



Avaya Aura® Conferencing 7.2
Release Notes v4.0

Contents

1	Introduction	4
2	Avaya Aura® Conferencing 7.2 feature overview	4
2.1	Release Summary	4
2.2	Detailed Feature Summary	4
2.3	Licensing	6
2.4	Java Support Matrix	7
2.5	Deployment Options	8
3	Software Versions	8
3.1	Avaya Aura® Conferencing 7.2 Software Line-up:	8
3.2	Avaya Clients Load Line-up	11
3.3	Recommended Avaya Aura® Load Line-up	11
3.4	Minimum Avaya Aura® Load Line-up	12
3.5	Load Line-up for other servers	12
3.6	Audio/Video in Collaboration Agent Software	12
4	Technical documentation	13
5	Software updates	13
6	Technical Advisements	13
6.1	Alarm for WCMS remote synchronization failure	14
6.2	DCS file uploads can hang	15
6.3	Ad hoc conference calls initiated by Avaya Flare® Experience or 96X1	16
6.4	Checkpoint versioning on redundant systems	16
6.5	Call server failover	16
	Issue: If the CM or CS1K does a failover, the active Avaya Aura® Conferencing 7 calls will get dropped. This issue will be addressed in a future release.	16
6.6	Supported JAVA versions	16
	• Desktop/Region/Application Sharing	16
	• MAC OS X 10.7.X+	16
	• DCS	17
6.7	Excel documents in MyLibrary	17
6.8	Avaya Flare® Experience moderator dial out to a CS1000 Mobile-X client	17
6.9	Operator in an active call	17
	Issue: Participants can dial *0 to get access to an operator only when they are in an active conference call. They will not be able to do so when dialing into the bridge.	17
6.10	Audible feedback prompt when entering ad hoc conference	17
6.11	Roster list	17
6.12	Avaya Flare® Experience - Carousel of participant	18
6.13	Subscribers unable to upload documents using the Web Collaboration interface in certain scenarios.	18
6.14	Duplicate CA Roster Entry After CA Moderator Force Out.	19
6.15	Aura 6.2.3 SM Removing Video for Ad-Hoc Video Escalations	20
6.16	Lose Conference Events when H.323 Transfers to Flare	20
6.17	Video will not work if call held prior to conference start	20
6.18	Use of PAMgr FQDN	20
6.19	Conference Stays up during Avaya Aura Session Manager failover	20
6.20	Use of Application Layer Gateways (ALGs) with AAC is Not Recommended	20
6.21	Limitation with using Google Chrome on MacOSX	21
6.22	Use of Moderator Passcode with Scopia solution not recommended	21
6.23	Java 1.7 support for Document Conversion Server	21
6.24	Using Recording with Avaya Flare Experience	22
6.25	Avaya Aura System Manager Multiple Device Access (MDA)	22
6.26	MacOS Upgrades Disable Screen Sharing	22
6.27	Trying to use Avaya Aura Conferencing Web Collaboration without Java installed	22
6.28	Re-joining a locked conference in Avaya Aura Conferencing Web Collaboration	22
6.29	Recording a conference that starts as a Standalone Web Conference	23
6.30	Using full screen sharing with large resolution displays	23
6.31	Alarm 220 DNSL after upgrade	23
6.32	Collaboration Agent not working after upgrade	23

6.33	Russian Conferencing Audio Prompts for Release 7.2	23
6.34	Support of Encrypted Passcodes from LDAP Directory.	23
6.35	Engineering Parameters when not using a Co-Res configuration	24
7	Technical Support	25

1 Introduction

This document includes important details for Avaya Aura Conferencing 7.2. This document provides the software load line-up of this product, Avaya Aura, supported Avaya clients, and other call servers with which this product interoperates. It also provides a list of advisements, limitations, and workarounds.

2 Avaya Aura® Conferencing 7.2 feature overview

2.1 Release Summary

Avaya Aura Conferencing 7.2 is the next release for Avaya's conferencing solution, and provides the additional functionality:

- Conference recording and playback
- Secure conferences
- Audio/Video in Collaboration Agent
- Customization of user interface
- Support for Active Directory
- Support for Passcode Feature and Participant Passcode for Conference
- Improved support for external users
- Support for CS 1000 7.6 Collaboration Pack
- Simple URL links

2.2 Detailed Feature Summary

2.2..1 Conference recording and playback

Using Collaboration Agent, moderators can record conferences. The recording captures audio, Web collaboration data, and conference events such as participants writing notes, participants joining or leaving, and participants interacting with each other. All aspects of the conference recording are synchronized within a conference timeline. When users play a recorded conference, they can easily jump forward and backwards in the conference timeline.

2.2..2 Secure conferences

If a conference is secure, the participants have all dialed into the conference using secure audio lines. Avaya Aura® Conferencing considers the lines to be secure if it identifies them as encrypted and authentic. If any participant in a given conference is not using a secure

audio line, the conference is not secure. Video conferences are not secure. Similarly, the Audio/Video in Collaboration Agent feature is not considered secure.

2.2..3 Audio/Video in Collaboration Agent

The Audio/Video in Collaboration Agent feature enables users to receive audio, video, and data content through a single device. Users can simply click on a conference URL (hyperlink), log in to the conference, and immediately share audio, video, and data using the Collaboration Agent Web page. Users do not need to dial into the conference and do not need to configure an additional application in order to share audio and video. This feature is aimed at guests and participants who reside outside of the enterprise and who do not have any other Avaya software products installed on their computers. The only requirement is that your computer must have a microphone.

2.2..4 Customization of user interface

Administrators can customize the Collaboration Agent user interface. This feature enables customers to insert their company branding and logos. Avaya Aura® Conferencing provides a default theme for the pages in Collaboration Agent. Administrators can create a custom theme and modify the default settings for the pages in Collaboration Agent. The default theme provides a large number of settings, such as logo images and the colors of borders, text, and backgrounds.

