Avaya Aura® Release Notes

Release 10.2.x.x
Issue 17
July 2026

© 2018-2026 Avaya LLC

All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, https://support.avaya.com/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA LLC., 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 LLC. 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.

License Compliance

Avaya and/or the Avaya Channel Partners have the right to inspect and/or audit (i) by remote polling or other reasonable electronic means at any time and (ii) in person during normal business hours and with reasonable notice End User's books, records, and accounts, to determine End User's compliance with these Software License Terms, including but not limited to usage levels. In the event such inspection or audit uncovers non-compliance with these Software License Terms, then without prejudice to Avaya's termination rights hereunder, End User shall promptly pay Avaya any applicable license fees. End User agrees to keep a current record of the location of the Software. Avaya software may securely transmit limited information to Avaya to ensure compliance with your End User License Agreement.

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. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of 15https://support.avaya.com/security

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

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com/ (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Change history 13
Introduction 14
Documentation Catalog 15
Product Release Matrix 15
What's new in Avaya Aura® 18
Discontinued support for IP Server Interface (TN2312, commonly known as "IPSI") 18
Future use fields visible in Avaya Aura® Release 10.2 18
Security Service Packs 18
Compatibility 18
Contact support checklist 18
Contact support tasks 19
Avaya Aura® Communication Manager 19
What's new in Communication Manager Release 10.2.x.x 19
What's new in Communication Manager Release 10.2.1.1.0 19
What's new in Communication Manager Release 10.2.1.0.0 19
What's new in Communication Manager Release 10.2.0.1.0 19
What's new in Communication Manager Release 10.2 19
Future use fields visible in Avaya Aura® Communication Manager Release 10.2.x.x 20
Future use fields visible in Avaya Aura® Communication Manager Release 10.2 20
Security Service Pack 20
Security Service Pack 20
Required artifacts for Avaya Aura® Communication Manager 10.2.x.x 20
Required artifacts for Communication Manager Release 10.2.1.4.0 20
Required artifacts for Communication Manager Release 10.2.1.3.0 21
Required artifacts for Communication Manager Release 10.2.1.2.0 21
Required artifacts for Communication Manager Release 10.2.1.1.0 21
Required artifacts for Communication Manager Release 10.2.1.0.0 21
Required artifacts for Communication Manager Release 10.2.0.1.0 22
Required artifacts for Communication Manager Release 10.2 22
Software information 23
Installation for Avaya Aura® Communication Manager 10.2.x.x 24
Installation for Avaya Aura® Communication Manager Release 10.2.1.4.0 24
Installation for Avaya Aura® Communication Manager Release 10.2.1.3.0 24
Installation for Avaya Aura® Communication Manager Release 10.2.1.2.0 24
Installation for Avaya Aura® Communication Manager Release 10.2.1.1.0 24
Installation for Avaya Aura® Communication Manager Release 10.2.1.0.0 24
Installation for Avaya Aura® Communication Manager Release 10.2.0.1.0 24
Installation for Avaya Aura® Communication Manager Release 10.2 24
Troubleshooting the installation 24
Enhanced Access Security Gateway (EASG) 25
Fixes in Communication Manager Release 10.2.x.x 25
Fixes in Communication Manager Release 10.2.1.4.0 25
Fixes in Communication Manager Release 10.2.1.3.0 26
Fixes in Communication Manager Release 10.2.1.2.0 28
Fixes in Communication Manager Release 10.2.1.1.0 29

Fixes in Communication Manager Release 10.2.1.0.0 31
Fixes in Communication Manager Release 10.2.0.1.0 34
Fixes in Communication Manager Release 10.2 36
Known issues and workarounds in Communication Manager Release 10.2.x.x 38
Known issues and workarounds in Communication Manager Release 10.2.1.4.0 38
Known issues and workarounds in Communication Manager Release 10.2.1.3.0 39
Known issues and workarounds in Communication Manager Release 10.2.1.2.0 40
Known issues and workarounds in Communication Manager Release 10.2.1.1.0 41
Known issues and workarounds in Communication Manager Release 10.2.1.0.0 42
Known issues and workarounds in Communication Manager Release 10.2.0.1.0 42
Known issues and workarounds in Communication Manager Release 10.2 43
Avaya Aura® Session Manager 44
What’s new in Session Manager Release 10.2.x.x 44
What’s new in Session Manager Release 10.2.1.1 44
What’s new in Session Manager Release 10.2 44
Future use fields visible in Avaya Aura® Session Manager Release 10.2.x.x 44
Future use fields visible in Avaya Aura® Session Manager Release 10.2 44
Security Service Pack 44
Security Service Pack 44
Required artifacts for Session Manager Release 10.2.x.x 44
Required artifacts for Session Manager Release 10.2.1.4 44
Required artifacts for Session Manager Release 10.2.1.3 45
Required artifacts for Session Manager Release 10.2.1.2 45
Required artifacts for Session Manager Release 10.2.1.1 45
Required artifacts for Session Manager Release 10.2.1.0 45
Required artifacts for Session Manager Release 10.2.0.1 46
Required artifacts for Session Manager Release 10.2 46
Software information 46
Installation for Session Manager Release 10.2.x.x 47
Backing up the software 47
Installing the Session Manager software 47
Upgrading the Session Manager software 47
Troubleshooting the installation 48
Restoring software to the previous version 48
Fixes in Session Manager Release 10.2.x.x 48
Fixes in Session Manager Release 10.2.1.4 48
Fixes in Session Manager Release 10.2.1.3 49
Fixes in Session Manager Release 10.2.1.2 49
Fixes in Session Manager Release 10.2.1.1 49
Fixes in Session Manager Release 10.2.1.0 50
Fixes in Session Manager Release 10.2.0.1 52
Fixes in Session Manager Release 10.2.0.0 52
Known issues and workarounds in Session Manager 10.2.x.x 56
Known issues and workarounds in Session Manager Release 10.2.1.4 56
Known issues and workarounds in Session Manager Release 10.2.1.3 57
Known issues and workarounds in Session Manager Release 10.2.1.2 57
Known issues and workarounds in Session Manager Release 10.2.1.1 58
Known issues and workarounds in Session Manager Release 10.2.1.0 59

Known issues and workarounds in Session Manager Release 10.2.0.1 60
Known issues and workarounds in Session Manager Release 10.2.0.0 61
Avaya Aura® System Manager 63
What's new in System Manager Release 10.2.x.x 63
What's new in System Manager Release 10.2.1.1.0 63
What's new in System Manager Release 10.2.1.0 63
What's new in System Manager Release 10.2.0.1 63
What's new in System Manager Release 10.2 63
Security Service Pack 63
Security Service Pack 63
Managing ASP using SDM in 10.2.x.x 64
Avaya Solutions Platform S8300 Release 5.1 64
Required artifacts for System Manager Release 10.2.1.4 64
Required artifacts for System Manager Release 10.2.1.3 65
Required artifacts for System Manager Release 10.2.1.2 65
Required artifacts for System Manager Release 10.2.1.1 66
Required artifacts for System Manager Release 10.2.1.0 67
Required artifacts for System Manager Release 10.2.0.1 68
Required artifacts for System Manager Release 10.2 68
Required patches for System Manager Release 10.2.x.x 69
Must read 70
Software information 71
How to find a License Activation Code (LAC) in PLDS for a product. 71
Installation for System Manager Release 10.2.x.x 72
Backing up the software 72
Installing the System Manager software 72
Upgrading the System Manager software 72
Troubleshooting the installation 72
Fixes in System Manager 10.2.1.4 72
Fixes in System Manager 10.2.1.3 73
Fixes in System Manager 10.2.1.2 74
Fixes in System Manager 10.2.1.1 75
Fixes in System Manager 10.2.1 76
Fixes in System Manager 10.2.0.1 78
Fixes in System Manager 10.2.0.0 80
Known issues and workarounds in System Manager in Release 10.2.1.4 87
Known issues and workarounds in System Manager in Release 10.2.1.3 87
Known issues and workarounds in System Manager in Release 10.2.1.2 88
Known issues and workarounds in System Manager in Release 10.2.1.1 88
Known issues and workarounds in System Manager in Release 10.2.1.0 89
Known issues and workarounds in System Manager in Release 10.2.0.1 90
Known issues and workarounds in System Manager in Release 10.2.0.0 91
Solution Deployment Manager Adopter Matrix 92
Avaya Aura® Presence Services 95
What's new in Presence Services Release 10.1.0.2.x 95
Presence Services Release 10.1.0.2 Support on Avaya Solution Platform 130 R6.x 95
Hardware requirements for installation on ASP 130 R6.x 95
Deployment procedure 95

What's new in Presence Services Release 10.1.x.x 96
Required artifacts for Presence Services Release 10.1.0.2.x 96
Required artifacts for Presence Services Release 10.1.0.1.x 96
Required patches for Presence Services 10.1 96
Backing up the software 97
Installing Presence Services Release 10.1.x.x 97
Troubleshooting the installation 97
Restoring software to the previous version 97
Migrating to the PS 10.1.x release from a PS 6.2.X release 97
Changes Affecting Migrations to 10.1 97
Minimum required versions by Release 97
Upgrade References to Presence Services Release 10.1.x 98
Interoperability and requirements/Applicability for Release 10.1.x 98
Software Development Kit 98
Functionality not supported in Presence Services 10.1.x.x 99
Functionality not supported in Presence Services 10.1 99
Fixes in Presence Services Release 10.1.x.x 99
Fixes in Presence Services Release 10.1.0.2 99
Fixes in Presence Services Release 10.1 99
Known issues and workarounds in Presence Services Release 10.1.x.x 100
Known issues and workarounds in Presence Services Release 10.1.0.2 100
Known issues and workarounds in Presence Services Release 10.1 100
Avaya Aura® Application Enablement Services 102
What's new in Application Enablement Services Release 10.2.x.x 102
What's new in Application Enablement Services 10.2.1.1 102
What's new in Application Enablement Services 10.2.1.0 102
What's new in Application Enablement Services 10.2 102
Security Service Packs 102
Security Service Packs 102
Required artifacts for Application Enablement Services Release 10.2.x.x 102
Required artifacts for Application Enablement Services Release 10.2.1.4 102
Required artifacts for Application Enablement Services Release 10.2.1.3 102
Required artifacts for Application Enablement Services Release 10.2.1.2 103
Required artifacts for Application Enablement Services Release 10.2.1.1 103
Required artifacts for Application Enablement Services Release 10.2.1.0 103
Required artifacts for Application Enablement Services Release 10.2.0.1 104
Required artifacts for Application Enablement Services Release 10.2 104
Software information for 10.2.x.x 105
Installation for Avaya Aura® Application Enablement Services Release 10.2.x.x 105
Installation for Avaya Aura® Application Enablement Services Release 10.2 105
Backing up the AE Services software 105
Interoperability and requirements 105
Installation for Avaya Aura® Application Enablement Services Release 10.2.x.x 106
Upgrading to AE Services 10.2.x.x 106
Upgrading to AE Services 10.2.1.4 106
Upgrading to AE Services 10.2.1.3 106
Upgrading to AE Services 10.2.1.2 106
Upgrading to AE Services 10.2.1.1 106

Upgrading to AE Services 10.2.1.0 106
Upgrading to AE Services 10.2.0.1 106
Upgrading to AE Services 10.2 106
AE Services Server Upgrade Instructions 107
RHEL 8.4 Support for AE Services 10.2 107
Installation for Avaya Aura® Application Enablement Services Software Only 10.2.x.x 107
Functionality not supported 107
Functionality not supported for Release 10.2.x.x 107
Changes and Issues 107
WebLM server compatibility 107
VM Foot Print Size and capacity 107
Fixes in Application Enablement Services in Release 10.2.x.x 108
Fixes in Application Enablement Services in Release 10.2.1.4 108
Fixes in Application Enablement Services in Release 10.2.1.3 108
Fixes in Application Enablement Services in Release 10.2.1.2 109
Fixes in Application Enablement Services in Release 10.2.1.1 109
Fixes in Application Enablement Services in Release 10.2.1.0 110
Fixes in Application Enablement Services in Release 10.2.0.1 110
Fixes in Application Enablement Services in Release 10.2 111
Known issues and workarounds in Application Enablement Services 10.2.x.x 112
Known issues and workarounds Application Enablement Services in Release 10.2.1.4 112
Known issues and workarounds Application Enablement Services in Release 10.2.1.3 112
Known issues and workarounds Application Enablement Services in Release 10.2.1.2 113
Known issues and workarounds Application Enablement Services in Release 10.2.1.1 113
Known issues and workarounds Application Enablement Services in Release 10.2.1.0 114
Known issues and workarounds Application Enablement Services in Release 10.2.0.1 114
Known issues and workarounds Application Enablement Services in Release 10.2 116
Avaya Solutions Platform 119
Avaya Solutions Platform S8300 119
Avaya Solutions Platform 130 119
Avaya Aura® G430 and G450 Media Gateways 120
What’s new in Avaya Aura® G430 and G450 Media Gateways Release 10.2.x.x 120
What’s new in G430 and G450 Media Gateways Release 10.2.1 (Builds 43.22.00 and 43.22.30) 120
What’s new in G430 and G450 Media Gateways Release 10.2 (Builds 43.09.00 and 43.09.30) 120
Installation for Avaya Aura® G430 and G450 Media Gateways Release 10.2.x.x 120
Required patches 120
Pre-Install Instructions 121
File Download Instructions 121
Backing up the software 121
Installing the release 121
Troubleshooting the installation 123
Restoring software to the previous version 123
Software Information 123
Fixes in G430 and G450 Media Gateways Release 10.2.x.x 123
Fixes in G430 and G450 Media Gateways Release 10.2.1.4 (Builds 43.30.00 and 43.30.30) 123
Fixes in G430 and G450 Media Gateways Release 10.2.1.3 (Builds 43.28.00 and 43.28.30) 124

Fixes in G430 and G450 Media Gateways Release 10.2.1.2 (Builds 43.26.00 and 43.26.30) 125
Fixes in G430 and G450 Media Gateways Release 10.2.1.1 (Builds 43.24.00 and 43.24.30) 126
Fixes in G430 and G450 Media Gateways Release 10.2.1.0 (Builds 43.22.00 and 43.22.30) 126
Fixes in G430 and G450 Media Gateways Release 10.2.0.1 (Builds 43.13.00 and 43.13.30) 126
Fixes in G430 and G450 Media Gateways Release 10.2 (Builds 43.09.00 and 43.09.30) 127
Known issues and workarounds in G430 and G450 Media Gateways Release 10.2.x.x 127
Known issues and workarounds in G430 and G450 Media Gateways Release 10.2 127
Languages supported 127
Documentation errata 127
Avaya Aura® Media Server 127
Avaya WebLM 128
Avaya Aura® Device Services 130
Required artifacts for Avaya Aura® Device Services Release 10.2.1.4 130
Installation for Avaya Aura® Device Services Release 10.2.1.4 130
Upgrading the Avaya Aura® Device Services software Release 10.2.1.4 130
Upgrade from 10.2.1.3.13 to 10.2.1.4.42 130
Software only deployment: Upgrade from 10.2.1.3.13 to 10.2.1.4.42 131
Additional supported upgrade paths 131
Fixes in Avaya Aura® Device Services 10.2.1.4 131
Required artifacts for Avaya Aura® Device Services Release 10.2.1.3 134
Installation for Avaya Aura® Device Services Release 10.2.1.3 134
Upgrading the Avaya Aura® Device Services software Release 10.2.1.3 134
Upgrade from 10.2.1.2.7 to 10.2.1.3.13 134
Software only deployment: Upgrade from 10.2.1.2.7 to 10.2.1.3.13 135
Additional supported upgrade paths 136
Fixes in Avaya Aura® Device Services 10.2.1.3 136
Required artifacts for Avaya Aura® Device Services Release 10.2.1.2 137
Installation for Avaya Aura® Device Services Release 10.2.1.2 137
Upgrading the Avaya Aura® Device Services software Release 10.2.1.2 137
Upgrade from 10.2.1.1.22 to 10.2.1.2.7 137
Software only deployment: Upgrade from 10.2.1.1.2 to 10.2.1.2.7 138
Additional supported upgrade paths 138
Fixes in Avaya Aura® Device Services 10.2.1.2 139
What’s new in Avaya Aura® Device Services Release 10.2.1.1 139
Required artifacts for Avaya Aura® Device Services Release 10.2.1.1 139
Installation for Avaya Aura® Device Services Release 10.2.x.x 140
Upgrading the Avaya Aura® Device Services software Release 10.2.1.1 140
Upgrade from 10.2.1.0.41 to 10.2.1.1.22 140
Software only deployment: Upgrade from 10.2.1.0.41 to 10.2.1.1.22 141
Additional supported upgrade paths 141
Fixes in Avaya Aura® Device Services 10.2.1.1 141
What’s new in Avaya Aura® Device Services Release 10.2.1.0 142
Security Service Pack 142
Security Service Pack 142
Required artifacts for Avaya Aura® Device Services Release 10.2.1.0 142
Software information 142
Installation for Avaya Aura® Device Services Release 10.2.x.x 143
Upgrading the Avaya Aura® Device Services software Release 10.2.1.0 143

Upgrade from 10.2.0.1.16 to 10.2.1.0.41 143
Software only deployment: Upgrade from 10.2.0.1.16 to 10.2.1.0.41 144
Fixes in Avaya Aura® Device Services 10.2.1.0 145
Known issues and workarounds in Avaya Aura® Device Services in Release 10.2.1.0 145

Change history

Issue	Date	Description
1	18-Dec-2023	GA Release of Avaya Aura® Release 10.2
2	15-Apr-2024	GA Release of Avaya Aura® Release 10.2.0.1
3	24-Apr-2024	Updates to availability of Software-only deployment based on Avaya Aura® BU approval
4	7-May-2024	Updates to required artifacts for AES 10.2.0.1 service pack installer
5	23-May-2024	Updates to Presence Services Release 10.1.0.1
6	4-Jul-2024	Updates to required artifacts for Communication Manager Release 10.2.0.1
7	28-Oct-2024	Update to support ASP R6.0
8	9- Dec-2024	GA Release of Avaya Aura® Release 10.2.1
9	14-Apr-2025	GA Release of Avaya Aura® Release 10.2.1.1
10	28-May-2025	Added note in CM what's new section and required artifacts section, Updated required artifacts with new CM build details and updated SM 10.2.1.1 known issues list.
11	11-Aug-2025	GA Release of Avaya Aura® Release 10.2.1.2
12	13-Aug-2025	Updates to System Manager, Session Manager 10.2.1.2, Presence Services Release 10.1.0.1 and Product Release Matrix to include WebLM Release.
13	31-Oct-2025	Updates to Presence Services Release 10.1.0.2 and Product Release Matrix
14	22-Dec-2025	● GA Release of Avaya Aura® Release 10.2.1.3 ● Updated required artifacts and support for Avaya Solution Platform 130 R660 (KVM on RHEL 8.10) to Avaya Aura® Presence Services 10.1.0.2
15	06-Jan-2026	Updated required artifacts and support for Avaya Solution Platform 130 R640 (KVM on RHEL 8.10) to Avaya Aura® Presence Services 10.1.0.2
16	08-Jun-2026	GA Release of Avaya Aura® Release 10.2.1.4
17	02-July-2026	Added note in AES What's New Section, related to JTAPI and TSAPI programmer's guides.

Introduction

This document provides late-breaking information to supplement Avaya Aura® 10.2.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.

IMPORTANT

Communication Manager (CM) Licensing Change

Communication Manager (CM) 10.2.1.1 is changing its licensing behavior to keep customers informed about license expiration dates so they can renew licenses on time and avoid service disruption. CM is introducing two new alarms that warns customers about license expiration date and its impact:

1. LIC-EXP90: This alarm is raised 90 days before the expiration of CM license
2. LIC-EXP60: This alarm is raised 60 days before the expiration of CM License

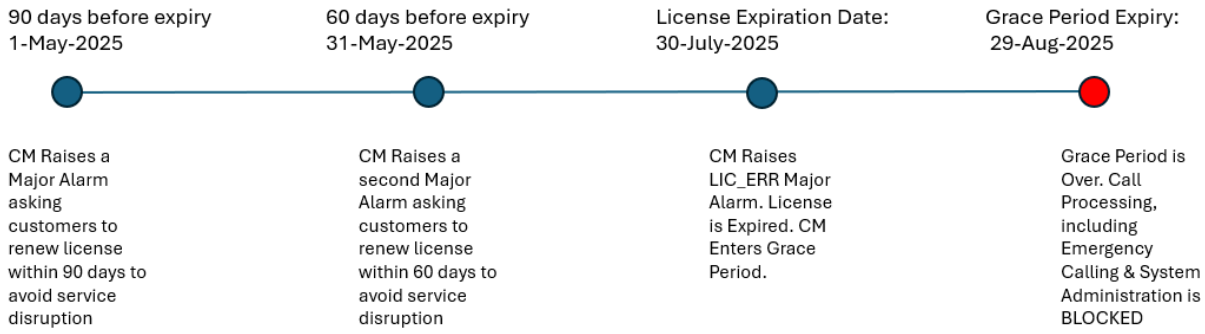
CM enters into a 30-day Grace Period on expiration of License. After 30-day grace period expiry, if license is not renewed:

- **Call Processing, including Emergency calling, will be BLOCKED**. That is, CM will NOT process any type of calls.
- System Administration will be BLOCKED.

Customers must renew their licenses on time to avoid this disruption.

Example:

Notes:



1. CM will check the Expiration Date for all the features in the License file and use the earliest date as expiration date. For example: If Elite License is expiring on 30-July while CM license is expiring on 30-August, CM will consider 30-July as License Expiration Date
2. This Licensing change behavior is only applicable for CM Main Server. This does not apply to Survivable Remote (LSP) or Survivable Core (ESS) Servers.
3. This Licensing Change is only applicable for Communication Manager and not for any other Aura Product

Note:

- The Avaya Solutions Platform R6.0.x will be supporting KVM on RHEL 8.10 as a Hypervisor and all Avaya Aura components released new KVM OVA to support ASP R6.0.x. All patches of R10.2 such as Service Pack, Feature Pack, Hot Fix, and Security Service Pack are applicable to VMs on ASP R6.0.x KVM hosts.
- The December 23 updated Aura 10.2 KVM OVAs now support the following:
  - The KVM OVAs include an *install_vm.py* script to simplify deployment of the KVM OVA
  - The *install_vm.py* script now supports the creation of a root login/password
  - The CM and AES updated 10.2 KVM OVAs also include support for disk encryption.
- For information about Avaya Solutions Platform S8300, see ASP S8300 (PCN2174S) and ASP 130 6.0.x (PCN2173S)

~~**Root Password:** Deploying applications on ASP R6.0.x KVM hypervisor using script, it is possible to set the root password. Which was in the SDM capability brought to ASP R6.0.x users if they deploy using the script documented on each deployment guide.~~

- 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).
- The Avaya Solutions Platform S8300 (ASP S8300) Release 5.1 is available for the Avaya Aura® 10.2 Communication Manager solutions that include LSPs/Survivable Remote Servers/BSM's that run on S8300Es and also for the Communication Manager solutions with embedded main profiles on S8300E's.

  Solutions with an existing S8300E or new deployments that require ASP S8300 Release 5.1 can begin their upgrade or new deployments by following the required order of upgrade.

  For information about deploying or upgrading Communication Manager 10.2.x and BSM 10.2.x upgrade/deployment steps on the ASP S8300 Release 5.1, see the product documentation.

  There is compatibility between Aura 10.2 and 8.1.x components as long as the required order of upgrade is followed. Reference the Upgrading Avaya Aura® Communication Manager Release 10.2, Chapter 3: Planning, Section: Upgrade sequence for Avaya components.

  For information about Avaya Solutions Platform S8300, see ASP S8300 (PCN2145SU) and ASP 130 5.1.x (PCN2146SU)
- Avaya Aura® Release 10.2 is supported on Avaya Solutions Platform (ASP) S8300 Release 5.1 and ASP 130 Release 5.1.

  Avaya Aura® Release 8.1.3.x is supported on ASP 130 Release 5.0 and Release 5.1.

  However, after migrating from Avaya Aura® Appliance Virtualization Platform (AVP) Release 8.1.x on an S8300E to ASP S8300 Release 5.1, Avaya Aura® Release 8.1.x applications are still running on ASP S8300 Release 5.1.

  Prolonged running in this type of mixed configuration is not supported. Avaya recommends running in a mixed configuration only as long as necessary to support application upgrades. If an issue is identified on an Avaya Aura® 8.1.x application running on ASP S8300 Release 5.1, Avaya will require an upgrade of the Avaya Aura® solution to Release 10.2.

  All future ASP 5.x security updates will only be provided on the latest ASP 5.x release currently available. For example, if ASP Release 5.1 is the most recent available release, security updates will only be provided on Release 5.1. They will not be provided on Release 5.0.

Documentation Catalog

The Documentation Catalog document lists down the various guides that are available for the Avaya Aura® solution. For details see: https://download.avaya.com/css/public/documents/101087511

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	10.2.1.4	10.2.1.3	10.2.1.2	10.2.1.1	10.2.1	10.2.0.1	10.2
Avaya Aura® Communication Manager	X	X	X	X	X	X	X
Avaya Aura® Session Manager	X	X	X	X	X	X	X
Avaya Aura® System Manager	X	X	X	X	X	X	X
Avaya Aura® Presence Services	10.1.0.1.40 10.1.0.2	10.1.0.1.40 10.1.0.2	10.1.0.1.401 0.1.0.2	10.1.0.1.30 10.1.0.2	10.1.0.1.30 10.1.0.2	10.1.0.1.301 0.1.0.2	10.1.0.1.30 10.1.0.2
Avaya Aura® Application Enablement Services	X	X	X	X	X	X	X
Avaya Aura® G430 and G450 Media Gateways	X	X	X	X	X	X	X
Avaya WebLM Release	10.1.3.7	10.1.3.7	10.1.3.6	10.1.3.5	10.1.3.4	10.1.3.2	10.1.3.1
Avaya Aura® Media Server Release	10.2	10.2	10.2	10.2	10.2	10.1 SP6	10.1 SP5
Avaya Aura® Device Services	X	X	X	X	X	X	X

Note:

- Security Service Packs (SSPs) will be released at or around the same time as the Feature Pack and / or Service Pack and sometimes on a more frequent cadence.
    - SSP required artifacts are tracked in the application specific Security Service Pack PCN. Please read the PCN for the appropriate SSP. The files integrate and are installed uniquely per application.
    - Please note that 10.1 SSPs won't work on Release 10.2 and there will be different SSPs for both 10.1 and 10.2.
- Customers may use AADS 10.2.x with the Avaya Aura® 10.2.x release line up.
- Avaya Aura® Media Server Release 10.1.x.x is compatible with Avaya Aura® Release 10.2.x. Media Server Releases have a different release version and schedule. For more information, see Avaya Aura® Media Server Release Note 10.1.x.x at the Avaya Support website.
- Avaya Aura® Presence Services 10.1.0.1.x with Avaya Breeze ® platform 3.9.0.0 is compatible with Avaya Aura® Release 10.2.x. Avaya Aura Presence Services Releases have a different release version and schedule.
- Avaya Aura® Presence Services 10.1.0.2.x with Avaya Breeze ® platform 3.9.0.3 is compatible with Avaya Aura® Release 10.2.x. Avaya Aura Presence Services Releases have a different release version and schedule.
- Avaya WebLM 10.1.3.1 and higher releases are compatible with Avaya Aura® Release 10.2.x. Avaya WebLM Releases have a different release version and schedule. For more information, see the Avaya WebLM documentation for Release 10.1.x at the Avaya Support website.
- 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).
- The deployment of Avaya Aura® applications as Software-only is available but a restricted offer for net new deployments and requires Avaya Aura® BU approval before proceeding. If you have a business requirement to deploy Avaya Aura® as Software-only, please get in touch with your Avaya Sales team. Existing customers using software only deployments continue to be supported.
- In Release 10.2, Communication Manager, System Manager, Session Manager, Application Enablement Services and G4xx are JITC compliant and currently certified solution on the DoDIN APL.

- In Release 10.1.0.2, Communication Manager, System Manager, Session Manager, G430 and G450 are JITC compliant and are the currently certified solution on the DoDIN APL

  As per the latest DISA STIG requirements, RHEL version 8.4 is also tested for JITC certification.

What’s new in Avaya Aura®

For more information, see ***What’s New in Avaya Aura® Release 10.2.1*** document on the Avaya Support site. https://download.avaya.com/css/public/documents/101087359

Discontinued support for IP Server Interface (TN2312, commonly known as “IPSI”)

With Release 10.2, Communication Manager does not support the IP Server Interface (IPSI). As a result, access and functionality are removed. This means, the IPSI connected cabinets and gateways do not work with Communication Manager Release 10.2. Examples of IPSI connected cabinets and systems include G3cfs, G3csi, G3i, G3r, G3s, G3si, G3vs, G3x, G600, G650, MCC, SCC, CMC, IPSI, IP Server Interface, and IP port network.

Discontinued support also includes the TN8412, which previously paired with the TN8400 blade server. TN8412 was last supported with Communication Manager Release 5.x.

For more information, see the End of sale G650 document published on the Avaya Support website.

Future use fields visible in Avaya Aura® Release 10.2

The underlying framework for an upcoming new Avaya Aura® Platform enhancement “Avaya Aura Distributed Architecture” will be seen in some Release 10.2 administration screens and deployment options. This applies to Communication Manager, System Manager, and Session Manager. These fields are for future use only. Reference the Communication Manager, System Manager, and Session Manager “What’s New” sections in this document for details on the new fields and deployment options that will be visible in 10.2, but not currently recommended for use.

Security Service Packs

Several of the Avaya Aura® applications are now publishing Security Service Packs (SSP) aligned with their application release cycle. This SSP will include all available, and applicable, updates for Red Hat Security Advisories (RHSA) published prior to the time of the building of the related software release. This SSP will be available for download via PLDS per normal procedures. The details of the SSP are published in a PCN specific to each product. Please refer to the product specific installation sections of this document for further details regarding SSPs being published for 10.2.x.

Beginning with the December 10.2 SSPs, the SSPs will be applicable for both RHEL 8.4 and RHEL 8.10. The common Security Service Pack will be introduced to support both RHEL 8.4 and RHEL 8.10.

Compatibility

For the latest and most accurate compatibility information, go to the **TOOLS** > **Product Compatibility Matrix** on the Avaya Support website.

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 website https://support.avaya.com.
5. Contact Avaya Technical Support for your Country/Region at one of the telephone numbers on the **Help** > **Contact Avaya Support** at the Avaya Support website.

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 website.

Contact support tasks

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

Avaya Aura® Communication Manager

What's new in Communication Manager Release 10.2.x.x

Note: Updated Communication Manager 10.2.x Feature Pack and Services packs to address an issue where certain security vendors are flagging the download of these artifacts. These scanners are reporting a FALSE positive yet can result in download of the artifacts failing or being blocked from use once downloaded.

Avaya has rebuilt the impacted artifacts to eliminate this issue. Please reference *PSN020650u - Avaya Aura® Communication Manager 10.2.x -Temporary removal of software* for additional details.

What's new in Communication Manager Release 10.2.1.1.0

For more information, see ***What's New in Avaya Aura® Release 10.2.x*** document on the Avaya Support site: https://download.avaya.com/css/public/documents/101087359

- Administrable grace period for Enterprise Survival Server (ESS)
  A new field "***Survivable License Grace Period (in days)***" in survivable-processor form. Which will be used when the ESS becomes active.
- Licensing Changes
  Introduction of 90-day (about 3 months) and 60-day (about 2 months) validation License alarms and once the grace period is over the call processing and admin will be blocked.
- VMware ESXi 8.0.3 U3 platform support.

What's new in Communication Manager Release 10.2.1.0.0

The December 23 updated Aura 10.2 KVM OVAs now support the following:

- The KVM OVAs include an *install_vm.py* script to simplify deployment of the KVM OVA
- The *install_vm.py* script now supports the creation of a root login/password
- The CM and AES updated 10.2 KVM OVAs also include support for disk encryption using the script deployment.

For more information, see ***What's New in Avaya Aura® Release 10.2.x*** document on the Avaya Support site: https://download.avaya.com/css/public/documents/101087359

What's new in Communication Manager Release 10.2.0.1.0

What's new in Communication Manager Release 10.2

Enhancement	Description
CM-53558	Communication Manager 10.1.3.1.0 and later supports active enhanced call pickup notification when IOS workplace client registers.

For more information, see ***What's New in Avaya Aura® Release 10.2.x*** document on the Avaya Support site: https://download.avaya.com/css/public/documents/101087359

Future use fields visible in Avaya Aura® Communication Manager Release 10.2.x.x

Future use fields visible in Avaya Aura® Communication Manager Release 10.2

The underlying framework for an upcoming Avaya Aura® Platform enhancement “Avaya Aura Distributed Architecture” will be seen in some Release 10.2.x and later administration screens and deployment options. This is applicable to Communication Manager, System Manager, and Session Manager. These fields are for future use only. Reference the Communication Manager, System Manager and Session Manager “What’s New” sections in this document for details on the new fields and deployment options that will be visible in 10.2, but not active/usable.

1. Avaya Aura® Communication Manager Release 10.2.x and later OVA will have the following deployment options visible but are for future use.
Caution: Selection of any of these options during deployment will result in a warning stating that moving forward will result in an unsupported configuration and require a reinstall with a supported profile.

1. CM Standard Duplex Array Max Users 300000
2. CM High Duplex Array Max Users 300000
3. CM Array Max users 300000

Avaya Aura® Communication Manager Release 10.2.x and later SMI page will have the following options but are for future use:

1. Administration -> Licensing -> Feature Administration -> Current Settings -> Display -> Optional Features -> Clustering
2. Administration -> Server Administration -> Server Role -> Configure Memory (for LSP) -> This Server’s Memory Setting -> X-Large/Cluster

Security Service Pack

Security Service Pack

For further information on SSP contents and installation procedures for CM 10.2.x, please see **PCN2159S**.

CM 10.2.x will have RedHat Enterprise Linux (RHEL 8.4) to its Avaya Aura platform. Common versions of RPMs are supported and consumed by the components. This results in a change to how security updates are provided for Communication Manager and Application Enablement Services.

Beginning with the December 2024 10.2.x SSPs, the SSPs will be applicable for both RHEL 8.4 and RHEL 8.10. The common Security Service Pack will be introduced to support both RHEL 8.4 and RHEL 8.10.

SSPs cannot be installed on “software-only” deployments.

