



Avaya Aura® Media Server (AAMS) Release Notes

Release 10.2 SP 3
Issue 1.6
August 11, 2025

© 2025 Avaya LLC

All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: <https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010> under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You

acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

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

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](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.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. “Named User,” means a user or device

that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

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

Heritage Nortel Software

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

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction,

transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

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

Third Party Components

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

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE

AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](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](http://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](http://www.mpegla.com).

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow

(<https://support.avaya.com/css/P8/documents/100161515>).

Trademarks

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

license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya 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	9
Introduction	10
What's new	10
What's new in 10.2	10
What's new in 10.2 SP 1	10
What's new in 10.2 SP 2	10
What's new in 10.2 SP 3	10
Contacting support.....	10
Contact support checklist	10
Contact support tasks	11
Avaya Aura® Media Server.....	11
Software Compatibility	11
Supported Upgrade Paths	11
8.0.2 to 10.2 Appliance Upgrade Considerations	11
10.1 to 10.2 Appliance Upgrade Considerations	12
10.2.0.x to 10.2.0.y Appliance Upgrade Considerations	12
Installation	12
10.2.0 New Installation File List (VMWare Virtual Appliance Only)	12
10.1.0 New Installation File List (ASP 130 KVM Virtual Appliance Only)	13
10.2.0 New Installation File List (Physical Appliance Only)	13
10.2.0 New Installation File List (Customer Supplied Hardware and OS Only)	13
10.2.0 Required Updates and Hotfixes (Appliance Only)	13
10.2.0 Required Updates and Hotfixes (Customer Supplied Hardware and OS Only)	14
10.2.0 Patch File list (Appliance Only)	14
10.2.0 Patch File list (Customer Supplied Hardware and OS Only)	14
Installing the release	14
Backing up the software	15
Troubleshooting the installation	15
Restoring software to previous version	15
Enhanced Access Security Gateway (EASG).....	15
SELinux and su operations.....	15
Session Detail Record Archiving	15
Debug Log Retention.....	16
Functionality not supported	16
Fixes	16
Fixes in System Layer for 10.2 GA (10.0.0.29)	16
Fixes in Media Server for 10.2 GA (10.2.0.52)	18
Fixes in System Layer for 10.2 SP 1 (10.0.0.30)	19
Fixes in Media Server for 10.2 SP 1 (10.2.0.61)	22

Fixes in System Layer for 10.2 SP 2 (10.0.0.31).....	22
Fixes in Media Server for 10.2 SP 2 (10.2.0.72)	24
Fixes in System Layer for 10.2 SP 3 (10.0.0.32).....	25
Fixes in Media Server for 10.2 SP 3 (10.2.0.80)	29
Known issues and workarounds	29
Known issues and workarounds	29
Languages supported	30
Documentation errata	30

Change history

Issue	Date	Description
1.6	August 11, 2025	AAMS 10.2 SP 3
1.5	April 28, 2025	AAMS 10.2 SP 2
1.4	March 24, 2025	AAMS 10.2 SP 1
1.3	March 3, 2025	Updated installer/recovery download that supported ASP-110 Dell R660.
1.2	February 14, 2025	Added clarification on how to configure TLSv1.2.
1.1	December 23, 2024	Added KVM and signed OVA artifacts.
1	December 9, 2024	Initial release of AAMS 10.2

Introduction

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

The Avaya Aura® Media Server delivers advanced multimedia processing features to a broad range of products and applications. Utilizing the latest open standards for media control and media processing, the highly scalable software-based solution deploys on standard server hardware. It is comprised of the following components:

- Media Server Software
- System Layer (appliance only).

What's new

What's new in 10.2

The following table lists enhancements in this release.

Enhancement	Description
AMS-16054	ASP 110 Dell R660 support
AMS-15387	TLSv1.3

What's new in 10.2 SP 1

The following table lists enhancements in this release.

Enhancement	Description
AXP-2598 AMS-15379	Secure boot support for customer supplied OS and appliance. Note that secure is only enabled on new deployments for all appliance types (physical, VMware virtual, and KVM virtual).

What's new in 10.2 SP 2

The following table lists enhancements in this release.

Enhancement	Description
N/A	

What's new in 10.2 SP 3

The following table lists enhancements in this release.

Enhancement	Description
N/A	

Contacting support

Contact support checklist

If you are having trouble with *Avaya Aura® Media Server*, you should:

1. Retry the action. Carefully follow the instructions in written or online documentation.

2. Check the documentation that came with your software for maintenance or software-related problems.
3. Note the sequence of events that led to the problem and the exact messages displayed.

If you continue to have a problem, contact Avaya Technical Support:

1. Log in to the Avaya Technical Support Web site <https://support.avaya.com>.
2. Contact Avaya Technical Support at one of the telephone numbers in the Support Directory listings on the Avaya support Web site.

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

Contact support tasks

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

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

Avaya Aura® Media Server

Software Compatibility

Prior to upgrading AAMS software you must review the Avaya [compatibility matrix](#) of the controlling application (i.e. CM) to ensure that the controlling application has been tested and is compatible with AAMS.