2.2..5 Support for Active Directory

The Lightweight Directory Access Protocol (LDAP) directory integration feature enables an enterprise administrator to regularly synchronize the Avaya Aura® Conferencing database with LDAP directories. When Avaya Aura® Conferencing is integrated with LDAP directory servers, the conferencing subscriber data is managed in the LDAP directory. When a user logs into Avaya Aura® Conferencing via Collaboration Agent or a mobile client, the user will be authenticated directly against the password in the LDAP directory. Avaya Aura® Conferencing supports any directory server that supports LDAP (for example, Microsoft® Active Directory 2003 and 2008 and OpenLDAP).

2.2..6 Support for Passcode Feature and Participant Passcode for Conference

If a conference has Passcode Flow enabled and Participant Passcodes Required, participants must enter a collaboration code and a passcode in order to gain access to the conference. Moderators can distribute the passcode and the collaboration code in separate e-mails, if they wish. Conference owners must contact a system administrator in order to investigate the possibility of adding a passcode feature to their conference. Users cannot enable or disable the passcode feature without the intervention of a system administrator.

2.2..7 Improved support for external users

For standalone with redundancy and standalone simplex deployment configurations, you can deploy the Web conferencing server within the Enterprise DMZ of your network firewall. This allows you to connect to an Avaya Aura® Conferencing conference as a member or guest from outside the company firewall while still ensuring a strong and secure network defense. The moderator of a conference can also be located outside of the corporate firewall and still have access to most command functions. You also have the benefit of using Avaya Aura® Conferencing for off-site conferences and events.

2.2..8 Support for CS 1000 7.6 Collaboration Pack

Avaya Aura® Conferencing supports deployment in an Avaya Communication Server 1000 7.6 Collaboration Pack architecture. This integration enables customers to leverage the new features within the Collaboration Pack.

2.2..9 Simple URL links

The conference link is now a short Uniform Resource Locator (URL), which consists of the Fully Qualified Domain Name (FQDN) or Internet Protocol (IP) address of the server running Collaboration Agent and the conference code, as follows: `https://<domain name>/<conference code>`. For example: <https://aac.examplecompany.com/12348765>.

2.3 Licensing

This section details product licensing changes for Avaya Aura Conferencing.

- 1) The purchased right to use all modes of conferencing and collaboration (audio, web, and video) is included in the license at time of implementation. All customers who install AAC 7.2 as new or apply it to an existing installation must ensure the license has the `VALUE_CONF_AUDIO_WEB_VIDEO_USERS` attribute in order to enable audio+web+video conferencing capabilities
- 2) The Audio and Web Recording functionality requires the use of an additional license with the `VALUE_CONF_MEDIA_RECORDING_SYSTEMS` attribute. Please note that the example license below shows 10 licenses for recording; only 1 is required per system.

Below is an example of a typical license for Avaya Aura Conferencing.

License File Host IDs: 00-CA-FE-11-69-63

Licensed Features

Feature (Keyword)	Expiration date	Licensed	Acquired
Maximum number of audio web users (lab use only) (VALUE_CONF_AUDIO_WEB_USERS)	permanent	200	0
Maximum number of audio video web users (lab use only) (VALUE_CONF_AUDIO_WEB_VIDEO_USERS)	permanent	200	2
Maximum number of media recording conferencing system (VALUE_CONF_MEDIA_RECORDING_SYSTEMS)	permanent	10	1
Maximum number of media servers allowed in the conferencing system (VALUE_CONF_MEDIA_SERVERS)	permanent	10	1

Acquired licenses

Feature	Acquired by	Count
VALUE_CONF_AUDIO_WEB_VIDEO_USERS	EM_10.130.88.241	2
VALUE_CONF_MEDIA_RECORDING_SYSTEMS	EM_10.130.88.241	1
VALUE_CONF_MEDIA_SERVERS	MS1_0_10.130.88.240	1

2.4 Java Support Matrix

The following table outlines which versions of Java are supported with the different Windows and MacOS versions available. The format is J<version number>u<update number>.

Note that Firefox is not listed since Firefox has its own version of Java; Firefox users should be using the latest release of the browser software.

Platform	Chrome	Safari	IE	Recommended
Windows				J7-latest update
32 (XP-Windows 7)	J6u18+	Not Supported	J6u18+	
64 (Windows 7)	J6u18+	Not Supported	J6u18+	
Mac OSX				
32 (Snow Leopard)	J6u18+	J6u18+	N/A	
64 (Mountain Lion)	Not supported	J7 latest update	N/A	

2.5 Deployment Options

This release provides several additional configurations to provide system administrators more options for an Avaya Aura Conferencing solution, such as the ability to have the WCMS network element be installed on a separate server.

More detailed information on these enhancements can be found in the documentation listed in Section 4.

3 Software Versions

3.1 Avaya Aura® Conferencing 7.2 Software Line-up:

Note: The data migration tool available on PLDS is only required if migrating from Avaya Aura® Conferencing 6.0 to Avaya Aura® Conferencing 7.2.

New Installations:

1. First install Linux OS “AAC7.2 Platform Installer 17.0.8” to bring the OS to the software level.
2. Next install “AAC7.2 Application Bundle 17.0.5.00”
3. Apply “AAC7.2 Application Patch 17.0.5.02”
4. Install “AAC7.2 Media Server Update 20130424_30”
5. Install “AAC7.2 AViCA Update 20130425”
6. Install “AAC7.2 PROMPTS Update”

Upgrading Previous Installations:

If upgrading from Avaya Aura Conferencing 7.0 and any related Service Packs, please use the following procedure:

Upgrading Co-resident Deployments from AAC7.0 to AAC7.2:

1. Upgrade to the latest AAC 7.0 Service Pack.
2. Perform a Full Backup of the AAC 7.0 system & store on a separate system (i.e. on a backup server). This step is done just in case you need to revert back to AAC 7.0 for some reason. Refer to Maintenance and Troubleshooting guide.
3. On all servers, upgrade your platform image from latest 7.0 SP (OS 15.1.x) to 17.0.8. Refer to Deployment Guide for Platform Patch instructions.
4. Download “AAC7.2 Application Bundle 17.0.5.00” and put it /var/mcp/extract folder or put DVD in drive.
5. As **ntappadm**, extract the bundle content by running **mcpExtractContent.pl -aat**
6. As **ntappadm**, upgrade Primary db by running **mcpDbSwUpgrade.pl -primary**
7. As **ntappadm**, upgrade to AAC7.2 by running **mcpUpgradeNextRel.pl**
8. Download and apply “AAC7.2 Application Patch 17.0.5.02”. Refer to Deployment Guide for Application Patch instructions.
9. Perform a Full Backup of AAC 7.2 for each Primary & Secondary (if it exists) co-resident servers & store on a separate system (i.e. on a backup server). Refer to Maintenance and Troubleshooting guide. Note that these backups will be used to restore the system after the Hard Drives are replaced later in this procedure.
10. Install the 2x900GB drives from the hardware upgrade kit into co-resident server(s). Refer to the instructions in the upgrade kit.