Required artifacts for Avaya Aura® Communication Manager 10.2.x.x

Note: Updated Communication Manager 10.2.x Feature Pack and Services packs to address an issue where certain security vendors are flagging the download of these artifacts. These scanners are reporting a FALSE positive yet can result in download of the artifacts failing or being blocked from use once downloaded.

Avaya has rebuilt the impacted artifacts to eliminate this issue. Please reference *PSN020650u - Avaya Aura® Communication Manager 10.2.x -Temporary removal of software* for additional details.

Required artifacts for Communication Manager Release 10.2.1.4.0

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

Filename	PLDS ID	File size	Version number	Comments
02.0.229.0-28475.tar	CM000002246	155MB	10.2.1.4.0	10.2.1 Service Pack #04,

Filename	PLDS ID	File size	Version number	Comments
				released on 8th Jun 2026

Required artifacts for Communication Manager Release 10.2.1.3.0

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

Filename	PLDS ID	File size	Version number	Comments
02.0.229.0-28425.tar	CM000002235	154MB	10.2.1.3.0	10.2.1 Service Pack #03, released on 22nd Dec 2025

Required artifacts for Communication Manager Release 10.2.1.2.0

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

Filename	PLDS ID	File size	Version number	Comments
02.0.229.0-28367.tar	CM000002231	150MB	10.2.1.2.0	10.2.1 Service Pack #02, released on 11th Aug 2025

Required artifacts for Communication Manager Release 10.2.1.1.0

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

Filename	PLDS ID	File size	Version number	Comments
02.0.229.0-28339.tar	CM000002226	150MB	10.2.1.1.2	10.2.1 Service Pack #01, released on 27th May 2025
~~02.0.229.0-28314.tar~~	~~CM000002221~~	~~153MB~~	~~10.2.1.1.0~~	~~10.2.1 Service pack #01 release on 14th April 2025.~~

Required artifacts for Communication Manager Release 10.2.1.0.0

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

Filename	PLDS ID	File size	Version number	Comments
02.0.229.0-28335.tar	CM000002225	150MB	10.2.1.0.1	10.2.1 Feature Pack, released on 27th May 2025
~~02.0.229.0-28240.tar~~	~~CM000002213~~	~~153MB~~	~~10.2.1.0.0~~	~~10.2.1 Feature Pack~~
AV-CM10.2-RHEL8.10-OSUpdate-003.tar.bz2	CM000002214	830MB	RHEL 8.10	RHEL 8.10 OS Bundle for
~~CMKVM-Simplex-010.2.0.0.229-e70-0.ova~~	~~CM000002211~~	~~4631MB~~	~~10.2.0.0.229~~	~~CM Simplex KVM OVA~~
~~CMKVM-Duplex-010.2.0.0.229-e70-0.ova~~	~~CM000002212~~	~~4631MB~~	~~10.2.0.0.229~~	~~CM Duplex KVM OVA~~
CM-Simplex-010.2.0.0.229-KVM-1.ova	CM000002217	4631MB	10.2.0.0.229	CM Simplex KVM OVA
CM-Duplex-010.2.0.0.229-KVM-1.ova	CM000002216	4631MB	10.2.0.0.229	CM Duplex KVM OVA

Note: New KVM OVAs has the capability of CM disk encryption using the script, the procedure is documented in the deployment guide.

Required artifacts for Communication Manager Release 10.2.0.1.0

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

Filename	PLDS ID	File size	Version number	Comments
02.0.229.0-28333.tar	CM000002224	124MB	10.2.0.1.2	10.2 Service pack #01 released on 27th May 2025.
~~02.0.229.0-28070.tar~~	~~CM000002205~~	~~125MB~~	~~10.2.0.1.0~~	~~10.2 Service pack #01~~
~~02.0.229.0-28126.tar~~	~~CM000002207~~	~~126MB~~	~~10.2.0.1.1~~	~~10.2 Service pack #01 released on 21st June 2024.~~

Note: Replacing 10.2.0.1.0 with 10.2.0.1.1 to address an issue where infinite re-invites are seen on SIP Trunk calls. Depending on the specific customer configuration, these infinite re-invites can result in audio issues, including one-way audio. PLDS ID CM000002205 will be obsolete. The new 10.2.0.1.1 is updated to support, for more information, see PCN2158S and PSN020637u.

Required artifacts for Communication Manager Release 10.2

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

Filename	PLDS ID	File size	Version number	Comments
CM-Simplex-010.2.0.0.229-e70-0.ova	CM000002200	2.39G	10.2.0.0.229	CM Simplex OVA

Filename	PLDS ID	File size	Version number	Comments
CM-Duplex-010.2.0.0.229-e70-0.ova	CM000002201	2.39G	10.2.0.0.229	CM Duplex OVA
CM-010.2.0.0.229-e70-0.iso	CM000002202	138M	10.2.0.0.229	CM SW Only ISO

Note: The deployment of Avaya Aura® applications as Software-only is available but a restricted offer for net new deployments and requires Avaya Aura® BU approval before proceeding. If you have a business requirement to deploy Avaya Aura® as Software-only, please get in touch with your Avaya Sales team. Existing customers using software only deployments continue to be supported.

Software information

Software	Version	Note
OS	Red Hat Linux Release 8.4 (Ootpa) Red Hat Linux Release 8.10	RHEL8.10 separate Bundle provided to upgrade the OS
Apache	2.4.37	
SSH	OpenSSH_8.0p1	
Supported Browsers	Chrome (minimum version 91.0) Edge (minimum version 93.0) Firefox (minimum version 93.0)	
VMware vCenter Server, ESXi Host	7.0.X, 8.0, 8.0 Update 2.	Avaya Aura® Release 10.2.x supports VMware 8.0 and VMware 8.0 Update 2. Avaya Aura® Release 10.2.x does not support VMware 8.0 Update 1. For information about known issues, see VMware 8.0 Update 1 Release Notes on the VMware website at https://docs.vmware.com/en/VMware-vSphere/index.htmlhttps://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-6vcenter-server-801-release-notes/index.html.
ASP R6.0 ASP R5.1	RHEL8.10	Avaya Aura Release 10.2.x supports ASP R6.0 KVM on RHEL8.10 and ASP R5.1x VMware ESxi.

Installation for Avaya Aura® Communication Manager 10.2.x.x

Installation for Avaya Aura® Communication Manager Release 10.2.1.4.0

Installation for Avaya Aura® Communication Manager Release 10.2.1.3.0

Installation for Avaya Aura® Communication Manager Release 10.2.1.2.0

Installation for Avaya Aura® Communication Manager Release 10.2.1.1.0

Installation for Avaya Aura® Communication Manager Release 10.2.1.0.0

RHEL 8.10 Upgrade using the command av-upgrade-os command available after the 10.2.1 Feature Pack deployment. Need to make sure that before upgrading RHEL8.10 on OVA based CM VMs should be on 10.2.1 Feature Pack.

Installation for Avaya Aura® Communication Manager Release 10.2.0.1.0

Installation for Avaya Aura® Communication Manager Release 10.2

For information on the installation of Release 10.2, see **Deploying Avaya Aura® Communication Manager in Virtualized Environment**.

For information on upgrading to Release 10.2, see **Upgrading Avaya Aura® Communication Manager**.

Communication Manager 10.2 software includes certain third-party components, including Open-Source Software. Open-Source Software licenses are included in the Avaya Aura® 10.2.

Communication Manager Solution Templates DVD. To view the licenses:

1. Insert the Avaya Aura® 10.2 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.

Note:

A Manual upgrade is a full backup and restore using the SMI pages. This process is supported on all deployment options. Best Practice prior to an upgrade is to copy the IP address and Naming information, your certificates, your logins, scheduled backup, syslog settings and SNMP configuration. You need to be prepared to install these manually after the restore.

The full automated upgrade using SDM can be used when migrating from a CM 8.1.3.8.0/10.1.3.x to 10.2 in a customer provided VMware environment.

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 website.

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 website 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.

Fixes in Communication Manager Release 10.2.x.x

Fixes in Communication Manager Release 10.2.1.4.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
CM-61833	Wrongly formatted SDP in SIP message	CM Interchange	10.2.0.0.0
CM-61825	Announcement played on incoming trunk call	Spurious proc errors logged	10.2.0.0.0
CM-61822	ISDN trunk incoming call to agent and Service Observer with Listen-Only mode	Service Observer can hear and speak with both caller and callee	10.2.1.3.0
CM-61805	DECT phone having bridge-aapr for MDA SIP device	when Multiple devices are registered with same extension and it has bridge-appr on DECT phone then the calling number display is with a + sign prepended	10.2.1.3.0
CM-61796	Blind transfer to another CM over SIP trunk.	When B blind transfers A call to C over trunk, then C gets the calling name/number of B instead of A.	10.2.1.1.2
CM-61784	AMS announcements and European Tone plan that uses Conference Tone Conference Tone enabled on system-parameters features	Delayed announcement start in combination with Conference Tone	10.2.0.0.0
CM-61775	Meet-me-conf and endpoints are configured on different CMs	Number of parties in meet-me-conference call is not updated on endpoints correctly	10.1.3.6.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
CM-61765	Endpoint missing 3PAD INVITE after sending “202 ACCEPTED” for 3PAD REFER and manual dial afterwards.	NULL deviceID in Service Initiated ASAI event to CTI side.	10.1.3.6.0
CM-61762	SIP stations with mixed MCA and non-MCA brdg-appr buttons.	Non-MCA brdg-appr buttons don't alert if MCA and non-MCA both types of brdg-appr are configured on SIP phones	10.2.1.3.0
CM-61754	Call scenario involving call park, unpark, park timeout, coverage, transfer.	Null DeviceID in Hold ASAI event to CTI application.	10.1.3.6.0
CM-61728	XMOBILE Station and Configure emergence extension number other than station extension	When calling to emergency number (911), from XMOBILE station, calling number is not getting updated as per Emergency Location Extension number configured on station form. Calling number is same as the station number.	10.2.1.0.0
CM-61723	Multi-button stations using brdg-appr buttons	Problems with calls originated on bridged-appearance buttons of multi-button stations. Including dropped calls using SIP Direct Media , display issues, and CTI data errors.	10.2.0.0.0
CM-61722	ASAI monitored station and call traversed multiple VDN’s.	Agent station number is passed in ASAI alerting event instead of the VDN.1	10.2.1.0.0
CM-59359	SIP stations configured.	SIP trunk shows blank in change station form	10.2.1.0.0
CM-59310	Remove a cabinet with active circuit packs.	Cabinet is removed while still having translations data filled actively in the CM	10.2.1.2.0
CM-59309	disable announcement-board xxxxx is executed from SAT	announcement-board is not disabled	10.2.0.0.0
CM-59303	Call going through multiple hops VDNs,Vector, coverage etc.	CM-CMS link flap	10.2.1.1.2
CM-59084	Call scenario involving blind transfer on BCA configured stations	Incorrect calling number/name is displayed after transfer	10.2.1.2.1
CM-58494	Site data configured with more than 250 buildings	cannot delete unused buildings if more than 250 buildings are configured in CM.	10.2.0.1.0

Fixes in Communication Manager Release 10.2.1.3.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
CM-59344	Agent makes outbound call while in AUX mode	Wrong AUX reason code sent to CMS	10.1.3.6.0
CM-59339	CM Installed	Addition of debugs for service hours issue	10.2.0.0.0
CM-59331	Network disruption on ASAI monitored station call while on hold and	When phone reconnects after network reconnection, call recording does not resume after call is un-held	10.2.0.1.1

ID	Minimum conditions	Visible symptoms	Issue found in Release
CM-59329	External Pairing is enabled	CM may send spurious agent status updates via CTI links for monitored stations	10.2.1.2.0
CM-59311	EAD-LOA skill with more than 1500 agents	Agent login fails to EAD-LOA skill after 1500 logged-in agents is reached	10.2.1.2.0
CM-59306	ISDN trunk incoming call to agent and Service Observer with Listen-Only mode	Service Observer can hear and speak with both caller and callee	10.1.3.6.0
CM-59300	Station-1 and Station-2 are externally measured. Station-1 is busy on call and Station-2 calls Station-1	For the failed call, CMS SPI showed wrong ITN for “FDISC24” SPI message.	10.2.1.2.1
CM-59252	External Pairing is enabled and caller disconnects the call while waiting in queue	call is not de-queued and still shows in queue	10.2.1.2.1
CM-59251	admin operations (starfish bulk operations)	Occasionally, SAT may terminate abruptly	10.2.1.0.0
CM-59248	CM, SIP station/H323 station/X-ported station	Bridge-appr originated calls may fail	10.2.1.2.1
CM-59244	SIP station with off-pbx-station mapping application type should be ops	Application type may not be correct and record corruption	10.2.1.0.0
CM-59243	SIP stations with team button for analog station	Team button pickup fails on SIP stations if call is placed to analog stations	10.2.1.2.0
CM-59223	Browse fileserv_* log files	fileserv_* log files cannot be seen	10.2.1.0.0
CM-59192	Agent data structure changes while the agents are logged-in and execute save trans	Agent data structure translation corruption	10.2.1.2.0
CM-59143	SIP Invite with **SDP media line m=text**	Call failure	10.2.0.1.1
CM-59108	Make a private call using auth code call from a SIP station A to B. (AAR/ARS access code + auth code + called party extension	Pin check condition code “P” is not visible in the CDR records.	10.2.1.0.0
CM-58740	External number calling CM extension and another extension picking up the call pressing team button.	Workplace shows wrong display at the user picking up the call via team button press.	10.1.3.7.0
CM-58559	SIP station with Language German installed. xmobile station on CM which has bridge appr for called station and mapping mode for xmobile station is both OR termination.	CM will send UPDATE messages to SIP STN-, but number in PAI/Contact header is missing	10.2.0.1.0
CM-58119	SRTP call on G450	2-way conversation audio failure in connection topologies involving G4x0 Media Gateways under rare conditions when one party changes the SRTP key mid-call	8.1.3.8.0

Fixes in Communication Manager Release 10.2.1.2.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
CM-59092	Deletion of an agent followed by a save_trans from the SAT	Save_trans may fail.	10.2.1.0.0
CM-59086	Trunk-Station Call transferred to another station. For 1st call origination station sends Off-hook INVITE to CM. For the 2nd call to transferred-to party, station doesn't send Off-hook INVITE to CM	Long hour Call due to missing ASAI events like "Single-Step-Conference", "Call Transfer".	10.1.3.4.0
CM-59014	CM enters License grace period	License Grace period is expiring earlier than 30 days.	10.1.3.6.0
CM-58975	Japanese enabled SIP Sta-A on CM-A calling Japanese enabled SIP Sta-B on CM-B. The "Display Language" is set to "Unicode". And "Unicode Name" set to "Auto" on SIP trunk between two CMs	Unexpected call drop before or after call answer between two Unicode enabled SIP stations on two CMs.	10.1.3.6.0
CM-58960	Any multi-function station with MCA bridged-appearance buttons on extended button modules.	MCA bridged-appearance buttons on multi-function sets may fail to function if the button is added to an extended button module.	8.1.3.8.0
CM-58927	Incoming call to DECT station and team pickup SIP station member answer the call	Team Pickup from SIP Station would fail	10.2.1.1.0
CM-58812	Trunk call to agent station (ASAI monitored) and the call is transferred multiple times	CTI application may not see ASAI "Connected" event	10.1.3.1.0
CM-58810	Incoming INVITE with replaces with "SessionExpires" value less than 3600.	The 200 OK for the INVITE goes with "Session-Expires" value of 3600 and other end may disconnect the call.	10.1.0.2.0
CM-58738	Audix button configured to start the recording	When customer presses Audix button again to stop the recording, the recording does not stop and continue till the call is ended	10.1.3.4.1
CM-58699	SIP stations with Unicode name, call involving transfer or inter-CM scenarios	Enhanced pickup alert is displayed before delay timer expired	10.1.0.0.0
CM-58689	Main CMS with survivable servers Add a avcommonos user on main CM	avcommonos users were not sync from main to survivable	10.2.1.0.0
CM-58651	CM is Unicode enabled with Arabic name. Arabic SIP station call routing to coverage group.	Customer saw English name instead of Arabic name on SIP station caller with Arabic language when call was covered to another Arabic SIP station.	10.2.1.0.0
CM-58621	SIP STN A1 is on CM1 SIP B1 and B2 are on CM2 CM1 and CM2 are connected through SIP trunk and "Mark Users as Phone?" is enabled on trunk	"user=phone" parameter missing in the Request URI and To header causing failed/misrouted emergency calls.	10.1.3.4.1

ID	Minimum conditions	Visible symptoms	Issue found in Release
	form. A1 calls B1. B1 answers the call A1 transfers call to B2		
CM-58405	CMS measured skill for agent have “Multiple Call Handling:” have value “on-request“. Agent-station going transition as below. Available ---> Aux (entering reason code) ----> Available ---- > Make outgoing call.	CMS saw wrong reason code in AUX24 SIP message when CMS measured agent-station made an outgoing call.	10.1.3.4.0
CM-58404	station transferring a SIP trunk call to another station which doesn’t answer and the call gets redirected to another SIP trunk	Long call recording due to missing disconnect ASAI even on such calls.	10.2.0.1.1
CM-58381	Primary and secondary DNS configured. Primary DNS is unreachable/unresponsive	SSH sessions from AES using SMS API may get timed out.	10.1.3.3.0
CM-58362	execute arping from any other linux box to eth0 interface.	If customers use arping to see if CM is reachable, it was giving incorrect MAC address associated with eth0, as a result customer's tool/firewall blocking the network traffic towards CM.	10.1.0.0.0
CM-58279	On same CM SIP station Sta-A calls SIP station Sta-B having EC500 configured other CM.	For internal station call, the EC500 leg of called party saw “Calling Number” as per config put in “Public Unknown Numbering” Plan	10.1.3.4.1
CM-58120	analog phone on G4x0 gateway	CM station button type 'signal' sends a ringing signal to analog phones on G4x0 gateways that has 200ms duration. This is too short for some external applications.	10.1.3.3.0
CM-21897	SIP agent to be configured in CM	Proc errors when SIP agent logs out	8.0.0.0.0

Fixes in Communication Manager Release 10.2.1.1.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
CM-58656	CM License expires and the system is in Grace period.	License server process crash and fails to start	10.1.0.0.0
CM-58542	Calls on an ISDN trunk	Frequent Proc error 7176/10200 logged in log file.	10.1.3.3.0
CM-58426	analog CO trunks or digital (non-ISDN/SIP) trunks.	incoming analog or digital (non-ISDN/SIP) trunk call that route to internal stations display the trunk group name instead of the Trunk Access Code.	10.1.3.2.0
CM-58378	ACD calls in queue from the PSTN. CM offers queued calls to SIP agents with Invite that gets a “305 User Proxy” response.	The call is offered to the same agent repeatedly until ROOF limits are hit and the PSTN call is dropped with a BYE from CM.	10.1.0.1.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
CM-58335	Configure 9640 station and configure 11th button e.g. autodial change the station type from 9640 to 9408	button number 11 gets wiped out.	10.1.3.3.0
CM-58278	H.323 Trunk between 2 CM's SIP station on CM1 makes call to SIP station on CM2 over H.323 Trunk	Calls between 2 CM's over H.323 Trunk fails.	10.2.0.1.0
CM-58247	Avaya Media Server Multiple DMCC recording ports attached to SIP agents via shared-control registration	memory leak builds up over an extended period and may lead to server interchange.	10.1.0.0.0
CM-58238	A SIP station call to SIP principal station with bridges behind SBC and one bridge answering the call.	Spurious re-Invites lead to call failures.	10.1.3.4.0
CM-58214	At least one terminating-extension-group configured, and station button "send-term" configured for same terminating-extension-group group	The "send-term" button can activate send-all-calls for a terminating-extension-group but cannot deactivate send-all-calls for the same group.	10.1.0.1.0
CM-58210	CM 10.2.1.0.0 running in standalone mode, and CTI application places monitor on VDN, Hunt Groups, Trunk Groups.	VDNs, Hunt Groups and Trunk Groups notifications are not sent to CTI applications	10.2.1.0.0
CM-58202	SIP trunk with Public network Incoming SIP message with body having multiple Content-Length headers	SIP Call failures for such scenarios.	10.1.2.0.0
CM-58165	Main CM with Survivable servers Execute Save Translations on Main server	on Survivable server, data inside existing user's home directories gets deleted.	10.1.3.2.0
CM-58153	Cabinet associated with an audio-group. remove the cabinet.	Cabinet with associated audio-groups is removed without any error/warning message causing translation corruption.	10.1.0.0.0
CM-58131	Call routed to Coverage Answer Group. CAG endpoints have Team button on SIP Endpoints. Call coming to CAG answered by Team buttons on SIP endpoints	When multiple calls are answered by Team button, the endpoint is getting corrupted.	10.1.3.3.0
CM-58115	trunk call to station with bridge/bridges and the bridge/one of the bridge answering the call. Station and its bridges are ASAI monitored.	Long calls are recorded, which are bogus.	10.1.2.0.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
CM-58107	SIP User-A service observing a call SIP User-B calls SIP-A on line 2 SIP User-A drops SO call and answers the second call.	One way talk path.	10.1.0.0.0
CM-57015	On unicode enabled CM and SIP stations and with DM enabled, call station-B from station-A.	Display name on the called/Callee is not as expected.	10.1.3.4.0

Fixes in Communication Manager Release 10.2.1.0.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
CM-58616	Calls routed to Workplace agents and wrong keys are pressed by the caller	Workplace client won't respond, and agent is marked in AUX mode	10.2.1.0.0
CM-58001	Add more than 255 trunk members to trunk-group with special application SA-8510 enabled	Unable to add more than 255 members to trunk-group	10.1.0.0.0
CM-57891	Run the **vm-support** command.	"**vm-support**" command fails.	10.1.0.0.0
CM-57810	Call comes in on VDN-1 which route the call to agent directly using 'route-to' command. Agent then transfers the call to VDN-2. Both the VDNs have "Display VDN for Route-To DAC" field set to "y" and use VDN variables in Vector to route the call.	VDN variables were not referenced correctly for transferred call if "Display VDN for Route-To DAC" is set on VDN.	10.1.3.0.0
CM-57802	Route files with incorrect syntax.	CM Web SMI > 'Static Routes' page shows "System error: Internal operation failed- please contact the system administrator and/or support team for assistance."	10.1.0.0.0
CM-57788	Make a call from SIP station to SIP Group-Paging extension and use AMS for media-anchoring.	Group-paging did not work (no audio to the paged users).	10.1.3.3.0
CM-57778	Bridge originating a call on behalf of principal	Long hour call recording	10.1.0.2.0
CM-57686	Change COR on agent form from sat when agent is logged in on a station	Agent logged off	10.1.3.1.0
CM-57679	CTI station status query for an H323 station whose audit is also in progress at the same time	Intermittently, CTI query may returns out-of-service for an in-service station	10.1.3.0.1
CM-57617	A calls B (B is a SIP phone with Audix rec button) B answers the call	Audix Recording Fails	10.1.3.2.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
	B presses audix rec button (The conference with audix takes about 2 seconds to complete) A hangs up immediately (within 2 seconds from the button press)		
CM-57597	EMX application sends triggerResponse (NOTIFY / 200 OK).	CM restarted / interchanged	10.1.3.3.0
CM-57563	SIP Endpoint with multiple team buttons configured. Call comes into the observed station	SIP endpoint not able to answer the Team calls.	10.1.3.3.0
CM-57556	An outgoing trunk call from CM and trunk side changing the connected party number to long (>= 12) digits number	Customer failed to get correct state for external party in the ASAI monitored call.	10.1.2.0.1
CM-57462	CM 10.2 and above	fileserver command won't work.	10.2.0.0.0
CM-57416	remove station from SAT terminal while it is registered in shared control mode (like from DMCC dashboard using independent / main mode)	CM restart while removing stations	8.0.0.0.0
CM-57095	3rd party auto dial request on behalf of CM's station.	CTI application side did not get call information passed during call origination causing application not to recognize the call	10.1.3.2.1
CM-56962	SMGR/third party signed CM certificate with reserved IP address- 192.11.13.6 used in the Subject CN field of the certificate.	Incorrect demo certificate warning is shown on CLI and SMI	10.1.0.0.0
CM-56887	MOH configured. call placed on hold. periodic Announcement audit is scheduled. Corruption in media ports index.	MOH failure	10.1.3.1.0
CM-56711	Pre 8.x CM version translations having an analog announcement.	After upgrade to 8.x or 10.x, "display port <announcement port>" command will display error "Error encountered can't complete request"	8.0.0.0.0
CM-56706	Configure SIG group 1749 for AFR (Alternate Failover Routing).	CM reload when connectivity is lost with primary ASM.	8.0.0.0.0
CM-56603	Incoming H323 trunk call to CM routes to a voice mail system over ISDN/PRI trunks in a G650	User unable to hear Voicemail prompt	10.1.3.1.0
CM-56563	Restore the backup on 10.x CM	During restore below message is observed in logs "Failed to stop	10.1.0.0.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
		chornyd.service: Unit chornyd.service not loaded.”	
CM-56456	H.323 station calling a busy dual-reg station having hunt-to station to another dual-reg station.	The calling H.323 station did not get ringback when a dual-reg station was called having no idle call appearance and call went to dual-reg station configured as hunt-to station of called station.	10.1.3.2.0
CM-56270	Anonymous SIP call with INVITE msg containing the Privacy:id header, tandem over a QSIG trunk.	In the case of an anonymous SIP call with privacy:id header, tandem over QSIG trunk, CM shows the "i" character in the Calling Party Name field.	10.1.3.2.0
CM-56227	Corruption in announcement structures.	Announcements cannot be rerecorded	10.1.3.1.0
CM-56217	Incoming SIP trunk call answered by Bridged user	Incoming SIP trunk call to any station goes in infinite display Invite and call drops	10.2.0.1.0
CM-56189	Run “list measurements coverage-path" and "list measurements principal" command on CM SAT Terminal	Commands "list measurements coverage-path" and "list measurements principal" returns error “Entry is bad'.”	10.1.3.1.0
CM-56183	Asymmetric DTMF with MG used as a media resource.	DTMF digits are not recognized in case of Asymmetric DTMF payload type with Media-Gateway.	10.1.3.0.1
CM-56113	sip trunk calls were answered by a sip station monitored by CTI application.	Incorrect called party numbers are sent in ASAI connected event.	10.1.3.2.0
CM-56082	CM 10.2.0.0.0 and above	The FP Filters Page on the CM SMI interface does not populate data for the selection fields like - Category, MO type, Equip type. Also, the page does not show active filters and unable to add new filters.	10.2.0.0.0
CM-55980	SIP station B & C having team button for SIP station A Call comes into SIP station A Station B and station C both answering the call via Team button at the same time.	For a station being observed by multiple SIP stations, when the call comes in, and multiple observing parties answer the call within 100 ms, the call first gets connected to the first party and then to the last party to answer the call.	10.1.2.0.0
CM-55904	BRI trunk with layer 2 down, a route pattern having 2 trunk groups configured, the first one being layer 2 down	call is stuck, not routed to next trunk group even when LAR is set to next	10.1.2.0.0
CM-55839	Corruption in the Adj_cid_tbl so that the ISG and Capro CIDs are different.	Frequent failure of the ECD Skill Route Select from Affinity.	8.1.3.7.0
CM-55719	DCP station logged on a softphone and its corresponding hardware (PN / MG on which the dcp station port was configured) removed and then save trans or reset	Errors during display station list station not listing all stations	10.1.3.0.0
CM-55665	Set field "Maximum Off-PBX Telephones - EMX:" on	Heap Leakage could lead to CM reload.	10.1.3.0.1

ID	Minimum conditions	Visible symptoms	Issue found in Release
	system-parameters customer-options to non-zero.		
CM-55662	A transfer call involving unicode supported stations.	un-expected display (not in expected language or random) on phones belonging to CM configured for unicode languages while doing transfer and after transfer.	10.1.3.2
CM-55637	Out of range uid sent for any ASAI event	CM traps, may interchange	10.1.3.1.0
CM-55635	A call to xported stn across a QSIG trunk, covered by CAG with unregistered sip stations	A trunk call hangs in silence	10.1.3.0.0
CM-55597	Disable the PING traffic between CM and AMS.	Avaya Media Server (AMS) showed In-service even if the corresponding SIG Group was Out-Of-Service.	10.1.3.1.0
CM-55584	SIP station to station call, station transferring the call to another SIP station having EC500 over SIP trunk. And trunk is configured to refer tandem-calling-party number form	EC500 leg of SIP transferred-to station does not get correct calling party number i.e. of original calling party if tandem-calling-party form is used to modify CPN	10.1.2.0.0
CM-55575	Call recording using ACS recorder, there should be a shared control station on Annex-LP station which is third party.	Call is not recorded.	10.1.3.1.0
CM-55333	Activate the hntpos-bsy button on the SIP station and then do a reset 4 or push to ESS.	After a reset 4 / ESS takeover, the hntpos-bsy button went out of sync, if state was turned on.	10.1.3.1.0
CM-55312	A duplex CM setup with a SS(LSP)	CM user directories for deleted users are not deleted on survivable servers	10.1.3.1.0
CM-55311	If a conference is done after enabling MCT	MCT button remains active after conf call drops.	10.1.3.2.0
CM-55122	Service Provider sends FMTP video attribute in the SDP before it’s related riprap attribute	Video will not work	10.1.3.0.1

Fixes in Communication Manager Release 10.2.0.1.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
CM-56089	CM 8 and above, run command “list measurement summary”	Output of "list measurements summary" page 4 shows incorrect value of 24000 for "Total Local and Persistent Variables".	10.1.0.0
CM-56082	Add filter on CM SMI (CM SMI Web interface > FP Filters Page)	The FP Filters Page on the CM SMI interface did not populate data for the selection fields like - Category, MO type, Equip type. Also, the page did not show the active filters and was unable to add new filters.	10.2.0.0.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
CM-55839	Some corruption in the Adj_cid_tbl so that the ISG and Capro CIDs are different.	Frequent failure of the ECD Skill Route Select from Afiniti.	8.1.3.7.0
CM-55719	DCP station logged on a softphone and its corresponding hardware (PN / MG on which the dcp station port was configured) removed and then perform save trans or system reset	Errors during display station. list station not listing all stations.	10.1.3.0.0
CM-55665	Set field "Maximum Off-PBX Telephones - EMX:" on system-parameters customer-options to non-zero.	Heap Leakage lead to CM reload.	10.1.3.0.1
CM-55637	CM version 8.x / 10.x	CM traps, may interchange	10.1.3.1.0
CM-55597	Disable the PING traffic between CM and AMS.	Avaya Media Server (AMS) showed In-service even if the corresponding SIG Group was Out-Of-Service	10.1.3.1.0
CM-55584	SIP station to station call, station transferring the call to another SIP station having EC500 over SIP trunk. And trunk is configured to refer tandem-calling-party number form.	EC500 leg of SIP transferred-to station does not get correct calling party number i.e. of original calling party if tandem-calling-party form is used to modify CPN	10.1.2.0.0
CM-55452	Call recording with Station Tone Forward Disconnect: "busy" or "intercept" on "system parameters features"	Long calls are recorded, which are bogus	10.1.3.1.0
CM-55369	MOH on, call on Hold, and audit for the announcement runs.	Callers hear silence instead of music when put on hold	10.1.0.2.0
CM-55312	Delete user from main server.	Deleted user home directory not removed from survivable servers.	10.1.3.1.0
CM-55311	If a conference is done after enabling MCT	MCT button remains active after conf call drops	10.1.3.2.0
CM-55310	H323 station pressing audix button and hanging up the call within 2 seconds	No disconnect event causing recording issues	10.1.3.0.1
CM-55283	Incoming call containing 14 (or more) digits and + sign lands on VDN which compares ANI with VRT.	In vector, only the first 13 digits of ANI were compared with VRT (Vector Routing Table) entries	10.1.2.0.0
CM-55211	Vector with collect digit step and announcement.	DTMF did not work during announcement after call held/unheld vector collect step	10.1.3.1.0
CM-55193	Enhanced call pickup alerting for SIP pickup group	Frequent Heap errors which may lead to CM reset	10.1.3.1.0
CM-55165	On unicode enabled CM, SIP station to station call and called station have display language configured as “user-defined“.	Unicode name displayed on the called SIP station where expected was English	10.1.0.2.0
CM-55122	Service Provider sends FMTP parameter before RTPMAP in SDP	Video will not work	10.1.3.0.1
CM-55099	SIP station to station call blind transferred to another SIP station with EC500 over H.323 trunk.	Calling party number sent on EC500 side for a blind transferred SIP-SIP station call was not as per configuration in Public Unknown Numbering	10.1.2.0.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
CM-55081	Local DNS server not working or misconfigured	CM attempted to contact DNS root servers at midnight when local DNS server is not working	10.1.2.0.0
CM-54328	Select a DMCC station via SSC for call recording	call cannot be recorded	8.1.3.6.0

Fixes in Communication Manager Release 10.2

ID	Minimum conditions	Visible symptoms	Issue found in Release
CM-55167	System was thousands of integrated announcements on Media Server-1 Other Media Servers do not have announcements. Place at least 4000 simultaneous calls which play these announcements	Announcements did not play and sometimes callers hear dead air in mid call.	10.1.3.1.0
CM-55053	A Computer Telephony application initiates transfer using Trunk Access Code dialing	Transfer does not complete	10.1.2.0.0
CM-54956	Register a Session Initiation Protocol (SIP) phone and administer Multiple Registration recording on it using Recorder (ACRA)	Intermittently the recordings would fail.	8.1.3.6.0
CM-54916	Keep a system running for a long time, till process ID goes over 65535	Ping all fails	10.1.0.2.0
CM-54897	audix-rec button is administered on the SIP endpoint No members should be available in the audix hunt group	The recordings on the SIP station after audix rec button is pressed are long calls because no disconnect event is sent.	10.1.2.0.0
CM-54893	Turn off IP sync on the system-parameters features form	Cannot access "change synchronization media-gateway X" command	10.1.2.0.0
CM-54883	Service Observe a H.323 station. Place a Make Call request from this station to another. Use DLG interface to make the request towards AES	Customer sees call origination fails on the application.	10.1.2.0.0
CM-54811	Administer a SIP station in a Network Region (NR) with no VoIP resources in the NR itself. Enable Dial Plan Transference (DPT) on this Network region	Calls from this SIP station was failing.	8.1.3.1.0
CM-54701	Place a call to a station press Malicious Cal trace (MCT) on the station SO this call. Drop the call	The MCT button was never turns off.	10.1.0.2.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
CM-54698	Enable SA8702 SIP contact URI should be longer than 40 chars	Universal Call ID (UCID) was corrupted in Call Detail Record (CDR).	10.1.0.2.0
CM-54668	Try to change the update the user-profile name using the "change user-profile X" command The new profile name should be smaller than the old name	The newly created name was corrupted. It puts the new name in first characters, while the rest is still the old name	10.1.3.0.1
CM-54469	Session Boarder Controller (SBCe) sends a call towards CM with a UCID generated by SBCe in User-User On the CM, make a transfer to another station.	Wrong UCID gets selected on the eventual call after transfer is completed.	10.1.2.0.0
CM-54466	Sig group should be set with DTMF mode set to Out of band.	No DTMF digits was get collected.	10.1.2.0.0
CM-54435	Install any SSP after SSP3 configure "Maximum time an idle CLI session remains active" from SMI.	The SSH session wasn't disconnected after terminal stays inactive for sufficient time.	10.1.3.0.0
CM-54422	Turn on SELinux Restart CM	CM server intermittently goes into crit_os state	10.1.3.0.0
CM-54104	Call made to a vector with Multiple Skill Queueing enabled. There are no available agents on the first skill	agent does not have audible ring	10.1.2.0.0
CM-54050	Keep a system running for a long time, till call processing process ID goes over 999999 Attach call processing on DDB Write a breakpoint where call processing is used in action list	The action list does not execute.	10.1.0.2.0
CM-53222	No customer visible symptom	No customer visible symptom	10.1.0.2.0
CM-52722	Elite in call surplus with 4000 sip agents high traffic. There are network delays causing messages towards the stations to be slowed down.	High CPU occupancy on CM.	10.1.0.2.0
CM-51946	Use one-touch recording on SIP phones by pressing the audix-rec button.	Encountered corruption on the audix-rec button data that prevents the recording attempt until it is cleared via TCM or a reboot	8.1.3.5.0
CM-51755	Turn on Peer Detection on sig groups	The "+" settings on sig group are inconsistently being set depending on Peer Detection status	8.1.12.0.0
CM-51741	System should be setup with SIP MDA	All members get the enhanced pickup group display regardless of their language settings.	8.1.3.4.0
CM-47380	SIP reachability feature is turned off	CM does not resubscribe after the socket comes back up.	6.3.0.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
	Trigger resubscription by resetting the socket to ASM		
CM-44692	Call from DCP station to SIP trunk. DCP station should be on a PN. SIP trunk should take its VoIP from AMS, and a IGC should be created between AMS and MP.	Talk path does not com up.	8.1.3.0.0
CM-17142	Setup NICE or Verint with AES encryption. Restart the socket between CM and AES	White noise gets recorded.	6.3.16.0

Known issues and workarounds in Communication Manager Release 10.2.x.x

Known issues and workarounds in Communication Manager Release 10.2.1.4.0

ID	Minimum conditions	Visible symptoms	Workaround
CM-61832	Race condition in UPDATE and 180 Ringing with DM enabled	Call drop	Disable DM
CM-61831	the E911 Inform options are enabled on system-parameters crisis-alert form and large number of stations reregister	SNMP traps are not sent for every station	No
CM-58360	SIP endpoints with 2 shared control DMCCs in split-stream recording (MR) mode. Agent1 receives an incoming call on one AMS and does a consultative transfer to another Agent2 on different AMS.	Intermittently No Audio after call transfer is complete	No
CM-58492	certificate-based authentication enabled on WebLM	CM unable to acquire license	Disable certificate-based authentication on WebLM
CM-58201	Encrypted DUP link and dumper process is restarted while standby is busied out	DUP link fails to come up	Disable Encryption on DUP link.
CM-58129	Incoming call to ACD SIP agent in shared control independent	ROOF feature not getting triggered, caller keeps on getting ringback tone, call never answered.	Use RONA

	mode with ROOF feature enabled.		
CM-58057	CM installed on KVM based ASP R6	S8300 Front Panel LED's do not function correctly. Refer PSN PSN020654u for more details.	NA
CM-56488	New license file with AMS Channel count less that the total allocated dedicated AMS channels	CM fail to allocate DSP resources from AMS resulting in call failures	Before generating new license file, Correct the dedicated channel count to match the new licenses file.