Supported Upgrade Paths

Prior to upgrading to AAMS 10.2.0 your prior installation must meet the following minimum software revisions for the Media Server software:

Release	Minimum Supported
8.0.2	8.0.2.56 or higher
10.1.0	10.1.0.77 or higher

8.0.2 to 10.2 Appliance Upgrade Considerations

Before upgrading the 8.0.2 AAMS appliance (virtual or physical) to 10.2 consider the following:

- Stage both media server and system layer updates before attempting upgrade. Ensure that you are using the most recent 10.2 versions of each update.
- Rollbacks from 10.2 to 8.0.2 is not supported. Prior to doing upgrade please ensure you take a backup and transfer the backup off the server. Installation media (ISO/OVA plus updates) of the previous 8.0.2 release should be on-hand in case you need to revert back to 8.0.2. For virtual appliances it is recommend you take a snapshot prior to doing the upgrade.
- TLSv1.3 only is enabled by default after upgrading. If AAMS is communicating with an application that requires TLSv1.2 you will need to update AAMS configuration to use TLSv1.2 or TLSv1.3. In EM navigate to **System Configuration » Network Settings » General Settings**, click **Connection Security**, set **Minimum TLS Version**, and reboot the Linux VM for the changes to take effect.

- Ensure that one of these partitions have approximately 2 GB of free space. If it doesn't customer should cleanup files in /root, /var, pub (/opt/ayaya/pub) and/or local media directory (/opt/avaya/app) to free up disk space.

/opt/avaya/app

/var

/

- 8.0.2 doesn't backup authenticated NTP configuration. After upgrading authenticated NTP configuration is not preserved and manual authenticated NTP configuration is required. Configuration setting **Reject SRTP Audio On SSRC Reuse** has been removed and SSRC reuse is enabled by default. There are no configuration settings to disable.

10.1 to 10.2 Appliance Upgrade Considerations

Before upgrading the 10.1 AAMS appliance (virtual or physical) to 10.2 consider the following:

- Stage both media server and system layer updates before attempting upgrade. Ensure that you are using the most recent 10.2 versions of each update.
- Rollbacks from 10.2 to 10.1 is not supported. Prior to doing upgrade please ensure you take a backup and transfer the backup off the server. Installation media (ISO/OVA plus updates) of the previous 10.1 release should be on-hand in case you need to revert back to 10.1. For virtual appliances it is recommend you take a snapshot prior to doing the upgrade.
- TLSv1.3 only is enabled by default after upgrading. If AAMS is communicating with an application that requires TLSv1.2 you will need to update AAMS configuration to use TLSv1.2 or TLSv1.3. In EM navigate to **System Configuration » Network Settings » General Settings**, click **Connection Security**, set **Minimum TLS Version**, and reboot the Linux VM for the changes to take effect.

10.2.0.x to 10.2.0.y Appliance Upgrade Considerations

Before upgrading the 10.2.0.x AAMS appliance (virtual or physical) to 10.2.0.y consider the following:

- Stage both media server and system layer updates before attempting upgrade. Ensure that you are using the most recent 10.2 versions of each update.

Installation

10.2.0 New Installation File List (VMWare Virtual Appliance Only)

Download ID	Filename	Notes
MSR000000218	MediaServer_10.2.0.61_A3_2025.01.14_OVF10.ova	<p>AAMS virtual appliance (OVA) for new deployments.</p> <p>Appliance contains Media Server 10.2.0.61 and System Layer 10.0.0.30.</p> <p>NOTE after deploying the OVA you MUST install the mandatory updates listed in the section titled "10.2.0 Required Updates and Hotfixes (Appliance Only)". If the updates are the same version as what is</p>

Download ID	Filename	Notes
		<i>installed on the appliance then no action is required.</i>

10.1.0 New Installation File List (ASP 130 KVM Virtual Appliance Only)

Download ID	Filename	Notes
MSR000000220	MediaServer_10.2.0.61_A3_2025.01.14_KVM.bin	<p>AAMS virtual appliance KVM image for new ASP 130 deployments.</p> <p>Appliance contains Media Server 10.2.0.61 and System Layer 10.0.0.30.</p> <p>NOTE after deploying the KVM you MUST install the mandatory updates listed in the section titled “10.2.0 Required Updates and Hotfixes (Appliance Only)”. If the updates are the same version as what is installed on the appliance then no action is required.</p>

10.2.0 New Installation File List (Physical Appliance Only)

Download ID	Filename	Notes
MSR000000219	MediaServer_10.2.0.61_A3_2025.01.14.iso	<p>AAMS physical appliance installer and recovery disk for new appliance deployments.</p> <p>Appliance contains Media Server 10.2.0.61 and System Layer 10.0.0.30.</p> <p>NOTE after installing the appliance you MUST install the mandatory updates listed in the section titled “10.2.0 Required Updates and Hotfixes (Appliance Only)”. If the updates are the same version as what is installed on the appliance then no action is required.</p>

10.2.0 New Installation File List (Customer Supplied Hardware and OS Only)

Download ID	Filename	Notes
MSR000000227	MediaServer_10.2.0.80_2025.07.28.bin	AAMS software only installer (PVI) for new deployments where customer is supplying the hardware and Linux OS.

10.2.0 Required Updates and Hotfixes (Appliance Only)

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

Download ID	Patch	Notes
MSR000000228	10.2.0.80	AAMS update for Media Server software that needs to be applied to all 10.2 appliance deployments.
MSR000000229	10.0.0.32	AAMS update for System Layer software that needs to be applied to all 10.2 appliance deployments.

10.2.0 Required Updates and Hotfixes (Customer Supplied Hardware and OS Only)

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

Download ID	Patch	Notes
MSR000000227	10.2.0.80	AAMS software only installer (PVI) for new deployments where customer is supplying the hardware and Linux OS.

