Avaya Aura® Media Server (AAMS) Release Notes

Release 8.0.2

Issue 1.0

October 8, 2019

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, https://support.avaya.com/LICENSEINFO, UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

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

License types

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

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

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

Downloading Documentation

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

Contact Avaya Support

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

Contents

Change history

Issue	Date	Description
1.0	October 8, 2019	Release of AAMS 8.0.2

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 8.0.2

The following table lists enhancements in this release.

Enhancement	Description
AMS-6841	FIPS support for WebRTC media sessions.
AMS-6840	FIPS support for Web Collaboration.
AMS-7317	WebRTC media added DTLSv1.2 support with preferred ciphers: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
AMS-6857	Update AAMS appliance to use Red Hat 7.6 and include latest security updates.
AMS-6828	Multi-Shared video composite mode.
AMS-6843	Force customer account password change on initial login.
AMS-7633	Enable root account when deploying with SDM.
WCS-2314	Web collaboration support for server certificate revocation check using OCSP or CRL.

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. Have the Avaya documentation available.

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 SMGR 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.

As of the date of this release note publication AAMS 8.0.2 has only been tested with the following applications:

- Avaya Equinox Conference 9.1.9
- Avaya Aura® Web Gateway 3.7

Supported 8.0.2 Upgrade Paths

Prior to upgrading to AAMS 8.0.2 your prior installation must meet the following minimum software revisions for the media server software:

Release	***Minimum Supported***
7.8.0	7.8.0.240 or higher
8.0.0	8.0.0.240 or higher
8.0.1	8.0.1.121 or higher

Installation

8.0.2 New Installation File List (Appliance Only)

Download ID	**Filename**	**Notes**
MSR000000119	MediaServer_8.0.2.43_A7_2019.07.17_OVF10.ova ***NOTE after deploying the OVA you MUST install***	AAMS virtual appliance (OVA) for new deployments. ***Ensure you install the latest***

Download ID	Filename	Notes
	the mandatory updates listed in the section titled "8.0.2 Required Updates and Hotfixes (Appliance Only)". ***NOTE 8.0.2.43 A7 contains system layer 8.0.0.19, which is newer than 8.0.0.18. If you are deploying this OVA, then you only need to install the media server update.***	***system layer and media server updates.***

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

Download ID	Filename	Notes
MSR000000115	MediaServer_8.0.2.56_2019.08.08.bin	AAMS software only installer (PVI) for new deployments where customer is supplying the hardware and Linux OS.

8.0.2 Required Updates and Hotfixes (Appliance Only)

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

Download ID	Patch	Notes
MSR000000116	8.0.2.56	AAMS update for Media Server software that needs to be applied to all 8.0.x deployments.
MSR000000117	8.0.0.18	AAMS update for System Layer software that needs to be applied to all 8.0.x appliance deployments.

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

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

Download ID	Patch	Notes
MSR000000115	8.0.2.56	AAMS software only installer (PVI) for new deployments where customer is supplying the hardware and Linux OS.

8.0.2 Patch File list (Appliance Only)

Filename	File size	Version
MediaServer_Update_8.0.2.56_2019.08.08.iso	880,384,000	8.0.2.56
MediaServer_System_Update_8.0.0.18_2019.07.10.iso	1,002,248,192	8.0.0.18

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

Filename	File size	Version
MediaServer_8.0.2.56_2019.08.08.bin	880,004,689	8.0.2.56

Speculative Execution Vulnerabilities (Spectre, Meltdown, and L1TF) Patches

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.

Spectre and Meltdown Patches and Capacity Impacts

Spectre and Meltdown patches have been applied to the operating system of the AAMS 8.0.0 appliance. In addition to the AAMS patches the following updates are required:

Platform	***Minimum version for patches***
Dell R630	BIOS version 2.7.1
Dell R230	BIOS version 2.4.3
Dell R220	BIOS version 1.10.2
HP DL360 G9	BIOS version 2.56
Avaya Aura® Appliance Virtualization	7.1.3.0.0.04

VMWare	Refer to https://kb.vmware.com/s/article/52245

Spectre and Meltdown patches may have performance degradation for the following deployments:

- Virtual Appliance Profile 3, 4, 5 and 6
- Physical Appliances (Dell R220, Dell R230, HP DL360 G9 and Del R630)
- Software only installs on customer supplied OS and hardware

In AAMS 7.8 SP8 a new report called traffic summary was introduced and is accessible using the AAMS Element Manager located under Home » System Status » Monitoring » Reports » Traffic Summary. This feature provides summary statistics for session usage, Load Factor and CPU over the previous 4 weeks for the local media server. It may be used to help determine if your deployment will be impacted by the Spectre/Meltdown performance degradation.