Known issues and workarounds in Communication Manager Release 10.2.1.3.0

ID	Minimum conditions	Visible symptoms	Workaround
CM-61728	XMOBILE Station and Configure emergence extension number other than station extension	When calling to emergency number (911), from XMOBILE station, calling number is not getting updated as per Emergency Location Extension number configured on station form. Calling number is same as the station number.	No
CM-58360	SIP endpoints with 2 shared control DMCCs in split-stream recording (MR) mode. Agent1 receives an incoming call on one AMS and does a consultative transfer to another Agent2 on different AMS.	Intermittently No Audio after call transfer is complete	No
CM-58494	remove site-data even though it is not used	error "Entry must be deleted from stations before removal"	No
CM-58492	certificate-based authentication enabled on WebLM	CM unable to acquire license	Disable certificate-based authentication on WebLM
CM-58201	Encrypted DUP link and dumper process is restarted while standby is busied out	DUP link fails to come up	Disable Encryption on DUP link.
CM-58129	Incoming call to ACD SIP agent in shared control independent mode with ROOF feature enabled.	ROOF feature not getting triggered, caller keeps on getting ringback tone, call never answered.	Use RONA

CM-58104	AUTOMATIC TRACE ROUTE is turned ON on system-parameters ip-options and Media-gateway lose connectivity to CM or are rebooted	High CPU usage on CM and Media gateway unable to register back to CM	Disable AUTOMATIC TRACE ROUTE on system-parameters ip-options
CM-58057	CM installed on KVM based ASP R6	S8300 Front Panel LED's do not function correctly. Refer PSN PSN020654u for more details.	NA
CM-56488	New license file with AMS Channel count less that the total allocated dedicated AMS channels	CM fail to allocate DSP resources from AMS resulting in call failures	Before generating new license file, Correct the dedicated channel count to match the new licenses file.

Known issues and workarounds in Communication Manager Release 10.2.1.2.0

ID	Minimum conditions	Visible symptoms	Workaround
CM-58559	SIP station with Language German installed. xmobile station on CM which has bridge appr for called station and mapping mode for xmobile station is both OR termination.	M will send UPDATE messages to SIP STN-, but number in PAI/Contact header is missing	No
CM-58360	SIP endpoints with 2 shared control DMCCs in split-stream recording (MR) mode. Agent1 receives an incoming call on one AMS and does a consultative transfer to another Agent2 on different AMS.	Intermittently No Audio after call transfer is complete	No
CM-58494	remove site-data even though it is not used	error "Entry must be deleted from stations before removal"	No
CM-58492	certificate-based authentication enabled on WebLM	CM unable to acquire license	Disable certificate-based authentication on WebLM
CM-58201	Encrypted DUP link and dumper process is restarted while standby is busied out	DUP link fails to come up	Disable Encryption on DUP link.

CM-58129	Incoming call to ACD SIP agent in shared control independent mode with ROOF feature enabled.	ROOF feature not getting triggered, caller keeps on getting ringback tone, call never answered.	Use RONA
CM-58104	AUTOMATIC TRACE ROUTE is turned ON on system-parameters ip-options and Media-gateway lose connectivity to CM or are rebooted	High CPU usage on CM and Media gateway unable to register back to CM	Disable AUTOMATIC TRACE ROUTE on system-parameters ip-options
CM-58057	CM installed on KVM based ASP R6	S8300 Front Panel LED's do not function correctly. Refer PSN PSN020654u for more details.	NA
CM-56488	New license file with AMS Channel count less that the total allocated dedicated AMS channels	CM fail to allocate DSP resources from AMS resulting in call failures	Before generating new license file, Correct the dedicated channel count to match the new licenses file.

Known issues and workarounds in Communication Manager Release 10.2.1.1.0

ID	Minimum conditions	Visible symptoms	Workaround
CM-58559	SIP station with Language German installed. xmobile station on CM which has bridge appr for called station and mapping mode for xmobile station is both OR termination.	M will send UPDATE messages to SIP STN-, but number in PAI/Contact header is missing	No
CM-58360	SIP endpoints with 2 shared control DMCCs in split-stream recording (MR) mode. Agent1 receives an incoming call on one AMS and does a consultative transfer to another Agent2 on different AMS.	Intermittently No Audio after call transfer is complete	No
CM-58494	remove site-data even though it is not used	error "Entry must be deleted from stations before removal"	No
CM-58492	certificate-based authentication enabled on WebLM	CM unable to acquire license	Disable certificate-based authentication on WebLM

CM-58201	Encrypted DUP link and dupmgr process is restarted while standby is busied out	DUP link fails to come up	Disable Encryption on DUP link.
CM-58129	Incoming call to ACD SIP agent in shared control independent mode with ROOF feature enabled.	ROOF feature not getting triggered, caller keeps on getting ringback tone, call never answered.	Use RONA
CM-58104	AUTOMATIC TRACE ROUTE is turned ON on system-parameters ip-options and Media-gateways lose connectivity to CM or are rebooted	High CPU usage on CM and Media gateway unable to register back to CM	Disable AUTOMATIC TRACE ROUTE on system-parameters ip-options
CM-56488	New license file with AMS Channel count less that the total allocated dedicated AMS channels	CM fails to allocate DSP resources from AMS resulting in call failures	Before generating new license files, Correct the dedicated channel count to match the new licenses file.

Known issues and workarounds in Communication Manager Release 10.2.1.0.0

Note: The new KVM OVAs published on 23rd Dec 2024 has the Disk Encryption capability.

ID	Minimum conditions	Visible symptoms	Workaround
~~CM-58084~~	~~Communication Manager Deployed on ASP R6.0 Host~~	~~CM Disk Encryption feature is not available~~	~~No~~

Known issues and workarounds in Communication Manager Release 10.2.0.1.0

ID	Minimum conditions	Visible symptoms	Workaround
CM-56270	Anonymous SIP call to CM with header "Privacy: id" is routed to a 3rd party PBX via DS1 QSIG trunk	CM adds a single character as “i” as calling name in case of privacy.	No
CM-56227	Corruption in internal CM structures	intermittent failures on announcement re-recording attempts	Clear corruption by services engineer
CM-56183	Asymmetric DTMF with MG used as a media resource	DTMFs not getting exchanged.	Use AMS as media resource

CM-56168	On the " TONE GENERATION" page, set the value of the field "Base Tone Generator Set" to 4. Go off-hook on a h.323 phone	Incorrect dial tone being played when the base tone generator set is set to 4.	No
CM-56052	ACD call on a domain-controlled VDN The call is answered by a SIP agent.	Intermittently, CM sends '#####' for the calling party number in the connected event, after sending the correct ANI in the alerting event.	No
CM-55980	team button on more than 2 SIP stations.	incoming call to a station answered simultaneously by 2 SIP stations using team buttons, sometimes talk path get connected to both endpoints.	No
CM-55904	The BRI-trunk between CM and MG is in in-service but layer 2 state is assigned instead of established. LAR configured in route pattern to next.	Call gets stuck if layer2 is down on trunk grp, and LAR is not triggered	No
CM-55662	H.323 station calling SIP station supporting English language.	For calls, SIP stations sees display in unicode when the expected display is English for the other party in the call.	No
CM-55635	Trunk is H323 with SS-B signaling with following settings QSIG Value-Added? y QSIG-Value Coverage Encoding: proprietary On customer-options page 9 Value-Added (VALU)? y	The calling station ends up hearing nothing in this scenario and connected to nothing.	No

Known issues and workarounds in Communication Manager Release 10.2

ID	Minimum conditions	Visible symptoms	Workaround
FI-2142	STIR SHAKEN Feature on IOS and MacOS	IOS and MacOS devices on version 3.35 were crashing while STIR/SHAKEN message received.	Disable STIR/SHAKEN feature for IOS and MacOS. Issue will be fixed by Feb 2024

Avaya Aura® Session Manager

What's new in Session Manager Release 10.2.x.x

What's new in Session Manager Release 10.2.1.1

- VMware ESXi 8.0.3 U3 platform support.

The December 23 updated Aura 10.2 KVM OVAs now support the following:

- The KVM OVAs include an *install_vm.py* script to simplify deployment of the KVM OVA
- The *install_vm.py* script now supports the creation of a root login/password
- The CM and AES updated 10.2 KVM OVAs also include support for encryption.

What's new in Session Manager Release 10.2

For more information, see ***What's New in Avaya Aura® Release 10.2.x*** document on the Avaya Support site: https://download.avaya.com/css/public/documents/101087359

Future use fields visible in Avaya Aura® Session Manager Release 10.2.x.x

Future use fields visible in Avaya Aura® Session Manager Release 10.2

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

- Session Manager Global Settings Enable Load Balancer

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

- Session Manager Global Settings Enable SIP Resiliency

Security Service Pack

Security Service Pack

With the release 10.x Avaya introduces a common version on RedHat Enterprise Linux (RHEL 8.4) to its Avaya Aura platform. Common versions of RPMs are supported and consumed by the components. This results in a change to how security updates are provided for Session Manager (SM).

CRITICAL: The Security Service Pack installation framework for SM has changed in Release 10. x. It is imperative that the instructions in PCN2161S be reviewed for complete steps prior to installation of Security Service Packs on an SM 10.2.x system.
The SSP can only be installed via the command line. There is no Solution Deployment Manager (SDM) support for SSP installation.
In order to install the SSP for SM 10.2.x, you must use the new command ("av-update-os") and follow the detailed instructions in **PCN2161S**.

Required artifacts for Session Manager Release 10.2.x.x

Required artifacts for Session Manager Release 10.2.1.4

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

Filename	PLDS ID	File size	Version number	Comments
Session_Manager_10.2.1.4.1021408.bin	SM000001053	1.61 GB	1021408	SM 10.2.1 Service Pack #4

Required artifacts for Session Manager Release 10.2.1.3

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

Filename	PLDS ID	File size	Version number	Comments
Session_Manager_10.2.1.3.1021305.bin	SM000001040	1.6 GB	1021305	SM 10.2.1 Service Pack #3

Required artifacts for Session Manager Release 10.2.1.2

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

Filename	PLDS ID	File size	Version number	Comments
Session_Manager_10.2.1.3.1021207.bin	SM000001037	1.6 GB	1021207	SM 10.2.1 Service Pack #2

Required artifacts for Session Manager Release 10.2.1.1

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

Filename	PLDS ID	File size	Version number	Comments
Session_Manager_10.2.1.1.1021105.bin	SM000001030	1.6 GB	1021105	SM 10.2.1 Service Pack #1

Required artifacts for Session Manager Release 10.2.1.0

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

Filename	PLDS ID	File size	Version number	Comments
Session_Manager_10.2.1.0.1021007.bin	SM000001023	1.6 GB	1021007	SM 10.2 Feature Pack #1
~~SM-10.2.0.0.1020019-kvm-02.ova~~	~~SM000001018~~	~~2.6 GB~~	~~1020019~~	~~SM 10.2 KVM OVA~~
~~BSM-10.2.0.0.1020019-kvm-02.ova~~	~~SM000001019~~	~~1.8 GB~~	~~1020019~~	~~BSM 10.2 KVM OVA~~
AV-SM10.2-RHEL8.10-OSUpdate-003.tar.bz2	SM000001025	646 MB	Red Hat Linux	RHEL 8.10 OS Bundle

Filename	PLDS ID	File size	Version number	Comments
			Release 8.10 (Ootpa)	
BSM-10.2.0.0.1020019-kvm-04.ova	SM000001026	1.85GB	1020019	SM 10.2 KVM OVA
SM-10.2.0.0.1020019-kvm-04.ova	SM000001027	2.64GB	1020019	BSM 10.2 KVM OVA

Note: Replacing the KVM OVAs to cover the script-based deployment and the procedure is documented in deployment guide.

Required artifacts for Session Manager Release 10.2.0.1

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

Filename	PLDS ID	File size	Version number	Comments
Session_Manager_10.2.0.1.1020108.bin	SM000001009	1.2 GB	1020108	SM 10.2 Service Pack #1

Required artifacts for Session Manager Release 10.2

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

Filename	PLDS ID	File size	Version number	Comments
SM-10.2.0.0.1020019-e80-01.ova	SM000001001	3.2 GB	1020019	SM OVA
BSM-10.2.0.0.1020019-e80-01.ova	SM000001002	1.9 GB	1020019	BSM OVA
Session_Manager_10.2.0.0.1020019.iso	SM000001003	1.6 GB	1020019	SW Only ISO
dmutility-10.2.0.0.1020019.bin	SM000001004	392 KB	1020019	DM Utility

Note: The deployment of Avaya Aura® applications as Software-only is available but a restricted offer for net new deployments and requires Avaya Aura® BU approval before proceeding. If you have a business requirement to deploy Avaya Aura® as Software-only, please get in touch with your Avaya Sales team. Existing customers using software only deployments continue to be supported.

Software information

Software	Version	Note
OS	Red Hat Linux Release 8.4 (Ootpa)	
PostgreSQL Database	13.10	
Cassandra	3.11.14	
Open JDK 64-Bit	1.8.0_372-b07	
IBM Liberty Server	22.0.0.11	
Application Server	wildfly-24.0.0. Final	

Software	Version	Note
VMware vCenter Server, ESXi Host	7.0.X, 8.0, 8.0 Update 2.	Avaya Aura® Release 10.2.x supports VMware 8.0 and VMware 8.0 Update 2. Avaya Aura® Release 10.2.x does not support VMware 8.0 Update 1. For information about known issues, see VMware 8.0 Update 1 Release Notes on the VMware website at https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-6vcenter-server-801-release-notes/index.html.

Installation for Session Manager Release 10.2.x.x

Backing up the software

Refer to the Session Manager Backup and Restore section of the *Administering Avaya Aura® Session Manager* document at: https://support.avaya.com

Installing the Session Manager software

For more information about installing Session Manager, see the Avaya Aura® Session Manager deployment documents at: https://support.avaya.com

Upgrading the Session Manager software

Note 1: To preserve full system connectivity, it may be necessary to apply a pre-upgrade patch to each Session Manager in the network BEFORE updating System Manager to release 10.2. This is necessary only if BOTH the following conditions apply:

1. Session Manager is on release 8.1.x
2. Security Service Pack #12 or #13 have been applied to Session Manager

In this case, you must apply Security Service Pack #14 or later to each Session Manager - prior to initiating the 10.2 upgrade of System Manager.

Note 2: When upgrading directly from Session Manager 7.0.x to Session Manager 10.2, Centralized Call History records will not be retained.

Note 3: Due to significant architecture and security enhancements in post SM 10.1 release, in certain situations customers may experience Cassandra outages during upgrade procedures. This only applies to customers that are on 8.0.0 or earlier releases, have more than 2 session managers, and are unable to upgrade all session managers in a single maintenance window. During the time where some session managers are running 8.0.0 or earlier, while others are on 10.2, the Cassandra clusters in each release will operate in isolation. Noticeable impacts will be an interruption in Offline Call History operation, and the inability for end users to make changes to device data (e.g. button labels) or contact lists. The number of users impacted is difficult to predict, as it depends upon the topology of the system and the distribution of users across session managers. Once all session managers are upgraded to 10.2 the Cassandra nodes will again act as a single cluster and operation will return to normal.

Note 4: **For Systems operating in FIPS mode:**

Extra steps are required if all Session Managers cannot be upgraded to Release 10.2 in a single maintenance window from pre-10.1 release.

For each Session Manager that will remain on an earlier pre-10.1 release, execute the following via the Session Manager command line:

1. Edit the Cassandra configuration file (/data/var/avaya/cassandra/current/conf/cassandra.yaml) and change the listed *cipher_suites* under the *client_encryption* options section from:

   [TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA]

   To:

[TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_128_GCM_SHA256]

2. Execute "restart Cassandra"

For more information about upgrading Session Manager, see the *Upgrading Avaya Aura® Session Manager* document at: https://support.avaya.com

Troubleshooting the installation

Refer to the *Troubleshooting Avaya Aura® Session Manager* document at: https://support.avaya.com

Restoring software to the previous version

Refer to the product documentation.

Fixes in Session Manager Release 10.2.x.x

Fixes in Session Manager Release 10.2.1.4

Key	Minimum Conditions	Visible symptoms	Issue found in Release
ASM-95492	Add modify delete sip entity	added/Modified SIP entity link won't come UP	10.2.1.2
ASM-95489	Configure emergency numbers	PPM exception while retrieving emergency numbers data using ListOfEmergencyNumbers	10.2.0.0
ASM-95487	Run iniTM -f	Certs missing IP address of SM in SAN for mgmt, (spiritalias , syslog and postgres Identity certificates)	10.2.0.0.
ASM-95472	Register SIP extension and verify user registration page from SMGR UI	Device Data is missing on the User Registration page.	10.2.1.0
ASM-95446	Apply SSP 18 and later	DRS replication failure	10.2.0.0
ASM-95441	Add modify delete SIP entity links	periodically ConfigSoapServer.core is generated	10.2.0.0
ASM-95375	administrator user with View permission is still able to change the SM settings	administrator with View permission is still able to change the SM settings	10.2.1.0
ASM-95318	Enable CDR and trigger answer the call which is forwarded`	Forwarded/Answering Extension is not recorded.	10.2.1.0
ASM-95137	SIP SIP message more than 64KB	Asset service is restarted causing impact to call processing and registrations	10.2.0.1

Fixes in Session Manager Release 10.2.1.3

Key	Minimum Conditions	Visible symptoms	Issue found in Release
ASM-95341	Click on the SM help pages in SMGR	SM help pages may not work	10.1.3.6
ASM-95274	ASM 10.2.1.x installed	No Visible symptoms. IBM Liberty Java Version update to 1.8.0_461	10.2.1.0

Fixes in Session Manager Release 10.2.1.2

Key	Minimum Conditions	Visible symptoms	Issue found in Release
ASM-95177	Bad routing resulting loop between CM and ASM	Entity link goes down.	10.1.0.0
ASM-95155	2 core ASMs managed by SMGR. One of the ASM is powered OFF.	Fragmentation audit triggered every hour may cause service impact to new calls.	10.1.0.0
ASM-95099	Wrong or unreachable DNS configured	INVITE processing delayed by 31 seconds	10.2.0.0
ASM-95094	Attempt to register Zoom Room clients to SM	Zoom Room clients fail to register to SM as 3rd Party client.	10.2.1.0
ASM-95036	Enable SIP Resiliency, detach SM1 from network, SM2 should take over which triggers call re-construction.	SM maps wrong subid_ipcs after failover, causing 5XX response from SBCE resulting in call reconstruction failure.	10.1.0.0
ASM-94883	Workplace SIP stations registered to SM.	Device data is not shown under User registration page on SMGR	10.2.0.0
ASM-94882	SIP Stations registered to CM.	Actual location may not be displayed on the Registration page for registered users.	10.2.0.0
ASM-94807	SIP Stations registered with SM1 and SM2. SM rebooted unexpectedly due to some catastrophic reason.	Endpoint recovery may fail with 403 response code from SM while the SM services initialize after abrupt reboot.	8.1.3.0
ASM-94105	SM 10.2.x Installed	Security Vulnerability in a scan	10.2.0.0

Fixes in Session Manager Release 10.2.1.1

Key	Minimum Conditions	Visible symptoms	Issue found in Release
ASM-94668	Add implicit users' data using Web Service with App Sequence as NULL.	Customer could not add implicit user entry using WebService	10.2.1.0
ASM-94624	Large CM dialplans (e.g. number of entries exceeds 300) may be vulnerable.	Telephone numbers dialed from a SIP phone may have a 4 second pause before the phone	10.2.0.1

Key	Minimum Conditions	Visible symptoms	Issue found in Release
		makes the call, despite those numbers being handled by dialplan rules.	
ASM-94543	SM 10.1 with APN Configured Endpoint/Workplace Client	The expired Push Notification gets delivered to the device whenever it comes up	10.1.3.0
ASM-94232	SM 10.1 with APN Configured SMGR 10.1	APN Test shows failed randomly and recover after few seconds and frequent alarms are generated for the same.	10.2.0.0
ASM-94068	Add / import adaptation xml file which has two entries with same matching pattern, with different AddressToModify.	overlapping error is displayed	10.1.3.3
ASM-93686	Apply filter on adaptation entries, select and Delete adaptation entries	Wrong adaptation entry gets deleted	Select and delete without applying filters
ASM-92437	Upload SM/SMGR MIB to a MIB browser	Upload to MIB browser throws error	10.1.3.1

Fixes in Session Manager Release 10.2.1.0

Key	Minimum Conditions	Visible symptoms	Issue found in Release
ASM-93600	SM Version 10.2.0.0	PostgregreSQLSecurity Vulnerability detected	10.2.0.0
ASM-93588	SM Version 10.2.0.0	Spring Security Vulnerability detected	10.2.0.0
ASM-93372	Run cert_status script on the Session Manager	Added Certificate Validity date in the cert_status script output	8.1.0.0
ASM-93371	Multiple simultaneous ping requests made to SM	If more than 4 ping requests are initiated from multiple or same source, further ping requests gets dropped by SM Firewall	10.1.3.0
ASM-93366	Incomplete CRL configuration in SMGR	SM Process Asset goes down	10.1.3.2
ASM-93329	Bulk station reload from SM user registration page	Postgres process getting stuck at 99%, can be seen using top command	10.1.2.0
ASM-93319	SM version 10.1.3.x	System Manager Jboss crash due to no free swap memory	10.1.3.1
ASM-93302	Apply SP/Custom patch on SM connected to a Geo SMGR.	Postgres and Jboss fail to start, and SM status will show as not connected on SM dashboard.	10.1.0.0
ASM-93240	SM 10.2.0.1 installed and moderately busy	Java Cores and Deadlock and restart of SM processes	10.2.0.0

Key	Minimum Conditions	Visible symptoms	Issue found in Release
ASM-93212	SSH connection to SM from windows server 2016	SSH connection failure/timeout.	10.1.3.3
ASM-93094	Session manager with SIP user registered.	SM User Registration page on System Manager may not display all registered SIP users.	10.2.0.0
ASM-93024	Calls are queued to CM in a specific Vector Step Sequence	Queued calls are dropped after 3 min	10.2.0.0
ASM-93018	SM 10.x installed	Assets may not recover after failure.	10.1.0.0
ASM-93004	SM 10.2.0.0 installed	Asset process crashes	10.2.0.0
ASM-92904	SM 7.x/8.x/10.x Installed	Security vulnerability related to SM has been fixed.	7.1.0.0
ASM-92859	System with huge number of BSM's in the environment.	SM Dashboard refresh times out with following error "Refreshing status timed out, data displayed may be inconsistent or incorrect"	10.1.2.0
ASM-92811	SIP Trace Viewer configured on SM EM	Error displayed on UI and SIP Tracer cannot be configured.	10.2.0.0
ASM-92803	SIP user registered as RW through ASBCE, and multiple emergency number dial-patterns are configured	RW users unable to dial all the emergency numbers	10.1.3.1
ASM-92802	More than 2 LHNR entries with same CM IP address and SIP entity links with BSM	Entity link with BSM never comes up	10.1.3.1
ASM-92760	SM 10.1.3.x installed	Exceptions seen in the asm.log files	10.1.3.1
ASM-92641	SM 10.2.0.0 installed, and Calls are configured to route through another SM	Memory leak observed and SM restarts	10.2.0.0
ASM-92609	SM 10.2.0.0 installed	SM process restarts with deadlock error	10.2.0.0
ASM-92590	A dialplan configuration where there are multiple patterns with the same length and leading digits.	A SIP phone may dial a number before all of the digits have been entered.	8.1.3.0
ASM-92348	SIP User registered via SBC to both primary and secondary ASM.	Actual location changes every 20-30 seconds when extension registered via SBC	10.1.3.0
ASM-90117	SM installed and configured	SM Restarts in a specific case	10.1.3.0
ASM-85900	SM 8.1.3.x or above installed	Security Vulnerability detected	8.1.3.0

Fixes in Session Manager Release 10.2.0.1

ID	Minimum Conditions	Visible symptoms	Issue found in Release
ASM-92811	View SIP traces using SM EM trace viewer	SMGR Trace Viewer on SM EM UI throws error.	10.2.0.0
ASM-92786	SIP station with IP Video enabled.	Query failure statement logged in mgmt.log file.	10.1.3.1
ASM-92760	N/A	Null Pointer Exception seen in TextLogs.	10.1.3.1
ASM-92707	SM on release 10.1.3.2	Continuous ALARM-SYNFLOOD messages are observed in /var/log/messages.	10.1.0.0
ASM-92698	Execute dmutility command on ASM	dmutility command fails.	10.2.0.0
ASM-92664	Execute “setSecurityPolicy” with custom rules, with password parameters	Parameters modified like password complexity/polices do not work after modification and execution using “setSecurityPolicy”.	10.1.0.0
ASM-92590	Create more than 3 dial patterns, with same length and starting digit, which can be compressed.	Incorrect compression causing routing failure for some compressed patterns.	8.1.3.8
ASM-90992	Session Manager 10.1 installed and observe /var/log/messages file	The /var/log/messages file is flooded with ALARM-ICMPFLOOD and ALARM-SYNFLOOD logs.	10.1.0.0
ASM-90117	N/A	NumberFormatException seen in TextLogs resulting into Call processing restart.	8.1.3.4
ASM-88725	SIP Entity associated with the Adaptation which replaces IP addresses with Domain Name	Domain based routing fails.	8.1.3.4

Fixes in Session Manager Release 10.2.0.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
ASM-92439	Session Manager 8.1.3 or 10.1 installed and run security scan	The scanner flag ActiveMQ Vulnerability (CVE-2023-46604)	8.1.3.0
ASM-92425	Install Branch Session Manager 10.x and observe asm.log files	Observed exceptions callprocessing.pushnotification.OAuth 2Token ERROR even though Push Notification is not enabled	10.1.0.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
ASM-92415	Large number of Branch Session Managers managed by a System manager	Errors displayed on the Session Manager Dashboard	8.1.3.0
ASM-92333	Session Manager 10.1 installed with an unreachable DNS server configured.	Running traces or network reports might show SM trying to access public DNS servers	10.1.0.0
ASM-92204	Session Manager 8.1.3.x installed as SW Only deployment	Software only does not install custom net-snmp rpm if net-snmp rpms already present	8.1.3.6
ASM-92070	Session Manager 10.1.3.x installed and run security scan.	Deprecated SSH Cryptographic settings were discovered	10.1.3.1
ASM-91978	Session Manager 10.1.3.1 installed and navigate to SM Dashboard on the System Manager	The dashboard shows stale data and doesn't refresh	10.1.3.1
ASM-91938	Session Manager Management interface hostname is alphanumeric	Cassandra Nightly repair job fails to run	10.1.3.1
ASM-91890	Session Manager Management interface hostname is combination of uppercase and lowercase	Cassandra Nightly repair job fails to run	10.1.3.1
ASM-91780	Session Manager Management interface added as FQDN instead of IP in the System Manager	Cassandra audit job fails to run	8.1.3.0
ASM-91779	Install Session Manager 10.1.2 with IPv6 address family and SSH to the SM	Unable to SSH to SM using IPv6 address	10.1.2.0
ASM-91698	Configure Aura Core with large number of Feature buttons with extensions as argument and then update extensions on the SMGR UI	Postgres processes hung and SM encounters performance issues.	10.1.2.0
ASM-91629	Session Manager 10.1.x installed, and Postgres process goes down	No alarms generated indicating Postgres is down	10.1.3.0
ASM-91406	Customer makes inbound SIP Trunk call to SIP agent and then cancels before agent could answer	SIP agent heard silence and is not informed of canceled calls	10.1.2.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
ASM-91232	Upgrade SMGR and Session Manager from 8.1.x to 10.1.x	Users with Workplace Clients fail to download PPM data	10.1.2.0
ASM-91132	Enable Push Notification feature with HTTP/HHTPS forward proxy	The connection to the Push Notification provider fails	10.1.0.2
ASM-90996	Session Manager configured with 3rd Party CA with Sub CA in the certificate chain	The initTM script fails intermittently.	10.1.0.0
ASM-90995	Run traceSM command and observer SIP entity name in the columns.	The SIP entity names are not displayed and only IP addresses are displayed	10.1.2.0
ASM-90835	Session Manager 10.1.3.x running with moderate load	Observed AsmUAInfo WARN logs	10.1.3.0
ASM-90826	Upgrade Session Manager from 10.1.0.2 to 10.1.2	The SM/BSM VM sometimes become unresponsive during an upgrade.	10.1.0.0
ASM-90722	Register a 3rd Party SIP phone and observe actual location under User Registrations screen	Actual Location information is not displayed under user registration page	8.1.3.7
ASM-90716	Call to an extension which has hidden/special character in number	PPM throws error for getCallHistory requests and call log is not displayed	8.1.3.5
ASM-90555	System configured with Multiple ports between SM and CM SIP Entity with same protocol	During rainy day, only one port is marked as trusted	8.1.3.4
ASM-90547	Session Manager 10.1.0.2 installed and run sm-report command	One of the CPU cores get blocked with 100% usage by IBM WebSphere	10.1.0.0
ASM-90539	Session Manager 8.1.3.x installed	Rarely it was observed that the RHEL database is corrupted	8.1.3.6
ASM-90425	Export Call Count data in the CSV format	The exported CSV file for Call Counts data is empty	10.1.0.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
ASM-90405	Session Manager experiencing moderate to high Push Notification traffic	Observed in the log files exception java.lang.IllegalThreadStateException	8.1.3.6
ASM-90170	Start User Registration export job from SMGR and make it recurrent	The exports use the same old filename every time.	8.1.3.6
ASM-90013	A SIP station has Primary and Secondary registration and monitored using AES (TSAPI MonitorDevice)	SM incorrectly sends out the registration state as "active".	8.1.3.6
ASM-90005	Push Notification feature enabled with HTTP Proxy	Error on Session Manager Dashboard while enabling the feature	8.1.3.0
ASM-89925	Enable PPM Debug logging using sm ppmlogon command	The mgmt.log file is flooded with the SMCallHistoryDM migrateCallLogsToGlobalDCSpecialCallLog related logs	8.1.3.5
ASM-89835	Register SIP Deskphones to Session Manager and observe Device tab under User Registrations page	The Device information is not displayed under user registrations screen	10.1.0.2
ASM-89829	Run the command "runsmconsole" and attach to the Management member.	SM's server.log file filled with "Missing short name for class" messages	8.1.0.0
ASM-89128	Add SIP Entity links using Routing Web Service API and incorrect value for Connection Policy.	The Web Service request with incorrect value for Connection Policy is not rejected	8.1.3.0
ASM-89053	Aura Core system with more than 6 Session Managers	The nightly User Data Storage repair of Cassandra nodes fails sometimes.	8.1.3.3
ASM-88806	An automatic certificate renewal or a manual replacement of certificates on the Session Manager happens	The WebSphere certificates are not getting updated	8.1.3.4
ASM-88362	SIP Remote worker registered to two data centers through SBC where data centers have two SMs.	Incorrect Actual Location is displayed under User Registration page	8.1.12.0