10.2.0 Patch File list (Appliance Only)

Filename	File size	Version
MediaServer_System_Update_10.0.0.32_2025.07.11.iso	2,281,039,872	10.0.0.32
MediaServer_Update_10.2.0.80_2025.07.28.iso	830,167,040	10.2.0.80

10.2.0 Patch File list (Customer Supplied Hardware and OS Only)

Filename	File size	Version
MediaServer_10.2.0.80_2025.07.28.bin	829,786,831	10.2.0.80

Installing the release

For appliance installations, see procedures documented in *Deploying and Updating Avaya Aura® Media Server Appliance* on the Avaya Support website at: <https://support.avaya.com/css/secure/documents/101092087>.

For Customer Supplied Hardware and OS installations, refer to procedures documented in *Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS* on the Avaya Support at: <https://support.avaya.com/css/secure/documents/101092091>.

When upgrading an appliance, use the following procedure:

1. Backup the system.
2. Upload both system layer and media sever updates.
3. Place system in pending lock (one node at a time).
4. Click "Install Updates" in Element Manager to initiate update install.

5. Once installation complete place system in an unlocked state.

Backing up the software

For appliance installations, see procedures documented in *Deploying and Updating Avaya Aura® Media Server Appliance* on the Avaya Support website at: <https://support.avaya.com/css/secure/documents/101092087>.

For Customer Supplied Hardware and OS installations, see procedures documented in *Implementing and Administering Avaya Aura® Media Server* on the Avaya Support website at: <https://support.avaya.com/css/secure/documents/101092091>.

Troubleshooting the installation

For appliance installations, see procedures documented in *Deploying and Updating Avaya Aura® Media Server Appliance* on the Avaya Support website at: <https://support.avaya.com/css/secure/documents/101092087>.

For non-appliance installations, see procedures documented in *Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS* on the Avaya Support website at: <https://support.avaya.com/css/secure/documents/101092091>.

Restoring software to previous version

For appliance installations refer to procedures documented in *Deploying and Updating Avaya Aura® Media Server Appliance* on the Avaya Support site at: <https://support.avaya.com/css/secure/documents/101092087>.

For non-appliance installations, see procedures documented in *Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS* on the Avaya Support website at: <https://support.avaya.com/css/secure/documents/101092091>.

Enhanced Access Security Gateway (EASG)

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

On the AAMS appliance EASG is disabled by default so customers that are deploying a new appliance for the first time are encouraged to enable EASG, which can be done by issuing the following command after upgrading.

```
EASGManage --enableEASG
```

SELinux and su operations

When SELinux is enabled su operations will prompt first for the current users credentials followed by the target users credentials.

Session Detail Record Archiving

As of AAMS 8.0.2 SP2 Session Detail Record (SDR) archiving is disabled by default. SDR archiving can be enabled with AAMS Element Manager by navigating to *Home » System Configuration » Logging Settings* and clicking the *Session Logging*. To enable SDR archiving ensure the *Session Detail Record Archiving* is check and click save.

Debug Log Retention

As of AAMS 8.0.2 SP2 debug log rotation will be enabled by default when debug logging is enabled. Debug logs will rotate every hour and will only be retained for 1 day. Log retention settings can be disabled, or retention time can be modified using AAMS Element Manager. To modify log retention settings, navigate to *Home » System Configuration » Debug Tracing » General Settings* and update *Trace File Retention Limit* setting accordingly.

Functionality not supported

N/A

Fixes

Fixes in System Layer for 10.2 GA (10.0.0.29)

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AMS-15845	All appliance	Include virtualization type in log capture
AMS-15930	All appliance	Update to clamav 1.0.7
AMS-15955	All appliance	<p>Update RPMs to address outstanding security advisories</p> <p>RHSA-2024:8856 https://access.redhat.com/errata/RHSA-2024:8856</p> <p>kernel-4.18.0-553.27.1.el8_10.x86_64</p> <p>kernel-core-4.18.0-553.27.1.el8_10.x86_64</p> <p>kernel-modules-4.18.0-553.27.1.el8_10.x86_64</p> <p>https://access.redhat.com/security/cve/CVE-2022-48773</p> <p>https://access.redhat.com/security/cve/CVE-2022-48936</p> <p>https://access.redhat.com/security/cve/CVE-2023-52492</p> <p>https://access.redhat.com/security/cve/CVE-2024-24857</p> <p>https://access.redhat.com/security/cve/CVE-2024-26851</p> <p>https://access.redhat.com/security/cve/CVE-2024-26924</p> <p>https://access.redhat.com/security/cve/CVE-2024-26976</p> <p>https://access.redhat.com/security/cve/CVE-2024-27017</p> <p>https://access.redhat.com/security/cve/CVE-2024-27062</p> <p>https://access.redhat.com/security/cve/CVE-2024-35839</p> <p>https://access.redhat.com/security/cve/CVE-2024-35898</p> <p>https://access.redhat.com/security/cve/CVE-2024-35939</p> <p>https://access.redhat.com/security/cve/CVE-2024-38540</p>

