Avaya Aura® Contact Center

Release 7.0 Feature Pack 1

Release Notes

This document contains information on software lineup, known issues and workarounds specific to this release of Avaya Aura®Contact Center.

TABLE OF CONTENTS

PURPOSE

This document contains known issues, patches and workarounds specific to this build and does not constitute a quick install guide for Contact Centre components. Please refer to the information below to identify any issues relevant to the component(s) you are installing and then refer to the Avaya Aura® Contact Center Installation and Commissioning guides for full installation instructions

PUBLICATION HISTORY

Issue	Change Summary	Author(s)	Date
1.0	Avaya Aura® Contact Center, 7.0 Feature Pack 1 GA Release	CC Release Engineering	19th December 2016
2.0	Avaya Aura® Contact Center, 7.0 Feature Pack 1 Localization GA Release	CC Release Engineering	30th January 2017
3.0	Avaya Aura® Contact Center, 7.0 Feature Pack 1 Localization GA Release	CC Release Engineering	22nd February 2017

SOFTWARE INFORMATION

Hardware Appliance

There are no software downloads associated with the Hardware Appliance deployment.

Software Appliance

The following are the files required to deploy Avaya Aura® Contact Center Release 7.0 into a virtualization environment. Please ensure you are using this version for all new software installation.

Avaya Aura Media Server OVA

File Name	MD5 Checksum
MediaServer_7.7.0.334_A15_2016.04.13_OVF10.ova	f845d3d252bde6123d3bd79396b0ae62

Avaya WebLM 7.0 OVA

The Avaya WebLM 7.0 software is a required piece of software when deploying the OVAs in a virtualisation environment. This software is used for product licensing. Please download this software from http://support.avaya.com
File name - WebLM-7.0.0.9-16703-e55-19.ova

DVD Product Installation

The following are the files required when deploying Avaya Aura® Contact Center using the Avaya Aura® Contact Center DVD. Please note, as part of the deployment of the product you are required to install the latest available service pack bundle when installing the product.

The supported Avaya Aura® Contact Center DVD version is outlined below. Please ensure you are using this version for all new software installation.

File Name	MD5 Checksum
AACC_7.0.1.0-405.iso	82bee195389d4eeccfafcc4bc0503255

Important Note:

Information on the latest feature packs available with this release is documented in the **Release Pack Bundle** section below.

Release Pack Bundle

The Avaya Aura® Contact Center software is delivered to customers as a release pack bundle. The release pack is installed on your base software and contains the latest software updates for the release.

File Name	MD5 Checksum
ACC_7.0.1.0_FeaturePack1-709.zip	c2583b3c2ab750d82105c8c4ac334d5f

Additional Required Updates

Avaya Aura® Contact Center Server

The following are additional Avaya Aura® Contact Center updates containing critical fixes that **must** be applied to your system.

File Name	MD5 Checksum
ACC_7.0.1.0_FeaturePack01_GA_Patches-301.zip	24ec157e653c13024238f509df486d04
ACC_7.0.1.0_FeaturePack01_GA_Patches-303.zip	f70a11f070b6f7a5e0fb6159714be8c4
ACC_7.0.1.0_FeaturePack01_GA_Patches-304.zip	55659763f0169c1fe6db3bd5b1ca735c

You must download all files listed. Please verify the MD5 checksums after download to ensure all files have been downloaded successfully

Localization support is provided by the deployment of the ACC_7.0.1.0_FeaturePack01_GA_Patches-303.zip software bundle

Avaya Aura Media Server OVA

The AAMS OVA version is: 7.7.0.334 with System Layer Version 15. Both need to be upgraded to the latest version. The Media Server needs to be updated to 7.7.0.359 and the System layer needs to be updated to 20. This is accomplished by downloading the two ISO files:

MediaServer_Update_7.7.0.359_2016.07.20.iso
MediaServer_System_Update_7.7.0.20_2016.06.22.iso

The procedure: Upgrading Avaya Aura Media Server 7.0.1 OVA from 7.7.0.334 to 7.7.0.359 details the steps required to upgrade the AAMS OVA.

File Name	MD5 Checksum
MediaServer_System_Update_7.7.0.20_2016.06.22.iso	603536de950fe009a3ba04a18ab42b14
MediaServer_Update_7.7.0.359_2016.07.20.iso	ef810c92d0e09499761643503191b9f0

Additional Optional Updates

ASG Plugin

The ASG Plugin is a serviceability application which enables secure access to the server when installed using a challenge-response mechanism. This update removes the presence of unnecessary accounts which are given permission to access the files in the applications directory. This effectively restricts access to the applications files to administrator users only.

The ASG Plugin currently placed on the server, not installed, does not have this patch and if required this version can be downloaded and placed on the server instead of the incumbent version.

This is optional in that only if you wish to install and use this plugin should it be installed; otherwise it is not required for normal Contact Center operations.

File Name	MD5 Checksum
ASGPlugin4WindowsX64.zip	76aaa6844a4863a86884d19a0b409558

SNMP Trap Configuration File

An SNMP Trap Configuration File (.cnf) is delivered containing the Avaya recommended events for SNMP capture. The configuration file can be imported into the SNMP Event Translator that is available after installing SNMP on the Windows Server 2012 R2. SNMP traps will be automatically generated and forwarded to the configured NMS system for all Event Viewer events that have a match in the configuration file.

The SNMP Trap Configuration File can be imported into the SNMP Event Translator using evntcmd.exe from the command prompt. A restart of the SNMP service is required after which the file content can be viewed using the SNMP Event Translator GUI (evntwin.exe). Exact details for the procedure are available in Windows Server 2012 R2 documentation.

The SNMP Trap Configuration File is available for download from the support site.

This is optional in that it should only be imported if you wish to forward SNMP traps to an NMS system for treatment or monitoring. Otherwise it is not required for normal Contact Center operations.

Note: As detailed in the AACC deployment guide, SNMP should be installed on the Windows Server 2012 R2 prior to deployment of the AACC application.

File Name	MD5 Checksum
ACC_7_0_1_0_SNMP_Trap_File_ver1_0.cnf	08a97caf629637aa7f9b4d9cd31beb8e

Patch Scanner

The following is an additional utility Avaya Aura® Contact Center support tool. This Patch Scanner utility is released with every Release Pack and Patch bundle from AACC 6.4 SP13 onwards.
If you are moving from an Avaya Aura® Contact Center 6.4 lineup to Avaya Aura® Contact Center 7.0 you must use the version of the Patch Scanner published in the 7.0 Release Notes document.

This version of the tool can be used prior to moving to Avaya Aura® Contact Center 7.0. See readme with the application zip file for further information.

File Name	MD5 Checksum
PatchScanner_1.0.0.21.zip	2815dc647b9bf0457072937f5c9d8cd3

Downgrade Utilities

File Name	MD5 Checksum
ARPI_7.0.0.0_Downgrade_7.zip	421b1513e5fa85f44e0ac831133e8db8
ARPI_7.0.0.1_Downgrade_0.zip	91f6db9fd727da8f3781df022274cebf

Migration Tool for RCW Generated Reports

This application is required when exporting Historical Reporting templates on an NES6/NES7/ACC 6.x server as part of a server migration. The most up to date version of the application is available with the "additional required updates" from the AACC lineup below.

