upgrades of AVP. Be sure to upgrade SDM to Release 7.1.3.x first before using it to upgrade AVP.

Restoring software to previous version

Back up the application Virtual Machines using the applications' standard backup procedures before rolling back AVP. This is just a precaution in case anything goes wrong, and you have to reinstall and restore.

From AVP root prompt execute the following command to stop all Virtual Machines:

```
/opt/avaya/bin/stopallvms.py
```

Copy the previous patch (`avaya-avp-7.x.x.x.x.x.zip`) to the system's local disk (`/vmfs/volumes/server-local-disk`). If you're restoring back to AVP 7.1.2, unzip the `upgrade-avaya-avp-7.1.2.0.0.09.zip` file and copy the `avaya-avp-7.1.2.0.0.09.zip` file to the system's local disk.

For rolling back from AVP 7.1.3.x to AVP 7.x.x.x (example using AVP 7.1.0.0.0.9 release):

```
/opt/avaya/bin/rollback_bootbank.sh /vmfs/volumes/server-local-
disk/avaya-avp-7.1.0.0.0.9.zip
```

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

Be sure to substitute in the correct patch name and path. The full pathname to the rollback patch is required. You cannot use a relative path.

After rebooting you may need to enable SSH using SDM Client.

Issue the following commands after reboot:

```
/opt/avaya/bin/reduceReservation.sh

reboot
```

If SDM has trouble connecting with the AVP, you may need to generate a new AVP certificate by selecting the AVP host on SDM then selecting “More Actions” → “Generate/Accept Certificate”.

Installation for Avaya Aura® Appliance Virtualization Platform Release 7.1.2

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

Download ID	Filename	File size	Notes
AVP00000017	avaya-avp-7.1.2.0.0.09.iso	418 MB	Use this ISO file for new AVP 7.1.2 installations. This ISO also contains the upgrade-avaya-avp-7.1.2.0.0.09.zip upgrade bundle.
AVP00000018	upgrade-avaya-avp-7.1.2.0.0.09.zip	198 MB	Use this ZIP file for upgrade from AVP 7.0.x.

Note: Customers can install CMM 7.0.0.1 on a new AVP 7.1.2 Host. The same applies for upgrades of other Avaya Aura VMs on a shared AVP host with CMM 7.0.0.1, they also can upgrade to 7.1.2.

Installing the release

This release can be used as a new install of AVP 7.1.2 or as an upgrade to an existing AVP 7.0.x or 7.1.x installation. For an upgrade, it will not be necessary to reinstall the guest VMs.

Please note that VMware ESXi 6.0 hypervisor on AVP 7.1.2 uses about 1 GB of more memory than ESXi 5.5 did on AVP 7.0 – 7.1.0.1. If you’re using Avaya Aura® System Manager Solution Deployment Manager 7.1.2 or SDM Client 7.1.2 to perform the upgrade to AVP 7.1.2, SDM will check for available memory on the server before continuing with the upgrade. If there is insufficient memory available on the server, SDM will display a message to either upgrade the memory on the common server or upgrade to a later generation of the common server with more memory before upgrading to AVP 7.1.2. The memory check is not required for dedicated System Manager System on 12GB Common Server R1. The AVP 7.1.2 upgrade will automatically reduce the System Manager’s memory reservation for these systems as part of the upgrade process. Similarly, memory check is not required on the S8300D and S8300E servers.

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

Memory check when upgrading from AVP 7.x to AVP 7.1.2:

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

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

- Look for an output similar to the following:

  ```
  ~ # memstats -r group-stats -s name:availResv:consumed -l 1 -u mb
  GROUP STATS
  -----------
     Start Group ID   : 0
     No. of levels    : 1
  ```

Copyright 2017 – 2021 Avaya Inc. All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

```
   Unit             : MB
   Inclusion filter : (all)
   Exclusion filter : (none)
   Selected columns : gid:name:availResv:consumed

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

- Note the value displayed underneath the "availResv" column and ensure that this value is > 1126 MB.
- If this value is < 1126 MB, then before being able to upgrade to AVP 7.1.2, either the memory of the server must be upgraded, or the server must be upgraded to a later generation with more memory.

Memory check when upgrading from System Platform 6.x to AVP 7.1.2:

Using System Platform Web console:

- Logon to System Platform Web console as user admin.
- Navigate to Server Management → System Information → Memory
- Note the Available value displayed and ensure that this is > 3700 MB. If < 3700MB, then before being able to upgrade to AVP 7.1.2, either the memory of the server must be upgraded, or the server must be upgraded to a later generation with more memory.

Using Dom0 Command Line Interface:

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

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

- Note the free_memory value displayed and ensure that this is > 3700MB.
- If < 3700MB, then before being able to upgrade to AVP 7.1.2, either the memory of the server must be upgraded, or the server must be upgraded to a later generation.

If the memory check shows that extra memory is needed before upgrading to AVP 7.1.2, please refer to **PSN027060u Avaya Appliance Virtualization Platform Release 7.1.2 Memory Upgrade Instructions** for details on the memory kit and instructions on upgrading the server memory.

Note: The memory check is not required for dedicated System Manager systems on 12GB Common Server R1. The AVP 7.1.2 upgrade will automatically reduce the System Manager's memory reservation for these systems as part of the upgrade process. Memory check is also not required on the S8300D and S8300E servers.

Refer to the **Migrating and Installing Avaya Appliance Virtualization Platform Release 7.1.2** document for instructions on new installs and upgrades of AVP. Be sure to upgrade SDM Client to Release 7.1.2 first before using it to upgrade AVP.

Restoring software to previous version

Back up the application Virtual Machines using the applications' standard backup procedures before rolling back AVP. This is just a precaution in case anything goes wrong, and you have to reinstall and restore.

From AVP root prompt execute the following command to stop all Virtual Machines:

```
/opt/avaya/bin/stopallvms.py
```

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

For rolling back from AVP 7.1.2 to AVP 7.1.0.x (example using AVP 7.1.0.0.0.9 release):

```
/opt/avaya/bin/rollback_bootbank.sh /vmfs/volumes/server-local-disk/avaya-avp-7.1.0.0.0.9.zip

/opt/avaya/bin/avpshutdown.sh –r
```

Be sure to substitute in the correct patch name and path. The full pathname to the rollback patch is required. You cannot use a relative path.

After rebooting you may need to enable SSH using SDM Client.

Issue the following commands after reboot:

```
/opt/avaya/bin/reduceReservation.sh

/opt/avaya/bin/installvibs.sh

reboot
```

If SDM has trouble connecting with the AVP, you may need to generate a new AVP certificate by selecting the AVP host on SDM then selecting "More Actions" → "Generate/Accept Certificate".

For rolling back from AVP 7.1.2 to AVP 7.0.x.x (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

ramgb=$(($(esxcli --formatter=keyvalue hardware memory get | grep -e "Memory\.PhysicalMemory\.integer" | cut -d "=" -f 2) / (1024 * 1024 * 1024)))

if [ "$ramgb" -le 48 ]; then

  memMinFreePct=1

  if [ "$ramgb" -le 16 ]; then

    memMinFreePct=2

  fi

  esxcli system settings advanced set -o /Mem/MemMinFreePct -i $memMinFreePct

fi

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

Be sure to substitute in the correct patch name and path. The full pathname to the rollback patch is required. You cannot use a relative path.

After rebooting you may need to enable SSH using SDM Client.

Issue the following commands after reboot:

```
/opt/avaya/bin/reduceReservation.sh

/opt/avaya/bin/installvibs.sh

reboot
```

If SDM has trouble connecting with the AVP, you may need to generate a new AVP certificate by selecting the AVP host on SDM then selecting “More Actions” → “Generate/Accept Certificate”.

Installation for Avaya Aura® Appliance Virtualization Platform Release 7.1.0.1

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

Download ID	Filename	File size	Notes
AVP00000014	avaya-avp-7.1.0.1.0.2.zip	372 MB	Use this ZIP file for upgrade from AVP 7.0.x or 7.1.x

Installing the release

This release is an upgrade bundle to be applied onto an existing AVP 7.0.x or AVP 7.1.x installations. It will not be necessary to reinstall 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.

Restoring software to previous version

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

Issue the following commands (example using AVP 7.1.0.0.0.9 release):

```
/opt/avaya/bin/rollback_bootbank.sh /vmfs/volumes/server-local-disk/avaya-avp-7.1.0.0.0.9.zip

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

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

Installation for Avaya Aura® Appliance Virtualization Platform Release 7.1

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 Aura® Appliance Virtualization Platform Release 7.1.x.x

What’s new in Avaya Aura® Appliance Virtualization Platform Release 7.1.3.8

Enhancement	Description
None	

What’s new in Avaya Aura® Appliance Virtualization Platform Release 7.1.3.7

Enhancement	Description
None	

What’s new in Avaya Aura® Appliance Virtualization Platform Release 7.1.3.6

Enhancement	Description
None	

What’s new in Avaya Aura® Appliance Virtualization Platform Release 7.1.3.5

Enhancement	Description
None	

What’s new in Avaya Aura® Appliance Virtualization Platform Release 7.1.3.4

Enhancement	Description
None	

What’s new in Avaya Aura® Appliance Virtualization Platform Release 7.1.3.3

Enhancement	Description
AVP-740	AVP has updated DELL RAID controller management interface (PERC CLI).

What’s new in Avaya Aura® Appliance Virtualization Platform Release 7.1.3.2

Enhancement	Description
None	

What’s new in Avaya Aura® Appliance Virtualization Platform Release 7.1.3

Enhancement	Description
None	

What’s new in Avaya Aura® Appliance Virtualization Platform Release 7.1.2

Enhancement	Description
ESXi 6.0	The hypervisor on Avaya Appliance Virtualization Platform has been upgraded from VMware ESXi 5.5 to ESXi 6.0 Update 3. Note that ESXi 6.0 hypervisor uses about 1 GB more memory than ESXi 5.5 did. Please follow the instructions in the **Installation for Avaya Appliance Virtualization Platform Release 7.1.2** section above to check for sufficient available memory before upgrading to AVP 7.1.2.
AVP Licensing	Avaya Appliance Virtualization Platform will obtain license from a WebLM server either embedded with Avaya Aura® System Manager or standalone.
AVP Remote Deployment	This feature will allow Avaya Aura® System Manager Solution Deployment Manager (SDM) to remotely migrate from the following platform and releases to Appliance Virtualization Platform 7.1.2: • R6.x Embedded Survivable Remote on S8300D and S8300E servers • R5.2.1 Bare Metal Communication Manager on S8300D server • R6.x Simplex Survivable Remote Template on Common Server R1, R2 and R3. See Avaya Aura® System Manager section for details.
Commercial Security Hardening	Extended security hardening functions for commercial customers via documented procedures and automated scripts.
Root lock out after upgrading from AVP 7.0.x	After upgrading to AVP 7.1.2 the customer may choose to lock out the root account by running the following command from the AVP host command line while logged in as root: /opt/avaya/bin/root_lockout.sh NewAdminUser Where NewAdminUser is the user name you would like to use for your administrator account instead of root. You will then be prompted for a password and be asked to verify that you can now log in with the new credentials. Note that new installations of AVP 7.1.x will automatically lock out the root account.