ID	Minimum conditions	Description
		https://access.redhat.com/security/cve/CVE-2024-38541 https://access.redhat.com/security/cve/CVE-2024-38586 https://access.redhat.com/security/cve/CVE-2024-38608 https://access.redhat.com/security/cve/CVE-2024-39503 https://access.redhat.com/security/cve/CVE-2024-40924 https://access.redhat.com/security/cve/CVE-2024-40961 https://access.redhat.com/security/cve/CVE-2024-40983 https://access.redhat.com/security/cve/CVE-2024-40984 https://access.redhat.com/security/cve/CVE-2024-41009 https://access.redhat.com/security/cve/CVE-2024-41042 https://access.redhat.com/security/cve/CVE-2024-41066 https://access.redhat.com/security/cve/CVE-2024-41092 https://access.redhat.com/security/cve/CVE-2024-41093 https://access.redhat.com/security/cve/CVE-2024-42070 https://access.redhat.com/security/cve/CVE-2024-42079 https://access.redhat.com/security/cve/CVE-2024-42244 https://access.redhat.com/security/cve/CVE-2024-42284 https://access.redhat.com/security/cve/CVE-2024-42292 https://access.redhat.com/security/cve/CVE-2024-42301 https://access.redhat.com/security/cve/CVE-2024-43854 https://access.redhat.com/security/cve/CVE-2024-43880 https://access.redhat.com/security/cve/CVE-2024-43889 https://access.redhat.com/security/cve/CVE-2024-43892 https://access.redhat.com/security/cve/CVE-2024-44935 https://access.redhat.com/security/cve/CVE-2024-44989 https://access.redhat.com/security/cve/CVE-2024-44990 https://access.redhat.com/security/cve/CVE-2024-45018 https://access.redhat.com/security/cve/CVE-2024-46826 https://access.redhat.com/security/cve/CVE-2024-47668 RHSA-2024:8833 https://access.redhat.com/errata/RHSA-2024:8833 libtiff-4.0.9-33.el8_10.x86_64 https://access.redhat.com/security/cve/CVE-2024-7006 RHSA-2024:9502 https://access.redhat.com/errata/RHSA-2024:9502 expat-2.2.5-16.el8_10.x86_64 https://access.redhat.com/security/cve/CVE-2024-50602 RHSA-2024:8922 https://access.redhat.com/errata/RHSA-2024:8922

ID	Minimum conditions	Description
		bzip2-1.0.6-27.el8_10.x86_64 bzip2-libs-1.0.6-27.el8_10.x86_64 https://access.redhat.com/security/cve/CVE-2019-12900 RHSA-2024:8860 https://access.redhat.com/errata/RHSA-2024:8860 krb5-libs-1.18.2-30.el8_10.i686 krb5-libs-1.18.2-30.el8_10.x86_64 https://access.redhat.com/security/cve/CVE-2024-3596

Fixes in Media Server for 10.2 GA (10.2.0.52)

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AMS-15905	Deployments enrolled with MPC.	Fixed the validation in Media Processing Core Advanced Settings
AMS-15846	Deployments enrolled with MPC.	Updated MPC enrollment key handling
AMS-15848	Deployments enrolled with MPC.	Added the location and data center tag for MPC configuration
AMS-15854	Deployments enrolled with MPC.	MPCAgent invalid location enrollment status and alarm
AMS-15854	Deployments enrolled with MPC.	mpcagent to send ISO country code and region
AMS-15824	All deployments	Security update to Apache HttpComponents (Client)
AMS-15820	All deployments	Major release upgrade failure with new mariadb
AMS-15801	Deployments with FIPS enabled	Fixed EM load issue in FIPS mode
AMS-15799	WebRTC deployments	ICE restart after disabled
AMS-15793	All deployments	Cancel on-hold timeout on renegotiation to active session
AMS-15798	All deployments	Security update for Spring Framework
AMS-14820	All deployments	Security update for PrimeFaces

ID	Minimum conditions	Description
AMS-15677	Deployments enrolled with MPC.	AAMS OAMWS Local Media MPC Automation Support
AMS-15726	All deployments	Go security updates

Fixes in System Layer for 10.2 SP 1 (10.0.0.30)

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AMS-15844	KVM appliance	Add virtualization type on EM system info screen
AMS-15882	All appliance deployments	Support secure boot for vmware virtual appliance. Note that it requires AAMS 10.2 or higher.
AMS-15986	All appliance deployments	Update physical appliance to use secure boot. Note that it requires AAMS 10.2 or higher.
AMS-15985	All appliance deployments	Support secure boot for kvm virtual appliance. Note that it requires AAMS 10.2 or higher.
AMS-16019	All appliance deployments	<p>Address RHSA-2024:10379</p> <p>RHSA-2024:10379 https://access.redhat.com/errata/RHSA-2024:10379</p> <p>pam-1.3.1-36.el8_10.x86_64</p> <p>https://access.redhat.com/security/cve/CVE-2024-10041</p> <p>https://access.redhat.com/security/cve/CVE-2024-10963</p> <p>Other security updates</p> <p>RHSA-2025:0083 https://access.redhat.com/errata/RHSA-2025:0083</p> <p>cups-libs-1:2.2.6-62.el8_10.x86_64</p> <p>https://access.redhat.com/security/cve/CVE-2024-47175</p> <p>RHSA-2024:10281 https://access.redhat.com/errata/RHSA-2024:10281</p> <p>kernel-4.18.0-553.30.1.el8_10.x86_64</p> <p>kernel-core-4.18.0-553.30.1.el8_10.x86_64</p> <p>kernel-modules-4.18.0-553.30.1.el8_10.x86_64</p> <p>https://access.redhat.com/security/cve/CVE-2024-27043</p> <p>https://access.redhat.com/security/cve/CVE-2024-27399</p>