The utility is available in: **Install Software\CCMA\RCW_Migration_Utility**

SWITCH SOFTWARE SUPPORT

Avaya Aura® Software

This section outlines the software requirements for the Avaya Aura© communications infrastructure. Avaya Aura® Contact Center supports minimum versions of the following Avaya Aura® components:

Avaya Aura Components	Release
Avaya Aura System Platform	6.2 FP4, 7.0, 7.0.1
Avaya Aura Solution for Midsize Enterprise	6.2 FP4, 7.0
Avaya Aura Communication Manager	6.2 FP4, 7.0, 7.0.1
Avaya Aura Application Enablement Services	6.2 FP4, 7.0, 7.0.1
Avaya Aura System Manager	6.2 FP4, 7.0, 7.0.1
Avaya Aura Session Manager	6.2 FP4, 7.0, 7.0.1
Avaya Aura Presence Services	6.2.6, 7.0.1

Avaya Communication Server 1000

This section outlines the software requirements for the Avaya Communication Server 1000 infrastructure.

Avaya Aura® Contact Center 7.0.1.0 is only supported with CS 1000 R7.6.

Required Packages

The following are the required CS1000 packages

Converged Office	77, 153, 164, 242, 243, 324 41, 42, 43, 50, 114, 155, 214 215, 218, 247, 311, 324
SIP CTI	77, 153, 164, 242, 243, 324 41, 42, 43, 50, 114, 155, 214, 215, 218, 247, 311, 324
2000 CDNs	388, 411

DepList for CS 1000 R7.6

DepList Patch	PI PEP Enabler	Comments
MPLR33345		CS1000 doesn't send AML/MLS Transfer Complete message when POM Dialler completes an external transfer MPLR33345 – GEN PEP – included in R7.6 SP6 and higher.
MPLR33041	MPLR32229	Multimedia contact cannot return to queue while agent is holding a CDN call. Package 411 prevents agent acquired by AACC from going NOT_READY without dropping the active call. MPLR32229 – Free of charge PI PEP for AACC

		MPLR33041 – GEN PEP – included in R7.6 SP5 and higher.
MPLR32413	MPLR30038	New constant required when CCMS pulls call from interruptible IVR & presents to agent. Free of charge PI PEP for AACC. MPLR32413 – GEN PEP – included in R7.6 SP5 and higher.
MPLR33045 (CPPM, CPPL) **MPLR33072 (CPP4)**	MPLR28837	CS1000 – Different CLID on CCT desktop and acquired phone when DAPC feature is used. MPLR28837 –Chargeable PI PEP for AACC MPLR33045, MPLR33072 – GEN PEP – included in R7.6 SP5 and higher.
MPLR32439		AACC USM Ringing event is missing if the call goes back to SCR of the original agent /RGNA feature. Only required if agent configured for RGNA, and only applicable for AACC-SIP (not AACC-AML). GEN patch for AACC – included in R7.6 SP5 and higher.
MPLR33744		CTI cannot control CDN call after making emergency and supervisor calls. MPLR33744: GEN PEP – included in R7.6 SP6 and higher

NOTE: Channel Partners will need to follow the standard PI Request process (per **Communication Server 1000 Product Improvement by PEP (Patch) Policy**). These patches will be available at no charge on approval to support this configuration.

Note that Unified Communication products (CS1000, CM, AES etc.) and other products in your solution follow independent lifecycle dates. Depending on their lifecycle state, full support may not be available on older versions of these products. In case where AACC patches require a dependent patch on the switch, that patch may not be available on an old switch release that is in End of Manufacture Support lifecycle state. Please refer to lifecycle bulletins specific to the products/versions in your solution.

NOTE: The PI PEP enabler is required, ONLY if the customer already had that functionality on an earlier release or if the customer now wants to add that functionality. Please review CS1000 patch information on ESPL to determine if any of the noted PI PEPs are applicable for your customer environment; note that some are chargeable and require an order (and PO) on Avaya before they can be provided. More information on CS1000 PI PEPs is available on ESPL @ https://downloads.avaya.com/css/P8/documents/100166145

PLATFORM VENDOR INDEPENDENCE (PVI)

Hardware Requirements

For Single Server deployments (Voice and Multimedia with Avaya Media Server on a physical platform) a Gigabit Network Adapter is required that supports Receive Side Scaling (RSS) with 4 RSS queues.

Network Adapter known issues

There is currently an open issue with Microsoft Windows Server 2012 R2 with Broadcom NetXtreme Gigabit Ethernet Adapter (BCM5720) that can result in Windows OS kernel crash for AACC 7.0 Single Server deployments. The bug resides in Microsoft's pacer.sys (QoS packet scheduler) and is exposed by the Broadcom NetXtreme Gigabit Network Adapter (BCM5720) when RSS is enabled and configured for more than 1 queue. This issue has only been found with Broadcom NetXtreme Gigabit Ethernet Adapter and (specifically the Broadcom 5720 Adapter). The issue has been accepted by Microsoft and they are working on a fix.

Recommended Network Adapter

The following RSS capable Gigabit Network adapter has been tested successfully with Single Server deployments – **Intel(R) Gigabit 4P I350-t Adapter**

OPERATING SYSTEM & VIRTUALIZATION

Operating System

All Avaya Aura® Contact Center server applications are supported on the following operating systems:

- Windows Server 2012 R2 Standard (64-bit Edition)
- Windows Server 2012 R2 Data Center (64-bit Edition)

The Avaya Aura Media Server is supported installed co-resident with AACC on a Windows Server 2012 R2 platform. AAMS installed on a standalone Windows Server 2012 R2 is not supported.

AAMS is supported on Red Hat Enterprise Linux (RHEL) 6.x 64-bit OS. It is not supported 32-bit RHEL. It is not supported on any other version of Linux.

Microsoft Service Packs

None.

Microsoft Hotfixes

Before deploying any new Windows Security Patches and Hotfixes – you must confirm that any Windows patches are listed as supported in the Avaya Aura® Contact Center Security Hotfixes and Compatibility listing – published every month on support.avaya.com.

Additionally, please install all required Microsoft Operating System update listed in the Microsoft Operating System Updates section of this document.

Please ensure that you do not enable Automatic Updates on your Avaya Aura® Contact Center Server or Client PCs. All Windows Security patches and hotfixes must be manually deployed after consulting the supported Avaya Aura® Contact Center Security Hotfixes and Compatibility listing

Red Hat Enterprise Linux Updates

AAMS is only supported on Red Hat Enterprise Linux (RHEL) 6.x 64-bit servers.
For an AAMS installed on a customer installed RHEL 6.x 64-bit server, it is mandatory to register the RHEL OS with Red Hat Networks (RHN) and to apply all of the latest updates. AAMS is tested regularly against all the latest RHEL updates.

The AAMS OVA AAMS ships with the most recent RHEL updates as of GA. Avaya are responsible for supplying any mandatory Red Hat updates for the OVA installed OS. This is supplied as an AAMS System Update ISO file that is uploaded via AAMS Element Manager and applied by logging into an SSH session using the same account to access AAMS Element Manager. The OVA does not need to be registered with Red Hat Networks.

