Avaya Aura® Conferencing 7.0 SP4 + Patch1
Release Notes v1.0

Contents

1 Introduction 4
2 Avaya Aura® Conferencing 7.0 SP4 feature overview 4
2.0 Existing functionality 4
2.1 AAC 7.0 SP2 5
2.2 AAC 7.0 SP3 6
2.3 AAC 7.0 SP3 patch 1 6
2.4 AAC 7.0 SP3 patch 2 6
2.5 AAC 7.0 SP4 + Patch1 6
2.6 Java Support Matrix 7
2.7 Licensing 7
3 Software Versions 7
3.1 Avaya Aura® Conferencing 7.0 SP4 Software Line-up: 7
3.2 Avaya Clients Load Line-up 8
3.3 Avaya Aura® Load Line-up 8
3.4 Radvision/ Scopia Load Line-up 9
4 Technical documentation 10
5 Software updates 10
6 Technical Advisements 10
6.1 Single Sign On parameter 10
6.2 Alarm for WCMS resynchronization failure 11
6.3 DCS file uploads can hang 12
6.4 Ad hoc conference calls initiated by Avaya Flare® Experience or 96X1 12
6.5 Checkpoint versioning on redundant systems 12
6.6 Call server failover 12
6.7 Supported JAVA versions 13
6.8 Excel documents in MyLibrary 13
6.9 Supported Flash versions with Firefox 13 13
6.10 Avaya Flare® Experience moderator dial out to a CS1000 Mobile-X client 13
6.11 Operator in an active call 14
6.12 Audible feedback prompt when entering ad hoc conference 14
6.13 Roster list 14
6.14 Avaya Flare® Experience - Carousel of participant 14
6.15 Subscribers unable to upload documents using the Web Collaboration interface in certain scenarios. 14
6.16 Duplicate CA Roster Entry After CA Moderator Force Out. 16
6.17 Aura 6.2.3 SM Removing Video for Ad-Hoc Video Escalations 16
6.18 Potential CA login failure after applying AAC7.0 SP1 Patch2 or AAC 7.0 SP2 or AAC 7.0 SP3 16
6.19 Lose Conference Events when H.323 Transfers to Flare 17
6.20 Video will not work if call held prior to conference start 17
6.21 Android App Limitations 17
6.22 Music on Wait media file upload issues 17
6.23 Conference Stays up during Avaya Aura Session Manager failover 17
6.24 Use of ALG with AAC is Not Recommended 17
6.25 Limitation with using Google Chrome on MacOSX 18
6.26 Use of Moderator Passcode with Radvision solution not recommended 18
6.27 Handling Anonymous callers from a cascade location. 18
6.28 Customer specific enhancement related to inter-region bandwidth management of conference calls. 18
6.29 Enhancement for AAC-RV Bulk User Import Interoperability 19
7 Technical Support 21
8 AAC 7.0 Capacity Limits 22
8.1 Standalone App Server 22
8.2 Standalone Web Server 22
8.3 Co-res Server 23

1 Introduction

This document includes important details for Avaya Aura Conferencing 7.0 Service Pack 4 pus Patch1. This document provides the software load line-up of Conferencing 7, the Service Pack, Avaya Aura, supported Avaya clients, and other call servers with which Conferencing 7 interoperates. It also provides a list of advisements, limitations, and workarounds.

2 Avaya Aura® Conferencing 7.0 SP4 feature overview

2.0 Existing functionality

Conferencing 7 delivers audio conferencing, Web collaboration capabilities and advanced user experience via Avaya Flare® Experience clients, Avaya one-X® Communicator R6.1 and 96x1 R6 clients . Clients that utilize all or some of the Conferencing 7 advanced UX/UI are: Avaya Flare® Experience for Windows and iPad, Avaya Collaboration Agent/Web Collaboration and the 96x1 phones. Conferencing 7 features are accessible on clients using the advanced UI or TUI commands.

The following are the highlights of the Conferencing 7 features:

- System Features
    - MeetMe audio/web conference
    - Event audio/web conferencing
    - Support for Aura Communication Manager, CS1000, Branch Call servers and clients.