ID	Minimum conditions	Description
		https://access.redhat.com/security/cve/CVE-2024-38564 https://access.redhat.com/security/cve/CVE-2024-46858 RHSA-2025:0733 https://access.redhat.com/errata/RHSA-2025:0733 bzip2-1.0.6-28.el8_10.x86_64 bzip2-libs-1.0.6-28.el8_10.x86_64 https://access.redhat.com/security/cve/CVE-2019-12900 RHSA-2025:0065 https://access.redhat.com/errata/RHSA-2025:0065 kernel-4.18.0-553.34.1.el8_10.x86_64 kernel-core-4.18.0-553.34.1.el8_10.x86_64 kernel-modules-4.18.0-553.34.1.el8_10.x86_64 https://access.redhat.com/security/cve/CVE-2024-53088 https://access.redhat.com/security/cve/CVE-2024-53122 RHSA-2024:10779 https://access.redhat.com/errata/RHSA-2024:10779 platform-python-3.6.8-69.el8_10.x86_64 python3-libs-3.6.8-69.el8_10.x86_64 https://access.redhat.com/security/cve/CVE-2024-11168 https://access.redhat.com/security/cve/CVE-2024-9287 RHSA-2025:1266 https://access.redhat.com/errata/RHSA-2025:1266 kernel-4.18.0-553.40.1.el8_10.x86_64 kernel-core-4.18.0-553.40.1.el8_10.x86_64 kernel-modules-4.18.0-553.40.1.el8_10.x86_64 https://access.redhat.com/security/cve/CVE-2024-53104 RHSA-2024:9689 https://access.redhat.com/errata/RHSA-2024:9689 binutils-2.30-125.el8_10.x86_64 https://access.redhat.com/security/cve/CVE-2018-12699 RHSA-2025:1068 https://access.redhat.com/errata/RHSA-2025:1068 kernel-4.18.0-553.37.1.el8_10.x86_64 kernel-core-4.18.0-553.37.1.el8_10.x86_64 kernel-modules-4.18.0-553.37.1.el8_10.x86_64 https://access.redhat.com/security/cve/CVE-2024-26935 https://access.redhat.com/security/cve/CVE-2024-50275 RHSA-2024:10943 https://access.redhat.com/errata/RHSA-2024:10943

ID	Minimum conditions	Description
		<p>kernel-4.18.0-553.32.1.el8_10.x86_64</p> <p>kernel-core-4.18.0-553.32.1.el8_10.x86_64</p> <p>kernel-modules-4.18.0-553.32.1.el8_10.x86_64</p> <p>https://access.redhat.com/security/cve/CVE-2024-46695</p> <p>https://access.redhat.com/security/cve/CVE-2024-49949</p> <p>https://access.redhat.com/security/cve/CVE-2024-50082</p> <p>https://access.redhat.com/security/cve/CVE-2024-50099</p> <p>https://access.redhat.com/security/cve/CVE-2024-50110</p> <p>https://access.redhat.com/security/cve/CVE-2024-50142</p> <p>https://access.redhat.com/security/cve/CVE-2024-50192</p> <p>https://access.redhat.com/security/cve/CVE-2024-50256</p> <p>https://access.redhat.com/security/cve/CVE-2024-50264</p> <p>RHSA-2025:0012 https://access.redhat.com/errata/RHSA-2025:0012</p> <p>python3-requests-2.20.0-5.el8_10.noarch</p> <p>https://access.redhat.com/security/cve/CVE-2024-35195</p> <p>RHSA-2025:1301 https://access.redhat.com/errata/RHSA-2025:1301</p> <p>libgcc-8.5.0-23.el8_10.i686</p> <p>libgcc-8.5.0-23.el8_10.x86_64</p> <p>libgomp-8.5.0-23.el8_10.x86_64</p> <p>libstdc++-8.5.0-23.el8_10.i686</p> <p>libstdc++-8.5.0-23.el8_10.x86_64</p> <p>https://access.redhat.com/security/cve/CVE-2020-11023</p> <p>RHSA-2025:1517 https://access.redhat.com/errata/RHSA-2025:1517</p> <p>libxml2-2.9.7-18.el8_10.2.x86_64</p> <p>python3-libxml2-2.9.7-18.el8_10.2.x86_64</p> <p>https://access.redhat.com/security/cve/CVE-2022-49043</p> <p>RHSA-2025:0288 https://access.redhat.com/errata/RHSA-2025:0288</p> <p>NetworkManager-1:1.40.16-18.el8_10.x86_64</p> <p>NetworkManager-initscripts-updown-1:1.40.16-18.el8_10.noarch</p> <p>NetworkManager-libnm-1:1.40.16-18.el8_10.x86_64</p> <p>https://access.redhat.com/security/cve/CVE-2024-3661</p>

Fixes in Media Server for 10.2 SP 1 (10.2.0.61)

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AMS-16026	WebRTC	WebRTC agent is unable to make blind transfer/consult transfer/consult conference
AMS-16818	Inband DTMF	Prop DTMF twist configuration
AMS-15851	All	Update apache/xerces-c to address reported security vulnerabilities
AMS-15958	All	Switch from kernel based timing driver to standard POSIX timer
AMS-15951	All	AMS backup from webpage is showing 500 internal error Release10.2
AMS-15950	All	Filter out internal media endpoints when sending out dual-unicast reports.