Microsoft Operating System Updates

The section outlines additional Microsoft Updates that must be applied to your system. Click on the link below to bring you directly to the KB article on the update.

Update ID	Summary
KB3100956	You may experience slow logon when services are in start-pending state in Windows Server 2012 R2

Important Notes:

1. **Important** If you install a language pack after you install this update, you must reinstall this update. Therefore, we recommend that you install any language packs that you need before you install this update. For more information, see Add language packs to Windows.

Update ID	Summary
KB2973337	SHA512 is disabled in Windows when you use TLS 1.2

Important Notes:

1. This KB is contained in the August 2014 update rollup **KB2975719** listed below and does not need to be installed individually if the rollup is applied.
2. **Important** Do not install a language pack after you install this update. If you do, the language-specific changes in the update will not be applied, and you will have to reinstall the update. For more information, see Add language packs to Windows.

Update ID	Summary
KB2975719	August 2014 update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2

Important Notes:

1. **Important** When you install this update (2975719) from Windows Update, updates 2990532, 2979582, 2993100, 2993651, and 2995004 are included in the installation.

Update ID	Summary
KB3101694	"0x000000D1" Stop error in Pacer.sys when there's heavy QoS traffic in Windows Server 2012 R2

Important Notes:

1. **Important** If you install a language pack after you install this hotfix, you must reinstall this hotfix. Therefore, we recommend that you install any language packs that you need before you install this hotfix. For more information, see Add language packs to Windows.
2. **Important** This KB should only be applied to servers which include Avaya Aura Media Server on

Windows Server 2012 R2, i.e. where AACC and AAMS have been installed co-resident on a single physical server. It is not required on any deployment which does not include Avaya Aura Media Server on Windows Server 2012 R2.

Update ID	Summary
KB3140245	Update to enable TLS 1.1 and TLS 1.2 as a default secure protocols in WinHTTP in Windows

Important Notes:

1. **Important** This hotfix is required for windows 7 SP1 clients. Do not apply to AACC server.
2. **Important** Please read the Microsoft update at the link provided, as there are manual steps required with this hotfix.
3. **Important** This update is **NOT** required if Certificate Manager on AACC server is has Current TLS Protocol Level for CCMA-MM set to TLSv1.0.

Update ID	Summary
KB3100956	Remote desktop connection logins and local console logins can fail with a “please wait” message if some AACC services do not complete startup.

Internet Explorer Support

Element Manager and CCMA require that Internet Explorer 10.0 and Internet Explorer 11.0 be configured to run the web sites in “Compatibility Mode”.
Microsoft support indicates that some websites might not display correctly in Windows Internet Explorer 9. For example, portions of a webpage might be missing, information in a table might be in the wrong locations, or colors and text might be incorrect. Some webpages might not display at all. If a portion of the webpage doesn't display correctly, try one or more of the following procedures:

Note: IE Compatibility Mode must be enabled on IE 10.0 and IE 11.0.

To turn on Compatibility View

1. Open Internet Explorer by clicking the Start button
2. In the search box, type Internet Explorer, and then, in the list of results, click Internet Explorer
3. Click the Compatibility View button on the Address bar

The supported browser is Microsoft Internet Explorer 10.0 or later (32 Bit only – 64 Bit not supported).

DEPLOYMENT & CONFIGURATION INFORMATION

Pre-Installation Considerations

Windows Automatic Maintenance

Windows Server 2012 R2 provides a centralized mechanism for maintaining the operating system. This feature is called Automatic Maintenance, and is used to carry out tasks such as hard disk defragmentation and application of Microsoft Windows updates among others.

This mechanism can sometimes interfere with the deployment of Contact Center software, resulting in failed installations. It is recommended that this feature be disabled for the duration of Contact Center software installs.

To disable Automatic Maintenance:

1. Start – Run 'Taskschd.msc'
2. In the Task Scheduler Library browse to Microsoft – Windows – TaskScheduler
3. Select the *Idle Maintenance* task, right-click and choose 'Disable'
4. Select the *Regular Maintenance* task, right-click and choose 'Disable'
5. Alternatively, modify the properties of the *Regular Maintenance* task and ensure it is not set to run during your installation maintenance window.

After installation is complete you may re-enable Automatic Maintenance

To enable Automatic Maintenance:

1. Start – Run 'Taskschd.msc'
2. In the Task Scheduler Library browse to Microsoft – Windows – TaskScheduler
3. Select the *Idle Maintenance* task, right-click and choose 'Enable'
4. Select the *Regular Maintenance* task, right-click and choose 'Disable'

Changes to Universal Networking in AACC 7.x

The new 10.1 version of Gigaspaces deployed with AACC 7.x is not compatible with the version deployed in AACC 6.x. This impacts the Universal Networking feature (UNE). It will not function between AACC 7.x and AACC 6.x without the deployment of a UNE alignment patch on 6.x which adds UNE Web Services.

Before adding AACC 7.x to an existing AACC 6.x network or upgrading a networked deployment to AACC 7.x, the network must first be upgraded with the UNE alignment patch using the following steps:

- If customer are on AACC 6.4 SP14 or earlier they need to contact Avaya Support to request an alignment patch
- For customers on AACC 6.4 SP15
  1. Install the UNE alignment patch on each 6.x node. Patch name is AvayaAura_CCCC_6.4.215.208
  2. Proceed with adding or upgrading AACC 7.x nodes as required.
- For customer on AACC 6.4 SP16 no additional steps are required.

Migrating Report Creation Wizard Reports from pre AACC 6.4 SP15 Systems

The migration procedure for Report Creation Wizard based reports on an AACC system requires that the server hosting CCMA be at the AACC 6.4 SP14 or SP15 patch level prior to the report export step. The MigrationRPTToRCWX.exe utility has a dependency on the version of Crystal Reports and is only compatible with the version on the AACC 6.4 SP14 or SP15 lineup.

Equinox 3.0 Not Supported for use as an Agent Softphone

Equinox 3.0 is not support for use as a Contact Center Agent Softphone

Hot Patching Support

Hot patching is supported from Avaya Aura© Contact Center Release 7.0.0.0 and 7.0.0.1 to this Avaya Aura© Contact Center 7.0 Feature Pack 1 (7.0.1.0)

POM Support

AACC 7.0.1 supports POM Service Pack 3.0.4. No prior version of POM is supported with AACC 7.0.1. If AACC site is operating with POM then site **must upgrade to POM 3.0.4 before upgrading to AACC 7.0.1 (7.0 Feature Pack 1)**.

Open Interfaces Web Services and SIP Call Recording Configuration must be manually re-entered after upgrade

If you are upgrading from 7.0.0.x and are using Call Recording or AACC Open Interfaces you need to reconfigure Open Interfaces Web Services after the upgrade has completed. Prior to upgrading, note the CCT Web Services settings in the CCT Console utility and the WS Open Interfaces settings in the Sever Configuration utility. Alternatively, take a screenshot. After the upgrade process has completed, use the CCT Console utility to check the CCT Web Services configuration and the Server Configuration utility to check the WS Open Interfaces configuration. Reapply the settings noted prior to the upgrade if different.

