



Avaya Aura® Conferencing 8.0 SP14
Release Notes v2

(8.0 SP14)

July 2019

Contents

1. Introduction	4
2. Avaya Aura® Conferencing (AAC) 8.0 Service Pack 14 (8.0 SP14) Overview	4
3. AAC 8.0 SP14 Release Line-up information	6
3.1. AAC 8.0 SP14 Release Line-up	6
4. Installation of AAC 8.0 SP14	7
4.1. Supported Upgrade Paths	7
4.2. Avaya Clients Load Line-up	7
4.3. Latest AAC Mobile Client Downloads	8
4.4. Recommended Avaya Aura® Load Line-up	8
4.5. Supported web browsers	9
5. Technical documentation	9
6. Technical Advisements	9
6.1. SNMP profiles should be re-applied on each AAC server after fresh install	9
6.2. Spectre and Meltdown security fixes needs manual enabling on AAC servers	10
6.3. Strengthened certificate validation	10
7. Technical Support	10

Revision History

Date	Version	Reason For Update
June 14, 2019	V1	AAC8.0 SP14 Release Notes.
July 23, 2019	V2	Security notes adjusted

1. Introduction

This document includes important details about the AAC 8.0 SP14 update, including the software load line-ups, important installation & upgrade notes, a list of key fixes and a list of advisements, limitations, and workarounds.

*****You must ensure that your System Manager is version 7.1 or later before upgrading to this release*****

2. Avaya Aura® Conferencing (AAC) 8.0 Service Pack 14 (8.0 SP14) Overview

AAC 8.0 SP14 delivers a new OS Platform Patch and a new Application Bundle. The Application bundle contains the following new loads since FP6:

AAC8.0 SP14 Application Bundle:

- MCP Application Load (**NEW for SP14**)
- Media Server Load (Same as SP9)
- Outlook Plugin (Same as SP10)
- HELP Files (Same as FP6)
- WebLM (Same as SP10)
- DataBase (**NEW for SP14**)
- PROMPT Files (Same as FP6)
- FMG Load (Same as FP6)

AAC8.0 SP14 contains the following key content:

- Plugins drastically changed in SP13 patch 1 propped into this release along with Mac plugins changes
- Due to plugin rework, starting from SP13 patch 1 to ensure correct web collaboration service functionality on AAC **websocket connections have to be allowed**.
- Minor plugin updates will no longer create any popups for the users in CA
- Certificate status is now displaying missing required extensions
- Database software was upgraded to improve security

Bug fixes list:

Key	Summary
AAC-13116	Phase 7: Prop the changes for Mac plugins
AAC-13098	CA - wcs - reports - Selected line of session list is reset if update-button clicked or if detail mode of current session closed.
AAC-13066	Mac Plugins: Update EULA in plugins
AAC-13053	PROV OPI compatibility issues with users search
AAC-13042	PROV OPI compatibility issues
AAC-13031	AAC doesn't provide the requirement of Client Authentication usage extension in certificates
AAC-13020	AAC 8.0 SP12 - P3S3 - "Add audio or video" is overlap in France
AAC-12774	AAC 8.0 SP11 patch 1 - P1S2 - MacOS 10.14 - Safari 12.0 - Installing AAC plugin has to change security setting and after installing and starting conference, user has to download and install again
AAC-12480	AAC: P3/S3 - intermittent: Cannot start eAViCA on Chrome because of Error message for network issue
AAC-12408	AAC 8.0.9 - P3S3 - chat disabled-The screenshot function should be disabled
AAC-12406	AAC8.0.9-P3S3-Disable or enable chat impacts to in-progress meeting
AAC-12389	AAC8.0.9-P3S3-Cannot download recording file with special characters in the name ` , ^ { }

AAC-12387	AAC8.0 SP9-P3S3 - Share/download/close buttons disappear after user presses cancel or X button on Share Recording link pop-up. See attached video for more detail
AAC-12373	AAC8.0 SP9-P3S3 - Intermittent - eAViCA user Chrome/Firefox fails to start A/V
AAC-12362	AAC 8.0.9-P3S3-Failed to restore recording if there is a space in a path of subdirectory
AAC-11959	Rename, Delete, Open buttons should be grayed after deletion of report