What’s new in Avaya Aura® Appliance Virtualization Platform Release 7.1.0.1

Avaya Appliance Virtualization Platform will only be releasing security fixes with Avaya Aura® 7.1.1 release. No new features are included in this AVP 7.1.0.1 service pack.

What’s new in Avaya Aura® Appliance Virtualization Platform 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.

Enhancement	Description
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 Aura® Appliance Virtualization Platform Releases 7.1.x.x

Fixes in Avaya Aura® Appliance Virtualization Platform 7.1.3.8

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Found in Release
AVP-1291	AVP 7.1.3.x	root_lockout.sh script does not work run manually if run after upgrade from 7.0	7.1.3.7

Fixes in Avaya Aura® Appliance Virtualization Platform 7.1.3.7

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Found in Release
None			

Fixes in Avaya Aura® Appliance Virtualization Platform 7.1.3.6

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Found in Release

ID	Minimum Conditions	Visible symptoms	Found in Release
AVP-928	AVP 7.1.x	MEM_FAULT alarm not cleared after DIMM replacement	8.0.1.0
AVP-936	AVP 7.1.x	VMSA-2019-0020 - Hypervisor-Specific Mitigations for Denial-of-Service and Speculative-Execution Vulnerabilities (CVE-2018-12207, CVE-2019-11135)	8.1.1.0
AVP-948	AVP 7.1.x	VMSA-2019-0022 - ESXi DaaS updates address OpenSLP remote code execution vulnerability (CVE-2019-5544)	8.1.1.0
AVP-963	AVP 7.1.3.5	After deploying AVP 7.1.3.5.0.08 as a new install EASG sroot login was not recognized	7.1.3.5
AVP-1003	AVP 7.1.3.5	S8300E heartbeat broken with GW due to SDM 8.1.1 kickstart file generated for 7.1.3.5 installation	7.1.3.5

Fixes in Avaya Aura® Appliance Virtualization Platform 7.1.3.5

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Found in Release
AVP-769	AVP 7.1.x or AVP 7.x	AVP Shutdown/Reboot powers off VMs resulting in VM disk corruption	7.1.3.3
AVP-917	AVP 7.1.x or AVP 7.x	VMSA-2019-0014 - address use-after-free and denial of service vulnerabilities. (CVE-2019-5527, CVE-2019-5535)	7.1.3.4
AVP-908	AVP 7.1.x	VMSA-2019-0013 - Address command injection and information disclosure vulnerabilities. (CVE-2017-16544, CVE-2019-5531, CVE-2019-5532, CVE-2019-5534)	7.1.3.4
AVP-907	AVP 7.1.x in Hardened DoD mode	License issues on AVP running Hardened DoD mode caused the SSH banner to revert to the US DoD banner and was not recovered after the license issues were corrected.	7.1.3.3
AVP-898	AVP 7.1.3.x	AVP CPU occupancy would spike up to 100% for 10 minutes when SMGR jboss was restarted	7.1.3.3
AVP-935	Upgrade from AVP 7.1 to AVP 7.1.x	AVP upgrade from 7.1.0.0.0.9 to 7.1.3.3.0.02 failed on slow/S8300 hosts	7.1.3.3
AVP-897	Upgrade from AVP 7.1 to AVP 7.1.x	AVP upgrade from 7.1.0.0.0.9 to 7.1.3.3.0.02 failed on slow/S8300 hosts	7.1.3.3
AVP-876	AVP 7.1.x on ACP 120 servers	Single CPU ACP120 servers showed SYS_FAULT alarms indicating “System Board 1 Riser 2 Presence 0: Connected”	7.1.3.0

ID	Minimum Conditions	Visible symptoms	Found in Release
AVP-860	AVP 7.1.x	If an incorrect license was selected during installation process, there was no easy way to recover and install the correct license.	7.1.3.3
AVP-866	AVP 7.1.3.x	AVP showed several alarms of type SYS_FAULT indicating "CIM monitoring encountered error while fetching CIM_Sensor details"	7.1.3.3
AVP-750	AVP 7.1.x on S8300	S8300 hardware and firmware versions not recognized in gateway and CM	7.1.3.2

Fixes in Avaya Aura® Appliance Virtualization Platform 7.1.3.4

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Found in Release
AVP-843	AVP 7.1.x or AVP 7.x	VMSA-2019-0008 - Microarchitectural Data Sampling (MDS) Vulnerabilities for Hypervisors. Advisory: https://www.vmware.com/security/advisories/VMSA-2019-0008.html and Mitigation: https://kb.vmware.com/s/article/67577 .	7.1.3.2
AVP-839	AVP 7.1.2 or higher	Dell R630 showed disk status degraded	8.0.1.1
AVP-813	AVP 7.1.x or AVP 7.x	VMSA-2019-0005 - UHCI out-of-bounds read/write and TOCTOU vulnerabilities. Advisory: https://www.vmware.com/security/advisories/VMSA-2019-0005.html	7.1.3.2

Fixes in Avaya Aura® Appliance Virtualization Platform 7.1.3.3

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Found in Release
AVP-724 VMSA-2018-0027	AVP 7.1.x or AVP 7.x	See VMware security advisory VMSA-2018-0027 for more details: https://www.vmware.com/security/advisories/VMSA-2018-0027.html	7.1.3.2
AVP-720	AVP 7.0.1.0.5	Upgrade from AVP 7.0.1.0.5 to AVP 7.1.3.2.0.04 was failing	7.1.3.0
AVP-736	AVP 7.1.x	Alarms were not getting generated by AVP on encountering problems.	7.1.3.0
AVP-713	AVP 7.1.x on Dell hardware	AVP DISK_FAULT alarm would only clear by a graceful reboot	7.1.3.0
AVP-652	AVP 7.1.2.0	AVP would incorrectly report certified VMware software packages as uncertified	7.1.2.0

Fixes in Avaya Aura® Appliance Virtualization Platform 7.1.3.2

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Found in Release
AVP-643	AVP 7.1.2 and 7.1.3 on Avaya S8300E Server	The S8300E front panel shutdown button and the LEDs (Application, Active and Alarm LEDs) do not function.	7.1.2
AVP-653	Upgrade AVP to 7.1.3	Upgrade to AVP 7.1.3 fails with the message “Error Code-GENERIC_ERROR::AVP Patch Installation Failed”	7.1.3
AVP-666	Installing AVP 7.1.3 on an Equinox spec’d server	When installing AVP 7.1.3 on an Equinox-spec’d server, it does not accept upper-case ‘Y’ or ‘N’ at the following prompt: "Equinox deployment option is available to this system. Do you want to configure the system using this option? [Y]es/[N]o"	7.1.3
AVP-680	Upgrade to AVP 7.1.2 or 7.1.3	In rare situations, an Avaya S8300D server may request a license type of a Common Server.	7.1.2, 7.1.3
VMSA-2018-0012.1	Avaya Appliance Virtualization Platform 7.0.x.x or 7.1.x.x	See VMware Security Advisory VMSA-2018-0012 for details. http://www.vmware.com/security/advisories/VMSA-2018-0012.html	7.0.x.x, 7.1.x.x
VMSA-2018-0020	Avaya Appliance Virtualization Platform 7.0.x.x or 7.1.x.x	See VMware Security Advisory VMSA-2018-0020 for details. http://www.vmware.com/security/advisories/VMSA-2018-0020.html	7.0.x.x, 7.1.x.x
ESXi600-201807001	Avaya Appliance Virtualization Platform 7.1.2 or 7.1.3	See VMware patch release notes for VMware ESXi 6.0, Patch Release ESXi600-201807001 (53627)	7.1.2, 7.1.3

Fixes in Avaya Aura® Appliance Virtualization Platform 7.1.3

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Found in Release
VMSA-2018-0004	Avaya Appliance Virtualization Platform 7.0.x.x or 7.1.x.x	See VMware Security Advisory VMSA-2018-0004 for details. https://www.vmware.com/security/advisories/VMSA-2018-0004.html Note: This VMware hypervisor patch includes Intel microcode updates for Avaya Common Server R3 (Dell R630 & HP DL360 Gen9), Avaya Common Server R2 (Dell R620 & HP DL360p Gen8), and Avaya S8300E servers. Microcode updates for all other servers require BIOS updates from the server vendors.	7.0.x.x, 7.1.x.x
VMSA-2018-0002	Avaya Appliance Virtualization Platform 7.0.x.x or 7.1.x.x	See VMware Security Advisory VMSA-2018-0002 for details. https://www.vmware.com/security/advisories/	7.0.x.x, 7.1.x.x

ID	Minimum Conditions	Visible symptoms	Found in Release
ASA-2018-011		VMSA-2018-0002.html	
AVP-603	Enabling dual stack with IPv4 and IPv6 on Avaya Appliance Virtualization Platform 7.1.x.x	The NTP settings may not be preserved when enabling dual stack with IPv4 and IPv6.	7.1.x.x

Fixes in Avaya Aura® Appliance Virtualization Platform 7.1.2

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Found in Release
ESXi 6.0 Update 3	Avaya Appliance Virtualization Platform 7.0.x.x or 7.1.0.x	See VMware ESXi 6.0 Update 3 Release Notes for details. https://docs.vmware.com/en/VMware-vSphere/6.0/rn/vsphere-esxi-60u3-release-notes.html	7.0.x.x, 7.1.0.x

Fixes in Avaya Aura® Appliance Virtualization Platform 7.1.0.1

The following table lists the fixes in this release.

ID	Minimum Conditions	Visible symptoms	Found in Release
AVP-491	Avaya Appliance Virtualization Platform 7.0.x.x or 7.1.0.0	Avaya Aura® Appliance Virtualization Platform had certain vulnerabilities described in the following Avaya Security Advisory. To see the document, go to http://support.avaya.com and search for the ASA number. • ASA-2017-081 (VMware ESXi, Workstation and Fusion updates address critical and moderate security issues VMSA-2017-0006)	7.0.x.x, 7.1.0.0

Fixes in Avaya Aura® 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. Avaya Aura® adds support for HP DL360PG8 and Dell R630 in Avaya Virtual Deployment configurations.	Server hardware alarms, such as power supply or disk alarms may be delayed by up to 3 hrs.	7.0.1.0

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

Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform 7.1.3.8

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

ID	Minimum conditions	Visible symptoms	Workaround
None			

Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform 7.1.3.7

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

ID	Minimum conditions	Visible symptoms	Workaround
AVP-1222	AVP on Dell R630 systems	RAID Battery failure on Dell R630 generates BATTERY_FAULT instead of DISKBATTERY_FAULT	None
AVP-704	AVP on Dell R630 systems	On Dell R630 DISK_FAULT alarm only cleared by graceful reboot	None

Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform 7.1.3.6

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

ID	Minimum conditions	Visible symptoms	Workaround
None			

Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform 7.1.3.4

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

ID	Minimum conditions	Visible symptoms	Workaround
AVP-747	AVP 7.1.3.0 on HP hardware	AVP incorrectly gives RAID battery failure alarm	The alarm can be disabled on Utility Services 7.1.3.4 by Avaya representative.
AVP-733	AVP 7.1.3.0 on HP hardware	AVP gives a power fault alarm on single power supply Some HPG9 DL360 and Dell R630 systems shows degraded redundant power supply status: POWER_FAULT,Power Supply 3 Power Supplies,POWER_FAULT, MAJ	The alarm can be disabled on Utility Services 7.1.3.4 by Avaya representative.

Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform 7.1.3.3

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
AVP-733	AVP 7.1.3.0 on HP hardware	AVP gives a power fault alarm on single power supply Some HPG9 DL360 and Dell R630 systems shows degraded redundant power supply status: POWER_FAULT,Power Supply 3 Power Supplies,POWER_FAULT, MAJ	None.
AVP-747	AVP 7.1.3.0 on HP hardware	AVP incorrectly gives RAID battery failure alarm	None.
AVP-750	AVP 7.1.0 and higher versions on a S8300 card on a G450.	S8300 not recognized in gateway and CM	None.
AVP-707	AVP 7.1.2.0 on S8300D card.	AVP incorrectly reports overheating alarms for S8300D card	None.
AVP-656	AVP 7.1.0.0	AVP syslog.log and US remote.log filling with 'handler could not derive port number messages'	None.

Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform 7.1.3.2

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.

ID	Minimum conditions	Visible symptoms	Workaround
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 subnet	Cannot change the IP address of the AVP if there is a duplicate IP address on the subnet.	Follow the directions in the VMware Knowledge Base https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1020647
AVP-429	Attended installation of AVP 7.1.x	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.x with an IPv6 address or administer IPv6 address using System Manager SDM or AVP CLI command "/opt/avaya/bin/set_dualstack enable"
AVP-466	Enabling OOBM via CLI command on AVP 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"	This error message can be ignored if the next line shows "Out of Band Management is now enabled on the host".
AVP-706	AVP 7.1.3 and HP DL360 G8 or G9 servers	An HP DL360 G8 or G9 server with a single power supply may incorrectly show degraded redundant power supply status: POWER_FAULT,Power Supply 3 Power Supplies,POWER_FAULT, MAJ	
ESXi 6.0 Update 3	Active Directory is enabled on AVP	Active Directory settings are not retained post-upgrade. The Active Directory settings configured in the ESXi host before upgrade are not retained when the host is upgraded to ESXi 6.0. See VMware ESXi 6.0 release notes for details: https://docs.vmware.com/en/VMware-vSphere/6.0/rn/vsphere-esxi-60u3-release-notes.html	1. Logon to the AVP host using the VMware Embedded Host Client via a web browser. Use the local management IP address of the AVP host in the following URL: https://<AVP host IP address>/ui If necessary, enable access to the VMware vSphere Host Client … • Logon to AVP host using an SSH client. • Note: Ensure SSH enabled,

ID	Minimum conditions	Visible symptoms	Workaround
			see Enable SSH Access for AVP Host section. • Enter the local management IP address of the AVP host. • Logon using admin or other Administrator user. Execute the following command on the AVP CLI: `/opt/avaya/bin/set_ehc enable` Logon using user admin or another Administrator user. 2. Where previously defined, confirm that the Active Directory domain is configured for the host and if not, configure this: In the left-hand Navigator window, select Manage under Host. In the central Manage window, select the Security & Users tab. Select Authentication Click on the Join domain link and ensure the following configuration data is defined (where applicable): • Domain Name: <Active Directory Domain Name> • Use authentication proxy: <tick box> • User name: <user name> • Password: <password> Click on the Join domain button.

ID	Minimum conditions	Visible symptoms	Workaround
General issues and workarounds			If watching an Avaya Appliance Virtualization Platform (AVP) installation via a monitor Note the following: A message about the scratch partition will appear briefly in red after which the screen will go black for 10 minutes while the installation continues. This is expected, and no action should be taken. After the black screen the system will reboot, and the installation will continue. When the CD is ejected, remove the CD and the USB stick and the installation will continue. If the installation continues to show a black screen after 30 minutes, the AVP network setup may not be correct and will need to be re-installed. Verify that the correct values were used to generate the kickstart file, check the USB stick and re-attempt the installation.
General issues and workarounds			The Avaya Appliance Virtualization Platform (AVP) End User License Agreement (EULA) must be accepted by logging into the AVP via an SSH client. If virtual machine deployments are attempted prior to accepting the EULA, the deployments will fail. The VMs will not power on failing the deployment flow.
General issues and workarounds			After the EULA is accepted, SSH to AVP will be disabled after 24 hours and activation after that is via the onboard Utility Services VM 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.

Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform 7.1.3

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 subnet	Cannot change the IP address of the AVP if there is a duplicate IP address on the subnet.	Follow the directions in the VMware Knowledge Base https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1020647
AVP-429	Attended installation of AVP 7.1.x	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.x with an IPv6 address or administer IPv6 address using System Manager SDM or AVP CLI command “/opt/avaya/bin/set_dualstack enable”
AVP-466	Enabling OOBM via CLI command on AVP 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	This error message can be ignored if the next line shows “Out of Band Management is now enabled on the host”.

ID	Minimum conditions	Visible symptoms	Workaround
		parameter. See the VMkernel log for detailed error information"	
AVP-643	AVP 7.1.2 and 7.1.3 on Avaya S8300E Server	The S8300E front panel shutdown button and the LEDs (Application, Active and Alarm LEDs) do not function.	For the shutdown button, please shutdown the server using Solution Deployment Manager, AVP ESXi command line, or VMware Embedded Host Client. For LED workaround, please check the status from Communication Manager.
AVP-653	Upgrade AVP to 7.1.3	Upgrade to AVP 7.1.3 fails with the message "Error Code-GENERIC_ERROR::AVP Patch Installation Failed"	Restart the ESXi management agent from the Direct Console User Interface (DCUI) or restart the hostd service using AVP CLI command "/etc/init.d/hostd restart" and then retry the AVP update. See VMware KB article for more info: https://kb.vmware.com/s/article/1003490
ESXi 6.0 Update 3	Active Directory is enabled on AVP	Active Directory settings are not retained post-upgrade. The Active Directory settings configured in the ESXi host before upgrade are not retained when the host is upgraded to ESXi 6.0. See VMware ESXi 6.0 release notes for details: https://docs.vmware.com/en/VMware-vSphere/6.0/rn/vsphere-esxi-60u3-release-notes.html	1. Logon to the AVP host using the VMware Embedded Host Client via a web browser. Use the local management IP address of the AVP host in the following URL: https://<AVP host IP address>/ui If necessary, enable access to the VMware vSphere Host Client … • Logon to AVP host using an SSH client. • Note: Ensure SSH enabled, see Enable SSH Access for AVP Host section. • Enter the local management IP address of the AVP host. • Logon using admin or another Administrator user. Execute the following command on the AVP CLI: `/opt/avaya/bin/set_ehc enable` Logon using user admin or another Administrator user. 2. Where previously defined, confirm that the Active Directory domain is configured for the host and if not, configure this: In the left-hand Navigator window, select Manage under Host.

ID	Minimum conditions	Visible symptoms	Workaround
			In the central Manage window, select the Security & Users tab. Select Authentication Click on the Join domain link and ensure the following configuration data is defined (where applicable): • Domain Name: <Active Directory Domain Name> • Use authentication proxy: <tick box> • User name: <user name> • Password: <password> Click on the Join domain button.
General issues and workarounds			If watching an Avaya Appliance Virtualization Platform (AVP) installation via a monitor Note the following: A message about the scratch partition will appear briefly in red after which the screen will go black for 10 minutes while the installation continues. This is expected, and no action should be taken. After the black screen the system will reboot, and the installation will continue. When the CD is ejected, remove the CD and the USB stick and the installation will continue. If the installation continues to show a black screen after 30 minutes, the AVP network setup may not be correct and will need to be re-installed. Verify that the correct values were used to generate the kickstart file, check the USB stick and re-attempt the installation.
General issues and workarounds			The Avaya Appliance Virtualization Platform (AVP) End User License Agreement (EULA) must be accepted by logging into the AVP via an SSH client. If virtual machine deployments are attempted prior to accepting the EULA, the deployments will fail. The VMs will not power on failing the deployment flow.
General issues and workarounds			After the EULA is accepted, SSH to AVP will be disabled after 24 hours and activation after that is via the onboard Utility Services VM or via SDM.

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

Known issues and workarounds in Avaya Aura® Appliance Virtualization Platform 7.1.2

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	Cannot change the IP address of the AVP if there is a duplicate IP	Follow the directions in the VMware Knowledge Base

ID	Minimum conditions	Visible symptoms	Workaround
	address in the subnet	address on the subnet.	https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1020647
AVP-429	Attended installation of AVP 7.1.x	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.x with an IPv6 address or administer IPv6 address using System Manager SDM or AVP CLI command "/opt/avaya/bin/set_dualstack enable"
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"	This error message can be ignored if the next line shows "Out of Band Management is now enabled on the host".
AVP-643	AVP 7.1.2 and 7.1.3 on Avaya S8300E Server	The S8300E front panel shutdown button and the LEDs (Application, Active and Alarm LEDs) do not function.	For the shutdown button, please shutdown the server using Solution Deployment Manager, AVP ESXi command line, or VMware Embedded Host Client. For LED workaround, please check the status from Communication Manager.
ESXi 6.0 Update 3	Active Directory is enabled on AVP	Active Directory settings are not retained post-upgrade. The Active Directory settings configured in the ESXi host before upgrade are not retained when the host is upgraded to ESXi 6.0. See VMware ESXi 6.0 release notes for details: https://docs.vmware.com/en/VMware-vSphere/6.0/rn/vsphere-esxi-60u3-release-notes.html	1. Logon to the AVP host using the VMware Embedded Host Client via a web browser. Use the local management IP address of the AVP host in the following URL: https://<AVP host IP address>/ui If necessary, enable access to the VMware vSphere Host Client … • Logon to AVP host using an SSH client. • Note: Ensure SSH enabled, see Enable SSH Access for AVP Host section. • Enter the local management IP address of the AVP host. • Logon using admin or

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

ID	Minimum conditions	Visible symptoms	Workaround
issues and workarounds			Platform (AVP) End User License Agreement (EULA) must be accepted by logging into the AVP via an SSH client. If virtual machine deployments are attempted prior to accepting the EULA, the deployments will fail. The VMs will not power on failing the deployment flow.
General issues and workarounds			After the EULA is accepted, SSH to AVP will be disabled after 24 hours and activation after that is via the onboard Utility Services VM 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.

Known issues and workarounds in Avaya Aura® 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	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.

ID	Minimum conditions	Visible symptoms	Workaround
		deployment time. See deployment documentation for further details.	
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 subnet	Cannot change the IP address of the AVP if there is a duplicate IP address on the subnet.	Follow the directions in the VMware Knowledge Base https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1020647
AVP-429	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

ID	Minimum conditions	Visible symptoms	Workaround
			generate the kickstart file, check the USB stick and re-attempt the installation.
General issues and workarounds			The Avaya Appliance Virtualization Platform (AVP) End User License Agreement (EULA) must be accepted by logging into the AVP via an SSH client. If virtual machine deployments are attempted prior to accepting the EULA, the deployments will fail. The VMs will not power on failing the deployment flow.
General issues and workarounds			After the EULA is accepted, SSH to AVP will be disabled after 24 hours and activation after that is via the onboard Utility Services VM 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!