11. Download and burn this [HP SmartStart CD](#). Boot to the HP SmartStart CD and follow procedure to create 2 RAID 1 arrays for the 2x300GB and 2x900GB Hard Drives.
12. Perform fresh install of AAC 7.2 Linux 17.0.8 Platform using the server backup data option. During the installation you must select the option to restore the data from your remote server that you backed-up earlier.
13. Format and mount the second RAID using 2x900GB Raid drives. As **ntsysadm**, execute **mcpDataDiskMgt.pl -q** to check disk presence, then **mcpDataDiskMgt.pl -f** to format and **mcpDataDiskMgt.pl -m** to mount.
14. Use the Server backups and restore each co-resident server. Reference Maintenance and Troubleshooting guide
15. As **root** reinstall the AMS platform using **mcpMsInstall.pl** on each co-resident server.
16. Run the following commands from the Primary EM Server (as the designated user):
 - a) Redeploy the DB software –
As **ntappadm**, execute **/var/mcp/install/mcpDbSwInstall.pl -primary** [and **-secondary** if redundant])
 - b) Restore the data in the Database –
As **ntappadm**, execute **/var/mcp/install/dbInstall.pl -fo**
As **ntdbadm**,
execute **/var/mcp/run/MCP_17.0/mcpdb_0/bin/util/dbRestore.pl <dbBackupName>**
 - c) Deploy and start the EM –
As **ntappadm**, execute **/var/mcp/install/emDeploy.pl**
As **ntappadm**, execute **/var/mcp/install/emStart.pl**
17. Deploy and start all other NEs from the EM GUI.
18. Install “AAC7.2 Media Server Update 20130424_30” using the procedure documented later in this section.
19. Install “AAC7.2 AViCA Update 20130425” using the procedure documented later in this section.
20. Install “AAC7.2 PROMPTS Update” using the procedure documented later in this section.

Upgrading Standalone Deployments from AAC7.0 to AAC7.2:

1. Upgrade to the latest AAC 7.0 Service Pack.
2. Perform a Full Backup of the AAC 7.0 system & store on a separate system (i.e. on a backup server). This step is done just in case you need to revert back to AAC 7.0 for some reason. Refer to Maintenance and Troubleshooting guide.
3. On all servers, upgrade your platform image from latest 7.0 SP (OS 15.1.x) to 17.0.8. Refer to Deployment Guide for Platform Patch instructions.
4. Download “AAC7.2 Application Bundle 17.0.5.00” and put it /var/mcp/extract folder or put DVD in drive.
5. As **ntappadm**, extract the bundle content by running **mcpExtractContent.pl -aat**
6. As **ntappadm**, upgrade Primary db by running **mcpDbSwUpgrade.pl -primary**
7. As **ntappadm**, upgrade to AAC7.2 by running **mcpUpgradeNextRel.pl**
8. Download and apply “AAC7.2 Application Patch 17.0.5.02”. Refer to Deployment Guide for Application Patch instructions.
9. Install “AAC7.2 Media Server Update 20130424_30” using the procedure documented later in this section.
10. Install “AAC7.2 AViCA Update 20130425” using the procedure documented later in this section.

11. Install “AAC7.2 PROMPTS Update” using the procedure documented later in this section.

What to do when there are new sub-components included in a patch:

From time to time Avaya may release new versions for software not usually included in a patch. This section details what to do when that happens.

If the patch includes a new Avaya Media Server load:

1. Download the file from PLDS
2. Using the ntappadm account and SFTP the AMS load to each AMS in the system and place the file in directory /var/mcp/loads
3. Follow the procedures outlined in the Deployment Guide for Installation or Upgrade/Patching as applicable; make sure to ignore any steps related to placing the AMS load on the servers as that was done in the above steps

If the patch includes a new Audio/Video in Collaboration Agent load:

1. Download the file from PLDS
2. Using the ntappadm account extract the contents of the file in PLDS to directory /var/mcp/media/avica
3. If this is a new installation please follow the installation instructions in the Deployment Guide
4. If this is an upgrade of an existing deployment please follow the upgrade instructions in the Deployment Guide

If the patch includes new audio prompts for the Avaya Media Server:

1. Download the file from PLDS
2. Using the ntappadm account to copy the prompts.zip file to directory /var/mcp/media/audio/default on EMServer1
3. Stop, undeploy, deploy and start all Avaya Media Server Network Elements

Latest Available PLDS Downloads:

PLDS ID	PLDS Name	File Name
AAC72000014	AAC7.2 Platform Patch 17.0.8	mcp_core_linux_ple2-17.0.8.patches.r-1.ext.iso
AAC72000015	AAC7.2 Platform Installer 17.0.8	mcp_core_linux_ple2-17.0.8.iso
AAC72000017	AAC7.2 Application Bundle 17.0.5.00	dvd_AAC_MCP_17.0.5.00_2013-04-15-1655_coreApps.iso
AAC72000019	AAC7.2 IT47 Beta Customer Documents	AAC72_IT47_Beta_Customer_Docs_20130423.zip
AAC72000020	AAC7.2 Application Patch 17.0.5.02	MCP_17.0.5.02_2013-04-25-1710.zip
AAC72000021	AAC7.2 AVICA Update 20130425	AacpaOtv-client-3.0-NIGHTLY.20130425-303.zip

AAC72000022	AAC7.2 PROMPTS Update	prompts.zip
AAC72000023	AAC7.2 Media Server Update 20130424_30	MCP_MediaServer_17.0_7.5.0.1078_2013.04.24_30.zip

Latest Mobile Client Downloads:

Android App -

https://play.google.com/store/apps/details?id=com.grapesoftware.wcca.gingerbread7_2&feature=search_result#?t=W251bGwsMSwyLDEsImNvbS5ncmFwZXNvZnR3YXJlLnJY2EuZ2luZ2VyYnJlYWQ3XzliXQ

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

3.2 Avaya Clients Load Line-up

**** Please use the latest load versions published in PLDS ****

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

SIP 96x1 R6.2 and Avaya Flare Experience 1.0/1.1 (Windows and iPad) provide support for advanced conference control such as roster controls and active speakers.

