Avaya Aura® Release Notes

Release 10.1.x.x

Issue 24

April 2024

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 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 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 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	13-December-2021	GA Release of Avaya Aura® Release 10.1.
2	24-December-2021	Updates to the Required Artifacts section of Application Enablement Services.
3	24-February-2022	Updates to the Functionality not supported for Release 10.1.x.x section of AE Services.
4	14-March-2022	Changes to the Introduction section for the ASP S8300 Release 5.1 supported for Communication Manager and Branch Session Manager.
5	18-April-2022	GA Release of Avaya Aura® Release 10.1.0.1.
6	04-May-2022	Updated the System Manager Known issues 10.1.0.1 section.
7	09-May-2022	Updated the Introduction section.
8	26-May-2022	Updates to the Avaya Aura® Device Services section.
9	17-June-2022	Updates to the Required artifacts for System Manager Release 10.1 section.
10	26-Sep-2022	GA Release of Avaya Aura® Release 10.1.0.2.
11	03-Oct-2022	Updates to the Known issues and workarounds in System Manager in Release 10.1.0.2 section.
12	14-Oct-2022	Updates to the Required artifacts for Session Manager Release 10.1.0.2 section.
13	03-Jan-2023	Updates to the Known issues and workarounds in Session Manager Release 10.1.0.2 section.
14	24-Jan-2023	Updates to the 10.1 GA OVA details in the Required artifacts section of Communication Manager, Session Manager, System Manager, and Application Enablement services. The 10.1 GA OVAs of these products are renewed and re-signed with the latest Avaya signed certificates and are also updated to support SHA256 hash algorithm.
15	13-Feb-2023	GA Release of Avaya Aura® Release 10.1.2.
16	23-Feb-2023	Updated the Communication Manager fixes section.
17	22-May-2023	GA Release of Avaya Aura® Release 10.1.3.
18	08-June-2023	Updates to the Required artifacts for System Manager Release 10.1.3 section.
19	11-June-2023	Updates to the Required artifacts for Avaya Aura® Communication Manager 10.1.2.0.0 section.
20	15-June-2023	Updates to the Required artifacts for Avaya Aura® Communication Manager 10.1.3.0.0 section.
21	14-July-2023	Updates to the Required artifacts for Avaya WebLM Release 10.1.2 section.
22	28-Aug-2023	GA Release of Avaya Aura® Release 10.1.3.1.
23	15-Jan-2024	GA Release of Avaya Aura® Release 10.1.3.2.
24	04-April-2024	Updated known issue and workarounds in System Manager 10.1.3.2.

Introduction

This document provides late-breaking information to supplement Avaya Aura® 10.1.x release software and documentation. For updated documentation, product support notices, and service pack information, go to the Avaya Support site at https://support.avaya.com.

Note:

- The Avaya Aura® System Manager release/version must always be greater than or equal to the release/version of the components of the solution (Session Manager, Communication Manager, Application Enablement Services).
- The Avaya Solutions Platform S8300 (ASP S8300) Release 5.1 is available for the Avaya Aura® 10.1 Communication Manager solutions that include LSPs/Survivable Remotes/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 10.1.x and BSM 10.1.x upgrade/deployment steps on the ASP S8300 Release 5.1, see the product documentation.

  There is compatibility between Aura 10.1 and 8.1.x components as long as the required order of upgrade is followed. Reference the Upgrading Avaya Aura® Communication Manager Release 10.1, Chapter 3: Planning, Section: Upgrade sequence for Avaya components.

  For information about Avaya Solutions Platform S8300, see PSN020547u.
- Avaya Aura® Release 10.1 is supported on Avaya Solutions Platform (ASP) S8300 Release 5.1 and ASP 130 Release 5.0 and 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 10.1.

  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://downloads.avaya.com/css/P8/documents/101078423

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	10.1.3.2	10.1.3.1	10.1.3	10.1.2	10.1.0.2	10.1.0.1	10.1
Avaya Aura® Communication Manager	X	X	X	X	X	X	X
Avaya Aura® Communication Manager SSP	X	X	X	X	X	X	
Avaya Aura® Session Manager	X	X	X	X	X	X	X
Avaya Aura® Session Manager SSP	X	X	X	X	X	X	
Avaya Aura® System Manager	X	X	X	X	X	X	X
Avaya Aura® System Manager SSP	X	X	X	X	X		
Avaya Aura® Presence Services	NA	NA	NA	NA	NA	NA	X
Avaya Aura® Application Enablement Services	X	X	X	X	X	X	X
Avaya Aura® Application Enablement Services SSP	X	X	X	X	X	X	
Avaya Aura® G430 and G450 Media Gateways	X	X	X	X	X	X	X
Avaya WebLM Release	X	X	NA	X	NA	NA	NA
Avaya WebLM SSP	X	X	X	X	NA	NA	NA
Avaya Device Adapter Snap-in	NA	NA	NA	X	NA	NA	X

Note:

- Security Service Packs (SSPs) will be released at or around the same time as the Feature Pack and / or Service Pack and sometimes on a more frequent cadence.
    - SSP required artifacts are tracked in the application specific Security Service Pack PCN. Please read the PCN for the appropriate SSP. The files integrate and are installed uniquely per application.
- Avaya Aura® Media Server Release 10.1.x.x is compatible with Avaya Aura® Release 10.1.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® Device Services Release 10.1.x..x is compatible with Avaya Aura® Release 10.1.x. Device Services Releases have a different release version and schedule. For more information, see Avaya Aura® Device Services Release Note 10.1.x.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).
- With this release 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 Communication Manager and Application Enablement Services.
- For software only environment, see PSN020558u - Avaya Aura® 10.1.x Software-only RPM updates.
- In Release 10.1.0.2, Communication Manager, System Manager, Session Manager, and G4xx 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 10.1.x*** document on the Avaya Support site. https://downloads.avaya.com/css/P8/documents/101078425

Future use fields visible in Avaya Aura® Release 10.1

The underlying framework for an upcoming new Avaya Aura® Platform enhancement "Avaya Aura Distributed Architecture" will be seen in some Release 10.1 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 10.1, 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 10.1.x.

With this release 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 Communication Manager and Application Enablement Services.

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 10.1.x.x

What's new in Communication Manager Release 10.1.3.1.0

Enhancement	Description
CM-53558	With CM 10.1.3.1.0 CM will support active enhanced call pickup notification when IOS workplace client registers.

For more information, see ***What's New in Avaya Aura® Release 10.1.x*** document on the Avaya Support site: https://downloads.avaya.com/css/P8/documents/101078425

IMPORTANT NOTE: Starting 10.1.3.1, licensing for Communication Manager (CM) and Application Enablement Services (AES) will only work with 10.1.3.1 and higher version of System Manager (SMGR) or Standalone WebLM (WebLM). If upgrading CM and/or AES to 10.1.3.1 and higher then the required order of upgrade is imperative i.e. SMGR and/or WebLM should be upgraded to 10.1.3.1 and higher first to ensure licensing for CM and/or AES does not stop working. CM and AES 10.1.3.0 were originally compatible with Standalone WebLM 10.1.2.0 (as there was no Standalone WebLM 10.1.3.0), however beginning with 10.1.3.1 and higher, Standalone WebLM 10.1.3.1 and higher is required for CM and AES. The Avaya Aura® System Manager release/version must always be greater than or equal to the release/version of the components of the solution (Session Manager, Communication Manager, Application Enablement Services).

What's new in Communication Manager Release 10.1.3.0.0

Enhancement	Description
CM-53057	With CM 10.1.3.0.0 CM will support OTHER24 Event to CMS for Calls originated from SIP endpoints that do NOT use off-hook INVITE for line reservation.
CM-53133	With CM 10.1.3.0.0 CM will speed up 911 SNMP call notification to Sentry.

For more information, see ***What's New in Avaya Aura® Release 10.1.x*** document on the Avaya Support site: https://downloads.avaya.com/css/P8/documents/101078425

What's new in Communication Manager Release 10.1.2.0.0

- From Release 10.1.2, System Manager Solution Deployment Manager and Solution Deployment Manager Client support the deployment and upgrade of application using the OVA with the SHA256 hash algorithm.
- Communication Manger 10.1 OVAs are re-spun to support SHA256 algorithm. For more information, see the Required artifacts section.
- The old 10.1 GA OVA contains the Avaya Signing certificate that is going to expire on Feb 20, 2023. Therefore, to address the Avaya signing certificate expiry, the new 10.1 GA OVAs are renewed and re-signed with the latest Avaya signed certificates. For more information, see PSN020586u - Avaya Aura® OVA Certificate Expiry February 2023.

For more information, see ***What's New in Avaya Aura® Release 10.1.x*** document on the Avaya Support site: https://downloads.avaya.com/css/P8/documents/101078425

What's new in Communication Manager Release 10.1.0.2.0

- Security Enhancement: JITC support for 10.1.0.2.0

- Security scans might flag the presence of Log4j 1.x files, Avaya is completely removing Log4j 1.x.
- All instances of Log4j 1.x have been removed from Communication Manager 10.1.0.2 as it is not utilized.

Enhancement	Description
CM-47762	The call routed to IVR (Interactive Voice Response) through CM (Communication Manager) vector/announcement could fail if the incoming invite contained SIP unknown header (X-*).
CM-38971	With CM10.1.0.2.0 SIP stations can be configured on Malicious Call Trace controller list to support launching a call to a group of users when one user invokes Malicious Call Trace. The SIP station will use crisis-alert button for notification.
CM-46980	With 10.1.0.2.0 SIP stations will show the “status station” with field “Service state” based on Reachability state or Registration event based instead of out-of-service. Also couple more fields added in the first page of “status station” status station 5381630 GENERAL STATUS Administered Type: 9611SIP Service State: out-of-service Connected Type: N/A Signal Status: not connected Extension: 538-1630 Network Region: Not Assigned Port: S005470 Parameter Download: pending Call Parked? no SAC Activated? no Ring Cut Off Act? No Active Coverage Option: 1 one-X Server Status: N/A EC500 Status: disabled Off-PBX Service State: (obsolete ?) Message Waiting: SIP STATION STATUS Connected Ports: Reg Subscription: active/not active CTI Monitoring: active/not Busied-out?: yes/no Active call(s)?: yes/no Note: • Removed in Red color • New fields in blue color

For more information, see ***What’s New in Avaya Aura® Release 10.1.x*** document on the Avaya Support site: https://downloads.avaya.com/css/P8/documents/101078425

What’s new in Communication Manager Release 10.1

With this release 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 Communication Manager (CM).

CRITICAL: The Security Service Pack installation framework for CM has changed in Release 10.1.x. It is imperative that the instructions in PCN2134S be reviewed for complete steps prior to installation of Security Service Packs on an CM 10.1.x system.

Beginning with CM Release 10.1, both Kernel and Linux updates will be provided in a Security Service Pack. There will no longer be a separate Kernel Service Pack (KSP).

The old method of installing Security Service Packs will not work in CM Release 10.1.
The minimum release of CM 10.1.x.x that you must be on in order to install the Security Service Packs for CM is 10.1.0.1.
The SSP can only be installed via the command line. There is no Solution Deployment Manager (SDM) or CM SMI support for SSP installation.
In order to install the SSP for CM 10.1.x.x, you must use the new command ("av-update-os") and follow the detailed instructions in PCN2134S.

For more information, see ***What’s New in Avaya Aura® Release 10.1.x*** document on the Avaya Support site: https://downloads.avaya.com/css/P8/documents/101078425

Future use fields visible in Avaya Aura® Communication Manager Release 10.1.x.x

Future use fields visible in Avaya Aura® Communication Manager Release 10.1

The underlying framework for an upcoming Avaya Aura® Platform enhancement "Avaya Aura Distributed Architecture" will be seen in some Release 10.1.x 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 10.1, but not active/usable.

1. Avaya Aura® Communication Manager Release 10.1.x 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 10.1.x 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 10.1.x, please see **PCN2134S**.

With this release 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 Communication Manager and Application Enablement Services.

CRITICAL: The Security Service Pack installation framework for CM has changed in Release 10.1.x. It is imperative that the instructions in PCN2134S be reviewed for complete steps prior to installation of Security Service Packs on an CM 10.1.x system.
Beginning with CM Release 10.1, both Kernel and Linux updates will be provided in a Security Service Pack. There will no longer be a separate Kernel Service Pack (KSP).

The old method of installing Security Service Packs will not work in CM Release 10.1.
The minimum release of CM 10.1.x.x that you must be on in order to install the Security Service Packs for CM is 10.1.0.1.
In order to install the SSP for CM 10.1.x.x, you must use the new command ("av-update-os") and follow the detailed instructions in PCN2134S.

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

Required artifacts for Avaya Aura® Communication Manager 10.1.x.x

Required artifacts for Avaya Aura® Communication Manager 10.1.3.2.0

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

Download ID	Artifact	Notes
CM000002034	01.0.974.0-28015.tar	10.1.3 Service Pack #02

Required artifacts for Avaya Aura® Communication Manager 10.1.3.1.0

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

Download ID	Artifact	Notes
CM000002029	01.0.974.0-27937.tar	10.1.3 Service Pack #01

IMPORTANT NOTE: Starting 10.1.3.1, licensing for Communication Manager (CM) and Application Enablement Services (AES) will only work with 10.1.3.1 and higher version of System Manager (SMGR) or Standalone WebLM (WebLM). If upgrading CM and/or AES to 10.1.3.1 and higher then the required order of upgrade is imperative i.e. SMGR and/or WebLM should be upgraded to 10.1.3.1 and higher first to ensure licensing for CM and/or AES does not stop working. CM and AES 10.1.3.0 were originally compatible with Standalone WebLM 10.1.2.0 (as there was no Standalone WebLM 10.1.3.0), however beginning with 10.1.3.1 and higher, Standalone WebLM 10.1.3.1 and higher is required for CM and AES. 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).

Required artifacts for Avaya Aura® Communication Manager 10.1.3.0.0

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

Filename	PLDS ID	File size In MB	S/W Version number	MD5 Check Sum	Comments
~~01.0.974.0-27867.tar~~	~~CM000002021~~	~~143.82~~	~~10.1.3.0.0~~	~~cdd9093de6d895767948eb6b062060c0~~	~~Feature Pack #03 released on 22nd May 2023~~
01.0.974.0-27893.tar	CM000002025	143.82	10.1.3.0.1	f312954e37c43b22fcfcc8d5aae19c8a	Feature Pack #03 released on 15th June 2023

Note: Replacing 10.1.3 with 10.1.3.0.1 to facilitate additional diagnostic capabilities for certain SIP troubleshooting scenarios. PLDS ID CM000002021 will be obsolete. The new 10.1.3.0.1 is updated to support, for more information, see PCN2133S.

Required artifacts for Avaya Aura® Communication Manager 10.1.2.0.0

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

Download ID	Artifact	Notes
~~CM000002017~~	~~01.0.974.0-27783.tar~~	~~Feature Pack #02~~
CM000002024	01.0.974.0-27892.tar	Feature Pack #02

Note: Replacing 10.1.2 with 10.1.2.0.1 to facilitate additional diagnostic capabilities for certain SIP troubleshooting scenarios. PLDS ID CM000002017 will be obsolete. The new 10.1.2.0.1 is updated to support, for more information, see PCN2133S.

Required artifacts for Communication Manager Release 10.1.0.2.0

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

Download ID	Artifact	Notes
CM000002012	01.0.974.0-27607.tar	Service Pack #02

Required artifacts for Communication Manager Release 10.1.0.1.0

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

Download ID	Artifact	Notes
CM000002006	01.0.974.0-27372.tar	Service Pack #01

Note: Service Pack 1 or later must be installed prior to installing any Security Service Pack.

Required artifacts for Communication Manager Release 10.1

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

Download ID	Artifact	Notes
CM000002000	CM-Simplex-010.1.0.0.974-e70-1.ova	CM Simplex OVA
CM000002001	CM-Duplex-010.1.0.0.974-e70-1.ova	CM Duplex OVA
~~CM000002000~~	~~CM-Simplex-010.1.0.0.974-e70-0.ova~~	~~CM Simplex OVA~~
~~CM000002001~~	~~CM-Duplex-010.1.0.0.974-e70-0.ova~~	~~CM Duplex OVA~~
CM000002002	CM-010.1.0.0.974-e70-0.iso	CM SW Only ISO
CM000002003	01.0.974.0-27247.tar	CM 10.1 SP0
CM000002005	01.0.974.0-27293.tar	SP0.1 of CM10.1

Note: The old 10.1 GA OVA contains the Avaya Signing certificate that is going to expire on Feb 20, 2023. Therefore, to address the Avaya signing certificate expiry, the new 10.1 GA OVAs are renewed and re-signed with the latest Avaya signed certificates. The new OVAs are also updated to support SHA256 hash algorithm. For more information, see PCN2133S.

For more information, see PSN020586u - Avaya Aura® OVA Certificate Expiry February 2023.

Installation for Avaya Aura® Communication Manager 10.1.x.x

Installation for Avaya Aura® Communication Manager 10.1.3.2.0

Installation for Avaya Aura® Communication Manager 10.1.3.1.0

Installation for Avaya Aura® Communication Manager 10.1.3.0.0

Installation for Avaya Aura® Communication Manager 10.1.2.0.0

Installation for Avaya Aura® Communication Manager Release 10.1

For information on the installation of Release 10.1, see **Upgrading Avaya Aura® Communication Manager.**

Communication Manager 10.1 software includes certain third-party components, including Open Source Software. Open Source Software licenses are included in the Avaya Aura® 10.1.

Communication Manager Solution Templates DVD. To view the licenses:

1. Insert the Avaya Aura® 10.1 Communication Manager Solution Templates DVD into the CD/DVD drive of a personal computer.
2. Browse the DVD content to find and open the folder D:\Licenses.
3. Within this folder are subfolders for Branch Gateway, Communication Manager, Installation Wizard, Session Manager, and Utility Services that contain the license text files for each application.
4. Right-click the license text file of interest and select Open With -> WordPad. This information is only accessible on the Communication Manager software DVD and is not installed or viewable on the Communication Manager Server.

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.

   a. Fully automated upgrade using SDM is not available for ASP 130 Release 5.0.
   b. The full automated upgrade using SDM can be used when migrating from a CM 7.x or 8.x to 10.x 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 Web site https://support.avaya.com.

Enhanced Access Security Gateway (EASG)

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

Fixes in Communication Manager Release 10.1.x.x

Fixes in Communication Manager Release 10.1.3.2.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
CM-55369	In certain situations, if there is a corruption of call records.	Callers hear silence instead of music when call is put on hold	10.1.0.2.0
CM-55323	Install SSP 18 and perform network config change via SMI.	SMI Network Config changes are not successful.	10.1.3.1.0
CM-55310	H323 station pressing audix button and hanging up the call within 2 seconds	Long calls are recorded, which are bogus.	10.1.3.0.1
CM-55283	Incoming call containing ANI length 14 (or more) digits and + sign lands on VDN which compares ANI with VRT.	Only first 13 digits get compared and rest get ignored.	10.1.2.0.0
CM-55211	Vector with collect digit step and announcement.	DTMF does not get collected, after call unhold	10.1.3.1.0
CM-55193	CM 10.1.3.1.0	NA	10.1.3.1.0
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-55165	Call between two SIP stations set to User-Defined in station form and using Sip trunk with Unicode set to Auto	Intermittently, unicode name gets sent to a user-defined phone.	10.1.0.2.0
CM-55099	Call transferred to a SIP station with EC500 enabled. Public number manipulation is enabled on the trunk.	Public number manipulation is not performed, wrong number sent to EC500 leg	10.1.2.0.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
CM-55081	Local DNS server not working or misconfigured.	CM trying to access DNS root server every night, which is visible in Firewall monitoring.	10.1.2.0.0
CM-55053	A Computer Telephony application initiates transfer using Trunk Access Code dialing	Transfer does not complete	10.1.2.0.0
CM-54956	Register a Session Initiation Protocol(SIP) phone and administer Multiple Registration recording on it using Recorder(ACRA)	Intermittently the recordings would fail.	8.1.3.6.0
CM-54916	Keep a system running for a long time, till process ID goes over 65535	Ping all fails	10.1.0.2.0
CM-54897	audix-rec button is administered on the SIP endpoint No members should be available in the audix hunt group	The recordings on the SIP station after audix rec button is pressed are long calls because no disconnect event is sent.	10.1.2.0.0
CM-54893	Turn off IP sync on the system-parameters features form	Cannot access "change synchronization media-gateway X" command	10.1.2.0.0
CM-54883	Service Observe a H.323 station. Place a Make Call request from this station to another. Use DLG interface to make the request towards AES	Customer sees call origination fails on the application.	10.1.2.0.0
CM-54811	Administer a SIP station in a Network Region(NR) with no VoIP resources in the NR itself. Enable Dial Plan Transference (DPT) on this Network region	Calls from this SIP station was failing.	8.1.3.1.0
CM-54708	Activate or deactivate 10.1.3.1 SP i.e. 01.0.974.0-27937 or patches built over the same	Server status may show crit_os on processes. Command history and /var/log/messages will not be generated during this time. Notify Sync to SMGR will also not work during this time	10.1.3.1.0
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

ID	Minimum conditions	Visible symptoms	Issue found in Release
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-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	8.1.3.0.0
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-24536	Enable SA8481 and place call on SIP trunk using 3rd party make call.	With SA8481 enabled, UCID won't pass to SIP trunks	7.1.3.2.0
CM-17142	Setup NICE or Verint with AES encryption. Restart the socket between CM and AES	White noise gets recorded.	6.3.16.0

Fixes in Communication Manager Release 10.1.3.1.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
CM-54369	Call to SIP station which has EC500 enabled. EC500 leg returns 480 response from PSTN.	When the WSfE agent makes a call to cellular that is powered off, two more calls are sent to same number during ringing phase.	10.1.0.2.0
CM-54303	Principal stn is logged off. Last bridge in the list is busy. Call placed to principal station.	No ringback / coverage treatment applied to the call.	8.1.3.8.0
CM-54105	SNMP Inform to Notify Adjunct When DCP and H.323 Stations Go In/Out-Service is set to "y" on the system-parameters crisis-alert form. Unregister the shared control DMCC phone.	Hardphone can't get dial tone after the shared control station is unregistered.	10.1.2.0.0
CM-54091	Service Observe a VDN and place multiple calls to the VDN.	Service Observe does not work after the first call is dropped.	10.1.2.0.0
CM-54052	Configure CallType Analysis on the station. Call is made from Analog / DCP station to the SIP station which uses the CTA above. Try and answer the call after 10 seconds.	Call drops after 10 seconds, if it is not answered in that time.	10.1.3.0.0
CM-53942	AMS in a network region greater than 1000. AMS has failure, which triggers VoIP recovery	System restarts	10.1.0.2.0
CM-53932	Forward to voice mail with "Station Coverage Path For Coverage After Forwarding:" to "last-fwd" in system-parameters coverage-forwarding.	Segmentation Fault on CM	10.1.2.0.0
CM-53930	Configure SIP Bridge for a SIP station and make inbound call to principal. Enable SIP debugs using TCM.	System restarts.	10.1.2.0.0
CM-53918	On a CM duplex CM, configure a user assigned to avcommonos group.	This user does not get synced to standby server	10.1.2.0.0
CM-53897	If the VDN extension length is 5, then the first two bytes of name become "Esc+e" sequence.	Duplicate vector command fails.	8.1.3.3.0
CM-53889	ACD call with MCT activated	call goes on hold rather than dropping	10.1.0.2.0
CM-53874	Special application SA9150 is disabled.	command "change holiday-table 10" fails	10.1.2.0.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
	Vectoring (3.0 Enhanced)? is turned on for "system-parameters customer-options"		
CM-53869	CM agent transfers an incoming call to a station on Cisco call master switch, thus making a SIP-SIP tandem call on CM. The cisco agent holds/unholds the call.	Call drops 32 seconds after the call is unheld.	8.1.3.7.0
CM-53824	Add an unprivileged user from CM SMI. Change password of this unprivileged user from SMI.	SMI password change failed for unprivileged user.	10.1.2.0.0
CM-53801	SIPCC station has agents logged in from it.	In case of CC stations, sometimes the CC data does not get updated.	10.1.0.2.0
CM-53797	The recorders need to be in a NR which derive VoIP from one AMS. While trunks and actual stations which are being recorded need to get their VoIp resource from another AMS. Trunk makes a call to another trunk, which uses second AMS. The trunk makes another call to a station, which is being stereo recorded. Complete the transfer from trunk side by sending REFER.	The recordings after transfer are mono rather than stereo.	8.1.3.5.1
CM-53794	Register a SIP phone which is recorded using Verint MR recorder.	Intermittently recordings are lost, when recorder gets unregistered.	8.1.3.6.0
CM-53785	Administer buttons on another station for primary station's busy-indicator or bridge appearance.	change extension station on primary station fails with message: "Extension in use; use 'list usage extension' to find"	10.1.2.0.0
CM-53763	Call goes to a coverage path where first point is CAG and second point is a station.	In some scenarios, the call would not flow to the second coverage point.	8.1.3.7.0
CM-53714	Run "list trace tac x/<calling num>" from SAT.	CM restarts when a call arrives on this trunk.	10.1.0.0
CM-53587	CM 10.1.3 Security Scan	N/A	10.1.0.2.0
CM-53334	A SIP station makes an outbound SIP call to an SBC. The SBC returns 180 Ringing, then 480 when the far end number cannot answer the call.	A SIP station receives 408 response rather than 480, differing the user behavior.	8.1.3.3.0
CM-52928	SEMT needs to be turned off on CM. The call has to be from one SIP endpoint to another SIP endpoint. Should try and escalate it to AAC	After escalation of call to AAC, the other SIP parties do not get the Call-Info header, thus having suboptimal conferencing experience.	8.1.3.3.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
CM-52694	Administer a few nodes to a cluster using "change cluster session manager <cluster_id>"	command "list usage node-name" does not show SM cluster node names	10.1.0.0
CM-52618	SIP agents blind transfers ACD call to a Station over a trunk that is COR restricted. The transfer should fail.	SIP agent stays stuck in ACW state.	8.1.3.5.1
CM-52361	Configure LSP and DPT for ip-network-regions. 1. Configure Main CM and LSP. 2. Setup 2 different ip-network-regions for LSP and Main CM. 3. Administer DPT and necessary fields (LDN, trunk etc.) 4. Configure 2 media-gateways for these 2 ip-network-regions. 5. Register two stations on Main CM and make sure that they are registered in different NRs (Main and LSP NRs) 6. Perform failover so that LSP becomes active	DPT calls failed from active LSP to Main in CM10.	10.1.0.2.0
CM-52086	Tandem a call out on SIP trunk with UTF8 name/user for PAI header having byte length > 69.	Call failed with 400 response.	8.1.3.2.0
CM-51319	Setup ISDN trunk between two CMs. A stn on CM1 calls a VDN on CM2 , the vector routes it to a port X stn which is covered unconditionally The coverage point rings. CTI application is monitoring the calling station.	Incorrect number is sent in Alert event to the CTI application.	8.1.3.3.0
CM-48896	Announcements should be played from AMS. AMS should have atleast 2000 simultaneous calls listening to announcements.	announcements will stop playing and system will go into overload.	8.1.3.1.0
CM-35911	Make call from TTI set to SIP trunk, this will send name/ number of AWOH station which has been used by TTI set.	Calling from TTI set to SIP trunk sends wrong Name/Number.	8.1.2.0.0

Fixes in Communication Manager Release 10.1.3.0.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
CM-36359	Call redirection, Vector Directory Number (VDN), Interactive Voice Response(IVR), transfer.	Counted call doesn't work if call is redirected to another Vector Directory Number (VDN) via SIP Interactive Voice Response (IVR) transfer	8.0.1.1.0
CM-48316	Call from a station registered in telecommuter mode. Press DTMF from SL. The call should be in digit collection mode. Media resource should be AMS	The digits get ignored, and are not processed by CM	8.1.3.3.0
CM-50810	SIP station to SIP station call with called station sending 200 OK with "sendonly" SDP to initial INVITE to establish the call. Shuffling is disabled.	SIP station to SIP station call with called station sending 200 OK with "sendonly" SDP to initial INVITE to establish the call. Shuffling is disabled.	8.1.3.4.0
CM-50922	Workplace Attendant transfers call to a SIP station with EC500 enabled.	In case of transfer, number conversion is not applied to the calling party number being sent to EC500 trunk.	8.1.3.3.0
CM-51215	CCElite with SIP IVR	After upgrade from CM7.1 to 8.1.3.3.0, the "counted-calls" in the VDNs/vectors that their AAEP was transferring calls to, was broken	8.1.3.1.0
CM-51840	Register a H.323 station from a stub MR, which has a local LSP as well.	In Alternate gatekeeper List, only the local LSP's IP was sent, hence in case of failover to survivable server, the station would only go to the local LSP, and not fall over to the core region's survivable servers	8.1.3.2.0
CM-51929	NA	CM would trap and reset.	8.1.3.4.0
CM-52180	Call from a trunk which routes to a H.323 attendant. H.323 attendant splits the call to local SIP station	Incorrect display on sip station when an LDN call is split to it	8.1.3.5.0
CM-52305	Station dials out with international/nation access codes	user see incomplete digits when call is answered.	8.1.3.5.0
CM-52417	Administer exactly 16 announcements on a media server	User couldn't execute list command due to command contention	8.1.3.5.0
CM-52603	A SIP station call to trunk. Then SIP station transferred the call another SIP station. First trunk call gets originated by SIP station by sending off-hook FNU INVITE.	Customer saw mis-leading ASAI events with wrong call-ID resulting into long hour call recordings	8.1.3.6.0
CM-52629	Enable "Inc Trunk Call Splitting" on system-parameters cdr form.	No CDR records generated for Consultative Transfer when incoming Trunk Call Splitting s ON	8.1.3.4.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
CM-52661	Configure SIP station to have '&' character in the name. Setup a pickup group between multiple SIP users.	SM gets exception while parsing PUBLISH message for SIP station with '&' character in its name.	8.1.3.6.0
CM-52676	Enable special feature SA7900 - Service Observe Physical Set Service observes the physical bridged station Call the principle station answer and then hold he call on main station, while un-holding on bridged station	After bridged station un-holds the call, the call never gets Service Observed.	8.1.3.1.0
CM-52715	Set the station coverage path to Time of Day coverage. This coverage path should pass the call to SIP MM hunt group.	Calls go with wrong domain in SIP history-Info/diversion, causing calls to be dropped.	8.1.3.3.0
CM-52839	Have 15+ MGs in a IP sync domain and the CSoIP sync source has to be a MG.	Multi-level fan out for IP sync does not happen when the CSoIP source is Media gateway. Due to which a MG's resources may be completely used up for IP sync.	8.1.3.4.0
CM-52848	Alarms Enabled	Daily Alarms on ESS when GMM terminated and restarts unexpectedly.	10.1.0.1.0
CM-52858	A SIP station calls to trunk. Then SIP station transferred the call another SIP station. First trunk call gets originated by SIP station by sending off-hook FNU INVITE.	When a call is made to such a station, after the call is answered from the mobile phone, there was no dial tone, so customer cannot press a DTMF to confirm the answer and allow talk path.	8.1.3.5.1
CM-52904	Agent is in Auto-In state, and that agent responds to INVITE with a 603 Decline response.	If an agent responds to INVITE with 603, all the calls queued on the hunt group the agent is logged in start dropping one by one.	8.1.0.0.0
CM-52916	external call to station-A that covers to a VDN/vector that plays an announcement and then does a route-to another station-B.	CDR reports showing announcement as dialed number instead of the dialed VDN.	8.1.3.3.0
CM-52940	Use remote access to login to the system from SIP trunk, and then use FAC to Service Observe a VDN.	As soon as the observing session is established, CM drops the call.	8.1.0.0.0
CM-52945	1. Auto answer - acd / all (on agent form) 2. VDN with VoA configured 3. Hear Zip After VoA set to y on system param features page 10 4. Place an ACD call VoA this VDN to the agent	No zip tone heard after VoA by workplace agents	10.1.0.1.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
CM-53221	announcement with audio group, where group members are AMS which are out of service.	Every time an announcement is played, we get a denial event for each OOS audio group member.	10.1.0.2.0
CM-53263	Enable SRTP, the far end of SIP endpoint should perform hold/un-hold, but it should keep the encryption key same. AMS must be used as the VoIP engine.	One-way talk path when call is over 22 minutes old, where voice is coming from AMS and the station user does hold/un-hold	8.1.12.0.0
CM-53264	Enable IP synchronization using "change system-parameters features" command. Configure one or more media-gateways to Use IP Sync option (set to "y") .	When the MG's synchronization is changed, the IP-NR of MG#1	8.1.3.5.0
CM-53285	A call is originated from SIP trunk with audio and video capabilities, but video part of the call is marked as inactive.	AACC received channel type as video from CM, even when the incoming call is coming with video is set to inactive.	8.1.3.4.0
CM-53299	Several unsuccessful registrations attempts from endpoints. Endpoint does not send RRQ after receiving GCF, after more than 3000 of such registrations, no more registrations happen on CM	After enough un-registrations, no more H.323 stations register to CM.	8.1.3.3.0
CM-53330	After customer changes H.323 station to SIP station, after restart DIG-IP-STA warnings appear on display alarms.	After customer changes H.323 station to SIP station, after CM restart DIG-IP-STA warnings appear on display alarms.	8.1.3.6.0
CM-53333	Call from SIP trunk to a station which is then blind transferred to a R2MFC trunk by the SIP trunk.	After the transfer is completed, R2MFC trunk does not get correct ANI.	8.1.3.7.0
CM-53341	Call is being held from the softphone in telecommuter mode, when the INVITE is tandem from one Service Link to calling trunk.	In case of Telecommuting to SIP when calling from SIP trunks, if we hold the call from softphone, call drops in some cases.	8.1.3.2.0
CM-53361	execute almdisplay command on CM 10.1.2	the almdisplay command does not display MO names	10.1.2.0.0
CM-53489	Incoming call to VDN with first step being wait for silence and the sig group should have "Initial IP-IP Direct Media" turned off	In-band information is not being played to the calling station, unless the call is answered.	8.1.3.6.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
CM-53714	An incoming SIP trunk call to CM (10.1.2 or above) and list trace tac x/calling_num should be running from sat	System was reset/trap for an incoming SIP trunk call when list trace tac command was running on sat terminal	10.1.2.0.0

Fixes in Communication Manager Release 10.1.2.0.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-31675	SIP, transfer	SIP, transfer	7.1.3.3.0
CM-36444	Call from Direct Media Enabled SIP phone to shuffling OFF H.323 phone (or ISDN trunk).	Delay in audio due to redundant shuffle.	8.1.2.0.0
CM-39143	SIP agents	UUI not preserved on consultative transfer at customer sit	8.1.0.0.0
CM-41393	Calls to a VDN/vector that plays an announcement.	Call Detail Recording reports were showing announcement as called number instead of the VDN.	8.1.3.1.0
CM-42254	AES DMCC	Communication Manager could experience a warm restart due to the internal message buffer exhaustion upon massive incoming h323 un-registration requests from AES (Application Enablement Services).	8.1.3.1.0
CM-47838	SRTP	If far end shuffled and changed the SRTP key, the announcement restarted and DTMF detection in vector failed sometimes	8.1.3.3.0
CM-49027	CM did not send early IDLE message to CMS for loop-start CO	With SEMT enabled, Communication Manager sent additional headers in INVITE URI to Breeze Topic when call involved blind transfer	8.1.3.3.0
CM-49615	If DMCC station was attached on the call then out of band DTMF digits were not processed or out pulsed if the dialed digits had leading pauses	CM did not send early IDLE message to CMS for loop-start CO	8.1.3.3.0
CM-49620	DMCC registered station	If DMCC station was attached on the call then out of band DTMF digits were not processed or out pulsed if the dialed	8.1.3.3.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
		digits had leading pauses	
CM-49673	SIP	When SIP reachability feature was turned on, the socket traffic between CM (Communication Manager) and SM (Session Manager) sometimes got congested.	8.1.3.3.0, 8.1.0.0.0
CM-49810	SIP phones, announcement, AMS	SIP phones could not stop announcement recording on AMS by pressing "#" if announcement length was 10 seconds or more when Remote-access was used	8.1.3.2.0
CM-49873	EC500 is enabled and If initial offer from EC500 has direction sendonly. After answer EC500 sends reinvite with sendrecv direction.	No audio on inbound calls from EC500 cell.	8.1.3.4.0
CM-50025	Register DMCC shared control station for a particular H.323 station	User could not record/playback announcement when DMCC shared station was registered.	8.1.3.3.0
CM-50154	Configure EC500 for two extensions and feature-nameextension on Communication Manager	Call Appearance buttons get stuck sometimes	8.1.3.3.0
CM-50169	Use AMS for trunk call to SIP station and then blind transfer the call	No talk path between trunk side caller and analog station residing on gateway.	8.1.3.4.0
CM-50195	MG with ISDN trunks register	Communication Manager experienced rolling reboots due to an internal data structure being out of range, when an MG with ISDN trunks registered	8.1.12.0.0
CM-50205	Elite with hunt group with no queue.	Incorrect reporting of queued skill call after DAC call has covered from agent with DAC skill that has queuing off.	8.1.3.4.0
CM-50281	3PCC make call	Off-hook INVITE rejected in case 200OK for REFER is not received	8.1.3.3.0, 8.1.0.0.0
CM-50543	Use AMS for media	Use AMS for media	8.1.3.0.1
CM-50612	Agent, VDN, announcement	CM failed to respond with 200 OK for second call on Oceana Workspace which was listening to announcement	8.1.3.3.0
CM-50657	logv, command history	SIP station state showed out-of-service even when station was registered	8.1.3.4.0, 8.0.0.0.0
CM-50658	SIP, 200 OK	Incorrect Encryption Attribute sent in 200 OK of reInvite caused one-way audio	8.1.3.3.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-50817	logv, command history	logv, command history	8.1.3.3.0
CM-50841	logv, command history	logv, command history	8.1.3.3.0
CM-50875	Segmentation-fault in CM when reasoncode in XML part of cc-info PUBLISH had <spaces>	Communication Manager did not increment the SDP version when the SDP was changed	8.1.3.4.0, 8.1.3.1.0
CM-50910	sip-station, with forwarding set to external number.	With SA9147 enabled, sip-station calling other sip-station, which had off-net forwarding set to a number which is connected via PSTN trunk, display got updated with off-net number, which was against SA9147 behavior.	8.1.3.4.0
CM-50926	PUBLISH message with XML having non-standard characters	Segmentation-fault in CM when reasoncode in XML part of cc-info PUBLISH had <spaces>	8.1.3.3.0
CM-50960	CTI transfer	CTI transfer event had bogus connected party	8.1.3.5.0
CM-50984	Generate an enhanced callforward from a phone.	Garbage in 'list history' login and qualifier entries when viewed from SMGR cut-through when entry generated from phone doing a call-fwd.	10.1.0.1.0
CM-51191	Far-end changed Payload type using update request	Call dropped by CM after DTMF Payload Type changed by far-end.	8.1.3.5.0
CM-51215	CCElite with SIP IVR	After upgrade from CM7.1 to 8.1.3.3.0, the "counted-calls" in the VDNs/vectors that their AAEP was transferring calls to, was broken	8.1.3.3.0, 8.1.3.1.0
CM-51216	SIP bridging, Send All Calls	Bridge phone kept ringing if principle had SAC enabled in its coverage path and AFR was used	8.1.3.4.0
CM-51241	SIP MCA (Multiple Call Arrangement)	MCA (Multiple Call Arrangement) bridge phone received 400 Bad Request when it tried to answer the original call to principal that was already answered or covered. A reason text "Bad Request (call was answered/covered/dropped)" was added with the 400 Bad Request response.	8.1.3.1.0
CM-51249	Simple Network Management Protocol	Simple Network Management Protocol	10.1.0.1.0
CM-51285	VDN, routing	ASAI connected event missing	8.1.3.5.0, 7.0.0.0
CM-51317	On ip-codec-set form set any media-encryption.	Incoming SIP call rejected by CM due to failure to allocate AMS channel	8.1.3.0.1
CM-51418	SIP, 180 Ringing	CM to implement the changes to differentiate 180 RINGING in case of	8.1.3.5.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
		multiple 180 RINGINGS from ASM (ASM-89565).	
CM-51584	SIP, video	Call drop due to missing 200 OK to SIP INVITE with video sendonly offer	8.1.2.0.0
CM-51593	Announcement in vector before multiple skill queueing	Multiple Skill Queueing led to no-ring on SIP agent Invites	8.1.12.0.0, 8.1.0.0.0
CM-51639	Addition of a sip endpoint using SMGR User Management.	SIP phone sometimes did not work correctly when newly added	8.1.3.3.0
CM-51640	SIP service observing	SIP service observer will not be connected in the call if it is in listen-talk mode and it has shared station record.	8.1.3.3.0
CM-51654	Duplex CM	The "Status Summary" page reports "crit_os" in the "Processes:" field for one or both servers. This status may result in unexpected server interchanges.	8.1.3.5.0
CM-51662	Station used by a pickup group	User couldn't do a 'change extension' station at the SAT if the station was in a pickup group.	8.1.3.5.0
CM-51681	EC500 set up without route pattern (so the ec500 orig fails and denial event 1751 is logged)	Unexpected orig event is received from CM	8.1.3.3.0
CM-51691	Group page on a MG.	Some group page members did not have talk path.	8.1.3.3.0
CM-51709	IP, TLS	CM (Communication Manager) experienced memory exhaustion and all IP devices sometimes stopped working if the TLS certificate expired.	8.0.1.2.0
CM-51725	SIP trunk call	SIP trunk call got dropped because the called sip client sent back 200 OK response to invite before PRACK was received.	8.1.3.2.0
CM-51729	Massive unregistration of DMCC stations due to AES failure (network issues or etc.).	CM restarts due to ALLOC_BUF failure.	8.1.3.4.0
CM-51741	SIP MDA	Even if the pickup group members had different language settings (unicode or non-unicode), all the pickup group members would get the enhanced pickup group display in the same language (either in unicode or in non-unicode) for the incoming internal sip station to sip station call.	8.1.3.4.0
CM-51831	SIP station blind transfers call to the IP station which is being monitored for ISG events.	CTI events failed after SIP blind transfer.	8.1.3.5.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-51868	MCA (Multiple Call Appearance) and bridge phone	MCA (Multiple Call Appearance) bridge phone may not ring for the next call after the 1st call to the principal was answered by another MCA bridge phone.	8.1.3.4.0
CM-51884	Incoming trunk call on SIP trunk to H323 station. Set Display Name for H323 station of less than 15 characters.	Display name less than 15 characters long did not get populated on terming station Display.	10.1.0.2.0, 10.1.0.1.0
CM-51914	Administer a dialing pattern in ARS and Toll-restricted table. Dial this digit string from a SIP phone.	Incorrect error message (4xx message in response) sent to SIP phone while dialing Toll-Restricted number. SIP phone receives 484 Address Incomplete rather than 404 Not Found.	8.1.3.4.0
CM-51925	Turn on SIP Direct Media on SIG group.	Call dropped with 488 not acceptable when called party didn't support DTMF codec.	8.1.3.4.0
CM-51931	ASAI	Sometimes CM interchanged	8.1.3.5.0
CM-52015	user within susers CM group	A user within susers CM group was able to exploit perl environment variable PERL5LIB to gain access as root using sudo command.	10.1.0.1.0
CM-52025	CM SMI	Server cipher order was not enforced accurately	10.1.0.1.0
CM-52075	MCA (Multiple Call Appearance) and bridging	If the MCA (Multiple Call Appearance) bridge phone had more than one calls active, one of the call could get dropped by CM internal call record audit.	8.1.3.1.0
CM-52092	Long duration CRI timeout configured in CM coverage	Missing HOLD24 to CMS making CMS to assume agent's presence on two calls simultaneously when the previous call was un-held	8.1.3.5.0
CM-52124	CM with more than 130 MGs administered	When executing "status media-gateways" command, some entries were missing and some were duplicated	8.1.3.5.0
CM-52169	A call for a logged off station is answered by a pickup group member	Missing ASAI "Connect" event for call answered by pickup group member pressing pickup button	8.1.2.0.0
CM-52200	Incoming INVITE should be set to Inactive and the codec in that SDP, should be first codec in our codec set administration	Incoming calls with initial INVITE having inactive in SDP, may get dropped in certain situations.	8.1.3.5.0
CM-52240	SIP and bridging	Sometimes CM reset during calls involving SIP stations and bridging	8.1.3.5.0
CM-52243	SIP trunk call	CM (Communication Manager) may experience a segmentation fault if it received a 18x response with extended ascii display name (unicode) from a non-optim sip trunk.	8.1.3.5.1

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-52255	An internal DAC call to agent logged on to SIP phone.	CTI application couldn't answer an incoming Direct Agent Call (DAC) at a SIP endpoint with a 3rd party answer request.	8.1.3.4.0
CM-52266	Enable Intra-Switch CDR and other CDR related options.	Incorrect "dialed-num" for Intra-Switch CDR when calling from H.323 to H.323 which follows coverage path to Hunt group. H.323 station from Hunt group answered the call.	8.1.3.4.0
CM-52292	Set "Message Lamp Ext." to VDN/Hunt on SIP station. Leave a message for the VDN/Hunt.	Message Lamp Indicator configured for VDN/Hunt on SIP phone did not light up.	8.1.3.5.1
CM-52306	configure duplex standalone CM.	CM resets and interchanges	8.1.3.4.0
CM-52417	Administer exactly 16 announcements on a media-server	User couldn't execute list command due to command contention	8.1.3.5.0
CM-52469	ssh	diffie-hellman-group-exchange-sha1 algorithm was allowed for key-exchange over ssh	8.1.3.5.1
CM-52470	VDN with vector steps having collect or announcement step before routing	Intermittently there was no talk path to voice mail after a messaging step in a vector.	8.1.3.4.0
CM-52472	Media Gateway	change synchronization media-gateway command was missing on CM	8.1.3.5.0
CM-52568	Tenant, call coverage	In case of call covering to attendant, and the caller and callee in different tenants, the call routes to wrong attendant.	8.1.3.5.1
CM-52661	Configure SIP station to have '&' character in the name. Setup a pickup group between multiple SIP users.	SM gets exception while parsing PUBLISH message for SIP station with '&' character in its name.	8.1.3.6.0
CM-52691	High traffic on the SIP CC system	CM restarted sometimes due to SIP socket failure with SM	10.1.0.2.0
CM-52693	Esig 16 digits via AMS.	In band tone detection failed if AMS was used as the media resource	8.1.3.6.0
CM-52719	Make H.323 call and try to do conference while station is in dialing.	System restarted due to some memory corruption	8.1.3.4.0
CM-52721	AAFD with wrong audio settings for SRTP.	ACD callers get dropped when SIP agent using AAFD has misconfigured audio settings and responds to Invites with 488 Not Acceptable Here.	8.1.0.0.0
CM-52749	Network Failure creating Socket Failure between CM and SM	Socket went down but nothing got logged by default.	8.1.3.0.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-52836	CM Main and Enterprise Survivable Server / Local Survivable Processor	File sync fails if TLS 1.0 specified as minimum TLS version across Main and ESS/LSP	10.1.0.2.0
CM-52848	Alarms Enabled	Daily Alarms on ESS when GMM terminated and restarts unexpectedly.	10.1.0.1.0

