Avaya Aura® Release Notes

Release 10.2.x.x

Issue 1

December 2023

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.

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

Issue	Date	Description
1	18-December-2023	GA Release of Avaya Aura® Release 10.2.

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.

Note:

- The Avaya Aura® System Manager release/version must always be greater than or equal to the release/version of the components of the solution (Session Manager, Communication Manager, Application Enablement Services).
- 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
Avaya Aura® Communication Manager	X
Avaya Aura® Session Manager	X
Avaya Aura® System Manager	X
Avaya Aura® Presence Services	10.1.0.1.30
Avaya Aura® Application Enablement Services	X
Avaya Aura® G430 and G450 Media Gateways	X
Avaya WebLM Release	10.1.3.1
Avaya Aura® Media Server Reléase 10.1.x	10.1 SP5

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 10.2 release 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 10.1.0.1.30 with Avaya Breeze ® platform 3.9.0.0.390028 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 is 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 now a restricted offer and is not available for net new deployments. Existing Aura customers that have been running their deployments as software only will remain supported in Aura 10.2, however they are advised to migrate to a supported deployment platform by Aura 10.3 timeframe (October 2025). If you have any questions, please get in touch with your Avaya Sales/Accounts team
- 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.x*** 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.

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

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

2. 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.

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

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

Required artifacts for Communication Manager Release 10.2

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

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
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 now a restricted offer and is not available for net new deployments. Existing Aura customers that have been running their deployments as software only will remain supported in Aura 10.2, however they are advised to migrate to a supported deployment platform by Aura 10.3 timeframe (October 2025). If you have any questions, please get in touch with your Avaya Sales/Accounts team.*

Software information

Software	Version	Note
OS	Red Hat Linux Release 8.4 (Ootpa)	
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/8.0/rn/vsphere-6vcenter-server-801-release-notes/index.html.

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

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

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.	Customer sees call origination fails on the application.	10.1.2.0.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
	Place a Make Call request from this station to another. Use DLG interface to make the request towards AES		
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
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 disconnect 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	The action list does not execute.	10.1.0.2.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
	Write a breakpoint where call processing is used in action list		
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 Trigger resubscription by resetting the socket to ASM	CM does not resubscribe after the socket comes back up.	6.3.0.0
CM-44692	Call from DCP station to SIP trunk. DCP station should be on a PN. SIP trunk should take it's VoIP from AMS, and a IGC should be created between AMS and MP.	Talkpath does not come 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

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

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/101087646

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

The following section provides Session Manager 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
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

Filename	PLDS ID	File size	Version number	Comments
dmutility-10.2.0.0.1020019.bin	SM000001004	392 KB	1020019	DM Utility

Note: *The deployment of Avaya Aura applications as Software Only is now a restricted offer and is not available for net new deployments. Existing Aura customers that have been running their deployments as software only will remain supported in Aura 10.2, however they are advised to migrate to a supported deployment platform by Aura 10.3 timeframe (October 2025). If you have any questions, please get in touch with your Avaya Sales/Accounts team.*

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	
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 10.2.0.0

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.OAuth2 Token ERROR even though Push Notification is not enabled	10.1.0.0
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

ID	Minimum Conditions	Visible symptoms	Issue found in Release
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
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-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-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

ID	Minimum Conditions	Visible symptoms	Issue found in Release
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
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 export uses 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

ID	Minimum Conditions	Visible symptoms	Issue found in Release
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-88725	SIP Entity associated with the Adaptation which replaces IP addresses with Domain Name	Domain based routing fails	8.1.3.4
ASM-88362	SIP Remote worker registered to two data centers through SBC where data centers has 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 10.2.0.0

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
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.

ID	Minimum conditions	Visible symptoms	Workaround
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

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.x.x

Required artifacts for System Manager Release 10.2

The following section provides the System Manager downloading information. For deployment and upgrade procedure, 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
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 now a restricted offer and is not available for net new deployments. Existing Aura customers that have been running their deployments as software only will remain supported in Aura 10.2, however they are advised to migrate to a supported* *deployment platform by Aura 10.3 timeframe (October 2025). If you have any questions, please get in touch with your Avaya Sales/Accounts team.*

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

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 Arjun Sharma (arjunsharma@avaya.com) before the design or deployment.
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 feature 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.x.x

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

ID	Minimum conditions	Visible symptoms	Issue found in Release
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
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

ID	Minimum conditions	Visible symptoms	Issue found in Release
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
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

ID	Minimum conditions	Visible symptoms	Issue found in Release
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
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

ID	Minimum conditions	Visible symptoms	Issue found in Release
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
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

ID	Minimum conditions	Visible symptoms	Issue found in Release
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
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

ID	Minimum conditions	Visible symptoms	Issue found in Release
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 doesn't 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.x.x

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.