Review the traffic summary for these deployment types to determine if the peak CPU or Load Factor exceeds 70%, or the average consistently exceeds 50%. If it does you should add additional media servers to the network to compensate for the Spectre/Meltdown performance degradation.

The traffic report is also available in so older releases by requesting a QFE from Avaya.

Release and Build	***QFE***
7.7 FP1 SP3 (7.7.0.398)	QFE-EMLite-7.7.0.398-0001-lnx.zip
7.8 SP6 (7.8.0.355)	QFE-EMLite-7.8.0.355-0001-lnx.zip
7.8 SP7 (7.8.0.384)	QFE-EMLite-7.8.0.384-0001-lnx.zip

L1TF Patches

L1TF patches have been applied to the operating system of the AAMS 8.0.0 SP2 appliance. In addition to the AAMS patches the following updates are required:

Platform	***Minimum version for patches***
Dell R630	BIOS version 2.8.0
Dell R230	BIOS version 2.5,0
Dell R220	BIOS version 1.10.3
HP DL360 G9	BIOS version 2.60
Avaya Aura® Appliance Virtualization	8.0.2.0.0.01

VMWare	https://blogs.vmware.com/security/2018/08/l1tf.html

Backing up the software

For appliance installations, refer to procedures documented in *Deploying and Updating Avaya Aura® Media Server Appliance* on the Avaya Support site at: https://downloads.avaya.com/css/P8/documents/101050431.

For Customer Supplied Hardware and OS installations, refer to procedures documented in *Implementing and Administering Avaya Aura® Media Server* on the Avaya Support site at: https://downloads.avaya.com/css/P8/documents/101050441.

Release 7.8 to 8.0.2 Upgrade Considerations

Before you upgrade from Release 7.8 to 8.0.2 the following should be considered:

- Element Manager OS Authentication has been removed. Please refer to the section "Element Manager OS Authentication Removed" for more details.
- When upgrading an 1+1 HA cluster or N+1 load sharing cluster the primary server must be upgraded first. This is due to the OS Authentication being removed. Until the primary server is upgrade you will not be able to login to EM since the default admin password needs to be changed and it may only be changed on the primary server.
- Customer supplied hardware and Operating System needs to be upgraded to Red Hat 7.x prior to doing the upgrade

8.0.0 SP4 or Higher Upgrade Considerations

Before you upgrade to release 8.0.0 SP4 (or higher) the following should be considered:

- Once you upgrade to 8.0.0 SP4 or later you can't restore a configuration backup from an earlier 8.0.0 release due to internal change with Element Manager configuration change. Please ensure you take a current backup after the upgrade completes.

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 8.0.0 appliance for the first time are encouraged to enable EASG, which can be done by issuing the following command after upgrading.

```
EASGManage –enableEASG
```

Element Manager OS Authentication Removed

Support for OS authentication has been removed in AAMS 8.0.0 and Element Manager accounts are managed by AAMS by default. For new deploys you will need to login with the default user name and password using the following procedure:

1. In a web browser, type the following URL https://serverAddress:8443/em where serverAddress is the address of the primary Avaya Aura® MS. (i.e. https://10.60.86.209:8443/em). ***NOTE initial login and password change will only work on the primary server. If this is a 1+1 HA cluster use the Management IP address and not the service IP address.***
2. Sign in to Element Manager by using the user name admin and specify the password Admin123$.
3. Element Manager will then prompt you to change the password for the Admin user.

If you are upgrading from 7.8 you will need to login to the emergency login https://serverAddress:8443/emlogin with user name admin and password Admin123$.

When upgrading an 1+1 HA cluster or N+1 load sharing cluster the primary server must be upgraded before you can login to EM emergency login for the first time. Until the primary server is upgrade you will not be able to login to EM since the default admin password needs to be changed on the primary only.