Note: A server restart is required as part of Service Pack installation if this configuration change is applied after the server restart CCT services must be restarted before the changes will take effect

.

Installation

New Installations

Install-time Patching

Install-time patching is mandatory for Avaya Aura Contact Center software deployments using the provided DVD media.

Mandatory Execution of Ignition Wizard – Patch Deployments

After deployment of the AACC software using the DVD installer, if the Ignition Wizard process is deferred, it will not be possible to install Patches (DPs) either via Update Manager or manually (double-clicking on the installer file). Successful execution of the Ignition Wizard prior to applying Patches to the system is **mandatory**.
This does **not** affect the removal or reinstallation of AACC Service Packs, only AACC Patches (DPs).

System Backup after Ignition (IMPORTANT)

A full AACC backup must be taken after the ignition process has completed and before the system is commissioned or used.
This is important for systems that will be used as migration targets. The CCMA data can only be migrated to a system that does not contain any customer data. The CCMA migration will fail if the system is found to contain data other than what was injected by the Ignition Wizard.
If the CCMA migration fails in this way, the solution is to go back to the post-ignition backup or re-install the system.

Upgrades

Avaya Release Pack Installer

A new application is provided within the Avaya Aura® Contact Center Release Pack bundle called the Avaya Release Pack Installer (ARPI). This application provides an automated method of updating existing Avaya Aura® Contact Center 7.0 software and must be used when upgrading from AACC 7.0.0.0 or AACC 7.0.0.1 to 7.0.1.0

The application will

1. remove all installed AACC 7.0.x.x Product Updates (Service Packs and Patches)
2. remove all unwanted AACC Third Party software
3. install AACC 7.0.1.0 required Third Party Software
4. install the latest AACC software from within the release pack bundle

Application Location:

The Avaya Release Pack Installer is contained within the Release Pack bundle in folder 'AvayaReleasePackInstaller'.

The application supports the installation of Generally Available Patch bundle content.

Generally Available Patch Bundle Installation

When the AvayaReleasePackInstaller.exe is launched, if you wish to install Generally Available Patch Bundle content, you should select the appropriate radio button option.

If you choose to proceed without installing GA Patch content, the Update Manager application must be used to install this patch content at a later time.

To install Patch bundle content, the complete ProductUpdates folder from within the GA Patch bundle must be copied locally. This folder should not be modified - the ReleasePackManifest.xml must not be moved to another location.

Limited Patch Installation

The Avaya Release Pack Installer application does not support the installation of limited patches. To deploy limited patches the Update Manager application must be used.

Instructions:

1. Download the **AACC 7.0.1.0 Release Pack Bundle** to your local system and unzip
2. Download all available **7.0.1.0 GA Patch Bundles** to your local system
3. Unzip each GA Patch bundle separately into a folder reflecting the patch bundle zip name
4. When all individual 7.0.1.0 GA Patch Bundles are extracted into their respective folders, copy **each folder** into a single parent folder called 'GA Patch ProductUpdates'
5. Launch the Avaya Release Pack Installer from folder 'AvayaReleasePackInstaller' which is located within the **7.0.1.0 Release Pack** bundle extracted in step 1 above
6. When available, choose the option to install GA Patches and browse to the extracted Patch Bundle 'GA Patch ProductUpdates' folder from step 4 above
7. Continue installation…

Note: If upgrading, the Avaya Aura® Contact Center Update Manager application resident on the system will fail to install the Contact Center 7.0.1.0 Release Pack software. This is due to third party software changes between Contact Center 7.0 Service Pack 0 or Service Pack 1, and AACC 7.0 Feature Pack 1.

Note: It is not possible to install Generally Available patch (DP) content until the Ignition Wizard has been run successfully.

Upgrading Avaya Aura Media Server 7.0.1 OVA from 7.7.0.334 to 7.7.0.359

The AACC 7.0.1 AAMS OVA comes with version 7.7.0.334 of the Media Server installed with System Layer Version 15. Both need to be upgraded to the latest version. The Media Server needs to be updated to 7.7.0.359 and the System layer needs to be updated to 20

1. Launch AAMS Element Manager.
2. Navigate to EM > Tools > Manage Software > Updates > Upload Updates.
3. Locate the System Layer Update ISO (available from the ftp site, please see section: Avaya Aura Media Server OVA):
   MediaServer_System_Update_7.7.0.20_2016.06.22.iso
4. Click Browse to select the software update to upload this file to the AAMS.
5. Click Upload
   Your browser shows a progress spinner until the upload completes.
   The web page refreshes when the update completes and displays the details of the update including the filename of the uploaded file.
6. Locate Media Server Update ISO (available from the ftp site, please see section: Avaya Aura Media Server OVA):
   MediaServer_Update_7.7.0.359_2016.07.20.iso
7. Click Browse to select the software update to upload this file to the AAMS.
8. Click Upload
   Your browser shows a progress spinner until the upload completes.
   The web page refreshes when the update completes and displays the details of the update including the filename of the uploaded file.
9. Click on “Install Updates”
   Wait until upgrade completes.
10. Logon to AAMS Element Manager and go to System Status->Element Status and verify that the AAMS version is 7.7.0.359 and Appliance version 20.

Upgrading Avaya Aura Media Server for AACC 7.0 to AAMS for AACC 7.0.1

This section details the upgrade steps for all supported AAMS deployments to upgrade the AAMS to the version shipped with AACC 7.0.1.

CAVEAT: *If the Contact Center is using RSS or SHOUTcast configuration for Music Streaming then this configuration is not maintained after the upgrade. This configuration must be noted down and manually re-entered (in a new configuration page) to the upgraded AAMS. Please refer to Issue:* ***CC-9854*** *below for further information.*

Upgrading AAMS OVA from 7.0 to 7.0.1

This section provides instructions on how to upgrade the Avaya Aura Media Server OVA from version 7.7.0.269 and System Layer 14 to 7.7.0.359 and System Layer 20.

1. Launch AAMS Element Manager.
2. Navigate to EM > Tools > Manage Software > Updates > Upload Updates.
3. Locate the System Layer Update ISO (available from the ftp site, please see section: Avaya Aura Media Server OVA):
   MediaServer_System_Update_7.7.0.20_2016.06.22.iso
4. Click Browse to select the software update to upload this file to the AAMS.
5. Click Upload
   Your browser shows a progress spinner until the upload completes.
   The web page refreshes when the update completes and displays the details of the update including the filename of the uploaded file.

6. Locate Media Server Update ISO (available from the ftp site, please see section: Avaya Aura Media Server OVA):
   MediaServer_Update_7.7.0.359_2016.07.20.iso
7. Click Browse to select the software update to upload this file to the AAMS.
8. Click Upload
   Your browser shows a progress spinner until the upload completes.
   The web page refreshes when the update completes and displays the details of the update including the filename of the uploaded file.
9. Using the cust login credentials, open a Linux shell and run the following command to install the update:
   installUpdate
10. Type "yes" to continue installation.
    The system will reboot and the install System Update 7.7.0.20 and Media Server update 7.7.0.359.
11. Logon to AAMS Element Manager and go to System Status->Element Status and verify that the AAMS version is 7.7.0.359 and Appliance version is 7.7.0.20.