Fixes in Communication Manager Release 10.1.0.2.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-29246	Call redirected off-net on SIP trunk and CCRON enabled.	Call failed when call was redirected off-net on SIP trunk and CCRON was enabled. Caller continued to hear ring back tone	8.0.1.1.0
CM-34164	H323, SIP	Communication Manager dropped entire conference call when it received 603 decline from SM for one party	7.1.3.5.0, 7.1.0.0.0
CM-34182	Telecommuting	Call was dropped by far end when a telecommuting call was held.	7.1.3.4.0
CM-34357	SIP	When an h323 station placed an outgoing call to the SIP trunk, if the capneg was turned off, and the outgoing trunk was configured as tcp, then the call would still fail even if "none" was put first in front of SRTP in the ip-codec form.	8.1.1.0.0
CM-39143	SIP agents	UUI not preserved on consultative transfer at customer site	8.1.0.0.0
CM-41383	Telecommuting does not work well from 1XAgent when service link mode is set to as-needed	Telecommuting does not work well from 1XAgent when service link mode is set to as-needed. If an available agent activates service observing when they complete the transaction and drop the station is left in a bad state causing the next call they receive to fail.	8.1.3.1.0
CM-41530	SIP call, reason header in BYE	Inconsistent proxying of reason header in BYE message.	8.1.3.1.0
CM-42254	AES DMCC	Communication Manager could experience a warm restart due to the internal message buffer exhaustion upon massive incoming h323 un-registration requests from AES (Application Enablement Services).	8.1.3.1.0
CM-47105	Cabinets, translation corruption	Translation corruption found after removing cabinets.	8.1.0.0.0
CM-47219	SIP	The SIP caller could get a ghost call if the far end SIP client responded 480 "SIPS Not Allowed	8.1.3.2.0
CM-47243	Overlapping ARS entries, short inter-digit timer.	Call was delivered to IX Messaging with 3 sec delay. After call was routed a messaging skill.	8.1.3.0.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-47330	Video call from SIP-A to SIP-B and answer with Audio only option. Configure A station as a Service observer for SIP-A	one-way audio when video call was being observed.	8.1.3.1.0
CM-47380	SIP station ASAI CTI client	CM (Communication Manager) didn't resubscribe the sip registration event from Session Manager (SM) after the old SIP registration event subscription got lost on SM upon SM upgrade. As a result, CTI (Computer Telephony Integration) couldn't use the SIP stations that were unregistered before the SM upgrade but registered after the upgrade.	8.1.3.3.0, 6.3.0.0
CM-47417	Send-calls	Can't remove send-calls button from some stations when it doesn't have data.	8.1.3.2.0
CM-47418	Non-EAS	non-EAS agents logged out	8.1.3.3.0
CM-47487	SIP or ISDN trunk with MLPP enabled.	SIP stations calling a "Vacant" PSTN number over SIP or ISDN trunks failed to hear the provided PSTN announcement, in a Communication Manager system with MLPP enabled	8.1.3.1.0
CM-47731	SIP-SIP transfer	After a SIP-SIP-SIP transfer using REFER without replaces, if the first digit of incoming PAI, was same as the transferring party's extension, then wrong PAI gets sent	8.1.3.2.0
CM-47838	SRTP	If far end shuffled and changed the SRTP key, the announcement restarted and DTMF detection in vector failed sometimes	8.1.3.3.0
CM-47853	H.248 MG	H.248 registration of Media Gateway fails when CM Minimum TLS version is 1.0 and Media Gateway TLS version is 1.0 or 1.2	10.1.0.0.0
CM-48302	Shared control station, VoIP channel	Recording continued even after call was dropped	8.1.3.2.0
CM-48313	TSAPI client, 2 CMs with H323 and SIP trunk, 1 agent and 1 h323 physical station, 2 SIP stations and 2 H323 stations.	Missing ASAI events to CTI side for agent call to trunk side	8.1.3.2.0
CM-48473	AMS as media resource for SIP stations, transfer	Blind Transfer failed while using AMS and 'referred-by' header was missing in INVITE message sent to transfer Target.	8.1.3.2.0
CM-48610	Principal station has SCA Bridge-appr and coverage-all calls	When call come to Principal and covers, the Bridge Appearance station keeps alerting the covered call and doesn’t update the call state.	8.1.3.4.0
CM-48721	SIP call	In a 200 OK response to an UPDATE without SDP, there was no Contact: header.	8.1.3.3.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-48774	Computer Telephony Integration with EC500	CTI (Computer Telephony Integration) controlled SIP station failed to answer or initiate new calls if both the EC500 and OPS station shared the same signaling group and the EC500 entry was before the OPS station in the off-pbx station mapping form.	8.1.3.1.0
CM-48864	Audix, node-name list	Unable to remove Audix node-name and Error: Remove name from signaling-group form(s) first.	8.1.3.2.0
CM-49027	SEMT (SIP Endpoint Managed Transfer)	With SEMT enabled, Communication Manager sent additional headers in INVITE URI to Breeze Topic when call involved blind transfer	8.1.3.3.0
CM-49208	Set Station Tone Forward Disconnect: busy, Bridge orig and bridge is domain controlled	Calls sometimes stayed up long after it was dropped at Communication Manager	8.1.3.3.0
CM-49294	MCT-act button on SIP phones	Verint recordings did not disconnect from agent station after MCT (Malicious Call Trace) feature was activated.	8.1.3.4.0
CM-49301	system-parameters features field '12-party Conferences?' is set to 'n', warm transfer	Communication Manager dropped held call if during warm transfer, transferee had 4 observers.	10.1.0.0.0
CM-49423	Calls arriving into CM, routed to H323 station with (OOB signaled DTMF) ports. Use AMS as media resource.	Incorrect encoding of 'A', 'C' and 'D' DTMF tones from AMS.	8.1.3.3.0
CM-49524	Hunt group with members/stations of type CallrID	After upgrading Avaya Aura Communication Manager to 8.1, calls transferred to hunt group with members/stations of type CallrID no longer carried external caller id.	8.1.3.2.0
CM-49530	SNMP VHEAP trap and trap receiver.	SNMP OID information was not displayed on trap receiver.	10.1.0.0
CM-49532	Multiple sockets using TLS encryption	When TLS was enabled for Media Gateways, some large H248 messages from an MG were mishandled causing Media Gateway link to drop	8.1.3.2.0
CM-49542	Tone Generation form.	Customer didn't have ability to administer 1000/-33.0 on Tone Generation form steps.	8.1.3.4.0
CM-49588	Media Gateway	CM could experience a system restart when the Media Gateway link bounced.	8.1.3.2.0
CM-49615	Trunk Flash CO trunk.	CM did not send early IDLE message to CMS for loop-start CO	8.1.3.3.0
CM-49620	DMCC registered station	If DMCC station was attached on the call then out of band DTMF digits were not	8.1.3.3.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
		processed or out pulsed if the dialed digits had leading pauses	
CM-49673	SIP	When SIP reachability feature was turned on, the socket traffic between CM (Communication Manager) and SM (Session Manager) sometimes got congested.	8.1.3.3.0, 8.1.0.0.0
CM-49825	SIP bridging	Make a call to a principal station with multiple SIP bridge stations, after the call is answered and then dropped, CM (Communication Manager) would send multiple same DSE (Dialog State Event) Publish message to each sip bridge station. That sometimes caused the sip bridge stations to reboot.	8.1.3.4.0
CM-49873	EC500 is enabled and If initial offer from EC500 has direction sendonly. After answer EC500 sends reinvite with sendrecv direction.	No audio on inbound calls from EC500 cell.	8.1.3.4.0
CM-49876	PRI endpoint	When trying to add a pri-endpoint, an EECCR was thrown	8.1.3.2.0
CM-49908	Station form, help message	Station form returned "is an invalid entry; please press HELP" when adding a route pattern or trunk group to SIP Trunk: for SIP stations.	10.1.0.0.0
CM-49932	Duplex CM	The "Status Summary" page reports "crit_os" in the "Processes:" field for one or both servers. This status may result in unexpected server interchanges.	8.1.3.5.0
CM-50027	Communication Manager SMI	CM SMI IP was accessible over insecure http.	8.1.3.4.0
CM-50031	SIP trunk-group with "Auto" assignment and more than 250 members.	User couldn't change "Number of Members" on "Auto" assign trunk-group to more than 250.	10.1.0.1.0
CM-50131	Communication Manager with SIP agents.	CM keeps sending 380 message loop on one agent.	8.1.3.4.0
CM-50154	Configure EC500 for two extensions and feature-name-extension on Communication Manager	Call Appearance buttons get stuck sometimes	8.1.3.3.0
CM-50195	MG with ISDN trunks register	Communication Manager experienced rolling reboots due to an internal data structure being out of range, when an MG with ISDN trunks registered	8.1.12.0.0
CM-50275	ping ip-address and H323 hard phone	ping ip-address sourced from a phone failed	8.1.3.1.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-50514	EC500, tandem calling number	Customers enabled EC500 on stations and configured tandem calling number form to change calling number and that was not working.	8.1.3.5.0
CM-50543	Use AMS for media.	Communication Manager had around 2 million pro=7168,err=203,seq=15716 errors on a daily basis.	8.1.3.0.1
CM-50544	CTI app and SIP trunk call	Extra dialed digits in the CDR record for SIP trunk calls	8.1.3.4.0
CM-50612	Agent, VDN, announcement	CM failed to respond with 200 OK for second call on Oceana Workspace which was listening to announcement	8.1.3.3.0
CM-50657	SIP station and monitored by Computer Telephony Interface - client	SIP station state showed out-of-service even when station was registered	8.1.3.4.0, 8.0.0.0.0
CM-50817	List trace TAC	The list trace 'tac' command failed to capture calls that are transferred.	8.1.3.3.0
CM-50841	logv, command history	Diagnostic web page sometimes gives out of date year range for command with year in the future.	8.1.3.3.0
CM-50875	SIP, media, SDP change	Communication Manager did not increment the SDP version when the SDP was changed	8.1.3.4.0, 8.1.3.1.0
CM-50926	PUBLISH message with XML having non-standard characters	Segmentation-fault in CM when reason-code in XML part of cc-info PUBLISH had <spaces>	8.1.3.3.0
CM-50984	Generate an enhanced call-forward from a phone.	Garbage in 'list history' login and qualifier entries when viewed from SMGR cut-through when entry generated from phone doing a call-fwd.	10.1.0.1.0
CM-51215	CCElite with SIP IVR	After upgrade from CM7.1 to 8.1.3.3.0, the "counted-calls" in the VDNs/vectors that their AAEP was transferring calls to, was broken	8.1.3.3.0, 8.1.3.1.0
CM-51216	SIP bridging, Send All Calls	Bridge phone kept ringing if principle had SAC enabled in its coverage path and AFR was used	8.1.3.4.0
CM-51241	SIP MCA (Multiple Call Arrangement)	MCA (Multiple Call Arrangement) bridge phone received 400 Bad Request when it tried to answer the original call to principal that was already answered or covered. A reason text "Bad Request (call was answered/covered/dropped)" was added with the 400 Bad Request response.	8.1.3.1.0
CM-51249	Simple Network Management Protocol	SNMP trap with string "system INET IPv4or IPv6 firewall is ok" generated each hour when firewall check was triggered	10.1.0.1.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-51654	Duplex CM	The "Status Summary" page reports "crit_os" in the "Processes:" field for one or both servers. This status may result in unexpected server interchanges.	8.1.3.5.0
CM-51758	JITC STIG RHEL-08-020041 with TMUX	CM and SMGR synchronization fails	10.1.0.0.0

Fixes in Communication Manager Release 10.1.0.1.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-23177	MG, analog boards	Avaya Aura Communication Manager did not send ALERT event to AES when agent was available and call was ringing on the agent.	7.1.1.0.0
CM-30262	Pickup group, IP Network Regions, AMS	Call dropped after it was picked up by a SIP station and then recording started	7.1.3.4.0
CM-32532	H.323 trunk with calling number and no name.	Transferring party name was displayed instead of calling number that was received over trunk.	7.1.3.4.0
CM-35703	H.323-A registered on One-X communicator in other phone mode (SVC link) going over SIP trunk.	Customer may experience talk path issue at service link leg	8.1.2.0.0
CM-38481	SIP calls	Intermittently, segmentation fault was observed when SIP SUBSCRIBE messages were received.	8.1.3.0.0
CM-38982	DECT station, bridge appearance, international call	"+" sign was missing in the call-log for J1xx sip station. DECT station had a bridge appearance of SIP J1xx station.	8.1.2.0.0
CM-40302	Group page, MG	Some large group page members did not have talk path.	8.1.2.0.0
CM-40775	AFR signaling group	Customers may experience a call drop issue if Alternate Routing Timer on a AFR signaling group expired	8.1.2.0.0
CM-41066	H.323 station, bridge, DMCC	Call to a H.323 station with bridge on caller was not recorded on calling side.	8.1.2.0.0
CM-41491	Bridge-appearance button, coverage path	Bridge station kept ringing when the call was covered for principal, even after the call got covered or the caller drops the call.	8.1.3.0.1
CM-41594	ECD enabled CM	ECD enabled Avaya Aura Communication Manager sent no EWT for ECD controlled calls in agent surplus	6.3.119.0
CM-42146	SIP, no talk path	There was no talk path when Avaya Aura Communication Manager gets 500 Incorrect CSeq and then we get new INVITE with IP/Port change.	7.1.3.8.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-42262	AMW buttons	When AMW or 3rd Party MWI is added, then MWI buttons were not lit when a new voice message was recorded.	8.1.3.1.0
CM-43359	AES and CM link, DMCC	Internal H.323 User related data structure robustness to prevent Avaya Aura Communication Manager resets	8.0.1.2.0
CM-43444	AMS as an announcement source.	Second announcement failed to play with back to back announcement steps in vector	8.1.3.1.0
CM-44448	SIP TLS trunk	SIP contact header was sent with SIP:URI on TLS trunk	8.1.3.2.0
CM-44796	An IP Agent, SIP service link for audio is user U1.	Active SIP service link call corrupted by bridged-appearance activity from another call. Further Invite on the corrupted call caused call to fail.	8.1.0.1.1
CM-46807	CM with multiple tenants each with their own music on hold announcements.	Music source was not set according to VDN Override rule if call transitioned through a VDN with VDN Override disabled to another VDN.	8.1.3.0.0
CM-46827	Incoming ISDN call, PSTN	User provided and verified calling party number was ignored.	8.1.3.2.0
CM-46917	SIP adjunct hunt group with IXM using SIP trunk	ISDN/SIP Caller Display for sip-adjunct hunt group was incorrect	8.1.3.2.0
CM-47098	ISDN trunk, MDA	Incoming EC500 call from public trunk, when sent to a MDA(Multi device-access) station, adds a + to the call logs.	8.1.3.2.0
CM-47123	SIP, OPTIM	Single Step Conference/conference attempt was denied with error object/call state not valid	8.1.3.1.0
CM-47218	call to physical station with agent logged in and then transfer	CTI application missing ASAI alerting and established events for the call resulting into multiple recording/reporting problems	8.1.3.2.0
CM-47289	CDR, tandem-calling-party-number, remote coverage point	CDR produced for a tandem call with remote coverage and having the entry on tandem calling party table lost the original Calling Party Number.	8.1.3.2.0
CM-47334	EC500 mapped extension, hunt group	Incoming call from an EC500 mapped extension, if it got queued on hunt group, did not get 182 Queued response causing repeated calls	8.1.3.3.0
CM-47341	X-port principal station, 70 bridge stations, coverage path	Avaya Aura Communication Manager reset with ALLOC_BUF failure when call to X-port with 110 bridges covered to another X-port with 110 bridges.	8.0.1.2.0
CM-47438	Shuffling on, Direct Media-off Users with different DTMF PT while shuffling call to direct-IP	After upgrade to 8.1.3.3.0, DTMF from SIP trunk to AAEP through Avaya Aura Communication Manager, did not work	8.1.3.3.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-47481	SIP endpoint user, call forward FAC.	Call-Fwd feature access code was not working on SIP endpoint with denial 1601: Software Invalid.	8.1.3.3.0
CM-47487	SIP or ISDN trunk with MLPP enabled.	SIP stations calling a "Vacant" PSTN number over SIP or ISDN trunks failed to hear the provided PSTN announcement, in a Communication Manager system with MLPP enabled and translated	8.1.3.1.0
CM-47598	Shuffling on DM -off User different DTMF PT while shuffling call to direct-IP	After upgrade to 8.1.3.3.0, DTMF from SIP trunk to AAEP through Avaya Aura Communication Manager, did not work	8.1.3.3.0
CM-47626	2 CMs with ISDN-PRI trunk	The CTI application saw in-consistencies in terms of connected parties on the call, after receiving ISDN FAC from the trunk side	8.1.3.2.0
CM-47627	1. 2 CMs with SIP trunk. 2. 2 SIP extension of CM1 and one H.323 extension for CM2	Avaya Aura Communication Manager incorrectly sent "#" in "call conferenced" in "CONNECTED NUMBER"	8.1.3.2.0
CM-47655	AFR (Alternate Failover Routing)	Avaya Aura Communication Manager restarted during AFR (Alternate Failover Routing) scenarios.	8.1.3.3.0
CM-47761	SA8967, H.323 station	Send-nn did not work for Vector Directory Number defined behind send-nn button.	8.1.2.0.0
CM-47776	Alternate Failover Routing	Memory leak observed during Alternate Failover Routing scenarios causing Avaya Aura Communication Manager to reset and interchange	8.1.3.0.0
CM-47830	SIP Direct Media, Encryption	For SDP offer with two non-ANAT audio lines, Avaya Aura Communication Manager didn't follow ip-codec-set filtering for the 2nd audio line.	8.1.3.1.0
CM-47902	3rd party CTI connection via Genesys IWS	Call initiated ASAI event was not received intermittently in high traffic scenarios involving voicemail.	8.1.3.2.0
CM-47940	CM 10.1.x or 8.1.3.3.x and a CTI link to be removed	Unable to delete/ remove CTI link	8.1.3.4.0
CM-47955	Loop start trunk, agent	Loop start trunk was hung when Komutel Sit2 soft client released the call.	8.1.3.3.0
CM-47992	Enable CDR and UCID, 3 SIP phones, consultative transfer	Different UCID in CDR for a consultative transfer call amongst three SIP phones.	8.1.3.3.0
CM-47993	SIP station, SIP trunk	If separate numbers come in PAI and Contact in 183 Session Progress, then Communication Manager copied number from Contact to PAI and dropped the PAI completely resulting in incorrect display on the caller.	8.1.3.2.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-48060	VDN, announcement	Avaya Aura Communication Manager did not send ASAI busy event if there was an announcement step prior to busy step in the vector.	8.1.3.3.0
CM-48167	Docker	Docker, JKC and Log4j removed to address vulnerabilities. Log4j is no longer present in CM 10.1.0.1.0	8.1.2.0.0
CM-48187	SIP-SIP call with Initial IP-IP Direct Media enabled. Register recorder station after call starts.	SIP call gets dropped after 30 seconds	8.1.3.3.0
CM-48189	1. 3 Stations, One principle station, 1 station used as call forwarding station and one should be caller. 2. TSAPI link should be up. 3. TSPAI client on client machine	Long call recording on ACRA, caused by CMs out of context alert for AWOH station. When enhanced call forwarding was enabled for busy and no reply call forwarding then alert event is seen in TSAPI client and mst even though principle station is not registered.	8.1.3.3.0
CM-48196	A "forced" interchange while the standby server was in the "not refreshed" state.	The 'server -i' command or 'interchange servers' SMI command sometimes resulted in a reload restart on the newly active server when a warm restart was expected.	8.1.3.1.0
CM-48331	SIP reachability for domain controlled station	When SIP reachability for domain controlled station was on and endpoint registration query was done, then the response received was without product type Pord_id "SIP_Phone"	8.1.3.3.0
CM-48339	Media-Gateway greater than 250, location	Customer could not administer a "Location" greater than 250 on the "Media-Gateway" form when 2000 should have been allowed	8.1.3.0.1
CM-48392	ESS, call reconstruction	Once ESS became active and calls were getting reconstructed , when third party domain control was enabled, it lead to call drop	8.1.1.0.0
CM-48439	UCID enabled for CDR, Incoming trunk calls terminating to SIP stations that were bridged to other SIP stations.	Under certain conditions, 2 completely unrelated calls had the same UCID in CDR	8.1.3.1.0
CM-48481	Timer buffers	Under rare conditions, the Avaya Aura Communication Manager experienced a warm system restart due to an internal resource exhaustion.	8.1.3.3.0
CM-48592	Stations with busy-indicator, SAC buttons	Executing "change extension-station" command sometimes resulted in corruption for buttons	8.1.3.3.0
CM-48675	SIP phones, bridging	Error message when SIP phones tried to get the features from Avaya Aura Communication Manager. SIP phone answered a call on a	8.1.3.3.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
		bridged appearance and transferred the call which resulted in button corruption	
CM-48720	Add, modify or delete uniform-dial plan table	Attempt to add, modify or delete uniform-dialplan table resulted in error "Extension invalid", please check dialplan message.	8.1.3.0.1
CM-48806	SIP station, enhanced call forward button	Avaya Aura Communication Manager restarted every 3 days when enhanced call forward button was configured on SIP stations	8.1.12.0.0
CM-48825	Alarm, error	Avaya Aura Communication Manager ECS log showed "Overflow" error entries occasionally when alarm exceeded 80 characters.	8.1.3.3.0

Fixes in Communication Manager Release 10.1

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-9508	QSIG, Communication Manager (CM), Look Ahead Routing (LAR)	History Info was lost in QSIG to SIP interworking calls involving LAR	6.3.12.0
CM-9955	AACC, REFER	AACC was not able to route the call properly when incoming call had anonymous in From header	6.3.0.0
CM-16308	DSP core busy on media gateway	Manual busyout of the used dsp core on media gateway lead to loss of talk path and call drop.	6.3.11.0
CM-16518	ciphersuite	TLS offered ciphers that were no longer considered secure.	7.1.0.0.0
CM-16543	server config, SMI, footprint	AES licensing for MEDIUM ADVANCED TSAPI was not functioning correctly	7.0.1.1.0
CM-17731	H.323, Network Address Translations(NAT)	The H323 station behind the Network Translated Device (NAT) couldn't get dial tone if the user tried to go offhook the first time after registration.	6.3.8.0
CM-18330	CM SMI pages	Missing HTTP Strict-Transport-Security-Header on Webhelp pages	7.1.0.0.0
CM-18378	H.323 IP stations	Sometimes system encountered "Maximum Concurrently Registered IP Stations" incorrectly.	6.3.116.0
CM-18825	Redirect On No Answer (RONA)/X-port station/SIP trunk	RONA (Redirect On No Answer) call that covered through a x-ported station to a remote coverage path got no History-Info header in the outgoing invite on the SIP trunk. As a result, the call couldn't cover to the right voice mail box	6.3.16.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-18948	Upgrade from cm7.0 to cm7.1 via SDM using the preserve-on-upgrade disk feature.	Customer was unable to activate Service Packs that contain RPMs, especially Kernel and Security service packs.	7.1.0.0.0
CM-24390	SIP, hold	The first call which was held by far-end gets dropped after SM connection was restored	7.1.3.2.0
CM-26859	Monitor Vector Director Number (VDN), Do predictive call to VDN	TSAPI client was not showing the trunk-group field when Predictive call was made.	8.1.0.0.0
CM-27384	DMCC registered in main mode	Split-stream recording was not possible using Main dependency mode recorder and SSC	8.0.1.0.0
CM-27469	A SIP trunk, SIP station, call transfer, AES	AES restarted when it received a hold event from CM for SIP transfer scenario where the SIP REFER method was used for transferring the call	8.0.1.1.0
CM-27648	NA	UDP sockets can be closed by sending zero-length packets.	7.1.2.0.0
CM-27751	CM with AMS	AMS remained stuck in pending-lock state and became unusable	7.0.1.2.0
CM-28203	SIP traffic	Communication Manager could experience a segmentation fault during SIP traffic.	8.0.1.1.0
CM-28277	SNMP trap configured	No SNMP Traps were sent.	7.1.3.4.0
CM-28731	Any servers 7.1.3.4.0 and later in the 7.1.x load line or 8.1.0.1.1 and later in the 8.1.x load line	In certain conditions, installing a patch could cause the system to issue a crit_os warning while restarting the logging service.	9.0.0.0.0
CM-29382	Tandem calling party number form, modification of existing entries	The tandem calling number form, when they have a particular combination of entries including some with the "any" choice in the CPN Prefix column, could not be changed	7.1.3.3.0
CM-29596	SIP stations, forking	SIP calls drop after 30 seconds if PRACK was received after 200 OK	8.1.0.1.0
CM-30072	CM administered to connect to an R18 or newer CMS. Large number of members in measured trunk groups. Failure to pump-up may occur only when the link to CMS is over the procr instead of a CLAN.	CMS link did not come up after adding a large number of trunk members.	8.1.1.0.0
CM-31376	ip-codec-set - On page 1, media-encryption is set. For FAX, t.38-G711-fallback is set.	T38 Fax fallback to G711 with encryption failed	7.0.1.3.0
CM-31390	SIP Vector Directory number (VDN) call	SIP call could be stuck after the originator dropped the call if the originator of the call to vector SIP agent did not get 18x response before 200OK.	7.1.3.3.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-31853	Outbound call, Communication Manager (CM), Adjunct/Switch Application Interface (ASAI)	When 3rd party application requested a snapshot of the outbound call, CM 8.x did not send trunk as second leg.	8.0.1.2.0
CM-31857	SA9095	Hunt group using SA9095 queuing did not work as expected	8.0.1.2.0
CM-31902	SIP INVITE, Av-Global-Session-ID header	Customer may experience system reset if incoming SIP call is received with an empty Av-Global-Session-ID header	8.0.1.1.0
CM-31930	Call pickup, H.323 station	Call continues ringing on H323 station on answering of call by another station using call pickup button	7.1.3.4.0
CM-31974	shared control registered for an H.323 station of 96x1 type	Customer might see a segmentation fault or mempool errors when trying to delete an H.323 station which has a corresponding shared control station registered.	8.0.1.2.0
CM-32139	Tandem call, Vector Directory Number (VDN), Adjunct/Switch Application Interface (ASAI)	In ASAI ALERT message, VDN number was seen instead of actual called party number.	7.1.3.4.0
CM-32217	Incoming SDP offer, G729Codec and connection address as 0.0.0.0	CM sent annexb=yes in SDP answer even though no G.729B in the ip-codec-set.	7.1.3.4.0
CM-32858	Station-A, Station-B, Station-C, CSDK workspace, CM (Enforce SIPS URI for SRTP? y)	User was unable to create transfer call using a Computer Telephony Interface (CTI) client	8.1.0.0.0
CM-33039	H323 1xagent	1X Agent on Citrix Server could be stuck and consistently sent KARRQ (keep alive registration request) with obsolete endpointID without stop, that would cause CM (Communication Manager) overload.	7.1.3.0.0
CM-33062	h323 sig group	CM could experience a segmentation fault and a server interchange when an H323 sig group with "RRQ Required" set to "y".	8.0.1.1.0
CM-33065	Adjunct/Switch Application Interface (ASAI), alerting and connected event, bridge-appearance	Alert and connected events were missing when transfer is completed using the bridge-appearance	8.0.1.1.0
CM-33095	SIP transfer	SIP transfer could fail if the refer-to URI has no user portion in the refer header when the SEMT (SIP Endpoint Managed Transfer) was turned on.	8.0.1.2.0
CM-33185	predictive calling/Dialer	When Predictive call was made via AES to CM and customer, Customer was not connecting to Agent	8.1.0.2.0
CM-33205	Server duplication	System may crash after the interchange after an upgrade.	8.1.2.0.0
CM-33214	Coverage path, Single Step Conference (SSC), out of service stations	Single Step Conference (SSC) can incorrectly fail when coverage path includes stations which are not in-service before an in-service coverage point station answers	7.1.3.5.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
		the call. This can lead to CTI call recording failures after failed routing to coverage points.	
CM-33251	Look Ahead Inter flow between 2 CMs	CTI-Applications was not receiving the delivered/Alert event for a customer call was queued to trunk and vector steps having multiple LAI(Look Ahead Inter flow) failed and connected to final Agent.	7.1.3.2.0
CM-33316	Any system running CM8.1	A listen socket was opened on port 111 for CM and reported as a vulnerability by a security scanner.	8.1.1.0.0
CM-33331	voice mail	When call goes to voice mail, CM (Communication Manager) could experience a segmentation fault.	7.1.3.4.0
CM-33345	H.323 trunks, 2 CMs	call drop during a H245 messaging race condition	7.1.3.2.0
CM-33357	Call Detail Recording (CDR), trunk member information	Incorrect trunk member information was captured in fixed format CDR report.	8.1.0.2.0
CM-33364	EC500	When a call was termed to an EC500 trunk, the media resource region was chosen from the principal instead of the EC500 trunk. As a result of this. wrong media codec was chosen for the call.	7.1.3.0.0
CM-33386	Endpoint that was both part of a hunt group and part of a multimedia complex.	CM (Communication Manager) could experience a segmentation fault when a call termed to an endpoint that was both part of a hunt group and part of a multimedia complex.	8.0.1.1.0
CM-33390	Blank hostname from CM SMI, it should not accept.	Network Configuration in CM SMI was accepting a blank hostname.	8.1.0.2.0
CM-33414	3rd party SIP endpoint	Call is dropped.	7.1.3.4.0
CM-33419	Long hold recall timer, Vector Directory Number (VDN), display	A two-party redirected display (e.g., for bridging or a VDN) reverted to a single-party display if the call was held and then returned due to the hold recall timeout.	8.0.0.0.0
CM-33433	SIP, blind transfer, drop event	Missing drop event for the agent on the held leg of the call for an IVR SIP blind transfer to an incorrect / intercepted number	8.1.1.0.0
CM-33529	EC500	It was required to have an extend button for the EC500 delayed call to be launched successfully.	7.1.3.5.0
CM-33530	OneX Station	Non-OneX stations show one-X Server Status as trigger or normal, causing misbehavior of calls termed to that station.	7.1.3.3.0
CM-33587	Avaya Aura Media Server (AMS), announcement/music	Occasionally an inter Gateway connection can lead to a segmentation fault	7.1.3.3.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-33599	SIP station	When a Non-SIP administered set type was put in the off-pbx station form for OPS SIP station registration, proc error 7171 8936 could be seen in /var/log/ecs log file and the call-appr in the expansion module wouldn't function well on the SIP station.	7.1.3.4.0
CM-33609	SIP trunk, Avaya Aura Media Server (AMS), ringback	Double ring back tone was being heard in SIP outgoing trunk calls when far-end connected ring back tone.	8.0.1.2.0
CM-33653	telecommuter Agent	Sometimes NICE recorder is not able to record Telecommuter agent's calls.	7.1.3.3.0
CM-33734	sip	Double deletion MEMPOOL error for Class Bytes_32 was seen in /var/log/ecs.	7.1.3.4.0
CM-33744	Avaya Aura Media Server (AMS), interchange, Call stuck in the Skill queue with agents available (CIQAA)	After an AMS interchange, CIQAA happened due to corruption of service link	7.1.3.4.0
CM-33749	Message Waiting Indicator (MWI)	If station A has it's 'Message Lamp Ext:' assigned to station B and an upgrade is performed to 8.1.x this resulted in translation corruption causing no MWI updates	8.1.1.0.0
CM-33752	SIP agent	CM (Communication Manager) would drop the queued hunt call if the sip agent returned 500 error response.	7.1.3.2.0
CM-33766	Place a call to Vector Directory Number (VDN)/Vector with adjunct route step and any of the following BITs set: + FLEXBILL_BIT + VDN_OVERRIDE_ADJRTE_BIT + DONT_QUERY_IAP_ADJRTE_BIT For instance, if VDN override is enabled on the VDN, this will cause the problem.	Calling Number is set to '*****' in Adjunct Route Request.	8.1.2.0.0
CM-33777	Simple Network Management Protocol (SNMP), Federal Information Processing Standards (FIPS)	Cannot remove V3 SNMP users from polling, incoming traps and traps when FIPS enabled.	7.1.3.5.0
CM-33804	Non-shuffable endpoints, service links	When 1X agent with service link transfers a call to another agent they hear a loud click.	8.1.1.0.0
CM-33817	Native H.323 phone	CM (Communication Manager) could experience a system restart when the native h.323 station's MWL (message waiting lamp) button was audited through maintenance.	8.0.1.1.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-33833	EC500, Feature Access Code (FAC), transfer	FAC for transfer from EC500 failed for transfer complete	8.1.3.0.0
CM-33850	one-x server	One-X server call back call could be dropped occasionally.	8.0.1.2.0
CM-33853	Circular hunt group	The first call to a circular hunt group will fail after the system starts up.	7.1.3.2.0
CM-33873	dual reg	For a DUAL registration configured extension, if the administered set type was H323 station type and the h323 station was registered and SIP station not registered, a call to this extension would follow the Coverage Path Point "Logged off/PSA/TTI" rule for coverage.	7.1.3.6.0
CM-33927	SIP, SRTP	Unattended transfer fails for SIP calls with encryption	7.1.3.3.0
CM-33940	Duplicate a DS1FD station type.	The SAT "duplicate station" command hangs and causes system reset when duplicating a DS1FD set type.	7.1.3.0.0
CM-33941	Personal CO Line (PCOL), incoming call, transfer	Incoming call to a PCOL group that is transferred to a station that covers to VM got a generic greeting.	8.1.1.0.0
CM-33943	SIP call	SIP station call failed with 400 Bad Request since CM (Communication Manager) put invalid (0xff) in the "From" header of the outgoing Invite message to the SIP station intermittently.	8.1.0.1.1
CM-33949	Clustered Signaling-group.	Question marks displayed in "Primary SM" and "Secondary SM" fields on SAT ROUTE PATTERN form when SIP Signaling-Group "Clustered" field is enabled.	8.0.1.2.0
CM-34056	Cisco security manager (CSM), Communication Manager (CM), Application Enablement Services (AES), Interactive Voice Response (IVR), DS1FD	Cisco's CSM restarted when the call scenario to CM involved multiple transfers and conferences.	7.1.3.0.0
CM-34079	EC500, Automatic Call Distributor (ACD), hunt group	IP station port was corrupted after failed EC500 call on ACD hunt group agent. IP phone becomes unusable and the agent stops getting calls. It requires a CM reboot to fix this.	7.1.3.2.0
CM-34104	AEP call to station, that is transferred (via REFER) to an outgoing trunk	Incoming AEP call to station that is transferred (via REFER) to an outgoing trunk results in the caller getting the generic greeting when the call covers to VM.	7.1.3.5.0
CM-34105	System Manager	International characters can be truncated when using System Manager Native Names feature..	8.1.2.0.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-34135	Avaya Aura Media Server (AMS), announcement	Delay in playing an announcement from AMS	8.1.2.0.0
CM-34144	SA9114, Computer Telephony Integration (CTI) app, monitoring	CTI-application was not receiving the country code for an out dialed call with SA9114 enabled	7.0.0.1.0
CM-34205	SIPCC agent, Busy/ Release	Busy/Release a SIPCC phone could potentially drop a SIP trunk call owned by other SIP station	7.1.3.5.0
CM-34232	Active SO, confirmation tone is activated	DMCC clients or recorders may get into bad state.	7.1.3.3.0
CM-34236	pick up group	CM (Communication Manager) could experience a segmentation fault after a warm restart due to an internal pick up group audit.	7.1.3.0.0
CM-34237	H323 station	CM (Communication Manager) could experience a server interchange due to message buffer exhaustion caused by the H323 IP station's TCP socket congestion	8.1.2.0.0
CM-34391	1) Dual Registered phone with H.323 set type. 2) Active call on the H.323 logged in station.	Bridging into an active call from the SIP station failed for a dual registration phone with H.323 set type,	8.1.3.0.0
CM-34406	H.323 endpoint, TTI	"disable ip-reg-tti old xxxx" did not work for H323 physical/hard phone	8.1.2.0.0
CM-34425	Station Service State query	Response to "Station status query" had service state as unknown	7.1.3.5.0
CM-34436	Voicemail, inter PBX call, X port	Call routing did not cover to voicemail when call originated on different PBX	7.1.3.2.0
CM-34437	Avaya Aura Messaging (AAM), Simple Network Management Protocol (SNMP).	The snmpinctrapconfig command fails in Voice Messaging Stand Alone mode.	7.1.3.3.0
CM-34456	Call Center with work-code buttons	Call Center work-code button fails to work in some scenarios while agent was in after-call-work.	8.1.2.0.0
CM-34467	Music On Hold (MOH), SIP direct media, incoming trunk call	ISG unhold event was not received when incoming trunk call to hunt and hold/resume from agent	8.1.2.0.0
CM-34505	Contact Center, Circular hunt group	Sometimes circular hunt group calls resulted in an internal software loop leading to reset of CM.	7.1.3.6.0
CM-34520	SIP call	If the SIP display update message is sent after the non 100 provisional response and gets 481 response, CM should resend the update msg instead of dropping the call.	8.1.2.0.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-34522	Communication Manager (CM), station service state, SIP reach-ability	When a device force re-registers and if NOTIFY with terminated state comes later, CM sets the registered state as unregistered	7.1.3.7.0
CM-34523	H323 phone	An H323 phone's TCP socket could be stuck after a Duplicate CM (Communication Manager) server interchange.	7.1.3.4.0
CM-34646	SIP, H.323 trunks	Sometimes SIP/H.323 calls resulted in CM interchange	7.1.3.2.0
CM-34653	sip agent	The call was returned to the skill after AAFD (Avaya Agent For Desktop) responded 380 with "Line Appearance In Use" to the incoming Invite. The direct agent call that got 380 response with "Line Appearance In use" should be redirected to the agent's coverage path or "Redirect on IP/OPTIM Failure" VDN if agent coverage path is not configured.	7.1.3.3.0
CM-34676	R2MFC, call coverage	Call from a R2MFC trunk on a Port Network to a station which then cover-all to another R2MFC trunk did not have a Talk Path after answer.	8.1.1.0.0
CM-34697	Announcement, recording	When customer tried to change the source location for announcement, object already in use was displayed and when trying to rerecord the announcement, denial event 1052 was generated	7.1.3.6.0
CM-34732	SIP header "User-Agent" containing empty	When CM receiving SIP header "User-Agent" with Empty then CM was generating core dump	8.1.2.0.0
CM-34737	h323 phone	If H323 bridge phone was configured in telecommuter mode and with NICE recorder attached, when bridge button was pressed to answer the incoming call to principal, the call couldn't be answered.	8.1.2.0.0
CM-34993	2 Vector Directory Numbers (VDNs), Coverage Answer Group (CAG), CAG member Monitored by Computer Telephony Integration (CTI)	ASAI alert even contains the VDN number in CALLED PARTY information instead of hunt group extension.	7.1.3.6.0
CM-35017	Multiple Avaya Aura Media Servers, announcement on only one AMS	Announcement heard from AMS after a delayed time.	8.1.2.0.0
CM-35035	Vector Directory Number (VDN), Vector, Redirection On No Answer (RONA), Off-net number	A RONA call that routes to the RONA VDN that does a route-to an external number fails to go out the trunks assigned to route-pattern. CM returns denial event 1311 and the caller is connected to intercept tone.	7.1.3.4.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-35040	Call Center, SIP agents, Blind Transfer, Call Management System (CMS)	Call Centers with SIP agents on stations that perform blind REFER may notice some calls transferred by those agents are not correctly tracked on CMS. The original SIP agent stations did not support a blind (plain) REFER.	7.1.3.2.0
CM-35055	Capability Negotiation (Capneg)	CM didn't send 200 OK to in dialog OPTIONS when the negotiated SDP is encrypted causing call failures	8.1.2.0.0
CM-35099	Bridge station, transfer, Voice Mail, calling number	Call to a station that is answered by a bridged station and then transferred to a station that covers to Voice Mail is getting incorrect greeting	7.1.3.5.0
CM-35100	SIP station, coverage	Principal SIP station gave audible ring even when call was ringing on the coverage point.	6.3.118.0
CM-35129	One X Agent, service link	In using One X Agent, Service Link (S/L) is set for as-needed but was acting as if permanent, and back to back calls were not ringing cell phone for each new call, and callers were immediately linked to the cell on the same S/L.	7.1.3.3.0
CM-35166	Avaya Aura® Experience Portal (AAEP), blind transfer	Intermittently, blind transfer from AAEP to agent caused no talkpath	7.1.3.7.0
CM-35275	Computer Telephony Integration (CTI), recording	One of the call was not recorded when an internal software data structure array boundary condition was met	8.0.1.2.0
CM-35279	Encryption	Call to Service Link drops when agent holds the call.	8.0.1.1.0
CM-35366	Communication Manager (CM) interchange, warm restart, H.323 stations/trunks	Sometimes H.323 calls resulted in CM interchange	7.1.3.4.0
CM-35395	Call routing through a Vector Directory Number (VDN) to Experience Portal, then back to Communication Manager (CM) and delivered to agent	User Information (UUI) information is missing in the Adjunct Switch Application Interface(ASAI) message after the call is transferred from Experience Portal to CM, and SIP trunking refer messages updated	7.1.3.5.0
CM-35407	Audix-rec button and VM/ sip-adj hunt group	Call was getting stuck when audix rec button was used, if the call was dropped within 0.5 seconds of pressing audix-rec button.	8.0.1.2.0
CM-35431	Adjunct/Switch Application Interface (ASAI), bridge appearance	Drop/disconnect event was not received when bridge-appearance dropped	7.1.3.6.0
CM-35547	Call Center with Special Application SA8702 with 'Copy UCID for Station Transfer/Conference" enabled.	SIP agent transferring calls with 'Transfer Now' produced two separate UCIDs despite enabling Special Application SA8702 with 'Copy UCID for Station Transfer/Conference".	8.1.2.0.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-35557	SIP station, Logged off/PSA/TTI, coverage path	Logged off SIP station with Logged off/PSA/TTI? was disabled for coverage path, and caller received ring back instead of busy tone.	7.1.3.6.0
CM-35589	2 SIP Signaling groups with different far-end ip and same far-end-port, near-end-ip, near-end-port.	Message Sequence Tracer(MST) traces on specific SIP signaling groups also trace other SIP traffic.	8.1.2.0.0
CM-35621	Announcement, re-recording	When trying to rerecord the announcement, denial event 1052 was generated	7.1.3.6.0
CM-35687	Primary Rate Interface (PRI) trunks	Sometimes CM reported a segmentation fault when processing calls over PRI trunks	8.1.2.0.0
CM-35688	Automated Call Distribution (ACD), hunt group	A call made to an ACD (automated call distribution) hunt group consistently requeued to the Hunt group and that drove CM (Communication Manager) towards CPU overload	7.1.3.6.0
CM-35756	Empirix H.323 stations	Could not make calls on Empirix phones after TCP link was down and then recovered.	7.1.3.6.0
CM-35778	Resource Inter Gateway Connectivity, Computer Telephony Interface(CTI)	Announcements gets delayed by 6 seconds for the 3rd party CTI merge calls.	8.1.2.0.0
CM-35810	unlock_time is set to 0	System will report that the login was not locked (even though it is) when the unlock_time is set to 0.	7.1.2.0.0
CM-35827	Traffic Run	System was reset in traffic case, when Call ID was above system limit	7.0.1.2.0
CM-35843	CC Elite Call Center using Externally Controlled Distribution (ECD) special application 9137.	CC Elite customer with Externally Controlled Distribution (ECD Special Application 9137) and agents that place outgoing calls may have delays in delivery of calls to ECD skills.	7.1.3.6.0
CM-35848	SIP stations routing over SIP trunks.	SIP stations sometimes cannot receive inbound calls, all SIP trunks are stuck in busy state.	8.1.1.0.0
CM-35876	VDN, agent transfer to another VDN	DABN event seen on spi.log when attended transfer was done by agent to a VDN after swapping the call appearances.	7.1.3.6.0
CM-35877	Calling-party number conversion, tandem calls	CM sat "CALLING PARTY NUMBER CONVERSION FOR TANDEM CALLS" form lost entries when "all" used in "delete" field sometimes.	8.1.1.0.0
CM-35910	Abbreviated-dial personal list, commandhistory log	The commandhistory log entry for "abbreviated-dialing personal" omits 'personal' from the entry.	8.1.2.0.0
CM-35979	Elite with CMS release 18 or higher connected.	Elite with CMS release 18 or higher connected.	7.1.3.0.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-35991	High volume of DSP resources in a network region.	CM SAT 'list measurements ip dsp-resource hourly' command displayed incorrect data that overflows the 'DSP Usage' field when high volume of DSP resources were used for an IP network region.	7.1.3.5.0
CM-36008	Aura Media Server(AMS), Secure Real-Time Transport Protocol (SRTP) enabled codec set and endpoints	No talk path issues seen when using Secure Real-time Transport Protocol (SRTP) with Aura Media Server (AMS)	8.1.1.0.0
CM-36009	CC Elite with special application SA9137 activated for Externally controlled distribution	False agent available messages were being sent to the Afiniti EBP product. This fix only applies to customers with SA9137 and Afinti EBP deployed.	7.1.3.6.0
CM-36029	Register sip-station with feature button 'hntpos-bsy' and either of team/SAC/Call-fwd button	When sip-station with button 'hntpos-bsy' and other feature like team/SAC/CF buttons, sends polling SUBSCRIBE, NOTIFY from CM in response contains malformed XML body	7.0.1.0.0
CM-36030	Adjunct route, vector collect step	Adjunct route failed while processing the vector collect steps.	8.1.2.0.0
CM-36086	CM active agent telecommuter service links	Increase max telecommuter service links from 3500 to 5000, thus allowing higher capacity.	7.1.3.1.0
CM-36126	Domain controlled SIP endpoint, Enhanced Call Forward	No CTI notification was sent for ECF (Enhanced Call Forward) invocation via button by SIP endpoints	7.1.3.4.0
CM-36155	SIP calls	Memory leak in transactionMap due to SIP INFOrmation method processing	8.0.1.2.0
CM-36195	J169 station, call-appr buttons, 6 buttons after autodial button	On J169 or J179 station types and others, autodial buttons can sometimes be corrupt if 6 call-appr buttons are administered after the autodial buttons.	8.0.1.2.0
CM-36199	Call appearance, EC500, IX workplace	Sometimes call appearance hangs after making EC500 call with IX Workplace	7.1.3.5.0
CM-36207	recorder setup in per call	Intermittently calls did not get recorded on NICE when per call registration is turned on	8.1.2.0.0
CM-36231	Unregistered SIP hunt-group user, EC500 enabled.	Unregistered SIP hunt-group user did not ring with EC500 enabled	7.1.3.0.0
CM-36235	Enterprise Survivable Server(ESS), recorded announcements on Aura Media Server(AMS)	Customer is not able to listen to Aura Media Server (AMS) announcements	7.1.3.5.0
CM-36280	One X Agents that are not ASAI controlled.	In using One X Agent, Service Link (S/L) is set for as-needed but is acting as if permanent and back to back calls are not ringing the cell phone for each new call,	8.1.2.0.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
		callers are immediately link to the cell on the same S/L.	
CM-36281	Original CM8.1 OVA that does not support disk encryption,	Log entry is expected every 15 minutes on systems running the original cm8.1 OVA that does not support disk encryption. Log entry does not occur on all systems.	8.1.2.0.0
CM-36323	One-X Communicator	Duplicated Communication Manager experienced a server interchange due to a segmentation fault caused by a rare race condition when an H.323 One-X Communicator Registered.	8.0.1.2.0
CM-36358	Make 7 calls to a meet-me conference bridge	Meet-me conference feature allows more than six parties to be in a call and logs multiple proc errors after that.	8.1.2.0.0
CM-36359	Call redirection, Vector Directory Number(VDN), Interactive Voice Response(IVR), transfer.	Counted-call doesn't work if call is redirected to another Vector Directory Number (VDN) via SIP Interactive Voice Response (IVR) transfer	8.0.1.1.0
CM-36383	AACC, ASAI, blind transfer	Agent cannot transfer a call to Network Skill CDN during a call	8.1.2.0.0
CM-36403	Incoming H323 trunk call to H323 station, which is being monitored by ASAI, and this call dropped due to NATO time expires.	No ASAI drop event when call dropped due to no answer time out expires.	7.1.3.5.0
CM-36404	Unregistered J169 and J179 phones, per-COline	J169 and J179 phones stay in incorrect internal ring state after release of the call causing incorrect ring for subsequent calls	8.1.0.2.0
CM-36420	SA8887, abbreviated list	Testing the "Hotline for IP telephones" (SA8887) feature and observed that this is working fine as long the DC for abbreviated list is lower or equal to 89.	8.1.2.0.0
CM-36421	Transport Layer Security (TLS), CLAN, large certificates	Transport Layer Security (TLS) handshake fails on CLANs with large certificates	8.1.2.0.0
CM-36474	Avaya Agent for Desktop (AAFD)	User having intermittent Avaya Agent for Desktop (AAFD) login issues.	7.0.1.3.0
CM-36495	Call Center with Externally Controlled Distribution (ECD) through an AES application.	CC Elite occasionally delivered a call to an agent without informing the ECD controller that the agent was available.	7.1.3.1.0
CM-36510	Call Centers without EAS and CMS connected	Call Centers with traditional ACD (not EAS) may encounter reset of the link to CMS after adding or removing an even-digit extension from an ACD hunt group.	7.0.0.0
CM-36574	Call Centers and Oceana customers with SIP agents.	SIP Agents were not moved to AUX after several failed attempts to route multiple Oceana DAC calls to the agent.	8.1.2.0.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-36666	Principal station, call forward, and bridged station is unregistered.	Phones with bridge-appearance keep ringing and customer has to unplug the phone (9608G) to stop the issue	8.1.0.2.0
CM-36676	Extension to Cellular (EC500), Aura Media Server (AMS) and Secure Real-time Transport Protocol (SRTP)	If EC500 answers too soon, and SIP Direct Media is on, Secure Real-time Transport Protocol (SRTP) key from EC500 leg gets sent with AMS's answer and the caller does not hear ringback	7.1.3.4.0
CM-36713	SA9050	Executing command "list ars route-chosen 1xxxxxxxxx (where x is any digit) loc 3 par 3y (0-2)" results in to segmentation fault that can lead to restart of Communication Manager application.	8.1.1.0.0
CM-36726	Repeatedly pickup buttons get "stuck" and have to be cleared by Corruption team.	Occasionally, pickup buttons get "stuck" and have to be cleared by Corruption team.	7.1.3.6.0
CM-36727	SIP IX iPhone dual-registered with H.323 phone	SIP IX iPhone dual-registered with H.323 phone couldn't answer a second incoming call if another call was active with the dual-registered H.323 phone.	7.1.3.6.0
CM-36729	Vectors with Lookahead Interflow.	Debugging logs filled up quickly with software process errors.	8.1.2.0.0
CM-36747	Faulty recovery, process trap	Recovery from a process trap is not handled correctly which results in delayed recovery and an unnecessary system restart.	8.0.1.2.0
CM-36749	Call Center with Externally Controlled Distributor and SIP agents.	An Externally Controlled Distributor sometimes received 'resource busy' upon attempt to route a call, only to find that CC Elite later sent a call to the agent.	7.1.3.6.0
CM-36750	All Communication Managers (CMs) that are not configured as cluster or array CMs.	Depending on the configuration of Communication Manager (CM), a warning is displayed for missing files that are not backed up. This is not an error, but the backup reports it as a warning which is concerning to some customers.	8.1.0.0.0
CM-36774	Video call, Session Initiation Protocol (SIP) and H.323 station	Sometimes video calls between sip and H.323 stations result in a segmentation fault	8.0.1.2.0
CM-36778	SIP Attendant, tenant partitioning, Return call timeout	The call never comes back to attendant when SIP attendant does blind transfer to another station if transferee does not pick up the call and return call timeout expired	8.1.3.0.0
CM-36820	Admin VOA on AMS and route the call on agent with service link	Customer and agent may not be able to connect if AMS is the media server used for VDN of origin announcement (VOA).	8.1.2.0.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-36849	Media Processor (MEDPRO), Voice over the LAN (VAL) ip-interface form that is enabled.	Cannot change or remove an enabled MEDPRO or VAL type ip-interface.	8.1.3.0.0
CM-36856	SIP agent, Look Ahead Routing (LAR)	SIP agent cannot be put into AUX mode after direct SIP agent call gets multiple 500 error responses if the last preference of LAR (Look Ahead Routing) route pattern had "next" or "rehu" configured.	8.1.2.0.0
CM-36886	Trunk call, Vector Directory Number (VDN), hunt group, Single Step Conferencing (SSC)	Automatic Call Distributor (ACD) auto answering agent is not able to auto answer the call after transfer.	8.1.2.0.0
CM-36994	Aura Media Server (AMS), Music on Hold (MOH) source	Music on Hold (MOH) terminates from Avaya Aura Media Server (AAMS) while listeners are connected.	8.1.2.0.0
CM-37018	Incoming trunk call	Incoming trunk call with leading destination digits similar to AUTO-IN Feature Access Code (FAC) code results in segmentation fault	8.1.1.0.0
CM-37019	Vector with wait step hearing ringback followed by queue-to skill step	Communication Manager (CM) reset as a result of an Intelligent Services Gateway (ISG) crash which is caused by an incoming call over QSIG trunk to a vector with a wait step providing ringback which is then queued to a skill with no available agents.	8.1.2.0.0
CM-37076	A small memory config Main CM with a survivable server registering to it.	A small main system experienced rolling reboot when Local Survivable Processor (LSP) registers to it.	8.1.3.0.0
CM-37139	Session Initiation Protocol (SIP) Direct Media (DM), media encryption	Call dropped when Avaya Agent for Desktop (AAfD) holds and unholds the Secure Real-Time Transport Protocol (SRTP) call on telecommuter	8.1.3.0.0
CM-37160	Call-Fwd Feature Access Code (FAC), Session Initiation Protocol (SIP)	Dialing Call-Fwd Feature Access Code (FAC) from SIP phone (9608) on dialpad results in denial event 1601.	8.1.3.0.0
CM-37254	Communication Manager (CM) 8.1.3, Amazon Web Services (AWS)	Communication Manager (CM) 81.3 running on Amazon Web Services (AWS), interchange sometimes	8.1.3.0.0
CM-37270	Incoming ISDN-PRI trunk call, consultative transfer	Call Detail Recording (CDR) report was not generated for 2nd leg in case of warm/consultative call transfer.	7.1.3.7.0
CM-37327	Make DM=off and make call and test rtppayload for DTMF	Customer may experience issue with DTMF dialing	8.1.11.0.0
CM-37487	Incoming SIP trunk call	Sometimes cannot hang up an incoming SIP trunk call if the call was ended from the external side.	8.0.1.1.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-37558	IX workplace (IXW), call park, call unpark	"Conference 2" appears on the endpoint display when a call parked by IX Workplace is un-parked. This results in no "Transfer" feature on the un-parked endpoint.	8.1.2.0.0
CM-37560	Port Networks (PNs) with a lot of announcements	Potential cross talk when the system has many announcements and agents across Port Networks (PNs) and announcements are configured only on 1 Port Network (PN)	7.1.3.3.0
CM-37561	SIP call	Due to a rare condition, SIP trunk traffic caused a Communication Manager segmentation fault and a server interchange.	8.1.2.0.0
CM-37623	Large number of trunks	Internal trunk translation corruption	8.1.2.0.0
CM-37722	SIP Direct media	Called name not displayed when calling from SIP phone to H.323 trunk and SIP were in Direct Media call.	8.1.3.0.0
CM-37723	J1xx phones in pickup group.	On J1xx phones if a call was dropped while Enhanced pickup display was active, UNKNOWN was shown on top line	7.1.3.3.0
CM-37864	Call Center Elite with CMS. Incoming calls to vector on sip trunks.	Incoming call over SIP trunk to vector. Incoming call had prepended + and ani was more than 13 digits	8.1.2.0.0
CM-37904	VDN, auto-msg wait button, SIP station	Message waiting lamp does not lit on SIP stations with Auto-msg wait button for VDN once they re-reregister after message was left for vdn	8.1.3.0.0
CM-37918	Call center with SIP agents.	SIP agents received more reserve skill calls than H.323 agents in a call center with both SIP and H.323 agents.	7.1.3.5.0
CM-37943	SIP routing configured on CM and SM for loop.	Communication Manager was reset because of SIP call looping between CM and SM.	8.1.2.0.0
CM-37944	data module, X-ported station, upgrade to 8.1.2	Command fails with "Error encountered, can't complete request" on executing "list data-module" after upgrade to 8.1.2.0.0	8.1.3.0.0
CM-38042	Enhanced call forward, External Ringing for Calls with Trunks, different destination for internal and external calls	Transferred call is forwarded to destination set for external call	7.1.3.5.0
CM-38050	SIP agent	CM could experience a segmentation fault and a server interchange when enabling service observe feature or logging into the agent using a very long agent ID.	7.1.3.6.0
CM-38256	Vector Directory Number (VDN), VDN of Origin Announcements (VOA), "Answer" button	We can't skip the VDN of Origin Announcements (VOA) by pressing "Answer" button twice on StationLink	8.0.1.1.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-38257	2 VDNs, IVR, converse on transfer,	Alert and connected ASAI event missing when trunk call is transferred to VDN	8.1.3.0.0
CM-38319	trunk to trunk transfer on same trunk group	ASAI Connected event missing when trunk to trunk call over same trunk group is transferred	8.1.3.0.0
CM-38371	Predictive dialing	Sometimes Communication Manager may reset when executing predictive dialing call flows	8.1.2.0.0
CM-38383	Call Park, Call Park Timeout Interval, shared extension.	Call Park was not providing ring back to originator after Call Park Timeout Interval had expired and if the call got parked from SIP phone to a shared extension.	8.1.1.0.0
CM-38400	VDN that terminates to AEP, call transfer to an agent.	CDN showed up with VDN number instead of the transfer number on internal calls.	8.0.1.2.0
CM-38666	SIP trunk, vector with converse step, agent, Auto In, Auto Answer, ASAI monitored	CTI-client was not receiving events	7.1.3.4.0
CM-38694	SA8312, paging users	Some paging users are not receiving page when SA8312 is enabled	8.1.3.0.0
CM-38820	SMGR, Duplicate hunt group command	System Manager "duplicate hunt-group" and "duplicate vdn" notification does not work	8.1.2.0.0
CM-38875	SIP Phones, Bridge appearance, Session Border Controller (SBC)	Calls may not ring on bridge appearance of a station with a special character "&" in its display name and principal station was called at a coverage point	7.1.3.6.0
CM-38900	MO_CTRK audit, Agent login using FNU	FNU feature activation/ deactivation fails	8.1.2.0.0
CM-38937	Extension must have the highest assignable station UID, 0xa028 or 41000 decimals.	Windows user 5521 cannot activate automatic callback for certain internal calls.	8.0.1.2.0
CM-38973	Coverage Answer Group (CAG), unregistered SIP phone	if one of the SIP members in CAG is not registered; the stations in CAG rings only once irrespective of the number of rings set on coverage path	8.1.3.0.0
CM-38986	Encryption enabled with media resource as AMS.	One way audio after SIP ReINVITE with SRTP key change having AMS (Avaya media Server) as media source.	8.1.1.0.0
CM-39054	Call Centers agent login after extension is deleted and added.	Occasionally a station becomes 'stuck' in a state that would not allow an agent to log in.	8.1.2.0.0
CM-39073	29 digit called party number	When a call was made on a trunk to a number more than 21 digits then a trap was seen in ISG when sending drop event.	8.1.3.0.1