Security issues fixed:

Key	Summary
AAC-13115	Need to update JRE in Windows plugins: 8u212
AAC-13114	Need to update JRE in Mac plugins: 8u212
AAC-13109	AAC Platform openssh update(RHSA-2019:0711)
AAC-13108	AAC Platform kernel update (RHSA-2019:0717)
AAC-13094	20007 - SSL Version 2 and 3 Protocol Detection (tcp)
AAC-13092	122463 - RHEL 6 : kernel (RHSA-2019:0415) (tcp)
AAC-13091	104842 - RHEL 6 / 7 : apr (RHSA-2017:3270) (tcp)
AAC-13090	122465 - RHEL 6 : polkit (RHSA-2019:0420) (tcp)
AAC-13046	Migrate AAC platform to OpenJDK
AAC-13060	XSS vulnerability in CA login page

3. AAC 8.0 SP14 Release Line-up information

3.1. AAC 8.0 SP14 Release Line-up

PLDS ID	PLDS Name	File Name	Notes
AAC80001400 (NEW)	AAC8.0 SP14 Application Bundle 18.2.14.00	dvd_AAC_MCP_18.2.14. 00_2019-06-04- 1501_coreApps.iso	For Aura deployment, ensure that you have SMGR 7.1 or later before installing or upgrading to AAC8.0 SP14. AAC8.0 SP14 Application Bundle 18.2.14.00 contains various AAC8.0 applications load files. It is used to fresh install new AAC8.0 SP14 systems or used to upgrade existing systems. See the Release Notes for supported upgrade paths and details. Also there are special instructions in the Upgrade Guide for upgrading from AAC7.2 systems. SHA1 = 1211329985e0e49bed4be7c8ff17d9072d35d8c0
AAC80001401 (NEW)	AAC8.0 SP14 Platform Installer 18.2.14	mcp_core_linux_ple2- 18.2.14.iso	Please ensure that you have a valid AAC8.0 License Key before proceeding - AAC8.0 SP14 Platform Installer 18.2.14 is to be used for fresh installation of new AAC8.0 systems or when first upgrading from existing AAC7.2 systems. It is applied to each Linux server. SHA1 = 59b50fcb520efdc32da3c1470d7d5a0f66f8c391
AAC80001402 (NEW)	AAC8.0 SP14 Platform Patch 18.2.14	mcp_core_linux_ple2- 18.2.14.patches.r- 1.ext.iso	Please ensure that you have a valid AAC8.0 License Key before proceeding with AAC8.0. AAC8.0 SP14 Platform Patch 18.2.14 is applied to existing AAC8.0 systems that are on the AAC8.0 Platform version 18.2.2 or later to bring the platform OS up to the latest SP14 version 18.2.14. See the Release Notes for supported upgrade paths and details. SHA1 = 25ea1309e217e367616702d5a7f8d12cd87798f3

3.2. AAC 8.0 SP14 OVA build information

Starting from SP13 there are OVAs prepared for fresh installations.

4. Installation of AAC 8.0 SP14

4.1. Supported Upgrade Paths

Please ensure that the minimum software load is on the system prior to applying this update. You should refer to the original AAC 8.0 GA Release Notes for information about how to install new AAC 8.0 systems or how to upgrade existing 7.2 systems to AAC 8.0. The following upgrade paths are the only supported paths for updating systems to AAC 8.0 SP14:

- AAC 8.0 SP13 -> AAC 8.0 SP14
- AAC 8.0 SP13 patch 1 -> AAC 8.0 SP14
- AAC 8.0 SP12 -> AAC 8.0 SP14
- AAC 8.0 SP11 -> AAC 8.0 SP14
- AAC 8.0 SP11 patch 1 -> AAC 8.0 SP14
- AAC 8.0 SP10 -> AAC 8.0 SP14
- AAC 8.0 SP10 patch 1 -> AAC 8.0 SP14
- AAC 8.0 SP10 patch 2 -> AAC 8.0 SP14
- AAC 8.0 SP9 -> AAC 8.0 SP14
- AAC 8.0 SP9 patch 1 -> AAC 8.0 SP14
- AAC 8.0 SP9 patch 2 -> AAC 8.0 SP14
- AAC 8.0 SP8 -> AAC 8.0 SP14
- AAC 8.0 SP8 patch 1 -> AAC 8.0 SP14
- AAC 8.0 SP8 patch 2 -> AAC 8.0 SP14
- AAC 8.0 SP8 patch 3 -> AAC 8.0 SP14
- AAC 8.0 SP8 patch 4 -> AAC 8.0 SP14
- AAC 8.0 SP7 -> AAC 8.0 SP14
- AAC 8.0 SP7 patch 1 -> AAC 8.0 SP14
- AAC 8.0 SP7 patch 2 -> AAC 8.0 SP14
- AAC 8.0 SP7 patch 3 -> AAC 8.0 SP14
- AAC 8.0 FP6 -> AAC 8.0 SP14
- AAC 8.0 FP6 patch 1 -> AAC 8.0 SP14
- AAC 8.0 FP6 patch 2 -> AAC 8.0 SP14

4.2. Avaya Clients Load Line-up

The following list of clients details the intended support with AAC 8.0 SP14.

Please note that clients (Avaya and 3rd party) are supported for basic audio meet-me conferencing.

Client	Provides advanced conference controls	Supports Audio SRTP	Supports Video SRTP
9600 Series IP Deskphones 96x1 H.323 6.2 – 6.6	No	Yes	Not applicable
9600 Series IP Deskphones 96x1 SIP 6.2 – 7.0	Yes	Yes	Not applicable
Avaya Client Applications 6.2	Not applicable	Not applicable	Not applicable
Avaya Client Applications 6.3, 6.3.1(SP), 6.3.2(FP)	No	Yes	Yes
Avaya Communicator for iPad 2.0	Yes	Yes	Yes
Avaya Communicator for iPhone 2.1	Yes	Yes	Yes
Avaya Communicator for Windows 2.0, 2.0.2 (SP)	Yes	Yes	Yes
Avaya Communicator for Android 2.0, 2.1, 2.0.1	No	Yes	Not applicable
Avaya one-X® Communicator 6.2.3 (FP)	No	Yes	Yes
E129 SIP Deskphone 1.0	No	Yes	Not applicable
Avaya Flare® Experience Windows 1.1	Yes	Yes	No
Avaya one-X® Communicator 6.1.6	No	Yes	Yes
B100 Series Conference Phones B179 SIP 2.3	No	Yes	Not applicable
Desktop Video Device 1.1	No	No	No
H175 1.0.1	Yes		

4.3. Latest AAC Mobile Client Downloads

Android App:

<https://play.google.com/store/apps/details?id=com.avaya.wcca.gingerbread&hl=en>

iOS App: <https://itunes.apple.com/us/app/avaya-web-collaboration-agent/id535948292?mt=8>

Note that IOS8.* and later are supported for iPhone & iPad.

4.4. Recommended Avaya Aura® Load Line-up

** The table below captures the recommended version for each Aura component – please use the load versions published in PLDS**

Notes:

- The SBCE reflects the Aura SBC that was verified with the SBC Gateway Feature that provides AAC support for utilizing an Avaya SBC as an access point to the AAC

SMGR	7.1.1 with latest patch releases in PLDS
SM	7.0.1 with latest patch releases in PLDS
CM	7.0.1 with latest patch releases in PLDS
SBCE	7.1 with latest patch releases in PLDS

Notes: AAC also supports SMGR 8.x.x releases, however sometimes requiring additional patched installed on top of them to solve some compatibility issues.

4.5. Supported web browsers

Web browser	Operating system	Supported features
Microsoft Internet Explorer 8 and later	Windows 7, 8, 10	Web collaboration Audio and video Screen sharing
Microsoft Edge	Windows 10	Web collaboration
Mozilla Firefox latest version	Windows 7, 8, 10 Apple OS X	Web collaboration Audio and video Screen sharing
Google Chrome latest version	Windows 7, 8, 10 Apple OS X	Web collaboration Audio and video Screen sharing
Apple Safari latest version	Apple OS X	Web collaboration Audio and video Screen sharing

5. Technical documentation

The AAC 8.0 SP14 documentation available is listed below is available on the Avaya Support Site. Please note that documents with asterisk indicate that the AAC 8.0 document has not been revised for this Service Pack 10 and can also be obtained from [Avaya Support website](#) or by contacting Avaya directly.