Known issues and workarounds in Session Manager 10.2.x.x

Known issues and workarounds in Session Manager Release 10.2.1.4

ID	Minimum conditions	Visible symptoms	Workaround
ASM-95136	Delete filtered adaptation entries	After deleting the filtered entries, filtered output may show inconsistent matching records	Click on Refresh icon to fetch the correct matching records Refer to PSN020656u
ASM-93986	Execute delete SIP station from CM which has a user in SMGR	Error seen on SMGR	Delete SIP station from SMGR
ASM-93888	CRL configured on SM	/data partition may grow upto 100% causing postgres failure	If /data partition is less than 95%, execute initTM command in Maintenance Window to free the disk space.
ASM-93595	SM and SMGR 10.2.0.1 Installed	Intermittently no data shown on SM dashboard	Refresh the dashboard using Refresh button
ASM-93031	ASM 10.x installed and Cassandra cluster connectivity issues between core SMs.	/var/log/messages file size may grow huge in GB.	Manually clean up the /var/log/messages log files
ASM-92906	HTTPS Proxy Host and Port configured for APN and working. ASM SP/FP Upgraded.	Rarely SM is unable to send CONNECT request to pnp.avaya.com after SP/FP upgrade.	set the instance value to NULL in SMGR DB.
ASM-92880	Run traceSM on SM 10.2.0.1	The console shows a warning message.	10.2.0.0
ASM-87752	NFS partition (remote datastore) is used for ASM performance data	NFS partition did not automatically get remounted after SMGR reboot	Manually mount the NFS partition
ASM-87031	Large number of users registered to the Session Manager	The user registration page intermittently throws connection exception	None
ASM-87752	Session Manager managed by SMGR which has additional storage with NFS and restart SMGR	The NFS configuration needs to be manually remounted after an SMGR reboot.	None
ASM-84318	Try to change data retention for Performance Data	Cannot change data retention for Performance Data	None

Known issues and workarounds in Session Manager Release 10.2.1.3

ID	Minimum conditions	Visible symptoms	Workaround
ASM-95136	Delete filtered adaptation entries	After deleting the filtered entries, filtered output may show inconsistent matching records	Click on Refresh icon to fetch the correct matching records
ASM-93986	Execute delete SIP station from CM which has a user in SMGR	Error seen on SMGR	Delete SIP station from SMGR
ASM-93888	CRL configured on SM	/data partition may grow upto 100% causing postgres failure	If /data partition is less than 95%, execute initTM command in Maintenance Window to free the disk space.
ASM-93595	SM and SMGR 10.2.0.1 Installed	Intermittently no data shown on SM dashboard	Refresh the dashboard using Refresh button
ASM-93031	ASM 10.x installed and Cassandra cluster connectivity issues between core SMs.	/var/log/messages file size may grow huge in GB.	Manually clean up the /var/log/messages log files
ASM-92906	HTTPS Proxy Host and Port configured for APN and working. ASM SP/FP Upgraded.	Rarely SM is unable to send CONNECT request to pnp.avaya.com after SP/FP upgrade.	set the instance value to NULL in SMGR DB.
ASM-92880	Run traceSM on SM 10.2.0.1	The console shows a warning message.	10.2.0.0
ASM-87752	NFS partition (remote datastore) is used for ASM performance data	NFS partition did not automatically get remounted after SMGR reboot	Manually mount the NFS partition
ASM-87031	Large number of users registered to the Session Manager	The user registration page intermittently throws connection exception	None
ASM-87752	Session Manager managed by SMGR which has additional storage with NFS and restart SMGR	The NFS configuration need to be manually remounted after an SMGR reboot.	None
ASM-84318	Try to change data retention for Performance Data	Cannot change data retention for Performance Data	None

Known issues and workarounds in Session Manager Release 10.2.1.2

ID	Minimum conditions	Visible symptoms	Workaround
ASM-95136	Delete filtered adaptation entries	After deleting the filtered entries, filtered output may show inconsistent matching records	Click on Refresh icon to fetch the correct matching records

ID	Minimum conditions	Visible symptoms	Workaround
ASM-93986	Execute delete SIP station from CM which has a user in SMGR	Error seen on SMGR	Delete SIP station from SMGR
ASM-93888	CRL configured on SM	/data partition may grow upto 100% causing postgres failure	If /data partition is less than 95%, execute initTM command in Maintenance Window to free the disk space.
ASM-93595	SM and SMGR 10.2.0.1 Installed	Intermittently no data shown on SM dashboard	Refresh the dashboard using Refresh button
ASM-93031	ASM 10.x installed and Cassandra cluster connectivity issues between core SMs.	/var/log/messages file size may grow huge in GB.	Manually clean up the /var/log/messages log files
ASM-92906	HTTPS Proxy Host and Port configured for APN and working. ASM SP/FP Upgraded.	Rarely SM is unable to send CONNECT request to pnp.avaya.com after SP/FP upgrade.	set the instance value to NULL in SMGR DB.
ASM-92880	Run traceSM on SM 10.2.0.1	The console shows a warning message.	10.2.0.0
ASM-87752	NFS partition (remote datastore) is used for ASM performance data	NFS partition did not automatically get remounted after SMGR reboot	Manually mount the NFS partition
ASM-87031	Large number of users registered to the Session Manager	The user registration page intermittently throws connection exception	None
ASM-87752	Session Manager managed by SMGR which has additional storage with NFS and restart SMGR	The NFS configuration need to be manually remounted after an SMGR reboot.	None
ASM-84318	Try to change data retention for Performance Data	Cannot change data retention for Performance Data	None

Known issues and workarounds in Session Manager Release 10.2.1.1

ID	Minimum conditions	Visible symptoms	Workaround
ASM-94883	Workplace SIP stations registered to SM.	Device data is not shown under User registration page on SMGR	No
ASM-94105	SM 10.1.3.0 Installed	Security Vulnerability in a scan	None
ASM-93986	Execute delete SIP station from CM which has a user in SMGR	Error seen on SMGR	Delete SIP station from SMGR

ID	Minimum conditions	Visible symptoms	Workaround
ASM-93888	CRL configured on SM	/data partition may grow upto 100% causing postgres failure	If /data partition is less than 95%, execute initTM command in Maintenance Window to free the disk space.
ASM-93595	SM and SMGR 10.2.0.1 Installed	Intermittently no data shown on SM dashboard	Refresh the dashboard using Refresh button
ASM-93031	ASM 10.x installed and Cassandra cluster connectivity issues between core SMs.	/var/log/messages file size may grow huge in GB.	Manually clean up the /var/log/messages log files
ASM-92906	HTTPS Proxy Host and Port configured for APN and working. ASM SP/FP Upgraded.	Rarely SM is unable to send CONNECT request to pnp.avaya.com after SP/FP upgrade.	set the instance value to NULL in SMGR DB.
ASM-92880	Run traceSM on SM 10.2.0.1	The console shows a warning message.	10.2.0.0
ASM-87752	NFS partition (remote datastore) is used for ASM performance data	NFS partition did not automatically get remounted after SMGR reboot	Manually mount the NFS partition
ASM-87031	Large number of users registered to the Session Manager	The user registration page intermittently throws connection exception	None
ASM-87752	Session Manager managed by SMGR which has additional storage with NFS and restart SMGR	The NFS configuration need to be manually remounted after an SMGR reboot.	None
ASM-84318	Try to change data retention for Performance Data	Cannot change data retention for Performance Data	None

Known issues and workarounds in Session Manager Release 10.2.1.0

ID	Minimum conditions	Visible symptoms	Workaround
ASM-94105	SM 10.1.3.0 Installed	Security Vulnerability in a scan	None
ASM-94068	Add / import adaptation xml file which has two entries with same matching pattern, with different AddressToModify.	overlapping error is displayed	None
ASM-93986	Execute delete SIP station from CM which has a user in SMGR	Error seen on SMGR	Delete SIP station from SMGR

ID	Minimum conditions	Visible symptoms	Workaround
ASM-93888	CRL configured on SM	/data partition may grow upto 100% causing postgres failure	If /data partition is less than 95%, execute initTM command in Maintenance Window to free the disk space.
ASM-93686	Apply filter on adaptation entries, select and Delete adaptation entries	Wrong adaptation entry gets deleted	Select and delete without applying filters
ASM-93595	SM and SMGR 10.2.0.1 Installed	Intermittently no data shown on SM dashboard	Refresh the dashboard using Refresh button
ASM-93031	ASM 10.x installed and Cassandra cluster connectivity issues between core SMs.	/var/log/messages file size may grow huge in GB.	Manually cleanup the /var/log/messages log files
ASM-92906	HTTPS Proxy Host and Port configured for APN and working. ASM SP/FP Upgraded.	Rarely SM is unable to send CONNECT request to pnp.avaya.com after SP/FP upgrade.	set the instance value to NULL in SMGR DB.
ASM-92880	Run traceSM on SM 10.2.0.1	The console shows a warning message.	10.2.0.0
ASM-92437	Upload SM/SMGR MIB to a MIB browser	Upload to MIB browser throws error	10.1.3.1
ASM-87752	NFS partition (remote datastore) is used for ASM performance data	NFS partition did not automatically get remounted after SMGR reboot	Manually mount the NFS partition
ASM-87031	Large number of users registered to the Session Manager	The user registration page intermittently throws connection exception	None
ASM-87752	Session Manager managed by SMGR which has additional storage with NFS and restart SMGR	The NFS configuration need to be manually remounted after an SMGR reboot.	None
ASM-84318	Try to change data retention for Performance Data	Cannot change data retention for Performance Data	None

Known issues and workarounds in Session Manager Release 10.2.0.1

ID	Minimum conditions	Visible symptoms	Workaround
ASM-92859	System with huge number of BSM's in the environment.	SM Dashboard refresh times out with following error "Refreshing status timed out, data displayed may be inconsistent or incorrect"	Restart the management interface with command "restart mgmt"

ID	Minimum conditions	Visible symptoms	Workaround
ASM-92809	multiple rules for the adaptation (starting with same prefix). Apply a filter on the rule and try to delete one rule from the adaptation	A different rule, other than the selected, from that adaptation gets removed.	Delete the adaptation rule without applying filter
ASM-92802	more than 2 LHNR entries with same CM IP address. SIP entity with these LHNR entries which has entity link between BSM.	CM entity link with BSM shows down instead of DENY.	None
ASM-92609	Moderate traffic with users associated with User defined snap-ins in Origination and termination leg	Session Manager restarts	None.
ASM-92421	Branch visiting user feature enabled and user logs in foreign branch in Sunny day/Rainy day scenario	The list of PPM controllers doesn't include BSM IP Address or FQDN	Configure BSM IP address manually.
ASM-87031	Large number of users registered to the Session Manager	The user registration page intermittently throws connection exception	None
ASM-92437	Upload Session Manger MIBs to SNMP Browser	The SNMP browser throws error stating Overlapped OIDs were found	Give each var bind unique name
ASM-91096	Import adaptations with duplicated entries of dial patterns in the XML file	Adaptation stops working	Remove duplicated entries
ASM-9117	Session Manager 8.1.3.4 with moderate load	Session Manager throws NumberFormatException and restarts	None
ASM-87752	Session Manager managed by SMGR which has additional storage with NFS and restart SMGR	The NFS configuration need to be manually remounted after an SMGR reboot.	None
ASM-81511	Session Manager with old and new ID certificates have the same Issuer and Root CAs but different CRL Distribution Points (CDP).	SM fails to download the new CRL and fails to validate the ID certificate of the other SM	None

Known issues and workarounds in Session Manager Release 10.2.0.0

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

ID	Minimum conditions	Visible symptoms	Workaround
ASM-92609	Moderate traffic with users associated with User defined snap-ins in Origination and termination leg	Session Manager restarts	None.
ASM-92593	Upgrade from 7.1.3.8 to 10.2 using CLI method	Intermittent failures in restoring certificates	Run initTM post restore

ID	Minimum conditions	Visible symptoms	Workaround
ASM-92421	Branch visiting user feature enabled and user logs in foreign branch in Sunny day/Rainy day scenario	The list of PPM controllers doesn't include BSM IP Address or FQDN	Configure BSM IP address manually.
ASM-87031	Large number of users registered to the Session Manager	The user registration page intermittently throws connection exception	None
ASM-92590	Aura core system with overlapping dial patterns	Incorrect dial pattern compression and calls cannot be dialed to certain range of extensions	Modify dal pattern to remove overlapping
ASM-92437	Upload Session Manger MIBs to SNMP Browser	The SNMP browser throws error stating Overlapped OIDs were found	Give each var bind unique name
ASM-91096	Import adaptations with duplicated entries of dial patterns in the XML file	Adaptation stops working	Remove duplicated entries
ASM-9117	Session Manager 8.1.3.4 with moderate load	Session Manager throws NumberFormatException and restarts	None
ASM-87752	Session Manager managed by SMGR which has additional storage with NFS and restart SMGR	The NFS configuration need to be manually remounted after an SMGR reboot.	None
ASM-81511	Session Manager with old and new ID certificates have the same Issuer and Root CAs but different CRL Distribution Points (CDP).	SM fails to download the new CRL and fails to validate the ID certificate of the other SM	None

Avaya Aura® System Manager

What's new in System Manager Release 10.2.x.x

The December 23 updated Aura 10.2 KVM OVAs now support the following:

- The KVM OVAs include an *install_vm.py* script to simplify deployment of the KVM OVA
- The *install_vm.py* script now supports the creation of a root login/password
- The CM and AES updated 10.2 KVM OVAs also include support for encryption.

What's new in System Manager Release 10.2.1.1.0

- VMware ESXi 8.0.3 U3 platform support.

What's new in System Manager Release 10.2.1.0

For more information, see ***What's New in Avaya Aura® Release 10.2.x*** document on the Avaya Support site: https://download.avaya.com/css/public/documents/101087359

What's new in System Manager Release 10.2.0.1

System Manager supports French-Canadian localization from 10.2.0.1 onwards.

What's new in System Manager Release 10.2

For more information, see ***What's New in Avaya Aura® Release 10.2.x*** document on the Avaya Support site: https://download.avaya.com/css/public/documents/101087359

Security Service Pack

Security Service Pack

For further information on SSP contents and installation procedures for SMGR 10.2.x, please see **PCN2163S**.

In this release Avaya supports a common version of RedHat Enterprise Linux (RHEL 8.4) for its Avaya Aura platform. Common versions of RPMs are supported and consumed by the components. This results in a change to how security updates are provided for Communication Manager and Application Enablement Services.

CRITICAL: The Security Service Pack installation framework for SMGR has changed from Release 10.1.x onwards.
It is imperative that the instructions in PCN2163S be reviewed for complete steps prior to installation of Security Service Packs on an SMGR 10.2.x system.
The minimum release of SMGR 10.2.x.x that you must be on in order to install the Security Service Packs for SMGR is 10.2.0.0.
The SSP can only be installed via the command line. There is no Solution Deployment Manager (SDM) Client support for SSP installation.
System Manager Solution Deployment Manager does not support the installation of the Avaya Aura 10.2.x Security Service Packs (SSPs).
In order to install the SSP for SMGR 10.2.x.x, you must use the new command ("av-update-os") and follow the detailed instructions in PCN2163S.
NOTE: For Dec 2023, there is no separate Security Service Pack installer for 10.2 release. The Dec 2023 10.2 release is equivalent to the SMGR 10.1 Oct 2023 SSP#18 release with respect to security rpms. There will be separate SSPs released for 10.1 and 10.2 (please note that 10.1 SSPs won't work on 10.2 release).
SSPs cannot be installed on "software-only" deployments.

Managing ASP using SDM in 10.2.x.x

Avaya Solutions Platform S8300 Release 5.1

- To add an ASP S8300 Release 5.1 host in SDM Application Management, use the FQDN only. Do not add an ASP S8300 Release 5.1 host using the IP address.

- After regenerating Certificate for ASP S8300 5.1 host from SDM Application Management, the 'Offer Type' column in the 'Platforms' tab displays the value as "Customer VE" and the 'Platform Type' column in 'Applications' tab does not display any information.
  Ensure that you remove that ASP S8300 5.1 host from the 'Platforms' tab and again add the same host using the 'Platforms' tab.

- Following are the supported profiles for migrating Communication Manager and Branch Session Manager on Avaya Solutions Platform S8300 Release 5.1:
  - For Communication Manager (LSP): CM Main Max User 1000' and 'CM Survivable Max User 1000'
  - For Branch Session Manager: 'BSM Profile 1 Max Devices 1,000'.

  Do not select any other profile that displays in Flexi Footprint drop-down field on the Pre-upgrade Configuration page and Edit Upgrade Configuration page of SMGR-SDM Upgrade Management page.

Required artifacts for System Manager Release 10.2.1.4

Filename	PLDS ID	File size (MB)	S/W Version number	Comments
System_Manager_10.2.1.4_r1021417905.bin	SMGR10214GA01	1557	10.2.1.4.1021417905	SMGR 10.2.1.4 GA bin
Avaya_SDMClient_win64_10.2.1.4.0040855_2.zip	SMGR10214GA02	266	10.2.1.4.0040855	SDM Client for System Manager 10.2.1.4
System_Manager_Datamigration-10.2.0.0.4-83.bin	SMGR10214GA03	7.69	10.2.0.0.4-83	Data Migration utility for System Manager 10.2.X. For more details on Data Migration Utility fixes, see the "Fixes in System Manager

				10.2.1.4” section.

Required artifacts for System Manager Release 10.2.1.3

Filename	PLDS ID	File size (MB)	S/W Version number	Comments
System_Manager_10.2.1.3_r1021317668.bin	SMGR10213GA01	1400	10.2.1.3.1021317668	SMGR 10.2.1.3 GA bin
Avaya_SDMClient_win64_10.2.1.3.0040592_1.zip	SMGR10213GA02	265	10.2.1.2.0040592_1	SDM Client for System Manager 10.2.1.3
System_Manager_Datamigration-10.2.0.0.4-83.bin	SMGR10213GA03	7.7	10.2.0.0.4-83	Data Migration utility for System Manager 10.2.X. For more details on Data Migration Utility fixes, see the “Fixes in System Manager 10.2.1.3” section.

Required artifacts for System Manager Release 10.2.1.2

Filename	PLDS ID	File size (MB)	S/W Version number	Comments
System_Manager_10.2.1.2_r1021217595.bin	SMGR10212GA01	1400	10.2.1.2.1021217595	SMGR 10.2.1.2 GA bin
Avaya_SDMClient_win64_10.2.1.2.0040467_1.zip	SMGR10212GA02	265	10.2.1.2.0040467_1	SDM Client for System

				Manager 10.2.1.2
~~System_Manager_Datamigration-10.2.0.0.4-81.bin~~	~~SMGR10212GA03~~	~~7.7~~	~~10.2.0.0.4-81~~	~~Data Migration utility for System Manager 10.2.X.~~ ~~For more details on Data Migration Utility fixes, see the "Fixes in System Manager 10.2.1.2" section.~~

Required artifacts for System Manager Release 10.2.1.1

Filename	PLDS ID	File size (MB)	S/W Version number	Comments
System_Manager_10.2.1.1_r1021117440.bin	SMGR10211GA01	1400	10.2.1.1_1021117440	SMGR 10.2.1.1 GA bin
Avaya_SDMClient_win64_10.2.1.1.0040422_5.zip	SMGR10211GA02	265	10.2.1.1.0040422_5	SDM Client for System Manager 10.2.1.1
~~System_Manager_Datamigration-10.2.0.0.4-81.bin~~	~~SMGR10211GA03~~	~~7.7~~	~~10.2.0.0.4-81~~	~~Data Migration utility for System Manager 10.2.X.~~ ~~For more details on Data Migration Utility fixes, see the "Fixes in System Manager 10.2.1.1" section.~~

Required artifacts for System Manager Release 10.2.1.0

Filename	PLDS ID	File size (MB)	S/W Version number	Comments
System_Manager_10.2.1.0_r1021117280.bin	SMGR1021GA01	1400	10.2.1.0_1021117280	SMGR 10.2.1.0 GA bin
Avaya_SDMClient_win64_10.2.1.0.0040270_5.zip	SMGR1021GA02	265	10.2.1.0.0040270_5	SDM Client for System Manager 10.2.1.0
~~System_Manager_Datamigration-10.2.0.0.4-80.bin~~	~~SMGR1021GA03~~	~~7.7~~	~~10.2.0.0.4-80~~	~~Data Migration utility for System Manager 10.2.X.~~ ~~For more details on Data Migration Utility fixes, see the "Fixes in System Manager 10.2.1.0" section.~~
AV-SMGR10.2-RHEL8.10-OSUpdate-005.tar.bz2	SMGR1021GA04	715	RHEL 8.10	RHEL 8.10 OS Bundle for SMGR
~~SMGR-10.2.0.0.439670-KVM-4E.ova~~	~~SMGR102GA09~~	~~5925~~	~~010.2.0.0.43967~~	~~SMGR profile 2 KVM OVA~~
~~SMGR-PROFILE3-10.2.0.0.439670-KVM-4E.ova~~	~~SMGR102GA10~~	~~5744~~	~~010.2.0.0.43967~~	~~SMGR profile 3 KVM OVA~~
~~SMGR-PROFILE4-10.2.0.0.439670~~	~~SMGR102GA11~~	~~5785~~	~~010.2.0.0.43967~~	~~SMGR profile 4 KVM OVA~~
SMGR-10.2.0.0.439670-KVM-4E-1.ova	SMGR102GA12	5925	10.2.0.0.439670	SMGR profile 2 KVM OVA
SMGR-PROFILE3-10.2.0.0.439670-KVM-4E-1.ova	SMGR102GA13	5744	10.2.0.0.439670	SMGR profile 3 KVM OVA

SMGR-PROFILE4-10.2.0.0.439670-KVM-4E-1.ova	SMGR102GA14	5785	10.2.0.0.439670	SMGR profile 4 KVM OVA

Note: Replacing the KVM OVAs to cover the script-based deployment method. The procedure is documented in the deployment guide.

Required artifacts for System Manager Release 10.2.0.1

Filename	PLDS ID	File size (MB)	S/W Version number	Comments
System_Manager_10.2.0.1_r1020116918.bin	SMGR10201GA1	1741	10.2.0.1_1020116918.bin	SMGR 10.2.0.1 GA bin
Avaya_SDMClient_win64_10.2.0.1.0039809_2.zip	SMGR10201GA2	266	10.2.0.1.0039809_2	SDM Client for System Manager 10.2.0.1
~~System_Manager_Datamigration-10.2.0.0.4-74.bin~~	~~SMGR10201GA3~~	8	10.2.0.0.4-74	~~Data Migration utility for System Manager 10.2.X.~~ ~~For more details on Data Migration Utility fixes, see the "Fixes in System Manager 10.2.0.1" section.~~ **Note** - Refer Required artifacts for System Manager Release 10.2.1.0 for new DM utility.

Required artifacts for System Manager Release 10.2

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

Filename	PLDS ID	File size (MB)	S/W Version number	Comments
SMGR-10.2.0.0.439670-e70-46E.ova	SMGR102GA01	5100	10.2.0.0.439670	Avaya Aura® System Manager 10.2 (Profile 2) OVA
SMGR-PROFILE3-10.2.0.0.439670-e70-46E.ova	SMGR102GA02	5000	10.2.0.0.439670	Avaya Aura® System Manager 10.2 High Capacity (Profile 3) OVA
SMGR-PROFILE4-10.2.0.0.439670-e70-46E.ova	SMGR102GA03	5300	10.2.0.0.439670	Avaya Aura® System Manager 10.2 High Capacity (Profile 4) OVA

Filename	PLDS ID	File size (MB)	S/W Version number	Comments
AvayaAuraSystemManager-10.2.0.0.439670_v46.iso	SMGR102GA04	3900	10.2.0.0.439670	Avaya Aura® System Manager 10.2 Software Only ISO
System_Manager_R10.2.0.0_S4_102016624.bin	SMGR102GA05	683	10.2.0.0.0416624	Avaya Aura® System Manager 10.2 Mandatory Patch bin file Post OVA deployment / Data Migration
Avaya_SDMClient_win64_10.2.0.0.0439696_9.zip	SMGR102GA06	266	10.2.0.0.0439696	Avaya Aura® SDM client for System Manager 10.2

Note: The deployment of Avaya Aura® applications as Software-only is available but a restricted offer for net new deployments and requires Avaya Aura® BU approval before proceeding. If you have a business requirement to deploy Avaya Aura® as Software-only, please get in touch with your Avaya Sales team. Existing customers using software only deployments continue to be supported.

Required patches for System Manager Release 10.2.x.x

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

Note: Please ensure that you run any required pre-upgrade patch for other Avaya Aura applications before upgrading System Manager.

Note: To preserve full system connectivity, it may be necessary to apply a pre-upgrade patch to each Session Manager in the network BEFORE updating System Manager to release 10.2. This is necessary only if BOTH the following conditions apply:

- Session Manager is on release 8.1.X
- Security Service Pack #12 or #13 have been applied to Session Manger

In this case, you must apply Security Service Pack #14 or later to each Session Manager - prior to initiating the 10.2 upgrade of System Manager.

Download Data Migration Utility

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

Note: The data migration utility is required only if you are upgrading from System Manager 7.x, 8.x. and 10.1.x Ensure that you run the data migration utility only on release 10.2. For more information, see Upgrading Avaya Aura® System Manager.

Filename	PLDS ID	File size (MB)	S/W Version number	Comments
~~datamigration-10.2.0.0.4-72.bin~~	~~SMGR102GA07~~	7.6	10.2.0.0.4-72	Data Migration utility for System Manager 10.2.x. **Note** - Refer Required artifacts for System Manager Release 10.2.1.3 for new DM utility.

Must read

1. Customer should either use an 'Alternate Source' or 'Use Avaya Support Site' option available under User Settings page before doing Refresh Families on SMGR SDM.
2. System Manager Web Console will not be launched If System Manager using certificates that have SHA1 or 1024 RSA keys in the certificate chain. Please check workarounds provided by browsers so that System Manager web console is accessible.
3. If System Manager is upgraded to Release 10.2 and AADS is on Release 10.1.1.1 or earlier, Data replication fails between System Manager and AADS. For more information, see PSN006192u.
4. For rebooting System Manager note the following:

   Important:

   If you configured a NFS mount on System Manager for Session Manager Performance Data (perfdata) collection, then, if and when you reboot/boot System Manager virtual machine, you need to ensure that you manually re-mount the NFS store once the System Manager VM is up and you are able to log in to the VM through SSH. Failure to re-mount the NFS partition will result in the Session Manager perfdata to go, by default, into a folder which is in the root (/) partition of the System Manager file system. This might cause the partition to get full which in-turn might cause issues with the System Manager application.
5. For Release 10.2 GA Installation:
   - Fresh: Deploy 10.2 GA OVA + Apply 10.2 GA Mandatory Patch bin.
   - Upgrade: Deploy 10.2 GA OVA + Execute Data Migration along with 10.2 GA Mandatory Patch bin.

It is required to apply the latest GA patch, Service Pack, or Feature Pack. For information, see PCN2162S

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

     It should only display the message: `Installation of latest System Manager Patch is mandatory`.
7. Perform the following steps to enable EASG on System Manager 10.2:
   - 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`
8. For VMware to VE System Manager Upgrade, remove all the snapshots from old VMware System Manager; otherwise, rollback operation will fail.
9. The versions*.xml is published on PLDS. To download the latest versions.xml file for SUM, search on PLDS using Download PUB ID “SMGRSUM0001” only. Do not use version or product on PLDS in the search criteria.
10. Breeze Element Manager in System Manager 10.2 is called Breeze 3.9.0.0
11. System Manager no longer supports Profile 1 from Release 8 onwards. If you are upgrading from Profile 1 in Releases 7.x, you will have to select Profile 2 or higher while installing R10.x. Note that Profile 2 will require more VM resources compared to Profile 1.
12. If you need to configure IP Office branches beyond 2000 with a single System Manager, please contact Avaya Technicenter.

13. The Update/Patch operation of Avaya Aura elements on Software Only Platform is not supported through System Manager Solution Deployment Manager considering limited support of System Manager Solution Deployment Manager to Avaya Aura elements on Software Only Platform for update/patch, it is recommended to use element CLI method for the update/patch operation.
14. The features to push, view, and delete syslog server profile on virtual machine is supported only for AVP Utilities, System Manager (through Solution Deployment Manager Client), and Session Manager applications.

Software information

Software	Version	Note
Database	Postgres 13.7	Used as a System Manager database.
OS	RHEL 8.4 64 bit	Used as the operating system for the System Manager OVA. It is required in the case of Software Only deployment.
Open JDK	1.8 update 382 64 bit	For Solution Deployment Manager Client, Open JDK 1.8.0-java-1.8.0-openjdk-1.8.0.382
Application Server	WildFly AS 26.1.0 Final	
Supported Browsers	Chrome (minimum version 117.0)	Earlier versions of Chrome are not supported
	Edge (minimum version 117.0)	Earlier versions of Edge are not supported
	Firefox (minimum version 118.0)	Earlier versions of Firefox are no longer supported.
VMware vCenter Server, ESXi Host	7.0.X, 8.0, 8.0 Update 2	Earlier versions of VMware are no longer supported. Avaya Aura® Release 10.2.x supports VMware 8.0 and VMware 8.0 Update 2. Avaya Aura® Release 10.2.x does not support VMware 8.0 Update 1. For information about known issues, see VMware 8.0 Update 1 Release Notes on the VMware website at https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-6vcenter-server-801-release-notes/index.html.
SDM Client Application Server	Tomcat 8.5.39	
SDM Client Supported OS	Windows 7, 8, 10, 11 Windows Server 2016, 2019, 2022	

Adobe Flash EOL impact:

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

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

- Log in to the PLDS at https://plds.avaya.com.
- From the Assets menu, select View Entitlements.
- In the Application field, select System Manager.
- Do one of the following:
  - To search using group ID, in the Group ID field, enter the appropriate group ID.
    Note: All group IDs are numeric without any leading zeros.

- To search using the SAP order number, click Advanced Search, and in the Sales/Contract # field, enter the SAP order number.
- Click Search Entitlements.
  The system displays the LAC(s) in the search results.

Installation for System Manager Release 10.2.x.x

Backing up the software

Refer to the System Manager Backup and Restore section of the *Administering Avaya Aura® System Manager* document at: https://support.avaya.com

Installing the System Manager software

For detailed information about installing System Manager, see Avaya Aura® System Manager deployment documents at: https://support.avaya.com

Upgrading the System Manager software

For detailed information about upgrading System Manager, see *Upgrading Avaya Aura® System Manager* at: https://support.avaya.com

Note 1: If System Manager is upgraded to Release 10.2 and AADS is on Release 10.1.1. or earlier, Data replication fails between System Manager and AADS. For more information, see PSN006192u.

Note 2: To preserve full system connectivity, it may be necessary to apply a pre-upgrade patch to each Session Manager in the network BEFORE updating System Manager to release 10.2. This is necessary only if BOTH the following conditions apply:

1. Session Manager is on release 8.1.X
2. Security Service Pack #12 or #13 have been applied to Session Manager

In this case, you must apply Security Service Pack #14 or later to each Session Manager - prior to initiating the 10.2 upgrade of System Manager.