Fixes in System Layer for 10.2 SP 2 (10.0.0.31)

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AMS-16317	All appliance deployments	<p>Update RPMs to address security vulnerabilities</p> <p>RHSA-2025:1675 https://access.redhat.com/errata/RHSA-2025:1675</p> <p>bind-32:9.11.36-16.el8_10.4.x86_64</p> <p>bind-libs-32:9.11.36-16.el8_10.4.x86_64</p> <p>bind-libs-lite-32:9.11.36-16.el8_10.4.x86_64</p> <p>bind-license-32:9.11.36-16.el8_10.4.noarch</p> <p>bind-utils-32:9.11.36-16.el8_10.4.x86_64</p> <p>python3-bind-32:9.11.36-16.el8_10.4.noarch</p> <p>https://access.redhat.com/security/cve/CVE-2024-11187</p> <p>RHSA-2025:3421 https://access.redhat.com/errata/RHSA-2025:3421</p> <p>freetype-2.9.1-10.el8_10.x86_64</p> <p>https://access.redhat.com/security/cve/CVE-2025-27363</p> <p>RHSA-2025:3260 https://access.redhat.com/errata/RHSA-2025:3260</p> <p>kernel-4.18.0-553.46.1.el8_10.x86_64</p>

ID	Minimum conditions	Description
		<p>kernel-core-4.18.0-553.46.1.el8_10.x86_64 kernel-modules-4.18.0-553.46.1.el8_10.x86_64 https://access.redhat.com/security/cve/CVE-2025-21785</p> <p>RHSA-2025:2473 https://access.redhat.com/errata/RHSA-2025:2473 kernel-4.18.0-553.44.1.el8_10.x86_64 kernel-core-4.18.0-553.44.1.el8_10.x86_64 kernel-modules-4.18.0-553.44.1.el8_10.x86_64 https://access.redhat.com/security/cve/CVE-2024-50302 https://access.redhat.com/security/cve/CVE-2024-53197 https://access.redhat.com/security/cve/CVE-2024-57807 https://access.redhat.com/security/cve/CVE-2024-57979</p> <p>RHSA-2025:3026 https://access.redhat.com/errata/RHSA-2025:3026 kernel-4.18.0-553.45.1.el8_10.x86_64 kernel-core-4.18.0-553.45.1.el8_10.x86_64 kernel-modules-4.18.0-553.45.1.el8_10.x86_64 https://access.redhat.com/security/cve/CVE-2023-52922</p> <p>RHSA-2025:2686 https://access.redhat.com/errata/RHSA-2025:2686 libxml2-2.9.7-19.el8_10.x86_64 python3-libxml2-2.9.7-19.el8_10.x86_64 https://access.redhat.com/security/cve/CVE-2024-56171 https://access.redhat.com/security/cve/CVE-2025-24928</p> <p>RHSA-2025:3367 https://access.redhat.com/errata/RHSA-2025:3367 grub2-common-1:2.02-162.el8_10.noarch grub2-efi-x64-1:2.02-162.el8_10.x86_64 grub2-pc-1:2.02-162.el8_10.x86_64 grub2-pc-modules-1:2.02-162.el8_10.noarch grub2-tools-1:2.02-162.el8_10.x86_64 grub2-tools-efi-1:2.02-162.el8_10.x86_64 grub2-tools-extra-1:2.02-162.el8_10.x86_64 grub2-tools-minimal-1:2.02-162.el8_10.x86_64 https://access.redhat.com/security/cve/CVE-2025-0624</p> <p>RHSA-2025:2722 https://access.redhat.com/errata/RHSA-2025:2722 krb5-libs-1.18.2-31.el8_10.i686 krb5-libs-1.18.2-31.el8_10.x86_64</p>

ID	Minimum conditions	Description
		https://access.redhat.com/security/cve/CVE-2025-24528 FEDORA-EPEL-2025-80c00be088 - https://bodhi.fedoraproject.org/updates/FEDORA-EPEL-2025-80c00be088 clamav-1.0.8-1.el8.x86_64.rpm clamav-data-1.0.8-1.el8.noarch.rpm clamav-filesystem-1.0.8-1.el8.noarch.rpm clamav-freshclam-1.0.8-1.el8.x86_64.rpm clamav-lib-1.0.8-1.el8.x86_64.rpm https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-20128

Fixes in Media Server for 10.2 SP 2 (10.2.0.72)

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AMS-16354	All deployments	Address EM runtime errors with media management
AMS-16326	1+1 HA deployments	ConfMP -- HA standby node incorrect SDP incorrect origin check
AMS-16211	All deployments	Upgrade jQuery UI to 1.14.1
AMS-16205	All deployments	InstallAnywhere 2024 R2
AMS-16110	All deployments	Update Tomcat to 9.0.102
AMS-16150	All deployments	Apache-ant 1.10.5
AMS-16108	All deployments	Java OpenJDK 17 LTS upgrade
AMS-16114	1+1 HA deployments	Prevent second arp series during high-availability address takeover
AMS-15977	All deployments	SDP processing corrections identified by static analysis

Fixes in System Layer for 10.2 SP 3 (10.0.0.32)