ID	Minimum conditions	Visible symptoms	Workaround
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/)	

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	
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	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	
Functionality												
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

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	
Virtual Machine M4anagement (start, stop, reset, status, dashboard)	Y	N	Y	Y	n/a	Y	Y	Y	Y	Y	Y	N
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.x.x

Logging framework is based on framework provided by Breeze platform. Framework version for PS 10.1.0.2 has been upgraded from Apache Log4j version 1.x to Apache Log4j version 2.x.

For more information see ***What's New in Avaya Aura® Release 10.1.x*** document on the Avaya Support site: https://download.avaya.com/css/public/documents/101087359

Note: TLS 1.2 will be used for Avaya Aura® Presence Services 10.1.0.0.63 until a future release of Breeze is able to support TLS 1.3.

Required artifacts for Presence Services Release 10.1.x.x

Required artifacts for Presence Services Release 10.1.x.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-10.1.0.0.76.zip	PS100100000	219 MB	10.1.0.0.76	Requires the use of Breeze 3.8.1 as a platform (minimum release)

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)
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)

Release	Minimum Required Version
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)

Upgrade References to Presence Services Release 10.1.x

Upgrade Quick Reference	Download	Prerequisite Downloads
Presence Services Customer Documentation	PresenceServices-Bundle-10.1.0.0.63.zip (PLDS ID: PS100100000)	Breeze 3.8.1 or higher Platform OVA – PS 10.1.0.0 is only compatible with Breeze 3.8.1 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
PresenceServices-LPS-SDK-7.1.2.0.182.zip	7.1.2	PS 7.1.2, PS 7.1.0 and PS 7.0.1
PresenceServices-LPS-SDK-7.1.0.0.556.zip	7.1.0	PS 7.1 and PS 7.0.1

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

Functionality not supported in Presence Services 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

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 display incorrectly when the user in a meeting (or OOTO) with 2 PS on the same SMGR	8.1.2

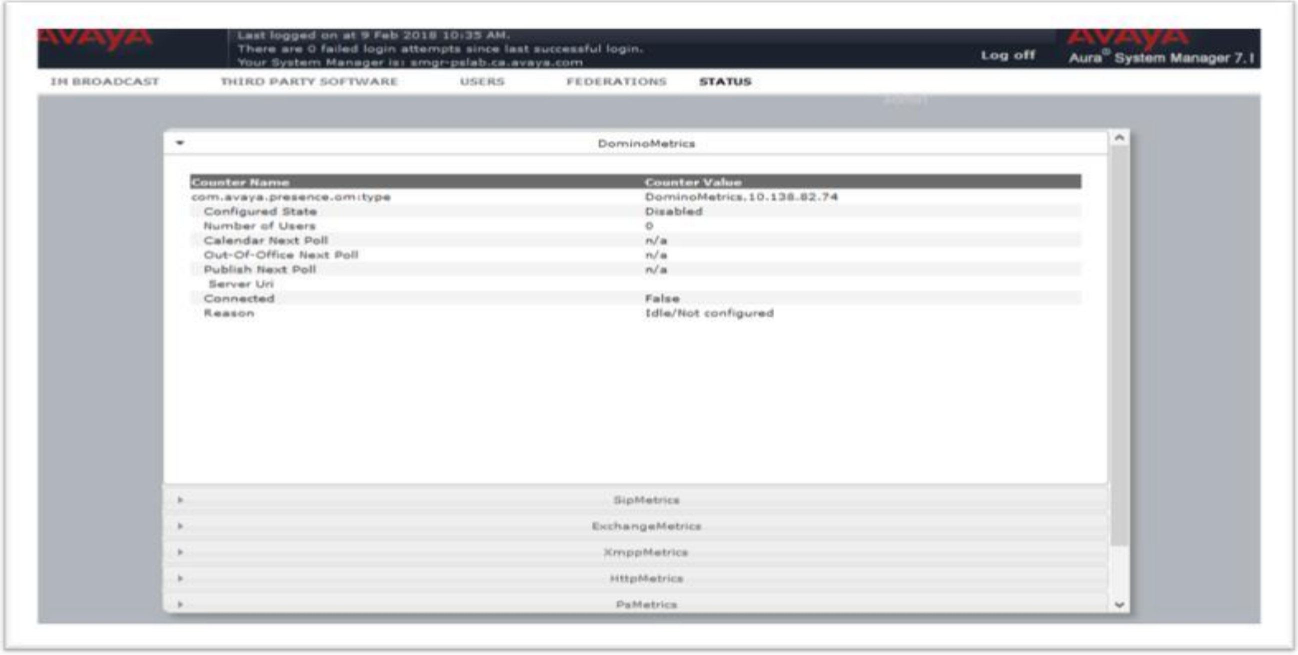
Known issues and workarounds in Presence Services Release 10.1.x.x

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

ID	Minimum conditions	Visible symptoms	Workaround
PSNG-12284		After the active node had lost network connection, it took 20 minutes for IM to back to normal	NA