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-39123	H323 and SIP stations with crss-alert buttons.	Crisis-alert was not working on SIP Phones.	8.1.1.0.0
CM-39124	CTI, conference, ISDN trunk, Look ahead routing	Bad party count on CTI conference event seen when LAR was enabled.	8.1.3.0.1
CM-39140	Avaya CM system with small memory config.	Avaya Communication Manager system running on small memory model experienced rolling reboots.	8.1.3.0.1
CM-39196	SSH, FIPS mode	SSH to CM 8.1.3.1 failed after FIPS mode was enabled	8.1.3.1.0
CM-39229	3PCC make call	Blind transfer fails as 3PCC make call was not handled in CM due to pending refer dialog.	8.1.3.2.0
CM-39386	Call Center with CMS processing agent skill changes.	Link to CMS could bounce after CMS changed agent skills.	7.1.3.8.0
CM-39466	list trace command on SAT	Avaya Communication Manager restarted when executing "list trace ewt medium 402194"	8.1.3.0.0
CM-39518	Cover to 'attd' with tenant attendant or console SIP enabled and routing/server to a VDN that does a route-to UDP attendant number.	If SIP Attendant was configured, call kept ringing on station after coverage.	8.1.3.1.0
CM-39596	SIP call	Communication Manager experiences a segmentation fault if the incoming Invite had a very large user portion in the Request URI.	8.1.3.0.0
CM-39609	AWOH in circular hunt group	CM sent CTI monitor related DOMAIN alert messages for AWOH station with EC500 disabled.	8.1.3.0.0
CM-39646	Agents using as-needed service links.	As-needed agent service links dropped by CM prematurely.	8.1.3.1.0
CM-39669	Coverage answer group with more than 10 members and all 10 members are unregistered and 11th member is registered and monitored	If call covers to coverage answer group and it gets answered by a member of CAG, which is present at higher index than 10 , then the ISG connected event was not sent by CM	8.1.3.0.0
CM-39697	SIP stations, enhanced call forward, bridge	No ring back for SIP calls termed to unregistered and bridged SIP station having enhance call forwarding enabled.	8.1.3.0.0
CM-39723	Server with combination of 41,000 stations and EAS agents with TDM stations and H.323 stations.	Translation corruption was observed when merge failure of station endpoint or softphone if server is near or out of station records as shown on page 8 of the 'display capacity' form.	7.1.3.5.0
CM-39732	SIP phone non-call/bridged appearance button, bridged appearance and call transfer	SIP phone with non-call/bridged appearance button gets into corrupted state if B_AACC_ONE_CONF flag is assigned to it.	8.1.3.1.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-39748	Session Manager-Cluster signaling group	Avaya Communication Manager may experience system reset when handling AFR (Alternate Failover Routing) call scenarios	8.1.3.0.0
CM-39974	CDR for Origination field is set to 'none' on the off-pbx-telephone configuration-set form.	CDR OPTIM account code 88888 is output in the auth-code field of the CDR record.	8.1.3.0.0
CM-40002	Incoming trunk call, transfer over hunt group and VDN having announcements configured in between	CDR for calls transferred over hunt group and VDN populates announcements extension instead of station's/agent's extension.	8.1.2.0.0
CM-40090	Attendant transfer recall trunk, VDNs in different Network Region	Attendant transfer recall was not working when calling trunk was in different tenant than the called VDN's tenant	8.1.3.0.0
CM-40092	SIP service link, AMS (Avaya Media Server)	After hold, unhold 1 way talk path was observed on SIP service link call	8.1.3.1.0
CM-40317	SIP endpoint, record this call using SSC, Hold, Unhold	After Unhold, the Unhold tag is sent in reason header twice to the far end, if a call recorder is attached to a call placed from a SIP endpoint	8.1.1.0.0
CM-40402	Media Gateway with network outages	Communication Manager sometimes experiences segmentation fault when there's network instability to the Media Gateways.	8.1.3.0.0
CM-40455	VDN, vector, skills	Call Transferred event had additional connected number blocks when vector to VDN had multiple skill splits. Also, ASAI party query shows additional skills in the call.	8.1.3.0.0
CM-40470	2 CMs Connected via SIP-Trunk, SIP-A, SIP-B connected to CM-1, SIP-C connected to CM-2, SIP-B enables Call-forward-all to SIP-C.	Call-forwarding display should hide external contact info from SIP	8.1.3.1.0
CM-40485	SIP traffic	Communication Manager (CM) can experience a system restart if the far end SIP client sends 200OK response to the INVITE message followed by a BYE method before it sends the 200OK response to an outstanding PRACK message.	8.1.3.0.1
CM-40565	SIP conference without SEMT	When SEMT (SIP Endpoint Managed Transfer) was turned off, Communication Manager did not tandem the P-Conference header to the conference server. As a result, the conference participants may not land on the same conference room.	8.1.3.0.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-40583	Inbound call, DMCC registered on SIP station with independent mode	Inbound call not connected due to ACK timeout at station when SIP DM is on	8.1.3.1.0
CM-40584	SA9122, call from caller in same location as station, but station's SIP trunk should route to different location	Sometimes the system is blocking calls to SIP stations in same location as caller if SA9122 is enabled	8.1.3.0.1
CM-40593	SIP bridge	Call answered by a SIP principal, put on hold then picked up by a bridged user fails to update the principal's call appearance and the call does not drop with the principal but gets stuck.	8.1.3.0.0
CM-40604	SIP service observer station under DMCC shared control	Toggling of Service Observer mode on a SIP service observer while observers station is under DMCC shared control.	8.1.3.0.0
CM-40643	Call Center customers using BCMS.	Agents were getting login denials with denial event "2127 DNY_IAGENT_TOT" though the number of agents logged in was well under the allowed limits. The agents (skills) were measured as "internal" or "both".	8.1.3.0.1
CM-40668	Change trunk-group xx Dial Access? y Digit Handling (in/out): enbloc/overlap	When trunk is called using dial access code, party query response was giving incorrect party count.	8.1.3.1.0
CM-40680	Call from SIP trunk with SIP Direct Media turned on, Call answered on a bridge, which has a shared control DMCC (device media and call control) softphone registered	Calls answered at bridged extension which had a shared control DMCC did not have talk path when incoming SIP trunk had SIP DM turned on.	8.1.3.0.1
CM-40695	Service Observing agents, incoming trunk call, conference	Service observed agent answers incoming trunk call and conferences another service observed agent and then drops from the conference and all the parties got dropped.	8.1.3.0.1
CM-40708	Direct Media enabled for SIP originator, SIP station to SIP trunk call with H.323 call-recorder, AMS	One-way talk path issue was observed on a SIP station to SIP trunk call with an H.323 call-recording resource involved and an AMS providing VoIP resources for the call. The issue happened when DM was enabled for SIP originator.	8.1.3.0.0
CM-40722	BRI trunk, location based routing	Calls from some trunks do not follow OPTIM location based routing	7.1.3.6.0
CM-40811	SOSM enabled and pickup group, SA9124 enabled	For SOSM domain controlled stations: 1. The call pickup event was not sent to principal pickup member for incoming trunk call. Also the party id was incorrect in case of internal station pickup. 2. connected number was not set properly when SA9124 is enabled	8.1.2.0.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-40812	SOSM enabled, call forwarding	Duplicate EVNT_TERM seen for SOSM controlled station when the call was forwarded to another station	8.0.0.0.0
CM-40872	SIP trunk call	When the far end SIP client sent an invite with invalid number to CM, if the call type analysis table was configured and used, CM sent 200OK and then a BYE message. This behavior has been changed to send 484 error response.	8.1.2.0.0
CM-40889	Dual registered DCP station with OPS mapping	A call made from a DCP station with an OPS (Off-PBX Station) mapping occasionally drops during VDN collect step.	8.0.1.1.0
CM-40913	SIP call, transfer	P-Asserted Identity SIP header showed display name of the original caller and number of the transferring party in the outgoing INVITE during a transfer call.	8.1.1.0.0
CM-40938	"Send UCID" flag disabled on SIP trunk group, Incoming call over ISDN trunk.	UCID was sent in the User-to-User header even if "Send UCID" flag was disabled on SIP trunk group.	8.1.3.1.0
CM-40966	Incoming SIP trunk, ISDN, NR, TAC	Avaya Aura Communication Manager was sending the trunk's TAC as calling party number when making emergency call over ISDN trunk.	8.1.2.0.0
CM-40968	Calling Name on CO trunk, SIP stations with bridged appearances	SIP bridged appearance display was incorrect for CO trunk calls.	8.1.1.0.0
CM-41013	Enhanced Call Pickup Alerting	Call transfer while a call is ringing on pickup group did not work.	8.1.3.0.0
CM-41039	SA9095 enabled, hunt group call, coverage, RONA	Hanging transactions in CTI app due to missing ASAI redirect event	7.1.3.5.0
CM-41069	SIP ACD call	A call to a hunt group or agent could drop during a short network outage.	8.1.2.0.0
CM-41203	EC500, VoiceMail	When timed Voice Mail detection on EC500 settings was turn on and the far end cell EC500 user answered the call on EC500 before timer expires then a denial event was published in list trace station on which EC500 was enabled	8.1.3.1.0
CM-41218	SA9106 enabled, ASAI monitored call, EC500, SSC	Missing disconnect event for the monitored station who dropped from the call using EC500	7.1.3.5.0
CM-41297	SSTA recorder, service observer	Station with SSTA recorder could not Service Observe.	8.1.3.1.0
CM-41313	Remote Service Observer and encryption enabled display remote-access REMOTE ACCESS	When service observer was remote, it got dropped when idling the service link.	8.1.3.1.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-41317	SIP call	On rare occasions, Communication Manager experienced segmentation fault if the contact header had no display name.	8.1.2.0.0
CM-41319	SIP phone, J179, call forwarding	Call forwarding to a non-exist number may freeze J179.	8.1.0.0.0
CM-41340	Incoming SIP trunk call with bad SDP FMTP attribute	Sometimes Communication Manager crashed when SIP SDP contained incorrect FMTP attribute format	8.1.2.0.0
CM-41347	SIP station calls, VDN	VDN or diversion information was missing in case of SIP call terming to another SIP station through VDN.	8.1.3.1.0
CM-41393	Calls to a VDN/vector that plays an announcement.	CDR reports show announcement as dialed number instead of the dialed VDN.	8.1.3.1.0
CM-41579	QSIG, H.323 trunk, SIP phone	When a call was transferred to a SIP station through H323 QSIG trunk, the transfer target's	8.1.3.1.0
CM-41627	CM server with physical port network cabinets.	The "Expansion Port Networks" field on page 4 of the SAT 'display capacity' form, did not show the correct number of EPNs.	8.1.3.1.0
CM-41647	DMCC, shared station	Incorrect understanding as "Softphone Enabled on Station Form" field in display capacity was marked as 0 unless a shared station was registered	8.0.1.0.0
CM-41737	CDR, Diverted call, IVR, VDN, Agent	CDR - Diverted call from PRI to SIP to IVR and to VDN did not produce CDR when answered by agent.	8.1.3.1.0
CM-41740	Duplex CM, IP endpoints	CM Interchanged sometimes when processing IP endpoint call flows	8.1.1.0.0
CM-41757	SIP station, transfer	Transferrer SIP station could not be dropped if it tried to transfer the call to an unregistered SIP station which had a bridge phone registered.	8.1.3.1.0
CM-41788	CM interop with Microsoft Teams over SIP trunks using TLS. OR Any Downlink forking scenario with Mid field in 183 provisional response SDP.	CM could not handle mid field in 183 SDP for some reason. Proc errors 7171/9929 and 7171/64611 were logged and CM sent Cancel to end the call.	8.1.0.2.0
CM-41896	Stations with call-fwd buttons.	PPM did not work right when 'call-fwd', 'send-calls', etc... were removed.	8.1.3.0.1
CM-41902	Enable SIP Agent Reachability? y Enable Reachability for Domain Control SIP Stations? y Monitored stations	When SIP Reachability for agent was enabled, TSAPI endpoint registration query sometimes responded with service state as unknown.	8.1.3.0.1

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-42173	CM 8.1.x, enable DMCC shared control for the SIP station and then unpark a call using that SIP station	No media received at recorder / shared control when associated sip phone unparks a call	8.1.3.1.0
CM-42177	Duplicated CMs, shared control stations.	Sometimes, duplex CM interchanged when exercising call flows related to shared control stations	8.1.3.0.1
CM-42293	DMCC recorder per call	CM restarts after 6 days of memory leak due to stale H323UserSelLisInfo objects in DMCC recorders	8.1.3.1.0
CM-42295	SA9142 enabled, hunt group	When SA9142 was enabled, the pickup group members were able to see the hunt group member's name and number, instead of the hunt group name.	8.1.3.2.0
CM-42333	Record Agent ID on Incoming?' enabled on the system-parameters cdr form, PRI, VDN, CDR	CM CDR was capturing VDN numbers instead of agent's extension for calls diverted from PRI to SIP to IVR.	8.1.2.0.0
CM-42365	ASAI make-call, AAR feature access code CM off-hook timeout.	ASAI make-call dialing/calling AAR feature access code didn't follow CM off-hook timeout.	8.1.3.1.0
CM-43174	Shared control port	Communication Manager (CM) experienced Multiple server interchange a day due to frequent segmentation faults when the shared-control port was disconnected from an active station.	8.0.1.2.0
CM-43176	Internal calls, analog stations, display	Calling party extension length displays the entire 10 digits on analog endpoints when calls were originated internally	8.1.3.0.1
CM-43177	SA9095 enabled, SIP stations, hunt group	CM tried only 20 times to reach a hunt-group member, if first 20 hunt-group members were unregistered and the call failed.	8.1.3.1.0
CM-43186	configured SIP signalling grp > 1023	TSAPI station registration query failed for higher sig group number / index	8.0.0.0.0
CM-43241	CC Elite Agent SIP station with Q-stats button configured.	Q-stats button displays incorrect value when queue length exceeds 999	8.1.3.1.0
CM-43242	EC500 configured but disabled Coverage path taking to CAG set Main station is logged off Main station is domain controlled	Hanging SIP transactions when a domain controlled, logged off station having ec500 was configured but disabled, and still received a call	8.1.3.1.0
CM-43681	Far end modifying SRTP key in 200 Ok response to session refresh INVITE.	When far end changed SRTP key while responding to a session refresh ReINVITE, it caused one way talkpath.	8.1.3.2.0
CM-43704	IP-DECT phone configuration	Event redirect is not received if call for IP-DECT phones were rejected or busy and call termed to next agent in skill	8.1.3.2.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-43722	ASAI, monitored SIP station, call transfer	Incorrect calling party number in ASAI ALERT and CONNECT message during transfer	8.1.3.2.0
CM-43723	NHC (No Hold Conference) preset destination	no-hold-conf preset destination got changed if 10th digit is 7 , it changes to 5 in NHC flow.	8.1.1.0.0
CM-43789	SIP with 100 rel	The text value in reason header of the 200 OK was corrupted when CM tried to tandem the 200 OK out to the calling side when PRACK was delayed.	8.1.3.1.0
CM-43790	Call forwarding, PSTN	When call forwarding (CF) is enabled and destination number is external/PSTN number, after call routes back to extension's voicemail, call still kept ringing.	8.1.3.1.0
CM-43864	SIP features, SIP stations	Due to memory leak related to SIP features, customers need to restart the system sometimes.	8.1.3.2.0
CM-44395	SA9095, hunt group, H.323, SIP, dual registration	Calls to a SA9095 hunt group with 1 or more dual registration H323+SIP members failed to ring the H323 station if the SIP station was unregistered.	8.1.3.1.0
CM-44611	CM with stations translated	CM reload and Interchange occurred. Station button audit compaction routine over wrote critical button memory management data resulting in a CM reset and an eventual interchange.	8.1.0.2.0
CM-44697	CTI - AES - CM 8.1, failed incoming xfer over a trunk	Issues at CTI app end due to unexpected reconn event	8.1.3.1.0
CM-44736	IGAR calls	After specific limit of IGAR calls, customer was not able to use IGAR feature	8.1.3.1.0
CM-44757	EC500 with MFC trunk--group	EC500 trunk was not dropped when principal station drops	8.1.3.1.0
CM-44837	SAC/CF Override', consultative transfer	SAC/CF Override' did not work in a consultative transfer when 2nd leg was initiated on a bridged call appearance by pressing a team button and terminating to a SAC station.	8.1.3.0.1
CM-44909	CS1K set, one call appearance	Call forward feature couldn't work on CS1K set type if the CS1K set only had one call appearance and this call appearance button was active on the call.	8.1.3.1.0
CM-44910	SIP SUBSCRIBE for reg-event	Even after unregistered event on CTI the stations status query returned the state of station as in-service.	8.1.3.1.0
CM-45055	SIP station, registration	After SM upgrade (reboot), AACC (Avaya Aura Contact Center) couldn't use lots of SIP stations (agents) anymore because CM (Communication Manager) always reported	8.1.3.1.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
		the sip stations's registration state as unregistered although the sip stations were already reregistered to the SM after SM upgrade.	
CM-46660	SAT with media-gateway	The user was able to execute the 'change Synchronization media-gateway' command even when the "Synchronization over IP?" field was set to 'n'	8.1.3.2.0
CM-46669	Display Capacity from on the SAT interface and go to page 8 where the Administered IP SoftPhones field resides.	On the SAT 'display capacity' form the "Administered IP SoftPhones" field displayed the incorrect system Limit.	8.1.2.0.0
CM-46753	SIP station dialing external ISDN call	Privacy:ID header was inserted in SIP 183 method for unrestricted user	8.1.3.2.0
CM-46843	SA8967 enabled and add more than 10 'send-nn' buttons to a station that supports them.	User couldn't add more than 10 'send-nn' buttons to a station.	8.1.3.0.1
CM-46864	SMDR configured	Warm restart was happened	8.1.3.2.0
CM-46880	TSAPI monitor	EVNT_INIT and EVNT_HOLD were sent out of sequence for AAFD and onex clients when they attempted to initiate conference	8.1.3.2.0
CM-46951	SIP station, group page	When only 1 SIP Phone was configured in a group-page, phone speaker was turned on and call to the group page resulted in busy notification to the caller.	8.1.3.3.0
CM-47076	SIP Station and SIP agents and trunk transfer	Calling party information not updated upon receiving a supervised transferred call.	71.3.8.0
CM-47100	H.323, DCP, SAT	On the CM SAT station form for H.323 station, the DCP port was displayed if the station was changed from DCP to H.323 while the station's softphone was registered.	8.1.0.1.1
CM-47128	call to physical station with agent logged in and then transfer	CTI application missing ASAI alerting and established events for the call resulting into multiple recording/reporting problems	7.1.2.0.0
CM-47238	vector with announcement step before queue to and sip signaling-group with IMS enabled	CPN for ASAI alerting and connected events is displayed as <no number> when announcement is played before queue to agent and orig is sip station	8.1.3.3.0
CM-47240	Base set was not registered and one shared control h323 station registered in independent mode	The extension's service state was stuck in IN-SERVICE state if the base set was not registered and one shared control h323 station registered in independent mode, and then unregistered.	8.1.3.3.0
CM-47243	!X messaging with skill configured	After messaging skill x for extension, CM takes around 3 sec to route the call to IX Messaging	8.1.3.0.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
CM-47418	Non-EAS agents	Non-EAS CM login 2 agents into a split and leave for 100 minutes	8.1.3.3.0

Known issues and workarounds in Communication Manager Release 10.1.x.x

Known issues and workarounds in Communication Manager Release 10.1.3.2.0

ID	Minimum conditions	Visible symptoms	Workaround
CM-55575	Call recording using ACS recorder, there should be a shared control station on Annex-LP station which is third party	Call is not recorded	No
CM-55452	Call recording with Station Tone Forward Disconnect: "busy" or "intercept" on "system-parameters features"	Long calls are recorded, which are bogus.	Set field Station Tone Forward Disconnect: to "silence" instead of "busy" or "intercept" on "system-parameters features" form.
CM-55312	Delete user from main server	Deleted user home directory not removed from survivable servers	Manually delete the deleted user home directory on survivable server
CM-55311	If a conference is done after enabling MCT	MCT button remains active after conf call drops	No
CM-55122	Service Provider sends FMTP parameter before RTPMAP in SDP	Video will not work	No
CM-54328	Select a DMCC station via SSC for call recording	call cannot be recorded	No

Known issues and workarounds in Communication Manager Release 10.1.3.1.0

ID	Minimum conditions	Visible symptoms	Workaround
CM-54708	Activate or deactivate 10.1.3.1 SP i.e. 01.0.974.0-27937 or patches built over the same	Server status may show crit_os on processes. Command history and /var/log/messages will not be generated during this time.	The status will clear itself up in 9 mins Or Reboot the CM server to correct the status immediately.

		Notify Sync to SMGR will also not work during this time	
CM-54435	ssh session to CM	Inactive SSH sessions will not get terminated.	No
CM-54811	Administer SIP station in a NR with no VoIP resource Enable DPT on the NR where the SIP station exists.	Calls made to SIP stations in this NR from another NR which has DTP enabled will fail.	Turn OFF DPT
CM-54701	Agent is being service observed and invoke MCT.	When SO drops, MCT lamp on station turns OFF.	No
CM-54698	Contact header value is greater than 40 characters in the SIP message	UCID is corrupted in the CDR record.	No
CM-54469	CM generates UCID	Timestamp in UCID is wrong	No
CM-54422	Selinux enabled on CM	Server status will show crit_os on processes	Set Selinux to permissive

Known issues and workarounds in Communication Manager Release 10.1.3

None

Known issues and workarounds in Communication Manager Release 10.1.2

ID	Minimum conditions	Visible symptoms	Workaround
CM-52417	list directory source mx 16 announcements	SAT commands was stuck	Use only one SAT terminal
CM-52858	Called party has to be SIP phone with EC500 turned on. EC500 leg should be on a SIP trunk which has Initial IP Direct Media turned on. EC500 Off-pbx config set must have Confirmed answer turned on.	When a call is made to such a station, after the call is answered from the mobile phone, there was no dial tone, so customer cannot press a DTMF to confirm the answer and allow talk path.	Turn off Initial IP Direct media on the EC500 leg.
CM-52904	603 error responses from far end	All queued calls were cleared when CM receives 603 error response from far end	Usually 603 is not sent from any far end. Far end had Bug which sent 603.

Known issues and workarounds in Communication Manager Release 10.1

ID	Minimum conditions	Visible symptoms	Workaround
CM-51758	JITC STIG RHEL-08-020041 with TMUX	CM and SMGR synchronization fails	Disable FIPS mode in CM

Avaya Aura® Session Manager

What's new in Session Manager Release 10.1.x.x

What's new in Session Manager Release 10.1.3.0.0

- From Release 10.1.3, the Session Manager supports displaying SIP user agent information of the endpoint on the **Elements** > **Session Manager** > **System Status** > **User Registrations** page in the Details section under the **Device** tab.

For more information, see ***What's New in Avaya Aura® Release 10.1.x*** document on the Avaya Support site: https://downloads.avaya.com/css/P8/documents/101078425

What's new in Session Manager Release 10.1.2.0

- From Release 10.1.2, System Manager Solution Deployment Manager and Solution Deployment Manager Client support the deployment and upgrade of application using the OVA with the SHA256 hash algorithm.
- Session Manager 10.1 OVAs are re-spun to support SHA256 algorithm. For more information, see the Required artifacts section.
- The old 10.1 GA OVA contains the Avaya Signing certificate that is going to expire on Feb 20, 2023. Therefore, to address the Avaya signing certificate expiry, the new 10.1 GA OVAs are renewed and re-signed with the latest Avaya signed certificates. For more information, see PSN020586u - Avaya Aura® OVA Certificate Expiry February 2023.
- From Release 10.1.2, you can set the time zone configuration for J100 phones in the new Time zone field on the Elements > Session Manager > Device and Location Configuration > Device Settings Groups page. The endpoint can locally determine the Daylight Savings settings appropriate to the time zone selected.

For more information, see ***What's New in Avaya Aura® Release 10.1.x*** document on the Avaya Support site: https://downloads.avaya.com/css/P8/documents/101078425

What's new in Session Manager Release 10.1.0.2

From Release 10.1.0.2, logging framework 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://downloads.avaya.com/css/P8/documents/101078425

What's new in Session Manager Release 10.1

With this release 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 10.1.x. It is imperative that the instructions in PCN2136S be reviewed for complete steps prior to installation of Security Service Packs on an SM 10.1.x system.

The old method of installing Security Service Packs will not work in Release 10.1.
The minimum release of SM 10.1.x.x that you must be on in order to install the Security Service Packs for SM is 10.1.0.1.
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 10.1.x.x, you must use the new command ("av-update-os") and follow the detailed instructions in PCN2136S.

For more information, see ***What's New in Avaya Aura® Release 10.1.x*** document on the Avaya Support site: https://downloads.avaya.com/css/P8/documents/101078425

Future use fields visible in Avaya Aura® Session Manager Release 10.1.x.x

Future use fields visible in Avaya Aura® Session Manager Release 10.1

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 this release 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 10.1.x. It is imperative that the instructions in PCN2136S be reviewed for complete steps prior to installation of Security Service Packs on an SM 10.1.x system.
The old method of installing Security Service Packs will not work in Release 10.1.
The minimum release of SM 10.1.x.x that you must be on in order to install the Security Service Packs for SM is 10.1.0.1.
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 10.1.x.x, you must use the new command ("av-update-os") and follow the detailed instructions in PCN2136S.

Required artifacts for Session Manager Release 10.1.x.x

Required artifacts for Session Manager Release 10.1.3.2

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	S/W Version number	MD5 Check Sum	Comments
Session_Manager_10.1.3.2.1013201.bin	SM000000295	1.99 GB	1013201	f93cbcfe6471b89212e423d331375b3b	Released on 15th Jan, 2024

Required artifacts for Session Manager Release 10.1.3.1

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	S/W Version number	MD5 Check Sum	Comments
Session_Manager_10.1.3.1.1013103.bin	SM000000280	1.9 GB	1013103	c3dd685cccc0a7980ef67f5f2b7724a1	Released on 28th Aug, 2023

Required artifacts for Session Manager Release 10.1.3.0

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	S/W Version number	MD5 Check Sum	Comments
Session_Manager_10.1.3.0.1013007.bin	SM000000269	1.9 GB	1013007	f3631a2527cb1906a3c5f39d45485207	Released on 22nd May, 2023

Required artifacts for Session Manager Release 10.1.2.0

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
Session_Manager_10.1.2.0.1012016.bin	SM000000257	1.9GB	1012016	Released on 13th February, 2023

Required artifacts for Session Manager Release 10.1.0.2

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
~~Session_Manager_10.1.0.2.1010215.bin~~	~~SM000000243~~	~~1.7 GB~~	~~1010215~~	Replaced by Session_Manager_10.1.0.2.1010219.bin For details, see PCN2135S.
Session_Manager_10.1.0.2.1010219.bin	SM000000246	1.7GB	1010219	Released on Oct 11, 2022

Required artifacts for Session Manager Release 10.1.0.1

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
Session_Manager_10.1.0.1.1010105.bin	SM000000228	1.7 GB	1010105	

Required artifacts for Session Manager Release 10.1

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-10.1.0.0.1010009-e70-02.ova	SM000000211	3.1 GB	1010009	Core SM
BSM-10.1.0.0.1010009-e70-02.ova	SM000000212	3.1 GB	1010009	Branch SM
~~SM-10.1.0.0.1010009-e70-01.ova~~	~~SM000000211~~	~~3.1 GB~~	~~1010009~~	~~Core SM~~
~~BSM-10.1.0.0.1010009-e70-01.ova~~	~~SM000000212~~	~~3.1 GB~~	~~1010009~~	~~Branch SM~~
Session_Manager_10.1.0.0.1010009.iso	SM000000213	2.1 GB	1010009	SW only
dmutility-10.1.0.0.1010007.bin	SM000000214	1.1 GB	1010007	
Session_Manager_10.1.0.0.1010012.bin	SM000000215	425 KB	1010012	SP0

Note: The old 10.1 GA OVA contains the Avaya Signing certificate that is going to expire on Feb 20, 2023. Therefore, to address the Avaya signing certificate expiry, the new 10.1 GA OVAs are renewed and re-signed with the latest Avaya signed certificates. The new OVAs are also updated to support SHA256 hash algorithm. For more information, see PCN2135S.

For more information, see PSN020586u - Avaya Aura® OVA Certificate Expiry February 2023.

Installation for Session Manager Release 10.1.x.x

Backing up the software

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

Installing the Session Manager software

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

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 10.1. 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 Manger

In this case, you must apply Security Service Pack #14 or later to each Session Manager - prior to initiating the 10.1 upgrade of System Manager.

Note 2: When upgrading directly from Session Manager 7.0.X to Session Manager 10.1, Centralized Call History records will not be retained.

Note 3: Due to significant architecture and security enhancements in 10.1, 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 10.1, 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 10.1 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 10.1 in a single maintenance window.