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AXP-14448	All appliances deployments	Move service cleanup for upgrade robustness
AXP-17856 AXP-15843 AXP-12866	All appliances deployments	<p>RPM security updates:</p> <p>RHSA-2025:8686 https://access.redhat.com/errata/RHSA-2025:8686</p> <p>glibc-2.28-251.el8_10.22.i686 glibc-2.28-251.el8_10.22.x86_64 glibc-common-2.28-251.el8_10.22.x86_64 glibc-gconv-extra-2.28-251.el8_10.22.i686 glibc-gconv-extra-2.28-251.el8_10.22.x86_64 glibc-langpack-en-2.28-251.el8_10.22.x86_64 glibc-minimal-langpack-2.28-251.el8_10.22.x86_64 libnsl-2.28-251.el8_10.22.i686 libnsl-2.28-251.el8_10.22.x86_64</p> <p>https://access.redhat.com/security/cve/CVE-2025-4802</p> <p>libsoup-2.62.3-9.el8_10.x86_64</p> <p>https://access.redhat.com/security/cve/CVE-2025-2784 https://access.redhat.com/security/cve/CVE-2025-32049 https://access.redhat.com/security/cve/CVE-2025-32914 https://access.redhat.com/security/cve/CVE-2025-4948</p> <p>RHSA-2025:8056 https://access.redhat.com/errata/RHSA-2025:8056</p> <p>kernel-4.18.0-553.53.1.el8_10.x86_64 kernel-core-4.18.0-553.53.1.el8_10.x86_64 kernel-modules-4.18.0-553.53.1.el8_10.x86_64</p> <p>https://access.redhat.com/security/cve/CVE-2024-40906 https://access.redhat.com/security/cve/CVE-2024-44970 https://access.redhat.com/security/cve/CVE-2025-21756</p> <p>RHSA-2025:8432 https://access.redhat.com/errata/RHSA-2025:8432</p> <p>perl-CPAN-2.18-402.el8_10.noarch</p> <p>https://access.redhat.com/security/cve/CVE-2020-16156</p> <p>RHSA-2025:8246 https://access.redhat.com/errata/RHSA-2025:8246</p>

ID	Minimum conditions	Description
		<p>kernel-4.18.0-553.54.1.el8_10.x86_64</p> <p>kernel-core-4.18.0-553.54.1.el8_10.x86_64</p> <p>kernel-modules-4.18.0-553.54.1.el8_10.x86_64</p> <p>https://access.redhat.com/security/cve/CVE-2024-43842</p> <p>RHSA-2025:7540 https://access.redhat.com/errata/RHSA-2025:7540</p> <p>libjpeg-turbo-1.5.3-14.el8_10.x86_64</p> <p>https://access.redhat.com/security/cve/CVE-2020-13790</p> <p>RHSA-2025:3913 https://access.redhat.com/errata/RHSA-2025:3913</p> <p>expat-2.2.5-17.el8_10.x86_64</p> <p>https://access.redhat.com/security/cve/CVE-2024-8176</p> <p>RHSA-2025:4051 https://access.redhat.com/errata/RHSA-2025:4051</p> <p>gnutls-3.6.16-8.el8_10.3.x86_64</p> <p>https://access.redhat.com/security/cve/CVE-2024-12243</p> <p>RHSA-2025:7531 https://access.redhat.com/errata/RHSA-2025:7531</p> <p>kernel-4.18.0-553.52.1.el8_10.x86_64</p> <p>kernel-core-4.18.0-553.52.1.el8_10.x86_64</p> <p>kernel-modules-4.18.0-553.52.1.el8_10.x86_64</p> <p>https://access.redhat.com/security/cve/CVE-2022-49011</p> <p>https://access.redhat.com/security/cve/CVE-2024-53141</p> <p>RHSA-2025:4658 https://access.redhat.com/errata/RHSA-2025:4658</p> <p>libtiff-4.0.9-34.el8_10.x86_64</p> <p>https://access.redhat.com/security/cve/CVE-2017-17095</p> <p>RHSA-2025:4049 https://access.redhat.com/errata/RHSA-2025:4049</p> <p>libtasn1-4.13-5.el8_10.x86_64</p> <p>https://access.redhat.com/security/cve/CVE-2024-12133</p> <p>RHSA-2025:8411 https://access.redhat.com/errata/RHSA-2025:8411</p> <p>krb5-libs-1.18.2-32.el8_10.i686</p> <p>krb5-libs-1.18.2-32.el8_10.x86_64</p> <p>https://access.redhat.com/security/cve/CVE-2025-3576</p> <p>RHSA-2025:8958 https://access.redhat.com/errata/RHSA-2025:8958</p> <p>libxml2-2.9.7-20.el8_10.x86_64</p>

ID	Minimum conditions	Description
		<p>python3-libxml2-2.9.7-20.el8_10.x86_64 https://access.redhat.com/security/cve/CVE-2025-32414</p> <p>RHSA-2025:8743 https://access.redhat.com/errata/RHSA-2025:8743 kernel-4.18.0-553.56.1.el8_10.x86_64 kernel-core-4.18.0-553.56.1.el8_10.x86_64 kernel-modules-4.18.0-553.56.1.el8_10.x86_64 https://access.redhat.com/security/cve/CVE-2022-49395</p> <p>RHSA-2025:3828 https://access.redhat.com/errata/RHSA-2025:3828 glibc-2.28-251.el8_10.16.i686 glibc-2.28-251.el8_10.16.x86_64 glibc-common-2.28-251.el8_10.16.x86_64 glibc-gconv-extra-2.28-251.el8_10.16.i686 glibc-gconv-extra-2.28-251.el8_10.16.x86_64 glibc-langpack-en-2.28-251.el8_10.16.x86_64 glibc-minimal-langpack-2.28-251.el8_10.16.x86_64 libnsl-2.28-251.el8_10.16.i686 libnsl-2.28-251.el8_10.16.x86_64 https://access.redhat.com/security/cve/CVE-2025-0395</p> <p>RHSA-2025:3893 https://access.redhat.com/errata/RHSA-2025:3893 kernel-4.18.0-553.50.1.el8_10.x86_64 kernel-core-4.18.0-553.50.1.el8_10.x86_64 kernel-modules-4.18.0-553.50.1.el8_10.x86_64 https://access.redhat.com/security/cve/CVE-2024-53150 https://access.redhat.com/security/cve/CVE-2024-53241</p> <p>RHSA-2025:3615 https://access.redhat.com/errata/RHSA-2025:3615 libxslt-1.1.32-6.1.el8_10.x86_64 https://access.redhat.com/security/cve/CVE-2024-55549 https://access.redhat.com/security/cve/CVE-2025-24855</p> <p>RHSA-2025:9878 https://access.redhat.com/errata/RHSA-2025:9878 libblockdev-2.28-7.el8_10.x86_64 libblockdev-crypto-2.28-7.el8_10.x86_64 libblockdev-fs-2.28-7.el8_10.x86_64 libblockdev-loop-2.28-7.el8_10.x86_64 libblockdev-mdraid-2.28-7.el8_10.x86_64</p>