- User features
    - Conference Roster
    - Mute self
    - Mute participants (some or all)
    - Media mute self
    - Media Mute participants (some or all)
    - Lecture Mode
    - Conference Lock/un-Lock
    - Assume Moderator Role
    - Promote to Moderator or Presenter
    - Entry/Exit tones on/off
    - Conference Continuation on/off
    - Terminate Conference
    - Add User
    - Drop User
    - Count Users
    - Document sharing and Whiteboard Collaboration

Note: A change was introduced in Avaya Aura Conferencing 7.0 SP1 that allows an administrator to determine how Collaboration Agent authentication will be done; the choice is either to use the Aura Session Manager PPM functionality for Collaboration Authentication or use the Avaya Aura Conferencing 7 network elements. The default for fresh installations is to use Avaya Aura Conferencing for CA authentication; for upgrades the system retains the current method.

Use of Avaya Aura Conferencing for CA authentication is recommended for any system which utilizes multiple Avaya Media Servers in the conferencing solution. The procedure to enable this method is documented in the "Administering Avaya Aura® Conferencing" document.

2.1 AAC 7.0 SP2

With the release of service pack 2 in December 2012 the following new content is introduced to Avaya Aura Conferencing 7:

- Support for video conferencing on the following endpoints
    - One-X Communicator
    - Avaya Flare Experience 1.1
        - Windows version is available now
        - iPad version will be supported when released to the market
    - Radvision/Scopia
        - Availability is expected in Feb. 2013
    - ADVD 1.1 has been supported for Audio only since AAC 7.0 launched and continues to be supported for Audio. Video and web collaboration are not supported with Conferencing 7.
- Web Collaboration App for Android
    - Client App is expected to be available in late March 2013
- Permanent audio roster association in the web-based Collaboration Agent
- Support of Avaya Aura FP2
- CS1000 Collaboration Pack interoperability with AAC7.0

  In addition, support for use of Collaboration Pack 1.1 with Communication Server 1000 R7.6 for Meet-Me functionality will be available in March 2013; support for Ad-Hoc and Dial-Out functionality with Collaboration Pack 1.1 will be available in May 2013. Collaboration Pack 1.0 with Communication Server R7.5 is not supported. Communication Server R7.5 continues to be supported for standard dial in meet me conferencing as noted in Section 3.4.

- **Radvision/ AAC Interworking**

  This section outlines the capabilities available with the Radvision/AAC Interworking feature. Details on Radvision are available at https://support.avaya.com
  "Administering Avaya Aura Conferencing and Radvision Scopia Interoperability"

Feature	AAC	Radvision	AAC/Radvision Interoperability
Audio Bridging	Yes	Yes	Yes
Video Bridging	Yes	Yes	Yes, Active Speaker
Content sharing	Yes	Yes	No, Radvision users must login to AAC to see content. AAC users must login to Radvision to see content.
Per-participant controls	Yes	Yes	No, AAC moderator can control AAC participants and MCU Moderator can control MCU participants.
HD video	Yes	Yes	Yes, if the AAC bridge is AVC-Only with HD 720p. Otherwise the SVC base layer resolution is exchanged (e.g. 360p for Class D and 180p for Class C).

2.2 AAC 7.0 SP3

The release of SP3 in February 2013 is focused on several bug fixes including several updates when interworking with Radvision/ Scopia.

2.3 AAC 7.0 SP3 patch 1

Two updates are introduced in SP3 patch 1:

a) Customer specific enhancement related to inter-region bandwidth management of conference calls.
b) Enhancement for AAC-RV Bulk User Import Interoperability

Please refer to section 6.28 and 6.29 for more details

2.4 AAC 7.0 SP3 patch 2

AAC supports the following conference/meeting invite format starting with this version of the 7.0 SP3 patch: **https://<domain name>/<conference code>**.

Example: **https://aac.examplecompany.com/12348765**.