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_ECDH
   E_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_SH
   A256,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_A
   ES_256_GCM_SHA384,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDH_RSA_WITH_AE
   S_128_GCM_SHA256,TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_A
   ES_128_GCM_SHA256]
   ```

2. Execute “restart Cassandra”

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

Special Case Upgrade Paths

1. VMware based Session Managers
   The supported upgrade paths to Session Manager 10.1 are from:
   - SM 8.1 and subsequent feature or service packs
   - SM 8.0 and subsequent feature or service packs
   - SM 7.1 and subsequent feature or service packs
   - SM 7.0 and subsequent feature or service packs

   Note: Systems running any earlier SM release must be upgraded to one of the above releases before they can be upgraded to Session Manager 10.1.

2. KVM-based Session Manager
   The supported upgrade paths to Session Manager 10.1 are:
   - SM 8.1 and subsequent feature or service packs
   - SM 8.0 and subsequent feature or service packs
   - SM 7.1.1 and subsequent feature or service packs

   Note: Avaya no longer supplies KVM OVA files as of Session Manager 10.1. KVM installations should be done using the ISO file as described in *Deploying Avaya Aura® Session Manager in a Software Only Environment*

3. AWS-based Session Manager
   The supported upgrade paths to Session Manager 10.1 are:
   - SM 8.1 and subsequent feature or service packs
   - SM 8.0 and subsequent feature or service packs
   - SM 7.1 and subsequent feature or service packs
   - SM 7.0.1 and subsequent feature or service packs

   Note: Avaya no longer supplies AWS OVA files as of Session Manager 10.1. AWS installations should be done using the ISO file as described in *Deploying Avaya Aura® Session Manager in a Software Only Environment*

Troubleshooting the installation

Refer to Troubleshooting Avaya Aura® Session Manager.

Restoring software to the previous version

Refer to the product documentation.

Fixes in Session Manager Release 10.1.x.x

Fixes in Session Manager Release 10.1.3.2

Key	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-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

Key	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-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-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-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-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

Fixes in Session Manager Release 10.1.3.1

ID	Minimum Conditions	Visible symptoms	Issue found in Release
ASM-90996	Make sure SM is configured with third party certificates with rootca->subCA->ID certs. once configured execute initTM command, it may get failed while trying to retrieve subject-ID from the certificate chain.	initTM failed on the SM when SM has 3rd Party CA signed certificates.	10.1.2.0
ASM-90995	10.1 SM installed and run traceSM. Once traceSM started capturing SIP messages, Entity link name for a given administered entity should be displayed at the top in the traceSM ladder diagram instead of IP address.	SIP Entity names are not displayed at top of output of traceSM tool.	10.1.2.0
ASM-90716	1. Enable "Centralized call history" for a specific SIP user. 2. Make a station to station call, but while dialing the number, make sure it has hidden/special character (e.g. \x0f)	PPM throws error for getCallHistory requests and call log is not displayed.	8.1.3.5

ID	Minimum Conditions	Visible symptoms	Issue found in Release
ASM-90005	Enable HTTPS proxy server host and port from Session manager global settings.	If there are combination of 8.1.x and 10.1.x ASMs under 10.1.x SMGR Push Notification using proxy server cannot be enabled.	10.1.0.2
ASM-90835	This message comes whenever SM gets a BYE message from far end.	AsmUAInfo warning messages in /var/log/Avaya/asm.log file	10.2.0.0
ASM-91232	Any user addition/modification/deletion operation using SMGR User management page.	Data access objects required for user registration and downloading of Personal Profile Management (PPM) data do not get updated. Refer to PSN020605u.	10.1.2.0
ASM-91406	Issue can happen if CANCEL comes from far end before the call being answered by an endpoint.	SM does not process CANCEL message properly, resulting call gets dropped after 30 seconds	10.1.2.0
ASM-91132	Push Notification Provider with "Use Forward Proxy" box checked and HTTPS proxy configured on Global Settings page.	Push notifications stop working because code is not setting up HTTPS proxy properly in all cases.	10.1.0.2
ASM-90992	Can happen on Any ASM from 10.1.0.0 to 10.1.3.0 release.	/var/log/messages file filled up with ALARM-SYNFLOOD messages	10.1.0.0
ASM-90826	10.1 OVA that is upgraded to a later Service Pack.	The SM/BSM VM is unresponsive during an upgrade. The VM needs to be manually reset to start running again.	10.1.2.0

Fixes in Session Manager Release 10.1.3.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
ASM-90722	A non-Avaya SIP Phone registered to Session Manager	Actual Location information is not displayed under user registration page	8.1.3.7
ASM-90555	Multiple ports configured between SM and CM with same protocol	Only one port is marked as trusted.	8.1.3.4
ASM-90547	Run command sm-report on the Session Manager	SM CPU core to get blocked with 100% usage by IBM WebSphere.	10.1.0.2
ASM-90539	Not Known	All commands run on SM throw error indicating RPM database corruption.	8.1.3.6
ASM-90445	Run command sm-report on the Session Manager	Java core and hung thread on SM	10.1.0.2
ASM-90425	Export Performance Call Count data in the CSV format	The exported CSV file for Call Counts data is empty	10.1.2.0
ASM-90405	Session Manager configured with Apple Push notification feature and heavy traffic of Push Notification calls	Push Notification failure when more than one thread is attempting to send push	8.1.3.6

ID	Minimum Conditions	Visible symptoms	Issue found in Release
ASM-90170	Perform User Registration Export operation	User Registration Export for daily interval, reuses the old filename from the first day the job was created	8.1.3.6
ASM-90158	Use SMGR SDM for administering remote syslog servers.	The operation results in error and cannot administer remote syslog servers using SDM	10.1.0.2
ASM-89925	Enable PPM Debug logging using sm ppmlogon command.	The mgmt.log file is flooded with the SMCallHistoryDM migrateCallLogsToGlobalDCSpecial CallLog related logs	8.1.3.5
ASM-90116	Run traceSM command on the Session Manager	traceSM stops showing SIP messages when tracer_asset.log file is rotated	10.1.0.2
ASM-87134	Large numbers of route policies and dial patterns	S P registration failures after adding/deleting dial patterns from a route policy	8.1.3.2
ASM-85284	Run traceSM command while SM is under heavy traffic	If CPU occupancy reaches certain limit finest level of logging is turned off	8.1.3.1
ASM-90219	SIP Entity administered with (real DNS) FQDN	Inbound INVITE from SIP entity gets rejected by SM with Indeterminate Originating Entity response	8.1.3.6

Fixes in Session Manager Release 10.1.2.0

ID	Minimum Conditions	Visible symptoms	Issue found in Release
ASM-89850	SM 10.1.0.2 installed	SM becomes unstable	10.1.0.2
ASM-89849	“Endpoint Display Name” field with a double quote (“) character in it	Exceptions in SM Logs	6.1.0.0
ASM-89747	Push Notification Provider Settings are configured on SMGR with User defied description	CM-SMGR sync stops working after SMGR upgrade from 8.1.3.5 to 10.1.0.1	10.1.0.1
ASM-89828	SM has identity certificates with 3rd Party CA signed certificates	initTM/initDRS fails with Postgres exceptions displayed when restoring the backup.	8.1.0.0
ASM-89758	SM 8.1.3.0 installed	Some log files not readable using customer account.	8.1.3.0
ASM-89747	Push Notification enabled and had 3rd Party endpoint registered to SM.	Push Notification Status not displayed from System Status Menu of System Manager	8.1.3.5
ASM-89643	Upgrade the SM from 10.1.0.0 or 10.1.0.1.1 to 10.1.0.2	The "statapp" command will show the Cassandra application as being down	10.1.0.2

ID	Minimum Conditions	Visible symptoms	Issue found in Release
ASM-89630	An endpoint with 100 calls in call history.	New call history is not updated on the endpoint	10.1.0.1
ASM-89570	Run traceSM and enable Push Notification messages	TraceSM not capturing Push Notification messages when enabled.	8.1.3.6
ASM-89565	Push Notification feature enabled on AES monitored stations	Not able to answer the call using CTI Application	8.1.3.6
ASM-89370	SM 10.1.0.1 installed with Security Service Pack #4	User Data Storage Repair fails	8.1.3.5
ASM-89287	SIP traces are enabled using SMGR	Need to generate a Warning Alarm when SIP Traces are enabled	8.1.3.4
ASM-89140	Cal transfer from AAfD	Call transfer from AAfD fails	8.1.3.1
ASM-89123	SMGR installed and upgraded	Newy added CM is not visible while adding Application on CM	8.1.3.4
ASM-89053	Aura Solution with more than 6 SMs	Cassandra DB repair fails	8.1.3.3
ASM-88830	Remote Syslog configured with UDP Transport Protocol	Remote Syslog fails	10.1.0.1
ASM-88806	An automatic ID certificate renewal or a manual replacement of certificates at least one time	WebSphere ID certificates are not getting modified	8.1.3.4
ASM-87786	SMs are processing heavy traffic load.	The server.log file will contain messages about DAOs initialization.	8.1.3.7
ASM-87752	SMGR configured with NFS partition for storing SM performance data.	NFS partition for performance data was not automatically remounted after an SMGR reboot	8.1.3.3
ASM-86421	SMGR, CMs, SMs, and a large number of BSMs	Administrators may experience long delays or GUI timeouts when adding or removing a team button	8.1.3.1
ASM-89916	A J100 phone with newer firmware used with SM 8.1.3.x. 0r 10.1.x	The ppm.log and server.log on the SM may get getHomeCapabilities error many times	8.1.3.5
ASM-90122	Make push notification call, with/without mobile network and verify the behavior.	Client will get an incoming call alert, but when answered it gets dropped.	8.1.3.6
ASM-89836	Multiple 8.1.3.x ASMs managed by SMGR.	Cassandra repair failure under data storage	8.1.3.5

Fixes in Session Manager Release 10.1.0.2

ID	Minimum Conditions	Visible symptoms	Issue found in Release
ASM-89630	An endpoint with 100 calls in call history.	New call history is not updated on the endpoint	10.1.0.1
ASM-89287	SIP traces are enabled using SMGR	Need to generate a Warning Alarm when SIP Traces are enabled	8.1.3.4
ASM-89140	Cal transfer from AAfD	Call transfer from AAfD fails	8.1.3.1
ASM-89053	Aura Solution with more than 6 SMs	Cassandra DB repair fails	8.1.3.3
ASM-88226	System Manager signed certificates issued more than 2 years ago	Session Manager entity links go down after a reboot	8.1.3.3
ASM-87889	Push Notification feature enabled and Proxy between SM and PNP server	Push notification request fail and SM restarts	8.1.3.5
ASM-88806	An automatic ID certificate renewal or a manual replacement of certificates at least one time	WebSphere ID certificates are not getting modified	8.1.3.4
ASM-89370	SM 10.1.0.1 installed with Security Service Pack #4	User Data Storage Repair fails	8.1.3.5
ASM-89643	Incorrect ownership of Cassandra cofig file	Cassandra fails to come up	8.1.3.5
ASM-88830	Remote Syslog configured with UDP Transport Protocol	Remote Syslog fails	10.1.0.1
ASM-88856	Large setup with 200+ BSMs and 20+ SMs	Longer time taken by SMGR to sync CM ad to update user	8.1.3.0

Fixes in Session Manager Release 10.1.0.1

ID	Minimum Conditions	Visible symptoms	Issue found in Release
ASM-85473	Special characters in Data Center names	Cassandra database replication failures	8.1.3.1
ASM-85734	A Session Manager that was in-service is decommissioned (shutdown and removed from the Session Manager administration page on System Manager).	The output from the listSMInfo.sh utility when run on another Session Manager will still display the information for the Session Manger that was decommissioned.	8.1.3.1
ASM-86795	Null data in Cassandra keyspace	System Manager User Registration page missing device data	8.1.1.0
ASM-87297	Dummy Communication Manager entries in database	Dummy entries show up in list of available Communication Managers when they should be filtered	8.1.3.0
ASM-87751	Rare occurrence of Cassandra database corruption after upgrade	The Session Manager Status page on System Manager will have a failed User Data Storage Status for the upgraded Session Manager.	8.1.3.3
ASM-87988	CS1000 adapter administered for SIP Entity.	Adapted History-Info header is missing the 302 Redirection Reason header present in the	8.1.3.3

ID	Minimum Conditions	Visible symptoms	Issue found in Release
		inbound header. User reaches the system and not mailbox.	

Fixes in Session Manager Release 10.1

ID	Minimum Conditions	Visible symptoms	Issue found in Release
N/A			

Known issues and workarounds in Session Manager 10.1.x.x

Known issues and workarounds in Session Manager Release 10.1.3.2

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

ID	Minimum conditions	Visible symptoms	Workaround
ASM-92664	Apply custom Security policy	Custom security policy settings are not effective	Use change utility to set the password aging parameters.
ASM-92590	Multiple overlapping dial plan entries	Unable to dial higher matching numbers if lower matching overlapping dial plans are matched	Remove overlapping dial plans
ASM-91096	Import the xml file containing adaptation information	The import doesn't validate improper entries	Modify the XML files and correct the improper entries.
ASM-89853	ASM 8.1.3.2 installed	Unconfined daemons are found on the host.	No Workaround
ASM-89829	ASM 8.1.3.5 installed	The logfile asm.log is flooded with logs related SMConsoleListner	No Workaround
ASM-89128	Perform Routing Web Service operations	Improper response to a request with invalid parameter	Modify the Routing Web Service with correct parameter
ASM-88725	DigitConversionAdapter adaptations are applied to a SIP Entity	IP addresses are not getting replaced with the domain name as part of the DigitConversionAdapter adaptations	No Workaround
ASM-87752	NFS partition (remote datastore) is used for ASM performance data	NFS partition did not automatically get remounted after SMGR reboot	Manually mount the NFS partition

ID	Minimum conditions	Visible symptoms	Workaround
ASM-87031	Multiple ASMs with User Registrations	User Registrations Screen on Session Manager System Status throws error related to connections	No Workaround
ASM-81511	ASM configured with CRL.	A M is not accepting certificate if CRL is different (with same Issuer) in renewed Cert	Set the CRL validation from BEST_EFFORT to NONE on the SMGR.

Known issues and workarounds in Session Manager Release 10.1.3.1

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

ID	Minimum conditions	Visible symptoms	Workaround
ASM-91780	SM management interface configured with FQDN	User data storage Audit fails.	No Workaround
ASM-91779	SSH to SM IPv6 management IP	SSH session fails to connect.	Restart sshd service with below command “service sshd restart”
ASM-91698	Add or modify or delete SIP stations or altering any parameters under SM or CM communication profile under user.	Refer to PSN020605u.	Refer to PSN020605u
ASM-91096	Import the xml file containing adaptation information	The import doesn’t validate improper entries	Modify the XML files and correct the improper entries.
ASM-89853	ASM 8.1.3.2 installed	Unconfined daemons are found on the host.	No Workaround
ASM-89835	SIP Stations registered to ASM 10.1.0.2	Intermittently, The Device information is not displayed under user registrations screen	No Workaround
ASM-89829	ASM 8.1.3.5 installed	The logfile asm.log is flooded with logs related SMConsoleListner	No Workaround
ASM-89128	Perform Routing Web Service operations	Improper response to a request with invalid parameter	Modify the Routing Web Service with correct parameter
ASM-88725	DigitConversionAdapter adaptations are applied to a SIP Entity	IP addresses are not getting replaced with the domain name as part of the DigitConversionAdapter adaptations	No Workaround

ID	Minimum conditions	Visible symptoms	Workaround
ASM-87752	NFS partition (remote datastore) is used for ASM performance data	NFS partition did not automatically get remounted after SMGR reboot	Manually mount the NFS partition
ASM-87031	Multiple ASMs with User Registrations	User Registrations Screen on Session Manager System Status throws error related to connections	No Workaround
ASM-81511	ASM configured with CRL.	A M is not accepting certificate if CRL is different (with same Issuer) in renewed Cert	Set the CRL validation from BEST_EFFORT to NONE on the SMGR.

Known issues and workarounds in Session Manager Release 10.1.3.0

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

ID	Minimum conditions	Visible symptoms	Workaround
ASM-91096	Import the xml file containing adaptation information	The import doesn't validate improper entries	Modify the XML files and correct the improper entries.
ASM-90996	ASM with 3rd Party CA certificate and run initTM command	initTM command fails	No Workaround
ASM-90995	Run traceSM on 10.1.x ASM	SIP Entity names are not displayed in the column headings	No Workaround
ASM-90986	Install/upgrade to ASM 10.1.x	Continuous flood of ALARM-SYNFLOOD and ALARM-ICMPFLOOD	No Workaround
ASM-90826	Upgrade ASM from 10.1.0.2 to 10.1.2	In rare cases, upgrade from 10.1.0.2 to 10.1.2 fails	No Workaround
ASM-90716	Dial the number with the special character in it – copy and paste the number in the client	PPM Operation getCallHistory fails	Make sure there no special characters in the dialed number
ASM-90005	SMGR on 10.1.0.1/2 and ASM on 8.1.3.x and try to enable Push Notification Proxy server settings	Improper error messages thrown	Upgrade all the SMs to 10.1.x
ASM-89853	ASM 8.1.3.2 installed	Unconfined daemons are found on the host.	No Workaround
ASM-89835	SIP Stations registered to ASM 10.1.0.2	Intermittently, The Device information is not displayed under user registrations screen	No Workaround
ASM-89829	ASM 8.1.3.5 installed	The logfile asm.log is flooded with logs related SMConsoleListner	No Workaround

ID	Minimum conditions	Visible symptoms	Workaround
ASM-89128	Perform Routing Web Service operations	Improper response to a request with invalid parameter	Modify the Routing Web Service with correct parameter
ASM-88725	DigitConversionAdapter adaptations are applied to a SIP Entity	IP addresses are not getting replaced with the domain name as part of the DigitConversionAdapter adaptations	No Workaround
ASM-87752	NFS partition (remote datastore) is used for ASM performance data	NFS partition did not automatically get remounted after SMGR reboot	Manually mount the NFS partition
ASM-87031	Multiple ASMs with User Registrations	User Registrations Screen on Session Manager System Status throws error related to connections	No Workaround
ASM-81511	ASM configured with CRL.	A M is not accepting certificate if CRL is different (with same Issuer) in renewed Cert	Set the CRL validation from BEST_EFFORT to NONE on the SMGR.

Known issues and workarounds in Session Manager Release 10.1.2.0

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

ID	Minimum conditions	Visible symptoms	Workaround
ASM-90445	SM 10.1.0.1 and above installed	When parsing SIP messages containing bad/garbage characters, CPU resources are not released, thus causing CPU usage to continue to increase.	Restart SM. For information, see PSN020588u - Avaya Aura® Session Manager CPU usage increase may result in severe failures.
ASM-90405	APN provider/application administered	Push Notification failure when more than one thread is attempting to send push and time to re-create the HTTP client has occurred.	No Workaround
ASM-90446	SMGR 10.1 and above installed	Duplicate User operation with UPR fails	Create user without duplication or without UPR
ASM-90251	DRS Initial Load happens when the SM is under load	SM generated Java Core and Heap dump.	Restart SM

ID	Minimum conditions	Visible symptoms	Workaround
ASM-90013	Stations are monitored by AES and CM SIP Reachability Feature is disabled	SM sends incorrect status upon station un-registration	No Workaround.
ASM-89925	SM 8.1.3.5 and 10.1 and above installed	Too many log statements in mgmt.log	No Workaround.
ASM-89835	Devices/ clients registered and subscribed to SM	The device /client information is not displayed properly	No Workaround.
ASM-89637	Add users using UPR when “Enable Policy Based Assignment of Session Managers" from Global settings is enabled	Add user operation fails with error on the UI	Add users without UPR

Known issues and workarounds in Session Manager Release 10.1.0.2

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

ID	Minimum conditions	Visible symptoms	Workaround
ASM-89637	Add users using UPR when “Enable Policy Based Assignment of Session Managers" from Global settings is enabled	Add user operation fails with error on the UI	Add users without UPR
ASM-88839	Aura Solution with Session Manager	Security Module goes down.	Reboot SM.
ASM-89751	Push Notification requests timeout	traceSM crashes while opening pushnotification.log file	No Workaround.
ASM-89731	Large number Push Notification requests per day in an impaired network	SM Restarts	No Workaround
ASM-89570	Push Notification feature enabled	traceSM not capturing Push Notification messages	No Workaround
ASM-89347	Push Notification requests timeout	Not enough details in log file	No Workaround
ASM-88656	ASM 10.1 installed	Audit partition reaching 75%	Run setSecurityPolicy command and set the mode to Standard.
ASM-88647	Serviceability command executed to get system dump	The serviceability command fails to execute	No Workaround
ASM-89565	Push Notification feature enabled and the stations are monitored by AES.	Not able to answer the call using CTI Application	No Workaround

Known issues and workarounds in Session Manager Release 10.1.0.1

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

ID	Minimum conditions	Visible symptoms	Workaround
ASM-87637	Session Manager Communication Profile Editor page	Communication Profile Editor page show incorrect format at first time access	Click Communication Profile Editor link again to reload the page
ASM-89747	Access Push Notification Activations menu under Session Manager > System Status	Error displayed on the screen	NA
ASM-87752	NFS data store enabled for storing the performance data	Perf data page hung.	NA

Known issues and workarounds in Session Manager Release 10.1

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

ID	Minimum conditions	Visible symptoms	Workaround
ASM-87541	SW only installation on Azure cloud	The swversion command is showing extraneous hardware_info errors.	None. Errors can be ignored
ASM-87637	Session Manager Communication Profile Editor page	Communication Profile Editor page show incorrect format at first time access	Click Communication Profile Editor link again to reload the page
ASM-87604	Deletion of Session Manager from system configuration.	Stale Cassandra entries may be seen in the listSMinfo command.	None. Errors can be ignored.

Avaya Aura® System Manager

What's new in System Manager Release 10.1.3.2

Supported Browsers - Chrome (minimum version 117.0), Edge (minimum version 117.0) and Firefox (minimum version 118.0). Earlier versions are no longer supported.

What's new in System Manager Release 10.1.3.1

- From Release 10.1.3.1, Change in report execution workflow is done so If present, then remove old report definitions associated with commands "list measurements announcement all last-hour", "list trunk-group", "list aar analysis" and "list ars analysis" then re-create new report definitions associated with those commands to get correct data in reports.
- From Release 10.1.3.1, "Updated Time" attribute added in User Identity section to provide information on time when the user details were last modified.
  Note – This attribute is not present in 8.x, 10.1.0.0, 10.1.0.1, 10.1.0.2, 10.1.3.0 releases, re-introduced in 10.1.3.1 and higher release.

IMPORTANT NOTE: Starting 10.1.3.1, licensing for Communication Manager (CM) and Application Enablement Services (AES) will only work with 10.1.3.1 and higher version of System Manager (SMGR) or Standalone WebLM (WebLM). If upgrading CM and/or AES to 10.1.3.1 and higher then the required order of upgrade is imperative i.e. SMGR and/or WebLM should be upgraded to 10.1.3.1 and higher first to ensure licensing for CM and/or AES does not stop working. CM and AES 10.1.3.0 were originally compatible with Standalone WebLM 10.1.2.0 (as there was no Standalone WebLM 10.1.3.0), however beginning with 10.1.3.1 and higher, Standalone WebLM 10.1.3.1 and higher is required for CM and AES. The Avaya Aura® System Manager release/version must always be greater than or equal to the release/version of the components of the solution (Session Manager, Communication Manager, Application Enablement Services).

What's new in System Manager Release 10.1.2.0

- From Release 10.1.2.0, System Manager Solution Deployment Manager and Solution Deployment Manager Client support the deployment and upgrade of application using the OVA with the SHA256 hash algorithm.
- System Manger 10.1 OVAs are re-spun to support SHA256 algorithm. For more information, see the Required artifacts section.
- The old 10.1 GA OVA contains the Avaya Signing certificate that is going to expire on Feb 20, 2023. Therefore, to address the Avaya signing certificate expiry, the new 10.1 GA OVAs are renewed and re-signed with the latest Avaya signed certificates. For more information, see PSN020586u - Avaya Aura® OVA Certificate Expiry February 2023.

For more information, see What's New in Avaya Aura® Release 10.1.x document on the Avaya Support site: https://downloads.avaya.com/css/P8/documents/101078425

What's new in System Manager Release 10.1.0.2

From Release 10.1.0.2, logging framework 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://downloads.avaya.com/css/P8/documents/101078425

What’s new in System Manager Release 10.1.0.1

Corrections to Military Grade hardening

- If Military Grade hardening is applied on SP1 and later Patch, security policy profile harden will be applied.
- If Military Grade hardening is applied on 10.1 SMGR before applying SP1 Patch, the security policy profile will be standard. After applying SP1 patch the profile will remain same.

What’s new in System Manager Release 10.1

With this release 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 System Manager (SMGR).

CRITICAL: The Security Service Pack installation framework for SMGR has changed in Release 10.1.x.
It is imperative that the instructions in PCN2138S be reviewed for complete steps prior to installation of Security Service Packs on an SMGR 10.1.x system.
The old method of installing Security Service Packs will not work in Release 10.1.
The minimum release of SMGR 10.1.x.x that you must be on in order to install the Security Service Packs for SMGR is 10.1.0.1.
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 10.1.x Security Service Packs (SSPs).
In order to install the SSP for SMGR 10.1.x.x, you must use the new command ("av-update-os") and follow the detailed instructions in PCN2138S.

NOTE: For April 2022, there is no separate Security Service Pack binary. The April 2022 Security Service Pack is embedded in the SMGR Service Pack 1 and will be installed automatically when you install Service Pack 1.

For more information, see ***What’s New in Avaya Aura® Release 10.1.x*** document on the Avaya Support site: https://downloads.avaya.com/css/P8/documents/101078425

Future use fields visible in Avaya Aura® System Manager Release 10.1.x.x

Future use fields visible in Avaya Aura® System Manager Release 10.1

The underlying framework for an upcoming Avaya Aura® Platform enhancement “Avaya Aura Distributed Architecture” will be seen in Release 10.1 administration screens. The “Avaya Aura Distributed Architecture” changes are applicable to Communication Manager, System Manager, and Session Manager. The following fields that will be visible in System Manager Release 10.1.x are for future use only.

1. The ‘Elements > Communication Manager > Cluster Management’ page and all the screens and options on this page.
2. On ‘Services > Inventory > Manage Elements’ page, during New/Edit of the Communication Manger element type, the CM Type field has an additional option of ‘Node’ which is for future use.
3. On ‘Services -> Inventory -> Manage Elements’ page, during a New/Edit of the Communication Manager Element type, it has additional ‘Alias Ipv4 Address’ and ‘Alias Ipv6 Address’ fields for future use.

Security Service Pack

Security Service Pack

For further information on SSP contents and installation procedures for SMGR 10.1.x, please see **PCN2138S**.

With this release 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 Communication Manager and Application Enablement Services.

CRITICAL: The Security Service Pack installation framework for SMGR has changed in Release 10.1.x.
It is imperative that the instructions in PCN2138S be reviewed for complete steps prior to installation of Security Service Packs on an SMGR 10.1.x system.
The old method of installing Security Service Packs will not work in Release 10.1.
The minimum release of SMGR 10.1.x.x that you must be on in order to install the Security Service Packs for SMGR is 10.1.0.1.
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 10.1.x Security Service Packs (SSPs).

In order to install the SSP for SMGR 10.1.x.x, you must use the new command ("av-update-os") and follow the detailed instructions in PCN2138S.
NOTE: For April 2022, there is no separate Security Service Pack binary. The April 2022 Security Service Pack is embedded in the SMGR Service Pack 1 and will be installed automatically when you install Service Pack 1.

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

Managing ASP using SDM in 10.1.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 displays 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 10.1.x.x

Required artifacts for System Manager Release 10.1.3.2

Filename	PLDS ID	File size (MB)	S/W Version number	MD5 Check Sum	Comments
System_Manager_10.1.3.2_r1013216669.bin	SMGR10132GA1	2211.84	10.1.3.2.1013216669	227cff125af6ebde5e1ddfd4f40d9396	SMGR 10.1.3.2 GA bin
Avaya_SDMClient_win64_10.1.3.2.0039703_8.zip	SMGR10132GA2	264	10.1.3.2.0039703_8	9d4af0c8b918012e94c5333743abfc65	SDM Client for System Manager 10.1.3.2. For more details on SDM client fixes, see the “Fixes in System Manager 10.1.3.2” section.
datamigration-10.1.0.0.5-23.bin	SMGR10132GA3	34.7	10.1.0.0.5-23	92d768d2f861661f0f352f4be6987d77	Data Migration utility for System Manager 10.1.X. For more details on Data Migration Utility fixes, see the “Fixes in System Manager 10.1.3.2” section.

Required artifacts for System Manager Release 10.1.3.1

Filename	PLDS ID	File size (MB)	S/W Version number	MD5 Check Sum	Comments
System_Manager_10.1.3.1_r1013116149.bin	SMGR10131GA1	2092	10.1.3.1.1013116149	1f0f921b6689202920757f3cd4c74a14	SMGR 10.1.3.1 GA bin
Avaya_SDMClient_win64_10.1.3.1.0039462_6.zip	SMGR10131GA2	265	10.1.3.1.0039462_6	c22b3ce4ab9576d749ab10842c18a19f	SDM Client for System Manager 10.1.3.1. For more details on SDM client fixes, see the “Fixes in System Manager 10.1.3.1” section.

Filename	PLDS ID	File size (MB)	S/W Version number	MD5 Check Sum	Comments
datamigration-10.1.0.0.5-20.bin	SMGR10131GA3	35	10.1.0.0.5-20	c1b3d70832b4032f5649ca7e58e066d6	Data Migration utility for System Manager 10.1.X. For more details on Data Migration Utility fixes, see the "Fixes in System Manager 10.1.3.1" section.

IMPORTANT NOTE: Starting 10.1.3.1, licensing for Communication Manager (CM) and Application Enablement Services (AES) will only work with 10.1.3.1 and higher version of System Manager (SMGR) or Standalone WebLM (WebLM). If upgrading CM and/or AES to 10.1.3.1 and higher then the required order of upgrade is imperative i.e. SMGR and/or WebLM should be upgraded to 10.1.3.1 and higher first to ensure licensing for CM and/or AES does not stop working. CM and AES 10.1.3.0 were originally compatible with Standalone WebLM 10.1.2.0 (as there was no Standalone WebLM 10.1.3.0), however beginning with 10.1.3.1 and higher, Standalone WebLM 10.1.3.1 and higher is required for CM and AES. 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).

Required artifacts for System Manager Release 10.1.3.0

Filename	PLDS ID	File size (MB)	S/W Version number	MD5 Check Sum	Comments
System_Manager_10.1.3.0_r1013015713.bin	SMGR1013GA1	1772	10.1.3.0.1013015713	04a49e112a928e72c181ca4b2d18efde	SMGR 10.1.3.0 GA bin
Avaya_SDMClient_win64_10.1.3.0.0039294_10.zip	SMGR1013GA2	264	10.1.3.0.0039294-10	32fe8df4ee5643d19064fe3b95234704	SDM Client for System Manager 10.1.3.0. For more details on SDM client fixes, see the "Fixes in System Manager 10.1.3.0" section.

Filename	PLDS ID	File size (MB)	S/W Version number	MD5 Check Sum	Comments
datamigration-10.1.0.0.5-19.bin	SMGR1013GA3	34.7	10.1.0.0.5-19	b2dc687f8796389ef9efe44300538aaa	Data Migration utility for System Manager 10.1.X. For more details on Data Migration Utility fixes, see the "Fixes in System Manager 10.1.3.0" section.

Required artifacts for System Manager Release 10.1.2.0

Artifact	PLDS Download ID	File size (MB)	Notes/Comments
SMGR 10.1.2.0 GA Bin	SMGR1012GA1	1772	System_Manager_R10.1.2.0_r1012015476.bin Md5sum : dc962d049c7dd428136c148730e55fbd
SDM Client for System Manager 10.1.2.0	SMGR1012GA2	264	Avaya_SDMClient_win64_10.1.2.0.0039191_17.zip Md5sum : 28b018fe912a447c9d95c07939e21f77
Data Migration utility for System Manager 10.1.X	SMGR1012GA3	34.7	datamigration-10.1.0.0.5-15.bin Md5sum : 6c0ae907896a2dc3ed3be3f61455e87e

Required artifacts for System Manager Release 10.1.0.2

Artifact	PLDS Download ID	File size (MB)	Notes/Comments
SMGR 10.1.0.2 GA Bin	SMGR10102GA1	1733 MB	System_Manager_10.1.0.2_r1010215038.bin Md5sum : 8a5b1ef4349bc2e0e37169ea263a3cde
SMGR 10.1.0.2 HF1	SMGR10102HF1	251 MB	System_Manager_R10.1.0.2_HotFix1_1010215160.bin

Artifact	PLDS Download ID	File size (MB)	Notes/Comments
			Md5sum:181e619e9c9a7b5fc7a3fe1093dc865f
SDM Client for System Manager 10.1.0.2	SMGR10102GA2	263 MB	Avaya_SDMClient_win64_10.1.0.2.0038603_19.zip Md5sum : a6725893ce6c403683e847032ffc348f

Required artifacts for System Manager Release 10.1.0.1

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.

Artifact	PLDS Download ID	File size (MB)	Notes/Comments
System Manager 10.1.0.1 Release	SMGR10101GA1	1,213	System Manager 10.1.0.1 Software. This software can be installed on top of System Manager 10.1.0.0 release. File Name: System_Manager_10.1.0.1_r1010114394.bin Md5sum:2f1a65a82c049774f5e0290369021334
SDM Client for System Manager 10.1.0.1	SMGR10101GA2	232	Solution Deployment Manager Client tool that can be installed on your Windows desktop / laptop and then used for deploying the Avaya Aura 10.1.X application OVAs on the Avaya Solutions Platform 130 environment or VMware environment. File Name:Avaya_SDMClient_win64_10.1.0.1.0037958_16.zip MD5sum:b73c583a4fc50f47549b5a3203103385
Data Migration utility for System Manager 10.1.X	SMGR10101GA3	35	Avaya Aura System Manager 10.1.X data migration utility. For instructions on how to use the data migration utility please see the Avaya Aura System Manager upgrade documents available on the Avaya Support site. File Name: datamigration-10.1.0.0.5-12.bin Md5sum: c9d3b66985b0d3d5495d0a9a4f9ddd63

Required artifacts for System Manager Release 10.1

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.

Artifact	PLDS Download ID	File size (MB/GB)	Notes/Comments
Avaya Aura® System Manager 10.1 (Profile 2) OVA	SMGR101GA01	4.4GB	Verify that the md5sum for the downloaded OVA image matches the number on the Avaya PLDS website. SMGR-10.1.0.0.537353-e70-21E-01.ova Md5sum : 815f07578a5d59324e7da0e7d5172719
Avaya Aura® System Manager 10.1 High Capacity (Profile 3) OVA	SMGR101GA02	4.5GB	Verify that the md5sum for the downloaded OVA image matches the number on the Avaya PLDS website. SMGR-PROFILE3-10.1.0.0.537353-e70-21E-01.ova Md5sum : bd8a3ecfa1b32200dd9010d89b658911
Avaya Aura® System Manager 10.1 High Capacity (Profile 4) OVA	SMGR101GA03	4.6GB	Verify that the md5sum for the downloaded OVA image matches the number on the Avaya PLDS website. SMGR-PROFILE4-10.1.0.0.537353-e70-21E-01.ova Md5sum : 8e88e75f4879e1d4f4b2d60d20202b85
~~Avaya Aura® System Manager 10.1~~ ~~(Profile 2) OVA~~	~~SMGR101GA01~~	~~4.4GB~~	~~Verify that the md5sum for the downloaded OVA image matches the number on the Avaya PLDS website.~~ ~~SMGR-10.1.0.0.537353-e70-21E.ova~~ ~~Md5sum : 6deee1669c71814249826cf45f1f8391~~
~~Avaya Aura® System Manager 10.1 High Capacity (Profile 3) OVA~~	~~SMGR101GA02~~	~~4.5GB~~	~~Verify that the md5sum for the downloaded OVA image matches the number on the Avaya PLDS website.~~ ~~SMGR-PROFILE3-10.1.0.0.537353-e70-21E.ova~~ ~~Md5sum : b4f330b92d9278292172acb67bf0565f~~
~~Avaya Aura® System Manager 10.1 High Capacity (Profile 4) OVA~~	~~SMGR101GA03~~	~~4.6GB~~	~~Verify that the md5sum for the downloaded OVA image matches the number on the Avaya PLDS website.~~ ~~SMGR-PROFILE4-10.1.0.0.537353-e70-21E.ova~~ ~~Md5sum : ae5986a5509c475066bb307ddf9c03ab~~
~~Avaya Aura® System Manager 10.1 Software Only ISO**~~	~~SMGR101GA04~~	~~3.7GB~~	~~Verify that the md5sum for the downloaded OVA image matches the number on the Avaya PLDS website.~~ ~~AvayaAuraSystemManager-10.1.0.0.537353_v21.iso~~ ~~Md5sum : bdd8755f847f79d724ff97c48137c885~~
Avaya Aura® System Manager 10.1 Software Only ISO**	SMGR101GA12	3.8GB	Verify that the md5sum for the downloaded OVA image matches the number on the Avaya PLDS website. AvayaAuraSystemManager-10.1.0.0.537353_v21_15June2022.iso Md5sum : 1f4418de253f2ed68dd3685c39c199a4

Artifact	PLDS Download ID	File size (MB/GB)	Notes/Comments
Avaya Aura® System Manager 10.1 Patch bin file Post OVA deployment / Data Migration	SMGR101GA05	954MB	Verify that the md5sum for the downloaded OVA image matches the number on the Avaya PLDS website. `System_Manager_10.1.0.0_GA_Patch1_r101013949.bin` Md5sum : `c2a02d375908840d4e2b045ffa6e20b5`
Avaya Aura® SDM client for System Manager 10.1	SMGR101GA06	231MB	Verify that the md5sum for the downloaded OVA image matches the number on the Avaya PLDS website. Avaya_SDMClient_win64_10.1.0.0.0637498_40.zip Md5sum: d37fab4e8d033d9cb0e7025db77642db

Note: ** Updated Avaya Aura® System Manager 10.1 Software Only installer ISO. The System Manager 10.1 Software only ISO is re-released on June 15, 2022 to fix certain installation related issues. If you already installed System Manager 10.1 using the previous ISO then no action is required. You can continue with the setup. For customers who want to install System Manager 10.1 Software only, use this new ISO going forward. The previous ISO is removed. If you have any local copies, please discard them. Use this new ISO to install System Manager on a customer provided Red Hat linux operating system. For more information, see PCN2137S.

Note: The old 10.1 GA OVA contains the Avaya Signing certificate that is going to expire on Feb 20, 2023. Therefore, to address the Avaya signing certificate expiry, the new 10.1 GA OVAs are renewed and re-signed with the latest Avaya signed certificates. The new OVAs are also updated to support SHA256 hash algorithm. For more information, see PCN2137S.

For more information, see PSN020586u - Avaya Aura® OVA Certificate Expiry February 2023.

Required patches for System Manager Release 10.1.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 10.1. 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 10.1 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, and 8.x. Ensure that you run the data migration utility only on 10.1 release. For more information, see the Upgrading Avaya Aura® System Manager to Release 10.1.x document.

Artifact	PLDS Download ID	File size (MB)	Notes/Comments
Data Migration utility for System Manager 10.1.X	SMGR10132GA3	34.7	**File Name:** datamigration-10.1.0.0.5-23.bin **MD5:** 92d768d2f861661f0f352f4be6987d77
~~Data Migration utility for System Manager 10.1.X~~	~~SMGR10131GA3~~	~~35~~	~~**File Name:** datamigration-10.1.0.0.5-20.bin~~ ~~**MD5:** c1b3d70832b4032f5649ca7e58e066d6~~
~~Data Migration utility for System Manager 10.1.X~~	~~SMGR1012GA3~~	~~34.7~~	~~datamigration-10.1.0.0.5-15.bin~~ ~~Md5sum : 6c0ae907896a2dc3ed3be3f61455e87e~~
~~Avaya Aura® Data Migration utility for System Manager 10.1~~	~~SMGR101GA07~~	~~7.6MB~~	~~Verify that the md5sum for the downloaded OVA image matches the number on the Avaya PLDS website~~ ~~datamigration-10.1.0.0.5-13.bin~~ ~~Md5sum: 5e5d7d98c53ef80300600927619f22d7~~

Must read

1. 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.
2. If System Manager is upgraded to Release 10.1.3 and AADS is on Release 10.1.1.X or earlier, Data replication fails between System Manager and AADS. For more information, see PSN006192u.
3. 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.

4. For Release 10.1 GA Installation:
   - Fresh: Deploy 10.1 GA OVA + Apply 10.1 GA Patch bin.
   - Upgrade: Deploy 10.1 GA OVA + 10.1 Data Migration Bin + 10.1 GA Patch bin.

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

5. 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`.

6. Perform the following steps to enable EASG on System Manager 10.1:
   - To enable EASG on System Manager via Command Line Interface via Cust user type the following command:
     `# EASGManage --enableEASG`
   - To disable the EASG on System Manager type the following command:
     `# EASGManage –disableEASG`

7. For VMware to VE System Manager Upgrade, remove all the snapshots from old VMware System Manager; otherwise, rollback operation will fail.
8. 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.
9. Breeze Element Manager in System Manager 10.1 is called Breeze 3.8.1.0
10. 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.
11. 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.
12. 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.
13. Release 10.1.2.0, System Manager Solution Deployment Manager does not support the installation of the Communication Manager 10.1.x Security Service Packs (SSPs). Please refer PCN2134S for more details.
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.

Software	Version	Note
Open JDK	1.8 update 342 64 bit	For Solution Deployment Manager Client, Open JDK 1.8.0-java-1.8.0-openjdk-1.8.0.342
Application Server	WildFly AS 26.1.0 Final	
Supported Browsers	Chrome (minimum version 91.0)	Earlier versions of Chrome are not supported
	Edge (minimum version 93.0)	Earlier versions of Edge are not supported
	Firefox (minimum version 93.0)	Earlier versions of Firefox are no longer supported.
VMware vCenter Server, ESXi Host	6.7, 7.0.X	Earlier versions of VMware are no longer supported.
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 10.1.x.x

Backing up the software

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

Installing the System Manager software

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

Upgrading the System Manager software

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

Note: If System Manager is upgraded to Release 10.1.3 and AADS is on Release 10.1.1.X or earlier, Data replication fails between System Manager and AADS. For more information, see PSN006192u.

System Manager upgrade path

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

The following upgrade paths are currently supported.

System Manager running this version	Can upgrade to this version
7.0.X	10.1 or 10.1.2.0
7.1.X	10.1 or 10.1.2.0
8.0.X	10.1 or 10.1.2.0
8.1.3.1	10.1 or 10.1.2.0
8.1.3.2	10.1 or 10.1.2.0
8.1.3.3	10.1 or 10.1.2.0
8.1.3.4	10.1 or 10.1.2.0
8.1.3.5	10.1.0.2 or 10.1.2.0
8.1.3.6	10.1.0.2 HF or 10.1.2.0
8.1.3.7	10.1.2.0 and Higher
8.1.3.8	10.1.3.0 and Higher

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 10.1.x.x

Fixes in System Manager 10.1.3.2

ID	Minimum conditions	Visible symptoms	Issue found in Release

SMGR-73306	User Interface	Cannot add shortcuts for users with username more than 30 characters	10.1.2.0
SMGR-73410	Upgrade Management	Block Data Migration utility if Post Installation is not yet completed	10.1.0.0
SMGR-73876	OfficeLinx	Officelinx Mailbox # is getting created without leading zeros	10.1.3.0
SMGR-73729	Installation	Unable to upgrade from 10.1.0.1 or 10.1.2 to 10.1.3 on secondary SMGR	10.1.0.1
SMGR-59603	Installation	Abort patch installation if Environment Variables are not set properly	10.1.3.0
SMGR-73293	Infrastructure	HTTP response from the server reveals information about the type and version of the server	10.1.0.0
SMGR-73358	Infrastructure	ecdsa and ed25529 keys in SMGR are not unique across OVA deployments	10.1.0.0
SMGR-74211	Infrastructure	Remove http-connector from activemq subsystem within System Manager	10.1.0.0
SMGR-73624	Infrastructure	Set JBoss Server log level to ERROR mode	10.1.0.0, 10.1.3.1.0
SMGR-74264	Infrastructure	Software Only Deployments- Users With Blank Password", modification in /etc/shadow file is required	10.1.3.0
SMGR-73696	Inventory Management	SBCE Element is missing from RTS when upgrade of SMGR from 7.1.x to 10.1.x	10.1.0.1
SMGR-71632	Upgrade Management	Patch installation status shows failed sometime on SDM UI - Intermediate issue	10.1.2.0
SMGR-74260	Upgrade Management	SDM SUM Release status column shows "Ready for Upgrade" status even if they are upgraded to latest load	10.1.3.1.0
SMGR-73298	Upgrade Management	Remove sdm.iso file from vm datastore after successful vm operation.	10.1.3.0
SMGR-73788	Fault Management	Quantum Logs not updating when user is password reset, login Disable and enable	10.1.3.0
SMGR-73261	User Management	User cannot be edited if SIP handle and Presence handle are same and they have domain name in mixed case	10.1.3.0
SMGR-73836	User Management	Selfprovisioning login not possible anymore through reverse proxy	10.1.3.0
SMGR-73752	User Management	Duplicate User from User management not copying the feature buttons on new stations	10.1.3.0
SMGR-73397	User Management	Can't edit profile users with error: "Invalid content was found starting with element 'userUpdateDateTime'. One of 'isPublic} is expected. "	10.1.3.1
SMGR-74255	User Management	Unable to permanently delete user if user added with user preference, then System Manager upgrade from 7.1.x to the latest releases.	10.1.0.0

SMGR-74409	Communication Manager Management	“Turn on mute for remote off hook attempt" and few more fields missing from 10.1 Endpoint template fields	10.1.3.0
SMGR-72212	Communication Manager Management	Display alarms report: Cannot deselect "Warning" effectively when report generated for multiple CM.	10.1.3.0
SMGR-74387	Communication Manager Management	Help link not available for CM from Inventory	10.1.3.1
SMGR-73968	Communication Manager Management	CMs cannot be synched, cut through stops working and few Basic reports stop working after SMGR IP changed with “changeIPFQDN” command	10.1.3.0
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-73286	Infrastructure	Unable to configure account lockout policy settings using setSecurityPolicy utility.	10.1.3.1

Fixes in System Manager 10.1.3.1

ID	Minimum conditions	Visible symptoms	Issue found in Release
SMGR-73232	Upgrade Management	WebLM refresh is not working in SMGR -SDM Upgrade/update	10.1.2.0
SMGR-73102	User Management	Reset commPassword does not work for user which has 2 handles of same name.	10.1.2.0
SMGR-73087	Tenant Management	User Tenant organization level is not populated on GUI as per hierarchy during update operation	10.1.3.0
SMGR-71282	User Management	"Reset Password" button on the Self Provisioning page is broken	8.1.3.5
SMGR-72730	Fault Management	System Manager serviceability agent is missing under serviceability agents list	10.1.0.2
SMGR-73291	Configuration Management	Upgrade from 7.x to 10.1.x, SMGR: Services - Configurations - Settings - SMGR - No configurable attributes found	10.1.3.1
SMGR-73230	OfficeLinx	Empty SMGR list sent to officelinx after long idle time causing issue	8.1.3.8
SMGR-72366	Geo Redundancy	GR Health Heartbeat graph not getting displayed	8.1.3.5
SMGR-52347	Geo Redundancy	License popup warning for GEO on secondary server	7.1.3.3
SMGR-73042	User Interface	Equinox Conferencing link missing depending on upgrade scenario / fresh install	10.1.2.0
SMGR-72849	Administration	Certificate based login not working when using Microsoft UPN	10.1.2.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
SMGR-71393	Administration	After SMGR upgrade to 10.1.x, users cannot open the Role page with the Firefox. Works correctly with Chrome and Edge.	10.1.0.1
SMGR-67520	Administration	security concern on sensitive info presented by in 8.1.3.x	8.1.3.3
SMGR-72735	Solution Deployment Manager	Clear text password present inside 10.1 SDM Client vmmgmtDebugLog.log file	10.1.2.0
SMGR-72736	Solution Deployment Manager	Input json file present in SDM Client contains password attribute in clear text format	10.1.2.0
SMGR-67586	Geo Redundancy	"Primary server status: Not Reachable" notification on secondary server GUI when Extended Hostname Validation is set to true	8.1.3.4
SMGR-73055	Upgrade Management	Default 10.1 endpoint templates are missing after 8.1.3.6 to 10.1.2 upgrade.	10.1.2.0
SMGR-72567	Infrastructure	xstream jar related vulnerabilities	10.1.0.2
SMGR-71561	Infrastructure	Exposure of Sensitive Information to an Unauthorized Actor	10.1.0.0
SMGR-73270	Infrastructure	CLI Login locked after 3 wrong attempts for all cli users	10.1.2.0
SMGR-71854	Infrastructure	Resource leak happens when SAL agents trying to create the ConfigureNMSLocations and SNMP user profile have password less than 8 characters.	8.1.3.5
SMGR-73056	Upgrade Management	Cannot edit user after upgrade from 8.1.3.4 to 10.1.2	
SMGR-72190	Infrastructure	Duplicate http headers	10.1.0.1
SMGR-69748	Trust Management	CRL generation failed after changing FQDN using changeIPFQDN script due to which web interface went down after next JBoss restart.	10.1.0.1
SMGR-72790	Trust Management	Secondary Server (if in activated state more than 7 days), unable to access SMGR UI after reboot or restart.	10.1.0.2
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-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-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

ID	Minimum conditions	Visible symptoms	Issue found in Release
SMGR-72581	Communication Manager Management	After INIT sync special German characters like ö and ü disappear from the name	8.1.3.5
SMGR-73265	Communication Manager Management	Frequent NullPointerException while generating "list measurements announcement all last hour" report	10.1.0.1

Fixes in System Manager 10.1.3.0

The following table lists the fixes in this release:

ID	Minimum conditions	Visible symptoms	Issue found in Release
SMGR-72439	Software Deployment Manager, SDM Client	Cleartext password showing in SDM debug log	10.1.2.0
SMGR-71074	Alarming	Serviceability Agents do not have the correct 'System Name' or 'System OID' when the SM is administered with an FQDN	10.1.0.2
SMGR-71240	Alarming	The AVPU cannot register to SMGR such as trap receiver by using command line "/opt/avaya/common_services/Set_SMGR SMGR_IPAddress and /opt/avaya/common_services/ovf_set_spirit [SMGR_FQDN] [enrollment password]"	8.1.3.5
SMGR-71665	Alarming	In SMGR10.x MIB file, duplicate event names exist	10.1.0.2
SMGR-55507	Alarming	after upgrading SMGR from 7.1.x to 8.1.1 the log_store table is not in the avaya_system_audit_data01 table space	8.1.2.0
SMGR-68655	User Interface	Announcement broadcast: not able to select multiple announcement files.	10.1.0.1
SMGR-71816	Upgrade Management(DM Utility)	Data migration should throw correct validation message in case of IP/FQDN values mismatch with third party certificates.	10.1.0.0
SMGR-72418	Upgrade Management(DM Utility)	Data Migration fails on 10.1.x releases when different IP/FQDN is used(System Manager source and destination release IP/FQDN are different).	10.1.0.0
SMGR-61657	Documentation	CRL download failure if it contains Windows Freshest CRL extension	8.1.3.2
SMGR-67758	Documentation	Unclear documentation for Provision SAML Remote Identity Provider using xml file	8.1.3.2
SMGR-72629	Documentation	display incorrectly value default of "Authentication Protocol" field in add new SNMPv3 User Profiles form	10.1.3.0

ID	Minimum conditions	Visible symptoms	Issue found in Release
SMGR-60770	Documentation	System Resource Utilization detail improvement	8.1.3.2
SMGR-60021	Geographic Redundancy	Geo configuration is allowed although profile information is empty	8.1.3.1
SMGR-71526	Geographic Redundancy	Patch installation failure on SMGR secondary system	10.1.2.0
SMGR-71623	Geographic Redundancy	Configuration GEO redundancy is failed on SMGR 10.1.2 case firewall is down	10.1.2.0
SMGR-71638	Geographic Redundancy	Geo Configuration fails at FINALIZE CONFIGURATION Step	8.1.3.5.1
SMGR-67586	Geographic Redundancy	"Primary server status: Not Reachable" notification on secondary server GUI when Extended Hostname Validation is set to true	8.1.3.4
SMGR-52347	Geographic Redundancy	License popup warning for GEO on secondary server	7.1.3.3
SMGR-67822	Infrastructure	Vulnerability: Cookies with missing, inconsistent or contradictory properties	8.1.3.3
SMGR-71866	Infrastructure	Installation of SSP fails due to RPMs corrupted but the results show as SUCCESSFULLY INSTALLED	10.1.0.1
SMGR-72442	Infrastructure	Upgrade failed to 10.1.2 for Profile 3 & 4 customers	10.1.2.0
SMGR-71864	Infrastructure	ChangeIPFQDN using script "pairIpFqdnChange.sh" did not work	10.1.2.0
SMGR-72441	Installer	SSP Installation get skip if hot fix is installed on existing 10.1.x release	10.1.2.0
SMGR-72509	Software Deployment Manager	Clear Text password showing in SDM debug logs	10.1.2.0
SMGR-71604	Software Deployment Manager	upgrade job status is not showing under upgrade jobs status web page	10.1.2.0
SMGR-54468	Trust Management	SMGR - FIPS MODE - PEM Certificate Error	8.1.2.0
SMGR-71972	Trust Management	Minimum TLS version 1.2 not working for most of the ports	10.1.0.0, 10.1.0.1, 10.1.0.2
SMGR-72188	Trust Management	manageEntityClassWhitelist failed after SMGR upgrade from 8.1.x to 10.1.x release	10.1.0.2
SMGR-72503	Trust Management	TM Entity Class log file not generating while sending SCEP Subject Whitelisting certificate request	10.1.0.2
SMGR-71143	Administration	Cannot change FQDN by using command changeIPFQDN successfully.	10.1.0.2

ID	Minimum conditions	Visible symptoms	Issue found in Release
SMGR-71495	Administration	Administrators unable to set password more than 20 characters using change password web page	8.1.3.5
SMGR-60306	Administration	Still shows old UPM link after Migrating System Manager from 6.3.22 to 8.1,3	8.1.3.1
SMGR-71122	Administration	Custom role behaves differently compared to the role that it was exactly copied from	8.1.3.3
SMGR-70760	User management	"Export User to Excel" operation doesn't export comm profile data on 8.1.3.5	8.1.3.5
SMGR-71924	User management	Unable to assign a tenant to an existing user	10.1.0.2
SMGR-72356	User management	Cannot Duplicate user with SM Fixed policy from user Location-Region Policy	8.1.11.0
SMGR-71285	User management	no error popup shown when add new user with empty "Home Location" is required field in Session Manager Profile	10.1.0.2
SMGR-72137	License Management	Enterprise WebLM does not show license expiration date on the web interface	8.1.3.6
SMGR-72381	Communication Manager Management	Display software report fails showing "No data found"	10.1.0.2
SMGR-72363	Communication Manager Management	Multiple display reports that cannot take qualifier in SAT require a qualifier (blank character) to run	10.1.0.2
SMGR-72214	Communication Manager Management	Locations detailed: Location field wrong; reports "1" for every location	10.1.0.2
SMGR-72204	Communication Manager Management	Display multifrequency-signaling appears twice in the object list	10.1.0.2
SMGR-72200	Communication Manager Management	Group page detailed: Group extension field wrong; reports erroneous data	10.1.0.2
SMGR-72197	Communication Manager Management	ARS analysis detailed: Location field wrong; reports erroneous data for every location	10.1.0.2
SMGR-72184	Communication Manager Management	Signaling groups detailed: Far-end NR data wrong; reports erroneous data for every SG	10.1.0.2
SMGR-72182	Communication Manager Management	Dial plan parameters detailed: All N-digit Ext fields duplicated; inclusion of any duplicates causes failure	10.1.0.2
SMGR-72166	Communication Manager Management	Duplicate/non-functional detailed reports in dropdown ('trunk'; 'off-pbx-telephone')	10.1.0.2

ID	Minimum conditions	Visible symptoms	Issue found in Release
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-72126	Communication Manager Management	COR detailed: Inclusion of Work State Change Can Be Forced field causes failure	10.1.0.2
SMGR-72125	Communication Manager Management	Coverage time-of-day detailed report: No coverage path data and included details wrong	10.1.0.2
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-71726	Communication Manager Management	Missing Endpoint "site data" fields in detailed reports	10.1.0.2
SMGR-71599	Communication Manager Management	Detailed report generation for Agent fails if "Agent Template ID Name" field is selected	10.1.0.2
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-72123	Communication Manager Management	Cannot save "ISDN" trunk changes using SMGR native pages if SA8983 is enabled	10.1.0.1
SMGR-72219	Communication Manager Management	Issue with title/header while editing VDN using Global search/Khoi	10.1.0.1.1
SMGR-71601	Communication Manager Management	Issue with "Buttons per Page" value for cs1k set type CS1k-39xx	10.1.0.1
SMGR-71727	Communication Manager Management	IPTCM.EAR getting failed to deploy during data migration	10.1.0.0
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-71427	Communication Manager Management	Missing field "Attribute" in the Agent detailed reports	10.1.0.2

Fixes in System Manager 10.1.2.0

The following table lists the fixes in this release:

ID	Minimum Condition	Visible Symptoms
SMGR-71582	Software Upgrade Management	SDM client 10.1.2.0 cannot deploy SHA256 OVA file

ID	Minimum Condition	Visible Symptoms
SMGR-51045	Alarming	CPU alarms should be cleared when the condition goes away.
SMGR-71665	Alarming	In SMGR 10.x MIB file, duplicate event names exist.
SMGR-58507	Alarming	generateTestAlarm may not work when there is heavy logging on the system.
SMGR-51013	Alarming	Leading or Trailing spaces for IP-address field inside the SNMP target profile causes an error while assigning target profiles to the serviceability agent.
SMGR-71562	Software Deployment Manager	App version is not populating for SDM due to build issue
SMGR-59961	Inventory	After upgrading System manager from 7.1.3.x to 8.1.x inventory import is not working.
SMGR-69411	User Interface	Unable to select more than 500 users when Services -> Configurations -> Settings -> SMGR -> Common Console field “Max No of Records Selectable” is set to 9999
SMGR-59653	User Interface	Help link unable to display any content.
SMGR-68769	Officelinx Element Manager	System Manager should not push the Officelinx Profile user passwords (numericPassword & applicationUserPassword) unless they are specifically updated by administrator.
SMGR-70918	Geographic Redundancy	Geo Redundancy configuration failing on MUDG mode
SMGR-60021	Geographic Redundancy	Geo Redundancy configuration is allowed although profile information is empty
SMGR-70578	Geographic Redundancy	Geo Redundancy configuration failing with release 10.1.0.2
SMGR-67586	Geographic Redundancy	"Primary server status: Not Reachable" notification on secondary server GUI when Extended Hostname Validation is set to true.
SMGR-70954	Geographic Redundancy	Geo Redundancy Health status of services is not shown
SMGR-71781	Geographic Redundancy	Activation of secondary SMGR is not working
SMGR-68546	Geographic Redundancy	Geo Redundancy enable should fail instead of showing as completed.
SMGR-68715	Infrastructure	Every JBoss restart on 10.1 shows message "GeoSelectProfile: conferencing-ear-8.0.0.0.4.ear not found. It cannot be deployed" on CLI log
SMGR-66978	Infrastructure	System Manager upgrade fails if deployment have larger number of IPOffice servers.
SMGR-68545	Infrastructure	In System Manager 10.1.0.1: getSecurityprofile command is not working from non-root user on MUDG enabled SMGR.
SMGR-71314	Infrastructure	CLI users not able to switch to "root" using "su" after 10.1.0.2 installation.
SMGR-71539	Infrastructure	System Manager 10.1.0.2 installation fails in certain scenarios on Software Only Deployment.
SMGR-61725	Infrastructure	Certain commands were missing from the history file (/var/log/userShellLog.log)
SMGR-70432	Infrastructure	System Manager not sending full messages to syslog.
SMGR-70727	Infrastructure	System Manager 10.1.0.2 - Unable to login UI after configuring MUDG mode.

ID	Minimum Condition	Visible Symptoms
SMGR-68761	Infrastructure	changeIPFQDN command does not update new FQDN in database configuration file.
SMGR-50476	Infrastructure	Utility which checks for authorized keys causes 100% CPU
SMGR-69673	Infrastructure	Following weak key exchange algorithms are enabled in Licensing component - diffie-hellman-group-exchange-sha1
SMGR-71290	Backup and Restore	Backup and Restore timer not working properly resulting in Alarm is not raised even if remote Backup's have not been taken for more than 7 days.
SMGR-60412	Software Upgrade Management	The re-establish of AVPU 8.1 cannot update the information on System Manager inventory after upgrading the US 7.1.x or US 7.0 to AVPU 8.1.0.
SMGR-67926	Software Upgrade Management	Pre-stage process allows you to press Next even when mandatory field Data Store is blank.
SMGR-69059	Software Upgrade Management	The ASP SSH is enabled with the default value 300 seconds when user's add ASP 130 host or while generating the certificate by using SDM when the ASP SSH is disabled.
SMGR-70213	Software Upgrade Management	New System Manager was installed with same virtual machines name as already installed causing corruption of existing VM.
SMGR-71604	Software Upgrade Management	Upgrade job status is not showing under upgrade jobs status web page.
SMGR-70156	Software Upgrade Management	AVP refresh jobs should be marked as failed automatically if they are stuck for 5 min or so.
SMGR-68194	Software Upgrade Management	Updating VM information in Inventory failing for AVP Utilities.
SMGR-71846	Software Upgrade Management	SMGR SDM saved job cannot be located.
SMGR-71043	Software Upgrade Management	Upgrade/Update To field does not populate platform and kernel patch values during pre-upgrade check operation.
SMGR-59228	Trust Management	migrateORRegenSecureStores.sh script does not work in 8.1.x and higher releases.
SMGR-54468	Trust Management	PEM Certificate Error in System Manager FIPS mode deployment.
SMGR-67986	Scheduler	System Manager reports alarms: A scheduled job UserMgmtJob failed to execute.
SMGR-49616	User Interface	After Upgrade from 7.0.x to 8.0.x and higher release External Authentication and Policy links stop working
SMGR-56205	Infrastructure	CLI access lost after upgrade from 8.0.1.1 to 8.1.2 for custom users which were enabled through GUI.
SMGR-71143	Infrastructure	Cannot change FQDN by using utility changeIPFQDN.
SMGR-71495	Authentication	Administrators unable to set password more than 20 characters using change password web page
SMGR-70336	User Interface	When selecting a Admin Role and cancelling the operation, system logs you out.
SMGR-67620	User management	Cannot close pop-up when Delete job at Directory Synchronization on Chrome and Microsoft Edge browsers.
SMGR-69218	User management	Messaging Profile Template resets to Select after pressing Editor Done.

ID	Minimum Condition	Visible Symptoms
SMGR-70620	User management	Implement logic to purge records for Export List on export user page if exported entry is older than 30 days.
SMGR-71019	User management	Presence handle cannot be updated through bulk import operation using web services API call in Merge Mode.
SMGR-58826	User management	Presence handle cannot be updated through bulk import operation using Excel sheet.
SMGR-69515	User management	When using XML file for bulk import, users fail to get added to a group (Edit User -> Membership tab -> groups).
SMGR-70534	User management	Changing login name and removing "Other XMPP" communication address doesn't work together
SMGR-68073	User management	Missing HTTP header "cache-control" for self-provisioning causes failures while accessing self-provisioning through reverse proxy
SMGR-71286	User management	Clear Text password after Password Reset not sent through email for Self-Provisioning.
SMGR-71727	Communication Manager Management	Communication Manager Element Manager deployment getting failed to deploy on upgraded system.
SMGR-71295	Communication Manager Management	Data for "System" column is wrong in Report when "list registered-ip-station" report is generated with qualifier
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.
SMGR-70758	Communication Manager Management	disassociateUser.sh doesn't work properly when admin wants to delete users from System Manager associated with decommissioned Communication Manager.
SMGR-70645	Communication Manager Management	Button alignment is displaced for SIP endpoints in 8.1.3.5 release.
SMGR-70516	Communication Manager Management	Loading Bulk Edit page is very slow from User Management
SMGR-70227	Communication Manager Management	After System Manager upgrade to 8.1.3.5, Global search stops working
SMGR-70168	Communication Manager Management	Detailed agent report doesn't have correct values in all columns.
SMGR-70154	Communication Manager Management	Using an alias (J189) cannot enable more than 9 favourite buttons.
SMGR-70117	Communication Manager Management	Adding additional parameters in detailed agent report columns leads to showing wrong values in columns.
SMGR-70090	Communication Manager Management	Incremental sync fails if Notify sync is enabled for CM and hunt groups are deleted from Communication Manager.
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.
SMGR-70035	Communication Manager Management	System Manager not displaying "Select Destination for Broadcasting Announcements" list while broadcast announcement operation.
SMGR-69778	Communication Manager Management	Element Cut Through of abbreviated command "li tra sta 8000" stuck, while full command "list trace station 8000" works fine.

ID	Minimum Condition	Visible Symptoms
SMGR-69763	Communication Manager Management	WAV files gets stuck on remote servers in announcement backup failure scenarios and leads to error "SCP - Permission denied" on next announcement backup.
SMGR-69324	Communication Manager Management	Scheduled Incremental jobs stop running after upgrade from 8.1.3.3 to 8.1.3.4
SMGR-68788	Communication Manager Management	Invalid handle should not be accepted to sip URI.

Fixes in System Manager 10.1.0.2

The following table lists the fixes in this release:

ID	Minimum Conditions	Visible Symptoms
SMGR-67052	Software Upgrade Management	Alpha could not add host to SDM due to mismatch in FQDN case.
SMGR-58507	Alarming	generateTestAlarm may not work when there is heavy logging on the system
SMGR-67521	User Interface	Navigation Menu Shortcuts on the SMGR Dashboard are not intuitive
SMGR-69411	User Interface	Unable to select more than 500 users when Services > Configurations > Settings > SMGR > Common Console field “Max No of Records Selectable” is set to 9999
SMGR-68655	User Interface	Announcement broadcast: not able to upload large announcement files.
SMGR-54254	Infrastructure	log rotation not working as configured
SMGR-68743	Infrastructure	Customer user must not be able to switch to root user without root password
SMGR-50476	Infrastructure	Utility that checks for authorized keys causes 100% CPU
SMGR-70771	Infrastructure	Unable to login SMGR UI after configuring MUDG mode.
SMGR-69082	Infrastructure	Change the Facility value for spiritOperationAppender to the correct value like it was back in 7.x release
SMGR-68871	Scheduler Management	When "Discover Endpoints Eligible for Migration" job is enabled on 8.1 SMGR, job gets triggered immediately instead of scheduled time
SMGR-69726	Software Upgrade Management	Issue with Element upgrade in SMGR-SDM
SMGR-56205	Infrastructure	CLI access lost after upgrade from 8.0.1.1 to 8.1.2 for custom users which were enabled through GUI
SMGR-69172	User Management	Edit User > Membership > Groups > add Group to the user > switch to any other page on User and Group details will be vanished
SMGR-68073	User Management	Missing HTTP header "cache-control" for self-provisioning causes failures while accessing self-provisioning through reverse proxy
SMGR-69515	User Management	When using XML file for bulk import, users fail to get added to a group (Edit User -> Membership tab -> groups)
SMGR-68737	User Management	AD-sync wipes all secondary communication profile set values
SMGR-69856	Licensing Management	AES Enterprise Licensing showing incorrect value for Available License count for features after allocation to local WebLMs

ID	Minimum Conditions	Visible Symptoms
SMGR-70538	Licensing Management	License/WebLM issues after deploying 8.1.3.5-HF build 9 (8.1.3.5.1014828)
SMGR-68506	Licensing Management	WebLM to use new Avaya Logging Client and not use log4j directly
SMGR-68106	Licensing Management	Cannot over-install Centralized CM license file if the old file is mapped with two IP addresses
SMGR-70227	Communication Manager Management	After SMGR upgrade to 8.1.3.5, Global search/Khoj stops working
SMGR-70168	Communication Manager Management	Default detailed agent report doesn't have correct values in all columns
SMGR-70157	Communication Manager Management	Add more loggers to find issue in announcement upload scenarios with AMS and certificates
SMGR-70117	Communication Manager Management	Adding additional parameters in detailed agent report columns leads to showing wrong values in columns
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
SMGR-70035	Communication Manager Management	SMGR not displaying "Select Destination for Broadcasting Announcements" list while broadcast announcement operation
SMGR-69763	Communication Manager Management	.wav files gets stuck on remote servers in annc backup failure scenarios and leads to error "SCP - Permission denied" on next annc backup annc
SMGR-69743	Communication Manager Management	“Edit Extension” feature on SMGR doesn't release the old extension to available pool
SMGR-69742	Communication Manager Management	Cannot upload OR backup announcements having '&' char in the filename
SMGR-69575	Communication Manager Management	Notify sync job marked as failed in scheduler with exceptions in logs and wrong notificationreplayed column values in ipt_cm_notify table
SMGR-69569	Communication Manager Management	Operation log show failed even when announcement backup is successful
SMGR-69564	Communication Manager Management	Download announcement shows blank page second time onwards
SMGR-69561	Communication Manager Management	Changing Set type using Global Endpoint Change operation for H323 station does not work
SMGR-69560	Communication Manager Management	Global search does not work properly for all objects
SMGR-69556	Communication Manager Management	Announcement shows wrong path for backed up announcement
SMGR-69324	Communication Manager Management	Scheduled Incremental jobs stop running after upgrade from 8.1.3.3 to 8.1.3.4