Installing the release

For appliance installations, refer to procedures documented in *Deploying and Updating Avaya Aura® Media Server Appliance* on the Avaya Support site at: *https://downloads.avaya.com/css/P8/documents/101033404*.

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://downloads.avaya.com/css/P8/documents/101033406*.

When upgrading an 8.0.2 appliance the following procedure should be used:

- Backup the system
- Upload both system layer and media sever updates
- Place system in pending lock (one node at a time)
- Click “Install Updates” in Element Manager to initiate update install
- Once installation complete place system in an unlocked state

Troubleshooting the installation

For appliance installations, refer to procedures documented in *Deploying and Updating Avaya Aura® Media Server Appliance* on the Avaya Support site at: https://downloads.avaya.com/css/P8/documents/101050431.

For non-appliance installations, refer to procedures documented in *Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS* on the Avaya Support site at: https://downloads.avaya.com/css/P8/documents/101050445.

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://downloads.avaya.com/css/P8/documents/101050431.

For non-appliance installs refer to procedures documented in Implementing and Administering Avaya Aura® Media Server on the Avaya Support site: https://downloads.avaya.com/css/P8/documents/101050441.

Functionality not supported

N/A

Fixes

Fixes in System Layer for 8.0.0 (8.0.0.19) – New Appliance deployments Only

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AMS-6843	New appliance deployments (8.0.2.43 A7 or higher)	Force customer account password change on initial login.
AMS-7633	New virtual appliance deployments (8.0.2.43 A7 or higher)	Enable root account activation when deployed via SDM.
AMS-7458	New appliance deployments (8.0.2.43 A7 or higher)	Accept spaces between entries for NTP and DNS on OVA deploy

Fixes in System Layer for 8.0.0 (8.0.0.18)

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AMS-6891	All appliance deployments.	Mount /dev/shm with noexec option.
AMS-6857	All appliance deployments.	Update to RHEL 7.6.
AMS-6837	All appliance deployments.	Update packages to address outstanding security advisories

ID	Minimum conditions	Description
		RHSA-2019:0710 - https://access.redhat.com/errata/RHSA-2019:0710 python-2.7.5-77.el7_6.x86_64 python-libs-2.7.5-77.el7_6.x86_64 https://access.redhat.com/security/cve/CVE-2019-9636 RHSA-2019:0818 - https://access.redhat.com/errata/RHSA-2019:0818 kernel-3.10.0-957.12.1.el7.x86_64 https://access.redhat.com/security/cve/CVE-2019-6974 https://access.redhat.com/security/cve/CVE-2019-7221 RHSA-2019:1168 - https://access.redhat.com/errata/RHSA-2019:1168 kernel-3.10.0-957.12.2.el7.x86_64 https://access.redhat.com/security/cve/CVE-2018-12126 https://access.redhat.com/security/cve/CVE-2018-12127 https://access.redhat.com/security/cve/CVE-2018-12130 https://access.redhat.com/security/cve/CVE-2019-11091 RHSA-2019:1228 - https://access.redhat.com/errata/RHSA-2019:1228 wget-1.14-18.el7_6.1.x86_64 https://access.redhat.com/security/cve/CVE-2019-5953 RHSA-2019:1294 - https://access.redhat.com/errata/RHSA-2019:1294 bind-license-32:9.9.4-74.el7_6.1.noarch bind-utils-32:9.9.4-74.el7_6.1.x86_64 bind-32:9.9.4-74.el7_6.1.x86_64 bind-libs-32:9.9.4-74.el7_6.1.x86_64 https://access.redhat.com/security/cve/CVE-2018-5743 RHSA-2019:1481 - https://access.redhat.com/errata/RHSA-2019:1481 kernel-3.10.0-957.21.3.el7.x86_64 https://access.redhat.com/security/cve/CVE-2019-11477 https://access.redhat.com/security/cve/CVE-2019-11478 https://access.redhat.com/security/cve/CVE-2019-11479

ID	Minimum conditions	Description
		RHSA-2019:1587 - https://access.redhat.com/errata/RHSA-2019:1587 python-2.7.5-80.el7_6.x86_64 python-libs-2.7.5-80.el7_6.x86_64 https://access.redhat.com/security/cve/CVE-2019-10160 RHSA-2019:1619 - https://access.redhat.com/errata/RHSA-2019:1619 vim-minimal-2:7.4.160-6.el7_6.x86_64 https://access.redhat.com/security/cve/CVE-2019-12735