The current version of the URL will continue to work after SP3 patch 2 is applied. New versions of the mobile clients and Outlook plugin are also available to support the shorter URL

2.5 AAC 7.0 SP4 + Patch1

The release of SP4 in June 2013 is focused on bug fixes including the following updates:

- Wi01096584 RV Interworking- Conf is not started after MCU endpoint joins when AAC participant is waiting
- Wi01096585 WebCollab-Android client cannot join collaboration using ShortURL
- Wi01096589 Fast Start Participant joins conf on audio and CA first, CA moderator cannot start WC
- Wi01095740 Guest cannot join Standalone Web Collab

- AAC-1735 Timeout due to low bandwidth connection
- wi01087775 Alarm required on system when replication is not enabled on media servers within a cluster
- wi01055050 Converted pdf from doc server missing images
- wi01090938 Location Table cache isn't updated
- AAC-1768 Regional Cascading-Cascading trunk is created incorrectly while user hears waiting music (SP4 Patch1)

2.6 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>.

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	

2.7 Licensing

This section details how product licensing works 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 SP3 as new or apply it to an existing installation can use the new video conferencing capability as a right of original purchase.
2) However, during the Controlled Introduction interval, video usage must be enabled with a special license feature which is added during product installation. This special feature will be provided to all SP3 users who request it from their Business Partner or Avaya contact.

3 Software Versions

3.1 Avaya Aura® Conferencing 7.0 SP4 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 7.0.

New Installations:

1. First install Linux OS “AAC Platform Installer 15.1.1” and then apply “AAC Platform Patches 15.1.9” to bring the OS to the software level.

2. Next install “AAC Application Bundle 15.0.10.0” and then upgrade to Service Pack “AAC Application Bundle 15.0.20.0 (SP4)”.
3. Next apply the latest patch “AAC Application Patch 15.0.20.1 (SP4 Patch1)”.

Upgrading Previous Installations:

1. First apply Linux OS patch “AAC Platform Patches 15.1.9”, if not already done, to bring the OS to the software level.
2. Next upgrade to Service Pack “AAC Application Bundle 15.0.20.0 (SP4)” to bring the applications to the latest software level.
3. Next apply the latest patch “AAC Application Patch 15.0.20.1 (SP4 Patch1)”.

Latest Available PLDS Downloads:

PLDS ID	PLDS Name	File Name
AAC00000008	AAC Data Migration Tool 1.0.14	AAC_Data_Migration_Tool 1.0.14.msi
AAC00000015	AAC Platform Installer 15.1.1	mcp_core_linux_ple2-15.1.1.iso
AAC00000016	AAC Application Bundle 15.0.10.0	dvd_AAC_MCP_15.0.10.0_2012-05-21-0556_coreApps.iso
AAC00000071	AAC Platform Patches 15.1.9 (SP4)	mcp_core_linux_ple2-15.1.9.patches.r-1.ext.iso
AAC00000072	AAC Application Bundle 15.0.20.0 (SP4)	dvd_AAC_MCP_15.0.20.0_2013-05-09-1602_coreApps.iso
AAC00000073	AAC Application Patch 15.0.20.1 (SP4 Patch1)	MCP_15.0.20.1_2013-06-05-1153.zip

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.

3.3 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 SP1 with latest patch releases in PLDS

SM	6.3 SP1 with latest patch releases in PLDS
CM	6.2 SP5 with latest patch releases in PLDS

3.4 Radvision/ Scopia Load Line-up

Documentation on Administering Avaya Aura® Conferencing and Radvision Scopia Interoperability is available at http://support.avaya.com/downloads/
Radvision/ Scopia software release: 8.0 Maintenance Release 2

** 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.IPTEL-52-2
CS1000 R7.5	patch: cs1000-vtrk-7.50.17.16-36.i386.000 + MPLR31809
B5800	8.0.067011

4 Technical documentation

See the latest versions of documents published on Avaya Support website.