- **G430 Gateways running a release prior to Release 7.1.2 Build 39.5.0** MUST first install Release 7.1.0.4 (Build 38.21.02 or Build 38.21.32) or newer 38.xx.yy release before installing Release 7.1.3.x.

- **G450 Gateways running a release prior to Release 7.1.2 Build 39.5.0** MUST first install Release 7.1.0.5 (Build 38.21.03 or Build 38.21.33) or newer 38.xx.yy release before installing Release 7.1.3.x.

If you attempt to download Release 7.1.3.x prior to having installed Release 7.1.0.4 or Release 7.1.0.5 and execute the "`show download software status 10`" command, the system will display the following error message:

```
Incompatible software image for this type of device.
```

After installing Release 7.1.0.4 or Release 7.1.0.5, you must enable or disable Avaya Logins before downloading Release 7.1.3.x via CLI or SNMP. You can enable or disable Avaya Logins by using one of the following CLI commands:

- `login authentication services` – To enable Avaya Logins.
- `no login authentication services` – To disable Avaya Logins.

If you neglect to enable or disable Avaya Logins by using one of the above commands, you will be prompted to do so when any of the following CLI commands are used to perform a firmware download:

- `copy ftp SW_imageA`
- `copy ftp SW_imageB`
- `copy scp SW_imageA`
- `copy scp SW_imageB`
- `copy tftp SW_imageA`
- `copy tftp SW_imageB`
- `copy usb SW_imageA`
- `copy usb SW_imageB`

Notes:

- The G430 will only download the G430 firmware specific to its vintage. Firmware for G430 Vintage 3 must only use firmware having "g430v3_" indicated in the firmware image's filename. All other G430 vintages must only use firmware having "g430_" indicated in the firmware image's filename.

The 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 the latest fixes. New gateway features and functionality will not be supported in configurations running newer series of gateway firmware with older Communication Manager Releases. To help ensure the highest quality solutions for our customers, Avaya recommends use of like gateway firmware series and Communication Manager releases. This means the latest version within the GW Firmware Series are recommended with the following Communication Manager software releases:

Gateway Firmware Series	Communication Manager Release
33.xx.xx	6.3
34.xx.xx	6.3.2
35.xx.xx	6.3.5
36.xx.xx	6.3.6
37.xx.xx	7.0.0
38.xx.xx	7.1.2
39.xx.xx	7.1.3

Newer gateway firmware versions running with older Communication Manager software releases are still supported. For example, running gateway firmware version series 36.xx.xx with Communication Manager 6.3 is still supported. However, prolonged running in this type of mixed configuration is not recommended. Avaya recommends running in a mixed configuration only if necessary to support gateway upgrades prior to upgrading Communication Manager software. Newer Communication Manager software releases running with older gateway firmware versions are not supported.

Gateway firmware support follows the Communication Manager software end of manufacturer support model. This means that as soon as a Communication Manager release goes end of manufacturer support, new gateway firmware will no longer be supported with that 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.

File Download Instructions

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

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

.

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

Backing up the software

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

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

Installing the release

IMPORTANT!

- **G430 Gateways running a release prior to Release 7.1.2 Build 39.5.0** MUST first install Release 7.1.0.4 (Build 38.21.02 or Build 38.21.32) or newer 38.xx.yy release before installing Release 7.1.3.x.

- **G450 Gateways running a release prior to Release 7.1.2 Build 39.5.0** MUST first install Release 7.1.0.5 (Build 38.21.03 or Build 38.21.33) or newer 38.xx.yy release before installing Release 7.1.3.x.

If you attempt to download Release 7.1.3.x prior to having installed Release 7.1.0.4 or Release 7.1.0.5 and execute the “`show download software status 10`” command, the system will display the following error message:

```
Incompatible software image for this type of device.
```

After installing Release 7.1.0.4 or Release 7.1.0.5, you must enable or disable Avaya Logins before downloading Release 7.1.3.x via CLI or SNMP. You can enable or disable Avaya Logins by using one of the following CLI commands:

- `login authentication services` – To enable Avaya Logins.
- `no login authentication services` – To disable Avaya Logins.

If you neglect to enable or disable Avaya Logins by using one of the above commands, you will be prompted to do so when any of the following CLI commands are used to perform a firmware download:

- `copy ftp SW_imageA`
- `copy ftp SW_imageB`
- `copy scp SW_imageA`
- `copy scp SW_imageB`
- `copy tftp SW_imageA`
- `copy tftp SW_imageB`
- `copy usb SW_imageA`
- `copy usb SW_imageB`

Notes:

- The gateway defaults to using TLS 1.2, PTLS, and unencrypted H.248 communication with CM. Refer to the "set link-encryption" command to adjust these settings.
- The "show system" CLI command can be used display the gateway's model and mainboard hardware vintage.
- The G430 will only download the G430 firmware specific to its hardware vintage. Firmware for G430 Vintage 3 must only use firmware having "g430v3_" indicated in the firmware image's filename. All other G430 vintages must only use firmware having "g430_" indicated in the firmware image's filename.
- The G450 will only download the G450 firmware specific to its hardware vintage. Firmware for G450 Vintage 4 must only use firmware having "g450v4_" indicated in the firmware image's

filename. All other G450 vintages must only use firmware having "g450_" indicated in the firmware image's filename.

- Solution Deployment Manager (SDM) does not currently support download to the G430v3 and G450v4 hardware. This will be provided in future releases of SDM.

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.

Meltdown and Spectre Vulnerabilities

The G430/G450 Branch Gateway is not vulnerable to the Spectre/Meltdown hardware issue.

The processor used by the G430/G450 is not included in the list of processors identified to be impacted by the Spectre and Meltdown vulnerabilities. However, an S8300D installed within the gateway that is upgraded to Release 7.1.3 may be impacted as indicated below.

For more information about Spectre and Meltdown fixes included in Avaya Aura® Release 7.1.3, see PSN020346u on the Avaya Support site at: https://downloads.avaya.com/css/P8/documents/101048606.

Important note regarding S8300D upgrading to 7.1.3

The introduction of Spectre and Meltdown fixes with 7.1.3 has an impact on S8300D scalability performance. A Survivable Remote configuration (CM LSP and BSM) with the Spectre and Meltdown fixes enabled can only now support 200 users with up to 500 BHCC traffic.

Since these fixes are enabled by default, consider whether configuration changes are to plan a 7.1.3 upgrade.

The following options should be considered if higher capacity is required from the S8300D:

- Disabling the Spectre and Meltdown fixes on the S8300Ds – this will allow the S8300D to deliver the same level of capacity as with 7.1.2 and before.

  or

- if disabling the fixes on the S8300D is not a viable option for you/your customer, plan to upgrade the embedded server to the latest S8300E model.

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 7.1.3.7 (Builds 39.49.00 and 39.49.30)

No new features added for this release.

What's new in G430 and G450 Media Gateways 7.1.3.6 (Builds 39.40.00 and 39.40.30)

No new features added for this release.

What's new in G430 and G450 Media Gateways Release 7.1.3.5 (Builds 39.34.00 and 39.34.30)

No new features added for this release**.**

What's new in G430 and G450 Media Gateways Release 7.1.3.4 (Builds 39.27.00 and 39.27.30)

Enhancement	Description
Security / Syslog	Syslog over TLS has been added to 7.1.3.4 version of the gateway. Included with this feature is the addition and/or enhancement of following certificate-options commands: certificate-options syslog set validate-alternate-name set validate-common-name set validate-expiration show certificate-options show certificate-options syslog The following certificate management commands have been updated to include the syslog application: copy scp root-ca syslog <filename> <ip> copy usb root-ca syslog <source-usb-device> <source-filename> erase root-ca syslog <index> show root-ca syslog [index] copy scp gw-identity syslog <filename> <ip> copy usb gw-identity syslog <source-usb-device> <source-filename> erase gw-identity syslog show gw-identity syslog The following commands have been updated to add tls as a protocol choice for syslog: set link-encryption syslog <all | tls | tls1.2 | tls1.1 | tls1.0> <yes | no> set logging server <ip-addr> tls [port] show logging server condition

What's new in G430 and G450 Media Gateways Release 7.1.3.2 (Builds 39.16.00 and 39.16.30)

Enhancement	Description
G430v3	New G430 firmware has been introduced to support to latest vintage of G430 gateway (G430v3). The G430 will only download the G430 firmware specific to its vintage. Firmware for G430 Vintage 3 must only use firmware having "g430v3_" indicated in the firmware

Enhancement	Description
	image's filename. All other G430 vintages must only use firmware having "g430_" indicated in the firmware image's filename. Make sure to download the appropriate 7.1.3.2 firmware image for your G430! • G430 Vintage 1 and 2: G430_sw_39_16.0.bin • G430 Vintage 1 and 2: G430_sw_39_16.30.bin (Russia) • G430 Vintage 3: G430v3_sw_39_16.0.bin • G430 Vintage 3: G430v3_sw_39_16.30.bin (Russia)

What's new in G430 and G450 Media Gateways Release 7.1.3 (Builds 39.12.00 and 39.12.30)

No new features were added to the G430 or G450 in Release 7.1.3.

What's new in G430 and G450 Media Gateways Release 7.1.2 (Builds 39.05.00 and 39.05.30)

The following table lists enhancements in this release.

Enhancement	Description
Security	G430 and G450 Media Gateways now support 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 Logins 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. Upgrades to Release 7.1.2 and later cannot be completed without first installing Release 7.1.0.5, Release 7.1.0.4, Release 7.1.0.3 or Release 7.1.0.2.

What's new in G450 Media Gateways Release 7.1.0.5 (Builds 38.21.03 and 38.21.33)

The following table lists enhancements in this release.

Enhancement	Description
G450 Installation	With Release 7.1.0.5, the G450 gateway is now more tolerant of the time it takes to load larger firmware images into memory at boot time. In addition, the size of the firmware download image also has been reduced. If your G450 gateway is already running Release 7.1.0.2, 7.1.0.3, or 7.1.0.4, there is no need to immediately upgrade to Release 7.1.0.5. However, upgrading to Release 7.1.0.5 may be necessary to allow installation of future G450 releases that have larger firmware images.

What's new in G430 and G450 Media Gateways Release 7.1.0.4 (Builds 38.21.02 and 38.21.32)

The following table lists enhancements in this release.

Enhancement	Description
G430 and G450 Installation	Release 7.1.0.4 fixes an issue where continuous reboots have been experienced in a small number of gateways upgrading from builds prior to Build 37.38 to Builds 37.38 through 38.21.01. Those who are experiencing continuous reboots should first use the ASB recessed button on the front panel to boot from the alternate boot bank before loading this release. 7.1.0.4.