SMGR-69211	Communication Manager Management	sipuri and etc should be cleared when creating template from an existing endpoint
SMGR-60696	Communication Manager Management	Help links for Communication Manager sub pages
SMGR-69071	Communication Manager Management	"Away Timer Value" on profile settings tab is only allowed from 5 to 480 but phone accept till 999

ID	Minimum Conditions	Visible Symptoms
SMGR-68788	Communication Manager Management	Invalid handle should not be accepted to sip URI.
SMGR-68782	Communication Manager Management	Group membership tab doesn't work for new user, it moves back to general option page.
SMGR-68725	Communication Manager Management	Backup wave files operation fails for Audio Group
SMGR-68448	Communication Manager Management	Issues with "Calculate Route Pattern" and "SIP Trunk" fields on CM comm profile
SMGR-68244	Communication Manager Management	some role permission NOT working properly
SMGR-68210	Communication Manager Management	Notify Sync/Incremental sync fail to process "change extension-station" command if extension value includes "-"
SMGR-68105	Communication Manager Management	Element cut-through columns show wrong values for "list station" command
SMGR-68009	Communication Manager Management	Option usage page will be blank after moving back from other pages
SMGR-67546	Communication Manager Management	slowness/latency happens when trying to administer the extension using Element Cut Through
SMGR-67518	Communication Manager Management	Missing options in RBAC configurations
SMGR-67455	Communication Manager Management	Lot of OP_IPT000273 errors are observed on SMGR for Notify sync job failures for "add recorded-ann" commands.
SMGR-67158	Communication Manager Management	change holiday-table in element cut through does not display two digits
SMGR-67070	Communication Manager Management	Can not add new CM element on SMGR with the error "System with Node IP Address 'a.a.a.a' already exists or some operations are in progress with this IP Address, please try again after some time"
SMGR-62056	Communication Manager Management	Enabling "Allow H.323 and SIP Endpoint Dual Registration" needs two clicks
SMGR-62039	Communication Manager Management	SMGR opens multiple SAT sessions on duplex CM instead of using existing connections
SMGR-70918	Geographic Redundancy	Geo Redundancy Failing on MUDG mode
SMGR-70727	Infrastructure	Unable to login SMGR UI after configuring MUDG mode
SMGR-70810	User Interface	After Upgrade from 7.0.x to 8.0.x external authentication and Policy links stop working

Fixes in System Manager 10.1.0.1

The Following table lists the fixes in this release:

ID	Minimum Conditions	Visible Symptoms
SMGR-67000	Software Upgrade Management	System Manager Load-to-Load upgrade/migration is failed when deployment is done through SDM client.

ID	Minimum Conditions	Visible Symptoms
SMGR-68472	Software Upgrade Management	After accepting the certificate by SDM, On the ASP S8300 host, the Offer type in Platform tab was changed unexpectedly.
SMGR-68054	Software Upgrade Management	Deploy CM 10.1 using SDM-SMGR on S8300E ASP completed with CONNECT_NOT_ESTABLISHED warning.
SMGR-67886	Software Upgrade Management	Generate certificate is failed for ASP130 and S8300E on SDM client.
SMGR-67900	Software Upgrade Management	Migration CM Main/LSP and BSM failed with S8300E card
SMGR-67010	Communication Manager Management	Receive Analog incoming Call ID" field is missing on SMGR.
SMGR-67044	Communication Manager Management	"Reserve Level" field is missing on the detailed report for Agent.
SMGR-67530	Communication Manager Management	"No data found" for detailed reports for VDN and Endpoints.
SMGR-66927	Communication Manager Management	Announcement Backup fails if it takes more than 5 minutes to complete.
SMGR-67947	Communication Manager Management	IP Network Map entries not showing up in SMGR even though it's programmed in CM.
SMGR-60053	Communication Manager Management	Adding a new network range for network-region is not populated in the correlated SM Location.
SMGR-59936	Communication Manager Management	CM sync fails at cleaning step while processing "change extension-station xxx".
SMGR-67519	Communication Manager Management	Broadcast Announcements for a Media server recreated all old Announcements.
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.
SMGR-67420	Communication Manager Management	CM-SMGR Sync Status stuck in "SM asset IP changed"
SMGR-66880	Communication Manager Management	When multiple CMs are selected, Element cut-through defaults to first selected CM always
SMGR-68318	Communication Manager Management	Broadcast Announcement failed it take more than 5 min to transfer the file
SMGR-67999	Communication Manager Management	SIP Trunk field is getting disabled with cluster CM
SMGR-67654	Communication Manager Management	Edit Endpoint missing field validation msg/hints/tool-tips after upgrade from 7.1.3.4.
SMGR-67887	Communication Manager Management	After self-provisioning change of password for SIP user, the preferred handle in CM disappears.
SMGR-67361	Communication Manager Management	Activating "Dual Registration" fails if SIP user is converted from SIP to H323.
SMGR-68242	Communication Manager Management	Customer role with CM endpoint edit permission cannot edit/assign buttons after upgrade from 8.1.3.1.
SMGR-68580	Communication Manager Management	Jumping cursor while typing inside CM element cut-through command line.
SMGR-67892	User Interface	outdated version of Moment.js being used on SMGR.

ID	Minimum Conditions	Visible Symptoms
SMGR-67850	Geographic Redundancy	SSP 14 patch installation failures when secondary GEO is involved.
SMGR-61744	Infrastructure	Postgress down sometimes automatically
SMGR-58568	Infrastructure	Executing collectLogs script causes SMGR Web Interface to go down and stay down till JBoss restart
SMGR-68348	Infrastructure	Polkit vulnerability (CVE-2021-4034) RHSA-2022:0274
SMGR-67191	Infrastructure	PairIPFQDN script is failing on primary SMGR
SMGR-67190	Infrastructure	In inventory page of secondary SMGR, after executing change IP/FQDN it is still showing old IP and FQDN
SMGR-68604	Infrastructure	Update the swversion output and About info on SMGR to display the hot fix build number
SMGR-60284	Installer	SMGR upgrade across major release fails if the old SMGR FQDN is subset of the new SMGR FQDN.
SMGR-67600	Logging	log4j vulnerability - CVE-2021-44228
SMGR-67488	Infrastructure	JBoss getting stopped intermittently due to load.
SMGR-61661	Software Upgrade Management	On Scheduler upgrade Job Details section always shows the date the upgrade job was entered into SMGR.
SMGR-60302	Software Upgrade Management	CM Refresh Element via SDM Upgrade Management fails if CM has special characters in password.
SMGR-68039	Software Upgrade Management	DigiCert root and subordinate CA certificates missing from SMGR trusted store.
SMGR-60323	Access Control	View permissions to SMGR Core and Breeze not fully restrictive.
SMGR-67879	User Management	Advanced user search filter gives wrong results when both E164 handle and first name are added to filter.
SMGR-67622	User Management	AD Sync job get stuck if we don't give proper DN value.
SMGR-67210	User Management	Issues with self-provisioning password reset.
SMGR-67189	User Management	Create User Management Web Service gives 201- Created in response
SMGR-67768	User Management	Change password through self-provisioning fail for SIP user.
SMGR-58098	User Management	Unable to delete user, fails with error as "Unable to find com.avaya.coreservice.persistence.user.CsPerson with id xyz"
SMGR-67872	Communication Manager Management	Customer role with CM endpoint edit permission cannot edit/assign buttons after upgrade from 8.1.3.1 to 8.1.3.3
SMGR-68105	Communication Manager Management	Element cut-through columns show wrong values for "list station" command
SMGR-68107	Communication Manager Management	Jumpin cursor while typing inside CM element cut-thru "Command:" line
SMGR-55769	System Manager RTS	"Enable" filter of all tables in Create Profiles and Discover SRS/SCS Inventory doesn't work

Fixes in System Manager 10.1

The Following table lists the fixes in this release:

ID	Minimal Condition	Visible Symptoms
SMGR-60639	Communication Manager Management	SMGR triggers incremental sync for every change notification from CM
SMGR-61829	Data Migration	Data migration failure with 'TM upgrade fail'
SMGR-59333	Data Replication System	System Manager goes Out of Memory
SMGR-66803	Data Replication System	BS DRS Repair Failure
SMGR-58508	Geographic Redundancy	Geo redundancy database replication fails
SMGR-49615	Installer	Software only installer corrupts the /etc/fstab
SMGR-59173	Scheduler Management	Schedule completed jobs purge should run automatically
SMGR-59126	Infrastructure	Misleading authentication failure logs
SMGR-59175	User Interface	Login attempt failure
SMGR-59174	Infrastructure	Quantum log don’t show Source IP
SMGR-60993	Infrastructure	JBoss unable to start properly
SMGR-61837	Infrastructure	Twiddle Script failing on secondary
SMGR-49327	Infrastructure	Misleading security logs when web login fails
SMGR-53806	User management	user can soft delete all SIP users from system even if they do not have access to all the users
SMGR-54769	User management	Export Select all option is not working
SMGR-56816	User management	"Export selected users" exports fewer users
SMGR-60233	User management	Issues with "Auto Generate Communication Profile Password:"
SMGR-60072	User management	User edit time increases exponentially
SMGR-58339	User management	Automatic generation of communication profile password" fails
SMGR-58293	User management	Custom user with view only permissions can edit user
SMGR-57282	User management	Export all users not completing
SMGR-60609	User management	Edit user to show if comm profile password is et
SMGR-61870	User management	Buttons are disabled post upgrade from 7.1.X
SMGR-56045	WebLM	WebLM license crashing intermittently
SMGR-55563	WebLM	TLS Configuration not working

ID	Minimal Condition	Visible Symptoms
SMGR-59142	WebLM	CIS vulnerabilities
SMGR-67849	Scheduler	Remote Backup Job is not created when remote backup is enabled on OVA deployment
SMGR-67815	Trust Management	Patch installation fixes.
SMGR-67800	Scheduler	CM synchronization fails after System Manager upgrade from 7.x to 10.1
SMGR-67753	Infrastructure	System Manager virtual machine does not boot up after enabling Military mode hardening.
SMGR-67706	Infrastructure	Older 8.1SSP showing under swversion after installing 8.1 System Manager.
SMGR-67703	Infrastructure	All scripts having java process shall communicate over TLSv1.3 without any changes
SMGR-67661	Infrastructure	Add Log Retention in System Manager 10.1
SMGR-67642	Infrastructure	Update Firewall scripts to adapt to the iptables backend in FirewallD
SMGR-67629	Trust Management	System Manager Restore failed when TLS 1.3 is configured.
SMGR-67592	Software Upgrade Management	Hide screens, which are not relevant, during OVA deployment using System Manager SDM
SMGR-67564	SMGR Performance	Performance issues
SMGR-67535	Infrastructure	Include hmac-sha1 to MACs in sshd_config file
SMGR-67531	Infrastructure	editHosts and securityHardeningOptions alias doesn't work on fresh deployment of System Manager 10.1
SMGR-67504	Software Upgrade Management	ASP Default password population in kickstart
SMGR-67490	Software Upgrade Management	The behaviour when user deploys the VMs on ASP on S8300E should be same as AVP on S8300E
SMGR-67395	Infrastructure	CS1000 - VxWorks target join fails due to incorrect dir permissions on SMGR
SMGR-67314	Infrastructure	Update and Validate plugins.d/syslog.conf in /etc/audit/
SMGR-67287	User Management	Display Proper error messages should be displayed on the Web Interface if creating a user with a CM station number that already exists.
SMGR-67191	Infrastructure	PairIPFQDN script is failing on primary SMGR
SMGR-67145	User Management	The New button in Shared Address Task doesn't work and get stuck in inactive status.
SMGR-67132	Software Upgrade Management	During CM upgrade using SDM, if auto-commit is selected, then the upgrade should be committed after upgrading completes successfully
SMGR-67109	Infrastructure	Update MUDG Hardening scripts to RHEL 8
SMGR-61551	User Interface	UI issues on certain Multi Tenancy pages in System Manager 10.1
CVE-2021-44228 and CVE-2021-45046	Logging	Log4J Vulnerability fixes.ee PSN005565u for details.

ID	Minimal Condition	Visible Symptoms
CVE-2021-45105	Logging	Log4J Vulnerability fixes. See PSN005565u for details. See PSN005565u for details.

Known issues and workarounds in System Manager in Release 10.1.x.x

Known issues and workarounds in System Manager in Release 10.1.3.2

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

ID	Minimum conditions	Visible symptoms	Work around
SMGR-71664	Infrastructure	SMGR Console scrolls audit errors – 'kauditd hold queue overflow'.	Using root account, execute "systemctl enable auditd.service " and reboot System Manager.
SMGR-59670	Administrator	User cannot login and see dashboard directly but stuck on loginrouter.jsp	Remove part consisting of /network-login/* from URL and hit Enter button, which should show SMGR dashboard page as expected.
SMGR-71983	Inventory Management	While editing discovery profile, Commit button gets greyed out after any change in selection of subnet configurations	
SMGR-70675	Inventory Management	Issues with Email configurations	
SMGR-72612	Administrator	The Administrators tab is accessible even after Disabling Allow Administrator Web UI Access as part of creating custom role through Copying from Service Provider Administrator Template.	
SMGR-58509	Trust Management	System Manager CRL generation stops automatically	Set CRL check to 'NONE' and Restart JBoss service.
SMGR-73328	Infrastructure	Disk encryption is not properly enable when localkey option is used	Execute below steps with root account - 1. encryptionLocalKey disable 2. encryptionLocalKey enable
SMGR-73448	Infrastructure	IPv6 interface stops responding after upgrading to SMGR 10.1.3.0 from SMGR 10.1.0.0	
SMGR-74282	Infrastructure	SMGR is sending out DNS query to public root hints server	
SMGR-74443	Infrastructure	Updating DNS entries using changeIPFQDN command doesn't work as expected	If you have root user access, update below files and reboot 1) /etc/sysconfig/network-scripts/ifcfg-eth0 2) /etc/resolv.conf
SMGR-74211	Geo Redundancy	Geo Auto-Disable gets triggered when FQDN includes capitals letters	
SMGR-74476	Global Search Component	Global Search is not working for administrative users associated with custom roles.	

ID	Minimum conditions	Visible symptoms	Work around
SMGR-74488	License Management	Unable to install more than 39 product license files on SMGR Licensing Manager (WebLM).	Uninstall unused license file if any and install required file. Or Use alternate licensing server to install license file.
SMGR-74218	Communication Manager Management	CM synch radio buttons are greyed out for first attempt.	Refresh the table
SMGR-74444	Communication Manager Management	Appropriate language is not populated in the "Multibyte Language" field through User Management operations	Uncheck override display name in CM comm profile page and view the data from Manage Endpoints page.
SMGR-74248	Communication Manager Management	Incremental sync stops working after 10.1.x upgrade.	
SMGR-75066	Infrastructure	Unable to change the Subnet on System Manager 10.x using changeIPFQDN utility.	

Known issues and workarounds in System Manager in Release 10.1.3.1

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

ID	Minimum conditions	Visible symptoms	Work around
SMGR-72408	User Management	Using Rest Tool to search all the users above 32767 it fails with error	
SMGR-71664	Infrastructure	SMGR Console scrolls audit errors – ‘kauditd hold queue overflow’.	Using root account, execute “systemctl enable auditd.service ” and reboot System Manager.
SMGR-59670	Administrator	User cannot login and see dashboard directly but stuck on loginrouter.jsp	Remove part consisting of /network-login/* from URL and hit Enter button, which should show SMGR dashboard page as expected.
SMGR-71983	Inventory Management	While editing discovery profile, Commit button gets greyed out after any change in selection of subnet configurations	
SMGR-70675	Inventory Management	Issues with Email configurations	
SMGR-72612	Administrator	The Administrators tab is accessible even after Disabling Allow Administrator Web UI Access as part of creating custom role through Copying from Service Provider Administrator Template.	
SMGR-58509	Trust Management	System Manager CRL generation stops automatically	Set CRL check to ‘NONE’ and Restart JBoss service.
SMGR-73328	Infrastructure	Disk encryption is not properly enable when localkey option is used	Execute below steps with root account - 3. encryptionLocalKey disable 4. encryptionLocalKey enable

ID	Minimum conditions	Visible symptoms	Work around
SMGR-73448	Infrastructure	IPv6 interface stops responding after upgrading to SMGR 10.1.3.0 from SMGR 10.1.0.0	
SMGR-74218	Communication Manager Management	CM synch radio buttons are grayed out for first attempt.	Refresh the table
SMGR-73968	Communication Manager Management	CMs cannot be synched, Cut-through stops working, and few Basic reports stop working after SMGR IP changed with changeIPFQDN command	
SMGR-73286	Infrastructure	Unable to configure account lockout policy settings using setSecurityPolicy utility.	

Known issues and workarounds in System Manager in Release 10.1.3.0

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

ID	Minimum conditions	Visible symptoms	Workaround
SMGR-71983	Inventory Management	While editing discovery profile, Commit button gets grayed out after any change in selection of subnet configurations	
SMGR-70675	Inventory Management	Issues with Email configurations	
SMGR-72790	Trust Management	Secondary Server (if in activated state more than 7 days), unable to access SMGR UI after reboot or restart	Once Secondary is activated, set crl check to 'NONE' and restart.
SMGR-72612	Administrator	Administrators Tab is accessible even after Disabling Allow Administrator Web UI Access	
SMGR-72190	Infrastructure	Duplicate http headers	
SMGR-69748	Infrastructure	CRL generation failed after changing FQDN using changeIPFQDN script due to which web interface went down after next JBoss restart after 7 days	After FQDN change, set crl check to 'NONE' and restart.
SMGR-58509	Trust Management	System Manager CRL generation stops automatically	Set crl check to 'NONE' and restart.

Known issues and workarounds in System Manager in Release 10.1.2.0

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

ID	Minimum Condition	Visible Symptoms/ Summary	Workaround
SMGR-71972	Security Management	Changing the Minimum TLS Version to 1.2 from SMGR Web Page In Security -> Configuration -> Security Configuration, only port 443 gets changed to TLS 1.2 and rest all ports doesn't get changed to TLS 1.2.	

ID	Minimum Condition	Visible Symptoms/ Summary	Workaround
SMGR-72188	Certificate Management	Utility command 'manageEntityClassWhitelist' from SMGR Command Line Interface is not working in 10.1.x Release.	
SMGR-71924	User Interface	Administrator unable to assign a tenant to an existing user from Web Interface.	
SMGR-71289	User Interface	Cannot go to next page in Dial Pattern page if 1 or more records are selected	
SMGR-71866	Installation	Patch installation fails if RPM database is already in corrupted state.	Please refer Option#1 in PSN005562u document.
SMGR-71122	Role Management	Custom role behaves differently compared to the role that it was exactly copied if custom role is copied from default role 'Service Provider Administrator Template'.	Instead of copying permission from default role 'Service Provider Administrator Template, assign required permissions manually to custom role.
SMGR-71288	User management	Required field error messages are not displayed when assigning a Session Manager Profile.	
SMGR-71287	User management	Adding a user does not result in error when fields are missing	
SMGR-71285	User management	no error popup shown when add new user with empty "Home Location" is required field in Session Manager Profile	
SMGR-70782	Administration	Purging the exportedUser.zip files	
SMGR-70505	User management	Duplicate station operation from user management creates 3 call-appr always even if original user has only one or two	
SMGR-70381	User management	Duplicate user operation creates CM endpoint with all default values	
SMGR-70047	Software Upgrade Management	Custom Patch should not be displayed on pre-upgrade check page	
SMGR-69170	Scheduler	CM command notification coming from CM is not processed by SMGR because it thinks job is already running	
SMGR-67366	User management	Dup of an existing user which has already assigned feature button from CM endpoint profile tab only does not dup of feature button	
SMGR-61939	Administration	Loading Export Users page is very slow from User select under more option	
SMGR-72366	Geo Redundancy	GR Health Heartbeat graph not getting displayed	
SMGR-61846	Software Upgrade Management	Cannot upload the OVA file in Download Management using My Computer source	Use 'Sync Files from directory' feature from Solution Deployment Manager -> Software Library Management page
SMGR-72161	Communication Manager Management	Incremental sync goes into loop for Synchronizing Endpoints	This issue is fixed in CM under Jira CM-90584. Upgrade CM to minimum 10.1.0.2 version.

ID	Minimum Condition	Visible Symptoms/ Summary	Workaround
			NOTE: System Manager version should be higher or equivalent to CM version.

Known issues and workarounds in System Manager in Release 10.1.0.2

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

ID	Minimum Condition	Summary	Workaround
SMGR-60333	Data Replication System	Session Manager Replication Failure with SMGR on 8.1.3.2 system due to error related to ipt_station	
SMGR-60005	Infrastructure	customer is unable to configure GEO in mixed environment 8.1.3.1 release	
SMGR-59382	Infrastructure	Unable to start jboss because of missing module.xml file	
SMGR-59005	Geographic Redundancy	Geo configuration failing after cold standby	
SMGR-58509	Trust Management	System Manager CRL generation stops automatically	
SMGR-57820	Infrastructure	Idle Postgres connection is not getting dropped	
SMGR-54822	Alarming	SMGR to handle CM SNMP trap translation before sending email notify to user	
SMGR-54528	Data Replication System	Thread leak in System Manager	
SMGR-53558	UCM	SMGR being in a bad state of causing java core dumps and issues on the Breeze nodes because of the openSSO client that SMGR provides	
SMGR-51013	Alarming	Leading or trailing spaces for IP-address field inside the SNMP target profile causes an error while assigning target profiles to the serviceability agent.	
SMGR-49616	UCM	After Upgrade from 7.0.x to 8.0.x external authentication and Policy links stop working	
SMGR-68835	UCM	JBoss gets stuck in Initialize mode once secondary is activated	
SMGR-60412	Software Upgrade Management	The re-establish of AVPU 8.1 cannot update the information on SMGR inventory after upgrading the US 7.1.x or US 7.0 to AVPU 8.1.0	
SMGR-70156	Software Upgrade Management	AVP refresh jobs should be marked as failed automatically if they are stuck for 5 min or so	

ID	Minimum Condition	Summary	Workaround
SMGR-70957	Software Upgrade Management	Upgrading MUDG SMGR 8.1.3.3 to MUDG 10.1.0.2 via SDM shows Patch installation Status on UI as failed though in the back-end its successful	
SMGR-71345	Software Upgrade Management	After updating Session Manager from 10.1.0.1 SP1 to 10.1.0.2 SP2 through SMGR-SDM if you have not auto committed the patch, then by default the auto-commit of patch installation happens after 24 hours. If auto-commit fails, you need to manually Commit the patch.	Go to the Solution Deployment Manager > Upgrade Management patch. Select the SM element and click Upgrade Actions > Installed Patches. Select the required patch, select the Commit Patch operation, and schedule the patch commit.

Known issues and workarounds in System Manager in Release 10.1.0.1

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

Key	Minimum Conditions	Summary	Workaround
SMGR-68899	Data Migration	SMGR can't be installed patch when enabling Military Mode and upgrading to 10	Work-around when patch fails after Data Migration. Only apply the workaround when below error is seen in /var/log/Avaya/applyPatch.out.xxx FAILURE: Starting postgresql service 1. confirm postgresql service is down 2. Execute below three command as root chown admin:admin /var/lib/pgsql chmod admin:admin /var/run/postgresql userdel postgres 3. Start Postgresql service service postgresql start 4. Start Patch installation again
SMGR-69104	Software Upgrade Management	The FP10.10.1 is not installed on AES after migration finished through SDM	Need to manually install patch using AES CLI
SMGR-68944	Communication Manager Management	Cannot import contacts in SMGR 8.1 if dual registration is enabled	
SMGR-68871	Scheduler Management	When "Discover Endpoints Eligible for Migration" job is enabled on 8.1 SMGR, job gets triggered immediately instead of scheduled time	
SMGR-68835	UCM	JBoss gets stuck in Initialize mode once secondary is activated	
SMGR-68788	Communication Manager Management	Invalid handle should not be accepted to sip URI.	
SMGR-68778	License Management	Customer can switch to root on the WebLM without providing root password	

Key	Minimum Conditions	Summary	Workaround
SMGR-68761	Infrastructure	changeIPFQDN command does not update new FQDN in pg_ident.conf file	
SMGR-68737	User Management	AD-sync wipes all secondary communication profile set values	
SMGR-68725	Communication Manager Management	Backup wave files operation fails for Audio Group	
SMGR-68722	SMGR UCM	EASG login on the GUI does not generate challenge in certain scenarios.	
SMGR-68546	Geographic Redundancy	Geo enable should fail instead of showing as completed	
SMGR-68448	Communication Manager Management	Issues with "Calculate Route Pattern" and "SIP Trunk" fields on CM comm profile	
SMGR-68210	Communication Manager Management	Notify Sync/Incremental sync fail to process "change extension-station" command if extension value includes "-"	
SMGR-68194	Software Upgrade Management	Updating VM information in Inventory failing for AVP Utilities.	
SMGR-68105	Communication Manager Management	Element cut-through columns show wrong values for "list station" command	
SMGR-68073	User Management	Missing HTTP header "cache-control" for selfprovisioning causes failures while accessing selfprovisioning through reverse proxy	
SMGR-68071	User Management	Issue in selfprovisioning logs	
SMGR-68040	UCM	Provision User Certificate Authentication broken in SMGR 8.1.3.3 and 10.1	
SMGR-68030	Software Upgrade Management	SDM Upgrade Management hung when attempting to apply Log4j custom patch to Branch Session Manager	
SMGR-67985	License Management	Remove or provide a way to disable weak Ciphers in WebLM 8.1.x	
SMGR-67872	Communication Manager Management	customer role with CM endpoint edit permission cannot edit/assign buttons after upgrade from 8.1.3.1 to 8.1.3.3	
SMGR-67455	Communication Manager Management	OP_IPT000273 errors are observed on SMGR for Notify sync job failures	
SMGR-67454	Communication Manager Management	CM Cut-through for Network Region editing is awful and badly aligned	
SMGR-67011	Communication Manager Management	With custom user, unable to edit set type field in CM Endpoint template	

Key	Minimum Conditions	Summary	Workaround
SMGR-66997	Communication Manager Management	CM cannot be removed from System Manager if the CM is no longer available / on the network	Contact Avaya Support Team
SMGR-60333	Data Replication System	Session Manager Replication Failure with SMGR on 8.1.3.2 system due to error related to ipt_station	
SMGR-60043	Geographic Redundancy	Wrong IP in nodes after disaster recovery	
SMGR-60005	Infrastructure	Unable to configure GEO in mixed environment 8.1.3.1 release	
SMGR-59382	Infrastructure	unable to start jboss because of missing module.xml file	
SMGR-59005	Back up & Restore	Geo configuration failing after cold standby	
SMGR-58509	Trust Management	System Manager CRL generation stops automatically	
SMGR-57820	Infrastructure	Idle Postgres connection is not getting dropped	
SMGR-54822	Alarming	SMGR to handle CM SNMP trap translation before sending email notify to user	
SMGR-54528	Data Replication System	Thread Leak in System Manager	
SMGR-53558	UCM	SMGR in a bad state of causing java core dumps and issues on the Breeze nodes because of the openSSO client that SMGR provides	
SMGR-51320	Infrastructure	System Manager database growing because postgres autivacuum proce is not running properly	
SMGR-49616	UCM	After Upgrade from 7.0.x to 8.0.x external authentication and Policy links stop working	

Known issues and workarounds in System Manager in Release 10.1

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

Key	Minimum Conditions	Summary	Workaround
SMGR-67486	Infrastructure	SMGR could not boot up after enabling Military security profile	Enable security option "FIPS" before enabling Military security profile
SMGR-67191	Geo Infrastructure	Changing network parameters like IP, FQDN etc doesn’t work in 10.1 on Geo SMGR through change IPFQDN utility	Update network parameters on Standalone SMGR
SMGR-67209	SDM UI	Error message is not displayed even if mandatory field like location is not entered	Configure all mandatory fields
SMGR-67551	Infrastructure	Updating host file through editHosts command doesn’t work in SMGR 10.1	Use root user to update /etc/hosts file

Key	Minimum Conditions	Summary	Workaround
SMGR-67132	SDM Upgrade Management	During migrate if auto-commit is selected, then CM should be committed after upgrading completed successfully	Do not select Auto commit. After upgrade is done, perform Commit manually
SMGR-67505	SDM UI	View output for check environment does not show on SDM client	No
SMGR-67551	Security	SMGR restore doesn't work on TLSv1.3 configured SMGR	Don't try SMGR restore on TLSv1.3 as a minimum TLS version configured SMGR
SMGR-67548	SDM Client /Software only ISO	Installation of Software-Only + GA Patch using SDM Client fails at Patching step if /var partition is separate and of recommended size.	Deploy Software only ISO first and then apply GA Patch.
SMGR-66880	Communication Manager Management	When multiple CMs are selected, Element cut-through defaults to first selected CM always	
SMGR-62056	Communication Manager Management	Enabling "Allow H.323 and SIP Endpoint Dual Registration" needs two clicks	
SMGR-67010	Communication Manager Management	"Receive Analog incoming Call ID" field is missing on SMGR for CO trunk	
SMGR-62039	Communication Manager Management	SMGR opens multiple SAT sessions on duplex CM instead of using existing connections	
SMGR-66997	Communication Manager Management	CM cannot be removed from System Manager if the CM is no longer available / on the network	Manually go into the SMGR database and make changes so that the CM can be deleted using the IPTCM maintenance job.
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	execute an existing report definition if a job is already created for it.
SMGR-66927	Communication Manager Management	Announcement Backup fails if it takes more than 5 minutes to complete	
SMGR-67455	Communication Manager Management	Lot of OP_IPT000273 errors are observed on SMGR for Notify sync job failures for "add recorded-ann" commands	
SMGR-67011	Communication Manager Management	With custom user, unable to edit set type field in CM Endpoint template	
SMGR-60053	Communication Manager Management	Adding a new network range for network-region is not populated in the correlated SM Location if Notes field contains more than one emulate characters	
SMGR-67454	Communication Manager Management	CM Cut-through for Network Region editing is awful and badly aligned	
SMGR-67491	Security	Not able to add whitelist subject names for the Entity Classes	This issue is caused due to the recent Postgres upgrade. Null constraint in

Key	Minimum Conditions	Summary	Workaround
			the db tables has been changed
SMGR-67145	User Management	The New button in Shared Address Task doesn't work and get stuck in inactive status.	
SMGR-67358	User Management	SMGR tenant user can create public contact at user management tab	
SMGR-67339	User Management	UI issues occurred when login by user assigned Tenant Administrator role	
SMGR-61841	User Management	Minor UI issue on SMGR (Tenant page/HELP page)	
SMGR-67209	User Management	No error displays on the User profile page after committing editing user which selected application seq but not enabled CM profile	
SMGR-67309	SDM Upgrade Management	SMGR SDM show Certificate Details as blank when pre-upgrade configuration	
SMGR-62057	SDM Application Management	Unable to discover ESXi host on 10.1 SDM in first attempt able to discover in second attempt	1.Retry vCenter discovery by editing already added vCenter details through Map vCenter again 2. This should discover all required hosts from that vCenter again.
SMGR-60043	Geo Redundancy	Wrong IP in nodes after disaster recovery	
SMGR-67593	On Fresh Installation	System Manager product not available for SMGR log harvester	
SMGR-67412		Recover agent CLI scripts fails	Use Recover agent UI option
SMGR-68472	SDM UI	After regenerating and accepting Certificate using SDM for the ASP S8300 host, the “Offer type” column in the Platform tab changes unexpectedly to “Customer VE” and the Platform type column in the Applications tab does not display any information.	Ensure that you remove the ASP S8300 5.1 host from the ‘Platforms’ tab and again add the same ASP S8300 host using the ‘Platforms’ tab.
SMGR-68473	SDM UI	The host type of AVP host is not displayed properly on the Platform type column	
SMGR-68597	SDM UI	The profile of CM and BSM should only display the options "CM Main Max User 1000 and CM Survivable Max User 1000" and "BSM profile 1 Max Devices 1000 " when execute the migration on ASP S8300 by SMGR SDM	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):

Key	Minimum Conditions	Summary	Workaround
			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.

Solution Deployment Manager Adopter Matrix

Solution Deployment Manager Adopter Matrix	Adopting Product (System Manager Release 10.1)													
System Manager Solution Deployment Manager – Centralized									Breeze				Avaya Aura®	
Functionality	Appliance Virtualization Platform	System Manager	Session Manager	Communication Manager	CM Adjuncts (MM, TN Boards, Gateways)	Branch Session Manager	AVP Utilities	CM Messaging		Secure Access Gateway	WebLM	Application Enablement Services	Media Server	Session Border Controller (SBCE 8.0.1)
OVA Deployment R 7.0.0/7.1/8.0/8.1 (Configuration and Footprint)	N	Y(only through SDM client)	Y	Y	n/a6	Y	Y	Y	Y	Y	Y	Y	Y	Y[2] [Supported from 8.1.1]
OVA Deployment R 10.1 (Configuration and Footprint)	n/a	Y(only through SDM client)	Y	Y	n/a	Y	n/a	Y	Y	Y	n/a	Y	Y	Y
Patching Deployment (hotfixes)	Y [Other than AVP hosting System Manager]	Y(only through SDM client)	Y	Y	n/a	Y	Y	Y	N	N	Y	Y	N	N
Custom Patching Deployment	n/a	n/a	Y	Y	n/a	Y	Y	Y	N	N	Y	Y	N	Y

Solution Deployment Manager Adopter Matrix	**Adopting Product (System Manager Release 10.1)**														
System Manager Solution Deployment Manager – Centralized									Breeze				Avaya Aura®	
Functionality	Appliance Virtualization Platform	System Manager	Session Manager	Communication Manager	CM Adjuncts (MM, TN Boards, Gateways)	Branch Session Manager	AVP Utilities	CM Messaging		Secure Access Gateway	WebLM	Application Enablement Services	Media Server	Session Border Controller (SBCE 8.0.1)
Service/Feature Pack Deployment	Y [Other than AVP hosting System Manager]	Y(only through SDM client)	Y	Y	n/a	Y	Y	Y	N	N	Y	Y	N	N
Automated Migrations R7.x to R8.0/R8.1 (analysis and pre-upgrade checks) [Target Platform: AVP / customer VMware]	Y [Other than AVP hosting System Manager]	Y [Only using SDM Client]	Y	Y	n/a [Covered as Firmware Updates]	Y	Y	Y	N (Breeze Upgrade Supported from Breeze 3.3 Onwards)	N	Y	Y	N	N
Automated Migrations R7.x/R8.x to R10.1 (analysis and pre-upgrade checks) [customer VMware]	n/a	Y [Only using SDM Client]	Y	Y	n/a [Covered as Firmware Updates]	Y	Y	n/a	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	n/a	n/a

Solution Deployment Manager Adopter Matrix	**Adopting Product (System Manager Release 10.1)**													
System Manager Solution Deployment Manager – Centralized									Breeze				Avaya Aura®	
Functionality	Appliance Virtualization Platform	System Manager	Session Manager	Communication Manager	CM Adjuncts (MM, TN Boards, Gateways)	Branch Session Manager	AVP Utilities	CM Messaging		Secure Access Gateway	WebLM	Application Enablement Services	Media Server	Session Border Controller (SBCE 8.0.1)
Scheduler (upgrades and patching)	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N
Virtual Machine Management (start, stop, reset, status, dashboard)	Y	N	Y	Y	n/a	Y	Y	Y	Y	Y	Y	Y	Y	N
Support for changing VM Flexible Footprint	n/a	Y [Only using SDM Client]	Y	N	n/a	Y	n/a	Y	Y	Y	Y	Y	Y	N
Change Network Parameters	Y	n/a	n/a	n/a	n/a	n/a	Y	n/a	n/a	n/a	n/a	n/a	n/a	n/a

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

Y^1: Session Manager Bare Metal which is not on System Platform.

Y^2: SBCE OVA Deployment supported only using the SDM Client and not SMGR SDM

AVP: Appliance Virtualization Platform

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://downloads.avaya.com/css/P8/documents/101078425

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)

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

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

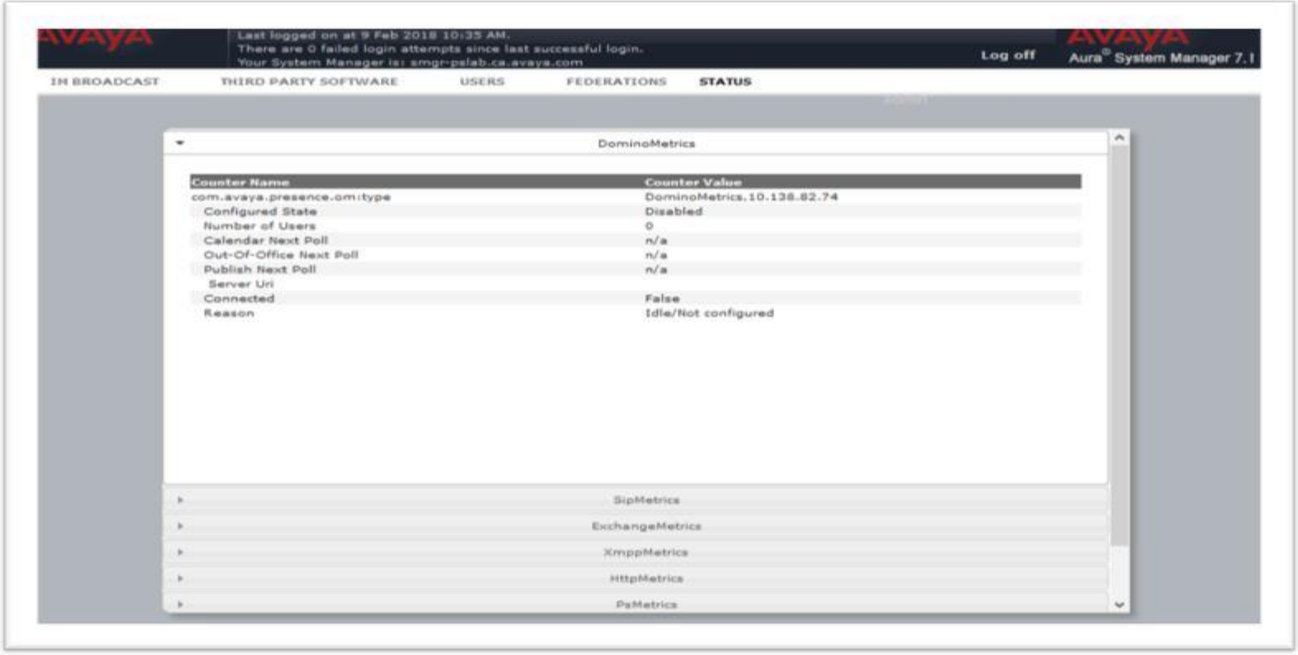
Known issues and workarounds in Presence Services Release 10.1.x.x

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

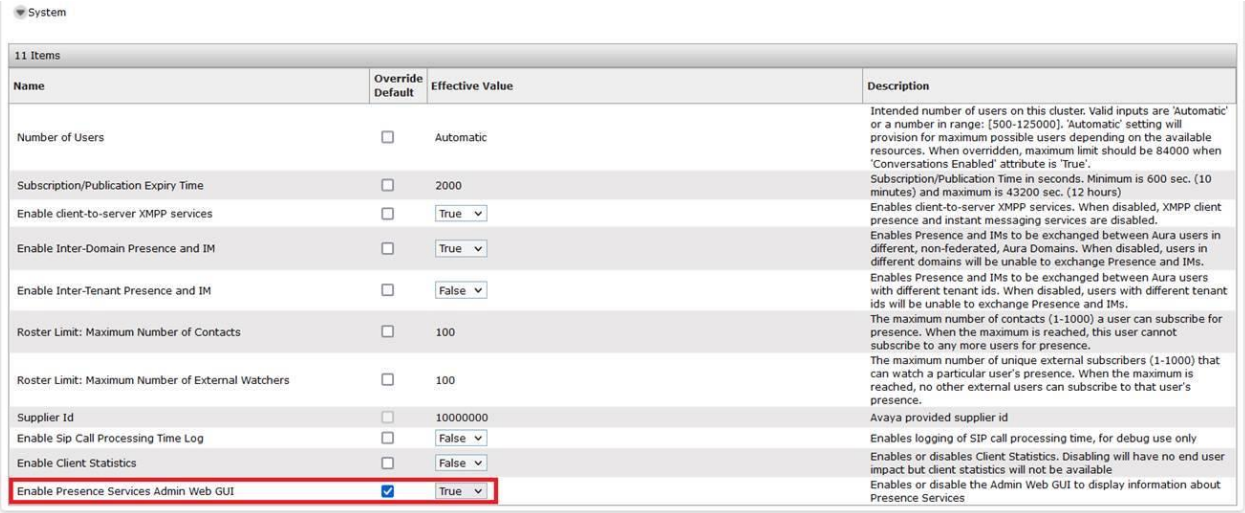
Note: The Presence Services Admin Web GUI, as shown below, is disabled by default in PS 8.1.1.0



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

What's new in Application Enablement Services 10.1.3.1

AE Services TSAPI Encrypted Services port added

Earlier to Release 10.1.3.1, you can enable or disable the TSAPI port 450 for the TSAPI listener.

With Release 10.1.3.1, a new TSAPI Encrypted Services Port 453 is added in the TSAPI Ports section on the Networking > Ports page. Additionally, TSAPI Services Port 450 is changed to Unencrypted Services Port 450.

By default, the Encrypted Services Port and Unencrypted Services Port are enabled.

For more information, see ***What's New in Avaya Aura® Release 10.1.x*** document on the Avaya Support site: https://downloads.avaya.com/css/P8/documents/101078425

IMPORTANT NOTE: Starting 10.1.3.1, licensing for Communication Manager (CM) and Application Enablement Services (AES) will only work with 10.1.3.1 and higher version of System Manager (SMGR) or Standalone WebLM (WebLM). If upgrading CM and/or AES to 10.1.3.1 and higher then the required order of upgrade is imperative i.e. SMGR and/or WebLM should be upgraded to 10.1.3.1 and higher first to ensure licensing for CM and/or AES does not stop working. CM and AES 10.1.3.0 were originally compatible with Standalone WebLM 10.1.2.0 (as there was no Standalone WebLM 10.1.3.0), however beginning with 10.1.3.1 and higher, Standalone WebLM 10.1.3.1 and higher is required for CM and AES. The Avaya Aura® System Manager release/version must always be greater than or equal to the release/version of the components of the solution (Session Manager, Communication Manager, Application Enablement Services).

What's new in Application Enablement Services 10.1.3

For more information, see ***What's New in Avaya Aura® Release 10.1.x*** document on the Avaya Support site: https://downloads.avaya.com/css/P8/documents/101078425

What's new in Application Enablement Services 10.1.2

- From Release 10.1.2, System Manager Solution Deployment Manager and Solution Deployment Manager Client support the deployment and upgrade of AES using the OVA with the SHA256 hash algorithm
- Application Enablement Services 10.1 OVAs are re-spun to support SHA256 algorithm. For more information, see the Required artifacts section.
- The old 10.1 GA OVA contains the Avaya Signing certificate that is going to expire on Feb 20, 2023. Therefore, to address the Avaya signing certificate expiry, the new 10.1 GA OVAs are renewed and re-signed with the latest Avaya signed certificates. For more information, see PSN020586u - Avaya Aura® OVA Certificate Expiry February 2023.

For more information, see What's New in Avaya Aura® Release 10.1.x document on the Avaya Support site: https://downloads.avaya.com/css/P8/documents/101078425

What's new in Application Enablement Services 10.1.0.2

From Release 10.1.0.2, logging framework 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://downloads.avaya.com/css/P8/documents/101078425

What’s new in Application Enablement Services 10.1.x.x

With this release 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 Application Enablement Services (AES).

CRITICAL: The Security Service Pack installation framework for AES has changed in Release 10.1.x. It is imperative that the instructions in PCN2140S be reviewed for complete steps prior to installation of Security Service Packs on an AES 10.1.x system.

Beginning with Release 10.1 AE Services Linux Security Updates (LSU) will be referred to as Security Service Packs (SSP).

The old method of installing LSUs (now renamed as Security Service Packs) will not work in Release 10.1.

The minimum release of AES 10.1.x.x that you must be on in order to install the Security Service Packs for AES is 10.1.0.1.

The SSP can only be installed via the command line. There is no Solution Deployment Manager (SDM) for support for SSP installation.

In order to install the SSP for AES 10.1.x.x, you must use the new command ("av-update-os") and follow the detailed instructions in PCN2140S.

For more information, see ***What’s New in Avaya Aura® Release 10.1.x*** document on the Avaya Support site: https://downloads.avaya.com/css/P8/documents/101078425

Security Service Packs

Security Service Packs

For further information on SSP contents and installation procedures for AES 10.1.x, please see **PCN2140S**.

CRITICAL: The Security Service Pack installation framework for AES has changed in Release 10.1.x. It is imperative that the instructions in PCN2140S be reviewed for complete steps prior to installation of Security Service Packs on an AES 10.1.x system.

Beginning with Release 10.1 AE Services Linux Security Updates (LSU) will be referred to as Security Service Packs (SSP).

The old method of installing LSUs (now renamed as Security Service Packs) will not work in Release 10.1.

The minimum release of AES 10.1.x.x that you must be on in order to install the Security Service packs for AES is 10.1.0.1.

In order to install the SSP for AES 10.1.x.x, you must use the new command ("av-update-os") and follow the detailed instructions in PCN2140S.

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

Required artifacts for Application Enablement Services Release 10.1.x.x

Required artifacts for Application Enablement Services Release 10.1.3.2

Filename	PLDS ID	File size	S/W Version number	MD5 Checksum	Comments
aesvcs-10.1.3.2.0.13-servicepack.bin	AES00001016	309.12 MB (316,545 KB)	10.1.3.2.0.13	8e4f24bb36ab4d548fb3f87cae824752	Avaya Aura® Application Enablement Services 10.1.3 Service Pack 2 (AES 10.1.3.2.0.13) PCN: Please refer to PCN2139S for additional details.

Required artifacts for Application Enablement Services Release 10.1.3.1

Filename	PLDS ID	File size	S/W Version number	MD5 Checksum	Comments
aesvcs-10.1.3.1.0.49-servicepack.bin	AES00000976	322.96 MB (330,715 KB)	10.1.3.1.0.49	2407704745b3003fc2aad76ab11c8c6c	Avaya Aura® Application Enablement Services 10.1.3 Service Pack 1 (AES 10.1.3.1.0.49) PCN: Please refer to PCN2139S for additional details.

IMPORTANT NOTE: Starting 10.1.3.1, licensing for Communication Manager (CM) and Application Enablement Services (AES) will only work with 10.1.3.1 and higher version of System Manager (SMGR) or Standalone WebLM (WebLM). If upgrading CM and/or AES to 10.1.3.1 and higher then the required order of upgrade is imperative i.e. SMGR and/or WebLM should be upgraded to 10.1.3.1 and higher first to ensure licensing for CM and/or AES does not stop working. CM and AES 10.1.3.0 were originally compatible with Standalone WebLM 10.1.2.0 (as there was no Standalone WebLM 10.1.3.0), however beginning with 10.1.3.1 and higher, Standalone WebLM 10.1.3.1 and higher is required for CM and AES. 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).

Required artifacts for Application Enablement Services Release 10.1.3

Filename	PLDS ID	File size	S/W Version number	MD5 Checksum	Comments
aesvcs-10.1.3.0.0.11-featurepack.bin	AES00000968	323 MB (338182.93 KB)	10.1.3.0.0.11	ad1ae696177b1e6998401d1267fb7dd2	Avaya Aura® Application Enablement Services 10.1 Feature Pack 3 **(AES 10.1.3.0.0.11)** **PCN:** Please refer to PCN2139S for additional details.

Required artifacts for Application Enablement Services Release 10.1.2

Filename	PLDS ID	File size	Version number	Comments
aesvcs-10.1.2.0.0.12-featurepack.bin	AES00000957	282 MB (295239.332 KB)	10.1.2.0.0.12	Avaya Aura® Application Enablement Services 10.1 Feature Pack 2 **(AES 10.1.2.0.0.12)** **MD5 Checksum:** cc2f7414e2069176d679024c7f8a3c7f **PCN:** Please refer to PCN2139S for additional details.

Required artifacts for Application Enablement Services Release 10.1.0.2

Filename	PLDS ID	File size	Version number	Comments
aesvcs-10.1.0.2.0.12-servicepack.bin	AES00000931	317.47 MB (325,095.29 KB)	10.1.0.2.0.12	Avaya Aura® Application Enablement Services 10.1 Service Pack 2 **(AES 10.1.0.2.0.12)** **MD5 Checksum:** 866e81a2f3b8fa968987f64dfde83971 **PCN:** Please refer to PCN2139S for additional details.

Required artifacts for Application Enablement Services Release 10.1.0.1

The following section provides Application Enablement Services downloading information.

Filename	PLDS ID	File size	Version number	Comments
aesvcs-10.1.0.1.0.7-servicepack.bin	AES00000907	229.41 MB (234,923.950 KB)	10.1.0.1.0.7	Avaya Aura® Application Enablement Services 10.1 Service Pack 1 **(AES 10.1.0.1.0.7)** **MD5 Checksum:** b471dfa103606fd6a7f7b5c3e8e51dd7 **Note:** This is a mandatory patch which needs to be installed after the 10.1 OVA or ISO installation. **PCN:** Please refer to PCN2139S for additional details.

Required artifacts for Application Enablement Services Release 10.1

The following section provides Application Enablement Services downloading information.

Filename	PLDS ID	File size	Version number	Comments
AES-10.1.0.0.0.13.20221201-e70-00.ova	AES00000870	2469.88 MB (2,529,160 KB)	10.1.0.0.0.13	Avaya Aura® Application Enablement Services 10.1 OVA Media **MD5 Checksum:** 4b21d1450163e30d8ff4d68414e378e0 **PCN:** Please refer to PCN2139S for additional details.
~~AES-10.1.0.0.0.11.20211130-e70-00.ova~~	~~AES00000870~~	~~2,405.08 MB (2,462,810 KB)~~	~~10.1.0.0.0.11~~	~~Avaya Aura® Application Enablement Services 10.1 OVA Media~~ ~~**MD5 Checksum:** b954f1c6db0c26a6dd0744071a119cec~~ ~~**PCN:** Please refer to PCN2139S for additional details.~~

Filename	PLDS ID	File size	Version number	Comments
Swonly-10.1.0.0.0.11-20211130.iso	AES00000871	523.91 MB (536,496 KB)	10.1.0.0.0.11	Avaya Aura® Application Enablement Services 10.1 Software Only ISO **MD5 Checksum:** f168063ae72b6e61084f72f066a8251c **PCN:** Please refer to PCN2139S for additional details.
Aesvcs-10.1.0.0.2-superpatch.bin	AES00000897	148.75 MB (152,321.45 KB)	10.1.0.0.2	Avaya Aura® Application Enablement Services 10.1 Aura® Super Patch 2 (Please refer: **PSN020545u**) **Note:** This patch is deprecated and removed from the Avaya Support website. If this patch is already installed then you have to install ***AES 10.1 Service Pack 1 (AES 10.1.0.1.0.7)*** **MD5 Checksum**: 1cb8cfb887a63fbb3d42423b9f1e5100
aesvcs-10.1.0.0.1-superpatch.bin	AES00000872	126.61MB (1,29,649.96 KB)	10.1.0.0.1	Avaya Aura® AE Services 10.1 Aura® Super Patch 1 **Note:** This patch is deprecated and removed from the Avaya Support site. If this patch is already installed then you have to install ***AES 10.1 Service Pack 1 (AES 10.1.0.1.0.7)*** **MD5 Checksum:** 57045d4e6cd6efed99ed34736ea0ebbc

Note: The old 10.1 GA OVA contains the Avaya Signing certificate that is going to expire on Feb 20, 2023. Therefore, to address the Avaya signing certificate expiry, the new 10.1 GA OVAs are renewed and re-signed with the latest Avaya signed certificates. The new OVAs are also updated to support SHA256 hash algorithm. For more information, see PCN2139S.

For more information, see PSN020586u - Avaya Aura® OVA Certificate Expiry February 2023.

Required patches for Application Enablement Services Release 10.1

AES 10.1 Service Pack 1 (AES 10.1.0.1.0.7) contains CRITICAL bug fixes. It is also required for application of all AES 10.x Security Service Packs.

If AES 10.1.0.1.0.7 is not applied, installation of any AES 10.x Security Service Pack will fail.

For information about patches and product updates, see the Avaya Technical Support Website https://support.avaya.com. For more details, see PSN020545u on the Avaya Technical Support site.

Installation for Avaya Aura® Application Enablement Services Release 10.1.x.x

Installation for Avaya Aura® Application Enablement Services Release 10.1

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 10.1.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 10.1.x
- Deploying Avaya Aura® Application Enablement Services in a Software-Only and Infrastructure as a Service Environments Release 10.1.x
- Upgrading Avaya Aura® Application Enablement Services Release 10.1.x

Note: 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 10.1.x.x

Upgrading to AE Services 10.1.3.2

An upgrade to AES 10.1.3.2 can be achieved by upgrading existing 10.1.3 or 10.1.3.1 systems to AES 10.1.3.2 using the service pack installer aesvcs-10.1.3.2.0.13-servicepack.bin

Upgrading to AE Services 10.1.3.1

An upgrade to AES 10.1.3.1 can be achieved by upgrading existing 10.1.3 systems to AES 10.1.3.1 using the service pack installer aesvcs-10.1.3.1.0.49-servicepack.bin

Note: Systems prior to 10.1.3 must be upgraded to 10.1.3 first and then to 10.1.3.1.

Upgrading to AE Services 10.1.3

An upgrade to AES 10.1.3 can be achieved by upgrading existing 10.1 or 10.1.0.1 or 10.1.0.2 or 10.1.2 systems to AES 10.1.3 using the feature pack installer aesvcs-10.1.3.0.0.11-featurepack.bin

Upgrading to AE Services 10.1.2

An upgrade to AES 10.1.2 can be achieved by upgrading existing 10.1 or 10.1.0.1 or 10.1.0.2 systems to AES 10.1.2 using the feature pack installer aesvcs-10.1.2.0.0.12-featurepack.bin

Upgrading to AE Services 10.1

Important:

6.x and 7.x versions are only supported in the transient period when upgrading the Avaya Aura® solution.

AE Services Server Upgrade Instructions

Please refer to "Upgrading Avaya Aura® Application Enablement Services" for detailed instructions.

RHEL 8.4 Support for AE Services 10.1

AE Services 10.1 is supported on RHEL 8.4. Upgrading AE Services 10.1 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 10.1.x.x

Please see, *Deploying Avaya Aura® Application Enablement Services in Software-Only and Infrastructure as a Service Environments Release 10.1.x* and *Upgrading Avaya Aura® Application Enablement Services Release 10.1.x*.

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 10.1.x.x

- Certificates become invalid after migrating to Avaya Aura® Application Enablement 10.1, for more details please refer to PSN020555u
- When Avaya Aura® Communication Manager is upgraded to 10.1 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

Starting 10.1.3.1, licensing for Communication Manager (CM) and Application Enablement Services (AES) will only work with 10.1.3.1 and higher version of System Manager (SMGR) or Standalone WebLM (WebLM) . If upgrading CM and/or AES to 10.1.3.1 and higher then the required order of upgrade is imperative i.e. SMGR and/or WebLM should be upgraded to 10.1.3.1 and higher first to ensure licensing for CM and/or AES does not stop working. CM and AES 10.1.3.0 were originally compatible with Standalone WebLM 10.1.2.0 (as there was no Standalone WebLM 10.1.3.0), however beginning with 10.1.3.1 and higher, Standalone WebLM 10.1.3.1 and higher is required for CM and AES. 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).

Interaction between McAfee Antivirus and Executables

It has been observed that the following AES SDK files for Windows do not install successfully when McAfee Antivirus is installed on the system:

cmapijava-sdk-10.1.0.0.0.12.exe

cmapixml-sdk-10.1.0.0.0.12.exe

dmcc-dotnet-sdk-10.1.0.0.0.110.exe

smssvc-sdk-10.1.0.0.0.12.exe

jtapi-sdk-10.1.0.0.0.12.exe

Customers may attempt to add these to the exclusion list on the McAfee Application.

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: Microsoft OCS/Lync, IBM Sametime, Avaya Aura Contact Center)		**DMCC (First Party call control)**		**TSAPI/DLG/CVLAN**
Footprint	**Resources**	**Maximum # of users or agents**	**Maximum BHCC**	**Maximum # of users or agents**	**Maximum BHCC**	**Maximum Messages per second (MPS) Rate**
Small	1 CPU, 4 GB RAM 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 10.1.x.x

Fixes in Application Enablement Services in Release 10.1.3.2

ID	Minimum Conditions	Visible Symptoms	Issue found in Release
AES-32938	AES 10.1.2	TSAPI service may crash while trying to acquire TSAPI license from WebLM.	10.1.2.0.0
AES-32910	AES 10.1.3.1	TSAPI Test in OAM diagnostics not working.	10.1.3.1.0

ID	Minimum Conditions	Visible Symptoms	Issue found in Release
AES-32906	AES 10.1.2 or higher	AES TSAPI service might crash while trying to renew license with WebLM.	10.1.3.0.0
AES-32901	Agent transferring call to VDN/Vector/hunt and call been queued to skill as agents are not available.	CTI side doesn't get correct state for the connected party in the call.	10.1.3.0.0
AES-32818	Add/Edit DLG link.	DLG service summary was showing the information. It was blank.	10.1.3.1.0
AES-32814	AES 10.1.3.1	TSAPI link status will be down.	10.1.3.0.0
AES-32504	Enable WebLM logs on AES.	Disk space utilization due to WebLM logs	10.1.0.2.0
AES-32488	Security scan run on AES 8.x or 10.x	Scan reports the vulnerability with respect to log4j-1.x present on the server.	8.1.3.5.0
AES-32296	AES 10.1.3.1	If ToneDetection monitor is placed, then AES may send same tone detected event twice.	10.1.3.0.0
AES-32226	AES 10.1.x SELinux Enabled server with newly created security user.	User cannot login using EASG account on OAM as the challenge is not thrown.	10.1.0.2.0
AES-31777	AES 10.1.0.1	The enabled ports were disabled after AES10.1.0.2 update.	10.1.0.1.0
AES-31529	10x versions of the DMCC .NET library	Unable to use in an environment that requires all assemblies to be strongly named.	10.1.0.0.0
AES-31054	Re-installation new valid License on WebLM.	DMCC License mode is in License_Expired mode on OAM even after installing new valid License on WebLM.	7.0.0.0.1
AES-30249	API GetDisplay, GetDeviceId, UnregisterTerminal invocation from DMCC .net SDK	Caught "Index was outside the bounds of the array." exception while performing an API call through NICE recorder.	8.1.0.0.0
AES-29836	TSAPI CLIENT/SDK 10.1.0.2	French characters are not shown properly of the EULA in InstallShield Wizard.	8.1.0.0.0
AES-29726	TSAPI CLIENT/SDK 10.1	Due to missing dependency, TSAPI client application shows error message as msvcr100.dll missing.	10.1.0.0.0

ID	Minimum Conditions	Visible Symptoms	Issue found in Release
AES-23159	Add device monitor from JTAPI	JTAPI crashes with null pointer exception while processing CSTA FAILED event having empty failing Device.	8.1.2.1.0

Fixes in Application Enablement Services in Release 10.1.3.1

ID	Minimum Conditions	Visible Symptoms	Issue found in Release
AES-32152	Run the SMS queries using SMS test utility page of AES or any SMS application.	SMS applications fails to work intermittently and error states that the Maximum Connections are in use.	10.1.0.2.0
AES-32064	AES 10.1 and snmpTrapReceiver utility.	When command line utility snmpTrapReceiver is used to add the SNMP Trap Receiver, it adds the wrong Security Name with all letters in Lower Case even after name is given in mixed or upper case.	10.1.0.1.0
AES-32063	AES 8.1.3 CM 8.1.3 Application performing Single Step Transfer	If Single Step Transfer request fails because of any reason, the originator station remains on hold as AES does not reattempt the SST request.	8.1.3.0.0
AES-32021	AES 10.1 and frequent ICMP ping request from other server/applications.	ICMP Ping requests to AES are dropped, so monitoring tools reports intermittently that AES is down.	10.1.0.0.0
AES-31935	DMCC services getting used and dmcc-logging.properties file is modified through CLI or DMCC logging level is changed from AES OAM.	DMCC services gets restarted after 4-5 days.	10.1.0.2.0
AES-31776	AES 10.1 reboot	If AES is rebooted, False High Memory Usage Alarm is generated.	10.1.0.2.0
AES-31568	AES 10.1, 8.x TSAPI Client using TLSv1	Clients Application could not connect to AES	10.1.0.2.0
AES-30039	AES SMS service in 10.1.	SMS query do not generate any result if there is segfault in ossicm process, the logs are not logged to the ossicm.log file . The information is only seen while running journalctl -f.	10.1.0.1.0
AES-31836	SMS test tool xml version and run the	SMSXML application will not be able to use TrunkGroup model.	10.1.0.2.0

ID	Minimum Conditions	Visible Symptoms	Issue found in Release
	TrunkGroup model with List operation.		
AES-28716	Security Scan	The JsessionID cookie in HTTP response remains same, after successful login to AES.	8.1.3.2.0

Fixes in Application Enablement Services in Release 10.1.3

ID	Minimum Conditions	Visible Symptoms	Issue found in Release
AES-31831	AES 10.1.2	For Enterprise wide licensing configuration, the Master WebLM was not able to push the ALF file to the local WebLM on AES.	10.1.2.0.0
AES-31481	8.1 AES with 8.1.3.4 patch or above.	mDNS service is enabled on AES system on port 5353.	8.1.3.4.0
AES-31333	SMS application and AES.	Intermittent connection error while doing SMS query on application side.	10.1.0.2.0
AES-31279	Linux machine and tsapi and cvlan 64 bit client binaries.	Failed to install TSAPI & CVLAN Client 64 bit Linux binary with error "Expected version of glibc rpm is not present on system. Please install 32-bit version of glibc rpm."	8.1.3.0.0
AES-31203	AES 10.1.0.2 and DMCC Java Client older than 10.1.0.2	After upgrading AES from 10.1.0.1 to 10.1.0.2, the application is no longer able to receive GetDisplayResponse responses to GetDisplay requests.	10.1.0.2.0
AES-31149	AES 8.1.3.6	DTMF tone events are not sent to clients if DMCC station re-registers after monitor is placed.	8.1.3.0.0
AES-30893	AES 8.1 or later. TSAPI client.	DistributingVDN parameter will be empty in CstaDelivered or subsequent events, if call is transferred to monitored VDN.	8.1.3.1.0
AES-30149	AES 10.1.0.1	AES SNMP traps are not send to the configured SNMP trap receiver.	10.1.0.1.0
AES-29927	Voice Unit service APIs called.	When a recording is done by DMCC station using server mode, the recorded files fail to play.	8.1.0.0.0
AES-29293	SMGR signed Certs are used with "server" alias on AES with GRHA Configured.	AES HA Status on OAM shows as "Far End Unreachable".	10.1.0.0.0

Fixes in Application Enablement Services in Release 10.1.2

Key	Minimum Config	Customer Visible Symptom
AES-19692	Upgrading TSAPI client & SDK from 8.1 to newer release.	The new version of TSAPI client installed on top of old version the log4cx.dll is not get replaced and it causes TSSPY crash.
AES-24091	JTAPI 6.3.3	If Conferenced Event was received before SnapshotCallConfEvent of the previous delivered event in a scenario where the conferencing party is not being monitored by JTAPI, then it lead mismatched UCID causing the call to fail
AES-26647	AES 8.1.3.2	If the password field is kept empty while modifying the user then the user modification fails from OAM -> user Management
AES-27808	AES 8.1.3.1/ AES-10.1	CTI application don't see CSTA_MONITOR_ENDED (Call Monitor Ended) event for the monitored call after complete call disconnection.
AES-28138	AES 8.1.3.1	The CTI application saw few CAG members ringing forever and thus were not getting new calls.
AES-28405	AES 10.1	If in server certificate(CM) extended key usage contains clientAuth as first parameter certificate validation is failing.
AES-28446	AES 10.1	Server certificate is validated against clientAuth, but it has to validate against serverAuth. So if server (AES) was sending certificate with extended key usage parameter as serverAuth the certificate validation was failing.
AES-28489	AES 10.1	If extended key usage is not enabled in client certificate the certificate validation is failing
AES-28610	AES 10.1	Unused login audit' fields in OAM > Security > Audit could not be changed
AES-29261	8.1.3.4 GRHA	AES super patch , service patch or feature patch installation on AES GRHA pair fails.
AES-29296	64-bit version TSAPI client	TSAPI Exerciser crashes and become unresponsive if try to create Route Table for 64 bit client version
AES-29768	AES 10.1	SSH was working with weak CBC ciphers. Below commands when executed from the external systems, were able to login to AES. ssh -c aes128-cbc <user>@<AES_IP> or ssh -c aes256-cbc <user>@<AES_IP>
AES-29775	TSAPI ASL 10.1 SDK	TSAPI ASL exerciser 10.1 crashes while trying to setup ASL session with getPrivilegereequest()
AES-29822	AES 10.1 and LDAPS is disabled on AES OAM-> Security ---> Standard Reserved Ports page.	NMAP command output shows the port 636 open though it is disabled.
AES-29849	AES 8.1.3 with TSAPI client.	CstaClearConnection request will fail, if application will use dynamic deviceID present in CstaEstablished event.

Key	Minimum Config	Customer Visible Symptom
AES-30043	Telephony Web Service used.	When TWS URL is accessed on AES 8.1.3.1 or earlier version. It would show message "Axis is running". https://[ID_ADDRESS]/axis/services/TelephonyService However, from AES 8.1.3.2 onward it is showing SOAP error which is false positive.
AES-30046	DMCC dashboard 10-1	DMCC dashboard fails to perform ASL handshake with DMCC
AES-30051	AES 10.1 and DMCC client	It fails to generate DFMF warning tone on the call when the 3rd party call control API request is generated to generate a tone on the calls using CTI application
AES-30076	AES 8.1.2.0 or later with external ldap configuration.	/var/log/sssd/ldap_child.log file will not rotate. It may cause disk space exhaustion.
AES-30145	DMCC Voice Unit service being used CTI application and SERVER Media mode is used.	AES/DMCC application fails to play valid recorded file after same application attempts to play invalid file.
AES-30227	AES 10.1.0.2	garbage value present in EULA of CMAPI SDK installation.
AES-30233	AES 8.1.3.3	AES reports wrong disk name in the Disk Full Alarm. The trapVarbinds logs and alarm reports the /dev/mapper/rhel-var_log_audit disk as full while the disk which is actually filled is /dev/mapper/rhel-var_log .
AES-30236	DMCC registration attempted with CM without Media Resources.	DMCC registration fails with GENERIC ERROR specifying no reason for registration rejection.
AES-30527	AES 10.1 OVA with AES 10.1.0.1 and AES 10.1.0.2 installed	LDAP users were not able to login to AES OAM

Fixes in Application Enablement Services in Release 10.1.0.2

Key	Minimum Config	Customer Visible Symptom
AES-28220	AES 8.1.3.1	The CTI application at the customer did not see trunk side information in CSTA confirmation event for Single Step Conference hence it didn’t show the actual number of parties in the call.
AES-29649	AES 8.1.3.4, CM 8.1.3	The CTI application did not get notified of the call ended event at call termination.
AES-29717	AES 8.1.x or later release with ECD enabled and multiple queue-to-skill steps in call surplus.	Uneven call distribution to skills in Monitor mode which was different in behavior when compared with in Full mode.
AES-28525	AES 10.1, CM 10.1, CVLAN Client 10.1	Call dropped so call route to agent failed because, caller call to VDN resulted into adjunct route to CVLAN client for which it sent Route Select Request to AES and received Abort message.

Key	Minimum Config	Customer Visible Symptom
AES-22774	AES 8.1.1	CTI application did not receive CSTA Diverted and CSTA Established events if call is answered by bridge station of the called station
AES-27690	AES 8.1.3	Missing Service Observer Activate, Service Observer Deactivate and Query Service Observer API support in GetAPICapsConfEvent.
AES-28930	AES 10.1	Deleting default server certificate using serverCertificates API failed with an error code 18
AES-29279	AES-10.1.0.1	TWS request failed on port 8443/8080 as the ports were closed however OAM showed that the ports are open.
AES-29774	AES 10.1.0.1	The ports which were enabled on AES were disabled after upgrading to 10.1.0.2 Service Pack.
AES-27310	AES 8.1.3	The agent was receiving dual ringing event from JTAPI for every Single Step Transfer.
AES-28598	AES-8.1.3.2 and JTAPI 8.1.3.0	When Conference call was done from CRM, CRM panel displays it as a "Normal Call" between two parties in spite of "Conference"
AES-29420	AES 8.1.3.1	The CTI application at the customer site saw trunk side information missing in CSTA confirmation event for Single Step Conference. Hence was not getting actual number of parties in the call.
AES-28810	AES-8.1.3, JTAPI-8.1.3	JTAPI query getLoggedOnAgents() returned wrong results. It returned agent info not belonging to skill in query.
AES-28195	AES 8.1.2	While creating a CSR from OAM -> Security -> certificate Management, all the key usage and extended key usage values were not getting added to the CSR
AES-29186	AES 8.1.3.4	AES changing external num from EXPLICIT_PRIVATE_UNKNOWN to EXPLICIT_PRIVATE_LOCAL_NUMBER in ATT_SINGLE_STEP_CONFERENCE_CALL. Also, in the ATT_SINGLE_STEP_CONFERANCE_CALL_CONF event the number of connection count was wrong.
AES-29675	AES 8.1.3.5	AES missed sending CSTA_DELIVERED in SST call scenario.
AES-28212	10.1 TSAPI SDK/CLIENT	Redistributable.txt was missing from TSAPI and CVLAN Clients and SDKs install directory.
AES-28240	JTAPI 8.1.3	When the JTAPI Client received an event it made many CSTAQueryDeviceInfo requests to AES which caused the DistributeCSTAEvent thread to block until it received a response which resulted in application hung state.

Key	Minimum Config	Customer Visible Symptom
AES-29330	AES 10.1.0.0.2	SMS hunt group list query sent to CM failed with a segfault
AES-29726	TSAPI CLIENT/SDK 10.1	Due to missing dependency TSAPI client application showed error message as msvcr100.dll missing.
AES-29062	AES 10.1.0.1	The "User Management" tab will not be visible on the OAM after uninstalling service pack because of failed slapd service.
AES-29839	AES 10.1	The below command will showed the wrong OID: snmptranslate -m /usr/share/snmp/mibs/AV-CORE-SERVICES-MIB.txt -On -IR csMemoryUtilisation
AES-29648	AES 8.1.3.2	When starting a session without credentials, the error code returned was 500 instead of 401
AES-22651	AES 8.1.3 Standalone or AES 8.1.3 GRHA Setup required	On a Standalone AES, after deleting default users and restarting aesvcs service, the deleted default users were restored.

Fixes in Application Enablement Services in Release 10.1.0.1

ID	Minimum Conditions	Visible Symptom
AES-29062	AES 10.1.0.1	After uninstalling 10.1.0.1, slapd service will not come up. Because of this, the "User Management" tab will not be visible on the OAM.
AES-28759	Install feature / service pack on AES 10.1.	Tomcat version before installing FP/SP is 9.0.43 and after is 8.5.57.
AES-28525	AES 10.1, CM 10.1, CVLAN Client 10.1	Caller call to VDN resulted in adjunct route to CVLAN client for which it sends Route Select Request to AES and receives Abort message due to which call dropped and call route to agent failed.
AES-28489 AES-28446 AES-28531	Migration from AES 8.1.x to AES 10.1	Under certain conditions when certificates did not contain the correct Key Usage or Extended Key usage parameters,10.1 TSAPI and 10.1 DMCC CTI apps failed to establish connections with 10.1 AES server ***Changes have been made to 10.1.0.1 AES and the following new 10.1.0.1 artefacts have been released to address this issue*** 1. AES00000910 - DMCC dotNet SDK 10.1.0.1 2. AES00000911 - TSAPI Client 32-Bit Linux R10.1.0.1 3. AES00000912 - TSAPI Client 64-Bit Linux R10.1.0.1 4. AES00000913 - TSAPI Client 32-Bit MS Windows 10.1.0.1 5. AES00000914 - TSAPI Client 64-Bit MS Windows 10.1.0.1

ID	Minimum Conditions	Visible Symptom
		Refer to PCN 2139S and support.avaya.com for more instructions on using the new artefacts
AES-28405	Migration from AES 8.1.x to AES 10.1	If extended key usage contains “clientAuth” as the first parameter within the CM server certificate, certificate validation and, consequently, connectivity between CM and AES failed.
AES-28350	AES 8.1.2	AES 8.1.3.1 runs out of crossrefIDs and will require a reboot to recover.
AES-28347	Import SDB file attached.	500 Bad Gateway is displayed
AES-28261	Importing Server Certificate via pending CSR in AES10.1.	After importing Server Certificate via CSR, the following issue is observed: [root@aes101logs]# ll /opt/coreservices/avaya/certs/pfxs/aeservices.pfx -rw------- 1 tomcat5 avcertmgmtgrp 3018 Nov 16 09:36 /opt/coreservices/avaya/certs/pfxs/aeservices.pfx Expected privileges :- [root@aes60~]# ll /opt/coreservices/avaya/certs/pfxs/a*.pfx -rw-r--r-- 1 tomcat5 avcertmgmtgrp 3730 Nov 16 16:00 /opt/coreservices/avaya/certs/pfxs/aeservices.pfx
AES-28257	AES 8.1.2.0.0.9	The command to add an SNMP Agent returns code 9.
AES-28251	Have an expired WEB certificate imported in AES 8.1.	A false "LDAP certificate" expiry alarm is triggered, after a WEB certificate is expired
AES-28233	AES 8.1.3 GRHA	When the database is restored after HA configuration, interchange and synchronize work for the first time, but fail the next time.
AES-28220	AES 8.1.3.1	The CTI application at the customer saw trunk side information missing in CSTA confirmation event for Single Step Conference. Thus, not getting actual number of parties in the call.
AES-28138	AES 8.1.3.1	The CTI application saw few CAG members ringing forever and thus were not getting new calls.
AES-27946	TWS CTI application (at customer setup) is not preserving the sessions between each TWS request and hence new sessions are created as the default TWS behavior.	OAM access gets denied with error "Bad Gateway" intermittently.
AES-27808	AES 8.1.3.1/ AES-10.1	CTI application don't see CSTA_MONITOR_ENDED (Call Monitor Ended) event for the monitored call after complete call disconnection.

ID	Minimum Conditions	Visible Symptom
AES-27260	AES 8.1.3.2	The DMCC application at the customer faced service disruption for few mins regularly. This happened when a bunch of DMCC stations registering and making calls played WAV files present on AES. Problem was seen at the calls termination when devices monitors stopped un-registering devices.
AES-26647	AES 8.1.3.2	If the password field is kept empty while modifying the user then the user modification fails from OAM -> user Management

Fixes in Application Enablement Services in Release 10.1

ID	Minimum Conditions	Visible Symptom
AES-28229	Migration from 6.3.3 to 10.1	User Management tab was not visible after migration from 6.3.3 to 10.1
AES-27809	AES 8.1 and JTAPI 8.1 client. CM 8.1 with AMS as media resource. Inbound trunk call is transferred from one agent to another agent.	JTAPI application gets CS_NONE state of Off-PBX party or trunk party in Call.getConnections response and JTAPI sends Unknowns events for Off-PBX Extension when it receives CSTA Delivered event.