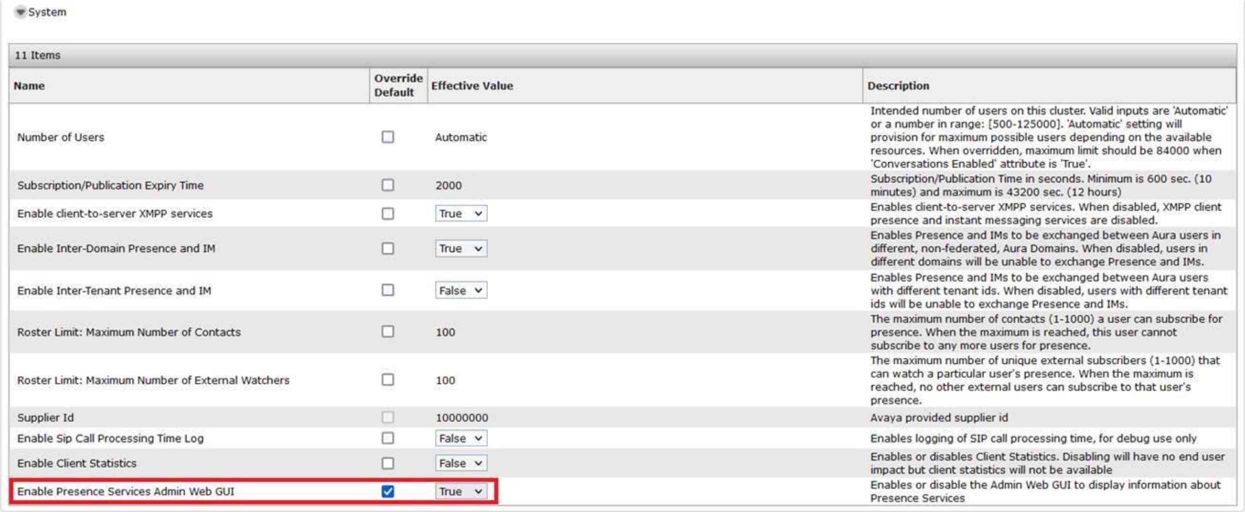
Note: The Presence Services Admin Web GUI, as shown below, is disabled by default in PS 8.1.1.0



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

Counter Name	Counter Value
com.avaya.presence.om:type	DominoMetrics.10.138.82.74
Configured State	Disabled
Number of Users	0
Calendar Next Poll	n/a
Out-Of-Office Next Poll	n/a
Publish Next Poll	n/a
Server Uri	
Connected	False
Reason	Idle/Not configured

To enable the Presence Services Admin Web GUI, 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 10.2.x.x

What’s new in Application Enablement Services 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 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

Filename	PLDS ID	File size	Version number	Comments
AES-10.2.0.0.0.198.20231107-e70-00.ova	AES00000990	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	AES00000991	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 now a restricted offer and is not available for net new deployments. Existing Aura customers that have been running their deployments as software only will remain supported in Aura 10.2, however they are advised to migrate to a supported deployment platform by Aura 10.3 timeframe (October 2025). If you have any questions, please get in touch with your Avaya Sales/Accounts team.*

Software information

Software	Version	Note
OS	Red Hat Linux Release 8.4 (Ootpa)	
Web Server	Apache Server 2.4.37	
Application Server	Apache Tomcat 9.0.71	

Software	Version	Note
Database	PostgreSQL 13.11	
Java	Open JDK 1.8.0_382-b05	
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

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			
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

ID	Minimum Conditions	Visible Symptoms
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

ID	Minimum Conditions	Visible Symptoms	Workaround
AES-32814	AES 10.1.3.1	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"
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-	Re-start the Media Monitor after DMCC station re-registers.

ID	Minimum Conditions	Visible Symptoms	Workaround
		registers after monitor is placed.	
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 Address/FQDN", "WebLM Port" and valid configuration of "Secondary WebLM IP Address/FQD	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
	N" and "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-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

ID	Minimum Conditions	Visible Symptoms	Workaround
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

Avaya Solutions Platform

Avaya Solutions Platform S8300

For latest information refer to Avaya Solutions Platform S8300 Release 5.1 Release Notes on the Avaya Support website at: https://download.avaya.com/css/public/documents/101080815

Avaya Solutions Platform 130

For latest information refer to Avaya Solutions Platform 130 Release 5.1 Release Notes on the Avaya Support website at: https://download.avaya.com/css/public/documents/101081340

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 (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, and only provides support for diffie-hellman-group14-sha1.

With 10.2, 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. 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 (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	Use as wide a range as possible when using the "set registration source-port-

ID	Visible symptoms	Workaround
	registration source port range was configured to use a very small range of ports (e.g. "set registration source-port-range 1024 1025").	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://download.avaya.com/css/public/documents/101081316

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 10.1.x*** at: https://download.avaya.com/css/public/documents/101087359

Avaya Aura® Device Services

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

- Release 10.1.1.1 Release Notes at:
  https://download.avaya.com/css/public/documents/101084735