What's new in G430 and G450 Media Gateways Release 7.1.0.3 (Builds 38.21.01 and 38.21.31)

The following table lists enhancements in this release.

Enhancement	Description
Security	Release 7.1.0.3 is identical in functionality to Release 7.1.0.2 except that gateways running firmware earlier than Release 7.0 are no longer required to first install Release 7.x (Builds 37.x.y). There is no need to upgrade to Release 7.1.0.3 if your gateway is already running Release 7.1.0.2. Release 7.1.0.3 assures that a local gateway administrator has confirmed whether Avaya Login access is to be enabled or disabled prior to allowing any firmware to be downloaded.

What's new in G430 and G450 Media Gateways Release 7.1.0.2 (Builds 38.21.00 and 38.21.30)

The following table lists enhancements in this release.

Enhancement	Description
Security	Release 7.1.0.2 assures that a local gateway administrator has confirmed whether Avaya Login access is to be enabled or disabled prior to allowing any firmware to be downloaded.

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.

Enhancement	Description
	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> – 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

Enhancement	Description
	ciphers, key exchange algorithms, and MAC options for the SSH server and SSH client: **show ssh-server-configuration** – 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. **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.

Enhancement	**Description**
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 7.1.3.7 (Builds 39.49.00 and 39.49.30)

ID	Minimum Conditions	Visible symptoms	Found in Release
CMG4XX-1639	G430, G450 OSPF	Several internal timer calculations were fixed to prevent the possibility of premature rollover. For example, the internal OSPF timer was fixed so that it should now only rollover once every 136 years. Originally the OSPF timer was incorrectly rolling over every 248 days.	7.1.3
CMG4XX-1652	G430, G450 No Tone Detectors	Fixed a memory leak that caused the gateway to reboot as a result of the log being flooded with an excessive number of 'No tone detector' log entries.	7.0.1.1
CMG4XX-1667	G430, G450 Busy-out DSP	Busy-out of a DSP that is not present will no longer cause an alarm.	8.1
CMG4XX-1668	G430, G450 Busy-out DSP	Fixed a condition that only occurred when a DSP is busied out whereby the gateway would sometimes use the local RTP port range instead of the RTP range configured for the IP Network-Region.	7.1.3.3
CMG4XX-1734	G430, G450 Nessus Scan	Fixed an issue where multiple Nessus security scans using SSH would sometimes cause the gateway to reboot.	8.1

Fixes in G430 and G450 Media Gateways Release 7.1.3.6 (Builds 39.40.00 and 39.40.30)

ID	Minimum Conditions	Visible symptoms	Found in Release
CMG4XX-1577	G430, G450	The "show logging file content" CLI command displayed an incorrect IP address in the logs for unsuccessful login attempts made by a user logging in remotely.	8.1.2
CMG4XX-1586	G430, G450	In rare cases, upload operations using the "copy file scp" commands would cause the gateway to reboot.	8.1
CMG4XX-1595	G430, G450	The number of log entries and traps generated by TLS certificate and connection related errors has been reduced to once every 30 minutes.	8.1.2

Fixes in G430 and G450 Media Gateways Release 7.1.3.5 (Builds 39.34.00 and 39.34.30)

ID	Minimum Conditions	Visible symptoms	Found in Release
CMG4XX-1540	G430, G450 Spanning Tree	While powering up the Gateway, spanning-tree packets were being sent even though spanning tree was disabled.	7.1.3.4
CMG4XX-1549	G450, G430 SSH	In some cases, SSH connections were being refused after many SSH connections have occurred over an	7.1.3.4

ID	Minimum Conditions	Visible symptoms	Found in Release
		extended period of time. Access via console and/or telnet were unaffected.	
CMG4XX-36, CMG4XX-1564	G450, G430 DHCP Server	In some cases when the gateway is used as a DHCP Server, IP bindings that are no longer in use were not cleared and the gateway might reboot if the CLI command "clear ip dhcp-server bindings" is used.	6.3.2, 7.1.3.2
CMG4XX-1530	G430v3 Traceroute	The traceroute command in the G430v3 was not working correctly and indicated "request timeout" in the last route entry.	7.1.3.4

Fixes in G430 and G450 Media Gateways Release 7.1.3.4 Hotfix (Builds 39.28.00 and 39.28.30)

ID	Minimum Conditions	Visible symptoms	Found in Release
CMG4XX-1541	G430, G450	This version contains fixes for the Wind River TCP/IP stack security vulnerabilities discovered in July 2019 and known as Urgent/11.	7.1.3.3

Fixes in G430 and G450 Media Gateways Release 7.1.3.4 (Builds 39.27.00 and 39.27.30)

ID	Minimum Conditions	Visible symptoms	Found in Release
CMG4XX-1490	G430v3, MP120	There was a rare possibility on G430v3 gateways that an MP-120 DSP core would not be put into service following a media-gateway reset, and would instead be marked as impaired or faulted even though there was nothing wrong with the DSP core. If this occurs, the workaround is to reset the voip engine (MG CLI command "" reset voip"") or reset the media-gateway as a whole (MG CLI command ""reset"") , and monitor the results to make sure all cores are in service (show voip)."	7.1.3
CMG4XX-1414	Read-only users	Read-only users were unable to execute the "show ip telnet", "show ip ssh" and "show ip http" commands.	6.3.10
CMG4XX-1422	G430v3, SLA Monitor	The ADS SLA Monitor Server incorrectly showed packet loss when connected to a G430v3 gateway.	7.1.3.3
CMG4XX-1431	dadmin user account	The gateway would not allow a user account named "dadmin" to be created. Note that "dadmin" used to be a special service provider account that was removed with the addition of EASG.	7.1.3.2
CMG4XX-1481	G430v3 SNMP	G430v3 gateways were not sending SNMP traps to IPv6 addresses.	7.1.3.3
CMG4XX-1497, CMG4XX-1503	Firmware Download	The gateway is now more tolerant of the time it takes to download larger firmware image sizes. In addition, the size of the firmware download image also has	7.1.3.3

ID	Minimum Conditions	Visible symptoms	Found in Release
		been reduced.	
CMG4XX-1509	Primary Search Timer	The primary search timer was incorrectly getting set to a value of 1 minute when set to value greater than 30 minutes.	7.0.1.2

Fixes in G430 and G450 Media Gateways Release 7.1.3.3 (Builds 39.20.00 and 39.20.30)

ID	Minimum Conditions	Visible symptoms	Found in Release
CMG4XX-1216	G430, G450 Service Observing	A sixth party may now be added to a Service Observed call.	7.1.3
CMG4XX-1262	G450 Fan Faults	Fan Faults were not being displayed by the “show faults” CLI command.	6.1.13
CMG4XX-1300	G430, G450 MP120, MP160	In rare cases, MP160 and MP120 DSPs having hardware failures still appear to be in service.	7.1.2
CMG4XX-1279	G430, G450 SNMP	A 64-bit SNMP request to OID 1.3.6.1.2.1.31.1.1.1.6 was returning a 32-bit response (with lowest 32 bits as zero) instead of a 64-bit response.	7.0.1.3
CMG4XX-1296	G430, G450 V.32 Modem	v.32 modem rekey success rate has been improved by making it more tolerant of DC signal bias.	7.1.3.2
CMG4XX-1231	G430, G450 FTP	In rare cases, FTP transfer failures caused by network impairments could cause a gateway to reset.	6.3.14
CMG4XX-1274	G430, G450 SSH, SCP	ECSDA algorithm support for SSH and SCP has been added. The “crypto key generate” and “show crypto key” CLI commands have been updated to include ECDSA as an option. The default key size used is 256-bit, although 256-bit, 384-bit, and 521-bit key sizes are supported.	7.1.3.3
CMG4XX-1285	G430, G450 TLS Identity Certificates	TLS Identity certificate files encoded with RC2 might cause the gateway to reset when attempting to install from a USB stick in FIPS mode.	7.1.2
CMG4XX-1335	G430v3 Restore	Performing a restore of a backup on a G430v3 did not restore the TLS certificates.	7.1.3.2
CMG4XX-1343	G430, G450 M3K, DS1, V.150 Viper IP Phone	When an M3K system is connected to a gateway by way of DS1 trunk and an IP-Viper to IP-Viper call is placed over that DS1 trunk, it might fail to go secure when initiated from the G450 side.	7.1
CMG4XX-1353	G430, G450 V.150 Viper IP Phone	Reduced the time it takes for IP Viper to go secure during v.32 modem session establishment	7.1.3.3
CMG4XX-1241	G430, G450 PMI	Configured PMI is now the default interface used when sending network connectivity ping requests.	7.1.3

Fixes in G430 and G450 Media Gateways Release 7.1.3.2 (Builds 39.16.00 and 39.16.30)

ID	Minimum Conditions	Visible symptoms	Found in Release
CMG4XX-1104	G430/G450 SNMP	The cmgVoipTotalChannelsEnforcedbyCM SNMP Object ID (OID) is now a supported in the G430 and G450 MIB. Previously, any combination of SNMP commands attempting to get a response from the cmgVoipTotalChannelsEnforcedbyCM object ID (.1.3.6.1.4.1.6889.2.9.1.4.10) would fail.	7.0.1
CMG4XX-1131, CMG4XX-1153	G430/G450 V.150 Viper IP Phones	Fixed an issue with Viper IP secure phones responding to V.32 modem answer tone too quickly. This resulted in the far-end not always being able to initiate a secure session. The gateway now detects when this behavior occurs and correspondingly institutes a V.32 recommended delay in the AA response when needed.	6.3.17
CMG4XX-1148, CMG4XX-1167	G430/G450 Clock Sync Over IP (CSOIP)	Clock sync failures could occur if CM requests a codec that performs silent suppression when establishing Clock Sync over IP (CSoIP) communication between master and slave gateways. The gateway will now override codec requests that should not be used for CSoIP and will now select an appropriate codec to be used instead.	6.3.17
CMG4XX-1164	G430/G450 V.150 Viper IP Phones	Fixed an issue where IP Viper to IP Viper V.150 calls might not go secure when using a specific service provider's media-path having longer than 100ms round-trip delay.	6.3.18
CMG4XX-1180	G430/G450 Security Scans	Fixed an issue where Nessus Security Scan were causing the gateway to reset as a result of TCP sockets being exhausted.	7.1.3
CMG4XX-1206	G430/G450 Announcements, SCP	Fixed an issue where uploads or downloads of announcements using scp would fail if a ssh login banner is present.	6.3.16

Fixes in G430 and G450 Media Gateways Release 7.1.3 (Builds 39.12.00 and 39.12.30)

ID	Minimum Conditions	Visible symptoms	Found in Release
CMG4XX-1006	G430/G450 Camp-on-busy-out	Performing a "campon-busyout voip-dsp" would immediately busy-out the DSP and cause all active calls using that DSP to be dropped. This would occur when there is only one DSP installed or if all the channels on all other DSPs are completely in use or busied-out.	6.3.14
CMG4XX-1018	G430/G450 with MP-160 DSP	In rare cases, an MP160 DSP core would fail when an SRTCP encrypted packet was received in an unexpected format. When an unexpected packet was received, the core would become unavailable and a reset of the DSP	7.0.1.3

ID	Minimum Conditions	Visible symptoms	Found in Release
		was required to resolve the problem.	
CMG4XX-1063	G430/G450	Improvements were made for calls using V.150 in V.32 mode in the presence of long round trip delay. A long round trip delay would prevent secure-sessions to be established when the far-end tries to initiate a secure session.	6.3.16
CMG4XX-1016	G430	On the G430, the "EASGProductCert" command incorrectly indicated that the product certificate was for a G450 Media Gateway.	7.1.2

Fixes in G430 and G450 Media Gateways Release 7.1.0.1 (Builds 38.20.01 and 38.20.31)

ID	Minimum Conditions	Visible symptoms	Found in Release
CMG4XX-877	SSH	Additional security hardening has been added when connecting to the gateway using SSH. Avaya recommends that all 7.x gateways be updated to this version.	7.0.2
CMG4XX-846	VoIP Calls	DSP voice distortion was experienced when A-Law Companding is used and the Total Search Timer has expired.	6.3.12

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

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

ID	Visible symptoms	Workaround
None	G430, G450 This Branch Gateway version does not support multiple IPv6 VLAN interfaces.	Use single VLAN interface with IPv6.
hw090790	G430, G450 EM_WEB doesn't work via dial in session (usb modem).	Use another network interface, such as the PMI, for connecting to Embedded Web.