Troubleshooting the installation

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

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

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

Fixes in System Manager 10.2.1.4

ID	Minimum conditions	Visible symptoms	Issue found in Release
SMGR-78674	User Management	loginname change for user through import doesn't update stationuser column on ipt_station table	10.2.1.1
SMGR-79027	Fault Management	generateSeedData.sh broken on 10.2.1.3	10.2.1.3
SMGR-79113	User Management	10.2.1.x Adding contacts to a user shows duplicated input.	10.2.1.3
SMGR-79119	Fault Management	SMGR log rotation for est_trust_logs.log.	10.2.1.1
SMGR-79121	Geo Redundancy	SMGR 10.2.1.3 GA Geo error on License page of secondary	10.2.1.3
SMGR-79164	User Management	SMGR user AD sync fail if apostrophe occurs in the loginname.	10.2.1.3

SMGR-79012	Communication Management	Localized display name not updated in CM endpoint view page when attached an existing station to a user	10.2.1.1
SMGR-79014	Communication Management	"status" command on basic reports list does not work as expected with invalid qualifier	10.2.1.3
SMGR-78994	Communication Management	INIT sync fails with error "Array index out of range" for CapacityData	10.1.3.3
SMGR-79241	Communication Management	Issues with ip-network-map entries with more than 500 entries Known issue: SMGR-79239 Issues when ip-network-map changed directly on CM and Incremental sync Recommendation: If changes are made on CM, Run INIT sync	10.2.1.3
SMGR-79105	Communication Management	Cannot blank out agent password once set	10.2.01
SMGR-79076	Communication Management	After sort operation on the Synchronization screen, all CM elements disappear	10.1.0.0.2
SMGR-79074	Communication Management	Issues with call-appr and brdg-appr buttons when per button ring control field is enabled	10.2.0.0
SMGR-79254	Communication Management	Audio group board selection across pagination is not working	10.2.1.2
SMGR-79251	Communication Management	Global Endpoint Change duplicate button issue	10.2.1.0
SMGR-79249	Communication Management	Endpoint templates getting corrupted during duplicate and edit operations.	10.2.1.3.1

Fixes in System Manager 10.2.1.3

ID	Minimum conditions	Visible symptoms	Issue found in Release
SMGR-78427	Data Migration	Virtual FQDN(vFQDN) values is not getting updated properly at all places after upgrade from 10.1.x to 10.2.x	10.2.1.1.0
SMGR-78694	Infrastructure	SecurityHardenningOptions --showstate show invalid minimum TLS version on System Manager 10.2.x release	10.2.0.1.0
SMGR-78612	User Management	Reset password button is not working in self-provisioning workflow for certificate-based login mode.	10.2.1.2.0
SMGR-78524	Communication Manager Management	Editing Scheduled details through "edit report" scenario, doesn't push updated details to scheduler.	10.2.0.1.0
SMGR-78530	Communication Manager Management	"Redirect on No Answer (rings)" field on hunt form cannot be reset to blank from System Manager.	10.1.3.5.0

SMGR-78527	Communication Manager Management	Provided validation to block Comma(,) in Button labels.	10.2.0.1.0
SMGR-78593	Communication Manager Management	Support below basic report commands for media servers. 1. list media-server, 2. display media-server, 3. list measurements ip dsp-resource ms summary yest 4. list measurements ip dsp-resource ms summary today	10.1.3.2.0
SMGR-78646	Communication Manager Management	Missing "status media-server" command in Basic report	10.1.3.2.0
SMGR-78596	Communication Manager Management	Notify Sync Job gets corrupted during upgrades.	10.2.1.2.0
SMGR-78649	Communication Manager Management	Endpoint values getting reset to default values when endpoint editor is opened more than once.	10.2.0.0.0

Fixes in System Manager 10.2.1.2

ID	Minimum conditions	Visible symptoms	Issue found in Release
SMGR-77236	Geo Redundancy	Geo Redundancy Health goes down intermittently.	10.1.3.3.0
SMGR-77745	Administrator	Prevent Auto Population of login password when user ID is provided.	10.2.0.0.0
SMGR-77927	Backup and restore	Unable to restore system backup due to multiple requests being processed during restore process.	10.2.0.1.0
SMGR-78005 SMGR-71426	Administrator	Unable to re-configure UCM service due to “systemctl status” and file clean issues.	10.2.1.0.0
SMGR-78164	Licenses Manager	Licensing Manager doesn't handle duplicate license requests from the same application with the same request ID.	10.1.3.2.0
SMGR-78162	Infrastructure	Encryption Enabled deployments require 30+ minutes to come up and run after reboot.	10.2.1.1
SMGR-78253	Geo Redundancy	Geo Redundancy configuration failed if system is configured with 3rd party certificates.	10.2.1.0.0
SMGR-78273	Security Management	Certificate Renewal utility is not working if log level is enabled to Info Level.	10.2.1.2.0

SMGR-78252	User Management	User Provisioning Rule, with Messaging Profile enabled, will fail for user subsequent updates.	10.1.3.4.0
SMGR-78286	Administrator	A numeric digit is not allowed as the starting character of the host name or domain name for an external authentication server.	10.2.1.0.0
SMGR-78295	Schedular Management	Job "PurgeAgedExportUserJobDataRule" execution fails.	10.2.0.1.0
SMGR-78404	Geo Redundancy	Geo-redundancy file replication failure observed in cross platform deployments.	10.2.1.1.0
SMGR-77953	Communication Management	Blank page intermittently while viewing CM/Network/ARS digit conversion pages.	10.2.0.1.0
SMGR-78178	Communication Management	Incremental sync does not execute after installing any patches.	10.2.1.0.0
SMGR-78249	Communication Management	Clicking on Migrate Endpoints button does not work properly.	10.2.1.0.0
SMGR-75082	Communication Management	Broadcast of announcement from MG to AMS Fails.	10.1.3.1.0
SMGR-78311	Communication Management	Login Name change through LDAP sync OR xml import fails if user is associated with Communication Manager profile.	10.2.1.1.0
SMGR-78366	Communication Management	Cannot add announcement from SMGR which includes characters “wav” as part of an announcement name.	10.2.0.1.0
SMGR-78456	Communication Management	When creating agent profiles by selecting Agent profile as "Agent" and selecting "Use existing agents", if you display extension ranges the endpoint extension ranges are displayed and not existing Agent login IDs.	10.1.0.0.0

Fixes in System Manager 10.2.1.1

ID	Minimum conditions	Visible symptoms	Issue found in Release
SMGR-77759	Infrastructure	changePublicIPFQDN & changeIPFQDN utilities not working properly.	10.2.0.0.0
SMGR-77747	Infrastructure	Provide utility to disable “hmac-sha1’ algorithm.	10.1.3.3.0
SMGR-77524	Infrastructure	changeIPFQDN utility should abort if etc/hosts file doesn’t have System manager entries.	10.2.0.0.0
SMGR-77452	Infrastructure	exportUpmGlobalsettings.sh is not working on 8.1.x and 10.x SMGR.	10.1.3.1.0
SMGR-77439	Geo Redundancy	Log Messages dumping every 5 minutes in log viewer even after the GR replication is successfully enabled.	10.2.0.1.0
SMGR-77261	Data Migration	check the values of FQDN and public interface FQDN (eth1) while configuring OOBM	10.2.0.1.0

SMGR-76983	Data Migration	Upgrade to 10.2.x fails when OOBM is configured.	10.2.0.1.0
SMGR-77242	Upgrade Management	Host Refresh fails after vCenter mapping.	10.2.0.0.0
SMGR-77519	Upgrade Management	SDM System Manager upgrades hang when network name has a network label with more than 50 characters.	10.2.0.1.0
SMGR-52765	Data Replication Management	During initial load JMX connection attempt timeout not logged, and no attempt made to cleanup connection attempt threads	8.1.0.0.0
SMGR-77042	User Management	Custom user cannot view/edit/add/delete public contacts.	10.1.3.2.0
SMGR-77635	Trust Management	Unable to create Entity Class if Email Configuration Properties under SPM is blank	10.1.3.1.0
SMGR-70288	OfficeLinx Management	Officelinx data should not be cleared from SMGR if SMGR is not able to retrieve data from officelinx server.	8.1.3.4.0
SMGR-77564	Communication Management	Global Search component does not work after Breeze EM installation.	10.1.3.3.0
SMGR-77771	Communication Management	Favorites, Labels and profiles data is not sent from SMGR to SM when add user operation is executed with "use existing endpoint" and H323 station is changed from H323 to SIP	10.1.3.4.0
SMGR-77853	Communication Management	Converting H323 endpoints (with dual reg flag enabled) to SIP causing issues.	10.1.2.0.0
SMGR-77678	Communication Management	Detailed report for VDN doesn't include all VDNs in the report.	10.1.3.1.0
SMGR-77839	Communication Management	Detailed report for endpoint fails if building field is included.	10.1.3.0.1
SMGR-78028, SMGR-77828	Communication Management	SMGR web API is not working for template change scenarios.	10.1.3.1.1
SMGR-78024	Communication Management	Generate alarm for INIT/INCR/NOTIFY sync failures	10.1.3.1.0

Fixes in System Manager 10.2.1

ID	Minimum conditions	Visible symptoms	Issue found in Release
SMGR-75104	User Management	"No data" on Manage User page after committing OR canceling removing CM comm profile for user	10.1.3.1
SMGR-76039	User Management	Time zone field on user identity page does not get updated post DST change.	10.1.2.0
SMGR-76901	User Management	Error when using "Use Existing Endpoints" option for converting H323 endpoint to J179 while user add operation	10.1.3.1

SMGR-75466	User Management	Custom user who doesn't have permissions for Alarm page can view and check alarms by clicking Alarm Widget on Home page.	10.1.3.2
SMGR-75435	User Management	Custom user with view only permissions to Directory synchronization can edit/delete LDAP configuration and view option is missing from Directory Synchronization page.	10.1.3.1
SMGR-75085	User Management	Session Logout Warning message(pop-up) missing from System Manager 8.1.x and 10.x release	8.1.3.8
SMGR-71870	User Management	Edge and Chrome browsers give "Leave site?" popup when adding/editing VDNs/Announcements/Endpoint templates	10.1.0.1
SMGR-61975	User Management	Unable to login to SMGR CLI using users that are created by User Management after you enabled Command Line access for them.	8.1.3.1
SMGR-74757	User Management	"no action" on commit button click during duplicate user operation.	10.1.3.1
SMGR-74296	User Management	Custom users with view only permissions can add, edit and delete UPRs	10.1.3.1
SMGR-76860	Administration	Null Pointer exception while accessing selfprovisioning with bad OOBM configuration.	10.1.3.3
SMGR-75853	Administration	Unable to delete announcement from global search options.	10.1.3.2
SMGR-76857	Officelinx Element Management	Officelinx communication profile creation issue if mailbox # received with dashes from LDAP during LDAP sync activity.	10.1.3.1
SMGR-75946	OfficeLinx Element Management	Officelinx password resets to last (which is set from SMGR) password during AD sync during some rollback scenarios.	10.1.3.0
SMGR-75086	Officelinx Element Management	User update through LDAP sync, failure noticed in case user is associated with officelinx communication profile.	10.1.3.1.1
SMGR-75840	Backup and Restore Management	Restore backup is failing in case backup was taken from System where sdpdefault service certificate replaced with external CA.	10.2.0.0
SMGR-75518	Security Management	Access to internal resources of SMGR via SSRF vulnerability	10.1.3.0
SMGR-50333	Security Management	After running changeVFQDN, old vFQDN still appears in CRL Distribution Points & Authority Information Access	8.0.1.1
SMGR-74194	Security Management	Administrative User unable to run the command ‘manageEntityClassWhitelist’ when CLI access is enabled through UI.	10.1.3.3
SMGR-75468	Software Upgrade Management	CM_Custom_Patch option missing from SDM Sync Files	10.1.3.0
SMGR-73979	Infrastructure	After reboot, Encrypted SMGR deployment is taking 30 minutes to enter passphrase code for boot	10.1.3.0

SMGR-75463	Infrastructure	‘status_vm’ showing incorrect information for Software-Only Installation	10.1.3.0
SMGR-75066	Infrastructure	Unable to change the Subnet on SMGR 10.x using changeIPFQDN utility.	10.1.3.1
SMGR-75616	Self Provisining	No option to reset the communication profile password through self-provisioning if certificate authentication is used	10.1.3.2
SMGR-76034	Licensing	Licensing Page is not launching when access via ESAG/administrator user in spite of earlier session is closed.	10.1.3.3
SMGR-74541	Geo Redundancy	Geo shows enabled even though database replication is not working.	10.1.3.1
SMGR-76996	Geo Redundancy	Unable to disable Geo Redundancy from Primary SMGR in spite of secondary was in disabled state.	10.1.3.2
SMGR-74769	Fault Management	Server.log shows Unable to retrieve user information. Users file is corrupted	10.1.3.1
SMGR-75034	Schedular Management	UserMgmtJob failed to execute with error "Caused by: java.lang.NoClassDefFoundError: com/nortel/ems/mgmt/quantum/userRoleManagement/dto/UserInfo"	10.1.0.0
SMGR-74267	Fault Management	Log Retention on SMGR Not working	10.1.2.0
SMGR-75609	Data Migration	8.1.3.6 to 10.1.2.0 upgrade fails because of migration scripts.	10.1.2.0
SMGR-76076	Data Migration	Block data migration in case of eth0 value missing.	10.2.0.0
SMGR-75301	Data Migration	Cannot edit user after upgrade from 8.1.3.x to 10.2 due to Conferencing stale entries in the database.	10.2.0.0
SMGR-75437	Data Migration	Data migration from 7.1.x to 10.2.x fails in some scenarios.	10.2.0.0
SMGR-75610	Communication Manager	"Next Path Number" is being auto filled when editing/adding Coverage Path in SMGR	10.1.3.2
SMGR-76929	Communication Manager Management	Users not able to add OR edit coverage path from SMGR Native page	10.2.0.1
SMGR-75357	Communication Manager	Due to stale entry in database if SIP endpoint is removed from CM directly and SMGR doesn't show it in available extension list.	10.1.3.1
SMGR-75374	Communication Manager	Feature button #1 go blank on import and webservice scenarios.	10.1.2.0

Fixes in System Manager 10.2.0.1

ID	Minimum conditions	Visible symptoms	Issue found in Release

SMGR-75086	OfficeLinx Element Management	User with officelinx communication profile update failure with LDAP synchronization.	10.1.3.1.1
SMGR-73984	Geo Redundancy Management	Database partition size increase in one of the case where GEO is auto disabled.	10.1.3.0
SMGR-73834	Geo Redundancy Management	Geo Auto-Disable gets triggered when System Manager hostname includes capitals letters.	10.1.3.1
SMGR-74457	Infrastructure Management	CVE-2021-23926 -XMLBeans 3.0.0 upgrade	10.1.x
SMGR-74443	Infrastructure Management	Updating DNS entries using “changeIPFQDN” utility does not work as expected.	10.1.3.1
SMGR-74282	Infrastructure Management	System Manager is sending out DNS query to public root hints server list.	10.1.2.0.1
SMGR-73759	Inventory Management	Unable to Un-assign CM Cluster from AES Element in Inventory - Manage Elements.	10.1.0.2
SMGR-72106	Inventory Management	Unable to disable SNMP from Manage Elements for CM record.	10.1.0.0, 8.1.3.6
SMGR-75055	Schedular Management	Disable “sys_ConfRefreshConfig” Job if MX/Meeting Exchange and Conferencing 6.0 device type is not configured on SMGR.	10.1.3.2
SMGR-75216	Upgrade Management	IPO branch upgrade to 12.0.0.0 release failure in SMGR 10.2 release.	10.2.0.0
SMGR-74774	Upgrade Management	SMGR upgrade failure when upgrade done from 8.1.12 and higher release to 10.1 or 10.2 release.	8.1.3.5
SMGR-74420	Administration Management	External Authentication Page is blank after upgrade to 10.1.x or 10.2.x release.	10.1.3.0
SMGR-70759	User Interface Management	Cannot resize the pop-up and must use scroll bars to get to the import button.	8.1.3.3
SMGR-74671	User Management	OfficeLinx communication profile mailbox number shows wrong value when creating user through UPR on SMGR 10.1.x and 10.2 release	10.1.3.2
SMGR-74494	Self-Provisioning Management	Self-Provisioning password reset email contains OOBM FQDN(eth0) instead of Public FQDN(eth1) when OOBM is configured.	10.1.2.0
SMGR-74891	User Management	The User's OfficeLinx Communication Profile is disabled after editing & committing on existing user in SMGR 10.1.x and 10.2 release	10.1.3.2
SMGR-75080	User Management	Old browser supported version showing on self-provisioning page	10.1.3.2

SMGR-74476	User Management	Global Search stopped working for custom users after SMGR upgraded to 10.1.3.1 + hotfix release.	10.1.3.1
SMGR-74449	Infrastructure Management	Added pre-check in patch installation to make sure database is connected when super user mode is enabled, if not then abort patch installation.	10.1.x
SMGR-72420	Geo Redundancy Management	File Replication flag is displayed incorrect on Secondary after executing “pairIPFQDNchange” utility.	8.1.3.7
SMGR-74493	Licensing Management	Support to install 50 licenses file per SMGR(WebLM) server.	10.1.3.0
SMGR-74967	Communication Manager Management	'Trunk' and 'Off-pbx-telephone extension' missing from basic status reports in 10.1.3.x and later	10.1.3.0
SMGR-74861	Communication Manager Management	SMGR doesn't show MWI status for "Status station" command	10.1.2.0
SMGR-74539	Communication Manager Management	Broadcast announcements don’t work if AMS is configured with ipv6 address.	10.1.3.1.0
SMGR-74444	Communication Manager Management	Appropriate language is not populated in the "Multibyte Language" field through User Management operations	10.1.3.1.0
SMGR-74409	Communication Manager Management	"Turn on mute for remote off hook attempt" and few more fields missing from 10.1.x Endpoint template fields	10.1.3.0
SMGR-74248	Communication Manager Management	Incremental sync stops working after 10.1.3.x upgrade	10.1.3.1.0
SMGR-74218	Communication Manager Management	CM synch radio buttons are grayed out for first attempt on opening Synchronization page.	10.1.2.0
SMGR-73978	Communication Manager Management	If a SIP user is added with CM endpoint profile of type Agent, then if we edit the Agent and save it fails with error entity not managed	10.1.3.1.0
SMGR-72521	Communication Manager Management	In Report Generation Page, in dropdown of application field, there aren't any CM displayed for the user to choose	8.1.3.7
SMGR-71870	User Interface	Edge and Chrome browsers give "Leave site?" popup when adding/editing Announcement and Endpoint templates	10.1.0.1

Fixes in System Manager 10.2.0.0

The following table lists the fixes in this release:

ID	Minimum conditions	Visible symptoms	Issue found in Release
SMGR-72414	Geographic Redundancy Management	Secondary System Manager shows licensing error for Geographic Redundancy due to duplicate license	7.1.3.3
SMGR-73045	Self-Provisioning Management	"Reset Password" button on self-provisioning no longer works correct	8.1.3.5.1
SMGR-72574	Infrastructure Management	Duplicate http headers	10.1.0.1
SMGR-71854	Infrastructure Management	Memory leak due to invalid SNMP cloned user data.	8.1.3.3
SMGR-69122	User Management	AD-sync wipes all secondary communication profile set values	10.1.0.0
SMGR-69526	Administration Management	User Certificate Authentication broken	8.1.3.3
SMGR-67880	Installer Management	OVA to OVA upgrade fails if old System Manager's fully qualified domain name is a subset of new System Manager's fully qualified domain name	8.1.3.1
SMGR-67962	User Management	Advanced user search filter gives wrong results when both E164 handle, and first name are added to filter	8.1.3.3
SMGR-69288	User Management	Group details vanish if you switch to any other tab post entering it.	8.1.3.3
SMGR-69538	Console Management	Navigation Menu Shortcuts on the System Manager Dashboard are not intuitive	8.1.3.3
SMGR-69577	User Management	Able to export more users that available limit for a particular role	8.1.3.3
SMGR-69921	Administration Management	Users created using Graphical User Interface with option "Enable Command Line Access" are not able to login to Command Line Interface post upgrade	8.1.2.0.1
SMGR-70096	Infrastructure Management	ChangeIPFQDN is not updating new FQDN value in Database configuration files	8.1.3.3
SMGR-71421	Geo Redundancy Management	GEO enabled status shows successful while it has failed when checked in backend logs	8.1.3.3
SMGR-55507	Alarming Management	Logs database should be part of audit partition post upgrade.	8.1.2.0.1
SMGR-72539	Administration Management	Old User Management menu is shown post migration.	8.1.3.1

ID	Minimum conditions	Visible symptoms	Issue found in Release
SMGR-71410	User Management	Clear Text password not sent through email for Self-Provisioning when Password is reset	10.1.0.1
SMGR-71824	Geo Redundancy Management	Enable replication fails on secondary System manager	10.1.0.2.1
SMGR-72515	Upgrade Management	Data migration fails on 10.1.x release when different IP address/ Fully Qualified Domain Name is used	10.1.0.0
SMGR-70649	Console Management	Unable to select more than 500 users	8.1.3.0
SMGR-72824	Multi Tenancy Management	Automatic creation of tenant with dummy user import fails	10.1.0
SMGR-70760	User Management	"Export User to Excel" operation doesn't export communication Manager profile data	8.1.3.5
SMGR-69748	Infrastructure Management	Web console does not come up in case CRL file is expired and CRL check is set to “BEST_EFFORT”.	10.1.0.1
SMGR-67189	User Management	Wrong response when calling create user management web service	8.1.3.1
SMGR-73887	User Management	Self-provisioning login not possible anymore through reverse proxy	10.1.3.0
SMGR-73876	OfficeLinx Management	Officelinx Mailbox is getting created without leading zeros	10.1.3.0
SMGR-71601	Communication Manager Management	Issue with "Buttons per Page" value for cs1k set type CS1k-39xx	10.1.0.1
SMGR-70758	Communication Manager Management	Disassociate User utility does not work properly	8.1.3.4
SMGR-72219	Communication Manager Management	Issue with title/header while editing VDN using Global search component.	10.1.0.1.1
SMGR-68788	Communication Manager Management	Invalid handle should not be accepted to sip URI.	8.1.3.0
SMGR-68244	Communication Manager Management	Some role permission NOT working properly	8.1.2.0
SMGR-68448	Communication Manager Management	Issues with "Calculate Route Pattern" and "SIP Trunk" fields on CM comm profile	8.1.3.3

ID	Minimum conditions	Visible symptoms	Issue found in Release
SMGR-67518	Communication Manager Management	Missing options in RBAC configurations	8.1.3.1
SMGR-68725	Communication Manager Management	Backup wave files operation fails for Audio Group	8.1.3.3
SMGR-72825	Communication Manager Management	Detailed endpoint report generated by custom user doesn't have details of all endpoints for which it has access	10.1.0.2
SMGR-72204	Communication Manager Management	Display multifrequency-signaling appears twice in the object list	10.1.0.2
SMGR-69742	Communication Manager Management	Cannot upload OR backup announcements having '&' char in the filename	8.1.3.3
SMGR-67872	Communication Manager Management	Custom role with CM endpoint edit permission cannot edit/assign buttons after upgrade from 8.1.3.1 to 8.1.3.3 release.	8.1.3.3
SMGR-71427	Communication Manager Management	Missing field "Attribute" in the Agent detailed reports	10.1.0.2
SMGR-67530	Communication Manager Management	"No data found" for detailed reports for VDN and Endpoints	8.1.3.3
SMGR-72214	Communication Manager Management	Location field wrong; reports "1" for every location	10.1.0.2
SMGR-71726	Communication Manager Management	Missing Endpoint "site data" fields in detailed reports	10.1.0.2
SMGR-67158	Communication Manager Management	Change holiday-table in element cut through does not display two digits	8.1.3.2
SMGR-70516	Communication Manager Management	Loading Bulk edit page is very slow from User Management	8.1.3.3
SMGR-66927	Communication Manager Management	Announcement Backup fails if it takes more than 5 minutes to complete.	8.1.3.2
SMGR-70841	Communication Manager Management	Default values of the fields "Delete on Unassign from User or on Delete User" and "Override Endpoint Name and Localized Name" is lost when creating a new User using UPR.	8.1.3.3

ID	Minimum conditions	Visible symptoms	Issue found in Release
SMGR-70084	Communication Manager Management	Reports Generation produced 0 KB File Size if we remove any "Reserve Skill Level" field or "Skill Level" field from detailed Agent report	10.1.0.1
SMGR-72551	Communication Manager Management	Cannot add abbr-dial button from SMGR if MLPP feature is enabled on CM system-parameters customer-option form.	8.1.3.3
SMGR-69763	Communication Manager Management	.wav files gets stuck on remote servers in announcements backup failure scenarios and leads to error "SCP - Permission denied" on next announcements backup announcements.	8.1.3.3
SMGR-59936	Communication Manager Management	CM sync fails at cleaning step while processing "change extension-station xxx" command from CM command history	8.1.3.1
SMGR-69575	Communication Manager Management	Notify sync job marked as failed in scheduler with exceptions in logs and Database is updated with incorrect value.	10.1.0.0
SMGR-72817	Communication Manager Management	While assigning an additional profile set - "Delete on Unassign from User or on Delete User" and "Override Endpoint Name and Localized Name" are disabled by default	8.1.3.7
SMGR-69778	Communication Manager Management	Element Cut Through of abbreviated cmd "li tra sta 8000" stuck/hang, while full cmd "list trace station 8000" fine.	8.1.3.4
SMGR-69071	Communication Manager Management	"Away Timer Value" on profile settings tab is only allowed from 5 to 480 but phone accept till 999	8.1.3.3
SMGR-70090	Communication Manager Management	Incremental sync fails if Notify sync is enabled for CM and hunt groups are deleted from CM.	8.1.2.0
SMGR-71598	Communication Manager Management	Detailed report generation for Endpoint hangs if Main Buttons, Feature Buttons, Expansion/Module Button and Softkeys Buttons fields are selected.	10.1.0.2
SMGR-68210	Communication Manager Management	Notify Sync/Incremental sync fail to process "change extension-station" command if extension value includes "-".	8.1.3.3
SMGR-71830	Communication Manager Management	Updated SIP Trunk field is not reflected SMGR when the change is made via Endpoint Cut Through	8.1.3.5
SMGR-68107	Communication Manager Management	Cursor moves back initial entry while typing inside CM element cut-through "Command" line.	8.1.3.3

ID	Minimum conditions	Visible symptoms	Issue found in Release
SMGR-73811	Communication Manager Management	Import CM endpoint fails for set type 2410 if feature buttons are populated on excel sheet	10.1.3.0
SMGR-68105	Communication Manager Management	Element cut-through columns show wrong values for "list station" command	8.1.3.3
SMGR-67099	Communication Manager Management	Running an on-demand report from an existing report definition which already has a schedule will alter that existing schedule.	8.1.3.1.1
SMGR-67947	Communication Manager Management	IP Network Map entries not showing up in SMGR even though it’s programmed in CM	10.1.0.0
SMGR-71295	Communication Manager Management	Data for "System" column is wrong in Report when "list registered-ip-station" report is generated with qualifier.	10.1.0.1
SMGR-69561	Communication Manager Management	Changing Set type using Global Endpoint Change operation for H323 station doesn't work.	8.1.3.4
SMGR-71595	Communication Manager Management	"Status socket-usage" report shows data for only one CM when multiple CMs are selected.	10.1.0.2
SMGR-70035	Communication Manager Management	SMGR not displaying "Select Destination for Broadcasting Announcements" list while broadcast announcement operation initiated.	8.1.3.3
SMGR-70117	Communication Manager Management	Adding additional parameters in detailed agent report columns leads to showing wrong values in columns	10.1.0.1
SMGR-62039	Communication Manager Management	SMGR opens multiple SAT sessions on duplex CM instead of using existing connections.	8.1.3.2
SMGR-67010	Communication Manager Management	“Receive Analog incoming Call ID” field is missing on SMGR for CO trunk.	8.1.3.1
SMGR-72581	Communication Manager Management	After INIT sync special German characters like ö and ü disappear from the name.	8.1.3.5
SMGR-72128	Communication Manager Management	CM sync is unable to sync all paging group member data after SA9096 is enabled.	10.1.0.2
SMGR-67361	Communication Manager Management	Activating "Dual Registration" fails if SIP user is converted from SIP to H323.	8.1.3.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
SMGR-67654	Communication Manager Management	Edit Endpoint missing field validation msg/hints/tool-tips after upgrade from 7.1.3.4 to 8.1.3.2	8.1.3.2.1
SMGR-72166	Communication Manager Management	Duplicate/non-functional detailed reports in dropdown ('trunk'; 'off-pbx-telephone').	10.1.0.2
SMGR-72200	Communication Manager Management	Group extension field wrong; reports erroneous data	10.1.0.2
SMGR-72197	Communication Manager Management	Location field wrong; reports erroneous data for every location	10.1.0.2
SMGR-70168	Communication Manager Management	Default detailed agent report doesn't have correct values in all columns	10.1.0.1
SMGR-67519	Communication Manager Management	Broadcast Announcements for a Media server recreated all old Announcements which has been deleted early	8.1.3.1
SMGR-72123	Communication Manager Management	Cannot save "isdn" trunk changes using SMGR native pages if SA8983 is enabled	10.1.0.1
SMGR-72819	Communication Manager Management	Inconsistent data on "list trunk" reports if multiple reports are scheduled to run at the same time	10.1.0.1
SMGR-71599	Communication Manager Management	Detailed report generation for Agent fails if "Agent Template ID Name" field is selected.	10.1.0.2
SMGR-72363	Communication Manager Management	Multiple display reports that cannot take qualifier in SAT require a qualifier (blank character) to execute.	10.1.0.2
SMGR-69743	Communication Manager Management	“Edit Extension” feature on SMGR does not release the old extension to available pool.	8.1.3.4
SMGR-67420	Communication Manager Management	CM-SMGR Sync Status stuck in "SM asset IP changed"	8.1.3.3
SMGR-70154	Communication Manager Management	Using an alias (J189) cannot enable more than 9 favorite buttons on the SMGR.	8.1.3.3
SMGR-66880	Communication Manager Management	When multiple CMs are selected, Element cut-through always defaults to first selected CM.	8.1.3.2

Known issues and workarounds in System Manager in Release 10.2.1.4

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-70505	Communication Manager Management	Duplicate station operation from user management creates 3 call-appr always even if original user has only one or two.	Make changes in button assignment for Manage Endpoint Page.
SMGR-72183	Communication Manager Management	Creating new user using same set type template which already has user with custom language, shows custom language.	Manually change the user preferred language settings.
SMGR-73962	Communication Manager Management	Global endpoint change doesn't have new set type of J1xx phones.	Use Edit station for changing set type.
SMGR-77499	Trust Management	Trust re-establishment is failing for SMGR in DoD mode.	
SMGR-75065	Communication Manager Management	Error message while broadcasting announcement.	Select the board first and then select the announcement

Known issues and workarounds in System Manager in Release 10.2.1.3

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-70505	Communication Manager Management	Duplicate station operation from user management creates 3 call-appr always even if original user has only one or two.	Make changes in button assignment for Manage Endpoint Page.
SMGR-72183	Communication Manager Management	Creating new user using same set type template which already has user with custom language, shows custom language.	Manually change the user preferred language settings.
SMGR-73962	Communication Manager Management	Global endpoint change doesn't have new set type of J1xx phones.	Use Edit station for changing set type.
SMGR-77499	Trust Management	Trust re-establishment is failing for SMGR in DoD mode.	
SMGR-75065	Communication Manager Management	Error message while broadcasting announcement.	Select the board first and then select the announcement

Known issues and workarounds in System Manager in Release 10.2.1.2

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-78448	Communication Manager Management	"Redirect on No Answer (rings)" field on hunt form cannot be reset to blank from SMGR	
SMGR-77499	Trust Management	Trust re-establishment is failing for SMGR in DoD mode	
SMGR-70505	Communication Manager Management	Duplicate station operation from user management creates 3 call-appr always even if original user has only one or two	Make changes in button assignment for Manage Endpoint Page.
SMGR-72183	Communication Manager Management	Creating new user using same set type template which already has user with custom language, shows custom language	Manually change the user's preferred language settings.
SMGR-73962	Communication Manager Management	Global endpoint change doesn't have a new set type of J1xx phones.	Use Edit station for changing the set type.
SMGR-75065	Communication Manager Management	Error message while broadcasting an announcement	Select the board first and then select the announcement
SMGR-78427	Data Migration	vFQDN not getting updated properly at all places after DM from 10.1.x to 10.2.x	Manually update the VFQDN value for System Manager entry in the rts_attribute table

Known issues and workarounds in System Manager in Release 10.2.1.1

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-77 236	Geo Redundancy	Geo Redundancy Health goes down intermittently.	Restart System Monitor service
SMGR-77 499	Trust Management	Trust re-establishment is failing for SMGR in DoD mode	
SMGR-70 505	Communication Manager Management	Duplicate station operation from user management creates 3 call-appr always even if original user has only one or two	Make changes in button assignment for Manage Endpoint Page.
SMGR-72 183	Communication Manager Management	Creating new user using same set type template which already has user with custom language, shows custom language	Manually change the user preferred language settings.
SMGR-73 962	Communication Manager Management	Global endpoint change doesn't have a new set type of J1xx phones.	Use Edit station for changing set type.
SMGR-77 953	Communication Manager Management	Blank page intermittently while viewing CM/Network/ARS digit conversion page	

Known issues and workarounds in System Manager in Release 10.2.1.0

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-77025	Infrastructure	Provide options to disable hmac-sha1 algorithm for ssh communication.	
SMGR-77236	Geo Redundancy	Geo Redundancy Health goes down intermittently.	
SMGR-76983	Data Migration	Upgrade to 10.2.x fails when OOBM is configured with incorrect parameters in older release.	Disable OOBM on previous release, Take a new backup and then upgrade with new Backup to 10.2.x and configure OOBM again.
SMGR-70505	Communication Manager Management	Duplicate station operation from user management creates 3 call-appr always even if original user has only one or two	Make changes in button assignment for Manage Endpoint Page.
SMGR-72183	Communication Manager Management	Creating new user using same set type template which already has user with custom language, shows custom language	Manually change the user preferred language settings.
SMGR-73962	Communication Manager Management	Global endpoint change doesn't have new set type of J1xx phones.	Use Edit station for changing set type.
SMGR-77499	Trust Management	Trust re-establishment is failing for SMGR in DoD mode	
SMGR-77532	Backup and Restore	Restore of backup is failing incase backup is taken from System Manager having all Identity Certificates are signed by external CA	Only Replace Container TLS certificate with external CA and then take new backup before next restore attempt.

Known issues and workarounds in System Manager in Release 10.2.0.1

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-75294	Out Of Band Management (OOBM)	SMGR eth0 SSH stops after converting SMGR to OOBM states	Stop firewall service and access eth0 network via SSH
SMGR-74406	Security Updates	systemd security and bug fix update(http://rhsa-2023:3837/)	
SMGR-74769	Infrastructure Management	Server.log shows “Unable to retrieve user information. Users file is corrupted”	
SMGR-75066	Infrastructure Management	Unable to change the Subnet on SMGR 10.x	
SMGR-74194	Infrastructure Management	GUI User unable to run the command “manageEntityClassWhitelist” when CLI is enabled.	
SMGR-73980	Infrastructure Management	Cannot enable ‘Command Line Access’ on secondary SMGR.	
SMGR-75034	Scheduler Management	Job “UserMgmtJob” failed to execute with error "Caused by: java.lang.NoClassDefFoundError: com/Nortel/ems/mgmt/quantum/userRoleManagement/dto/UserInfo" in log file “server.log”	
SMGR-74726	Geo Redundancy Management	GR shows enabled even though Database replication is not working.	Make sure Database Identity Certificate (i.e., psqlSU CN as 'MGMTDB’.
SMGR-70505	Communication Manager Management	Duplicate station operation from user management creates 3 call-appr always even if original user has only one or two	Make changes in button assignment for Manage Endpoint Page.
SMGR-72183	Communication Manager Management	Creating new user using same set type template which already has user with custom language, shows custom language	Manually change the user’s preferred language settings.
SMGR-73962	Communication Manager Management	Global endpoint change doesn't have a new set type of J1xx phones.	Use Edit station for changing set type.