Title
Accounting Records for Avaya Aura Conferencing 7.0
Administering Avaya Aura® Conferencing
Avaya Aura Conferencing Security Hardening
Avaya Aura® Conferencing 7.0 Security Design
Avaya Aura® Conferencing Alarms and Logs
Avaya Aura® Conferencing Collaboration Quick Reference
Avaya Aura® Conferencing Overview and Specification
Maintaining and Troubleshooting Avaya Aura® Conferencing 7.0
Operational Measurements for Avaya Aura Conferencing 7.0
Planning and Design for Avaya Aura® Conferencing 7.0
Using Avaya Aura® Conferencing Collaboration Agent (PDF)
Deploying Avaya Aura® Conferencing
Using Avaya Web Collaboration Agent for Android App

5 Software updates

Regular patch advisements are provided on the Avaya Support website.

At this time there is one patch required on SP4.

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.

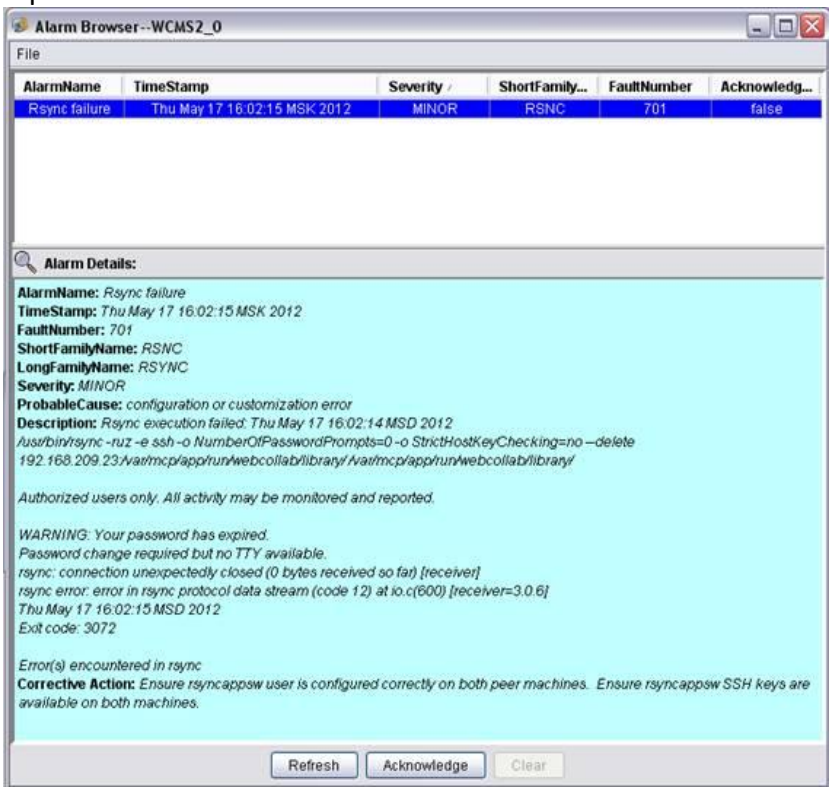
6.1 Single Sign On parameter

Issue: When upgrading from SMGR R6.1 to R6.2 the default setting for Single Sign On get set to False.
Workaround: You have to manually open the OpenSSO console. Go to Configuration -> Servers and Sites -> Default server settings and Set c66Encode to “true” and click save.

- **Note: This step is not required when upgrading from SMGR R6.2 to SMGR R6.2 SP2**

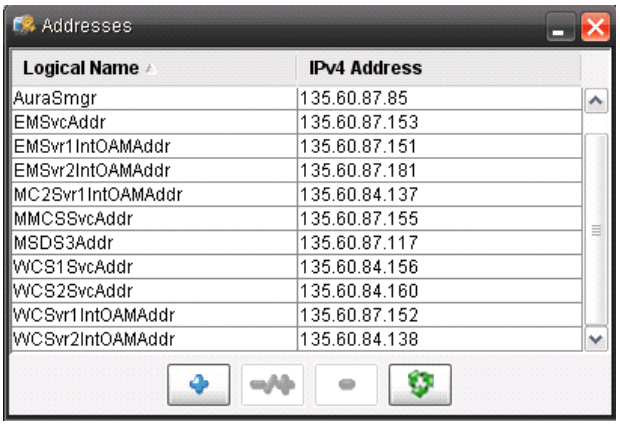
6.2 Alarm for WCMS resynchronization failure

Issue: You might encounter this alarm which is caused due to rsyncappsw password's expiration :



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 EMGUI. Normally the WCMS logical names follow a pattern of WCSSvr#IntOAMAddress; using the example picture below that means that WCSSvr2IntOAMAddr has the address.