Avaya Flare Experience 1.1 and one-X Communicator 6.1 (SIP and H.323) clients also provide video capabilities for conferencing.

Note that audio SRTP support is currently only supported on SIP 96x1 R6.2, one-X Communicator 6.2 (SIP and H.323) and Flare 1.1. In order to use audio SRTP with Flare 1.1 the user must disable video.

Since Flare and Avaya Aura Conference are so strongly integrated details on how to obtain that client are included below.

Avaya Flare® Experience for Windows Release 1.1 Service Pack 2
PLDS ID: FE000000007

Avaya Flare® Experience for iPad Release 1.1 Service Pack 1
<https://itunes.apple.com/us/app/avaya-flare-experience-customer/id562354739?mt=8>

3.3 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****

Also, please be aware that this load line-up applies to the solution regardless of the Aura deployment model used.

SMGR	6.3 with latest patch releases in PLDS
SM	6.3 with latest patch releases in PLDS
CM	6.2 FP2 with latest patch releases in PLDS

3.4 Minimum Avaya Aura® Load Line-up

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

Also, please be aware that this load line-up applies to the solution regardless of the Aura deployment model used.

SMGR	6.2 SP4 with latest patch releases in PLDS
SM	6.2 SP4 with latest patch releases in PLDS
CM	6.2 SP5 with latest patch releases in PLDS

3.5 Load Line-up for other servers

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

BCM450	BCM050.R600.CORE-TELEPHONY-51-1
	BCM050.R600.IPTTEL-52-2
CS1000 R7.5	patch: cs1000-vtrk-7.50.17.16-36.i386.000 + MPLR31809
CS1000 R7.6	R7.6 SP2 (June, 2013 launch)
B5800	8.0.067011

3.6 Audio/Video in Collaboration Agent Software

The Audio/Video in Collaboration Agent software is provided as part of the Application Bundle. Once the Administrator extracts the Applicable Bundle on **Element Manager Server 1** they will find the files in folder **/var/mcp/media/avica**.

The Administrator can then go to that directory and execute the documented installation procedures for Audio/Video in Collaboration Agent.

4 Technical documentation

See the latest versions of documents published on [Avaya Support website](#).

Title
Avaya Aura® Conferencing Overview and Specification
Avaya Aura® Conferencing Planning and Design
Avaya Aura® Conferencing Accounting Records Reference
Avaya Aura® Conferencing Alarms and Logs Reference
Avaya Aura® Conferencing Operational Measurements Reference
Administering Avaya Aura Conferencing and Radvision Interoperability
Deploying Avaya Aura® Conferencing
Administering Avaya Aura® Conferencing
Maintaining and Troubleshooting Avaya Aura® Conferencing
Avaya Aura® Conferencing Security
Using Avaya Web Collaboration Agent for iPhone app
Using Avaya Web Collaboration Agent for Android app
Using Avaya Aura® Conferencing Collaboration Agent
Avaya Aura® Conferencing Collaboration Agent Quick Reference
Using Conferencing Manager for Microsoft Outlook

The Beta versions of the technical documents are available on PLDS.

PLDS ID	PLDS Name	File Name
AAC72000019	AAC7.2 IT47 Beta Customer Documents	AAC72_IT47_Beta_Customer_Docs_20130423.zip

In addition, the document “Intelligent Workbook for Avaya Aura Conferencing 7.2” can be found in the "Anatomy of a Successful Cut" GMI Portal via Sales and Partner Portal.

5 Software updates

Regular patch advisements are provided on the [Avaya Support website](#).

The current patch for AAC 7.2 can be found in section 3.1.