Known issues and workarounds in System Manager in Release 10.2.0.0

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

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-74218	Communication Manager Management	CM synch radio buttons are grayed out for first attempt.	Refresh the table.
SMGR-72183	Communication Manager Management	Creating new user using same set type template which already has user with custom language, shows custom language	Manually change the user preferred language settings.
SMGR-73676	Software Deployment Manager	"Commit upgrade" still loading after upgrade SM success.	Remove host manager of SM from Application Management. After that, add that host again and re-establish connection the SM to get latest status
SMGR-73962	Communication Manager Management	Global endpoint change doesn't have new set type of J1xx phones.	Use Edit station for changing set type.
SMGR-74406	Security Updates	systemd security and bug fix update(http://rhsa-2023:3837/)	
SMGR-75353	User Interface	Edge and Chrome browsers give "Leave site?" popup when adding/editing VDNs/Messaging templates	

Solution Deployment Manager Adopter Matrix

Solution Deployment Manager Adopter Matrix	Adopting Product (System Manager Release 10.2)											
System Manager Solution Deployment Manager – Centralized Functionality	Avaya Solutions Platform (ASP 130/S8300)	System Manager	Session Manager	Communication Manager	CM Adjuncts (MM, Gateways)	Branch Session Manager	Breeze	Secure Access Gateway	WebLM	Application Enablement Services	Media Server	Session Border Control (SBCE 8
OVA Deployment R 10.2 (Configuration and Footprint)	n/a	Y(only through SDM client)	Y	Y	n/a	Y	Y	Y	n/a	Y	Y	Y
Patching Deployment (hotfixes)	Y [Other than ASP hosting System Manager]	Y(only through SDM client)	Y	Y	n/a	Y	N	N	Y	Y	N	N
Custom Patching Deployment	n/a	n/a	Y	Y	n/a	Y	N	N	Y	Y	N	Y
Service/Feature Pack Deployment	Y [Other than ASP hosting System Manager]	Y(only through SDM client)	Y	Y	n/a	Y	N	N	Y	Y	N	N

Solution Deployment Manager Adopter Matrix	**Adopting Product (System Manager Release 10.2)**											
System Manager Solution Deployment Manager – Centralized Functionality	Avaya Solutions Platform (ASP 130/S8300)	System Manager	Session Manager	Communication Manager	CM Adjuncts (MM, Gateways)	Branch Session Manager	Breeze	Secure Access Gateway	WebLM	Application Enablement Services	Media Server	Session Border Control (SBCE 8
Automated Migrations R10.1.x to R10.2/ R8.1.3.8 to R10.2 (analysis and pre-upgrade checks) [Target Platform: ASP / customer VMware]	Y [Other than AVP hosting System Manager]	Y [Only using SDM Client]	Y	Y	n/a [Covered as Firmware Updates]	Y	N (Breeze Upgrade Supported from Breeze 3.3 Onwards)	N	Y	Y	N	N
Automated Migrations R10.1.x to R10.2/ R8.1.3.8 to R10.2 (analysis and pre-upgrade checks) [customer VMware]	n/a	Y [Only using SDM Client]	Y	Y	n/a [Covered as Firmware Updates]	Y	N (Breeze Upgrade Supported from Breeze 3.3 Onwards)	N	n/a	Y	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
Scheduler (upgrades and patching)	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N
Virtual Machine M4anagement (start, stop, reset, status, dashboard)	Y	N	Y	Y	n/a	Y	Y	Y	Y	Y	Y	N

Solution Deployment Manager Adopter Matrix	**Adopting Product (System Manager Release 10.2)**											
System Manager Solution Deployment Manager – Centralized Functionality	Avaya Solutions Platform (ASP 130/S8300)	System Manager	Session Manager	Communication Manager	CM Adjuncts (MM, Gateways)	Branch Session Manager	Breeze	Secure Access Gateway	WebLM	Application Enablement Services	Media Server	Session Border Control (SBCE 8
Support for changing VM Flexible Footprint	n/a	Y [Only using SDM Client]	Y	N	n/a	Y	Y	Y	Y	Y	Y	N
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
Security Service Pack	n/a	n/a	n/a	Y	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

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

VMware: Virtualized Environment

Avaya Aura® Presence Services

What's new in Presence Services Release 10.1.0.2.x

Presence Services Release 10.1.0.2 Support on Avaya Solution Platform 130 R6.x

Presence Services Release 10.1.0.2 supports installation on Avaya Breeze® Platform 3.9.0.3 on Avaya Solution Platform 130 R6.x (KVM on RHEL 8.10)

Hardware supported –

- ASP 130 R6.x Dell PowerEdge R660xs server (Profile A3 and A31)
- ASP 130 R6.x Dell PowerEdge R640 server (Profile P5 and P51)
    - Profile 5 and 51 will require reconfiguration of the raid array prior to deploying ASP 130 R6.x.

Please refer to Avaya Breeze® Platform deployment guide on the support site - Deploying Avaya Breeze® platform on Avaya Solutions Platform 130 R6.x (KVM on RHEL 8.10) for installation of Avaya Breeze® Platform on KVM.

Only Avaya Breeze® platform 3.9.0.3 is supported for deployment on Avaya Solution Platform 130 R6.x (KVM on RHEL 8.10) with Presence Services 10.1.0.2.

Hardware requirements for installation on ASP 130 R6.x

The following table provides information about the memory, disk, and vCPU requirements for the components required to support Presence Services 10.1.0.2 on Avaya Solution Platform 130 R6.x (KVM on RHEL 8.10):

Component	Platform	Requirement	Avaya Aura® Presence Services 10.1.0.2
1000 and 5000 Presence User			
Avaya Aura® Presence Services 10.1.0.2	Avaya Breeze® platform 3.9.0.3	Number of Breeze nodes	2
		vCPU's	12
		Memory	34 GB
		Minimum disk size	300 GB
16000 Presence Users			
Avaya Aura® Presence Services 10.1.0.2	Avaya Breeze® platform 3.9.0.3	Number of Breeze nodes	3
		vCPU's	12
		Memory	34 GB
		Minimum disk size	300 GB

Deployment procedure

Please refer to Avaya Breeze® Platform deployment guide on the support site - Deploying Avaya Breeze® platform on Avaya Solutions Platform 130 R6.x (KVM on RHEL 8.10) for installation of Avaya Breeze® Platform 3.9.0.3.

What's new in Presence Services Release 10.1.x.x

Required artifacts for Presence Services Release 10.1.0.2.x

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

Filename	PLDS ID	File size	Version number	Comments
PresenceServices-Bundle-10.1.0.2.20082025.zip	PS100102001	211 MB	10.1.0.2.20082025	Requires the use of Breeze 3.9.0.3 as a platform (minimum release)

Presence Services 10.1.0.2 supports Breeze 3.9.0.3 Platform.

Required artifacts for Presence Services Release 10.1.0.1.x

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

Filename	PLDS ID	File size	Version number	Comments
PresenceServices-Bundle-10.1.0.1.25.zip	PS100101000	180 MB	10.1.0.1.25	Requires the use of Breeze 3.9 as a platform (minimum release)
PresenceServices-Bundle-10.1.0.1.30.zip	PS100101001	179 MB	10.1.0.1.30	Requires the use of Breeze 3.9 as a platform (minimum release)
PresenceServices-Bundle-10.1.0.1.40.zip	PS100101002	184 MB	10.1.0.1.40	Requires the use of Breeze 3.9 as a platform (minimum release) Refer PSN006378u for more details.

Presence Services 10.1.0.1 supports Breeze 3.9 Platform.

Required patches for Presence Services 10.1

Patches in 10.1.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 10.1.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 10.X and above uses the following version string syntax:

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

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

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

Backing up the software

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

Installing Presence Services Release 10.1.x.x

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

Note: To install the PS 10.1 SVAR, all previous versions of the PS SVAR will need to be uninstalled and the SVAR file needs to be deleted from the SMGR. This procedure (deleting previous versions of the SVAR from the SMGR) only needs to be performed when upgrading from releases older than 8.0.1. This procedure is not required when upgrading from 8.0.1 or newer versions.

Troubleshooting the installation

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

Restoring software to the previous version

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

Migrating to the PS 10.1.x release from a PS 6.2.X release

Changes Affecting Migrations to 10.1

Avaya Aura® Presence Services 6.X loads cannot be migrated directly to PS 10.1.x .

Customers wishing to migrate from PS 6.X loads must first migrate to the latest available PS 7.1.X release. Once a migration has been completed to PS 7.X it will then be possible to upgrade to PS 8.1.X Once in 8.1.x Release Customers could upgrade to 10.1.X release.

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

Note: At the time of general availability of Presence Services 10.1.X 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 10.1.x deployments.

Note: To install the PS 10.1.X SVAR, all previous versions of the PS SVAR will need to be uninstalled, and the SVAR file needs to be deleted from the SMGR. This procedure (deleting previous versions of the SVAR from the SMGR) only needs to be performed when upgrading from releases older than 8.0.1. This procedure is not required when upgrading from 8.0.1 or newer releases.

Migrations to release 10.1.x are supported from the following releases only:

Minimum required versions by Release

Release	Minimum Required Version
Avaya Aura® Presence Services 7.0	PresenceServices-7.0.0.0.1395.svar + any additional patch(es)
Avaya Aura® Presence Services 7.0 Service Pack 1	PresenceServices-7.0.0.1.1528.svar + any additional patch(es)
Avaya Aura® Presence Services 7.0 Feature Pack 1	PresenceServices-7.0.1.0.872.svar + any additional patch(es)

Release	Minimum Required Version
Avaya Aura® Presence Services 7.1	PresenceServices-7.1.0.0.614.svar + any additional patch(es)
Avaya Aura® Presence Services 7.1 Feature Pack 2	PresenceServices-7.1.2.0.231.svar + any additional patch(es)
Avaya Aura® Presence Services 8.0	PresenceServices-8.0.0.0.294.svar + any additional patch(es)
Avaya Aura® Presence Services 8.0 Feature Pack 1	PresenceServices-8.0.1.0.301.svar + any additional patch(es)
Avaya Aura® Presence Services 8.0 Feature Pack 2	PresenceServices-8.0.2.0.253.svar + any additional patch(es)
Avaya Aura® Presence Services 8.1	PresenceServices-8.1.0.0.277.svar + any additional patch(es)
Avaya Aura® Presence Services 8.1.1	PresenceServices-8.1.1.0.26.svar + any additional patch(es)
Avaya Aura® Presence Services 8.1.2	PresenceServices-8.1.2.0.27.svar + any additional patch(es)
Avaya Aura® Presence Services 8.1.3	PresenceServices-8.1.3.0.87.svar + any additional patch(es)
Avaya Aura® Presence Services 8.1.4	PresenceServices-8.1.4.0.69. svar + any additional patch(es)
Avaya Aura® Presence Services 10.1.0.0	PresenceServices-10.1.0.0.66. svar + any additional patch(es)

Upgrade References to Presence Services Release 10.1.x

Upgrade Quick Reference	Download	Prerequisite Downloads
Presence Services Customer Documentation	PresenceServices-Bundle-10.1.0.1.25.zip (PLDS ID: PS100101000)	Breeze 3.9 or higher Platform OVA – PS 10.1.0.1 is only compatible with Breeze 3.9 and newer platform loads.

Interoperability and requirements/Applicability for Release 10.1.x

Note: For full Avaya product compatibility information, go to the TOOLS > Product Compatibility Matrix on the Avaya Support website.

Software Development Kit

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

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

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

SDK Filename	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 https://www.avaya.com/en/partners/devconnect/program/.

Functionality not supported in Presence Services 10.1.x.x

Functionality not supported in Presence Services 10.1

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

Fixes in Presence Services Release 10.1.x.x

Fixes in Presence Services Release 10.1.0.2

The following issues are resolved in cumulative updates to the 10.1 release:

ID	Minimum conditions	Visible symptoms	Issue found in Release
PSNG-13142 PSNG-13148	WebSphere corruption	WebSphere corruption introduced when using Presence Services 10.1.0.1.25, 10.1.0.1.30, or 10.1.0.1.40 with Breeze 3.9.0.0 release.	10.1.0.1

Fixes in Presence Services Release 10.1

The following issues are resolved in cumulative updates to the 10.1 release:

ID	Minimum conditions	Visible symptoms	Issue found in Release
PSNG-12234		Incorrect response for contact presence	8.1.4
PSNG-12211		Fix for errors found in DCM logs	8.1.4
PSNG-11833		Unread messages count, in gray, searching for messages which are not read at other end gives unread badge	8.1.4
PSNG-11640		Unread messages count, in gray, is shown though the messages are read already	8.1.4
PSNG-11639		Getting error "Your message may not be up to date" after sending the attachment failed	8.1.4
PSNG-11311		InterPS Federation - Could not play audio which was recorded and sent from InterPS federated user	8.1.4.0
PSNG-11309		InterPS Federation - After a user has been re-added to a p2p conversation, it could not receive new messages in that conversation	8.1.4.0
PSNG-10915		InterPS Federation - After a user has been re-added to a p2p conversation, it could not receive new messages in that conversation	8.1.3
PSNG-10244		The subject is not sent to recipient in first time starting a new conversation between 2 PSs on 2 SMGRs	8.1.3

PSNG-6502		The status note displays incorrectly when the user in a meeting (or OOTO) with 2 PS on the same SMGR	8.1.2
PSNG-12284		After the active node had lost network connection, it took 20 minutes for IM to back to normal	10.1.0.0

Known issues and workarounds in Presence Services Release 10.1.x.x

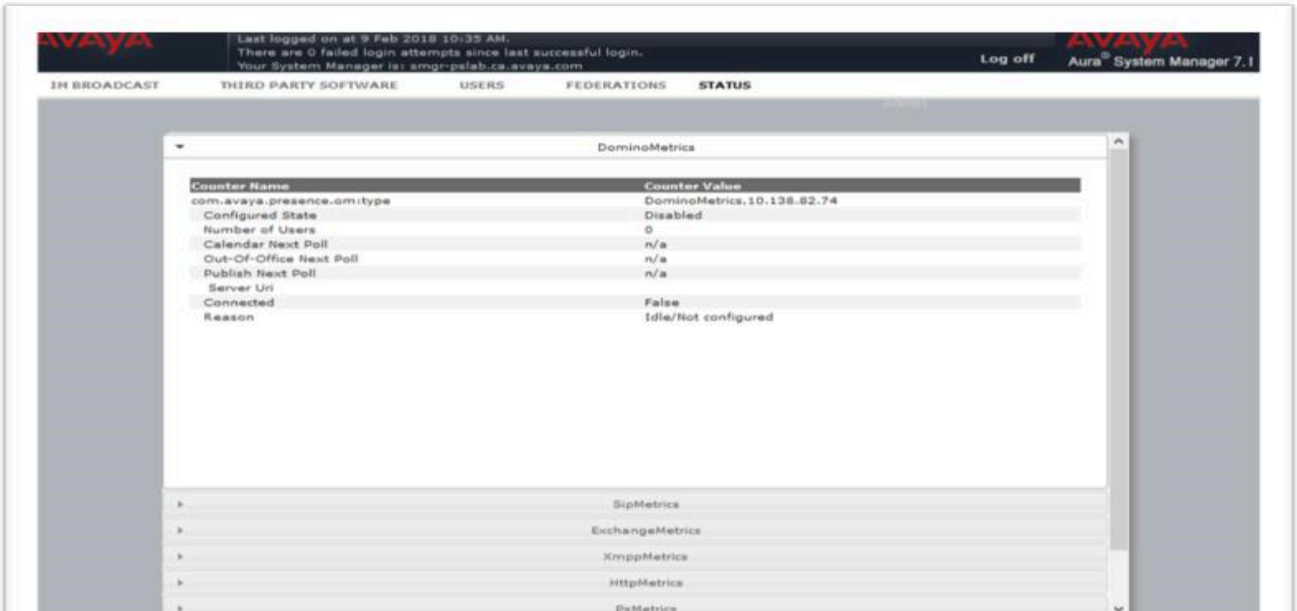
Known issues and workarounds in Presence Services Release 10.1.0.2

ID	Minimum conditions	Visible symptoms	Workaround
PSNG-13156		Presence Services - Error when setting "Text Messages Size" to valid value 2048.	Delete ALL Presence Services from System Manager and then re-load them.
PSNG-13155		Presence Services - Service Attributes allows changing Subscription/Publication Expiry Time beyond allowed limits.	Delete ALL Presence Services from System Manager and then re-load them.
PSNG-13170		IM service cannot auto-recover in network fluctuation scenario.	Continue exchange IM and presence on clients after logout and login back.
PSNG-13146		Presence Services cluster node goes into CPU Overload state frequently.	Reconfigure Breeze node to SMGR using the IP address instead of FQDN if Breeze node is added to System Manager using the FQDN address instead of IP address, i.e., Breeze Management hostname using FQDN value rather IP address.

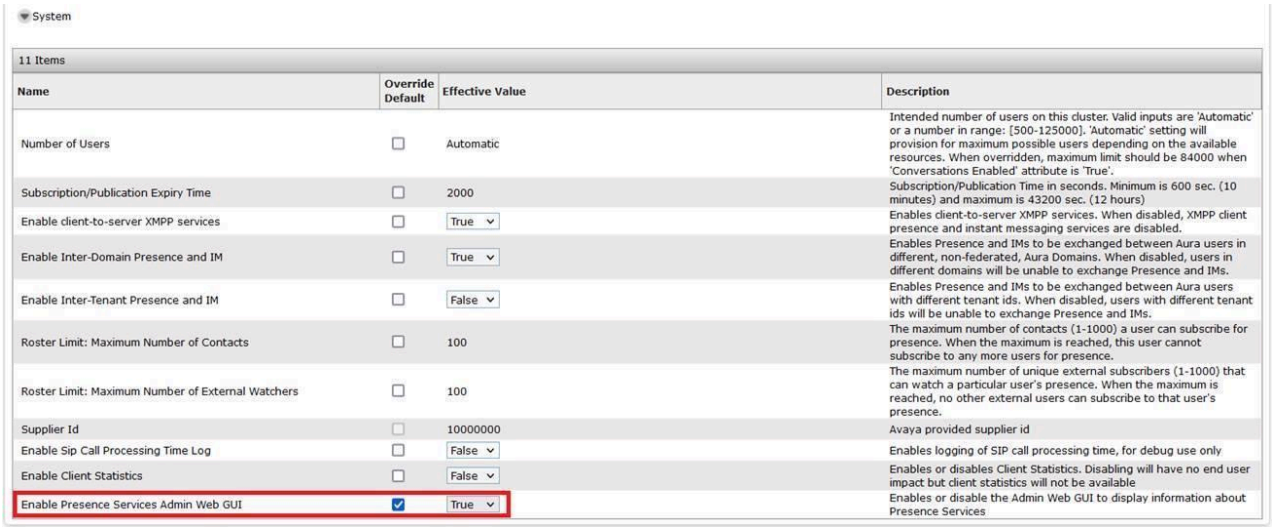
Known issues and workarounds in Presence Services Release 10.1

ID	Minimum conditions	Visible symptoms	Workaround
PSNG-12620		Equinox For Web not working when samesite is set to lax/ strict.	Disable samesite setting.
PSNG-11991		Exporting Conversation progress never stops after opening the conversation listed after messages search	NA

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



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


System

11 Items

Name	Override Default	Effective Value	Description
Number of Users	☐	Automatic	Intended number of users on this cluster. Valid inputs are 'Automatic' or a number in range: [500-125000]. 'Automatic' setting will provision for maximum possible users depending on the available resources. When overridden, maximum limit should be 84000 when 'Conversations Enabled' attribute is 'True'.
Subscription/Publication Expiry Time	☐	2000	Subscription/Publication Time in seconds. Minimum is 600 sec. (10 minutes) and maximum is 43200 sec. (12 hours)
Enable client-to-server XMPP services	☐	True	Enables client-to-server XMPP services. When disabled, XMPP client presence and instant messaging services are disabled.
Enable Inter-Domain Presence and IM	☐	True	Enables Presence and IMs to be exchanged between Aura users in different, non-federated, Aura Domains. When disabled, users in different domains will be unable to exchange Presence and IMs.
Enable Inter-Tenant Presence and IM	☐	False	Enables Presence and IMs to be exchanged between Aura users with different tenant ids. When disabled, users with different tenant ids will be unable to exchange Presence and IMs.
Roster Limit: Maximum Number of Contacts	☐	100	The maximum number of contacts (1-1000) a user can subscribe for presence. When the maximum is reached, this user cannot subscribe to any more users for presence.
Roster Limit: Maximum Number of External Watchers	☐	100	The maximum number of unique external subscribers (1-1000) that can watch a particular user's presence. When the maximum is reached, no other external users can subscribe to that user's presence.
Supplier Id	☐	10000000	Avaya provided supplier id
Enable Sip Call Processing Time Log	☐	False	Enables logging of SIP call processing time, for debug use only
Enable Client Statistics	☐	False	Enables or disables Client Statistics. Disabling will have no end user impact but client statistics will not be available
Enable Presence Services Admin Web GUI	☑	True	Enables or disable the Admin Web GUI to display information about Presence Services

Avaya Aura® Application Enablement Services

What's new in Application Enablement Services Release 10.2.x.x

What's new in Application Enablement Services 10.2.1.1

- VMware Esi 8.0.3 U3 platform support.

The December 23 updated Aura 10.2 KVM OVAs now support the following:

- The KVM OVAs include an *install_vm.py* script to simplify deployment of the KVM OVA
- The *install_vm.py* script now supports the creation of a root login/password
- The CM and AES updated 10.2 KVM OVAs also include support for disk encryption.

What's new in Application Enablement Services 10.2.1.0

AE Services supports RHEL 8.10 from 10.2.1 onwards. For more information, please refer ***Upgrading Avaya Aura® Application Enablement Services*** guide.

What's new in Application Enablement Services 10.2

Note: There are no changes in JTAPI and TSAPI programmer's guides in release 10.2. R10.1 JTAPI and TSAPI programmer's guides can be used for R 10.2 as well.

For more information, see ***What's New in Avaya Aura® Release 10.2.x*** document on the Avaya Support site: https://download.avaya.com/css/public/documents/101087359

Security Service Packs

Security Service Packs

AE Services releases Security Service Packs (SSPs) aligned with the application release cycle.
SSP contents for AE Services 10.2.x will be part of PCN2165S and installation procedure will be documented in the upgrade guide. PCN and installation procedure will be provided once the first SSP is generated.

SSPs cannot be installed on "software-only" deployments.

Required artifacts for Application Enablement Services Release 10.2.x.x

Required artifacts for Application Enablement Services Release 10.2.1.4

Filename	PLDS ID	File size	Version number	Comments
aesvcs-10.2.1.4.0.34-servicepack.bin	AES00001083	324.87 MB (332671.7 KB)	10.2.1.3.0	Avaya Aura® Application Enablement Services 10.2.1 Service Pack #4 MD5 Checksum: e803715afe745930cb7f0efb9054c78c

Required artifacts for Application Enablement Services Release 10.2.1.3

Filename	PLDS ID	File size	Version number	Comments

aesvcs-10.2.1.3.0.19-servicepack.bin	AES00001075	324.65 MB (332448.90 KB)	10.2.1.3.0	Avaya Aura® Application Enablement Services 10.2.1 Service Pack #3 MD5 Checksum: 1b66a1cefd89a3546fae3a505b984b77

Required artifacts for Application Enablement Services Release 10.2.1.2

Filename	PLDS ID	File size	Version number	Comments
aesvcs-10.2.1.2.0.29-servicepack.bin	AES00001067	324.54 MB (332,335 KB)	10.2.1.2.0	Avaya Aura® Application Enablement Services 10.2.1 Service Pack #2 MD5 Checksum: 8ade2693188a11a3285ce297eefc2919

Required artifacts for Application Enablement Services Release 10.2.1.1

Filename	PLDS ID	File size	Version number	Comments
aesvcs-10.2.1.1.0.161-servicepack.bin	AES00001055	324.43 MB (332,215 KB)	10.2.1.1.0	Avaya Aura® Application Enablement Services 10.2.1 Service Pack #1 MD5 Checksum: 4807d89beb371c43b3629613a8b17f1b

Required artifacts for Application Enablement Services Release 10.2.1.0

Filename	PLDS ID	File size	Version number	Comments
aesvcs-10.2.1.0.0.441-featurepack.bin	AES00001039	338.362962 MB (338362.962 KB)	10.2.1.0.0	Avaya Aura® Application Enablement Services 10.2 Feature Pack #1 MD5 Checksum: 09a6fe2e01b9bbf5cfbdfef010da6e08
~~AES-10.2.0.0.0.198.20231107-e70-00-kvm.ova~~	~~AES00001038~~	~~3,185.12 MB (3,185,121 KB)~~	~~10.2~~	~~Avaya Aura® Application Enablement Services 10.2 KVM OVA Media MD5 Checksum: 9196849dfbef04cb10af60cccba4b9d0e54a4c0d2ed50f6fccc1fe4acf53253f~~
AV-AES10.2-RHEL8.10-OSUpdate-006.tar.bz2	AES00001041	753.499663 MB 753499.663 (KB)	RHEL 8.10	Avaya Aura® Application Enablement Services RHEL 8.10 OS Bundle MD5 Checksum: 2c67ef13c7efb790fafaf192a8fcd5a7

AES-10.2.0.0.0.198.20231107-e70-01-kvm.ova	AES0000 1045	3022.32 MB (3094860 KB)	10.2	Avaya Aura® Application Enablement Services 10.2 KVM OVA Media MD5 Checksum: a823dbfb6a975c8a69979c7785e9240b

Note: Replacing the KVM OVA to cover the script-based deployment method. The procedure is documented in deployment guide. This also enables the Disk Encryption capability.

Required artifacts for Application Enablement Services Release 10.2.0.1

Filename	PLDS ID	File size	Version number	Comments
~~aesvcs-10.2.0.1.0.46-servicepack.bin~~	~~AES0000102 3~~	~~318 MB (316,545 KB)~~	~~10.2.0.1.0~~	~~Avaya Aura® Application Enablement Services 10.2 Service Pack #1~~ ~~**MD5 Checksum:**~~ ~~76858ca9f53f0d97df89960d1bba924 6~~
aesvcs-10.2.0.1.1.3-servicepack.bin	AES0000102 7	333.45 MB (333,452 KB)	10.2.0.1.1	Avaya Aura® Application Enablement Services 10.2 Service Pack #1 MD5 Checksum: 23cceca9e167dde8c2526f9b9fda82f6

Note: The original AES 10.2.0.1.0 (aesvcs-10.2.0.1.0.46-servicepack.bin) has been removed from PLDS and replaced with an updated Service Pack 1 (aesvcs-10.2.0.1.1.3-servicepack.bin) that updates the postgresql rpm to version 13.11-2. Customers who have deployed the original 10.2.0.1.0 should plan to update to 10.2.0.1.1.

Required artifacts for Application Enablement Services Release 10.2

Filename	PLDS ID	File size	Version number	Comments
AES-10.2.0.0.0.198.20231107-e70-00.ova	AES0000099 0	2,844.18 MB (2,912,440.5 KB)	10.2.0.0.0	Avaya Aura® Application Enablement Services 10.2 OVA Media **MD5 Checksum:** 653d2755768fe6008c84685db9c4c1a1
AES-10.2.0.0.0.198-20231107.iso	AES0000099 1	370.44 MB (379,338 KB)	10.2.0.0.0	Avaya Aura® Application Enablement Services 10.2 Software Only ISO **MD5 Checksum:** 2c46ee5664a63a24302a852b8d46c707

Note: The deployment of Avaya Aura® applications as Software-only is available but a restricted offer for net new deployments and requires Avaya Aura® BU approval before proceeding. If you have a business requirement to deploy Avaya Aura® as Software-only, please get in touch with your Avaya Sales team. Existing customers using software only deployments continue to be supported.

Software information for 10.2.x.x

Software	Version	Note
OS	Red Hat Linux Release 8.4 (Ootpa) / Red Hat Linux Release 8.10 (Ootpa)	RHEL8.10 is supported from 10.2.1 onwards through OS upgrade bundle
Web Server	Apache Server 2.4.37	
Application Server	Apache Tomcat 9.0.94 Apache Tomcat 9.0.102 in AES version 10.2.1.1.	
Database	PostgreSQL 13.11	
Java	Open JDK 1.8.0.432.b06-2	
VMware vCenter Server, ESXi Host	7.0.X, 8.0, 8.0 Update 2	Avaya Aura® Release 10.2.x supports VMware 8.0 and VMware 8.0 Update 2. Avaya Aura® Release 10.2.x does not support VMware 8.0 Update 1. For information about known issues, see VMware 8.0 Update 1 Release Notes on the VMware website at https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-6vcenter-server-801-release-notes/index.html.

Installation for Avaya Aura® Application Enablement Services Release 10.2.x.x

Installation for Avaya Aura® Application Enablement Services Release 10.2

Backing up the AE Services software

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

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

Interoperability and requirements

Note: For full Avaya product compatibility information, go to the TOOLS > Product Compatibility Matrix on the Avaya Support website.

Installation for Avaya Aura® Application Enablement Services Release 10.2.x.x

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

Additional references for Virtualized deployments:

- Deploying Avaya Aura® Application Enablement Services in Virtualized Environment Release 10.2.x
- Deploying Avaya Aura® Application Enablement Services in a Software-Only and Infrastructure as a Service Environments Release 10.2.x
- Upgrading Avaya Aura® Application Enablement Services Release 10.2.x

Note:

1. With Release 10.2, by default, TSAPI Unencrypted Services Port (450) is disabled and TSAPI Encrypted Services Port (453) is enabled.
2. From AE Services 10.1, only the Transport Layer Security (TLS) 1.3 and 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 1.2 is required, at a minimum, to mitigate various attacks on the TLS 1.0,1.1 protocol. The use of TLS 1.3 is strongly recommended.

Upgrading to AE Services 10.2.x.x

Upgrading to AE Services 10.2.1.4

An upgrade to AES 10.2.1.4 can be achieved by upgrading existing 10.2.0.0 or 10.2.0.1 or 10.2.1.0 or 10.2.1.1 or 10.2.1.2 or 10.2.1.3 systems to AES 10.2.1.4 using the service pack installer aesvcs-10.2.1.4.0.34-servicepack.bin.

Upgrading to AE Services 10.2.1.3

An upgrade to AES 10.2.1.3 can be achieved by upgrading existing 10.2.0.0 or 10.2.0.1 or 10.2.1.0 or 10.2.1.1 or 10.2.1.2 systems to AES 10.2.1.3 using the service pack installer aesvcs-10.2.1.3.0.19-servicepack.bin.

Upgrading to AE Services 10.2.1.2

An upgrade to AES 10.2.1.2 can be achieved by upgrading existing 10.2.0.0 or 10.2.0.1 or 10.2.1.0 or 10.2.1.1 systems to AES 10.2.1.2 using the service pack installer aesvcs-10.2.1.2.0.29-servicepack.bin.

Upgrading to AE Services 10.2.1.1

An upgrade to AES 10.2.1.1 can be achieved by upgrading existing 10.2.0.0 or 10.2.0.1 or 10.2.1.0 systems to AES 10.2.1.1 using the service pack installer aesvcs-10.2.1.1.0.161-servicepack.bin.

Upgrading to AE Services 10.2.1.0

An upgrade to AES 10.2.1.0 can be achieved by upgrading existing 10.2.0.0 systems to AES 10.2.1.0 using the feature pack installer aesvcs-10.2.1.0.0.441-featurepack.bin.

Upgrading to AE Services 10.2.0.1

An upgrade to AES 10.2.0.1 can be achieved by upgrading existing 10.2.0.0 systems to AES 10.2.0.1 using the service pack installer aesvcs-10.2.0.1.0.46-servicepack.bin.

Upgrading to AE Services 10.2

AE Services Server Upgrade Instructions

Refer to the *Upgrading Avaya Aura® Application Enablement Services* document at: https://support.avaya.com

RHEL 8.4 Support for AE Services 10.2

AE Services 10.2 is supported on RHEL 8.4. Upgrading AE Services 10.2 to any RHEL release greater than 8.4 is not supported and may cause the system to enter an unstable state.

Installation for Avaya Aura® Application Enablement Services Software Only 10.2.x.x

Refer to the *Deploying Avaya Aura® Application Enablement Services in Software-Only and Infrastructure as a Service Environments Release 10.2.x* and *Upgrading Avaya Aura® Application Enablement Services Release 10.2.x* at: https://support.avaya.com

Important Note:

The required upgrade order as documented in the Product Compatibility Matrix and in the application specific upgrade documentation must be followed.

Functionality not supported

Functionality not supported for Release 10.2.x.x

- Certificates become invalid after migrating to Avaya Aura® Application Enablement 10.1, for more details, see PSN020555u.
- When Avaya Aura® Communication Manager is upgraded to 10.2 and Avaya Aura® Application Enablement is lower than 8.1.3.1 then the ASAI link using minimum TLS version 1.2 will not be established. As per product compatibility matrix, the Avaya Aura® Application Enablement must always be greater than or equal to the release/version of the Avaya Aura® Communication Manager

Changes and Issues

WebLM server compatibility

The WebLM server supports N-1 backward compatibility with its client component. AE Services 10.2.x WebLM client is compatible with WebLM 10.1.3.1 server and later versions.

VM Foot Print Size and capacity

Note: Hard Drive has been increased to 55 GB from 30 GB in AE Services server 10.1 for all foot prints

		DMCC (Third-party call control: 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 55 GB HDD	1K	20K BHCC	1K	9K BHCC	1K MPS
		10K	6K BHCC			
Medium	2 CPU 4 GB RAM 55 GB HDD	2.5K	50K BHCC	2.4K	18K BHCC	1K MPS
		12K	12K BHCC			

		DMCC (Third-party call control: Avaya Aura Contact Center)		DMCC (First Party call control)		TSAPI/DLG/CVLAN
Large	4 CPU 6 GB RAM 55 GB HDD	5K	100K BHCC	8K	36K BHCC	2K MPS
		20K	24K BHCC			

Fixes in Application Enablement Services in Release 10.2.x.x

Fixes in Application Enablement Services in Release 10.2.1.4

ID	Minimum conditions	Visible Symptoms
AES-35378	Missing INVITE from SIP endpoint in response to 3PAD and then SIP endpoint dialing a call manually.	Null DeviceID in CSTA Service Initiated event.
AES-35376	TLS remote logging is enabled from the AES UI	syslogs to remote server are sent using TCP protocol
AES-35365	AES 10.2.x Installed	No Visible symptoms. Postgres version update to postgresql-13.23.x
AES-35349	DMCC TTS enabled.stations integration and CM interchange.	After CM interchange, recordings didn't happen for some DMCC extensions
AES-35271	AES 10.2.x Installed	No Visible symptoms. Spring Framework update to version NES 5.3.39
AES-35187	CTI user login to OAM	OAM Login fails

Fixes in Application Enablement Services in Release 10.2.1.3

ID	Minimum conditions	Visible Symptoms
AES-35315	Network disconnection and DMCC session recovery after > 5 mins	CTI bases recorder application may get dis-connected hampering the recordings.
AES-35287	TTS enabled DMCC recorders and their respective Q931 connections with CM are not up	AES may not put DMCC recorder station on "On-Hook" correctly and cause SSC failure for the next call on same recorder station.
AES-35270	AES 10.2.x Installed	No Visible symptoms. Tomcat version update to 9.0.111
AES-35269	AES 10.2.x Installed	No Visible symptoms. Postgres version update to postgresql-13.20.x
AES-35251	RONA trigger on the call	Unexpected drop for the party in the call
AES-35189	Activate/De-activate call forward feature on ASAI monitored extension.	***"Call-Forward"*** or other similar activation/de-activation events may not be visible to CTI application.