Upgrading AAMS on Customer Install Red Hat Linux 6.x 64 bit Server from 7.0 to 7.0.1

This section provides instructions on how to upgrade the Avaya Aura Media Server from version 7.7.0.269 to 7.7.0.359 on a server with a customer installed Red Hat Linux 6.x 64bit server.

1. Open putty session with root access.
2. Upload binary file (using winscp): **MediaServer_7.7.0.359_2016.07.20.bin**. Make sure to choose "Binary" mode of transfer.
3. chmod +x MediaServer_7.7.0.359_2016.07.20.bin
4. Run command: ./ MediaServer_7.7.0.359_2016.07.20.bin and follow instruction to complete installation.
5. After installation, logon to AAMS Element Manager and go to System Status->Element Status and verify that the AAMS version is 7.7.0.359.

Upgrading AAMS on Windows 2012 Server (co-resident with AACC) from 7.0 to 7.0.1

This section provides instructions on how to upgrade the Avaya Aura Media Server from version 7.7.0.269 to 7.7.0.359 on a Windows 2012 server that is co-resident with the AACC installation.

1. Shutdown Contact Center using SMMC.
2. Open services.msc and stop "**SMMC Daemon"** and "**SMMC service"**.
3. Run InstallerMAS.exe
4. After installation, logon to AAMS Element Manager and go to System Status->Element Status and verify that the AAMS version is 7.7.0.359.

Downgrades

Avaya Release Pack Installer

Two separate versions of the Avaya Release Pack Installer application are available, enabling the downgrade of systems from Contact Center 7.0.1.0 to 7.0.0.0 and 7.0.0.1

These versions of the Avaya Release Pack Installer are provided as separate downloads and contain all software required to successfully downgrade both third party and Contact Center software.

Each of the Avaya Release Pack Installer downloads also contains the Generally Available patch bundle pertinent to that target release.

Each application will

1. remove all installed Contact Center 7.0.1.0 Product Updates (Service Packs and Patches)
2. remove all unwanted Contact Center Third Party software
3. install Contact Center 7.0.0.1 or 7.0.0.0 required Third Party Software
4. install the latest Contact Center software from within the release pack bundle
5. optional – install Generally Available patches

Application Location:

The 7.0.0.0 and 7.0.0.1 Avaya Release Pack Installer is available on the Avaya support site, and accompanies the release of the 7.0.1.0 software. It is made available as a zip archive.

Note: the contents of the Avaya Release Pack Installer bundle should not be modified.

Generally Available Patch Bundle Installation

The application supports the installation of Generally Available Patch bundle content.
When the AvayaReleasePackInstaller.exe is launched, if you wish to install Generally Available Patch Bundle content, you should select the appropriate radio button option.

If you choose to proceed without installing GA Patch content, the Update Manager application must be used to install this patch content at a later time. The Update Manager application is available on the system with the installation of Contact Center software.

The GA Patch Bundle for each downgrade target release is incorporated into the Avaya Release Pack Installer zip download. There is no requirement to download the GA Patch Bundles separately.

Instructions:

1. Download the ARPI_7.0.0.0_Downgrade_7.zip or ARPI_7.0.0.1_Downgrade_0.zip to your system and extract the contents
2. Launch the AvayaReleasePackInstaller.exe from folder ‘ARPI’
3. When available, choose the option to install GA Patches and browse to folder ‘GA Patch Bundles’
4. Continue installation…

Post Installation Configuration

Avaya Aura Media Server

Avaya Aura Media Server Configuration

The following configuration must be carried out on all AAMS servers.

1. Launch AAMS Element Manager and browse to ***System Configuration >> Network Settings >> General Settings >> Connection Security***
2. Un-tick "***Verify Host Name***" setting and hit the "***Save***" button followed by "***Confirm***".
3. If using TLS SRTP media security then skip to step 6.
4. Browse to: ***System Configuration >> Media Processing>>Media Security***
5. Change ***Security Policy*** from **BEST EFFORT** to **SECURITY DISABLED** and hit the "***Save***" button.
6. Browse to ***System Configuration >> Network Settings >> General Settings >> SOAP***
7. Add AACC IP Address into ***SOAP Trusted Nodes***. If HA, add AACC Active, Standby and Managed IP Address.
8. Hit the "***Save***" button followed by "***Confirm***"
9. Browse to ***System Configuration >> Signalling Protocols >> SIP >> Nodes and Routes***
10. Add AACC IP Address into ***SIP Trusted Nodes***. If HA, add AACC Active, Standby and Managed IP Address.
11. Ensure that AAMS can resolve both the hostname and Fully Qualified Domain Name (FQDN) of the CCMA server by trying to ping the CCMA hostname or FQDN from the AAMS
    Name resolution can be achieved either by using a DNS server or editing the hosts file on the AAMS. The AAMS OVA does not allow root ssh access, so the ability to edit the hosts file is provided in Element Manager: On EM navigate to **System Configuration** > **Network Settings** > **Name Resolution** and enter the IP address and hostname of the CCMA server. If the AAMS is installed on a customer built Red Hat server, then EM does not provide this functionality. In this case /etc/hosts file needs to be edited on the Red Hat server (e.g. using a ssh putty session) using the root account.

Avaya Aura Media Server Installed on Red Hat Enterprise Linux Servers

The following configuration must be carried out on all servers with AAMS installed on Red Hat Enterprise Linux Servers. Note: This configuration is **not** required for the AAMS OVA.

1. Install firewall (iptables) policy file and enable firewall
2. Create AAMS Element Manager User account Group: ***susers*** Account: ***cust***
3. Configure and enable Network Time Protocol (NTP)
4. Install Access Security Gateway (ASG)

A RHEL shell script has been provided on the AACC DVD that applies all of the above configuration steps.
The script name is **sysconfig.sh** and is located at: ***Install Software\AMS\Linux***
Run the following steps on PVI RHEL Installed AAMS servers (Not required for co-resident Windows or OVA)

1. Copy the following file from the AACC DVD to the /tmp directory on the AAMS server:
   Install Software\AMS\Linux\sysconfig.sh
2. Log onto the AAMS server command line with root privileges (e.g. using putty), execute the following commands and then follow the prompts:
   cd /tmp
   chmod +x sysconfig.sh
   ./sysconfig.sh

Agent Greeting Recorder commissioning when CCMA managing Multiple CCMS Servers

In AACC 7.0, the Agent Greeting recorder application is always installed on the AACC Tomcat server that is co-resident with CCMS. By default, it will assume that CCMA is also installed on the same host. In cases where the CCMA instance managing CCMS is hosted elsewhere, the Agent Greeting recorder needs to be made aware of the remote CCMA address in order to operate correctly.

Currently, there is no GUI mechanism for updating this Agent Greeting recorder configuration. To set the CCMA address, edit the following file and update the ***ccma.address*** entry from its default value of 127.0.0.1 to the appropriate IP address:

D:\Avaya\Contact Center\apache-tomat\conf\agentgreeting.properties

CCMM Administration

Due to performance considerations for Avaya Agent Desktop 7.0, the interval value for *Agent Desktop Configuration-> User Settings -> Web Stats Refresh Interval* should be set to a *minimum* of 30 seconds.
Note that the default and recommended interval time is 60 seconds.