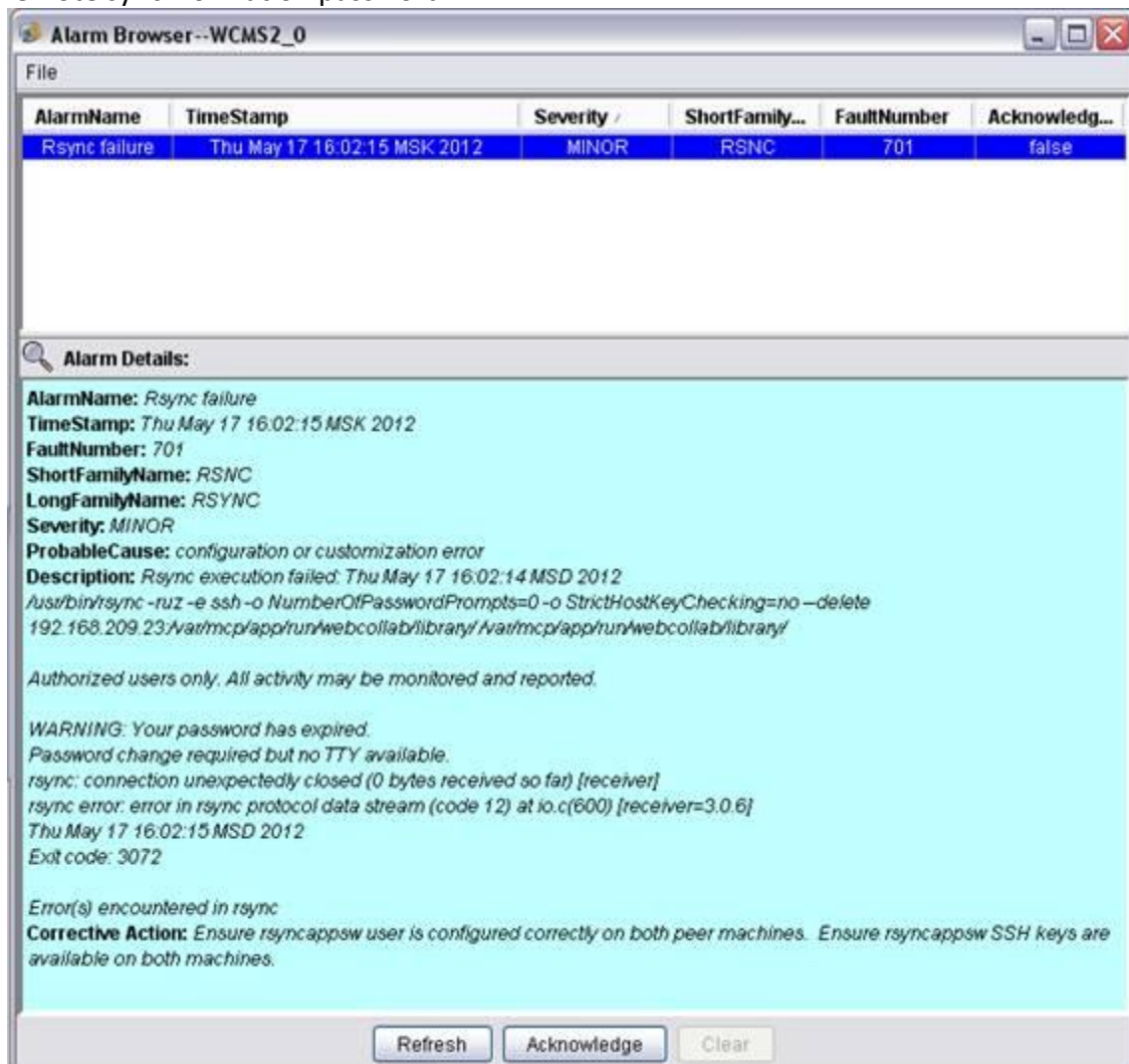
6 Technical Advisements

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.

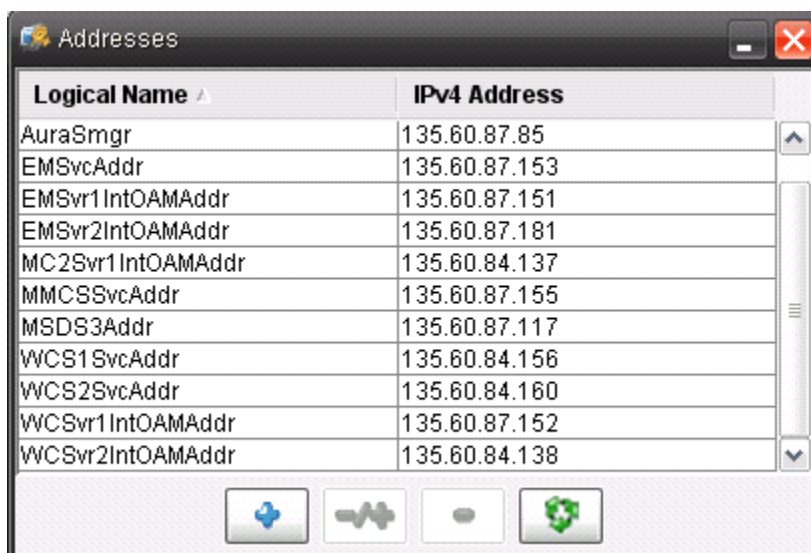
6.1 Alarm for WCMS remote synchronization failure

Issue: You might encounter this alarm which is caused due to the expiration of the remote synchronization password:



Workaround:

1. In the example shown above the alarm is seen on the instance called WCMS2. From the EM GUI, find the address on which instance WCMS2 is deployed, this can be retrieved using the Addresses option on the EM GUI. Normally the WCMS logical names follow a pattern of WCSSvr#IntOAMAddress; using the example picture below that means that WCSSvr2IntOAMAddr has the address.



Logical Name	IPv4 Address
AuraSmgr	135.60.87.85
EMSvcAddr	135.60.87.153
EMSvr1IntOAMAddr	135.60.87.151
EMSvr2IntOAMAddr	135.60.87.181
MC2Svr1IntOAMAddr	135.60.84.137
MMCS8SvcAddr	135.60.87.155
MSDS3Addr	135.60.87.117
WCS1SvcAddr	135.60.84.156
WCS2SvcAddr	135.60.84.160
WCSvr1IntOAMAddr	135.60.87.152
WCSvr2IntOAMAddr	135.60.84.138

2. Log into the server at address identified in step 1 using a program like putty using root privileges.
3. Disable password aging on the passwords by executing the command "chage --maxdays -1 rsyncappsw" with **root** permissions.
4. Change the password for the rsyncappsw account (required only to actually reset the expired password flag).

6.2 DCS file uploads can hang

Issue: We need to ensure that the DCS load is copied directly from the DVD image or the PLDS web site directly onto the DCS SERVER. If the DCS software is copied over to the DCS server by other means, it can result in DCS file uploads hanging.

Workaround: To ensure that the DCS software (zip file) is marked safe, on the DCS server desktop execute the instructions during installation:

1. Right click the downloaded ZIP download that has been marked unsafe.
2. Click Properties, choose General Tab, then you'll see at the bottom of the window the "Security" message saying "This file came from another computer and might be blocked to help protect this computer".
3. Click "Unblock" to make the file safe again.
4. Extract the files and they will run successfully.

6.3 Ad hoc conference calls initiated by Avaya Flare® Experience or 96X1

Issue: In CM you will need to administer between 2 and 8 call appearances for Avaya Flare® Experience clients (windows and iPad) and 96X1 sets in order for ad hoc conference calls to work with Avaya Flare® Experience and other set types.

There are 3 ways to reduce the administrative effort:

- In SMGR, you can create a Flare station template and then replicate that,
- On CM, you can duplicate the layout of a station or
- You can use the ProVision tool that allows bulk administration of users.