AES-27684	AES 8.1.3.4	asai_trace incorrectly parses AuditResponse message
AES-27648	AES 8.1.3.3	Not able to configure GRHA
AES-27634	8.1.3.2 with GRHA and FIPS enabled	Interchange was not successful in GRHA
AES-27575	AES 8.1.3.2	/var/log/avaya/aes/dmcc-trace.log logs are not getting compressed with logrotate.
AES-27548	AES 8.1.3.0.0 customer trunk IVR	Local Recorder is getting identified as remote trunk party (with dynamic ID as T#...) when station reconnects the customer call.
AES-27545	AES 8.1.3.2, CM 8.1.3	Call status showing as unknown on JTAPI Application
AES-27515	AES 8.0.1.0.0	/var/log/avaya/aes/TSAPI/g3trace.out and /var/log/avaya/aes/TSAPI/csta_trace.out logs were not rotated even though it fell in the criteria mentioned in /etc/logrotate.d/mvapLogrotate.conf
AES-27260	AES 8.1.3.2	The DMCC application at the customer faced service disruption for few mins regularly. This happened when a bunch of DMCC stations registering and making calls played WAV files present on AES. Problem was seen at the calls termination when devices monitors stopped un-registering devices.
AES-26984	AES 8.1.2, CM 8.1.2	SelectiveListenHold request failing with Universal Failure Resource Out of Service
AES-26970	AES 8.1.11	Failed to connect AES on secure link.

ID	Minimum Conditions	Visible Symptom
AES-26949	AES 8.1.3.0.0	/var/mvap/database was reaching 80% of the space frequently. Hence, customer was seeing "O_AMON-00002 "High disk utilization. /dev/mapper/rhel-var_mvap_database 80 percent used." alarm.
AES-26890	AES 8.1.3, CM 8.1.3	ACRA application crashes while processing Single Step Conference
AES-26876	AES 8.1	tsapiRouteRegister command failed in RTT for non-ECD scenario.
AES-26854	AES 8.1.3	Configuring GRHA resulted in error.
AES-26823	AES 8.1.3	Customer could see linking error for "oss shippable" header file after client installation.
AES-26822	AES 8.1.11	haConfigUtil script failed to configure WebLM servers during HA configuration
AES-26820	AES 8.1.3	32-bit rpms were present in 64-bit Linux client SDK package
AES-26704	AES-7.x	SNMPv3 traps were not sent on the SNMP receiver
AES-26701	AES 8.1.2 with secure H.323 connection	The DMCC service stopped working when secure H.323 connection was enabled.
AES-26699	AES 8.1.3, CM 8.1.3	Station Type shown as unknown in Endpoint Registered Event when J100 series type phone was registered on CM.
AES-26692	AES 8.1.3.2 GRHA	When uninstalling FP 8.1.3.2 in a GRHA system, aesvcs was stuck in activating mode on the primary server and was in inactive mode on the secondary server.
AES-26691	AES 7.1.3.4	When the user tries to import a Server certificate in the pfx format with multiple friendly names, then "Multiple Key Entries" error is displayed.
AES-26686	AES 8.x with CM 8.x	SMS only reported data for 995 CORs for Calling Permission and Service Observing Permission
AES-26665	AES 8.1.3	/var/log/secure logs were not rotated even though they adhered to the criteria mentioned in /etc/logrotate.d/securelogrotate
AES-26652	AES 8.1.3.2 GRHA	The license was in failed state after WebLM hostname was disabled on Licensing -> WebLM Server Address -> Enable Certificate Hostname Validation
AES-26559	SMS on AES-8.x	When a Vector was configured with a “disconnect“ step on CM, SMS incorrectly sent CollectAfterAnnouncement field which was not configured for disconnect command
AES-26542	While registering endpoint "IP Video Softphone?" field enabled on station form and "Allow Direct-IP Multimedia?" disabled on the "ip-codec-set" form in Communication Manager.	DMCC registrations were failing.

ID	Minimum Conditions	Visible Symptom
AES-26338	AES 8.1.3, 64-bit Linux SDK.	When running 8.1.3 TSAPI SDKs on Linux 64bit environment, customers could see empty strings in client connection confirmation events for apiVer, libVer, tsrvVer, drvrVer
AES-26182	Standard Reserved Port 8443 is enabled, TWS SDK - telSvcGuiClient sample app, AES>=7.1.3.6 (any supported combinations with TWS SDKs)	java.net.ConnectException was seen when TelSvcGuiClient sample app was run with 'Use SSL' checkbox selected i.e. when it tried to connect to TWS over secure port 8443
AES-24871	AES 8.1.2	If the user clicked on Help link on confirmation pages for clear logs, clear traces or retention period change pages on OAM, then the help page gave error "Page not found"
AES-24870	AES 7.1	If multiple interfaces were configured on AES then SMS IP configured in wsdl files was incorrect
AES-24857	AES 8.1.3	If the SDB backup had apostrophe marks in some of the entries, the importSDB failed with wrong attributes of some CTI Users.
AES-24790	CM-6.x and above with any AES	Display Trunk Group Query did not display Signaling Group field
AES-24538	DMCC Logging set to FINEST on AES 8-1-3-1 onwards & ASL application connecting to AES	AES 8.1.3.1 onwards , AES DMCC FINEST logging causes issues with ASL clients such as ACR/EMC/Oceana/EP/APC/ACR etc. to fail to establish connection with AES due to invalid nonce error.
AES-24486	TSAPI and CVLAN Client 10.1 and SDK 10.1	TSAPI and CVLAN Client and SDK version shown as 8.1.3.
AES-24373	A system with AES 8.1.3 should be present.	/var/log/wtmp* and /var/log/btmp* logs were not rotating as per the configuration present in /etc/logrotate.conf
AES-24202	AES 8.1.3.0.0 with securemode enabled	DMCC license was in error mode when the secure mode was enabled on AES 8.1.3.0
AES-24201	AES 8.1.3 FP system with Secure Mode is required.	After enabling Secure Mode in AES 8.1.3 FP, if the customer is upgrading to AES 8.1.3.1 or AES 8.1.11, SSHD service will not start.
AES-24166	AES 8.1	While upgrading software only system using FeaturePack or Servicepack ".bin" file the SOHD rpm failed to install.
AES-24160	AES 8.1.X TSAPI/DMCC application	Application received negative ack with cause RESOURCE_BUSY for ATTSingleStepConference request.
AES-24157	AES 8.1.3	When the default Server certificate was deleted from the OAM then upon the next restart of slapd service, the service didn't start. Due to this, the "User Management " tab is not visible in OAM.

ID	Minimum Conditions	Visible Symptom
AES-24132	AES 8.1.3, CM 8.1.3	In an ECD environment, "Add Skill Request" for both ECD and non-ECD controlled skills failed with cause OBJECT_NOT_KNOWN.
AES-24090	AES 8.1.3.1 should be available.	After restarting the AES Server, false "High CPU" alarms will get generated.
AES-23954	AES 8.1.3 GRHA with virtual IP	When Virtual IP configured in GRHA hostID change and because of that license went into grace period.
AES-23767	AES 8.1.3 GRHA	If an SNMP trap receiver was configured, all alarms from primary and secondary system were received. When customer logged into AES, the database on primary was updated and restored on the secondary database which restarted DBService on secondary and generated an alarm for DBService.
AES-23682	AES 8.1.2.1	When AE Services was upgraded to 8.1.2.1 or later, the HostID utilized by the embedded WebLM was changed. The original license was no longer valid since it was based on a different HostID. The system entered a 30-day license error grace period.
AES-23193	AES 7.1.3.6 with email notification configured	From OAM, if a user configured email notification using "Utilities --> Email Notifications", then the test email worked but the actual utility once configured did not send any alerts on email.
AES-22782	CMAPI Java SDK 8.1.3	Softphone sample app in cmapi-java sdk was not performing hostname validation for certificate as expected when TLS hostname validation was set to TRUE
AES-21502	8.1.3.2 GRHA	OAM page said 'Service Unavailable' despite tomcat restart.
AES-21271	AES 7.1.3	Tripwire shows a large number of modified files after installation of a Superpatch or ServicePack. As a result, the tripwire database needed to be re-initialized
AES-20815	AES 8.1.2	While adding an NTP server using OAM, if there was default RHEL NTP entries such as "server 0.rhel.pool.ntp.org iburst" present, then the new NTP server did not get added and a validation failure message was displayed.
AES-19204	Install any available 8.1.x FP.	While installing the FP, following errors were displayed: sed: -e expression #1, char 1: unknown command: `,' sed: -e expression #1, char 1: unknown command: `,' uid=515(ldap) gid=515(ldap) groups=515(ldap),504(avcertmgmtgrp) FirewallD is not running The service command supports only basic LSB actions (start, stop, restart, try-restart, reload, force-reload, status). For other actions, please try to use systemctl.
AES-19032	AES 6.3.3	If the application started a monitor on a call before monitoring the skill, calls to GetAgentLogin failed. This was because the DMCC module on AES threw an exception

ID	Minimum Conditions	Visible Symptom
AES-16099	AES 7.0.1.0.3	Call recording in ACR failed when caller device ID type was changed from explicitPrivateUnknown to implicitPublic.

Fixes in Application Enablement Services in Release 10.1 Super Patch 2 (PSN020545u)

ID	Minimum Conditions	Visible Symptom
AES-28319	AES 10.1 GRHA	Interchange and sync failed on GRHA 10.1
AES-28362	AES 10.1	"swversion" do not show Patch details when executed using cust user
AES-28435	AES 10.1	Upgrade log4j to 2.16. For more details please refer PSN020551u for more details
AES-28336	AES 10.1 and CM with Secure H323 Enabled	DMCC registration fails when "Secure H.323" is enabled. Please refer PSN020546u for more details

Known issues and workarounds in Application Enablement Services 10.1.x.x

Known issues and workarounds Application Enablement Services in Release 10.1.3.2

ID	Minimum Conditions	Visible Symptoms	Workaround
AES-32922	Apply SP or FP on 10.1 systems with removed default lab-only certificates.	Lab-only Default certificates added back after FP/SP Installation	Manually remove the lab-only default certs.
AES-32455	Create a new user with security profile set to change password on first login	User is not prompted to change password on first login	Change the password through CLI first.
AES-32308	AES 10.x	Errors related to connection to alarming.esp.avaya.com are logged in /var/log/messages	modify the below file /opt/spirit/config/agent/ SPIRITAgent_1_0_BaseAgentConfig_orig.xml <entry And change the below parameter to "false" key="SPIRIT.heartbeat.on">true</entry> ->
AES-32305	JTAPI 10.1 AES 10.1	JTAPI application may be come unresponsive, due to race condition among internal JTAPI threads.	No
AES-32299	AES 8.x AES 10.x	Alarm for /var/log disk utilization greater than 90%.	Cleanup old kernel.log from /var/log/avaya/aes/ directory
AES-31933 (SMGR-72838)	AES 8.1.x, SMGR 10.1.3, AES 10.1 OVA, AES 10.1.3 FP	The SDM only migrated to 10.1 OVA but did not install FP10.1.3.0.11.	Perform upgrade from AES 8.x to 10.1 first, and then apply the 10.1.3 patch explicitly using the patching section.
AES-31510	AES 10.1.0.2	After the JTAPI provider initialized the existing log4j setting of application shut downs.	No
AES-31202	JTAPI 10.1.x	A delay gets introduced in the JTAPI response when processing getLoggedOnAgents and ACD.addAddressListener API request which sometimes results in provider shutdown if the Q Size threshold (1000) is breached.	No
AES-31149	Add DMCC Tone event listener for device and reregister the device	Tone detected events are not received by application	No
AES-31143	AES 10.1.2	Editing the default user is failing from OAM -> User Management -> user Admin -> List all user -> Edit(any 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-31080	AES GRHA configured and CTI application subscribing for 3PCC Events.	CTI applications fails to updates state of the Call and Agent & doesn't work properly after GRHA fail-over.	Restart DMCC Service on AES or restart CTI application.
AES-30029	AES 10.1.0.x - GRHA Configured	AES 10.1.0.x - 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

ID	Minimum Conditions	Visible Symptoms	Workaround
AES-28813	AES 8.1.3.4.0.2: 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-28407	Workspaces build 1.19.143, AES 8.1.3, CM 8.1.3	Conference and transfer options are not visible on Agent.	No
AES-28193	One or more Service is stopped.	CTI link status for all services is shown as talking even if respective service is stopped	No
AES-28171	AES-8.1.2	An error "Cannot access the reference link" is generated on web browsers when URL "Comments on this documents?" is accessed on any help page of AES OAM	No
AES-27844	Invalid configuration of "WebLM IP Address/FQDN", "WebLM Port" and valid configuration of "Secondary WebLM IP Address/FQDN" and "Secondary WebLM Port" on "Licensing | WebLM Server Address" (OAM).	AE Services page showed License Information in red text as "Application Enablement Service is not licensed in the license file."	No
AES-27583	SNMP trap receiver configured	After migrating AES from 8.x to 10.1 the SNMP trap messages type and version displays v1 even if the SNMP version is 2c	Workaround: Login to AES CLI using root user & Replace following line; 'trapsink <IP> <PORT>' with 'trap2sink <IP> <PORT>' in below two files * /etc/snmp/snmpd.conf * /opt/mvap/conf/enableSnmpAgentAuthFailureTrap.conf - Restart snmpd service using command 'systemctl restart snmpd'.
AES-26653	snmp traps configured.	snmptrapd Linux cli utility doesn't give any output when invoked from command line for debugging purposes.	No
AES-23401	DMCC client application written using DMCC Java SDK.	If ServiceProvider.getServiceProvider() fails, two threads are left running	Kill DMCC client manually.
AES-22741	AES 7.1.3	Sample app "Tsapicnf" fails for 32 and 64 bit TSAPI SDK	No
AES-22740	TSAPI Spy (64bit)	When using the 64 bit version of TSAPI Client & SDK, TSAPI Spy does not decode the private data part of TSAPI messages. Instead, it shows a Hex dump. Issue not seen on 32 bit version.	Use TSAPI Spy (32bit)
AES-22385	AES 8.1	On OAM page Security -> certificate management -> server certificates -> add	Select manual enrollment instead of

ID	Minimum Conditions	Visible Symptoms	Workaround
		Keeping enrollment method as Automatic gives error "Auto Enrollment failed, did not receive certificate from CA."	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-19711	Decoding transport logs	asai_trace was not able to deal with larger ASAI messages (it did not decode them).	No
AES-19610	AES 7.1.3	LDAP configuration option for TSAPI user (cus_ldap) is not set following errors get printed in alarm.log, every time the cti user is logged in to AES pam_ldap(tsapi_service:account): unknown option: config=/etc/cus-ldap.conf pam_ldap(tsapi_service:auth): unknown option: config=/etc/cus-ldap.conf	No
AES-19365	AES 8.1.1	Tomcat partially sends logs bypassing the rsyslog utility. Hence, separate catalina log files are generated under /var/log/tomcat directory.	No
AES-18144	AES 8.1	If the SNMP device is configured to use SNMP version 1 or 2c then the community name of length more than 128 characters is not allowed in the Security Name field on OAM -> Utilities -> SNMP -> SNMP trap receivers -> Add.	No

Known issues and workarounds Application Enablement Services in Release 10.1.3.1

ID	Minimum Conditions	Visible Symptoms	Workaround
AES-32305	JTAPI 10.1 AES 10.1	JTAPI application may be come unresponsive, due to race condition among internal JTAPI threads.	No
AES-32299	AES 8.x AES 10.x	Alarm for /var/log disk utilization greater than 90%.	Cleanup old kernel.log from /var/log/avaya/aes/ directory
AES-32296	AES 10.1.3, add toneDetection monitor.	Application may receive ToneDetected event twice for every DTMF tone received.	No
AES-32226	SELinux is enabled	EASG user (craft) OAM login does not work	Run command " semanage permissive -a tomcat_t " with user root followed by reboot of the system
AES-31933 (SMGR-72838)	AES 8.1.x, SMGR 10.1.3, AES 10.1 OVA, AES 10.1.3 FP	The SDM only migrated to 10.1 OVA but did not install FP10.1.3.0.11.	Perform upgrade from AES 8.x to 10.1 first, and then apply the 10.1.3 patch explicitly using the patching section.
AES-31777	AES 10.1.0.1	The enabled ports were disabled after AES10.1.0.2 update.	No
AES-31529	10x versions of the DMCC .NET library	Unable to use in an environment that requires all assemblies to be strongly named.	No

ID	Minimum Conditions	Visible Symptoms	Workaround
AES-31510	AES 10.1.0.2	After the JTAPI provider initialized the existing log4j setting of application shut downs.	No
AES-31202	JTAPI 10.1.x	A delay gets introduced in the JTAPI response when processing getLoggedOnAgents and ACD.addAddressListener API request which sometimes results in provider shutdown if the Q Size threshold (1000) is breached.	No
AES-31143	AES 10.1.2	Editing the default user is failing from OAM -> User Management -> user Admin -> List all user -> Edit(any 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-31080	AES GRHA configured and CTI application subscribing for 3PCC Events.	CTI applications fails to updates state of the Call and Agent & doesn't work properly after GRHA fail-over.	Restart DMCC Service on AES or restart CTI application.
AES-31054	Re-installation new valid License on WebLM.	DMCC License mode is in License_Expired mode on OAM even after installing new valid License on WebLM.	No
AES-30249	AES 8.1.3	"Index was outside the bounds of the array." exception came while performing an API call through NICE recorder.	No
AES-30029	AES 10.1.0.x - GRHA Configured	AES 10.1.0.x - GRHA shows running on CLI and OAM with different versions of AES.	No
AES-29836	TSAPI CLIENT/SDK 10.1.0.2	French characters are not shown properly of the EULA in InstallShield Wizard.	No
AES-29742	JTAPI 8.1.3 AES 8.1	JTAPI make call using tac shows incorrect number of parties in getConnections()	No
AES-29726	TSAPI CLIENT/SDK 10.1	Due to missing dependency TSAPI client application shows error message as msvcr100.dll missing.	No
AES-28813	AES 8.1.3.4.0.2: 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-28407	Workspaces build 1.19.143, AES 8.1.3, CM 8.1.3	Conference and transfer options are not visible on Agent.	No
AES-28193	One or more Service is stopped.	CTI link status for all services is shown as talking even if respective service is stopped	No
AES-28171	AES-8.1.2	An error "Cannot access the reference link" is generated on web browsers when URL "Comments on this documents?" is accessed on any help page of AES OAM	No
AES-27844	Invalid configuration of "WebLM IP Address/FQDN", "WebLM Port" and valid configuration of "Secondary WebLM IP Address/FQDN" and "Secondary WebLM	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
	Port" on "Licensing | WebLM Server Address" (OAM).		
AES-27583	SNMP trap receiver configured	After migrating AES from 8.x to 10.1 the SNMP trap messages type and version displays v1 even if the SNMP version is 2c	Workaround: Login to AES CLI using root user & Replace following line; 'trapsink <IP> <PORT>' with 'trap2sink <IP> <PORT>' in below two files * /etc/snmp/snmpd.conf * /opt/mvap/conf/enableSnmpAgentAuthFailureTrap.conf - Restart snmpd service using command 'systemctl restart snmpd'.
AES-26653	snmp traps configured.	snmptrapd linux cli utility doesn't give any output when invoked from command line for debugging purposes.	No
AES-23401	DMCC client application written using DMCC Java SDK.	If ServiceProvider.getServiceProvider() fails, two threads are left running	Kill DMCC client manually.
AES-22741	AES 7.1.3	Sample app "Tsapicnf" fails for 32 and 64 bit TSAPI SDK	No
AES-22740	TSAPI Spy (64bit)	When using the 64 bit version of TSAPI Client & SDK, TSAPI Spy does not decode the private data part of TSAPI messages. Instead, it shows a Hex dump. Issue not seen on 32 bit version.	Use TSAPI Spy (32bit)
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-19711	Decoding transport logs	asai_trace was not able to deal with larger ASAI messages (it did not decode them).	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-18144	AES 8.1	If the SNMP device is configured to use SNMP version 1 or 2c then the community name of length more than 128 characters is not allowed in the Security Name field on OAM -> Utilities -> SNMP -> SNMP trap receivers -> Add.	No

Known issues and workarounds Application Enablement Services in Release 10.1.3

ID	Minimum Conditions	Visible Symptoms	Workaround
AES-31933 (SMGR-72838)	AES 8.1.x, SMGR 10.1.3, AES 10.1 OVA, AES 10.1.3 FP	The SDM only migrated to 10.1 OVA but did not install FP10.1.3.0.11.	Perform upgrade from AES 8.x to 10.1 first, and then apply the 10.1.3 patch explicitly using the patching section.
AES-31836	SMS test tool xml version and run the TrunkGroup model with List operation.	SMSXML application will not be able to use TrunkGroup model.	No
AES-31777	AES 10.1.0.1	The enabled ports were disabled after AES10.1.0.2 update.	No
AES-31776	AES rebooted.	False high memory usage alarm is generated.	No
AES-31568	AES 10.1, 8.x TSAPI Client	TSAPI application will not be able to connect on TLS 1.0/1.1, even though it is enabled.	Use TLS 1.2/1.3 for connecting to TSAPI.
AES-31529	10x versions of the DMCC .NET library	Unable to use in an environment that requires all assemblies to be strongly named.	No
AES-31510	AES 10.1.0.2	After the JTAPI provider initialized the existing log4j setting of application shut downs.	No
AES-31202	JTAPI 10.1.x	A delay gets introduced in the JTAPI response when processing getLoggedOnAgents and ACD.addAddressListener API request which sometimes results in provider shutdown if the Q Size threshold (1000) is breached.	No
AES-31143	AES 10.1.2	Editing the default user is failing from OAM -> User Management -> user Admin -> List all user -> Edit(any 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-31080	AES GRHA configured and CTI application subscribing for 3PCC Events.	CTI applications fails to updates state of the Call and Agent & doesn't work properly after GRHA fail-over.	Restart DMCC Service on AES or restart CTI application.
AES-31054	Re-installation new valid License on WebLM.	DMCC License mode is in License_Expired mode on OAM even after installing new valid License on WebLM.	No
AES-30249	AES 8.1.3	"Index was outside the bounds of the array." exception came while performing an API call through NICE recorder.	No

ID	Minimum Conditions	Visible Symptoms	Workaround
AES-30039	AES SMS service used.	If there is segfault in ossicm process, the logs are not logged to the ossicm.log file and neither the segfault file gets generated. We only see this information while running journalctl -f.	No
AES-30029	AES 10.1.0.x - GRHA Configured	AES 10.1.0.x - GRHA shows running on CLI and OAM with different versions of AES.	No
AES-29836	TSAPI CLIENT/SDK 10.1.0.2	French characters are not shown properly of the EULA in InstallShield Wizard.	No
AES-29742	JTAPI 8.1.3 AES 8.1	JTAPI make call using tac shows incorrect number of parties in getConnections()	No
AES-29726	TSAPI CLIENT/SDK 10.1	Due to missing dependency TSAPI client application shows error message as msvcr100.dll missing.	No
AES-28813	AES 8.1.3.4.0.2: 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-28407	Workspaces build 1.19.143, AES 8.1.3, CM 8.1.3	Conference and transfer options are not visible on Agent.	No
AES-28193	One or more Service is stopped.	CTI link status for all services is shown as talking even if respective service is stopped	No
AES-28171	AES-8.1.2	An error "Cannot access the reference link" is generated on web browsers when URL "Comments on this documents?" is accessed on any help page of AES OAM	No
AES-27844	Invalid configuration of "WebLM IP Address/FQDN", "WebLM Port" and valid configuration of "Secondary WebLM IP Address/FQDN" and "Secondary WebLM Port" on "Licensing | WebLM Server Address" (OAM).	AE Services page showed License Information in red text as "Application Enablement Service is not licensed in the license file."	No
AES-27583	SNMP trap receiver configured	After migrating AES from 8.x to 10.1 the SNMP trap messages type and version displays v1 even if the SNMP version is 2c	Workaround: Login to AES CLI using root user & Replace following line; 'trapsink <IP> <PORT>' with 'trap2sink <IP> <PORT>' in below two files * /etc/snmp/snmpd.conf * /opt/mvap/conf/enableSnmpAgentAuthFailureTrap.conf

ID	Minimum Conditions	Visible Symptoms	Workaround
			- Restart snmpd service using command 'systemctl restart snmpd'.
AES-26653	snmp traps configured.	snmptrapd linux cli utility doesn't give any output when invoked from command line for debugging purposes.	No
AES-23401	DMCC client application written using DMCC Java SDK.	If ServiceProvider.getServiceProvider() fails, two threads are left running	Kill DMCC client manually.
AES-22741	AES 7.1.3	Sample app "Tsapicnf" fails for 32 and 64 bit TSAPI SDK	No
AES-22740	TSAPI Spy (64bit)	When using the 64 bit version of TSAPI Client & SDK, TSAPI Spy does not decode the private data part of TSAPI messages. Instead, it shows a Hex dump. Issue not seen on 32 bit version.	Use TSAPI Spy (32bit)
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-19711	Decoding transport logs	asai_trace was not able to deal with larger ASAI messages (it did not decode them).	No
AES-19610	AES 7.1.3	LDAP configuration option for TSAPI user (cus_ldap) is not set following errors get printed in alarm.log, every time the cti user is logged in to AES pam_ldap(tsapi_service:account): unknown option: config=/etc/cus-ldap.conf pam_ldap(tsapi_service:auth): unknown option: config=/etc/cus-ldap.conf	No
AES-19365	AES 8.1.1	Tomcat partially sends logs bypassing the rsyslog utility. Hence, separate catalina log files are generated under /var/log/tomcat directory.	No
AES-18144	AES 8.1	If the SNMP device is configured to use SNMP version 1 or 2c then the community name of length more than 128 characters is not allowed in the Security Name field on OAM -> Utilities -> SNMP -> SNMP trap receivers -> add.	No

Known issues and workarounds Application Enablement Services in Release 10.1.2

Key	Customer Visible Symptom	Workaround
AES-16552	MonitorStop event is not sent to all the call control monitors when TSAPI service goes down	No
AES-17332	Call control events are not received by the application once the service provider has been shut down and restarted.	No
AES-18144	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	N0

Key	Customer Visible Symptom	Workaround
	the Security Name field on OAM -> Utilities -> SNMP -> SNMP trap receivers -> add.	
AES-19215	Not sure if it is actually visible to customer since it is reported via code perspective.	No
AES-19365	Tomcat partially sends logs bypassing the rsyslog utility. Hence, separate catalina log files are generated under /var/log/tomcat directory.	No
AES-19610	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-19711	asai_trace was not able to deal with larger ASAI messages (it did not decode them).	No
AES-21856	Calls didn't get drop properly and call recordings were missing on AWFOS	No
AES-22385	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-22740	When using the 64 bit version of TSAPI Client & SDK, TSAPI Spy does not decode the private data part of TSAPI messages. Instead, it shows a Hex dump.	The problem does not affect the 32 bit versions.
AES-22741	Sample app "Tsapicnf" fails for 32 and 64 bit TSAPI SDK	No
AES-23401	If ServiceProvider.getServiceProvider() fails, two threads are left running	Kill DMCC client manually.
AES-26653	snmptrapd linux cli utility doesn't give any output when invoked from command line for debugging purposes.	No
AES-27583	After migrating AES from 8.x to 10.1 the SNMP trap messages type and version displays v1 even if the SNMP version is 2c	Login to AES CLI using root user & Replace following line; 'trapsink <IP> <PORT>' with 'trap2sink <IP> <PORT>' in below two files * /etc/snmp/snmpd.conf * /opt/mvap/conf/enableSnmpAgentAuthFailureTrap.conf - Restart snmpd service using command 'systemctl restart snmpd'.
AES-27830	After completing the upgrade to AES 8.1.3.3.0.4: In the 1st login: AES OAM shows get time information from AWS. In the 2nd and subsequent times login: NTP information is not visible on AES OAM. After rebooting AES through CLI, AES OAM shows get time information from the user's IP PC.	No
AES-27844	AE Services page showed License Information in red text as "Application Enablement Service is not licensed in the license file."	No

Key	Customer Visible Symptom	Workaround
AES-28171	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-28193	CTI link status for all services is shown as talking even if respective service is stopped	No
AES-28407	Conference and transfer options are not visible on Agent.	No
AES-28436	JVM Shuts Down, OAM not comes up after login, and DMCC service restarts continuously when the external WebLM server is not reachable	Set local weblm server by running command on cli as below: setWeblm -pri 127.0.0.1:443 -pssl true -hostval false
AES-28813	Bad gateway error seen when trying to add all devices in a device group.	No
AES-29129	Able to login in a OAM sessions even after the PAM login limit exceeds	No
AES-29293	SSL_read fails on AES HA with "Far End Unreachable" status, if SMGR signed Certs are used with "server" alias	Use any other alias like "aeservices" etc to make identity certificate.
AES-29428	When login through CLI on AES if the account gets locked due to incorrect login attempts, it shows Access denied instead of showing account is locked	No
AES-29653	Customer saw DMCC registration denial alarms on ACRA. The alarms are false-positive as next subsequent registration request for same DMCC gets accepted by the CM and DMCC gets registered properly approximately at the same time.	Reattempt the DMCC registration
AES-29726	Due to missing dependency TSAPI client application shows error message as msvcr100.dll missing.	NA
AES-29742	JTAPI make call using tac shows incorrect number of parties in getConnections()	No
AES-29836	French characters are not shown properly of the EULA in InstallShield Wizard.	No
AES-29927	When a recording is done by DMCC station using server mode, the recorded files fail to play.	No
AES-30029	AES 10.1.0.x - GRHA shows running on CLI and OAM with different versions of AES.	No
AES-30039	If there is segfault in ossicm process, the logs are not logged to the ossicm.log file and neither the segfault file gets generated. We only see this information while running journalctl -f.	No
AES-30045	CVE-2016-5019 update require for Apache Trinidad Myfaces	No
AES-30104	After the JTAPI provider initialized the existing log4j setting of application shut downs.	
AES-30149	AES SNMP traps are not send to the configured SNMP trap receiver.	NA
AES-30249	"Index was outside the bounds of the array." exception came while performing an API call through NICE recorder.	NA

Key	Customer Visible Symptom	Workaround
AES-30729	Vulnerability scan flags following CVEs:- RHSA-2022:4855 and RHSA-2021:5236	No
AES-30893	Distributing VDN parameter will be empty in CstaDelivered or subsequent events, if call is transferred to monitored VDN.	No
AES-31080	CTI applications fails to updates state of the Call and Agent & doesn't work properly after GRHA fail-over.	Restart DMCC Service or CTI application.
AES-31054	DMCC License mode is in License_Expired mode on OAM even after installing new valid License on WebLM.	No
AES-31129	AES fails to retrieve license from Secondary License server and goes into ERROR MODE when the Primary WebLM IP becomes unreachable.	No
AES-31132	The wrong acshandle is returned to the application.	No
AES-31143	Editing the default user fails when attempted through OAM -> User Management -> user Admin -> List all user -> Edit (any default user)	Use "ctiUser" utility to edit the default users from CLI.
AES-31149	DTMF tone events are not sent to clients if DMCC station re-registers after monitor is placed.	Re-start the Monitor after DMCC station re-registers.
AES-31151	AES HTTPD process listens on port 80 even though on "Standard reserved ports" page port 80 is disabled.	No
AES-31202	A delay gets introduced in the JTAPI response when processing getLoggedOnAgents and ACD.addAddressListener API request which sometimes results in provider shutdown if the Q Size threshold (1000) is breached.	No
AES-31203	After upgrading AES from 10.1.0.1 to 10.1.0.2, the application is no longer able to receive GetDisplayResponse responses to GetDisplay requests.	Recompile application with newest DMCC SDK
AES-31279	Failed to install TSAPI & CVLAN Client 64 bit Linux binary with error "Expected version of glibc rpm is not present on system. Please install 32-bit version of glibc rpm."	No

Known issues and workarounds Application Enablement Services in Release 10.1.0.2

Key	Customer Visible Symptom	Workaround
AES-30527	Not able to login to AES OAM webpage using Windows Active Directory user (LDAP) **Note**: CT Users can still use Windows Active Directory users (LDAP) to login via CTI applications.	Add local administrator user to for all the admins and use those users to login to AES OAM
AES-30051	It fails to generate DFMF warning tone on the call when the 3rd party call control API request is generated to generate a tone on the calls using CTI application	
AES-21856	Calls didn't get drop properly and call recordings were missing on AWFOS	
AES-28171	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	

Key	Customer Visible Symptom	Workaround
AES-27583	After migrating AES from 8.x to 10.1 the SNMP trap message's type and version displays v1 even if the SNMP version is 2c	Login to AES CLI using root user Replace following line; 'trapsink <IP> <PORT>' with 'trap2sink <IP> <PORT>' in below two files * /etc/snmp/snmpd.conf * /opt/mvap/conf/enableSnmpAgentAuthFailureTrap.conf Restart snmpd service using command 'systemctl restart snmpd'.
AES-28193	CTI link status for all services is shown as talking even if respective service is stopped	
AES-30044	VMWare Fault tolerance cannot be enabled on AES 10.1 OVA.	
AES-28813	On AES OAM -> security -> Security Database -> Device groups if "Edit device Group" is pressed and device list has more than 5K devices then an error is generated as "Bad Gateway"	
AES-26653	snmptrapd linux cli utility doesn't give any output when invoked from command line for debugging purposes.	
AES-27844	When the Primary WebLM is wrongly configured or unreachable and secondary WebLM is configured and accessible the licenses are consumed from secondary. However an error "Application Enablement Service is not licensed in the license file." Is generated on OAM -> AE Services page	
AES-19610	If LDAP configuration option for TSAPI user (cus_ldap) is not set then the following errors is generated in alarm.log, pam_ldap(tsapi_service:account): unknown option: config=/etc/cus-ldap.conf pam_ldap(tsapi_service:auth): unknown option: config=/etc/cus-ldap.conf	
AES-18144	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.	
AES-22385	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.

Key	Customer Visible Symptom	Workaround
AES-29428	When login through CLI on AES if the account gets locked due to incorrect login attempts, it shows Access denied instead of showing account is locked	
AES-30039	If there is segfault in ossicm process, the logs are not logged to the ossicm log file	
AES-29836	French characters are not shown properly of the EULA in InstallShield Wizard.	
AES-19692	When the new version of TSAPI client installed on top of old version the log4cx.dll is not replaced and it causes TSSPY crash.	
AES-24091	If Conferenced Event was received before SnapshotCallConfEvent of the previous delivered event in a scenario where the conferencing party is not being monitored by JTAPI, then it lead mismatched UCID causing the call to fail	
AES-29296	TSAPI Exerciser crashes and become unresponsive if try to create Route Table for 64 bit client version	
AES-29293	If SMGR signed Certs are used with "server" alias AES HA Status on OAM shows as "Far End Unreachable".	
AES-22740	TSAPI Spy does not decode the private data part of TSAPI messages if the 64 bit TSAPI Client version is used. TSSPY shows a Hex dump as it comes from the AES server.	32 bit TSAPI SPY can be used.
AES-30076	Log rotation does not work for /var/log/sssd/ldap_child.log.	
AES-29849	On TSAPI client, CstaClearConnection request fails, if application will use dynamic deviceID present in CstaEstablished event.	
AES-19365	Tomcat partially sends logs bypassing the rsyslog utility. Hence, separate catalina log files are generated under /var/log/tomcat directory.	
AES-30149	AES SNMP traps are not send to the configured SNMP trap receiver.	
AES-30233	AES reports wrong disk name in the Disk Full Alarm. The trapVarbinds logs and alarm reports the /dev/mapper/rhel-var_log_audit disk as full while the disk which is actually filled is /dev/mapper/rhel-var_log .	
AES-29731	"ExeptionOnTimeoutLock" errors are seen in DMCC finest trace when Application sends re- Registration request of SIP Endpoint in DEPENDEDNT mode after receiving the rejection with state of device as "unknown".	
AES-30043	When TWS URL is accessed on AES 8.1.3.1 or earlier version. It would show message "Axis is running". https://[ID_ADDRESS]/axis/services/TelephonyService However, from AES 8.1.3.2 onward it is showing SOAP error which is false positive.	

Key	Customer Visible Symptom	Workaround
AES-30145	DMCC application fails to play valid recorded file after same application attempts to play invalid file.	DMCC Voice Unit service being used CTI application and SERVER Media mode is used.
AES-30236	DMCC registration fails with GENERIC ERROR specifying no reason for registration rejection.	DMCC registration attempted with CM without Media Resources.
AES-16552	When TSAPI service goes down for any reason, intermittently, MonitorStop event fails for some monitors	
AES-28436	OAM is not accessible while remote weblm not reachable.	Set local weblm server by running command on cli as below: setWeblm -pri 127.0.0.1:443 -pssl true -hostval false.
AES-29653	DMCC registration denial alarms on Avaya call recorder. The alarms are false-positive as next subsequent registration request for same DMCC gets accepted by the CM and DMCC gets registered properly approximately at the same time.	Re-attempt DMCC registration
AES-30029	AES GRHA installed on virtual platform and configured with same versions. If one of the servers snapshot is reverted to the older minor version still GRHA shows in running state.	Make sure both active and standby AES are on same version
AES-17332	Call control events are not received by the application once the service provider has been shut down and restarted.	
AES-23401	If ServiceProvider.getServiceProvider() fails, two threads are left running	Kill DMCC manually based on underlying OS. E.g. task manager for Windows.
AES-29391	When decryption fails for SSC facility message, recording for some calls is lost on Avaya call recorder.	Restart DMCC service
AES-29927	Deadlock is observed between "Timer-2" and "NIO-ChannelServicer Thread" DMCC thread	
AES-30227	Some special characters are shows on EULA note for CMAPI SDKs	
AES-26002	Special Application 8481 with SIP	JTAPI based CTI application cannot leverage new ASAI UUI IE Protocol descriptor
AES-30294	When upgrading log4j rpm to version v2 on a SW only AES, OAM becomes inaccessible.	Include log4j rpm in the exclude list while upgrading the rpms on the SW only AES.

Known issues and workarounds Application Enablement Services in Release 10.1.0.1

ID	Visible symptoms	Workaround
AES-29295	AES disclosed the HTTP Server Information as Apache in Server Header of HTTP Response message.	NA
AES-29293	AES HA Status on OAM shows as "Far End Unreachable".	Use any other alias like "aeservices" etc to make identity certificate.
AES-29291	OLH information is showing DES and 3DES options for Enrollment Method instead of Manual and Automatic under Security -> Certificate Management -> Server Certificates -> Add section.	NA
AES-29279	OAM is inaccessible with error 503 service unavailable shown on the page.	NA
AES-29129	Able to login Multiple OAM sessions than the set PAM Limit	NA
AES-29094	Enrolment of a new certificate takes a long time but does not fail with an error. The content of the new certificate is shown in a table. Restarting services to pick up the new certificate fails, or service is unreachable due to missing certificate.	NA
AES-28930	User is not able to delete default certificates even if third party certificates are imported.	NA
AES-28813	After selecting all imported devices to create a devices group, oam crashes.	NA
AES-28810	JTAPI query getLoggedOnAgents() returns wrong results. Returns agent info not belonging to skill in query	NA
AES-28616	SMSXML wsdl import failed when using https instead of http	Use http for imports
AES-28598	Retrieving data. Wait a few seconds and try to cut or copy again.	NA
AES-28436	OAM is not accessible while remote weblm not reachable.	Set local weblm server by running command on cli as below: setWeblm -pri 127.0.0.1:443 -pssl true -hostval false
AES-28269	sending transferredConnections.count as 0 after the Single Step Transfer	NA
AES-28240	When the JTAPI Client receives an event (e.g. Established event) it makes many CSTAQueryDeviceInfo requests to AES. Each/most of these causes the DistributeCSTAEvent thread to block until it receives a response.	NA
AES-28195	While creating a CSR from OAM -> Security -> certificate Management, all the key usage values are not getting added to the CSR	Create CSR using openssl commands from CLI. Below values should be added in req_extensions section of openssl.cnf file.

ID	Visible symptoms	Workaround
		[req_ext] basicConstraints = CA:FALSE keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment extendedKeyUsage = serverAuth, clientAuth Using above openssl.cnf file, create CSR request.
AES-28193	CTI link status for all services is shown as talking even if respective service is stopped	NA
AES-27583	SNMP version 2c trap message's type and version displayed as v1 after migrating from 8.0.1 or 8.1.2 to 10.1	Replace following line; 'trapsink <IP> <PORT>' with 'trap2sink <IP> <PORT>' in following two files:- * /etc/snmp/snmpd.conf */opt/mvap/conf/enableSnmpAgentAuth FailureTrap.conf Restart snmpd service using command 'systemctl restart snmpd'
AES-22744	SO Activate with VDN observee and location > 2000 sends GENERIC_UNSPECIFIED error instead of VALUE_OUT_OF_RANGE	NA
AES-22740	When using the 64 bit version of TSAPI Client & SDK, TSAPI Spy does not decode the private data part of TSAPI messages. Instead, it shows a Hex dump.	NA
AES-22651	1) On a Standalone AES, after deleting default users and restarting aesvcs service, the deleted default users are restored. 2) On GRHA setup: After deleting default users on Active AES and synchronizing and then interchange, on the new Active AES, the deleted default users are restored. 3) Delete Default users and take a backup. Restore the backup on AES. The deleted default users are restored.	NA
AES-21856	Calls didn't get drop properly and call recordings were missing on AWFOS	NA
AES-21028	AES OAM not accessible using 8443 port	<Connector port="8443" protocol="HTTP/1.1"

ID	Visible symptoms	Workaround

		SSLEnabled="true"
		maxThreads="500"
		enableLookups="false"
		disableUploadTimeout="true"
		acceptCount="500"
		scheme="https"
		secure="true"
		maxKeepAliveRequests="-1"
		
		address="0.0.0.0"
		*

AES-16552	DMCC will not receive MonitorStop for all the devices.	Restart DMCC and TSAPI service simultaneously

Known issues and workarounds Application Enablement Services in Release 10.1

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

ID	Visible symptoms	Workaround
AES-28361	For the AES OVA deployed from vCenter, the network configuration on OAM -> Networking -> Network config was shown only for the interface which was set while deploying the OVA and the remaining interfaces are not shown, hence could not modify the missing interfaces from OAM.	Set the required interface at the time of deployment and for after deployment modification, use the "netconfig" command line utility for network configuration
AES-28336	DMCC registration fails when “Secure H.323” is enabled in Switch Connection page.	Install hotfix AES_28336_10-1-0-0-1.bin. Refer PSN020546u for more details.
AES-28324	After installing TSAPI and CVLAN client, the readme will display older versions, for e.g. 8.x. Whereas TSAPI and CVLAN client are of release 10.1	NA
AES-28264	OAM takes time to respond to requests when WebLM is not reachable/responding.	Make sure WebLM IP is reachable. Or if the WebLM IP is wrong, enter the correct IP
AES-28257	If we pass '@' in SNMP V3 password it won't work	Avoid passing '@' in password
AES-28251	false "LDAP Certificate Expired" is reported when the LDAP certificate is still valid.	NA
AES-28240	When the JTAPI Client receives an event (e.g. Established event) it makes many CSTAQueryDeviceInfo requests to AES. Each/most of these causes the DistributeCSTAEvent thread to block until it receives a response.	NA
AES-28235	When same ip address as eth0 was added for eth1 and then apply changes was done, it gave error for the first time but after clicking the second time it showed as successful.	The incorrect value was not saved on AES, it just showed on OAM, once the page was changed and accessed again the values were gone
AES-28234	While installing 10.1 SWonly ISO on AWS platform, the precheck fails with the following	Move extra NIC present at below location to /tmp location:

ID	Visible symptoms	Workaround
	error: Starting Ethernet Name Check... --------------------------------- ens3 db0ba02f-1aad-4b4e-a67e-0b8db221bb33 ethernet Ethernet Name Check: [FAILED] Only eth0, eth1, or eth2 are allowed.	/etc/sysconfig/network-scripts
AES-28233	Interchange and synchronize work for the first time but fail next time.	GRHA must be removed and reconfigured
AES-28230	For AES installed on Cloud Platform, IP Address on OAM -> Networking -> Network Configure Page was shows blank instead of showing the eth0 ip address.	NA
AES-28225	eth2 displays duplicate IPv6 in normalized manner	NA
AES-28220	The CTI application at the customer saw trunk side information missing in CSTA confirmation event for Single Step Conference. Thus, not getting the actual number of parties in the call.	NA
AES-28195	While creating a CSR from OAM -> Security -> certificate Management, all the key usage values are not getting added to the CSR	NA
AES-28193	If the CVLAN service was stopped and if customer check the status on OAM -> Status -> Status and Control -> CVLAN, the link showed talking, whereas it shouldn't show any CTI link or the link status should be down. This happened for all the CTI services.	NA
AES-28175	JTAPI based application might show delayed update of call being delivered to Agent station.	NA
AES-28171	Clicking on "Comments on this documents?" on any help page of AES OAM it shows "Cannot access the reference link"	NA
AES-28138	The CTI application saw few CAG members ringing forever and thus were not getting new calls.	NA
AES-28136	DMCC license is in error mode while AES in secure mode	Use embedded webLM for DMCC
AES-27946	Couldn't access AES OAM intermittently	Restart tomcat service
AES-27844	AE Services page showed License Information in red text as "Application Enablement Service is not licensed in the license file."	NA
AES-27831	Couldn't make existing user a CT user from OAM and CLI	Create a new user and make it a CT user.
AES-27830	In the 1st login: AES OAM shows get time information from AWS. In the 2nd and subsequent times login: NTP information is not visible on AES OAM and after reboot AES through CLI, AES OAM shows get time information from my IP PC.	NA

ID	Visible symptoms	Workaround
AES-27808	CTI application don't see CSTA_MONITOR_ENDED (Call Monitor Ended) event for the monitored call after complete call disconnection.	NA
AES-27703	No 3PCC events are being received by CTI application.	NA
AES-27699	After restoring a backup, the timeout was not restored as expected	Add timeout manually via Security -> Session Timeouts -> HTTP Timeout and Apply Changes
AES-27690	Missing Service Observer Activate, Service Observer Deactivate and Query Service Observer API support in GetAPICapsConfEvent.	NA
AES-27583	SNMP version 2c trap message's type and version displayed as v1 after migrating from 8.0.1 or 8.1.2 to 10.1	- Replace following line; 'trapsink <IP> <PORT>' with 'trap2sink <IP> <PORT>' in below two files * /etc/snmp/snmpd.conf * /opt/mvap/conf/enableSnmpAgentAuthFailureTrap.conf - Restart snmpd service using command 'systemctl restart snmpd'.
AES-27549	DMCC Service is in unknown status in OAM. If checked from the command line, the DMCC service status is not running.	Restart DMCC service one more time.
AES-27418	Several Oceana Agents are unexpectedly put into auxilary mode.	Agent must manually be set to Ready Mode.
AES-27310	The agent is receiving dual ringing event from JTAPI for same alerting.	NA
AES-27260	The DMCC application at the customer faced service disruption for few mins regularly. This happened when a bunch of DMCC stations registering and making calls played WAV files present on AES. Problem was seen at the calls termination when devices monitors stopped un-registering devices.	NA
AES-27064	JTAPI API getConnections() misses a party in the list it provides for the connections in the call	NA
AES-26976	HMDC log collection will not work properly	NA
AES-26733	Customer is seeing /opt/spirit/ full with "LogTail*.logbuff".	Manually remove older logbuff files
AES-26679	JTAPI LucentAgent.getStateInfo() returns an incorrect lucentWorkMode and reasonCode	NA
AES-26653	snmptrapd linux cli utility doesn't give any output when invoked from command line for debugging purposes.	NA
AES-26648	TWS does not invalidate the session even if session timeout configured on OAM is reached.	NA

ID	Visible symptoms	Workaround
AES-26647	If the password field is kept empty while modifying the user then the user modification fails from OAM -> user Management	Do not keep the password field empty while modifying the user
AES-26219	CPU is spiking to 100% when GRHA is triggered on Profile 1 server.	Configure GRHA with profile 3
AES-26077	GRHA was not configured if the password of the remote server contains # at the end.	Do not set password which has "#"
AES-26002	Special Application 8481 with SIP	JTAPI based CTI application cannot leverage new ASAI UUI IE Protocol descriptor
AES-26001	When developing an application using the TSAPI SDK, ATTUUIProtocolType_t currently supports PDs 0x00 and 0x04, but not 0x10 and 0x14. 0x10 and 0x14 are required for SIP and SA8481.	Get in touch with AES dev connect or support.
AES-24526	Test application window is not closing after uninstalling.	Test application can be closed manually.
AES-24496	Customer won't find EULA in Client Readme.TXT after installing TSAPI Client.	NA
AES-24367	Incorrect number of login attempts have been displayed on OAM when account gets locked due to max failed login attempts.	NA
AES-23458	customers can send skill queued event without adding skills.	NA
AES-23401	If ServiceProvider.getServiceProvider() fails, two threads are left running	Kill DMCC manually based on underlying OS. E.g. task manager for Windows.
AES-23195	when Logging Facility is changed, on OAM -> Status - -> Log Manager --> System Logging, HTTPD service is restarted and on GRHA setup if customer execute "statapp" command then customer will see HTTPD service as deactivated.	HTTPD service can be restarted manually
AES-23159	JTAPI crashes with null pointer exception while processing CSTA FAILED event having empty failing Device.	Add an entry in reg_dword table of 'EnableGuessFailingDevice' for 'localhost' having value set to 1.
AES-22776	Wrong number of parties in Single Step Conference Response.	NA
AES-22774	CTI application does not receive CSTA Diverted and CSTA Established events if call is answered by bridge station of the called station	NA
AES-22744	Service observe activate request with VDN as observee and observeeLocation > 2000 gives wrong error code GENERIC_UNSPECIFIED (CS0/100)	NA
AES-22740	TSAPI TSSPY prints binary data instead of decoded structure for 64 bits	NA
AES-22659	WebLM Server Address page displays port number 443 instead of 8443 when Restore Default button is clicked	NA
AES-22651	1) On a Standalone AES, after deleting default users and restarting aesvcs service, the deleted default users are restored. 2) On GRHA setup: After deleting default	NA

ID	Visible symptoms	Workaround
	users on Active AES and synchronizing and then interchange, on the new Active AES, the deleted default users are restored. 3) Delete Default users and take a backup. Restore the backup on AES. The deleted default users are restored.	
AES-22592	RedirectMediaRequest fails silently if the encryption list contains more than one entry, one of which is an SRTP type	include only one encryption list
AES-22385	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-21939	CTI applications receives end point registration/unregistration events even though not subscribed for those events.	NA
AES-21856	Calls didn't get drop properly and call recordings were missing on AWFOS	NA
AES-21045	S/W only installation working even if the interface name is other than "eth0"	NA

AES-21028	AES OAM not accessible using 8443 port	Use 443 port or edit server.xml and add following line
		<Connector port="8443" protocol="HTTP/1.1"
		SSLEnabled="true"
		maxThreads="500"
		enableLookups="false"
		disableUploadTimeout="true"
		acceptCount="500" scheme="https"
		secure="true"
		maxKeepAliveRequests="-1"
		address="0.0.0.0"
		*

AES-20862	LSU installation logs are not there in AES 8.1.2	Refer the LSU installation logs present in /tmp. Log file name lsu_update.out-$date
AES-20587	After enabling encryption, customer sees blank screen on AES console after reboot for around 3 mins.	NA
AES-19692	TSAPI client installer couldn't install properly. The files doesn't get updated although installer indicates successful installation. This particularly happens to log4cx.dll. Hence, tsapi client applications doesn't work properly.	First uninstall 7.1 version and then install 8.1
AES-19610	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	NA

ID	Visible symptoms	Workaround
AES-19365	Tomcat partially sends logs bypassing the rsyslog utility. Hence, separate catalina log files are generated under /var/log/tomcat directory.	NA
AES-18144	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.	NA
AES-17495	DMCC Java Client throws java.lang.NoSuchMethodException for phone type 16XX.	NA
AES-17332	Call control events are not received by the application once the service provider has been shut down and restarted.	NA
AES-17260	3rd Party MIB receiver not able to connect with AES	try to use AES alarm viewer for alarms
AES-16984	The DMCC application does not terminate after a network interruption.	Kill DMCC manually based on underlying OS. E.g. task manager for Windows.
AES-16552	MonitorStop event is not sent to all the call control monitors when TSAPI service goes down for some reason.	NA
AES-16021	DMCC service goes unavailable with "JVM exited unexpectedly" error in dmcc-wrapper.log	NA
AES-14801	JTAPI application not getting call events for auto in calls	NA
AES-14676	DMCC application doesn't receive MediaStart events or RTP when a terminal is registered with a long list of codecs and encryption types	NA

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 10.1.x.x

What's new in G430 and G450 Media Gateways Release 10.1.3.2 (Builds 42.27.00 and 42.27.30)

No new features were added in this release.
Also see: Fixes in G430 and G450 Media Gateways Release 10.1.x.x

What's new in G430 and G450 Media Gateways Release 10.1.3.1 (Builds 42.24.00 and 42.24.30)

No new features were added in this release.
Also see: Fixes in G430 and G450 Media Gateways Release 10.1.x.x

What's new in G430 and G450 Media Gateways Release 10.1.3 (Builds 42.22.00 and 42.22.30)

No new features were added in this release.
Also see: Fixes in G430 and G450 Media Gateways Release 10.1.x.x

What's new in G430 and G450 Media Gateways Release 10.1.2 (Builds 42.18.00 and 42.18.30)

- The "set logging server' CLI Command for syslog now supports the use of FQDNs as well as IP addresses.

Also see: Fixes in G430 and G450 Media Gateways Release 10.1.x.x

What's new in G430 and G450 Media Gateways Release 10.1.0.2 (Builds 42.08.00 and 42.08.30)

No new features were added in this release.
Also see: Fixes in G430 and G450 Media Gateways Release 10.1.x.x

What's new in G430 and G450 Media Gateways Release 10.1.0.1 (Builds 42.07.00 and 42.07.30)

No new features were added in this release.
Also see: Fixes in G430 and G450 Media Gateways Release 10.1.x.x

What's new in G430 and G450 Media Gateways Release 10.1 (Builds 42.04.00 and 42.04.30)

For more information see ***What's New in Avaya Aura® Release 10.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101078425

Installation for Avaya Aura® G430 and G450 Media Gateways Release 10.1.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.

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`

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 the G450 firmware specific to its 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.

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 the 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
40.xx.xx	8.0.1
41.xx.xx	8.1.x
42.xx.xx	10.1.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 the manufacturer support model. This means that as soon as a Communication Manager release goes end of manufacturer support, new gateway firmware will no longer be supported with that 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, 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`

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 the G450 firmware specific to its hardware vintage. Firmware for G450 Vintage 4 must only use firmware having "g450v4_" indicated in the firmware image's filename. All other G450 vintages must only use firmware having "g450_" indicated in the firmware image's filename.

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.

Fixes in G430 and G450 Media Gateways Release 10.1.x.x

Fixes in G430 and G450 Media Gateways Release 10.1.3.7 (Builds 42.27.00 and 42.27.30)

ID	Minimum conditions	Visible symptoms	Issue found in Release
CMG4XX-4393	Services Port	Improved auto negotiation from 1GB connections.to Services port.	10.1
CMG4XX-4418	WAN Port	Improved auto negotiation from 1GB connections.to WAN port.	8.1.3
CMG4XX-4437	VPN	Fixed VPN connection failures in the G450v4 and G430v3 gateways.	10.1.3

Fixes in G430 and G450 Media Gateways Release 10.1.3.1 (Builds 42.24.00 and 42.24.30)

ID	Minimum conditions	Visible symptoms	Issue found in Release
CMG4XX-4351	SNMP Traps, USB devices	In some cases, SNMP traps generated for USB devices could cause a reset.	8.1.3

Fixes in G430 and G450 Media Gateways Release 10.1.3 (Builds 42.22.00 and 42.22.30)

ID	Minimum conditions	Visible symptoms	Issue found in Release
CMG4XX-4308	CLI	In rare cases, a gateway restart could occur if a user entered a CLI command that exceeded the maximum CLI command length (300 characters in older gateway vintages, 340 characters in newer gateway vintages).	8.1.3
CMG4XX-4312	Multicast	Burst of multicast packets addressed to other devices at a high rate that could cause a gateway to lose packets that were addressed to it.	8.1.3
CMG4XX-4298	IPv6	Fixed Network Connectivity (NR_CONN) alarms on CM when gateways in different network regions register using IPv6.	8.1.3
CMG4XX-4316	DSP	Enhancements were added to make the DSP sanity checking more resilient to heavy call-processing load, as well as some miscellaneous debug/diagnostic enhancements.	8.1.3
CMG4XX-4306	G430v3, G450v4	This release fixes an issue where in some models, on initial boot, reboot or cable insertion, the services port and/or WAN port on the G450 Hardware Vintage 4 are not immediately available as the link goes up and down repeatedly.	8.1.3

Fixes in G430 and G450 Media Gateways Release 10.1.2 (Builds 42.18.00 and 42.18.30)

ID	Minimum Conditions	Visible symptoms	Found in Release
CMG4XX-4062	S8300	Sanity monitoring is now disabled when the gateway detects that an S8300 board is extracted so that a reinserted S8300 board will not be reset while rebooting and therefore almost doubling the boot time.	8.1.3
CMG4XX-4225	syslog	The "set logging server' CLI Command for syslog now supports the use of FQDNs as well as IP addresses.	10.1.2
CMG4XX-4243	ASBCE, Edge Mode	Removed the undocumented "set sbc-common-ip" CLI command that was introduced temporarily to allow a gateway running Release 10.1.0 to register with a 10.1.1 SBC in Edge Mode. *Note: ASBCE Release 10.1.1 or later must be used with Gateway Release 10.1.2 in Edge Mode. ASBCE Release 8.1.3 or 10.1 must be used with Gateway Release 10.1.0.x.*	10.1.0
CMG4XX-4279	G430v3 or G450v4	The 'no autonegotiation' CLI command for fastEthernet is no longer supported on newer gateways (G430v3 and G450v4). New gateways will display the warning "This mode of operation is not supported" if the command is entered from the command line.	8.1.3

Fixes in G430 and G450 Media Gateways Release 10.1.0.2 (Builds 42.08.00 and 42.08.30)

ID	Minimum Conditions	Visible symptoms	Found in Release
CMG4XX-4169	TLS H.248 Registration	A random delay between 0.1 and 1.0 second has been introduced to the rate the gateway attempts to register with CM when using TLS. Prior to this change, the gateway would too rapidly try to register with CM making it difficult to login to the gateway and potentially negatively impact CM performance.	8.1.3
CMG4XX-4212	VLAN, TLS H.248 Registration	Miscellaneous internal improvements were introduced including: - Reducing the number of VLANs supported by a G450v4 to 24 (still larger then needed). - Reducing the CRL max refresh rate from 10 per hour to 2 per hour in the case of invalid/expired CRLs.	8.1.3
CMG4XX-4227	SLS Signaling Groups	The maximum circuit-number can now range from 1 to 999 when using the "set primary-dchannel" and "add nfas-interface" CLI commands in an SLS signaling group. Prior to this change, the gateway would not accept a value greater than 256.	8.1.3
CMG4XX-4232	"show temperature" CLI command	The "show temperature" command now includes the Fahrenheit temperature value as well as the Celsius value.	8.1.3
CMG4XX-4237	VoIP DSPs	In rare cases, the gateway would reboot when a message was received from a DSP that is no longer valid to be used. These messages are now ignored.	8.1
CMG4XX-4240	ISDN BRI Trunks	In rare cases, ISDN BRI Trunks would not properly come back in service after an CM interchange/reset.	8.1.3

Fixes in G430 and G450 Media Gateways Release 10.1.0.1 (Builds 42.07.00 and 42.07.30)

ID	Minimum Conditions	Visible symptoms	Found in Release
CMG4XX-4059	S8300	The time for an S8300 to come back into service was greatly improved whenever the S8300 is removed and reinserted.	8.1.3

Fixes in G430 and G450 Media Gateways Release 10.1 (Builds 42.04.00 and 42.04.30)

There are no fixes included in Release 10.1 since this is the first release.

Known issues and workarounds in G430 and G450 Media Gateways Release 10.1.x.x

Known issues and workarounds in G430 and G450 Media Gateways Release 10.1

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

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

Languages supported

- English

Documentation errata

- None

Avaya Aura® Media Server

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

- Release 10.1 Release Notes at: https://download.avaya.com/css/public/documents/101081316
- Release 8.0.x Release Notes at: https://download.avaya.com/css/public/documents/101086532

Avaya WebLM

What's new in Avaya WebLM for 10.1.3.2

Supported Browsers - Chrome (minimum version 117.0), Edge (minimum version 117.0) and Firefox (minimum version 118.0). Earlier versions are no longer supported.

WebLM 10.1.2 OVA and thus 10.1.3.1 and Higher WebLM releases are certified with ESXi 8.0 and 8.0 Update 2 (U2) deployments.

AvayaAuraWebLM_10.1.2.0.0-39457_72.iso will be removed from PLDS and support.avaya.com and replaced with AvayaAuraWebLM_10.1.2.0.0-39690_75.iso. Please refer **PSN006093u** for more details.

What's new in Avaya WebLM for 10.1.3.1

Security enhancements and Bug fixes.

IMPORTANT NOTE: Starting 10.1.3.1, licensing for Communication Manager (CM) and Application Enablement Services (AES) will only work with 10.1.3.1 and higher version of System Manager (SMGR) or Standalone WebLM (WebLM). If upgrading CM and/or AES to 10.1.3.1 and higher then the required order of upgrade is imperative i.e. SMGR and/or WebLM should be upgraded to 10.1.3.1 and higher first to ensure licensing for CM and/or AES does not stop working. CM and AES 10.1.3.0 were originally compatible with Standalone WebLM 10.1.2.0 (as there was no Standalone WebLM 10.1.3.0), however beginning with 10.1.3.1 and higher, Standalone WebLM 10.1.3.1 and higher is required for CM and AES. The Avaya Aura® System Manager release/version must always be greater than or equal to the release/version of the components of the solution (Session Manager, Communication Manager, Application Enablement Services).

What's new in Avaya WebLM for 10.1.3.0

Note: There is no Avaya WebLM Release 10.1.3.0 Avaya Aura® 10.1.3.0 Elements can use WebLM Release 10.1.2.0

What's new in Avaya WebLM for 10.1.2.x

- Avaya WebLM 10.1.2 is an OVA release.
- From Release 10.1.2, logging framework has been upgraded from Apache Log4j version 1.x to Apache Log4j version 2.x.
- Password policy for WebLM UI users.
- Password policy for CLI - OS users.
- Session timeout configuration for WebLM UI users.
- Secure communication
- TLSv1.3 Support.
- CLI utility for strict and relaxed cipher suite configuration.
- Option to mandate certificate-based communication with WebLM server and client.
- Web service login for WebLM UI – EASG (craft and init accounts)

For more information, see ***What's New in Avaya Aura® Release 10.1.x*** document on the Avaya Support site: https://downloads.avaya.com/css/P8/documents/101078425

Security Service Pack

Security Service Pack

For further information on SSP contents and installation procedures for WebLM 10.1.x, please see **PCN2154S**.

With this release 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 Communication Manager and Application Enablement Services.

CRITICAL: The Security Service Pack installation framework for WebLM has changed in Release 10.1.x.

It is imperative that the instructions in PCN2154S be reviewed for complete steps prior to installation of Security Service Packs on an WebLM 10.1.x system.

The old method of installing Security Service Packs will not work in Release 10.1.

The minimum release of WebLM 10.1.x.x that you must be on in order to install the Security Service Packs for WebLM is 10.1.2.0.

The SSP can only be installed via the command line. There is no Solution Deployment Manager (SDM) Client and System Manger Solution Deployment Manager (SDM) support for SSP installation.

In order to install the SSP for WebLM 10.1.x.x, you must use the new command ("av-update-os") and follow the detailed instructions in PCN2154S.

Required artifacts for Avaya WebLM Release 10.1.3.2

Filename	PLDS ID	File size (MB)	S/W Version number	MD5 Check Sum	Comments
WebLM_10.1.3.2_r1013216659.bin	SMGR10132GA4	556	10.1.3.2.1013216659	3700956df00f1d104872752aee943e7f	WebLM 10.1.3.2 GA bin

Required artifacts for Avaya WebLM Release 10.1.3.1

The following section provides Avaya WebLM downloading information.

Filename	PLDS ID	File size (MB)	S/W Version number	MD5 Check Sum	Comments
WebLM_10.1.3.1_r1013116147.bin	SMGR10131GA4	209	10.1.3.1.1013116147	393fe9d67ed81555f97de594dc8cf81c	WebLM 10.1.3.1 GA bin

IMPORTANT NOTE: Starting 10.1.3.1, licensing for Communication Manager (CM) and Application Enablement Services (AES) will only work with 10.1.3.1 and higher version of System Manager (SMGR) or Standalone WebLM (WebLM). If upgrading CM and/or AES to 10.1.3.1 and higher then the required order of upgrade is imperative i.e. SMGR and/or WebLM should be upgraded to 10.1.3.1 and higher first to ensure licensing for CM and/or AES does not stop working. CM and AES 10.1.3.0 were originally compatible with Standalone WebLM 10.1.2.0 (as there was no Standalone WebLM 10.1.3.0), however beginning with 10.1.3.1 and higher, Standalone WebLM 10.1.3.1 and higher is required for CM and AES. 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).

Required artifacts for Avaya WebLM Release 10.1.2.0

The following section provides Avaya WebLM downloading information.

Filename	PLDS ID	File size (MB)	Comments
WebLM 10.1.2 OVA	~~SMGR1012GA4~~ SMGR1012GA6	1320.96	~~WebLM-10.1.2.0.0-39162-e70-64.ova~~ WebLM-10.1.2.0.0-39457-e70-72.ova Please refer **PSN006085u** for more details. MD5sum : 9290fc7bb2fe37c334317182e018b424
WebLM 10.1.2 Software Only ISO	~~SMGR1012GA5~~ ~~SMGR1012GA7~~ SMGR1012GA8	90.7	~~AvayaAuraWebLM_10.1.2.0.0-39162_64.iso~~ ~~AvayaAuraWebLM_10.1.2.0.0-39457_72.iso~~ AvayaAuraWebLM_10.1.2.0.0-39690_75.iso Please refer **PSN006093u** for more details. Md5sum : 91541c18c22067725c9120a3ab2ca030

Installation for Avaya WebLM Release 10.1.2.x

Installing Release 10.1.2

Important Notes

1. WebLM Web Console will not be launched If WebLM using certificates that have SHA1 or 1024 RSA keys in the certificate chain. Please check workarounds provided by browsers so that WebLM web console is accessible.
2. Characters required in the hostname.

   WebLM hostnames must include only letters, numbers, and hyphens (-) and not underscores. For example, WebLM_62 is an invalid hostname.
3. Cloning WebLM on VMware.

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

   Ensure that the Application Server service is restarted after the WebLM restore functionality.
5. Rehost of licenses.

   - In VE deployments, the host ID of the WebLM server is a function of IP address and UUID of the system. So, if either change, a re-host of license files will be required. A re-host is required in the following scenarios:

  - Upgrade: This involves setting up a new VM with new UUID and restoring data on the same. Since UUID changes, host ID would change, and any existing files would become invalid. Re-host of licenses is required.

- An IP address is changed: If the IP address is changed, host ID changes and a re-host of license files is required.
- VMware cloning of WebLM: This would cause the UUID to change, and therefore, the host ID would change. A re-host of license files will be required.
- Re-host is not required for vMotion moves.

Resource allocation and reservation for standalone WebLM on VMware

VMware resource	Profile 1 Values that can support up to 5000 license requests (Default)	Profile 2 Values that can support more than 5000 license requests
vCPUs	1	1
CPU reservation	2290 MHz	2290 MHz
Memory	1 GB	2 GB
Memory reservation	1 GB	2 GB
Storage reservation	40 GB	40 GB
Shared NIC	1	1

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

To update the memory for WebLM on VMware:

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

Software information

Software	Version
OS	RHEL 8.6
Java	OpenJDK version "1.8.0_342" 64-bit
Application Server	WildFly Servlet 26.1.0.Final
Supported Browsers	Chrome (minimum version 91.0)
	Edge (minimum version 93.0)

Software	Version
	Firefox (minimum version 93.0)

Download *Deploying standalone Avaya WebLM in Virtualized Environment* and *Upgrading standalone Avaya WebLM* documents from Avaya Support website for WebLM on VMware deployment and upgrade.

Troubleshooting the installation

Collect logs and other information as specified below, and contact the support team.

- The status of the WebLM software. If the software is an upgrade, then the release from which the software is upgraded.

Execute the following command from Command Line Interface with customer user credentials to collect logs.