EWC – Server name change procedure: Steps when removing CCMM patches

This section is only applicable to systems running Enterprise Web Chat (EWC). EWC is a licensed feature in AACC 7.0 offering an alternative to the traditionally available Web Communications. EWC uses a new chat engine and because of this additional steps are required when performing a server name change on the CCMM server. These steps are fully documented in the *Avaya Aura Contact Center Server Administration* document. In the event that CCMM patches are removed from the CCMM server after a server name change operation has occurred, it will be necessary to reapply the EWC specific name change steps again. These steps are outlined below and should be run after CCMM patches have been removed/re-applied.

Before you begin

Shut down the CCMM services using SCMU.

Procedure

1. Log on to the Multimedia Contact Server
2. Right-click Start.
3. Select Run.
4. Type cmd.
5. Click OK.
6. In the command line window, enter
   `CD D:\Avaya\Contact Center\EnterpriseWebChat\eJabberd`
7. Enter `update_hostname.bat <CCMM_servername>` where `<CCMM_servername>` is the new Multimedia Contact Server name.
8. Restart the CCMM server to apply changes
9. Ensure CCMM services have started OR use SCMU to start CCMM services.

Agent Controls Browser Application – Mandatory certificate with IOS 9 and later

From IOS9 any IOS device running the Agent Controls Browser Application to connect to AACC will be required to provide a certificate.

SIP Networking in an Environment with pre-AACC 7 Nodes

In a networking configuration, every node in the network must have a unique Home Location Code (HLOC). The unique HLOC guarantees that call IDs are unique across the network. Prior to AACC 7, unique HLOCs for each SIP node were manually configured. AACC 7 introduced the automatic configuration of the unique HLOC for a node. Automatically configured HLOCs begin at 10001. In a network with manually configured nodes ensure that the manually configured nodes do not conflict with the automatically configured HLOCs. Configuration of HLOC is only applicable in a networking setup.

Enterprise Web Chat (EWC) enabled through CCMM Administration

EWC is disabled by default on installation of 7.0.1 even when EWC license enabled. To enable EWC it must be enable in CCMM administration under Web Comms Settings -> Enterprise Web chat. The Enterprise Web Chat setting in CCMM administration is only available when EWC license is enabled.

Agent Desktop Prerequisites

The following prerequisites are required for Agent Desktop on clients. Note: Administrative rights are required to install these prerequisites

- Microsoft .NET Framework 4.5.2 (DotNetFX452)
- Windows Installer 4.5 Redistributable (WindowsInstaller4_5)
- Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package ATL Security Update (vcredist_x86)
- Microsoft Visual C++ 2008 Redistributable Package (x86) (vcredist90_x86)

These prerequisites are available on the AACC server <Application Drive>:\Avaya\Contact Center\Multimedia Server\Agent Desktop

Note: Microsoft .NET Framework 4.5.2 is cumulative with 4.5.1, 4.5 and 4.0. So when you install .Net Framework 4.5.2 you also have 4.0 and 4.5.

Multimedia Prerequisites for server migration

This is only applicable to users migrating to new AACC 7.0 servers and keeping the same server names:

In this scenario users must select the same Multimedia Database Drive during the AACC 7.0 install as contained in Backup. If post install, users migrate a database backup from a previous version of AACC and the Multimedia Database drive defined in the backup does not match the Multimedia Database drive selected during the 7.0 install users will be unable to open attachments that were restored from the backup.

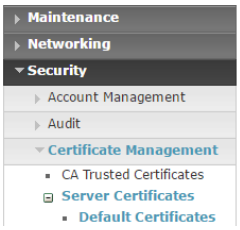
SECURITY INFORMATION

IMPORTANT NOTE: AACC supplied AES Security Certificate expiration notification

Expiration Date: Jan 6th, 2018 for certificate used for AE Services

The 7.0 and 7.0.1 installation supplies not only out of the box (OTB) security certificates for AACC, but also OTB security certificates for the AES server to assist the customer to configure AES, specifically the SIP-CTI link to AACC, to work with the out of the box certificates on AACC.

This default out of the box AES specific security certificate has an expiration date that will expire on **January 6, 2018.** This certificate is identified by the issued by tag of *Avaya HDTG Product Root* and used by AE Services when applied to AES.



Alias	Status	Issued To	Issued By	Expiration Date	Used By
serverCert	valid	AEServices	Avaya HDTG Product Root	Jan 6, 2018	AE Services
Avaya	valid	AE Services Management Console	AE Services Management Console	Apr 7, 2031	Web
Avaya_Common	valid	common	common	Mar 11, 2034	Web

After this date this certificate will not be viable and the mandatory secure link for SIP-CTI to AACC will not be established and functionality will be lost.

Any deployment which is using this certificate needs to plan to have it replaced prior to this date to avoid disruption of services. This will then involve additional configuration on AACC security store as the new AE services certificate will be signed by a different Certificate Authority (CA) and their root CA certificate will have to be placed into the AACC store.

Note:
The AES Security Certificate is an out of the box certificate intended to support lab or pre-production deployments only. It is not intended for use in a production environment.
This also applies to AACC out of the box certificates. While they have a longer expiration date they are not intended for production environments and must be replaced.

Avaya Aura® Contact Center security certificate migration considerations

Migration from 6.4 to 7.x

Due to the changes made in AACC 7.0 release regarding improved security stance, migration of the AACC 6.4 certificate store to AACC 7.X or higher is not possible.

The only path available when moving to AACC 7.X from AACC 6.4 is the creation of a new store on the AACC 7.X system, the signing of the certificate signing request (CSR) by a selected Certificate Authority and the importing of these new security certificates into the new store.

No elements of the security store from AACC 6.4 can be migrated to AACC 7.X

The following sections are applicable to migrations from 7.0 to later versions only.

Note: AACC 7.X come with the default store as standard and as such does not need to be migrated from previous releases. Please be advised this default store is not to be used in a production environment and is designed to be used in a test/configuration only situation.

Migrating AACC Security Store from AACC 7.0 to 7.x

The following sections are applicable to migrations from 7.0 to later versions only.

Note: AACC 7.0 and AACC 7.0.1 come with the default store as standard and as such does not need to be migrated from previous releases. Please be advised this default store is not to be used in a production environment and is designed to be used in a test/configuration only situation.

Name of Server is important

When intending to reuse existing security certificates on a new system then the receiving system will have to have the exact name as the donor system otherwise the security certificate will not match the underlying server. If the security certificate and underlying server name do not match, then warnings and errors will be presented to the user, when attempting to use this security certificate to establish a secure connection.

Note

The recommendation is that, if possible, new security certificates be generated for the new system rather than reuse security certificates from another system.

Restoring Certificate store to a new system

If the decision to reuse the security certificates then the migration of security certificates is a manual process and requires that the security certificate store on the server be backed up using the Certificate Manager Backup feature.

This will back up the necessary files required to be imported back in on the new system using the Certificate Manager Restore feature.

The receiving system name must be the same as the donor system otherwise errors will occur when attempting to use the security certificates to establish a secure connection.

Note

The backed up files will be modified if coming from a release prior to 7.0 during the restore process so it is recommended that you keep a copy of the original backed up files.