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).

6.3 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, follow 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.

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

Issue: In CM you will need to administer up to 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

6.5 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

6.6 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

6.7 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. This Java version has inherent issues as mentioned by the vendors. Users can continue to use it 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 their 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.

6.8 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.

6.9 Supported Flash versions with Firefox 13

Issue: Avaya does not recommend the use of Firefox 13.0.1 with Adobe Flash player 11.3 with Windows 7. (Note: this is not an issue with Windows XP.) With this setup, there may be issues with resizing the Collaboration Agent and the Firefox browser may be non-responsive if the user selects the “logout” button in the CA window to exit from the conference login page.

Workaround : If the user requires Firefox 13.0.1 with Flash player 11.3, Avaya recommends either reverting back to an earlier version of flash player or temporarily disabling the “Protected mode” in Flash.

To revert to a previous version of Flash Player, please see this Adobe FAQ: How do I revert to a previous version of Flash Player?

To disable Protected Mode in Adobe Flash player, please see the following Adobe FAQ (last section): How do I troubleshoot Flash Players Protected Mode for Firefox?

6.10 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.

6.11 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.

6.12 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

6.13 Roster list

Issue: In a specific call scenario involving out dialing to a user which who has call forward enabled, the original number used dialed in the out dial is shown on the roster, not the number to which the call was forwarded option specified. The call does get forwarded. The issue is related to it not being in the roster. The issue only happens if Call forward is set to a PSTN number.
Workaround: None

6.14 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

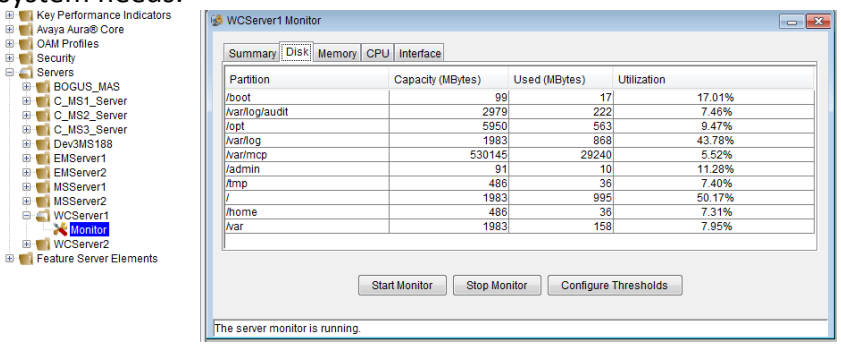
6.15 Subscribers unable to upload documents using the Web Collaboration interface in certain scenarios.

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 wherein the system runs out of space on the DCS server. Subscribers will see an “I/0 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.



    - 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. Value should be set in bytes.
            - /var/mcp/run/MCP_15.0/<<WCSNE>>/apache/www/meeting/Config-dist.php
            - /var/mcp/run/MCP_15.0/<<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_15.0/<<WCSNE>>/apache/www/meeting/Config-dist.php
        - /var/mcp/run/MCP_15.0/<<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_15.0/<<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

6.16 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 Conference by pressing the exit-door icon on the top-right corner of the CA Conference page, then press the “Conference” button to re-enter the conference, resulting in a Conference display without duplicate roster entries.

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

Issue: If deployed with Aura SM 6.2.3, when merging point to point calls to Adhoc conference, the SM SIP REFER Bandwidth processing results in the disabling the video which results in the client engaged in the escalated call with Audio only.
Workaround: Please refer to the Product Correction Notices for the Aura SM and determine the patch needed for the version of SM that is deployed and then apply the respective patch.