```
#collectLogs
```

This will create a file (WebLM_Logs_xxxxxxxxxxxxx.zip) at /tmp location.

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

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

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

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

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

For more information about Speculative Execution Vulnerabilities fixes included in Avaya Aura® Release 8.x, see the following PSNs on the Avaya Support Site:

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

Contacting support

Contact support checklist

Avaya Technical Support provides support for WebLM 10.1.2

For any problems with WebLM 10.1.2, you can:

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

If you continue to have problems, contact Avaya Technical Support by logging in to the Avaya Support website at http://support.avaya.com.

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

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

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

- The status of the WebLM software. If the software is an upgrade, then the release from which the software is upgraded.
- Execute the following command from Command Line Interface with customer user credentials to collect logs.

  ```
  #collectLogs
  ```

  This will create a file (WebLM_Logs_xxxxxxxxxxxxx.zip) at /tmp location.

You might be asked to send by email one or more files to Avaya Technical Support for an analysis of your application and the environment.

For information about patches and product updates, see the Avaya Support website at http://support.avaya.com.

Fixes in Avaya WebLM on VMware for 10.1.3.2

The following table lists the fixes in this release:

ID	Minimum conditions	Visible symptoms	Issue found in Release
SMGR-73617	License Management	Unable to configure IPv6 address, issue with both changeIPFQDN and deployment.	10.1.3.1
SMGR-73894	License Management	Redirect WebLM UI access to Login page once accessed through IP or FQDN.	10.1.2

Fixes in Avaya WebLM on VMware for 10.1.3.1

The following table lists the fixes in this release:

ID	Minimum conditions	Visible symptoms	Issue found in Release
SMGR-72778	License Management	Master WebLM (System Manager 10.1.2 or Standalone WebLM 10.1.2) unable to push ALF to AES 10.1.2 having local WebLM 10.1.2 war	10.1.2.0
SMGR-73077	License Management	WebLM 10.1.2 Trust establishment failing on 10.1.3.x SMGR SDM	10.1.3.0
SMGR-73231	License Management	Standalone WebLM crashing causing license issues.	10.1.2.0

Fixes in Avaya WebLM on VMware for 10.1.2

The following table lists the fixes in this release:

ID	Minimum Condition	Visible Symptoms
SMGR-60026	License Management	WebLM SSP version should be more clearly when command swversion -s executed.
SMGR-70837	License Management	Vulnerability-Unauthorized HTTP Methods Detected Vulnerability issue.
SMGR-60598	License Management	Daily license error seen on CM, AMS and etc
SMGR-70835	License Management	Vulnerability-Multiple Vulnerability issue regarding Wildfly reported on WebLM.
SMGR-70836	License Management	Vulnerability-Weak Password Policy Vulnerability issue reported on WebLM.
SMGR-70878	License Management	Vulnerability-Client side contrôle bypass Vulnerability issue reported on WebLM.
SMGR-71708	License Management	Permission denied errors during SSH login using "EASG" login
SMGR-71831	License Management	Error while command "swversion -s" executed by cust user.
SMGR-69599	License Management	Vulnerability-Multiple Password_Requirements issue on WebLM.
SMGR-69602	License Management	Vulnerability-Multiple Vulnerability issue reported by on WebLM.
SMGR-70398	License Management	Software only standalone WebLM does not generate challenge for EASG login.
SMGR-69673	License Management	Following weak key exchange algorithms are enabled in Licensing component. - diffie-hellman-group-exchange-sha1

Known issues and workarounds in Avaya WebLM for 10.1.x.x

Known issues and workarounds in Avaya WebLM for 10.1.3.2

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

ID	Minimum Condition	Visible symptoms	Workaround
SMGR-74488	License Management	Unable to install more than 39 product license files on SMGR Licensing Manager (WebLM).	Uninstall unused license file if any and install required file. Or Use alternate licensing server to install license file.

Known issues and workarounds in Avaya WebLM for 10.1.3.1

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

ID	Minimum Condition	Visible symptoms	Workaround
SMGR-73617	Infrastructure	WebLM: unable to configure IPV6 address, issue in both changeIPFQDN and deployment.	

Known issues and workarounds in Avaya WebLM for 10.1.2

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

ID	Visible symptoms	Workaround
SMGR-54491	Infrastructure	Run changeIPFQDN script to update new DNS entries. Ex: **changeIPFQDN -dns 135.10.209.250,135.64.19.82**

Avaya Device Adapter Snap-in

What's new in Avaya Device Adapter Snap-in Release 10.1.x.x

What's new in Avaya Device Adapter Snap-in for 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.

What's new in Avaya Device Adapter Snap-in for 10.1.2

For more information see ***What's New in Avaya Aura® Release 10.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101078425

What's new in Avaya Device Adapter Snap-in for 10.1

For more information see ***What's New in Avaya Aura® Release 10.1.x*** document on the Avaya Support site:

https://downloads.avaya.com/css/P8/documents/101078425

Required artifacts for Avaya Device Adapter Release 10.1.x.x

Required artifacts for Avaya Device Adapter Release 10.1.2

The following section provides Avaya Device Adapter downloading information.

Download ID	Artifacts	Notes
ADA0000016	DeviceAdapter-10.1.2.0.14002	File size: 86.2 Mb MD5:98D4086442A32FC29508830AA4ED1C0D

Required artifacts for Avaya Device Adapter Release 10.1.0.1

The following section provides Avaya Device Adapter downloading information.

Download ID	Artifacts	Notes
ADA0000014	DeviceAdapter-10.1.0.1.42464	File size: 85.7 MB MD5: 381d63ee9c98e4424a40e5c63fc810ce

Required artifacts for Avaya Device Adapter Release 10.1

The following section provides Avaya Device Adapter downloading information.

Download ID	Artifacts	Notes
ADA0000013	DeviceAdapter-10.1.0.0.82424	File size: 79.3 MB MD5: cb63f01e020e1a19e490a6f57d452b85

Installation for Avaya Device Adapter Snap-in for 10.1.x.x

Installation for Avaya Device Adapter Snap-in for 10.1.2

Refer to the Avaya Device Adapter Snap-in Reference Guide for installation instructions.

https://downloads.avaya.com/css/P8/documents/101078928

Installation for Avaya Device Adapter Snap-in for 10.1

Refer to the Avaya Device Adapter Snap-in Reference Guide for installation instructions.

https://downloads.avaya.com/css/P8/documents/101078928

Fixes in Avaya Device Adapter Snap-in for 10.1.x.x

Fixes in Avaya Device Adapter Snap-in for 10.1.2

ID	Problem
SETADAPT-9733	MGC upgrade causes deadlock in dsa application
SETADAPT-9321	Incoming PSTN PRI calls that terminate to ADA stations with BA of the dialed extension cannot answer the call on the BA.
SETADAPT-9936	ADA Units will not Registered
SETADAPT-9925	Breeze Critical error issue when TN was moved
SETADAPT-9924	Oneway speech path answering an incoming call when you are inside address book
SETADAPT-9883	Failed to get data for cluster Breeze1wcq_cluster: unable to retrieve MGC list
SETADAPT-9839	Wrong clid when we have configured "hidden internal number".
SETADAPT-9809	ADA does not send consistent UUID value
SETADAPT-9798	MGC Load Balancer improvement
SETADAPT-9740	DSA coredump when History Info header contains no username

Fixes in Avaya Device Adapter Snap-in for 10.1.0.1

ID	Problem
SETADAPT-9733	ADA TDM and UNIStim sets cannot register because of the blocked registration queue on ADA snapin side
SETADAPT-9724	Analog sets get stuck, no calls possible

Fixes in Avaya Device Adapter Snap-in for 10.1

ID	Problem
SETADAPT-9508	unbound-libs package is vulnerable to attacks related to CVE-2020-10772
SETADAPT-9471	Intermittent ADA snapin component TPS crashes because of double free() during PD request handling
SETADAPT-9541	Intermittent TPS coredump in VO operation
SETADAPT-9406	Intermittent DSA coredump during regular traffic
SETADAPT-9461	Issue with RTC (Real Time Clock) on TDM digital phones
SETADAPT-9516	Confusing context softkey handling during Call forward operation activation on 39xx sets

Known issues and workarounds for Avaya Device Adapter Snap-in for 10.1.x.x

Known issues and workarounds for Avaya Device Adapter Snap-in for 10.1.2

ID	Problem	Workaround
SETADAPT-9288	AVAYA EQUINOX CONFERENCING: Unable to join Conference with ADA phone, when have Meeting Type = Audio Service	No Workaround. Corrected on CM side, from release 10.2 – 3rd party issue. Exists from 8.1.4.
SETADAPT-5890	COREDUMP: ADA pbxserver coredumps are generated when restart DSA service when we have MGC's registered (This Coredump is not service impacting)	No Workaround. Exists from 8.1.3
SETADAPT-9695	ADA endpoints do not unregister in real time	No Workaround. Day one implementation, fix to be implemented in 10.2 ADA version

Known issues and workarounds for Avaya Device Adapter Snap-in for 10.1.0.1

ID	Problem	Workaround
SETADAPT-9288	AVAYA EQUINOX CONFERENCING: Unable to join Conference with ADA phone, when have Meeting Type = Audio Service	No Workaround. Corrected on CM side, from release 10.2 – 3rd party issue. Exists from 8.1.4.
SETADAPT-5890	COREDUMP: ADA pbxserver coredumps are generated when restart DSA service when we have MGC's registered (This Coredump is not service impacting)	No Workaround. Exists from 8.1.3
SETADAPT-9695	ADA endpoints do not unregister in real time	No Workaround. Day one implementation, fix to be implemented in 10.2 ADA version

Known issues and workarounds for Avaya Device Adapter Snap-in for 10.1

ID	Problem	Workaround
SETADAPT-9288	AVAYA EQUINOX CONFERENCING: Unable to join Conference with ADA phone, when have Meeting Type = Audio Service	No Workaround – 3rd party issue. Exists from 8.1.4
SETADAPT-5890	COREDUMP: ADA pbxserver coredumps are generated when restart DSA service when we have MGC's registered (This Coredump is not service impacting)	No Workaround. Exists from 8.1.3

Usually customers who works with ADA snapin are migrated from CS1000 – important note that at GA date 13 December before CS1000 can be used with AURA 10.1 need to perform the following manual steps on SMGR server:

Please apply this commands rights after installation (root access is required):

1) root >chmod 755 /var/opt/nortel/Jboss-Quantum

   root >chmod 755 /var/opt/nortel/Jboss-Quantum/conf

2) edit /etc/ssh/sshd_config:

   root >vim /etc/ssh/sshd_config

   in MACs line append **hmac-sha1**

   restart SSH:

   root >service sshd restart

This is to be corrected in SMGR GA patch from Dec 31 2021.

Avaya Device Adapter General Limitations 10.1.x.x

Avaya Device Adapter General Limitations for 10.1.2

NA

Avaya Device Adapter General Limitations for 10.1.0.1

NA

Avaya Device Adapter General Limitations for 10.1

Contacts handling logic limitation

When User adds new contact into his contact list from Personal directory there could occur 2 different situations:

- Newly added contact has exactly same phone number (extension of the station) as station number configured via SMGR
  - after contact added it will have same First and Last names as it was in PD search/or manually entered values unless:
    - station experienced network recovery
    - station re-registers
    - admin change any value for the station via SMGR/CM
  - if one of scenarios from previous bullet occurs new Contact information will be shown to the user - First and Last name exactly same as configured for station with same phone number/extension. This is known as **Associated contact**

        - **Associated contact**s can't be edited from endpoint site. Result of operation is **SUCCESS** but user will see exactly same First and Last name as station with same phone number/extension.
        - **Associated contact** can be changed only by admin via SMGR - change user's (with phone number as contact) First/Last name.
    - Newly added contact does not have matching phone number (extension of the station) as station number configured via SMGR
        - after contact added it will have same First and Last names as it was in PD search/or manually entered values
        - user is able to edit contact - no limitations.

Avaya Device Adapter General Limitations for 10.1.x.x

- SMGR, SM, CM, AMS, Breeze server installation, and initialize configuration must be ready to use. Refer to these product release notes for more information.

Specific requirements for Avaya Device Adapter include:

1. TLS links should be enabled for all Entities (Breeze and CM to SM, AMS links to CM, you can skip AMS if you have Media Gateway to provide DSP for your CM)
2. Certificates installation and configuration
3. Administrator user should have a dialing plan, a user (stations), signaling, and trunk groups to Session Manager be configured and ready to use before installing and using Avaya Device Adapter snap-in.
4. Activate root access for: SMGR, Breeze, Session Manager

    - The NODE IP of the CS1000 TPS mapping is not required anymore. Automatically it will be set to Secure/SIP IP address of the Breeze server (in case of a single server) or in case of using multiple Breeze servers within a cluster, the NODE IP automatically maps to the Cluster IP.

5. If you use the existing IP address, then the CS1000 phone admin doesn't need to change
6. If you use a new IP address, then you will have to have the phone admin change, but this is useful if you want to take a subset of your CS1000 population to test out the new configuration before cutting all your users.

    - Confirm your enrollment password is NOT expired before upgrading/installing new Breeze nodes.
    - Call Park is now supported for Unistim sets starting from Device Adapter 8.0 Service Park 1. To configure Call Park, need to install Call Park and Page Snap-in on a separate Breeze server.

For **each node** in the cluster, we require:

1. An additional SIP Entity of the "Endpoint Concentrator" type
2. An Entity Link from the above SIP Entity to every "relevant" SM in the solution (the Connection Policy of the Entity Link must be set to "Endpoint Concentrator")

    - You must uninstall **and delete** all previous Avaya Device Adapters on SMGR before loading the **SVAR** file of the new Device Adapter.

    In this case, SMGR will display a pop-up message about the necessity to restart Device Adapter when a user updates the attributes.

1. The "Signaling Security Error" message is displayed on the IP Deskphone display during the registration process.

   The following items should be checked:

   DTLS settings have been propagated to TPS form SMGR. Check /opt/Avaya/da/shared/config/config.ini
   Please note that snapin root path was changed from /opt/Avaya/snap_in/da/ to /opt/Avaya/da.

   ```
   # cat /opt/Avaya/da/shared/config/config.ini
   …
   [UNIStim DTLS]
   TPS_DTLS=1                          // 0 – Off, 1 – Best effort, 2 - Always
   DTLSClientAuthentication=0
   ```

   Note: Avaya Device Adapter snap-in must be restarted in SMGR UI after changing the attribute.

2. Check Port and action byte configured at the phone.

   Following security levels with DTLS (the terminology is kept from CS1000):
   - Basic. The DTLS policy is configured as Best effort. Phones are configured with action byte 1 and Port 4100. There is a brief period of insecure signaling at the beginning of registration. If IP Deskphone has installed the CA Root certificate, then it continues registration using DTLS after a brief period of insecure. In case of certificates, mismatch registration will fail.

   - Advanced. The policy is configured as Best Effort. DTLS-capable phones are configured with action byte of 7 and Port 4101. DTLS incapable configured with action byte of 1. If IP Deskphone is DTLS capable, configured with action byte of 1 and Port 4100, and has installed CA Root certificate, then it continues registration using DTLS after a brief period of insecure. In the case of a certificate mismatch registration will fail.

   - Complete. The policy is configured as Always. All IP Phones are DTLS-capable and configured with action byte 7 and Port 4101. Insecure registrations are not permitted. In the case of a certificate mismatch registration will fail.

3. Check that DTLS ports are open by csv and tps:

   ```
   # netstat -unap | grep -E "4101|5101|8301"
   udp      0      0 192.168.96.115:8301     0.0.0.0:*                   9190/tps
   udp      0      0 192.168.96.115:4101     0.0.0.0:*                   15320/csv
   udp      0      0 192.168.96.115:5101     0.0.0.0:*                   9190/tps
   ```

Important: If you have made keystore and truststore cert changes after snap-in installation, then following commands should be executed from Breeze cli as root:

```
# cd /opt/Avaya/da/
# ./avaya_securitymodule_pki_tool init da dauser > sm_pki_descriptor_da.txt
```

4. Try to reset the phone to factory defaults to delete the previous CA root certificate that was on the set. Procedure for resetting IP Deskphones factory defaults can be found in NN43001-368 "IP Deskphones Fundamentals Avaya Communication Server 1000".
   Then install the SMGR root CA again as described in NN43001-368 "IP Deskphones Fundamentals Avaya Communication Server 1000".
5. In case for 2050 CA certificate should be installed into Trusted Root Certification Authorities->Local Machine. By default, the certificate manager installs it into Trusted Root Certification Authorities->Registry (at least in Windows 7, see https://superuser.com/questions/647036/view-install-certificates-for-local-machine-store-on-windows-7).

- Mnemonics for Hotline buttons emulated using the brdg-appr or call-appr buttons
- Personal Directory: Stores up to 100 entries per user of user names and DNs.
- Callers List: Stores up to 100 entries per user of caller ID information and most recent call time
- Redial List: Stores up to 20 entries per user of dialed DNs and received Call Party Name Display with time and date.

MGC configuration

1. For MGC previously registered in Security Domain at CS1000 system:
   - Login to Call Server in CS1000 option;
   - Enable PDT2 mode for admin2 account at CS;
   - login to overlay supervisor -
     ld 17:

     REQ: chg

     TYPE: pwd

     ACCOUNT_REQ: chg

     USER_NAME: admin2

     PDT: pdt2

2. If you know your MGC ELAN IP address, you can skip this step:

2.1 Physically connect MGC (COM RS232 port) to your PC via COM-USB cable. Run any terminal application (For example, PuTTY) and use a SERIAL connection with following settings:

Port: COM3

Baud Rate: 9600

Data Bits: 1

Parity: None

Flow Control: None

2.2 With **mgcinfoshow** command at MGC you can determine your MGC ELAN IP address.

3. MGC Loadware upgrade.

3.1 **MGC Loadware upgrade from CS1000 release**.

1. Turn on "Enable legacy loadware upgrades" Breeze attribute and set it to "yes"
2. From MGC in ldb shell under pdt2 user:
3. enter “leaveSecDomain”, “isssDecom” command;

4. run “portAccessOff”;
5. run mgcsetup with changing the IP of DA.
6. From SMGR Inventory page, add new DA Media Gateway

3.2 **MGC manually Loadware upgrade**.

1. Connect to your MGC ELAN IP address via SSH connection and pdt2/2tdp22ler or admin2/0000 credentials.
2. Go to debug mode by pressing **ctrl+l+d+b** and enter pdt2/admin2 credentials
3. Run **ftpUnprotectP** command to unprotect **/p** partition.
4. Connect to your MGC ELAN IP address via SFTP.

   Now all MGC loadware is integrated inside snapin. All upgrade procedure for MGC loads NA08 and upper will be done automatically.

   To upgrade from old MGC release, need take MGC load file placed at /opt/Avaya/da/mgc/loadware/current on your Breeze server. The filename will be similar to MGCCNXXX.LD. Copy it on your machine.
5. Extract with zip archiver mainos.sym and mainos.sym files from *.LD loadware file and copy them to /p partition of MGC
6. Reboot MGC with **reboot** command from ldb.

MGC registration:

- Create new one or make changes at SMGR->Inventory->Manage elements->MGC
  - Recommended to use Mu-law for companding law settings for MGC and Avaya Device Adapter attributes;
  - Assign new MGC to Breeze cluster;
  - Commit changes
- Connect to your MGC via SSH and run **mgcsetup** command:

  1. Enter ELAN IP: **192.168.127.91** (for example) (enter)

     An important tip. Do not try to erase with Delete or Backspace buttons. It does not work. Just input new values and push Enter.
  2. Enter ELAN subnet mask: **255.255.255.0** (in my example) (enter)
  3. Enter ELAN gateway IP: **192.168.127.1** (in my example) (enter)
  4. Enter Primary CS IP: **192.168.39.26** (Breeze node's SIP/Secure interface in my example) (enter)
  5. Configure IPsec now? (y/[n]) : **n** (enter)
  6. Change MGC advanced parameters? (y/[n]) : **n** (enter)
  7. Is this correct? (y/n/[a]bort) : **y** (enter)
  8. Reboot MGC
- You can validate new configuration parameters at MGC with **cat /u/db/mgcdb.xml** from ldb **ONLY** with next successful connection establishing between MGC and Breeze.

Digital and analog sets registration

- Create new one user with **CS1k-1col_DEFAULT_CM_8_1, CS1k-2col_DEFAULT_CM_8_1, CS1k-39xx_DEFAULT_CM_8_1 or CS1k-ana_DEFAULT_CM_8_1** template at CM Endpoint profile. Select valid Sub type and Terminal number (System ID if need):

- Plug-in your digital or analog sets to DLC/ALC card at MGC.

- Validate your registration at SMGR with Session Manager->System status->User registrations

  You can verify digital sets registration with:

  At SMGR with Session Manager->System status->User registrations

  At digital phone by itself (keymap is presented)

From Breeze side: dsaShell dsaShow

From Breeze side - IPE card status with: ipeShow <loop>-<shelf>-<card>-<unit>

If your DLC card is still blinking red, remove the card from the cabinet and plug-in again, for re-detecting.

From Breeze side VGW channel status with: vgwShow <loop>-<shelf>-<card>-<unit>

- You can verify analog sets registration at SMGR with Session Manager->System status->User registrations

IPSEC configuration

- You must enable and fill PSK key (generate it according to description) at Avaya Breeze -> Configuration -> Attributes -> Service Globals -> DeviceAdapter service

  You can check created files (activate.txt and ipsec.xml) and configuration parameters at: /opt/Avaya/da/shared/config/MGC/ folder.

- Run **mgcsetup** at MGC and following the IPsec configuration procedure and **reboot**.
- To stop IPsec, run the following command:
  - Disable checkbox at Breeze attributes.
  - i**sssDecom** at MGC

Corporate Directory (AADS) configuration

For activation of Corporate directory necessary:

- Set CRPA flag in feature field on the phone;
- Configure AADS server (and LDAP server) on SMGR;
- Enable AADS server for cluster or global and fill URL and port for the AADS server.

Creating and configuration of users on LDAP.

For used Corporate Directory necessary to create a user on LDAP server with the next parameters: login and password should be as an extension for the user.

Device Adapter Limitations

There is no method to migrate customer settings for Call Forward feature.

Avaya Device Adapter Feature Interaction Limitations for 10.1.x.x

Avaya Device Adapter Product Interoperability for 10.1.x.x

Product	Release Details
Avaya Aura® System Manager	10.1.x
Avaya Aura® Session Manager	10.1.x
Avaya Aura® Communication Manager	10.1.x
Avaya Aura® Media Server	10.1.x
Avaya Aura® Device Services	10.1.x
SBCE	10.1
Avaya Breeze	3.8.1
Avaya Aura® Workspaces	3.6

Avaya Aura® Device Services

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

- Release 10.1.1.2 Release Notes at: https://support.avaya.com/css/public/documents/101086451
- Release 10.1.1.1 Release Notes at: https://download.avaya.com/css/public/documents/101084735
- Release 10.1.1.0 Release Notes at: https://download.avaya.com/css/public/documents/101083649
- Release 10.1.0.1 Release Notes at: https://download.avaya.com/css/public/documents/101081725
- Release 10.1.0.0.120 Release Notes at: https://download.avaya.com/css/public/documents/101079265