See Appendix C – Store Maintenance for details on backing up and restoring the certificate store.

TLS v1.2 as default level for TLS communication

Fresh installations

On fresh installations only, the default TLSv1 level enforced is TLS v1.2. This means that TLS v1.0 and TLS v1.1 protocol levels are disabled and are not available to be used in the solution or on the underlying Windows 2012 R2 operating system.

Migrations

Migrations can be considered in the same area as fresh installations in that the default TLSv1 level enforced is TLS v1.2.

Upgrades

On an upgrade where the feature pack is applied on an existing 7.0 release then there is no enforcement of TLS v1.2 on the server. This is relevant only to the Windows operating system level support of TLS versions.

For SIP traffic and Event Broker web services the enforcement of TLS v1.2 still applies and if these levels need to be modified then please refer to the section “Resetting TLSv1 Levels”.

In 7.0.1 the default TLSv1 level enforced is TLS v1.2. This means that TLS v1.0 and TLS v1.1 protocol levels are disabled and are not available to be used in the solution or on the underlying Windows 2012 R2 operating system.

Resetting TLSv1 Levels

If after a fresh install and application of the feature patch there is a mechanism in place to re-enable the lower level TLS levels if required as this new TLS v1.2 default setting may have an impact on any legacy applications that consume AACC services that cannot support this level of TLSv1. To allow backward compatibility with older releases and applications that consume AACC services the TLSv1 level can be lowered to reestablish functionality if found to be incompatible with the new TLSv1 level.

The general rule when setting the TLSv1 levels is shown in the table below

TLS Level Set	TLS v1.0 available	TLS v1.1 available	TLS v1.2 available
1.0	Yes	Yes	Yes
1.1	No	Yes	Yes
1.2	No	No	Yes

When the TLS v1 level is set the general rule is any level under that set level is disabled and any level above it is still available. It is configurable via Certificate Manager Security Configuration tab

How to change the TLSv1 levels

The new TLSv1 level settings can all be changed in the Certificate Manager application which can be launched from the AACC server.

In the Security Configuration Tab of the Certificate Manager application there are three drop boxes which allow the user to lower the TLSv1 levels for the following application and services outlined in the next section.

Services and Applications covered by new TLSv1 setting

The three main areas where this new setting covers are

- Windows operating system
- Web Traffic
- SIP Traffic

Windows operating system

This covers all of the windows operating system and any Microsoft based applications, such as IIS for example.

This can be lowered to TLS v1.0 or TLS v1.1 if required via the Certificate Manager application.
If TLS v1.0 is set as default for example, then TLS v1.1 and TLS v1.2 is still available.

Web Traffic

IIS

This is covered with the changes made to the underlying Windows Operating system. Which is also the same setting configurable via the Certificate Manager Security Configuration tab.

Tomcat

This web server is set to use TLS v1.2 only. It is currently not configurable.
All known applications that use Tomcat can operate at TLS v1.2 and thus no need to have an option to enable lower protocols.

Lightweight/framework web application servers

Event Broker Web Service TLS v1 level can be set on the Certificate Manager application.

SIP Traffic

This covers all SIP traffic to and from the AACC server. For AACC systems the SIP-CTI link is always TLS, the rest are configurable. This is configurable via Certificate Manager Security Configuration tab.

AACC has one permanent TLS connection, SIP-CTI and the following compatibility matrix shows below the supported TLS v1 levels when connecting to older AES's. If your deployment has an older version shown in the matrix below then lowering the TLSv1 level will reestablish a secure link.

AES releases TLSv1 support

AES Release	TLS v1.0 support	TLS v1.1 support	TLS v1.2 support	Options
6.3.3	Yes	No	No	Would require SIP Signaling TLS v1 level to be lowered on AACC via Certificate Manager GUI
7.X	Yes	Yes	Yes	
7.0.1	No	No	Yes	TLS v1.0 and TLS v1.1 can be enabled AES OAM/Admin Interface

For non-mandatory TLS SIP connections

While AES is a mandatory secure connection, the other servers that make up the solution can be configured to secure their connection to the AACC server and so below are the compatibility tables for the different versions that may be used in the solution.

Session Manager releases	See Appendix C – Session Manager releases TLSv1 support
Avaya Aura Media Server	See Appendix C – Avaya Aura Media Server releases and TLSv1 support

Known applications and services that cannot support TLS v1.2

There are applications and services which cannot support TLS v1.2 currently and a review of these applications and services should be made to determine the course of action prior to moving to 7.0.1. The table below lists all known application and services that cannot support TLS v1.2

HDX / DIW connection to databases	See Appendix C – HDX/DIW connection to databases
Remote desktop	See Appendix C – Remote Desktop
System Manager 7.0	See Appendix C – System Manager 7.0

SMB signing and Network-attached storage (NAS) devices

In this release SMB signing has been implemented and as such all connecting devices and platforms will have to be able to support SMB signing otherwise access to devices that cannot support the level of SMB signing in place on the Contact Center Server may become inaccessible.

This has been noted on older NAS devices where the current level of software cannot meet the SMB signing requirements and access to these devices has been shown not to be possible.

LOCALIZATION

Avaya Aura Contact Center 7.0 Feature Pack 1 (7.0.1) Avaya Agent Desktop (AAD), Outbound Campaign Management Tool (OCMT), Contact Center Manager Administration (CCMA) and Web Agent Controls UI and online Help is localized into French, German, LA Spanish, Simplified Chinese, Brazilian Portuguese, Russian, Japanese, Traditional Chinese, Korean and Italian.

Overview of AACC 7.0.1 I18N and L10N Products & Components

Components that are used by Contact Center agents or by Contact Center supervisors performing non-specialized functions are localized.
Interfaces to support administration or specialized functions (for example, creating routing applications) are not localized.

The following table lists all AACC 7.0.1 products and components in relation to Internationalization and Localization:

AACC 7.0.1 Products	Component	International OS Support? Yes/ No	Localized? Yes/No	Comments
CCMS	All components	Yes	No	
CCT	Web Agent Controls	Yes	Yes	
	Web Agent Controls online help	Yes	Yes	
	All other components	Yes	No	
Server Utility	All components	Yes	No	
License Manager	All components	Yes	No	
Web Collaboration	All components	Yes	n/a	
CCMA	Server Components	Yes	No	Only Administration users work with Server Components.
CCMA	Contact Center Management	Yes	Yes	
CCMA	Access and Partition Management	Yes	Yes	
CCMA	Real-Time Reporting	Yes	Yes	
CCMA	Historical Reporting	Yes	Yes	
CCMA	Configuration	Yes	Yes	
CCMA	Emergency Help	Yes	Yes	
CCMA	Outbound	Yes	Yes	
CCMA	Historical Report Templates	Yes	Yes	
CCMA	Agent Desktop Display	Yes	Yes	
CCMA	Online Help	Yes	Yes	

AACC 7.0.1 Products	Component	International OS Support? Yes/ No	Localized? Yes/No	Comments
CCMA	Orchestration Designer (OD)	Yes	No	The target audience of the Localization effort (call center agents and supervisors) do not use the OD tool.
CCMA	Configuration Tool	Yes	No	Only administrators use the Configuration Tool.
CCMA	Element Manager	Yes	No	Login page is localized.
CCMM	Server Components	Yes	No	
CCMM	AAD Client	Yes	Yes	
CCMM	AAD online Help	Yes	Yes	
CCMM	OCMT Client	Yes	Yes	
CCMM	OCMT online Help	Yes	Yes	

Software

Supported operating systems

A language patch contains all supported languages. For CCMA, only languages that are appropriate to the local operating system of the server can be enabled. For example, you can enable the simplified Chinese language on a simplified Chinese OS, however you cannot enable German on a simplified Chinese OS.