6.18 Potential CA login failure after applying AAC7.0 SP1 Patch2 or AAC 7.0 SP2 or AAC 7.0 SP3

Issue: AAC7.0 SP1 Patch2 will change how Collaboration Agent users are authenticated. Systems installed and users commissioned prior to AAC7.0 SP0 Patch1 “MCP_15.0.10.5_2012-06-22-2138.zip” will require manual action after applying AAC7.0 SP1 Patch2 to ensure that all uses can be authenticated properly.
Workaround: Administrators with systems falling into this category must perform an “edit/commit” action in the Avaya Aura System Manager for each user with a Conferencing Profile. Note that users that were added or updated after AAC7.0 SP0 Patch1 was installed are not affected by this change

6.19 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 user on the Flare device can join the call normally.

6.20 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 in 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 work 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.

6.21 Android App Limitations

Issue: The Android App has several limitations:

- On Android OS 2.X - The virtual keyboard Enter key is ignored when entering the conference ID to join; the user must hide the virtual keyboard and click Start
- On Android OS 2.X – Users can not send messages in the web collaboration message window when the device is in “landscape” mode

Workaround: Either use a more recent Android OS or do not execute the functions described above.

6.22 Music on Wait media file upload issues

Issue: If HTTP has been disabled on the AAC Element Manager (EM) or the Avaya Media Server (AMS) does not have TLS enabled with a valid certificate then problems can be experienced trying to upload Music on Wait media files.
Workaround: Ensure that the EM has HTTP enabled and that the AMS has TLS enabled with a valid certificate

6.23 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

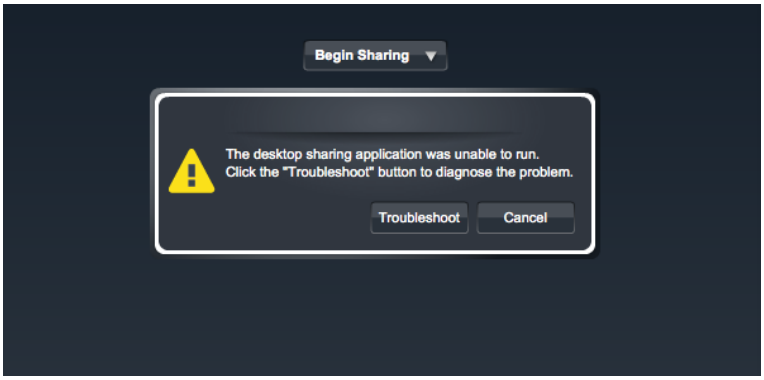
6.24 Use of ALG with AAC is Not Recommended

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

6.25 Limitation with using Google Chrome on MacOSX

Issue: When using Google Chrome on MacOSX screen sharing via AAC web collaboration does not work; both 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 requires 64-bit program versions when using Java 7 applets. A picture of the error experienced is provided below.
Workaround: Use either Safari or Firefox on the Mac when needing to do screen sharing



6.26 Use of Moderator Passcode with Radvision 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.

6.27 Handling Anonymous callers from a cascade location.

Issue: In order to handle anonymous callers joining from a cascade location, the domain name in the service URI from the incoming call will be used in setting up the cascading trunk. Therefore, this domain name must be configured as one of the system domain names in AAC7. Please double check the domain name has been configured in the AAC7. This issue is addressed in 7.0 SP2 patch 2 and 7.0 SP3

6.28 Customer specific enhancement related to inter-region bandwidth management of conference calls.

Issue: Customer specific enhancement related to inter-region bandwidth management of conference calls.