Fixes in Media Server for 8.0.2 (8.0.2.56)

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AMS-7339	All video Composite AAMS servers.	Audio and video out of sync and VCMP crashes due memory leak.
AMS-7312	All deployments enrolled with SMGR.	Failure occurs during non-primary server enrollment and EM enters an enrollment loop where it imports a new SMGR signed certificate into AAMS key store ever 3 minutes. Eventually EM runs out of memory and will not be accessible.
AMS-7296	All video deployments.	VidMP crashes when a video stream is removed from a session.
AMS-7317	All WebRTC deployments.	WebRTC Media added DTLSv1.2 support with preferred ciphers: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 and TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256.
AMS-7274	All deployments.	Certificate import/export fails if certificate password contains an XML reserved character.
AMS-7275	All WebRTC deployments.	WebRTC sessions lose audio and video due to FNTMP crashing when releasing session under traffic
AMS-7237	Deployments with EM cluster status failures.	EM cluster status fails when TLS version is TLSv1 or TLSv1.1.
AMS-7270	All deployments.	After upgrading from 7.8.x/8.0.x to 8.0.2 AAMS is out of service since DB is not running.
AMS-7256	All video deployments	Video block and unblock operation is not working.
AMS-7001	All video deployments.	VidMP crashes under traffic due to memory leak related to invalid video stream with repeated RTP timestamps and sequence numbers.

ID	Minimum conditions	Description
AMS-7189	All video composite AAMS servers.	Flicking of participants in composite video.
AMS-7185	All video deployments.	VidMP crashes when blocking video.
AMS-7168	All video composite AAMS servers.	Flicking of participants in composite video.
AMS-7169	All WebRTC deployments using Chrome browser.	Chrome WebRTC internals reported negative cumulative packet loss.
AMS-7123	All deployments.	OpenJDK security update 8u212b04.
AMS-6961	All 1+1 HA deployments.	Validate the backup server remote address for the MCHB protocol on the primary to avoid rogue connections. Added high-availability backup connection alarm and rogue connection attempt event log.
AMS-6960	Virtual appliance	Add logic to detect corrupted /proc/cpuinfo file.
AMS-7095	All video composite AAMS servers.	No video when long delay for media arrival after session setup.
AMS-6984	Deployments using secure FTP transfer of backup.	Backup secure FTP fails due to unsupported encryption algorithm requested by SFTP server.
AMS-6999	WebRTC deployments using static port configuration.	FNTMP enters a port manager infinite loop during startup and will not process new WebRTC sessions.
AMS-6987	All WebRTC deployments.	ICE aggressive nomination causing one-way media.
AMS-6968	All video deployments.	No receive video when making an audio/video call without a camera.
AMS-6830	All deployments.	MariaDB (10.3.15) and connector upgrade.
AMS-6841	All WebRTC deployments.	FIPS support for WebRTC media sessions.
AMS-6759	All deployments.	TLS handshake fails due to incorrect certificate chain order.
AMS-6821	All deployments.	Multiple log capture download clicks result in an incomplete log capture archive.

ID	Minimum conditions	Description
AMS-6826	All cluster (1+1 HA or N+1) deployments.	Configuration replication can be set on each AAMS server in a cluster.
AMS-6794	All deployments enrolled with SMGR.	Update SMGR FQDN constraint to allow numbers in top-level domain.
AMS-6893	All deployments.	Tomcat (9.0.13) upgrade.
AMS-3996	All deployments.	IPP upgrade.
AMS-6803	All video deployments.	VidMP crash on video de-escalation to audio-only when session not joined to conference.
AMS-6773	All deployments.	OpenSSL security update (1.0.2r).
WCS-2539	All web collaboration deployments.	Add audit to terminate web collaboration sessions that are around longer than 24 hours.

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
AMS-5318	Using latest Firefox, Chrome or Microsoft Edge browser.	Element Manager Session Detail Record Browser (located under Home » Tools » Session Detail Record Browser) doesn't work for Chrome, Firefox and Microsoft Edge since these browsers do not support Silverlight.	Use IE 11, older Firefox prior to 52, or older Chrome prior to 45.

Languages supported

List the languages supported in this release.

- *English*

Documentation errata

Document number	Title	Description

Document number	Title	Description
N/A		