Title
Avaya Aura Conferencing Overview and Specification Guide for Aura
Avaya Aura Conferencing Overview and Specification Guide for Turnkey
Solution Description for Large Enterprises
Solution Description for Medium Enterprises
Solution Description for SME
Deploying Avaya Aura Conferencing
Upgrading Avaya Aura Conferencing
Using Avaya Aura Conferencing Collaboration Agent
Administering Avaya Aura Conferencing
Maintaining and Troubleshooting Avaya Aura Conferencing
Migrating Avaya Aura Conferencing
Port Matrix for AAC 8.0*
Intelligent Workbook for AAC 8.0*

6. Technical Advisements

The following section details technical advisements and other items of interest that may not have been published in the Customer documentation. Readers are encouraged to read this section in its entirety before attempting a software installation or upgrade.

6.1. SNMP profiles should be re-applied on each AAC server after fresh install

Issue: AAC 8.0 SP7 and AAC 8.0 SP8 has SNMP protocol version 3 by default. AAC platform is still on SNMP v2. SNMP profile should be re-assigned to each AAC server in Element Manager Console to resolve the inconsistency.

6.2. Spectre and Meltdown security fixes needs manual enabling on AAC servers

Issue: Due to possible high performance impact, Spectre and Meltdown security fixes are disabled on AAC SP11 servers by default.

To enable the fix remove these flags to kernel command line, then reboot the server to have them take effect:

noibrs noibpb nopti

Note: you can individually enable/disable each parameter, for performance characterization it is not required that all 3 be simultaneously disabled.

To modify kernel command line open /boot/grub/grub.conf file, modify the kernel lines as needed.

In order to disable the fix add those parameters back.

6.3. Strengthened certificate validation

Issue: Some network elements have the alarm about the connection failed to ASM or other NE

Starting from AAC 8.0 SP10 certificate validation was changed to comply RFC specifications and currently checks the certificate sequentially in the following way:

1. If there is a Subject Alternative Name extension in the certificate, the FQDN or the IP used by NE should fully match one of the declared in SAN.
2. If there are no SANs in the certificate, Certificate's Common Name should be matching FQDN/IP instead
3. Otherwise, fail

The customers performing the upgrade are advised to check the certificates in case having underlined alarms. Very common ASM certificate is automatically created for an FQDN that is not present in DNS or hosts, this issue with connection to ASM can be solved either by adding this FQDN to AAC servers' hosts file or used DNS or instead have this certificate regenerated to comply the logic above by adding ASM IP to its certificate SANs on SMGR.

6.4. Reworked AAC plugins

AAC plugins were reworked to work without the browser extensions

There are some key changes brought in SP13 patch 1 that this release will carry on:

- Minor plugins update will no longer create any popups for users when they are trying to start a new meeting, instead they will be simply showing a link along the start meeting options
- All of the installers were merged into one and now working the same in all the browsers supported
- The installation is not requiring browser restarts, after a few seconds the system should pick up the installed plugin
- No browser extensions are required for plugins to work
- New plugins will be installed separately on the system as "Avaya Aura Conferencing Apps"

7. Technical Support

Support for Avaya Aura® Conferencing is available through Avaya Technical Support.

If you encounter trouble with Avaya Aura® Conferencing:

1. Retry the action. Carefully follow the instructions in written or online documentation.
2. Check the documentation that came with your hardware for maintenance or hardware-related problems.
3. Note the sequence of events that led to the problem and the exact messages displayed. Have the Avaya documentation available.
4. If you continue to have a problem, contact Avaya Technical Support by doing one of the following:
 - a. Logging into the Avaya Support Web site
<http://www.avaya.com/support>.
 - b. Calling or faxing Avaya Technical Support at one of the telephone numbers in the Support Directory listings on the Avaya support Web site.

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

Note: If you have difficulty reaching Avaya Technical Support through the above URL or email address, please go to <http://www.avaya.com> for further information.

When you request technical support, provide the following information: Configuration settings, including Avaya Aura® Conferencing configuration and browser settings.