Workaround: None

6.4 Checkpoint versioning on redundant systems

Issue: Checkpoint versioning on redundant systems is not supported so these swerrs can be ignored

AS1_1 SWERR 799 ALERT Mnthxx 12:10:47:657 MCP_15.0.10.3

com.nortelnetworks.ims.cap.prtcl.checkpoint.CallPCP: Error in decoding Checkpoint
java.lang.IllegalStateException

6.5 Call server failover

Issue: If the CM or CS1K does a failover, the active Avaya Aura® Conferencing 7 calls will get dropped. This issue will be addressed in a future release.

Workaround: None

6.6 Supported JAVA versions

• Desktop/Region/Application Sharing

Issue: If end users are running Java 1.7 update versions 1, 2 or 3, then they will be provided a warning stating that this version is not supported for desktop sharing. These Java versions have inherent issues as mentioned by the vendors. Users can continue to use them for sharing but they might experience issues; in particular, annotation tools will not work as expected.

Workaround: Users are recommended to downgrade to Java 1.6 or upgrade to Java 1.7, update version 4.

• MAC OS X 10.7.X+

Issue: If end users are running MAC OS X 10.7.x or higher with Java 1.7.x, the desktop/region sharing will result in loss of control of the region/desktop being shared. This Java version has inherent issues as mentioned by the vendor.

Workaround: There is no current workaround for using desktop/region sharing. The recommendation is to use document sharing by uploading documents to the personal library.

Once in this situation, the keyboard shortcut (cmd+q) or the OS X top menu bar can be used to kill the sharing application process.

- **DCS**

Issue: The installation guide incorrectly mentions the supported versions as Java 1.6 or higher.

The supported/recommended/tested version for the DCS is Java 1.6. DCS installation/setup will fail if Java 1.7 is installed on the server on which DCS is going to be installed.

Recommendation: Please downgrade to Java 1.6 for the DCS to be properly installed.

6.7 Excel documents in MyLibrary

Issue: MS Excel documents cannot be uploaded to My Library for sharing.

Workaround: These document types need to be shared using Desktop or Application sharing modes.

6.8 Avaya Flare® Experience moderator dial out to a CS1000 Mobile-X client

Issue: If an Avaya Flare® Experience 1.0 moderator that is dialed into an Avaya Aura® Conferencing 7 bridge attempts to dial out to a CS1000 Mobile X phone which is twinned to a CS1000 desk phone for simultaneous ringing, the CS1000 desk phone will be able to join the conference call as expected. But if the call is received by the Mobile-X phone, then the user will not hear a prompt to press 1 to join the conference and the call will be terminated. This is a known limitation.

Workaround: User will have to receive the call on the CS1K desk set.

6.9 Operator in an active call

Issue: Participants can dial *0 to get access to an operator only when they are in an active conference call. They will not be able to do so when dialling into the bridge.

Workaround: Participant has to dial into an Avaya Aura® Conferencing bridge and then press *0 to get access to an Operator.

6.10 Audible feedback prompt when entering ad hoc conference

Issue: In ad hoc audio conferences, when the moderator turns on lecture mode successfully, then invites a participant to join in the conference, the participant joining the conference will not hear the prompt "You entered a conference starting with lecture mode."

Workaround: None

6.11 Roster list

Issue: In a specific call scenario involving dialing out to a user who has call forwarding enabled, the original number dialed is shown on the roster, not the number to which the call was forwarded. The issue only happens if Call forward is set to a PSTN number.

Workaround: None

6.12 Avaya Flare® Experience - Carousel of participant

Issue: When using Flare Experience as a moderator you will not be able to tell when a participant goes on hold.

Workaround: None

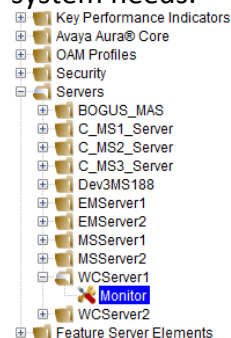
6.13 Subscribers unable to upload documents using the Web Collaboration interface in certain scenarios.

Issue: Subscribers will not be able to upload a document if they have more than 50 files in their personal library.

Subscribers will not be able to upload a document in cases in which the system runs out of space on the DCS server. Subscribers will see an “I/O error in this scenario”.

Workaround:

- Subscribers will need to delete some of the files from their personal library in order to upload new files.
- Administrators can also proactively correct this situation by monitoring the server and freeing up space when required.
 - The library data is stored in the “/var/mcp/app/run/webcollab/library” folder on the WCMS server. The AAC EM server monitor option can be used to view the current space utilization.
 - Minor, Major and Critical alarms will be generated by the system based on the utilization of space in the “var/mcp” partition. The default thresholds levels are 70%, 80% and 90% for minor, major and critical alarms respectively. The thresholds are also configurable and administrators can configure lower or higher levels based on their system needs.

A screenshot of the WServer1 Monitor window. The window has tabs for 'Summary', 'Disk', 'Memory', 'CPU', and 'Interface'. The 'Disk' tab is selected, showing a table of disk utilization for various partitions. The table has columns for 'Partition', 'Capacity (MBytes)', 'Used (MBytes)', and 'Utilization'. The data is as follows:

Partition	Capacity (MBytes)	Used (MBytes)	Utilization
/boot	99	17	17.01%
/var/log/audit	2979	222	7.46%
/opt	5950	563	9.47%
/var/log	1983	868	43.78%
/var/mcp	530145	29240	5.52%
/admin	91	10	11.28%
/tmp	486	36	7.40%
/	1983	995	50.17%
/home	486	36	7.31%
/var	1983	158	7.95%

- When the server reaches a certain threshold level, administrators can free up space in this folder so that users can upload new files to their personal library.
- The maximum number of files that a subscriber can upload is configurable and administrators can change the value based on their system needs. The default value is set to 50. A system restart is not

required for the change to take effect. **Increasing the value will have system performance impact and is not recommended.**