Languages supported

- English

Documentation errata

- None

Avaya Aura® Media Server

For latest information refer to Avaya Aura® Media Server Release 7.8 Release Notes on the Avaya Support site at: https://downloads.avaya.com/css/P8/documents/101059289

Avaya WebLM

Installation for Avaya WebLM Release 7.1.x.x

Installation for Avaya WebLM Release 7.1.3.8

Download ID	Artifacts	Notes
SMGR7138GA3	WebLM 7.1.3.8 Patch Bin	Verify that the md5sum for the downloaded bin image matches the number on the Avaya PLDS website. WebLM_7.1.3.8_r713812159.bin Size: 450 MB MD5sum: 7523d4196b7802b7b25e23527bc64ce9

Installation for Avaya WebLM Release 7.1.3.7

Download ID	Artifacts	Notes
SMGR7137GA2	WebLM 7.1.3.7 Patch Bin	Verify that the md5sum for the downloaded bin image matches the number on the Avaya PLDS website. WebLM_7.1.3.7_r713711856.bin Size: 448 MB MD5sum: 38b1cf23c5c2edf13374b7c1cf137b6a

Installation for Avaya WebLM Release 7.1.3.6

Download ID	Artifacts	Notes
SMGR7136GA2	WebLM 7.1.3.6 Patch Bin	Verify that the md5sum for the downloaded bin image matches the number on the Avaya PLDS website. WebLM_7.1.3.6_r713611190.bin Size: 400 MB MD5sum: 7457056d557a5885d5de982a579b2486

Installation for Avaya WebLM Release 7.1.3.5

Download ID	Artifacts	Notes
SMGR7135GA2	WebLM 7.1.3.5 Patch Bin	Verify that the md5sum for the downloaded bin image matches the number on the Avaya PLDS website. WebLM_7.1.3.5_r713510638.bin Size: 399 MB MD5sum: 86a7fc2d804b31dea0a7ed237e949dcb

Installation for Avaya WebLM Release 7.1.3.4

Download ID	Artifacts	Notes
SMGR7134GA2	WebLM 7.1.3.4 Patch Bin	Verify that the md5sum for the downloaded bin image matches the number on the Avaya PLDS website. WebLM_7.1.3.4_r713409902.bin Size: 364.5 MB

Download ID	Artifacts	Notes
		MD5sum: 244ff668a078db9e97d7cc6749492520

Installation for Avaya WebLM Release 7.1.3.3

Download ID	Artifacts	Notes
SMGR7133GA2	WebLM 7.1.3.3 Patch Bin	Verify that the md5sum for the downloaded bin image matches the number on the Avaya PLDS website. WebLM_7.1.3.3_r713309122.bin Size: 361 MB MD5sum: 1d1e6bf8a329785636b146ecd4fdf9c5

Installation for Avaya WebLM Release 7.1.3.2

Download ID	Artifacts	Notes
SMGR7132GA3	WebLM 7.1.3.2 Patch Bin	Verify that the md5sum for the downloaded bin image matches the number on the Avaya PLDS website. WebLM_7.1.3.2_r713208317.bin Size: 346 MB MD5sum: 884f9ef636e66c38ad32d021ee3daaa7

Installation for Avaya WebLM on VMware Release 7.1.3.1

Download ID	Artifacts	Notes
SMGR7131GA3	WebLM 7.1.3.1 Patch Bin	Verify that the md5sum for the downloaded bin image matches the number on the Avaya PLDS website. WebLM_7.1.3.1_r713108171.bin Size: 346 MB MD5sum: 570c71012372dab22be00dcf22cb7a31

Installation for Avaya WebLM Release 7.1.3

Download ID	Artifacts	Notes
SMGR713GA03	WebLM 7.1.3 GA Patch Bin	WebLM_7.1.3.0_r713007757.bin Size: 273 MB MD5sum: 6363d8540cdfdd174787636da1ca0df8

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

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

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

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

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

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

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

Installation for Avaya WebLM Release 7.1.2

Download ID	Artifacts	Notes
SMGR712GA03	WebLM 7.1.2 GA Patch Bin	WebLM_7.1.2.0_r712007342.bin Size: 300 MB MD5sum: 02c5734a02d6d310adf9d918b7f602c6
SMGR712GA04	WebLM KVM OVA 7.1GA OVA	WebLM-7.1.0.0.11-27074-kvm-10.ova Size: 925 MB MD5sum: 47ef1b939cb8773e6b48c425567d144e
SMGR712GA05	WebLM AWS OVA 7.1GA OVA	WebLM-7.1.0.0.11-27074-aws-17.ova Size: 943 MB MD5sum: d66677872dda87ee026ca630b3b2b27b

Installation for Avaya WebLM Release 7.1.1

Download ID	Artifacts	Notes
SMGR71GA003	WebLM 7.1GA OVA	WebLM-7.1.0.0.11-25605-e65-20.ova Size: 943 MB MD5SUM: 74cdcf0b962521f7e38d8ad937023fc1
SMGR711GA03	WebLM 7.1.1 GA Patch Bin	Verify that the md5sum for the downloaded OVA/Bin image matches the number on the Avaya PLDS website. WebLM_7.1.1.0_r711006919.bin Size: 239 MB Md5sum: 7e4042d3df215da0ab3c4da7966d8e7a

Installing the release 7.1.x

Important Notes

1. Characters required in the hostname

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

2. Cloning WebLM on VMware.

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

3. Restoring WebLM Backup.

   Ensure that the 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 change, a re-host of license files will be required. A re-host is required in following scenarios:
     - Upgrade: This involves setting up a new VM with new UUID and restoring data on the same. Since UUID changes, host ID would change, and any existing files would become invalid. Re-host of licenses is required.
     - Migration (from SP to VE): Since the host ID would change, a re-host of license files will be required.
   - IP address is changed: If IP address is changed, host ID changes and a re-host of license files is required.
   - VMware cloning of WebLM: This would cause the UUID to change and therefore the host ID would change. A re-host of license files will be required.
   - Re-host is not required for vMotion moves.

Resource allocation and reservation for standalone WebLM on VMware

VMware resource	Profile 1 Values that can support up to 5000 license requests (Default)	Profile 2 Values that can support more than 5000 license requests
vCPUs	1	1
CPU reservation	2290 MHz	2290 MHz
Memory	1 GB	2 GB
Memory reservation	1 GB	2 GB
Storage reservation	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
Red Hat	7.2
OpenJDK	OpenJDK version "1.8.0_131" 64-bit
Apache Tomcat	9.0.0.M26
Internet Explorer	9.x, 10.x and 11.x
Firefox	48,49,50

- 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.x release

For any problems with WebLM 7.1.x, 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 WebLM for 7.1.x.x

What's new in Avaya WebLM for 7.1.3.8

The following table lists enhancements in this release:

Enhancement	Description
N/A	N/A

What's new in Avaya WebLM for 7.1.3.7

The following table lists enhancements in this release:

Enhancement	Description
N/A	N/A

What's new in Avaya WebLM for 7.1.3.6

The following table lists enhancements in this release:

Enhancement	Description
N/A	N/A

What's new in Avaya WebLM for 7.1.3.5

The following table lists enhancements in this release:

Enhancement	Description
N/A	N/A

What's new in Avaya WebLM for 7.1.3.4

The following table lists enhancements in this release:

Enhancement	Description
N/A	N/A

What's new in Avaya WebLM for 7.1.3.3

The following table lists enhancements in this release:

Enhancement	Description
N/A	N/A

What’s new in Avaya WebLM for 7.1.3.2

The following table lists enhancements in this release:

Enhancement	Description
N/A	N/A

What’s new in Avaya WebLM for 7.1.3.1

The following table lists enhancements in this release:

Enhancement	Description
N/A	N/A

What’s new in Avaya WebLM for 7.1.3

The following table lists enhancements in this release:

Enhancement	Description
Infrastructure	Changed JDK to OpenJDK 8u161.

What’s new in Avaya WebLM for 7.1.2

The following table lists enhancements in this release:

Enhancement	Description
Support for old password after upgrade	The old password for Web UI is retained after upgrading to WebLM 7.1.2 from previous releases (7.1.x releases). If upgrade to 7.1.2 was from 7.0.x and earlier versions, then user is forced to change password to upgrade to a stronger encryption.
Infrastructure	• Changed JDK to OpenJDK 8u131. • Upgraded Tomcat to 9.0.0 M26

What’s new in Avaya WebLM for 7.1.1

The following table lists enhancements in this release.

Enhancement	Description
JDK Upgrade	Upgraded to OpenJDK8u131 from OpenJDK8u121 for Oracle Java SE Critical Patch Update

What’s new in Avaya WebLM 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

Enhancement	Description
	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) On Fresh install of WebLM port 52233 will be secured using self-signed certificates. If admin need to revert to the default SIP CA certificates on port 52233 on a fresh install of WebLM, use the command “toggleWeblmOldcert” for the same else use 3rd party certificates. Refer the WebLM admin guide for more details.