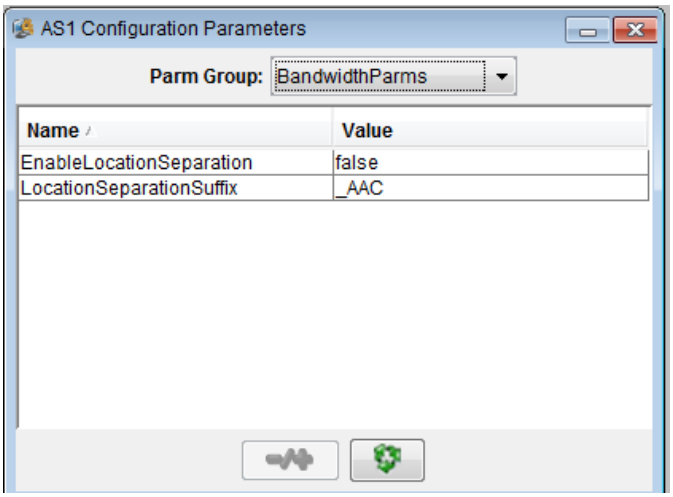
Summary:
When regional cascading is used it is possible that both the CM and SM will apply CAC for the same call leg. This enhancement allows for the inter-location bandwidth used for conference calls to be managed separately from bandwidth used between the same locations for regular non-conference related calls. This is accomplished by placing the media server clusters of an

existing location into a new location with the same name but with special suffix tag appended. The AAC will check for this tag when comparing the locations names and will not request WAN bandwidth from the SM when the only difference in the location names is the suffix tag. When the location does not match the AAC will request bandwidth as normal. For regions that should only have CAC enforced by the CM the corresponding locations on the SMGR should be configured with unlimited bandwidth. The AAC tagged locations should have the appropriate limits set on the SMGR.

Note: The CM's ip-network-region form should not have bandwidth limits set between regions belonging to subscribers and the region assigned to their local media server cluster. Only LAN bandwidth will be used between these regions.

New Application Server Configuration Parameters:
"EnableLocationSeparation" – default value is false. This parameter will enable bandwidth separation functionality when set to true. It is recommended that customers consult with Avaya before changing this parameter.

"LocationSeparationSuffix"- default value is "_AAC". This parameter specifies the suffix string used to identify SM/AAC managed bandwidth locations. When an originating location name matches the terminating location name minus the suffix then the two locations are treated as being the same and WAN bandwidth is not requested by the AAC. This parameter is only used when EnableLocationSeparation is set to true.



.

6.29 Enhancement for AAC-RV Bulk User Import Interoperability

Issue:
Currently on Radvision, Administrators wish to import Collaboration codes to the Virtual Rooms which are 10 digits. Having Collaboration codes that long on the AAC is not desired and provides poor usability.

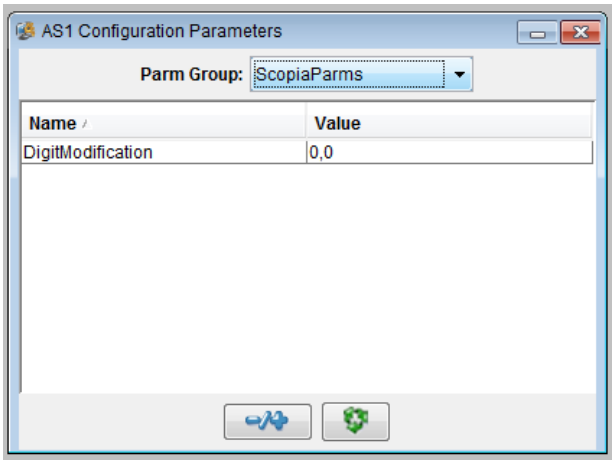
Solution:
New configuration group and parameter of "ScopiaParms/"Digit Modification" created for application server as shown by the following diagram. This configuration parameter specifies two indexes like "a,b" (both a,b are numbers and a>b) for the number of the digits to be used

for matching logic. The code first checks if there is a full match using the entire embedded collaboration code to find a conference on AAC side. If no match found then first or second digit modification will apply to find the match. The digit modification will use the right number of the digits in embedded collaboration code to find a conference.

The default value of (0,0) is used to imply that the AAC does not apply any digit modification and that the entire embedded Collaboration Code from RV should be used.

Example 1
Configuration parameter (7,4)
For AAC conference “6688520”, incoming call from RV with “virtualroom=23126688520”, exact look up fails, 7 digits look up matches.