ID	Minimum conditions	Description
		<p>libblockdev-part-2.28-7.el8_10.x86_64</p> <p>libblockdev-swap-2.28-7.el8_10.x86_64</p> <p>libblockdev-utils-2.28-7.el8_10.x86_64</p> <p>https://access.redhat.com/security/cve/CVE-2025-6019</p> <p>RHSA-2025:3845 https://access.redhat.com/errata/RHSA-2025:3845</p> <p>java-1.8.0-openjdk-1:1.8.0.452.b09-2.el8.x86_64</p> <p>java-1.8.0-openjdk-headless-1:1.8.0.452.b09-2.el8.x86_64</p> <p>https://access.redhat.com/security/cve/CVE-2025-21587</p> <p>https://access.redhat.com/security/cve/CVE-2025-30691</p> <p>https://access.redhat.com/security/cve/CVE-2025-30698</p> <p>RHSA-2025:8676 https://access.redhat.com/errata/RHSA-2025:8676</p> <p>libxslt-1.1.32-6.2.el8_10.x86_64</p> <p>https://access.redhat.com/security/cve/CVE-2023-40403</p> <p>RHSA-2025:4560 https://access.redhat.com/errata/RHSA-2025:4560</p> <p>libsoup-2.62.3-8.el8_10.x86_64</p> <p>https://access.redhat.com/security/cve/CVE-2025-32050</p> <p>https://access.redhat.com/security/cve/CVE-2025-32052</p> <p>https://access.redhat.com/security/cve/CVE-2025-32053</p> <p>https://access.redhat.com/security/cve/CVE-2025-32906</p> <p>https://access.redhat.com/security/cve/CVE-2025-32911</p> <p>https://access.redhat.com/security/cve/CVE-2025-32913</p> <p>https://access.redhat.com/security/cve/CVE-2025-46420</p> <p>https://access.redhat.com/security/cve/CVE-2025-46421</p> <p>RHSA-2025:3852 https://access.redhat.com/errata/RHSA-2025:3852</p> <p>java-17-openjdk-1:17.0.15.0.6-2.el8.x86_64</p> <p>java-17-openjdk-headless-1:17.0.15.0.6-2.el8.x86_64</p> <p>https://access.redhat.com/security/cve/CVE-2025-21587</p> <p>https://access.redhat.com/security/cve/CVE-2025-30691</p> <p>https://access.redhat.com/security/cve/CVE-2025-30698</p> <p>RHSA-2025:9580 https://access.redhat.com/errata/RHSA-2025:9580</p> <p>kernel-4.18.0-553.58.1.el8_10.x86_64</p> <p>kernel-core-4.18.0-553.58.1.el8_10.x86_64</p> <p>kernel-modules-4.18.0-553.58.1.el8_10.x86_64</p> <p>https://access.redhat.com/security/cve/CVE-2022-48919</p>

ID	Minimum conditions	Description
		https://access.redhat.com/security/cve/CVE-2024-50301 https://access.redhat.com/security/cve/CVE-2024-53064 https://access.redhat.com/security/cve/CVE-2025-21764 FEDORA-EPEL-2025-7afd2b91ab https://bodhi.fedoraproject.org/updates/FEDORA-EPEL-2025-7afd2b91ab clamav-1.0.9-1.el8.x86_64.rpm clamav-data-1.0.9-1.el8.noarch.rpm clamav-filesystem-1.0.9-1.el8.noarch.rpm clamav-freshclam-1.0.9-1.el8.x86_64.rpm clamav-lib-1.0.9-1.el8.x86_64.rpm

Fixes in Media Server for 10.2 SP 3 (10.2.0.80)

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AXP-19463	1+1 HA deployments	Incorrect control and media session count
AXP-17548	All deployments	Major release upgrade Tomcat connector
AXP-17046	Customer supplied OS deployments	Installer EPEL repository verification
AMS-15990	All deployments	ConfMP crash on RTCP BYE receipt
AMS-16426	All deployments	Cleanup EM libraries for minor upgrades
AMS-16370	All deployments	Replace Tomcat APR connector
AMS-16366	All deployments	Quartz security update
AMS-16332	1+1 HA deployments	Active server refresh failure when inactive server is unavailable

Known issues and workarounds

Known issues and workarounds

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

ID	Minimum conditions	Visible symptoms	Workaround

ID	Minimum conditions	Visible symptoms	Workaround
N/A			

Languages supported

List the languages supported in this release.

- *English*

Documentation **errata**

Document number	Title	Description
N/A		