Fixes in Avaya WebLM on VMware for 7.1.x.x

Fixes in Avaya WebLM on VMware for 7.1.3.8

ID	Description
SMGR-58748	(RHSA-2020:4032) Moderate: dbus security update
SMGR-58738	(RHSA-2020:4276) Important: kernel security update
SMGR-58782	(RHSA-2020:3848) Low: libmspack security update
SMGR-58772	(RHSA-2020:3908) Moderate: cpio security update
SMGR-58766	(RHSA-2020:3901) Low: libpng security update
SMGR-58774	(RHSA-2020:3901) Low: libpng security update
SMGR-58768	(RHSA-2020:3915) Moderate: libssh2 security update
SMGR-58770	(RHSA-2020:3911) Moderate: python security update
SMGR-58728	(RHSA-2020:5009) Moderate: python security update
SMGR-58746	(RHSA-2020:4041) Moderate: openldap security update
SMGR-58756	(RHSA-2020:4005) Moderate: libxslt security update
SMGR-58734	(RHSA-2020:4907) Important: freetype security update
SMGR-58730	(RHSA-2020:5002) Moderate: curl security update
SMGR-58764	(RHSA-2020:3952) Moderate: expat security update
SMGR-58718	(RHSA-2020:5566) Important: openssl security update
SMGR-58742	(RHSA-2020:4072) Moderate: libcroco security update
SMGR-58732	(RHSA-2020:4908) Important: libX11 security update
SMGR-58744	(RHSA-2020:4060) Important: kernel security, bug fix, and enhancement update
SMGR-58780	(RHSA-2020:3861) Low: glibc security, bug fix, and enhancement update
SMGR-58760	(RHSA-2020:3996) Moderate: libxml2 security and bug fix update
SMGR-58724	(RHSA-2020:5023) Moderate: kernel security and bug fix update
SMGR-58754	(RHSA-2020:4007) Low: systemd security and bug fix update

ID	Description
SMGR-58758	(RHSA-2020:4003) Moderate: Network Manager security and bug fix update
SMGR-58752	(RHSA-2020:4011) Moderate: e2fsprogs security and bug fix update
SMGR-58720	(RHSA-2020:5437) Important: kernel security and bug fix update
SMGR-58762	(RHSA-2020:3978) Moderate: glib2 and ibus security and bug fix update
SMGR-58726	(RHSA-2020:5011) Moderate: bind security and bug fix update
SMGR-58722	(RHSA-2020:5083) Moderate: microcode_ctl security, bug fix, and enhancement update
SMGR-58776	(RHSA-2020:3878) Low: dnsmasq security and bug fix update
SMGR-58740	(RHSA-2020:4076) Moderate: nss and nspr security, bug fix, and enhancement update
SMGR-58736	(RHSA-2020:4350) Moderate: java-1.8.0-openjdk security and bug fix update
SMGR-58750	(RHSA-2020:4026) Moderate: mariadb security and bug fix update
SMGR-58778	(RHSA-2020:3864) Moderate: cups security and bug fix update

Fixes in Avaya WebLM on VMware for 7.1.3.7

The following table lists the fixes in this release:

ID	Description
SMGR-54456	Vulnerability within the Avaya Web License Manager (WebLM) allows an authenticated user to read arbitrary files.
SMGR-54449	Remove AJP port 8009 from configurations.
SMGR-54968	(RHSA-2020:1020) Low: curl security and bug fix update
SMGR-54916	(RHSA-2020:1113) Moderate: bash security update
SMGR-56793 SMGR-57368	(RHSA-2020:2663) Moderate: ntp security update
SMGR-57385	(RHSA-2020:2894) Important: dbus security update
SMGR-54988	(RHSA-2020:1138) Low: gettext security and bug fix update
SMGR-54992	(RHSA-2020:1000) Moderate: rsyslog security, bug fix, and enhancement update
SMGR-54928	(RHSA-2020:1176) Low: avahi security update
SMGR-56794 SMGR-57380	(RHSA-2020:3217) Moderate: grub2 security and bug fix update
SMGR-54980	(RHSA-2020:1135) Low: polkit security and bug fix update
SMGR-56790 SMGR-57376	(RHSA-2020:2968) Important: java-1.8.0-openjdk security update
SMGR-55450	(RHSA-2020:2082) Important: kernel security and bug fix update
SMGR-54960	(RHSA-2020:1047) Moderate: wireshark security and bug fix update
SMGR-54920	(RHSA-2020:1512) Important: java-1.8.0-openjdk security update
SMGR-54984	(RHSA-2020:1061) Moderate: bind security and bug fix update
SMGR-54924	(RHSA-2020:1022) Low: file security update
SMGR-54972	(RHSA-2020:1080) Moderate: evolution security and bug fix update

ID	Description
SMGR-54976	(RHSA-2020:1050) Moderate: cups security and bug fix update
SMGR-54912	(RHSA-2020:1011) Moderate: expat security update
SMGR-56792 SMGR-57372	(RHSA-2020:3220) Important: kernel security and bug fix update
SMGR-55609 SMGR-57362	(RHSA-2020:2432) Moderate: microcode_ctl security, bug fix and enhancement update
SMGR-56791 SMGR-57358	(RHSA-2020:2664) Important: kernel security and bug fix update
SMGR-54936	(RHSA-2020:1016) Moderate: kernel security, bu
SMGR-54952	(RHSA-2020:1021) Moderate: GNOME security, bug fix, and enhancement update
SMGR-54898	(RHSA-2020:1131) Moderate: python security update
SMGR-54948	(RHSA-2020:1100) Moderate: mariadb security and bug fix update
SMGR-54944	(RHSA-2020:0897) Important: icu security update
SMGR-54902	(RHSA-2020:1181) Low: unzip security update
SMGR-57389	(RHSA-2020:2344) Important: bind security update
SMGR-54932	(RHSA-2020:1190) Moderate: libxml2 security update

Fixes in Avaya WebLM on VMware for 7.1.3.6

The following table lists the fixes in this release:

ID	Description
SMGR-53941	**(RHSA-2020:0630) Important: ppp security update**
SMGR-53938	(RHSA-2020:0540) Important: sudo security update
SMGR-53930	(RHSA-2020:0196) Important: java-1.8.0-openjdk security update
SMGR-53934	(RHSA-2020:0227) Important: sqlite security update
SMGR-53926	(RHSA-2020:0374) Important: kernel security and bug fix update
SMGR-53080	(RHSA-2019:3979) Important: kernel security and bug fix update
SMGR-53076	(RHSA-2019:4190) Important: nss, nss-softokn, nss-util security update
SMGR-53072	(RHSA-2019:3872) Important: kernel security update
SMGR-53068	(RHSA-2019:3834) Important: kernel security update
SMGR-53060	(RHSA-2019:3976) Low: tcpdump security update
SMGR-53064	(RHSA-2019:4326) Important: fribidi security update
SMGR-53846	(RHSA-2020:0663) ruby update
SMGR-52875	Patch installation fails due to unavailability of required space in /tmp partition.

Fixes in Avaya WebLM on VMware for 7.1.3.5

The following table lists the fixes in this release:

ID	Description

ID	Description
SMGR-50378	**(RHSA-2019:2053) Moderate: libtiff security update**
SMGR-50360	(RHSA-2019:2035) Low: python-requests security update
SMGR-50876	kernel (RHSA-2019:3872)
SMGR-50587	java-1.8.0-openjdk (RHSA-2019:1815)
SMGR-50586	python-urllib3 (RHSA-2019:2272)
SMGR-50597	openssl (RHSA-2019:2304)
SMGR-50585	glibc (RHSA-2019:2118)
SMGR-50589	curl (RHSA-2019:2181)
SMGR-50595	polkit (RHSA-2019:2046)
SMGR-50594	python-requests (RHSA-2019:2035)
SMGR-50603	kernel (RHSA-2018:2748)
SMGR-50598	nss, nss-softokn, nss-util, and nspr (RHSA-2019:2237)
SMGR-50592	bind (RHSA-2019:2057) (tcp)
SMGR-50590	ntp (RHSA-2019:2077)
SMGR-50602	libssh2 (RHSA-2019:2136)
SMGR-50593	unzip (RHSA-2019:2159)
SMGR-50599	ruby (RHSA-2019:2028)
SMGR-50600	python (RHSA-2019:2030)
SMGR-50601	binutils (RHSA-2019:2075)
SMGR-50605	openssh (RHSA-2019:2143)
SMGR-50604	kernel (RHSA-2019:2829)
SMGR-50609	elfutils (RHSA-2019:2197)
SMGR-50608	libmspack (RHSA-2019:2049)
SMGR-50610	procps-ng (RHSA-2019:2189)
SMGR-50611	systemd (RHSA-2019:2091)
SMGR-50614	sssd (RHSA-2019:2177)
SMGR-50606	libcgroup (RHSA-2019:2047)
SMGR-50613	Xorg (RHSA-2019:2079)
SMGR-50607	libjpeg-turbo (RHSA-2019:2052)
SMGR-50612	pango (RHSA-2019:2571)

Fixes in Avaya WebLM on VMware for 7.1.3.4

The following table lists the fixes in this release:

ID	Description
SMGR-47681	Provide a command line utility to add certificates to trust store. Refer Admin guide for more details.
SMGR-49438	(RHSA-2019:1587) python security and bug fix update
SMGR-48475	(RHSA-2019:0194) bind security update

ID	Description
SMGR-48472	(RHSA-2019:0230) polkit security update
SMGR-48466	(RHSA-2019:0109) perl security update
SMGR-48531	(RHSA-2019:0435) Moderate: java-1.8.0-openjdk security update
SMGR-49276	(RHSA-2019:0775) Important: java-1.8.0-openjdk security update
SMGR-49289	(RHSA-2019:1228) Important: wget security update
SMGR-48524	[RHSA-2019:0483) Moderate: openssl security and bug fix update
SMGR-49312	(RHSA-2019:1481) Important: kernel security update
SMGR-49297	(RHSA-2019:1235) Important: ruby security update
SMGR-48510	(RHSA-2019:0368) Important: systemd security update
SMGR-49281	(RHSA-2019:1294) Important: bind security update
SMGR-48517	(RHSA-2019:2019:0512) Important: kernel security, bug fix, and enhancement update
SMGR-48596	(RHSA-2019:0710) Important: python security update
SMGR-48481	(RHSA-2019:0679) Important: libssh2 security update
SMGR-48756	(RHSA-2019:0818) Important: kernel security and bug fix update
SMGR-49303	(RHSA-2019:1168) Important: kernel security update
SMGR-48469	(RHSA-2019:0163) kernel security, bug fix, and enhancement update
SMGR-48506	(RHSA-2019-0201) systemd security update
SMGR-48463	(RHSA-2019:0049) systemd security update

Fixes in Avaya WebLM on VMware for 7.1.3.3

The following table lists the fixes in this release:

ID	Description
SMGR-47412	(RHSA-2018:3071) Low: krb5 security, bug fix, and enhancement update
SMGR-47266	(RHSA-2018:3041) Moderate: python security and bug fix update
SMGR-46929	(RHSA-2018:2768) Moderate: nss security update
SMGR-46929	(RHSA-2018:2768) Moderate: nss security update
SMGR-46925	(RHSA-2018:2748) Important: kernel security and bug fix update
SMGR-47275	(RHSA-2018:3157) Moderate: curl and nss-pem security and bug fix update
SMGR-47244	(RHSA-2018:2942) Critical: java-1.8.0-openjdk security update
SMGR-47271	(RHSA-2018:3158) Low: sssd security, bug fix, and enhancement update
SMGR-47248	(RHSA-2018:3032) Low: binutils security, bug fix, and enhancement update
SMGR-47433	(RHSA-2018:3083) Important: kernel security, bug fix, and enhancement update
SMGR-47279	(RHSA-2018:3107) Moderate: wpa_supplicant security and bug fix update
SMGR-47417	(RHSA-2018:3327) Low: libmspack security update
SMGR-47252	(RHSA-2018:3052) Moderate: wget security and bug fix update
SMGR-47323	(RHSA-2018:3249) Low: setup security and bug fix update
SMGR-47422	(RHSA-2018:3059) Low: X.org X11 security, bug fix, and enhancement update

ID	Description
SMGR-47406	(RHSA-2018:3221) Moderate: openssl security, bug fix, and enhancement update
SMGR-47256	(RHSA-2018:3050) Moderate: gnutls security, bug fix, and enhancement update
SMGR-47550	(RHSA-2018:3651) Moderate: kernel security, bug fix, and enhancement update
SMGR-47544	(RHSA-2018:3092) Moderate: glibc security, bug fix, and enhancement update
SMGR-46117	Login Form and Change password form vulnerable to Brute Force.
SMGR-46116	Interchangeable GET and POST Request.
SMGR-47711	/opt/ partition filling up in 7.1 Standalone WebLM OVA because of tomcat access logs.
SMGR-46115	Standalone WebLM cross-site scripting (XSS) vulnerability.