Fixes in Application Enablement Services in Release 10.2.1.2

There are no bug fixes in the AES 10.2.1.2 Service Pack. Version information has been updated to ensure compatibility with all Avaya applications.

Fixes in Application Enablement Services in Release 10.2.1.1

ID	Minimum conditions	Visible Symptoms
AES-35047	AES 10.2.x Installed	No Visible symptoms. Tomcat version update to 9.0.102
AES-34481	AES 10.1 release with embedded WebLM configured.	Tomcat may throw Out-Of-Memory exception.
AES-34402	Initiate a call from ASAI monitored station.	JTAPI application going in hung state or restart.
AES-33956	JTAPI application with SDB enabled, and having large number of devices in a single deviceGroup.	If SDB is enabled with JTAPI application, then getaddress() API call may take longer time to process.
AES-33811	login to system from multiple different instances	Login is allowed more than configured PAM limits
AES-33956	JTAPI 10.1.0.2 client with restricted permission in SDB for CTI user.	JTAPI getaddress() API call may take longer time to process if there are large number of devices in SDB deviceGroup.
AES-33816	Third party make call from station monitored by to AESs with JTAPI client connected. One AES triggers the make call request.	JTAPI service provider crash because of NULL pointer access
AES-33217	JTAPI SDK invokes getloggedonAgents() or ACD.addaddresslistener API call	Event Q Size may breach threshold and causes provider to restart.
AES-32823	Generate an alarm from AES which will be received by the trap receiver.	The trap receiver at the customer might not interpret AES traps well.
AES-32824	JTAPI SDK with debug level set to zero in TSAPI.PRO file.	Debugs logs were generated for JTAPI even if debug level was set to zero.
AES-28240	JTAPI 10.1.0.2 with device monitor added.	When the JTAPI Client receives an event (e.g. Established event) it makes many CSTAQueryDeviceInfo requests to AES. It may cause the delay in processing of JTAPI event Q Size, and could result in provider shutdown.

Fixes in Application Enablement Services in Release 10.2.1.0

ID	Minimum conditions	Visible Symptoms
AES-34024	AES Server 10.1.x or 10.2.x	mDNS service is enabled on AES system on port 5353
AES-33995	AES 10.1.3 with JTAPI clients	JTAPI connection may receive invalid number of connections in getConnections response.
AES-33884	AES 10.1.3 with SOSM feature enabled on CM.	ATTSingleStepTransfer request will fail.
AES-33213	AES swonly offer deployed on AWS	DBService may not be running after reboot.
AES-31149	Mediamonitor with Tonedetection events enabled for a device	DMCC may not send tone detected events in case MediaMonitor is placed after device is registered.

Fixes in Application Enablement Services in Release 10.2.0.1

ID	Minimum conditions	Visible Symptoms
AES-33213	AES 10.1 deployed on AWS cloud.	After AES reboot on AWS, Postgresql service may not start.
AES-32938	AES 10.1.2 without TSAPI reserved licensing configured.	TSAPI service may crash while trying to acquire TSAPI license from WebLM.
AES-32922	10.1 AES with default as well as other required certificates	CA Trusted and Server Certificates Default certificates added back after FP/SP Installation even if they were deleted from system before update of SP/FP
AES-32910	AES 10.1.3.1	TSAPI Test in OAM diagnostics not working.
AES-32901	Agent transferring call to VDN/Vector/hunt and call been queued to skill as agents are not available.	CTI side doesn't get correct state for the connected party in the call.
AES-32814	TSAPI link with switch connection name with 13 characters or more.	TSAPI link status will be down.
AES-32616	AES 10.1 with TLSv1.3 enabled system.	The weak ciphers in JDK 8 gets enabled on the AES with TLSv1.3 enabled.
AES-32532	AES 10.1 with local DNS not working or misconfigured DNS server.	AES sends the DNS requests to public root servers every day at specified time.
AES-32455	AES 10.1.2. A newly created Security user.	When admin try to login through the newly created user on OAM, it does not ask to change password and neither take the current password to login.
AES-31149	DMCC station with Out-of-Band DTMF config, and a tone detection listener added.	DTMF tone events are not sent to clients if DMCC station re-registers after monitor is placed.
AES-29726	TSAPI CLIENT/SDK 10.1	Due to missing dependency, TSAPI client application shows error message as msvcr100.dll missing.
AES-23159	JTAPI client with device monitor.	JTAPI crashes with null pointer exception while processing CSTA FAILED event having empty failing Device.

Fixes in Application Enablement Services in Release 10.2

AES-23401	DMCC client application written using DMCC Java SDK.	If ServiceProvider.getServiceProvider() fails, two threads are left running
AES-29726	TSAPI CLIENT/SDK 10.1	Due to missing dependency, TSAPI client application shows error message as msvcr100.dll missing.
AES-29836	TSAPI CLIENT/SDK 10.1.0.2	French characters in the EULA are not shown properly during installation on InstallShield Wizard.
AES-30249	AES 8.1.3	Caught "Index was outside the bounds of the array." exception while performing an API call through NICE recorder.
AES-31054	AES connected to WebLM with expired license.	DMCC Service License mode showing as LICENSE_EXPIRED on OAM even after installing new valid License on WebLM.
AES-31510	JTAPI SDK 10.1.0.2	Customer saw logging been stopped due to existing Log4J configuration settings been overwritten after instantiating the JTAPI application in case of customer doing dynamic Log4J logging configuration.
AES-31529	10.1.0.0.0.13 versions of the DMCC .NET library	Unable to use it in an environment that requires all assemblies to be strongly named.
AES-31568	AES 10.1, 8.x TSAPI Client	Client Application is unable to connect with TSAPI service securely using TLSv1.0/1.1.
AES-31776	AES 10.1 rebooted.	If AES is rebooted, then it is possible false high memory usage is generated.
AES-31777	AES 10.1.0.1	Enabled ports in backup do not retain values after restoration.
AES-31935	DMCC services are getting used and dmcc-logging.properties file is modified through CLI or DMCC logging level is changed from AES OAM.	DMCC services get restarted after 4-5 days if dmcc-logging.properties file is modified through CLI or DMCC logging level is changed from AES OAM.
AES-32028	AES 10.1.x, JTAPI 10.1.3	Agent shown as logged into a station even though some other agent is already logged into the same station.
AES-32296	AES 10.1.3.1	If ToneDetection monitor is placed, then AES may send same tone detected event twice.
AES-32299	AES Release 8.1.x or 10.1.x with high volume of kernel logs.	AES servers have been alarmed due to the /var/log partition hitting 90%. /var/log/avaya/aes/kernel.log are not getting rotated.
AES-32305	JTAPI SDK 10.1.0.2 AES 10.1.0.2	JTAPI application going into hung state while trying to stop monitors.
AES-32495	AES 10.1.0.2, DMCC Java Client 10.1.0.2	characterSet in GetDisplayResponse gives unexpected value.
AES-32561	AES 10.2	The customer sees an error message as "This site can't provide a secure connection" while accessing OAM Web page.
AES-32563	TSAPI CLIENT/SDK 10.1.0.2	French characters in the EULA are not shown properly during installation on Windows command prompt.
AES-32582	AES 8.1.2 with JITC and TSAPI client authentication enabled. AES 8.1.2 TSAPI Client with OCSP and Verify Sever FQDN parameter enabled.	Unable to see T-Link information to connect to AES.
AES-32603	AES 10.1.0.2, DMCC .NET Client 10.1.0.2	characterSet in GetDisplayResponse gives unexpected value.

Known issues and workarounds in Application Enablement Services 10.2.x.x

Known issues and workarounds Application Enablement Services in Release 10.2.1.4

ID	Minimum conditions	Visible Symptoms	Workaround
AES-34129	AES 10.2	Open Stream Request fails on OAM	Login to AES and edit /usr/lib64/tslibrc file to point to correct AES.
AES-33750	AES 10.1, CM 10.1	Public Unknown Numbering displays another position on CM.	No Workaround
AES-33610	AES 10.1 without default server certificate.	AES will not be able connect to local embedded WebLM.	Use port 443 as weblm port with local embedded weblm.
AES-33461	DMCC Java Client 10.x	Not able to receive a ServiceLinkStatusEvent from AES.	No Workaround
AES-33335	AES 10.1	SMS response may contain invalid special characters.	Do not use special characters in trunk name on CM.
AES-32403	AES GRHA System	Reconnection of DMCC Sessions fails on fallback to primary AES in GRHA configuration.	No Workaround

Known issues and workarounds Application Enablement Services in Release 10.2.1.3

ID	Minimum conditions	Visible Symptoms	Workaround
AES-34129	AES 10.2	Open Stream Request fails on OAM	Login to AES and edit /usr/lib64/tslibrc file to point to correct AES.
AES-33750	AES 10.1, CM 10.1	Public Unknown Numbering displays another position on CM.	No Workaround
AES-33610	AES 10.1 without default server certificate.	AES will not be able connect to local embedded WebLM.	Use port 443 as weblm port with local embedded weblm.
AES-33461	DMCC Java Client 10.x	Not able to receive a ServiceLinkStatusEvent from AES.	No Workaround
AES-33335	AES 10.1	SMS response may contain invalid special characters.	Do not use special characters in trunk name on CM.
AES-32403	AES GRHA System	Reconnection of DMCC Sessions fails on fallback to primary AES in GRHA configuration.	No Workaround

Known issues and workarounds Application Enablement Services in Release 10.2.1.2

ID	Minimum conditions	Visible Symptoms	Workaround
AES-34129	AES 10.2	Open Stream Request fails on OAM	Login to AES and edit /usr/lib64/tslibrc file to point to correct AES.
AES-33750	AES 10.1, CM 10.1	Public Unknown Numbering displays another position on CM.	No Workaround
AES-33610	AES 10.1 without default server certificate.	AES will not be able connect to local embedded WebLM.	Use port 443 as WebLM port with local embedded WebLM.
AES-33461	DMCC Java Client 10.x	Not able to receive a ServiceLinkStatusEvent from AES.	No Workaround
AES-33335	AES 10.1	SMS response may contain invalid special characters.	Do not use special characters in trunk name on CM.
AES-32403	AES GRHA System	Reconnection of DMCC Sessions fails on fallback to primary AES in GRHA configuration.	No Workaround

Known issues and workarounds Application Enablement Services in Release 10.2.1.1

ID	Minimum conditions	Visible Symptoms	Workaround
AES-34129	AES 10.2	Open Stream Request fails on OAM	Login to AES and edit /usr/lib64/tslibrc file to point to correct AES.
AES-33750	AES 10.1, CM 10.1	Public Unknown Numbering displays another position on CM.	No Workaround
AES-33610	AES 10.1 without default server certificate.	AES will not be able connect to local embedded WebLM.	Use port 443 as WebLM port with local embedded WebLM.
AES-33461	DMCC Java Client 10.x	Not able to receive a ServiceLinkStatusEvent from AES.	No Workaround
AES-33335	AES 10.1	SMS response may contain invalid special characters.	Do not use special characters in trunk name on CM.
AES-32403	AES GRHA System	Reconnection of DMCC Sessions fails on fallback to primary AES in GRHA configuration.	No Workaround

Known issues and workarounds Application Enablement Services in Release 10.2.1.0

Note: The new KVM OVA published on 23rd Dec has the disk encryption capability

ID	Minimum conditions	Visible Symptoms	Workaround
~~AES-34695~~	~~AES 10.2.1, KVM SW Only~~	~~Switch connection shows garbage characters~~	~~Apply RHEL 8.10 upgrade on AES 10.2 SW Only, before applying Feature Pack 10.2.1~~
AES-34604	AES Deployed on ASP R6.0 Host	AES Disk Encryption is not available	No
AES-34402	JTAPI 10.2.0 with device monitor	JTAPI provider may shut down while processing CstaInitiated event.	No Workaround
AES-34129	AES 10.2	Open Stream Request fails on OAM	Login to AES and edit /usr/lib64/tslibrc file to point to correct AES.
AES-33956	JTAPI 10.1.0.2 client with restricted permission in SDB for CTI user.	JTAPI getaddress() API call may take longer time to process if there are large number of devices in SDB deviceGroup.	No Workaround
AES-33811	AES 10.1 or 10.2 with OAM with set Limit of PAM e.g 4	Multiple and parallel Login on OAM exceeds 4.	No Workaround
AES-33750	AES 10.1, CM 10.1	Public Unknown Numbering displays another position on CM.	No Workaround
AES-33610	AES 10.1 without default server certificate.	AES will not be able connect to local embedded WebLM.	Use port 443 as weblm port with local embedded WebLM.
AES-33461	DMCC Java Client 10.x	Not able to receive a ServiceLinkStatusEvent from AES.	No Workaround
AES-33335	AES 10.1	SMS response may contain invalid special characters.	Do not use special characters in trunk name on CM.
AES-32403	AES GRHA System	Reconnection of DMCC Sessions fails on fallback to primary AES in GRHA configuration.	No Workaround

Known issues and workarounds Application Enablement Services in Release 10.2.0.1

ID	Minimum conditions	Visible Symptoms	Workaround
AES-33217	JTAPI SDK invokes getloggedonAgents() or ACD.addaddresslistener API call	Event Q Size may breach threshold and cause provider to restart.	No

ID	Minimum conditions	Visible Symptoms	Workaround
AES-32823	Generate an alarm from AES which will be received by trap receiver.	The trap receiver at the customer didn't interpret AES traps well. The TYPE was wrong for *sysObjectID*.	No
AES-32403	AES GRHA System	Reconnection of DMCC Sessions fails on fallback to primary AES in GRHA configuration.	No
AES-32308	AES 10.1	Logs in /var/log/messages and network sniffers reports unauthorized connection request.	Modify the below file:- /opt/spirit/config/agent/SPIRITAgent_1_0_BaseAgentConfig_orig.xml <entry key="SPIRIT.heartbeat.on">true</entry> -> Change this to “false”.
AES-32193	Any DB update on primary AES server.	Customer saw DB Service restart alarms on trap receiver and couldn't sort out if the alarms are from primary AES or secondary.	No
AES-30029	GRHA Configured	GRHA shows running on CLI and OAM with different versions of AES.	No
AES-29742	JTAPI 8.1.3 AES 8.1	JTAPI make call using tac shows incorrect number of parties in getConnections()	No
AES-28813	Select ALL to add ALL device when the New Device Groups has been created	Bad gateway error seen on OAM when trying to add all devices in a device group.	No
AES-28496	AES 10.1	AES Services are not running properly so system is unresponsive to CTI applications.	Either reboot aes or restart aes SNMP subagent.
AES-28240	JTAPI 10.1.0.2 with device monitor added.	When the JTAPI Client receives an event (e.g. Established event) it makes many CSTAQueryDeviceInfo requests to AES. It may cause the delay in processing of JTAPI event Q Size, and could result in provider shutdown.	No
AES-28193	One or more Service is stopped.	CTI link status for all services is shown as talking even if respective service is stopped	No
AES-28171	AES 8.1.2	An error "Cannot access the reference link" is generated on web browsers when URL "Comments on this documents?" is accessed on any help page of AES OAM	No
AES-27844	Invalid configuration of "WebLM IP Address/FQDN", "WebLM Port" and valid configuration of "Secondary WebLM IP Address/FQDN" and	AE Services page showed License Information in red text as "Application Enablement Service is not licensed in the license file."	No

ID	Minimum conditions	Visible Symptoms	Workaround
	"Secondary WebLM Port" on "Licensing | WebLM Server Address" (OAM).		
AES-26653	snmp traps configured.	snmptrapd linux cli utility doesn't give any output when invoked from command line for debugging purposes.	No
AES-22385	AES 8.1	On OAM page Security -> certificate management -> server certificates -> add Keeping enrollment method as Automatic gives error "Auto Enrollment failed, did not receive certificate from CA."	Select manual enrollment instead of Auto Enrollment on same page.
AES-21856	AES 8.1.2, CM 8.1.2	Calls didn't get drop properly and call recordings were missing on AWFOS	No
AES-19610	AES 7.1.3	LDAP configuration option for TSAPI user (cus_ldap) is not set following errors get printed in alarm.log, every time the cti user is logged in to AES pam_ldap(tsapi_service:account): unknown option: config=/etc/cus-ldap.conf pam_ldap(tsapi_service:auth): unknown option: config=/etc/cus-ldap.conf	No
AES-19215	AES 8.1	Possible race condition in request and response and application not receiving the response.	No
AES-18144	AES 8.1	If the SNMP device is configured to use SNMP version 1 or 2c then the community name of length more than 128 characters is not allowed in the Security Name field on OAM -> Utilities -> SNMP -> SNMP trap receivers -> Add.	No

Known issues and workarounds Application Enablement Services in Release 10.2

ID	Minimum conditions	Visible Symptoms	Workaround
AES-32814	TSAPI link with switch connection name with 13 characters or more.	TSAPI link status will be down.	No
AES-32616	AES 10.1 with TLSv1.3 enabled system.	The unsupported weak ciphers in JDK 8 get enabled on the AES with TLSv1.3 enabled.	Use the setCipherSuite utility to remove the weak ciphers.
AES-32532	AES 10.1	AES sends the DNS requests to public root servers every day at specified time.	remove -R option from command "/usr/sbin/unbound-anchor -a /var/lib/unbound/root.key -c /etc/unbound/icannbundle.pem -f /etc/resolv.conf -R" present in file "/lib/systemd/system/unbound-anchor.service"

ID	Minimum conditions	Visible Symptoms	Workaround
AES-32455	AES 10.1.2. A newly created Security user.	When admin try to login through the newly created user on OAM, it does not ask to change password and neither take the current password to login	Choose option "Allow Linux Shell Access" while creating the new user, and do first login through CLI, it will ask to change the password and then login with new password through OAM.
AES-32403	AES GRHA System	Reconnection of DMCC Sessions fails on fallback to primary AES in GRHA configuration.	No
AES-32308	AES 10.1	Logs in /var/log/messages and network sniffers reports unauthorized connection request.	Modify the below file:- /opt/spirit/config/agent/SPIRITAgent_1_0_BaseAgentConfig_orig.xml <entry key="SPIRIT.heartbeat.on">true</entry> -> Change this to “false”.
AES-32193	Any DB update on primary AES server.	Customer saw DB Service restart alarms on trap receiver and couldn't sort out if the alarms are from primary AES or secondary.	No
AES-31149	AES 8.1.3.6	DTMF tone events are not sent to clients if DMCC station re-registers after monitor is placed.	Re-start the Media Monitor after DMCC station re-registers.
AES-31143	AES 10.1.2	An error occurred on AES OAM while editing the default user	Use "/opt/mvap/bin/ctiUser" utility to edit the default users from CLI.
AES-31132	AES TSAPI 64 bits client & SDK used.	The wrong acshandle is returned to the application.	No
AES-30029	GRHA Configured	GRHA shows running on CLI and OAM with different versions of AES.	No
AES-29742	JTAPI 8.1.3 AES 8.1	JTAPI make call using tac shows incorrect number of parties in getConnections()	No
AES-28813	Select ALL to add ALL device when the New Device Groups has been created	Bad gateway error seen on OAM when trying to add all devices in a device group.	No
AES-28496	AES 10.1	AES Services are not running properly so system is unresponsive to CTI applications.	Either reboot aes or restart aes SNMP subagent.
AES-28193	One or more Service is stopped.	CTI link status for all services is shown as talking even if respective service is stopped	No
AES-28171	AES 8.1.2	An error "Cannot access the reference link" is generated on web browsers when URL "Comments on this documents?" is accessed on any help page of AES OAM	No
AES-27844	Invalid configuration of "WebLM IP	AE Services page showed License Information in red text	No

ID	Minimum conditions	Visible Symptoms	Workaround
	Address/FQDN", "WebLM Port" and valid configuration of "Secondary WebLM IP Address/FQDN" and "Secondary WebLM Port" on "Licensing | WebLM Server Address" (OAM).	as "Application Enablement Service is not licensed in the license file."	
AES-26653	snmp traps configured.	snmptrapd linux cli utility doesn't give any output when invoked from command line for debugging purposes.	No
AES-22385	AES 8.1	On OAM page Security -> certificate management -> server certificates -> add Keeping enrollment method as Automatic gives error "Auto Enrollment failed, did not receive certificate from CA."	Select manual enrollment instead of Auto Enrollment on same page.
AES-21856	AES 8.1.2, CM 8.1.2	Calls didn't get drop properly and call recordings were missing on AWFOS	No
AES-19610	AES 7.1.3	LDAP configuration option for TSAPI user (cus_ldap) is not set following errors get printed in alarm.log, every time the cti user is logged in to AES pam_ldap(tsapi_service:account): unknown option: config=/etc/cus-ldap.conf pam_ldap(tsapi_service:auth): unknown option: config=/etc/cus-ldap.conf	No
AES-19365	AES 8.1.1	Tomcat partially sends logs bypassing the rsyslog utility. Hence, separate Catalina log files are generated under /var/log/tomcat directory.	No
AES-19215	AES 8.1	Possible race conditions in request and response and application not receiving the response.	No
AES-18144	AES 8.1	If the SNMP device is configured to use SNMP version 1 or 2c then the community name of length more than 128 characters is not allowed in the Security Name field on OAM -> Utilities -> SNMP -> SNMP trap receivers -> Add.	No
AES-34604	AES 10.2 KVM	The customer will not be able to enable encryption for 10.2 OVAs deployed on KVM (AES-10.2.0.0.0.198.20231107-e70-00-kvm.ova; **PLDS ID** AES00001038)	No

Avaya Solutions Platform

Avaya Solutions Platform S8300

For latest information, refer to the following Avaya solutions Platform Release Notes:

- Avaya Solutions Platform S8300 R6.x Release Notes
- Avaya Solutions Platform S8300 R5.1.x Release Notes

Avaya Solutions Platform 130

For latest information, refer to the following Avaya solutions Platform Release Notes:

- Avaya Solutions Platform 130 R6.x Release Notes
- Avaya Solutions Platform 130 R5.1.x Release Notes

Avaya Aura® G430 and G450 Media Gateways

What's new in Avaya Aura® G430 and G450 Media Gateways Release 10.2.x.x

What's new in G430 and G450 Media Gateways Release 10.2.1 (Builds 43.22.00 and 43.22.30)

The following new commands have been added for SSH Public Key Authentication:
copy authorized-keys usb

- copy https authorized-keys
- copy scp authorized-keys
- copy usb authorized-keys

These new Commands have been added under the ssh-server configuration command:

- show authorized-keys
- erase authorized-keys
- set pubkey-authentication
- show pubkey-authentication

Note: Admin users can modify keys for all users. Read-Write users can modify their own keys but no others. Read-Only users can view configuration but cannot modify any keys.

Finally, these commands have been modified:

- The "show ssh-server-configuration" was modified to display whether PKA is enabled and how much space is used.
- The "show ip ssh" was modified to also show whether PKA is enabled.

What's new in G430 and G450 Media Gateways Release 10.2 (Builds 43.09.00 and 43.09.30)

- TLS 1.3 support.
- wolfSSL Cryptographic Library replaces OpenSSL library used in previous G430 and G450 releases
- VxWorks OS updated to Release 6.9 in older gateways.
- New SNMP-server test trap CLI command.
- New Server Blade CLI commands (G450 only)
- Removed support for licensing of CM 5.2.1 and earlier CM releases.

For more information see ***What's New in Avaya Aura® Release 10.2.x*** document on the Avaya Support site: https://download.avaya.com/css/public/documents/101087359

Installation for Avaya Aura® G430 and G450 Media Gateways Release 10.2.x.x

Required patches

The following version of firmware is only applicable for G430 and G450 Media Gateways. Find patch information for other Avaya Aura® Media Branch Gateway products at https://support.avaya.com.
Customer impacting gateway issues will be addressed in new firmware versions within each supported gateway firmware series (e.g., 38.xx.xx is considered a firmware series). This ensures customer impacting fixes will be delivered and available within each supported gateway firmware series until designated as "End of Manufacturer Support". The latest gateway firmware version within a given firmware series should be used since it will have all the latest fixes. New gateway features and functionality will not be supported in configurations running newer series of gateway firmware with older Communication Manager Releases.
To help ensure the highest quality solutions for our customers, Avaya recommends the use of like gateway firmware series and Communication Manager releases. This means the latest version within the GW Firmware Series is recommended with the following Communication Manager software releases:

Gateway Firmware Series	Communication Manager Release

41.xx.xx	8.1.x
42.xx.xx	10.1.x
43.xx.xx	10.2.x

Newer gateway firmware versions running with older Communication Manager software releases are still supported. For example, running gateway firmware version series 42.xx.xx with Communication Manager 8.1.x is still supported. However, prolonged running in this type of mixed configuration is not recommended. Avaya recommends running in a mixed configuration only if necessary, to support gateway upgrades before upgrading Communication Manager software. Newer Communication Manager software releases running with older gateway firmware versions are not supported.
Gateway firmware support follows the Communication Manager software “End of Manufacturer Support” model (EoMS). This means that as soon as a Communication Manager release has gone End of Manufacturer Support, new gateway firmware will no longer be supported with that Communication Manager release.

For example, when Communication Manager 8.1.x goes End of Manufacturer Support, gateway firmware series 41.xx.xx will no longer be supported.

Pre-Install Instructions

The following is required for installation:

- Avaya Communication Manager Release 8.x.y or later should be used since earlier versions are no longer supported.
- Browser access to the Customer Support Web site (http://support.avaya.com), or another way to get the Target File.
- SCP, FTP, or TFTP applications on your PC or Local Computer or a USB drive formatted FAT32 file system.
- G430 or G450 Media Gateways hardware version 1 or greater.
- An EASG service login or a customer administrator login is required for gateway configuration.

File Download Instructions

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

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

.**Note:** To ensure a successful download when upgrading media modules, 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 10.1.x.y.

- **G450 Gateways running a release prior to Release 7.1.2 Build 39.5.0** MUST first install Release 7.1.0.5 (Build 38.21.03 or Build 38.21.33) or newer 38.xx.yy release before installing Release 10.1.x.y.

If you attempt to download Release 10.1.x.y prior to having installed Release 7.1.0.4 or Release 7.1.0.5 and execute the "`show download software status 10`" command, the system will display the following error message:

Incompatible software image for this type of device.

After installing Release 7.1.0.4 or Release 7.1.0.5, you must enable or disable Avaya Logins before downloading Release 10.1.x.y via CLI or SNMP. You can enable or disable Avaya Logins by using one of the following CLI commands:

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

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

- `copy ftp SW_imageA`
- `copy ftp SW_imageB`
- `copy scp SW_imageA`
- `copy scp SW_imageB`
- `copy tftp SW_imageA`
- `copy tftp SW_imageB`
- `copy usb SW_imageA`
- `copy usb SW_imageB`
- `copy https SW_imageA`
- `copy https SW_ImageB`

Beginning with the 10.2 release, the SSH client is now more restrictive in its support of key exchange (KEX) algorithms.
Prior to Rrelease 10.2, Build 43.30, the SSH client "kex" configuration must be set only to diffie-hellman-group14-sha1:

```
G450-120(super)# ssh-client-configuration
G450-120(super-ssh-client-configuration)# set kex
diffie-hellman-group14-sha1
KexAlgorithms: diffie-hellman-group14-sha1
Done!
G450-120(super-ssh-client-configuration)# exit
```

Failure to restrict the client kex configuration in this way may result in failed gateway to SSH-server connections (e.g. "copy scp" CLI commands).

Notes:

- The special "dadmin" login account previously associated with ASG in releases earlier than Release 7.1.2 is no longer available.
- The gateway defaults to using TLS 1.2, PTLS, and unencrypted H.248 communication with CM. Refer to the "set link-encryption" command to adjust these settings.
- The G430 will only download the G430 firmware specific to its vintage. Firmware for G430 Vintage 3 must only use firmware having "g430v3_" indicated in the firmware image's filename. All other G430 vintages must only use firmware having "g430_" indicated in the firmware image's filename.
- The G450 will only download G450 firmware specific to its hardware vintage. Firmware for G450 Vintage 4 must only use firmware having "g450v4_" indicated in the firmware image's filename. All other G450 vintages must only use firmware having "g450_" indicated in the firmware image's filename.

For information about installing G430 and G450 Gateway firmware, refer to the "Installing the Branch Gateway" section in the following documents:

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

Troubleshooting the installation

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

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

Restoring software to the previous version

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

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

Software Information

Software	Version	Note
OS	G430 hardware vintage 1 and 2: VxWorks 6.9 G430 hardware vintage 3: VxWorks 7 G450 hardware vintage 1 thru vintage 3: VxWorks 6.9 G450 hardware vintage 4 VxWorks 7	
Crypto Libraries	wolfSSL 5.6.3	The wolfSSL library replaces the OpenSSL library used in previous G430 and G450 releases. Prior to Build 43.30.00 and 43.30.30, Client and server key exchange (kex) algorithms restricted to diffie-hellman-group14-sha1.

Fixes in G430 and G450 Media Gateways Release 10.2.x.x

Fixes in G430 and G450 Media Gateways Release 10.2.1.4 (Builds 43.30.00 and 43.30.30)

ID	Minimum conditions	Visible symptoms	Issue found in Release
CMG4XX-4742	TLS Certificates	The show root-ca” and "show gw-identity-cert" commands caused an exception to be logged on older G450 and G430 hardware versions (G450 v1-3 and G430 v1-2).	10.2

CMG4XX-4742	TLS Certificates G430v3, G450v4	The "show root-ca” may cause a reboot when entering ‘q’ to break out of displaying a very large certificate bundle.	10.2
CMG4XX-4742	TLS Certificates	A new certificate index option was added to the "show root-ca" command to make it easier to display a specific certificate within a large bundle. Usage: show root-ca <app> [<index> [<cert>]]	10.2.1
CMG4XX-4782	SSH	Two new CLI commands have been added for hostkey algorithm configuration for SSH Client (ssh-client-configuration) and SSH Server (ssh-server-configuration): set hostkey-algorithms <alg> <alg> … show hostkey-algorithms These commands allow users to specify the hostkey algorithms used in the client/server proposals to the peer. This is in response to some customer's security scanners having objected to the use of ssh-rsa, mainly because of its use of SHA-1. The hostkey algorithms now available are: ssh-rsa rsa-sha2-256 rsa-sha2-512 ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp521	10.2.1
CMG4XX-4786	SSH	The default Key Exchange algorithms have been changed and new Key Exchange algorithms have been added for SSH Client and Server. The default kex algorithms used for the SSH client are now only those that won’t fail due to NIST SP 800-56A Rev. 3. The legacy diffie-hellman-group14-sha1 is still supported as a default, but security scanner complaints about SHA-1 required adding the following algorithms: ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521.	10.2.1

Fixes in G430 and G450 Media Gateways Release 10.2.1.3 (Builds 43.28.00 and 43.28.30)

ID	Minimum conditions	Visible symptoms	Issue found in Release
CMG4XX-4657	"test voip” CLI	The "test voip" CLI command reported incorrect DSP Test results on a fully functioning DSP immediately after a gateway was rebooted and prior to any VoIP calls being made (i.e. it would indicate ABORT Error Codes and loopback test failures).	10.2.1.2

Fixes in G430 and G450 Media Gateways Release 10.2.1.2 (Builds 43.26.00 and 43.26.30)

ID	Minimum conditions	Visible symptoms	Issue found in Release
CMG4XX-4590	Analog Ring Ping duration	Communication Manager provides the ability to program a station so that a button can remotely unlock a door using a relay connected to an analog port. The duration of the analog Ring-Ping signal used by the gateway to support this feature has been changed to 600ms when using Communication Manager (CM) Release 10.1.3.6 or later. A duration of 200ms will continue to be used when an earlier CM Release is used.	7.0
CMG4XX-4616	Service Port access after upgrade	Fixed an issue where gateways that upgraded from firmware versions 41.38.xx through 43.24.xx could not be accessed via the services port after a nvram init was performed.	10.1.0.2
CMG4XX-4625	Fast ethernet and Services port	The "show interface" command for the FastEthernet and Services ports has been updated to also display speed of 1 Gigabit for new gateways that support this speed (i.e. G430v3, G450v4).	10.1
CMG4XX-4627	HTTP Client download	Fixed an issue with the gateway's HTTP client being unable to successfully download files when TLS 1.3 is configured.	10.2
CMG4XX-4628	OSPF	Fixed an issue where a gateway that had OSPF enabled could not be accessed after upgrading to firmware version 42.32.0 and later.	10.1.2
CMG4XX-4633	SCP upload	Fixed issue where some SCP upload errors were not being reported by the CLI 'show upload status' command.	10.1

Fixes in G430 and G450 Media Gateways Release 10.2.1.1 (Builds 43.24.00 and 43.24.30)

ID	Minimum conditions	Visible symptoms	Issue found in Release
CMG4XX-4606	SSH	Fixed a small memory leak that was discovered to occur after SSH sessions using public key authentication are closed.	10.2.1
CMG4XX-4610	EASG	Fixed the EASGProductCert command to correctly display the product certificate's start and expiration dates.	10.2.1

Fixes in G430 and G450 Media Gateways Release 10.2.1.0 (Builds 43.22.00 and 43.22.30)

ID	Minimum conditions	Visible symptoms	Issue found in Release
CMG4XX-4508	G450v4 Compact Flash	On the G450v4, a reset could occur when an idle Compact Flash was inserted or removed. This behavior has been improved so that resets no longer occur on insertion or removal of idle Compact Flash.	10.2
CMG4XX-4523	G450v4 ASB Button	After pressing the ASB button the G450v4 gateway booted from the alternate bank as it should. However, subsequent CLI resets did not clear the ASB indicator, and the boot code continued to boot from the alternate bank.	10.1
CMG4XX-4575	QoS Traps	Fixed issue where the QoS Trap status was not saved correctly in the startup config.	10.1
CMG4XX-4582	SNMPv3 DES	DES is now allowed for SNMPv3 login authentication when not in FIPS mode in older G430s and G450s. This was added for backward compatibility.	10.2
CMG4XX-4586	FTP	Fixed a memory leak that was present in the gateway's FTP server.	8.1.3

Fixes in G430 and G450 Media Gateways Release 10.2.0.1 (Builds 43.13.00 and 43.13.30)

ID	Minimum conditions	Visible symptoms	Issue found in Release
CMG4XX-4450	Analog Lines	DTMF detection improved in analog lines having a very long length that experience a symptom known as "reverse twist".	8.1.3
CMG4XX-4466, CMG4XX-4467	VPN	Fixed an issue where a VPN session would fail due to an issue calculating the shared secret.	10.2
CMG4XX-4457	MM721 BRI Module	Fixed a sanity timeout issue that prevented an MM721 from properly coming into service immediately after its firmware has been updated.	10.1.3
CMG4XX-4471	SSH, “show crypto key” CLI command	Fixed the "show crypto key" CLI command so that gateway will not reset when invoked from an SSH session.	10.2

ID	Minimum conditions	Visible symptoms	Issue found in Release
CMG4XX-4476	TLS 1.3, “set link-encryption” CLI command	Fixed the "set link-encryption" CLI command so selecting TLS1.3 for H.248 will remain enabled after a reboot.	10.2
CMG4XX-4487	“copy https” CLI command	Fixed an issue where the ‘copy https’ commands did not use customer provided certificates and failed to download the startup-configuration.	10.2

Fixes in G430 and G450 Media Gateways Release 10.2 (Builds 43.09.00 and 43.09.30)

N/A

Known issues and workarounds in G430 and G450 Media Gateways Release 10.2.x.x

Known issues and workarounds in G430 and G450 Media Gateways Release 10.2

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

ID	Visible symptoms	Workaround
N/A	This BG version doesn't support multiple IPv6 VLAN interfaces.	Use single VLAN interface with IPv6.
N/A	In Edge Mode, the gateway may fail to register with CM after a gateway reboot if the registration source port range was configured to use a very small range of ports (e.g. "set registration source-port-range 1024 1025").	Use as wide a range as possible when using the "set registration source-port-range" command or use the "set registration default source-port-range" command.