Example 2
Configuration parameter (7,4)
For AAC conference “8520”, incoming call from RV with “;virtualroom=23116678520”, exact look up fails, 7 digits look up fails, 4 digit look up matches.



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.

8 AAC 7.0 Capacity Limits

8.1 Standalone App Server

Standalone AA Application Server	
#	**7.0 capacity**
# of provisioned users (moderator accnts)	150,000
# Audio/video active sessions (Meet-me+ Adhoc+Event)	10,000
# Web sessions*	7500
# CA sessions	7500
** Requires standalone WCMS server for >1000 web sessions;*	
WCMS can be co-resident with WCS and CA for =< 1000	

Standalone AMS -Meet- me /adhoc		
Codec Type	**Meet-me/Ad-hoc**	**Ad-hoc**
Audio sessions- G.711	**3000**	**3000**
Audio sessions- G.722	**2500**	**2500**
Audio sessions- G.729	**2000**	**2000**
Audio G.711+Video H.264 AVC 720p30@1.3Mbps	**600**	**600**
Audio G.711+Video H.264 SVC 720p30@1.6Mbps	**480**	**480**
Audio G.711+Video H.264 AVC 360p30@420kbps	**1500**	**1500**
Audio G.711+Video H.264 SVC 360p30@515kbps	**1200**	**1200**
Max # of sessions per conf call	**250 a/v +web**	**250 a/v+web**

Standalone AMS + Standalone web server -Event (lecture mode)	
Codec Type	**Event Conf**
Audio active sessions- G.711/722/729 (any combination)	**2000 a* +1000 web**
Audio(any codec)+VideoH.264 AVC 720p30@1.2Mbps	**2000 a+500v +1000 web**
Audio (any codec) +VideoH.264 SVC 720p30@1.5Mbps	**2000 a + 400v +1000 web**
Audio (any codec)+VideoH.264 AVC 360p30@420kbps	**2000a+1500v +1000 web**
Audio (any codec)+VideoH.264 SVC 360p30@515kbps	**2000 a+1200v +1000 web**

**Based on G729 numbers*

8.2 Standalone Web Server

Standalone Web Server (PA Mgr, WCS, WCMS)	
	Meet-me/Adhoc
# Web sessions	1000
# CA sessions	1000

Standalone WCMS Server (Required for>1500 web sessions)	
	Meet-me/Adhoc
# Web sessions	7500

8.3 Co-res Server

Co-Res Server (AS, AM, EM, DB, PROV, AMS, WCS, WCMS, PA Mgr)	
HP DL360G7, Dell R610	**Meet-me/Adhoc**
Audio G.711+Web/CA sessions+Video-H.264 AVC 720p30@1200kbps	500a+500web+400v
Audio G.711+Web/CA sessions +Video-H.264 SVC 720p30@1500kbps	500a+500web+320v
Audio G.711+Web/CA sessions +Video-H.264 AVC 360p30@420kbps	500a+500web+500v
Audio G.711+Web/CA sessions +Video-H.264 SVC 360p30@515kbps	500a+500web+500v
Audio G.722+Web/CA sessions +Video-H.264 AVC 720p30@1200kbps	500a+500web+400v
Audio G.722+Web/CA sessions +Video-H.264 SVC 720p30@1500kbps	500a+500web+320v
Audio G.722+Web/CA sessions +Video-H.264 AVC 360p30@420kbps	500a+500web+500v
Audio G.722+Web/CA sessions + Video-H.264 SVC 360p30@515kbps	500a+500web+500v
Audio G.729+Web/CA sessions + Video-H.264 AVC 720p30@1200kbps	300a+300web+300v
Audio G.729+Web/CA sessions + Video-H.264 SVC 720p30@1500kbps	300a+300web+300v
Audio G.729+Web/CA sessions +Video-H.264 AVC 360p30@420kbps	300a+300web+300v
Audio G.729+Web/CA sessions +Video-H.264 SVC 360p30@515kbps	300a+300web+300v

Note: Reduce all limits by 50% for the IBM S8800 server