Fixes in Avaya WebLM on VMware for 7.1.3.2

The following table lists the fixes in this release:

ID	Description
SMGR-46534	(RHSA-2018:2439) mariadb security and bug fix update
SMGR-46536	(RHSA-2018:2570) Important: bind security update
SMGR-46421	Login page should not show logged in username if another user tries to login
SMGR-46405	tzdata Linux RPM updated to tzdata-2018e

Fixes in Avaya WebLM on VMware for 7.1.3.1

The following table lists the fixes in this release:

ID	Description
SMGR-44855	(RHSA-2018:0378) Important: ruby security update
SMGR-45383	(RHSA-2018:0483) Important: dhcp security update
SMGR-46071	(RHSA-2018:1700) Important: procps-ng security update
SMGR-46066	(RHSA-2018:1649) Important: java-1.8.0-openjdk security update
SMGR-46062	(RHSA-2018:1629) Important: kernel security update
SMGR-46019	[RHSA-2018:1191-01] Critical: java-1.8.0-openjdk security update
SMGR-46084	/var/log partition getting full due to log rotation is not working for system log files like messages, secure and kern.log files.

Fixes in Avaya WebLM on VMware for 7.1.3

The following table lists the fixes in this release:

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

Fixes in Avaya WebLM on VMware for 7.1.2

The following table lists the fixes in this release:

ID	Description
SMGR-41909	C++ WebLM client (7.1.x) is unable to connect to WebLM 7.1.x release

Fixes in Avaya WebLM on VMware for 7.1.1

The following table lists the fixes in this release:

ID	Description
SMGR-40359	FT - IPOL - WebLM - CSRF attack is possible
SMGR-39867	CLID is incorrectly labelled "Element ID", Partners are confused
SMGR-40513	[WebLM] Host ID description shall be corrected for other Virtual environment

Fixes in Avaya 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 WebLM on VMware for 7.1.x.x

Known issues and workarounds in Avaya WebLM on VMware for 7.1.3.8

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

ID	Visible symptoms	Workaround
SMGR-37985	Email notifications from WebLM server do not have a valid From field	
SMGR-41362	In System Manager 7.1.x.x and Solution Deployment Manager Client 7.1.x.x used while deploying WebLM OVA if CLI / UI password of VM includes few special characters such as ',>,<,&,", = then the password will not be set properly for VM after post deployment	Do not use special characters mentioned in list during deployment. Once deployment successfully completed then reset the password as per requirement.
SMGR-45036	When WebLM 7.1 OVA is deployed on AVP 7.1, AVP shows a warning that configured Guest OS and OS of running VM doesn't match	Ignore the warning message
SMGR-48582	WebLM fails to generate hosts ID when system language is set to local language like de_DE.UTF-8 i.e. Germany (other than English)	Set the system language to English.

Known issues and workarounds in Avaya WebLM on VMware for 7.1.3.7

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

ID	Visible symptoms	Workaround

ID	Visible symptoms	Workaround
SMGR-37985	Email notifications from WebLM server do not have a valid From field	
SMGR-41362	In System Manager 7.1.x.x and Solution Deployment Manager Client 7.1.x.x used while deploying WebLM OVA if CLI / UI password of VM includes few special characters such as ',>,<,&,", = then the password will not be set properly for VM after post deployment	Do not use special characters mentioned in list during deployment. Once deployment successfully completed then reset the password as per requirement.
SMGR-45036	When WebLM 7.1 OVA is deployed on AVP 7.1, AVP shows a warning that configured Guest OS and OS of running VM doesn't match	Ignore the warning message
SMGR-48582	WebLM fails to generate hosts ID when system language is set to local language like de_DE.UTF-8 i.e. Germany (other than English)	Set the system language to English.

Known issues and workarounds in Avaya WebLM on VMware for 7.1.3.6

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

ID	Visible symptoms	Workaround
SMGR-37985	Email notifications from WebLM server do not have a valid From field	
SMGR-41362	In System Manager 7.1.x.x and Solution Deployment Manager Client 7.1.x.x used while deploying WebLM OVA if CLI / UI password of VM includes few special characters such as ',>,<,&,", = then the password will not be set properly for VM after post deployment	Do not use special characters mentioned in list during deployment. Once deployment successfully completed then reset the password as per requirement.
SMGR-54062	Remove AJP port 8009 from configurations.	
SMGR-45036	When WebLM 7.1 OVA is deployed on AVP 7.1, AVP shows a warning that configured Guest OS and OS of running VM doesn't match	Ignore the warning message
SMGR-48582	WebLM fails to generate hosts ID when system language is set to local language like de_DE.UTF-8 i.e. Germany (other than English)	Set the system language to English.

Known issues and workarounds in Avaya WebLM on VMware for 7.1.3.5

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

ID	Visible symptoms	Workaround
SMGR-37985	Email notifications from WebLM server do not have a valid From field	
SMGR-41362	In System Manager 7.1.x.x and Solution Deployment Manager Client 7.1.x.x used while deploying WebLM OVA if CLI / UI password of VM includes few special characters such as ',>,<,&,", = then the password will not be set properly for VM after post deployment	Do not use special characters mentioned in list during deployment. Once deployment successfully completed then reset the password as per requirement.
SMGR-45036	When WebLM 7.1 OVA is deployed on AVP 7.1, AVP shows a warning that configured Guest OS	Ignore the warning message

ID	Visible symptoms	Workaround
	and OS of running VM doesn't match	
SMGR-48582	WebLM fails to generate hosts ID when system language is set to local language like de_DE.UTF-8 i.e. Germany (other than English)	

Known issues and workarounds in Avaya WebLM on VMware for 7.1.3.4

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

ID	Visible symptoms	Workaround
SMGR-37985	Email notifications from WebLM server do not have a valid From field	
SMGR-41362	In System Manager 7.1.x.x and Solution Deployment Manager Client 7.1.x.x used while deploying WebLM OVA if CLI / UI password of VM includes few special characters such as ',>,<,&,", = then the password will not be set properly for VM after post deployment	Do not use special characters mentioned in list during deployment. Once deployment successfully completed then reset the password as per requirement.
SMGR-45036	When WebLM 7.1 OVA is deployed on AVP 7.1, AVP shows a warning that configured Guest OS and OS of running VM doesn't match	Ignore the warning message

Known issues and workarounds in Avaya WebLM on VMware for 7.1.3.3

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

ID	Visible symptoms	Workaround
SMGR-37985	Email notifications from WebLM server do not have a valid From field	
SMGR-41362	In System Manager 7.1.x.x and Solution Deployment Manager Client 7.1.x.x used while deploying WebLM OVA if CLI / UI password of VM includes few special characters such as ',>,<,&,", = then the password will not be set properly for VM after post deployment	Do not use special characters mentioned in list during deployment. Once deployment successfully completed then reset the password as per requirement.
SMGR-45036	When WebLM 7.1 OVA is deployed on AVP 7.1, AVP shows a warning that configured Guest OS and OS of running VM doesn't match	Ignore the warning message

Known issues and workarounds in Avaya WebLM on VMware for 7.1.3.2

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

ID	Visible symptoms	Workaround
SMGR-37985	Email notifications from WebLM server do not have a valid From field	
SMGR-41362	In System Manager 7.1.x.x and Solution Deployment Manager Client 7.1.x.x used	Do not use special characters mentioned in list during deployment.

ID	Visible symptoms	Workaround
	while deploying WebLM OVA if CLI / UI password of VM includes few special characters such as ',>,<,&,", = then the password will not be set properly for VM after post deployment	Once deployment successfully completed then reset the password as per requirement.
SMGR-45036	When WebLM 7.1 OVA is deployed on AVP 7.1, AVP shows a warning that configured Guest OS and OS of running VM doesn't match	Ignore the warning message

Known issues and workarounds in Avaya WebLM on VMware for 7.1.3.1

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

ID	Visible symptoms	Workaround
SMGR-37985	Email notifications from WebLM server do not have a valid From field	
SMGR-41362	In System Manager 7.1.x.x and Solution Deployment Manager Client 7.1.x.x used while deploying WebLM OVA if CLI / UI password of VM includes few special characters such as ',>,<,&,", = then the password will not be set properly for VM after post deployment	Do not use special characters mentioned in list during deployment. Once deployment successfully completed then reset the password as per requirement.
SMGR-45036	When WebLM 7.1 OVA is deployed on AVP 7.1, AVP shows a warning that configured Guest OS and OS of running VM doesn't match	Ignore the warning message

Known issues and workarounds in Avaya WebLM on VMware for 7.1.3

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

ID	Visible symptoms	Workaround
SMGR-37985	Email notifications from WebLM server do not have a valid From field	
SMGR-41362	In System Manager 7.1.x.x and Solution Deployment Manager Client 7.1.x.x used while deploying WebLM OVA if CLI / UI password of VM includes few special characters such as ',>,<,&,", = then the password will not be set properly for VM after post deployment	Do not use special characters mentioned in list during deployment. Once deployment successfully completed then reset the password as per requirement.

Known issues and workarounds in Avaya WebLM on VMware for 7.1.2

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

ID	Visible symptoms	Workaround
SMGR-37985	Email notifications from WebLM server do not have a valid From field	
SMGR-41362	In System Manager 7.1.x.x and Solution Deployment Manager Client 7.1.x.x used while deploying WebLM OVA if CLI / UI password of	Do not use special characters mentioned in list during deployment. Once deployment successfully

ID	Visible symptoms	Workaround
	VM includes few special characters such as ',>,<,&,", = then the password will not be set properly for VM after post deployment	completed then reset the password as per requirement.

Known issues and workarounds in Avaya WebLM on VMware for 7.1.1

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

ID	Visible symptoms	Workaround
NA	NA	NA

Known issues and workarounds in Avaya 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

For latest information refer to Avaya Aura® Device Services Release 7.1.x Release Notes on the Avaya Support site.

- AADS Releases 7.1.5 Release Notes: https://downloads.avaya.com/css/P8/documents/101045822