Languages supported

- English

Documentation errata

- None

Avaya Aura® Media Server

For latest information, see the following Avaya Aura® Media Server Release Notes on the Avaya Support website:

- Release 10.1 Release Notes at: https://support.avaya.com/css/public/documents/101081316
- Release 10.2 Release Notes at: https://support.avaya.com/css/public/documents/101092135

Avaya WebLM

Note: WebLM did not require an update in the Aura 10.2 release and therefore Standalone WebLM 10.1.3.1 and higher release should continue to be used.

10.1.3.1 and higher standalone WebLM release supported version with Aura 10.2

For more information, see:

- ***Avaya Aura® Release Notes Release 10.1.x*** at: https://support.avaya.com/css/public/documents/101078965
- ***What's New in Avaya Aura® Release 10.2.x*** at: https://download.avaya.com/css/public/documents/101087359

Avaya Aura® Device Services

NOTE: If System Manager is upgraded to 10.2.1.4 and AADS 10.2.1.x is upgraded to subsequent release other than 10.2.1.4, then the patch needs to applied to fix DRS Replication

Please refer PSN for details about the patch: https://support.avaya.com/css/public/documents/101095877

Required artifacts for Avaya Aura® Device Services Release 10.2.1.4

Filename	PLDS ID	File size (MB)	S/W Version number	Comments
aads-10.2.1.4.42.bin	AADS000000216	940	10.2.1.4	AADS 10.2.1.4 GA load

Installation for Avaya Aura® Device Services Release 10.2.1.4

Upgrading the Avaya Aura® Device Services software Release 10.2.1.4

IMPORTANT:

It would be recommended to take a snapshot of the existing load before the upgrade.

Upgrade from 10.2.1.3.13 to 10.2.1.4.42

- Upgrade SMGR to the latest 10.2/10.2.x GA load if needed.
- Upgrade SM(s) to the latest 10.2/10.2.x GA load if needed.
- Update to SSP20 (If not already updated)
    - Download SSP20 to admin user's home directory.
        - svc aads stop
        - av-update-os AV-AADS10.2-RHEL8.x-SSP-020-01.tar.bz2
        - SSP20 installation reboots the server at the end. After reboot, verify Security Service Pack 20 version
            - *av-version*
            - It shows the output as below

              OS_VERSION: Red Hat Enterprise Linux release 8.4 (Ootpa)
              AV_SSP_VERSION : 020
              AV_BUILD_NUMBER : 01

              Note:
              If cluster setup, please update SSP20 on all nodes before running "app upgrade"
    - svc aads start
- Download AADS 10.2.1.4 binary to admin user's home directory.
- Set executable permissions to AADS 10.2.1.4.42 binary.
    - *chmod 750 /home/admin/aads-10.2.1.4.42.bin*
- Remove inactive versions (if any) using command "*app removeinactive*"
- Use terminal multiplexer command "tmux" (useful in case if ssh connection drops during install/upgrade)
    - Start the install/upgrade on a tmux session.
    - To start tmux session, run
        - *tmux*

- Run install/upgrade as usual
- app upgrade ./aads-10.2.1.4.42.bin

- If the ssh terminal hangs or disconnects, login to vCenter VM console
  - First list all tmux sessions
  - *tmux ls* # output as shown below, the circled integer is session_id that will be used to re-attach in next step
  - 

- To reattach to the running tmux session, shown in above step
  - tmux attach-session -t 0
  - the screen should re-attach to earlier screen created using tmux

Note: If cluster setup, please install "aads-10.2.1.4.42.bin" first on seed node, later repeat this step for backup node

- Once installation/upgrade is done with all nodes, restart AADS services on seed node first. Once services on seed node are up and running, restart aads services on other nodes in cluster.
  - *svc aads restart*

Software only deployment: Upgrade from 10.2.1.3.13 to 10.2.1.4.42

- Upgrade SMGR to the latest 10.2/10.2.x GA load if needed.
- Upgrade SM(s) to the latest 10.2/10.2.x GA load if needed.
- Download AADS 10.2.1.4.42 binary to admin user's home directory.
- Set executable permissions to AADS 10.2.1.4.42 binary.
  - *chmod 750 /home/admin/aads-10.2.1.4.42.bin*
- Install AADS 10.2.1.4.42 binary
  - *app upgrade /home/admin/aads-10.2.1.4.42.bin*
- **Note:** If cluster setup, please install "aads-10.2.1.4.42.bin" first on seed node, later repeat this step for backup node
  - Once installation/upgrade is done with all nodes, restart AADS services on seed node first. Once services on seed node are up and running, restart aads services on other nodes in cluster.
    - *svc aads restart*
- **Note for AADS software only deployment on Fresh RHEL 8.10 system:** If want to install AADS 10.2.1 on fresh RHEL 8.10 system, please use "*aads-swonly-10.2.1.0.41.tgz*"

For detailed information about upgrading Avaya Aura® Device Services, please refer Avaya Aura® Device Services Administration Guide at: https://support.avaya.com

Additional supported upgrade paths

- AADS 10.2.1.x => AADS 10.2.1.4

Fixes in Avaya Aura® Device Services 10.2.1.4

ID	Minimum conditions	Visible symptoms	Issue found in Release
ACS-30758	All AADS services are up and running on all nodes	AADS clears the LOCKED_PREFERENCES	10.2.1.2

		and OBSCURE_PREFERENCES parameter in autoconfig	
ACS-30756		Improve backup/restore procedure	10.2, 10.2.x
ACS-30755	All AADS services are up and running on all nodes	After the httpd upgrade, the software is impacted: systemctl stop/start/restart commands are not working, and the encrypt/decrypt files are missing	10.2
ACS-30754	All AADS services are up and running on all nodes	CFD-1-APD3MOX AADS returns only 2 SMs with fixed-region policy	10.2.1.2
ACS-30629	All AADS services are up and running on all nodes	pgstartup.log file does not rotate, and its size increases when DRS is down or in a synchronizing state.	10.2.x
ACS-30628	All AADS services are up and running on all nodes	AADS installation failed when selecting Data Center DC2 while the seed node is configured in DC1	10.2.0.1
ACS-30603	All AADS services are up and running on all nodes	1-AJZ4N99 - For Aura setup SM options from configuration utility was disabled [Megatech Communication GmbH]	10.2.1
ACS-30578	All AADS services are up and running on all nodes	Role recursion value changes in the GUI are not updating in the database, causing a break-FI scenario	10.2.1.1
ACS-30780	All AADS services are up and running on all nodes	Java 482 security policy changes break DRS client connections as Java is updated in AADS	10.2.x
ACS-29487	All AADS services are up and running on all nodes	keepalived-config.properties and aads-rules.nft files doesn't get updated as part	10.2.1.1

		of GUI change when switching to LB	
ACS-24082	All AADS services are up and running on all nodes	[Logs] "CAS_notification.log" and "notification_operations.log " should follow rotated rule, don't generate new log every time AADS services restarts	10.2.x
ACS-21333	All AADS services are up and running on all nodes	[8.1.4.0] Enhancement - should update correct tooltip and some element in Automatic Backup Configuration.	10.2.x
ACS-30779	All AADS services are up and running on all nodes	Address CVE-2026-21945 identified in the java-17 component used by Keycloak.	10.2.1.3
ACS-30757	All AADS services are up and running on all nodes	PostgreSQL Security Update – Fix for CVE-2025-12817 and CVE-2025-12818	10.2.1.3
ACS-30761	All AADS services are up and running on all nodes	Update logrotate configuration to use correct syslog PID file	10.2.x
ACS-30760	All AADS services are up and running on all nodes	CFD- 1-ARJ70Y5 Need to set replication factor based on available node like if its 12 node then set 8 instead of 3	10.2.1.1
ACS-30252	All AADS services are up and running on all nodes	CFD: PEA - 1-ADPF84Y AADS 10.2 (tomcat 9.0.71), in the admin.war web.xml does not have error 404 html file configured, however 403/408 are configured	10.2.x
ACS-30759	All AADS services are up and running on all nodes	Misleading log message when no LDAP certificate import is required.	10.2.x

ACS-28625	All AADS services are up and running on all nodes	CFD: Cassandra table user_picture remains un-updated after ldap sync	10.2.x
ACS-28074	All AADS services are up and running on all nodes	[IWA] Send Keytab File should show the popup whether the action was successful	10.2.x
ACS-30774	All AADS services are up and running on all nodes	Enable CORS configuration for port 8448 in nginx	10.2.1.2
ACS-30770	All AADS services are up and running on all nodes	Increase LDAP Retry Count to 3 for Better Reliability	10.2.x
ACS-30250	All AADS services are up and running on all nodes	CFD: PEA - 1-ADPF84Y The AADS 10.2 has tomcat 9.0.71 in which the admin.war has JS JQuery UI of version 1.11.3 which is an old version of JQuery, while the customer wants this to be of the latest version.	10.2.0.1
ACS-30777	All AADS services are up and running on all nodes	add validation checks that prevent duplicate JSON imports in Dynamic configuration.	10.2.x

Required artifacts for Avaya Aura® Device Services Release 10.2.1.3

Filename	PLDS ID	File size (MB)	S/W Version number	Comments
aads-10.2.1.3.13.bin	AADS000000209	940	10.2.1.3	AADS 10.2.1.3 GA load

Installation for Avaya Aura® Device Services Release 10.2.1.3

Upgrading the Avaya Aura® Device Services software Release 10.2.1.3

IMPORTANT:

It would be recommended to take a snapshot of the existing load before the upgrade.

Upgrade from 10.2.1.2.7 to 10.2.1.3.13

- Upgrade SMGR to the latest 8.1.3.x/10.1/10.2.x GA load if needed.
- Upgrade SM(s) to the latest 8.1.3.x/10.1/10.2.x GA load if needed.
- Update to SSP15 (If not already updated)
    - Download SSP15 to admin user's home directory.

- svc aads stop
- av-update-os AV-AADS10.2-RHEL8.x-SSP-015-01.tar.bz2
- SSP15 installation reboots the server at the end. After reboot, verify Security Service Pack 15 version
  - *av-version*
  - It shows the output as below

    OS_VERSION: Red Hat Enterprise Linux release 8.4 (Ootpa)
    AV_SSP_VERSION : 015
    AV_BUILD_NUMBER : 01

    Note:
    If cluster setup, please update SSP15 on all nodes before running "app upgrade"
- svc aads start

- Download AADS 10.2.1.3 binary to admin user's home directory.
- Set executable permissions to AADS 10.2.1.3.13 binary.
  - *chmod 750 /home/admin/aads-10.2.1.3.13.bin*
- Remove inactive versions (if any) using command "*app removeinactive*"
- Use terminal multiplexer command "tmux" (useful in case if ssh connection drops during install/upgrade)
  - Start the install/upgrade on a tmux session.
  - To start tmux session, run
    - *tmux*
    - Run install/upgrade as usual
    - app upgrade ./aads-10.2.1.3.13.bin
  - If the ssh terminal hangs or disconnects, login to vCenter VM console
    - First list all tmux sessions
    - *tmux ls* # output as shown below, the circled integer is session_id that will be used to re-attach in next step
    - 

  - To reattach to the running tmux session, shown in above step
    - tmux attach-session -t 0
    - the screen should re-attach to earlier screen created using tmux

Note: If cluster setup, please install "aads-10.2.1.3.13.bin" first on seed node, later repeat this step for backup node

- Once installation/upgrade is done with all nodes, restart AADS services on seed node first. Once services on seed node are up and running, restart aads services on other nodes in cluster.
  - *svc aads restart*

Software only deployment: Upgrade from 10.2.1.2.7 to 10.2.1.3.13

- Upgrade SMGR to the latest 8.1.3.x/10.1/10.2 GA load if needed.
- Upgrade SM(s) to the latest 8.1.3.x/10.1/10.2 GA load if needed.
- Download AADS 10.2.1.3.13 binary to admin user's home directory.
- Set executable permissions to AADS 10.2.1.3.13 binary.

    - *chmod 750 /home/admin/aads-10.2.1.3.13.bin*
- Install AADS 10.2.1.3.13 binary
    - *app upgrade /home/admin/aads-10.2.1.3.13.bin*
- **Note:** If cluster setup, please install "aads-10.2.1.3.13.bin" first on seed node, later repeat this step for backup node
    - Once installation/upgrade is done with all nodes, restart AADS services on seed node first. Once services on seed node are up and running, restart aads services on other nodes in cluster.
        - *svc aads restart*
- **Note for AADS software only deployment on Fresh RHEL 8.10 system:** If want to install AADS 10.2.1 on fresh RHEL 8.10 system, please use "*aads-swonly-10.2.1.0.41.tgz*"

For detailed information about upgrading Avaya Aura® Device Services, please refer Avaya Aura® Device Services Administration Guide at: https://support.avaya.com

Additional supported upgrade paths

- AADS 10.2 GA => AADS 10.2.1.3
- AADS 10.2.x => AADS 10.2.1.3

Fixes in Avaya Aura® Device Services 10.2.1.3

ID	Minimum conditions	Visible symptoms	Issue found in Release
ACS-30525	All AADS services are up and running on all nodes	CFD: PEA - 1-AGBDAJU | AADS nginx:could not allocate new session in SSL	10.2.x
ACS-30591	All AADS services are up and running on all nodes	PCI Vuln - On-prem - 249644 - Red Hat Update for keepalived (RHSA-2025:0743)	10.2.x
ACS-30630	All AADS services are up and running on all nodes	Automated backup process removes only the current snapshot but does not delete old ones if the backup fails or there is a disk space issue	10.2.x
ACS-30632	All AADS services are up and running on all nodes	PEA 1-APH3GGV After successfully upgrade to 10.2.1.2.7 on backup node, unable to start httpd(utilserv) service	10.2.1.2.7
ACS-30633	All AADS services are up and running on all nodes	Update the java-17-openjdk package to address the security vulnerabilities covered under RHSA-2025:10867 for RHEL 8 x86_64	10.2.x

ACS-30640	All AADS services are up and running on all nodes	Upgrade Apache Tomcat 9 to version 9.0.111 patch CVE-2025-55752	10.2.x
ACS-30641	All AADS services are up and running on all nodes	PEA# 1-AMQ92VW: Configurations url does not work when iView Server is unreachable or disabled	10.2.x

Required artifacts for Avaya Aura® Device Services Release 10.2.1.2

Filename	PLDS ID	File size (MB)	S/W Version number	Comments
aads-10.2.1.2.7.bin	AADS000000200	938	10.2.1.2	AADS 10.2.1.2 GA load

Installation for Avaya Aura® Device Services Release 10.2.1.2

Upgrading the Avaya Aura® Device Services software Release 10.2.1.2

IMPORTANT:

It would be recommended to take a snapshot of the existing load before the upgrade.

Upgrade from 10.2.1.1.22 to 10.2.1.2.7

- Upgrade SMGR to the latest 8.1.3.x/10.1/10.2.x GA load if needed.
- Upgrade SM(s) to the latest 8.1.3.x/10.1/10.2.x GA load if needed.
- Update to SSP14
    - Download SSP14 to admin user's home directory.
        - svc aads stop
        - av-update-os AV-AADS10.2-RHEL8.x-SSP-014-01.tar.bz2
        - SSP14 installation reboots the server at the end. After reboot, verify Security Service Pack 14 version
            - *av-version*
            - It shows the output as below

              OS_VERSION: Red Hat Enterprise Linux release 8.4 (Ootpa)
              AV_SSP_VERSION : 014
              AV_BUILD_NUMBER : 01

              Note:
              If cluster setup, please update SSP14 on all nodes before running "app upgrade"
    - svc aads start
- Download AADS 10.2.1.2 binary to admin user's home directory.
- Set executable permissions to AADS 10.2.1.2.7 binary.
    - *chmod 750 /home/admin/aads-10.2.1.2.7.bin*
- Remove inactive versions (if any) using command "*app removeinactive*"
- Use terminal multiplexer command "tmux" (useful in case if ssh connection drops during install/upgrade)

- Start the install/upgrade on a tmux session.
- To start tmux session, run
  - *tmux*
  - Run install/upgrade as usual
  - app upgrade ./aads-10.2.1.2.7.bin
- If the ssh terminal hangs or disconnects, login to vCenter VM console
  - First list all tmux sessions
  - *tmux ls* # output as shown below, the circled integer is session_id that will be used to re-attach in next step
  - 

- To reattach to the running tmux session, shown in above step
  - tmux attach-session -t 0
  - the screen should re-attach to earlier screen created using tmux

Note: If cluster setup, please install "aads-10.2.1.2.7.bin" first on seed node, later repeat this step for backup node

- Once installation/upgrade is done with all nodes, restart AADS services on seed node first. Once services on seed node are up and running, restart aads services on other nodes in cluster.
  - *svc aads restart*

Software only deployment: Upgrade from 10.2.1.1.2 to 10.2.1.2.7

- Upgrade SMGR to the latest 8.1.3.x/10.1/10.2 GA load if needed.
- Upgrade SM(s) to the latest 8.1.3.x/10.1/10.2 GA load if needed.
- Download AADS 10.2.1.2.7 binary to admin user's home directory.
- Set executable permissions to AADS 10.2.1.2.7 binary.
  - *chmod 750 /home/admin/aads-10.2.1.2.7.bin*
- Install AADS 10.2.1.2.7 binary
  - *app upgrade /home/admin/aads-10.2.1.2.7.bin*
- **Note:** If cluster setup, please install "aads-10.2.1.2.7.bin" first on seed node, later repeat this step for backup node
  - Once installation/upgrade is done with all nodes, restart AADS services on seed node first. Once services on seed node are up and running, restart aads services on other nodes in cluster.
    - *svc aads restart*
- **Note for AADS software only deployment on Fresh RHEL 8.10 system:** If want to install AADS 10.2.1 on fresh RHEL 8.10 system, please use "*aads-swonly-10.2.1.0.41.tgz"*

For detailed information about upgrading Avaya Aura® Device Services, please refer Avaya Aura® Device Services Administration Guide at: https://support.avaya.com

Additional supported upgrade paths

- AADS 10.2 GA => AADS 10.2.1.2
- AADS 10.2.x => AADS 10.2.1.2

Fixes in Avaya Aura® Device Services 10.2.1.2

ID	Minimum conditions	Visible symptoms	Issue found in Release
ACS-22214	All AADS services are up and running on all nodes	Utility server logs under location /var/log/Avaya/httpd_log/ do not rotate	10.2.x
ACS-30388	All AADS services are up and running on all nodes	CFD: PEA - 1-AF1M8J6 | NESSUS SCAN showing no HSTS Header on Port 9443 for AADS	10.1.1.x
ACS-30480	All AADS services are up and running on all nodes	CFD: PEA - 1-AFIM3IN | Customer is using the SMGR GUI to send test alarm for AADS it's failing	10.1.1.x
ACS-30622	All AADS services are up and running on all nodes	Can't delete Appcast Item in AADS	10.2.1.1
ACS-30623	All AADS services are up and running on all nodes	cron logs getting logs messages about older AADS versions	10.2.1.0
ACS-30624	All AADS services are up and running on all nodes	CFD: PEA - 1-AJF44R9 | AADS and SMGR replication is getting failed	10.2.1.0

What's new in Avaya Aura® Device Services Release 10.2.1.1

The following table lists the enhancements in Avaya Aura® Device Services 10.2.1.1

Enhancement	Description
ACS-30548	Updated the oauth client code to use http proxy
ACS-30575	Upgraded the tomcat Version to 9.0.102
ACS-30488	Filter SMGR contacts from search contacts.

- VMware ESXi 8.0.3 U3 platform support.

Required artifacts for Avaya Aura® Device Services Release 10.2.1.1

Filename	PLDS ID	File size (MB)	S/W Version number	Comments
aads-10.2.1.1.22.bin	AADS000000188	938	10.2.1.1	AADS 10.2.1.1 GA load

Installation for Avaya Aura® Device Services Release 10.2.x.x

Upgrading the Avaya Aura® Device Services software Release 10.2.1.1

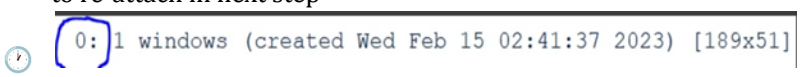
IMPORTANT:

It would be recommended to take a snapshot of existing load before the upgrade.

Upgrade from 10.2.1.0.41 to 10.2.1.1.22

- Upgrade SMGR to the latest 8.1/10.1/10.2.x GA load if needed.
- Upgrade SM(s) to the latest 8.1/10.1/10.2.x GA load if needed.
- Update to at least SSP11 (not required if already on SSP11)
    - Download SSP11 to admin user's home directory.
        - svc aads stop
        - av-update-os AV-AADS10.2-RHEL8.x-SSP-011-03.tar.bz2
        - SSP11 installation reboots the server at the end. After reboot, verify Security Service Pack 11 version
            - *av-version*
            - It shows the output as below

              OS_VERSION: Red Hat Enterprise Linux release 8.4 (Ootpa)
              AV_SSP_VERSION : 011
              AV_BUILD_NUMBER : 03

              Note:
              If cluster setup, please update SSP11 on all nodes before running "app upgrade"
    - svc aads start
- Download AADS 10.2.1.1 binary to admin user's home directory.
- Set executable permissions to AADS 10.2.1.1.22 binary.
    - chmod 750 /home/admin/aads-10.2.1.1.22.bin
- Remove inactive versions (if any) using command "*app removeinactive*"
- Use terminal multiplexer command "tmux" (useful in case if ssh connection drops during install/upgrade)
    - Start the install/upgrade on a tmux session.
    - To start tmux session, run
        - *tmux*
        - Run install/upgrade as usual
        - app upgrade ./aads-10.2.1.1.22.bin
    - If the ssh terminal hangs or disconnects, login to vCenter VM console
        - First list all tmux sessions
        - *tmux ls* # output as shown below, the circled integer is session_id that will be used to re-attach in next step
        - 

    - To reattach to the running tmux session, shown in above step
        - tmux attach-session -t 0
        - the screen should re-attach to earlier screen created using tmux

Note: If cluster setup, please install "aads-10.2.1.1.22.bin" first on seed node, later repeat this step for backup node

- On Seed node, cassandra rebuild may take 15-20 minutes during upgrade depending on the data.
- Once installation/upgrade is done with all nodes, restart AADS services on seed node first. Once services on seed node are up and running, restart aads services on other nodes in cluster.
    - svc aads restart

Software only deployment: Upgrade from 10.2.1.0.41 to 10.2.1.1.22

- Upgrade SMGR to the latest 8.1/10.1/10.2 GA load if needed.
- Upgrade SM(s) to the latest 8.1/10.1/10.2 GA load if needed.
- Download AADS 10.2.1.1.22 binary to admin user's home directory.
- Set executable permissions to AADS 10.2.1.1.22 binary.

chmod 750 /home/admin/aads-10.2.1.1.22.bin

- Install AADS 10.2.1.1.22 binary

app upgrade /home/admin/aads-10.2.1.1.22.bin

- **Note:** If cluster setup, please install "aads-10.2.1.1.22.bin" first on seed node, later repeat this step for backup node
    - On Seed node, cassandra rebuild may take 15-20 minutes during upgrade depending on the data.
    - Once installation/upgrade is done with all nodes, restart AADS services on seed node first. Once services on seed node are up and running, restart aads services on other nodes in cluster.
- **Note for AADS software only deployment on Fresh RHEL 8.10 system:** If want to install AADS 10.2.1 on fresh RHEL 8.10 system, please use "*aads-swonly-10.2.1.0.41.tgz"*

For detailed information about upgrading Avaya Aura® Device Services, please refer Avaya Aura® Device Services Administration Guide at: https://support.avaya.com

Additional supported upgrade paths

- AADS 10.1.1.x => AADS 10.2.1.1
- AADS 10.2 GA => AADS 10.2.1.1
- AADS 10.2.x => AADS 10.2.1.1

Fixes in Avaya Aura® Device Services 10.2.1.1

ID	Minimum conditions	Visible symptoms	Issue found in Release
ACS-30516	All AADS services are up and running on all nodes	"app status" command returns nftables error. Port 24010.2.1.0 (tcp) not found in nftables	10.2.x
ACS-29780	All AADS services are up and running on all nodes	SRV record does not switch when primary LDAP server is down	10.1.1.x
ACS-30522	All AADS services are up and running on all nodes	Alarm reported on Jan 16th is not cleared (SMGR/DRS)	10.2.0.1

What's new in Avaya Aura® Device Services Release 10.2.1.0

The following table lists the enhancements in Avaya Aura® Device Services 10.2.1.0

Enhancement	Description
ACS-29852	Keycloak logging improvement
ACS-29761	Keycloak with FIPS support
ACS-29959	RHEL 8.10 Support

For more information, see ***What's New in Avaya Aura® Release 10.2.x*** document on the Avaya Support site: https://download.avaya.com/css/public/documents/101087359

Security Service Pack

Security Service Pack

For further information on SSP contents and installation procedures for AADS 10.2.x, please see PSN document for SSP on https://support.avaya.com.

SSPs cannot be installed on "software-only" deployments.

Required artifacts for Avaya Aura® Device Services Release 10.2.1.0

Filename	PLDS ID	File size (MB)	S/W Version number	Comments
aads-10.2.1.0.41.bin	AADS000000183	960	10.2.1.0	AADS 10.2.1.0 GA load
aads-swonly-10.2.1.0.41.tgz	AADS000000184	969	10.2.1.0	AADS 10.2.1.0 software only bundle
AV-AADS10.2-RHEL8.10-OS Update-001.tar.bz2	AADS000000185	734	10.2.x	AADS RHEL 8.10 OS upgrade patch

Software information

Software	Version	Note
Database	Cassandra 4.1.3 Postgres 13.3	Avaya Aura Device Services databases. Cassandra: Application database Postgres: SMGR Replication and keycloak database
OS	RHEL 8.4 64 bit	Used as the operating system for the AADS OVA. It is required in the case of Software Only deployment.

Open JDK	1.8 update 382 64 bit java-17-openjdk-17.0.14.0.7-3.el8.x86_64	For AADS application, Open JDK 1.8.0-java-1.8.0-openjdk-1.8.0.382 For keycloak, java-17-openjdk- 17.0.14.0.7-3.el8.x86_64
Application Server	nginx-1.20.2-1 Tomcat- 9.0.102-1	Nginx: Reverse proxy server Tomcat: Application server
Supported Browsers	Chrome (minimum version 117.0)	Earlier versions of Chrome are not supported
	Edge (minimum version 117.0)	Earlier versions of Edge are not supported
	Firefox (minimum version 118.0)	Earlier versions of Firefox are no longer supported.
VMware vCenter Server, ESXi Host	7.0.X, 8.0, 8.0 Update 2	Earlier versions of VMware are no longer supported. Avaya Aura® Release 10.2.x supports VMware 8.0 and VMware 8.0 Update 2. Avaya Aura® Release 10.2.x does not support VMware 8.0 Update 1. For information about known issues, see VMware 8.0 Update 1 Release Notes on the VMware website at https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-6vcenter-server-801-release-notes/index.html.

Installation for Avaya Aura® Device Services Release 10.2.x.x

Upgrading the Avaya Aura® Device Services software Release 10.2.1.0

IMPORTANT:

It would be recommended to take a snapshot of existing load before the upgrade.

Upgrade from 10.2.0.1.16 to 10.2.1.0.41

- Upgrade SMGR to the latest 8.1/10.1/10.2.x GA load if needed.
- Upgrade SM(s) to the latest 8.1/10.1/10.2.x GA load if needed.
- Update to at least SSP8 (not required if already on SSP8 or any latest)
    - Download SSP8 to admin user's home directory.
        - svc aads stop
        - av-update-os AV-AADS10.1-RHEL8.4-SSP-008-02.tar.bz2
        - SSP8 installation reboots the server at the end. After reboot, verify Security Service Pack 8 version
            - *av-version*
            - It shows the output as below

              OS_VERSION: Red Hat Enterprise Linux release 8.4 (Ootpa)

```
AV_SSP_VERSION : 008
AV_BUILD_NUMBER : 02
---------------------------------
```

Note:
If cluster setup, please update SSP8 on all nodes before running "app upgrade"

- svc aads start

- Download AADS 10.2.1.0 binary to admin user's home directory.
- Set executable permissions to AADS 10.2.1.0.41 binary.
  - chmod 750 /home/admin/aads-10.2.1.0.41.bin
- Remove inactive versions (if any) using command "*app removeinactive*"
- Use terminal multiplexer command "tmux" (useful in case if ssh connection drops during install/upgrade)
  - Start the install/upgrade on a tmux session.
  - To start tmux session, run
    - *tmux*
    - Run install/upgrade as usual
    - app upgrade ./aads-10.2.1.0.41.bin
  - If the ssh terminal hangs or disconnects, login to vCenter VM console
    - First list all tmux sessions
    - *tmux ls* # output as shown below, the circled integer is session_id that will be used to re-attach in next step
    - `0: 1 windows (created Wed Feb 15 02:41:37 2023) [189x51]`
  - To reattach to the running tmux session, shown in above step
    - tmux attach-session -t 0
    - the screen should re-attach to earlier screen created using tmux

Note: If cluster setup, please install "aads-10.2.1.0.41.bin" first on seed node, later repeat this step for backup node

- On Seed node, cassandra rebuild may take 15-20 minutes during upgrade depending on the data.
- Once installation/upgrade is done with all nodes, restart AADS services on seed node first. Once services on seed node are up and running, restart aads services on other nodes in cluster.
  - svc aads restart

Software only deployment: Upgrade from 10.2.0.1.16 to 10.2.1.0.41

- Upgrade SMGR to the latest 8.1/10.1/10.2 GA load if needed.
- Upgrade SM(s) to the latest 8.1/10.1/10.2 GA load if needed.
- Download AADS 10.2.1.0.41 binary to admin user's home directory.
- Set executable permissions to AADS 10.2.1.0.41 binary.

  chmod 750 /home/admin/aads-10.2.1.0.41.bin

- Install AADS 10.2.1.0.41 binary

  app upgrade /home/admin/aads-10.2.1.0.41.bin

- **Note:** If cluster setup, please install "aads-10.2.1.0.41.bin" first on seed node, later repeat this

step for backup node
    - On Seed node, cassandra rebuild may take 15-20 minutes during upgrade depending on the data.
    - Once installation/upgrade is done with all nodes, restart AADS services on seed node first. Once services on seed node are up and running, restart aads services on other nodes in cluster.
- **Note for AADS software only deployment on Fresh RHEL 8.10 system:** If want to install AADS 10.2.1 on fresh RHEL 8.10 system, please use "*aads-swonly-10.2.1.0.41.tgz"*

For detailed information about upgrading Avaya Aura® Device Services, please refer Avaya Aura® Device Services Administration Guide at: https://support.avaya.com

Fixes in Avaya Aura® Device Services 10.2.1.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
ACS-29755	All AADS services are up and running on all nodes	AutoConfiguration Failure if SMGRLoginName is null for a given	10.2.x
ACS-30088	All AADS services are up and running on all nodes	CFD: PEA - 1-AB164LM | httpd process will not start on the SEED node after restarting aads services. (AVAYA - APS)	10.2.0.1
ACS-30052	All AADS services are up and running on all nodes	CFD: PEA - 1-AAGODRY | setSNMPTrapDestination.sh script does not work. (Daiwa Institute of Research)	10.2.x
ACS-30187	All AADS services are up and running on all nodes	Cassandra LOCAL_QUORUM issue for 2 Node Cluster.	10.2.0.1
ACS-30098	All AADS services are up and running on all (minimum 2 nodes)	AADS 10.2 needs at least 2 nodes in cluster up to function	10.2.0.1
ACS-30052	All AADS services are up and running on all nodes and any third-party SNMP server is configured	CFD: PEA - 1-AAGODRY | setSNMPTrapDestination.sh script does not work. (Daiwa Institute of Research)	10.2.x
ACS-30243	AADS software only system with RHEL 8.4 OS installed	swonly installer of system layer has RPM failures	10.2.x

Known issues and workarounds in Avaya Aura® Device Services in Release 10.2.1.0

ID	Summary	Affect versions	Workaround

ACS-29487	keepalived-config.properties and aads-rules.nft files updating don't get updated as part of GUI change when switching to LB	10.1	Update AADS_NODE_IP in /etc/nftables/aads-rules.nft manually if switched from internal LB to external LB, o.w. not required ip daddr <AADS_NODE_IP> tcp dport 443 counter packets 0 bytes 0 redirect to :8443
ACS-29461	Not able to login keyclaok admin GUI after rollback	10.2.x	Use Vmware snapshot feature before upgrading to 10.2