- Search for the “upload.maxfile” attribute in the following files and update as required..
 - /var/mcp/run/MCP_17.0/<<WCSNE>>/apache/www/meeting/Config-dist.php
 - /var/mcp/run/MCP_17.0/<<WCSNE>>/apache/www/meeting/Config.php
- The maximum allowed file size that a subscriber can upload is configurable and administrators can change the value based on their system needs. The default value is set to 32 MB. A system restart is not required for the change to take effect. **Increasing the value will have system performance impact and is not recommended.**
 - WCS Server: Search for the “upload.maxsize” attribute in the following files and update as required. Value should be set in bytes.
 - /var/mcp/run/MCP_17.0/<<WCSNE>>/apache/www/meeting/Config-dist.php
 - /var/mcp/run/MCP_17.0/<<WCSNE>>/apache/www/meeting/Config.php
 - WCS Server: Search for the “upload_max_filesize” attribute in the following file and update as required. Value should be set in bytes.
 - /var/mcp/run/MCP_17.0/<<WCSNE>>/apache/php.ini
 - DCS: Search for the “upload_max_filesize” attribute in the following file and update as required. Value should be set in bytes.
 - <<DCS InstallDir>>/php/php.ini

6.14 Duplicate CA Roster Entry After CA Moderator Force Out.

Issue: When a CA Moderator invokes the forced logout of another CA session, the invoking CA session may display duplicate and inconsistent CA roster entries (for the invoking subscriber) if the forced-out CA session user presses the “Logout” link.

Workaround: When seeing the duplicate entries, the subscriber may exit the Conference by pressing the exit icon on the top-right corner of the CA Conference page, then pressing the “Conference” button to re-enter the conference, resulting in a Conference display without duplicate roster entries.

6.15 Aura 6.2.3 SM Removing Video for Ad-Hoc Video Escalations

Issue: When merging video point-to-point calls into an ad hoc conference the SM SIP REFER bandwidth processing results in disabling the video..

Workaround: This issue is fixed in the latest Aura 6.2 SM patch list; please apply the latest patches or upgrade to a later release.

6.16 Lose Conference Events when H.323 Transfers to Flare

Issue: When an H.323 enabled endpoint transfers a Flare endpoint to an AAC conference, the Flare endpoint will not be able to receive conference events such as active speaker and will not be able to execute conference controls.

Workaround: The Flare user should join the conference manually.

6.17 Video will not work if call held prior to conference start

Issue: If a user dials into a conference with video and then places the call on hold prior to actually being put into the conference, that user will not have video for the call. This also happens in dial-out scenarios if the user called does a hold prior to pressing 1. Putting an endpoint on hold after the user joins the conference works fine. Video resumes when the call is taken off hold.

Workaround: Re-join the conference without using hold prior to being placed into the conference.

6.18 Use of PAMgr FQDN

Issue: The Microsoft Outlook Plug-in will not work correctly unless the Fully Qualified Domain Name of the PAMgr network element is entered into the WebConferencingHost field. This field is available in the AAC Element Manager for the PAMgr network element.

Workaround: Enter the data into the WebConferencingHost field.

6.19 Conference Stays up during Avaya Aura Session Manager failover

Issue: If the moderator on a conference is being served by an Avaya Aura Session Manager which either goes out of service or is taken out of service, the conference will not detect that the moderator has left the call, and the call will stay up.

Workaround: There is no workaround; the call will remain up until the moderator joins the conference again and then exits the call normally.

6.20 Use of Application Layer Gateways (ALGs) with AAC is Not Recommended

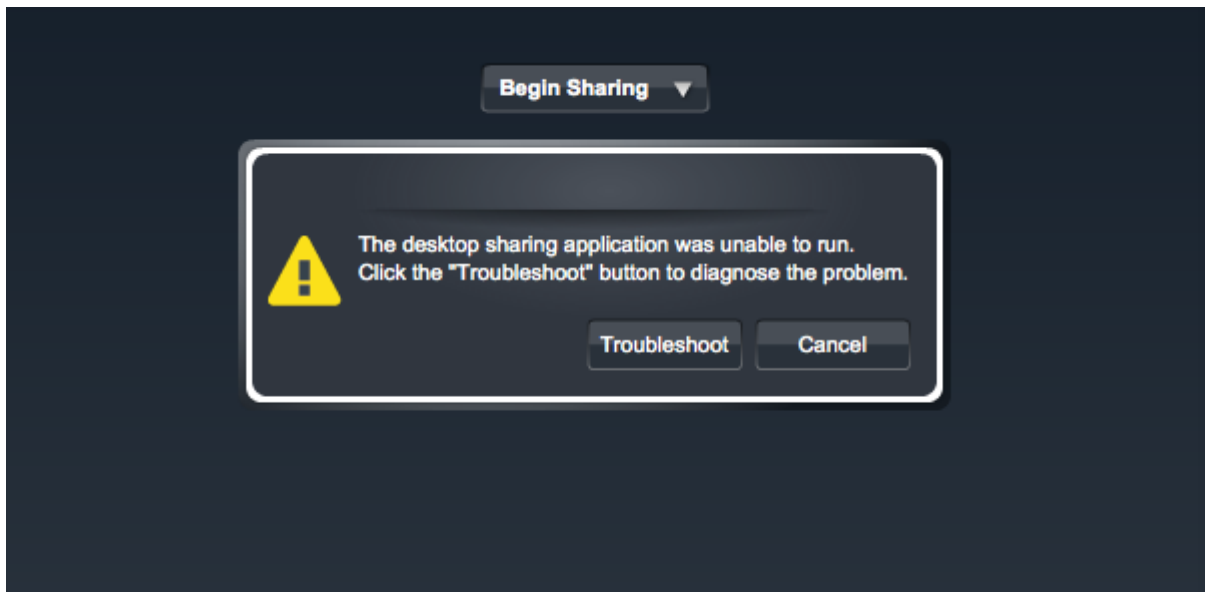
Issue: Use of an ALG with AAC results in AAC functionality no longer working due to the ALG limiting message sizes and restricting sequence numbering.

Workaround: Remove the ALG from the conferencing solution

6.21 Limitation with using Google Chrome on MacOSX

Issue: When using Google Chrome on MacOSX screen, sharing via AAC web collaboration does not work; both the entire screen and portion-of-screen options are affected. This is due to an interaction issue between Google Chrome, which is a 32-bit program, and MacOSX, which requires 64-bit program versions when using Java 7 applets. A picture of the error is provided below.

Workaround: Use either Safari or Firefox on the Mac when needing to do screen sharing



6.22 Use of Moderator Passcode with Scopia solution not recommended

Issue: If a participant in an AAC conference is connecting via a Radvision MCU (either 5000 or 6000 series) and he/she uses the moderator code to join the conference, then any users hearing music while they wait for the conference to start will never be joined into the conference.

Workaround: This issue does not happen if the participant code is used for people joining via a Radvision MCU. Only use of the participant code is recommended. When the participant code is used to join a call from Scopia, the AAC conference begins in fast start mode and the moderator code is not required. AAC Conference Moderators will need to join as participants if joining using the Scopia client. AAC Conference Moderators are encouraged to join via the AAC bridge in order to retain moderator controls.

6.23 Java 1.7 support for Document Conversion Server

Issue: The Document Conversion Server cannot be installed on a Windows server that runs Java 1.7. The server must run Java 1.6

Workaround: Change the %PATH% variable in the following file:

`\mcp_core_root\wars\dcS\Setup DCS.bat`

The %PATH% variable should be changed from jre7/bin to jre6/bin

6.24 Using Recording with Avaya Flare Experience

Issue: Starting and stopping Avaya Aura Conferencing Recording can only be activated by dial pad sequences when using Avaya Flare Experience

Workaround: To start or stop Recording, enter *2 in the Flare dial pad and follow the audio prompts.

6.25 Avaya Aura System Manager Multiple Device Access (MDA)

Issue: Using Avaya Aura System Manager's Multiple Device Access functionality is not supported with Avaya Aura Conferencing.

Workaround: There is no workaround; please disable this functionality for users accessing Avaya Aura Conferencing.

6.26 MacOS Upgrades Disable Screen Sharing

Issue: Some users have reported that following an upgrade of their MacOS that they can no longer use Avaya Aura Conferencing screen sharing capabilities

Workaround: The MacOS is disabling Java support following the upgrade; please re-install Java to enable this functionality. Java is required for the screen sharing functionality.

6.27 Trying to use Avaya Aura Conferencing Web Collaboration without Java installed

Issue: If a conference participant or moderator attempts to join or start a web collaboration session on a computer without Java installed, the user will receive an error: "This Webpage wants to run the following add-on: 'Control name is not available' from 'Not Available'.

Workaround: Install Java and ensure it is enabled for the browser.

6.28 Re-joining a locked conference in Avaya Aura Conferencing Web Collaboration

Issue: If a conference moderator starts a web collaboration session with no audio media, also called a Standalone Web Conference, and then locks the conference, he will be unable to join the conference if he leaves the conference

Workaround: There is no workaround; participants will need to leave the conference so that the session ends; once the conference ends then a new session can be started.

6.29 Recording a conference that starts as a Standalone Web Conference

Issue: If a Standalone Web Conference has audio participants join and the conference moderator has Auto Recording enabled, the conference is not recorded.

Workaround: The moderator will have to manually start recording.

6.30 Using full screen sharing with large resolution displays

Issue: If a presenter uses full screen sharing and has a display larger than 1600x1600, then the sharing may fail

Workaround: Use portion-of-the-screen sharing and keep the area size below 1600 pixels wide and/or tall.

6.31 Alarm 220 DNSL after upgrade

Issue: After upgrade from AAC 7.0 to AAC 7.2 there may be an alarm raised (AAC 220 DNSL) for a Document Conversion Server (DCS) in the system. This is a false alarm caused by the upgrade adding a new DCS with a server address of 0.0.0.1.

Workaround: Delete the new DCS.

6.32 Collaboration Agent not working after upgrade

Issue: After upgrade from AAC 7.0 to AAC 7.2 the Collaboration Agent may not process messages correctly if the upgrade procedure was not followed. This will manifest as users being unable to enter a conference via the Collaboration Agent.

Workaround: Restart the Collaboration Agent

6.33 Russian Conferencing Audio Prompts for Release 7.2

Issue: The 7.2 Core Apps Bundle does not contain the Russian localized prompts

Workaround: Please follow the procedure documented in section 3.1 on how to apply new prompt files.

6.34 Support of Encrypted Passcodes from LDAP Directory.

Issue: As per customer response through Beta Testing, the support for Encrypted Passcode from the LDAP database has changed to require a preceding Initialization Vector before the encrypted passcode value. This means that any existing deployments using Encrypted Passcodes will need to be updated.

Directions: Please review the following overview of encryption support, and contact your services or support team for assistance prior to converting your system to use encrypted passcodes.

Overview: For additional security you can store encrypted passcodes on the LDAP server to be synchronized to the Avaya Aura® Conferencing database.

Avaya Aura® Conferencing storage composed of the following elements:

- AES in CBC mode (128 or 256 bit keys)
- Random IV
- Base64 encoding

To encrypt passcodes, you must use the symmetric algorithm AES. Both 128 bit key and 256 bit key values for use with encryption are supported. The first step of encryption is to use the AES cipher in CBC mode with PKCS5 padding to create an encrypted value. Then second step requires a random Initialization Vector (IV). The IV is pre-pended to the encrypted value in from the first step. The new encrypted value is then base64 encoded for use with text files and storage in LDAP which can be synchronized to the AAC database. Encryption using non-random IV data is not supported will result in the inability to decrypt passcodes properly.

Avaya Aura® Conferencing will only decrypt passcodes based on the above criteria. Alternatives for attempting to decrypt passcodes are not reliable and therefore not performed. If a passcode fails to decrypt , then no additional attempt is made to validate the passcode value using clear text or different algorithm .

6.35 Engineering Parameters when not using a Co-Res configuration

Issue: When in a configuration different from the Co-Res configuration manual actions are needed to correctly set the WCMS engineering parameters.

Workaround: Please use the procedures in the Deployment Guide related to setting WCMS engineering values.

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.