The following language operating systems support Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), Contact Center Manager Administrator (CCMA) Server, Contact Center Multimedia (CCMM) Server, License Manager (CCLM) and Server Utility (CCSU) co-resident:

Supported Language OS	Languages									
	ZH-CN	FR	ES	DE	PT-BR	JA	ZH-TW	RU	KO	IT
Windows Server 2012 R2 Standard (64-bit Edition)	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Windows Server 2012 R2 Data Center (64-bit Edition)	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Localized Components (CCMA and CCMM)

The following table lists the compatibility between the CCMA language patch and the operating system language family. Only compatible languages can be enabled on the CCMA server

		Supported CCMA Languages									
OS Language		FR	DE	ES	PT-BR	IT	ZH-CN	ZH-TW	JA	RU	KO
	English	Y	Y	Y	Y	Y	N	N	N	N	N
	Any 1 Latin1 language	Y	Y	Y	Y	Y	N	N	N	N	N
	Simplified Chinese	N	N	N	N	N	Y	N	N	N	N
	Trad. Chinese	N	N	N	N	N	N	Y	N	N	N
	Japanese	N	N	N	N	N	N	N	Y	N	N
	Russian	N	N	N	N	N	N	N	N	Y	N
	Korean	N	N	N	N	N	N	N	N	N	Y

The following table lists the compatibility between the CCMM language patch and the server operating system language family.

Server OS Language	Language Patch Supported
English	Y
Any 1 Latin1 language	Y
Simplified Chinese	Y
Trad. Chinese	Y
Japanese	Y
Russian	Y
Korean	Y

Language specific support and configuration

NB: The local language operating system for example French should be a full language operating system (installed from the language DVD/CD) rather than as an OS language patch on top of an English operating system install, for example English Windows 2012 with Microsoft French language patch installed.

Support of CCMA Client

Language	CCMA Client
French	Supported on Internet Explorer 10 and 11, Browser's Language Preference set to fr-FR. CCMA will be displayed in French if the French language patch is installed on the server, otherwise it will appear in English.
German	Supported on Internet Explorer 10 and 11, Browser's Language Preference set to de-DE. CCMA will be displayed in German if the German language patch is installed on the server, otherwise it will appear in English.
LA Spanish	Supported on Internet Explorer 10 and 11, Browser's Language Preference set to es-CO. CCMA will be displayed in Spanish if the Spanish language patch is

	installed on the server, otherwise it will appear in English.
Simplified Chinese	Supported on Internet Explorer 10 and 11, Browser's Language Preference set to zh-CN. CCMA will be displayed in Simplified Chinese if the Simplified Chinese language patch is installed on the server, otherwise it will appear in English.
Brazilian Portuguese	Supported on Internet Explorer 10 and 11, Browser's Language Preference set to pt-BR. CCMA will be displayed in Brazilian Portuguese if the Brazilian Portuguese language patch is installed on the server, otherwise it will appear in English.
Russian	Supported on Internet Explorer 10 and 11, Browser's Language Preference set to ru-RU. CCMA will be displayed in Russian if the Russian language patch is installed on the server, otherwise it will appear in English.
Italian	Supported on Internet Explorer 10 and 11, Browser's Language Preference set to it-IT. CCMA will be displayed in Italian if the Italian language patch is installed on the server, otherwise it will appear in English.
Japanese	Supported on Internet Explorer 10 and 11, Browser's Language Preference set to ja-JP. CCMA will be displayed in Japanese if the Japanese language patch is installed on the server, otherwise it will appear in English.
Traditional Chinese	Supported on Internet Explorer 10 and 11, Browser's Language Preference set to zh-tw. CCMA will be displayed in Traditional Chinese if the Traditional Chinese language patch is installed on the server, otherwise it will appear in English.
Korean	Supported on Internet Explorer 10 and 11, Browser's Language Preference set to ko-KR. CCMA will be displayed in Korean if the Korean language patch is installed on the server, otherwise it will appear in English.

Support of CCMM Client

Language	CCMM Client
French	Supported on French Windows 7, 8.1 and 10
German	Supported on German Windows 7, 8.1 and 10
LA Spanish	Supported on LA Spanish Windows 7, 8.1 and 10
Simplified Chinese	Supported on Simplified Chinese Windows 7, 8.1 and 10
Brazilian Portuguese	Supported on Brazilian Portuguese Windows 7, 8.1 and 10
Russian	Supported on Russian Windows 7, 8.1 and 10
Italian	Supported on Italian Windows 7, 8.1 and 10
Japanese	Supported on Japanese Windows 7, 8.1 and 10
Traditional Chinese	Supported on Traditional Chinese Windows 7, 8.1 and 10
Korean	Supported on Korean Windows 7, 8.1 and 10

Support of CCMM Server and Configuration Notes

CCMM server / Regional Options Configuration

Language	CCMM Server
French	CCMM Server installed on French 2012. Regional option default (French)
German	CCMM Server installed on German 2012. Regional option default (German)
LA Spanish	CCMM Server installed on Spanish 2012. Regional option default (Spanish)
Simplified Chinese	CCMM Server installed on Simplified Chinese 2012. Regional option default (Simplified Chinese)
Brazilian Portuguese	CCMM Server installed on Brazilian Portuguese 2012. Regional option default (Brazilian Portuguese)

Russian	CCMM Server installed on Russian 2012. Regional option default (Russian)
Italian	CCMM Server installed on Italian 2012. Regional option default (Italian)
Japanese	CCMM Server installed on Japanese 2012 Regional option default (Japanese)
Traditional Chinese	CCMM Server installed on Traditional Chinese 2012. Regional option default (Traditional Chinese)
Korean	CCMM Server installed on Korean 2012. Regional option default (Korean)

Enable email analyzer

Language	**Email Analyzer**
French	Change default SimpleAnalyzer to FrenchAnalyzer
German	Change default SimpleAnalyzer to GermanAnalyzer
LA Spanish	Change default SimpleAnalyzer to AlphanumericAnalyzer
Simplified Chinese	Change default SimpleAnalyzer to ChineseAnalyzer
Brazilian Portuguese	Change default SimpleAnalyzer to BrazilianAnalyzer
Russian	Change default SimpleAnalyzer to RussianAnalyzer
Italian	Change default SimpleAnalyzer to ItalianAnalyzer
Traditional Chinese	Change default SimpleAnalyzer to ChineseAnalyzer
Japanese	Change default SimpleAnalyzer to CJKAnalyzer
Korean	Change default SimpleAnalyzer to CJKAnalyzer

See French as an example:
An English email analyzer (AlphanumericAnalyzer) is enabled by default for keyword analysis of English Latin-1 character sets on the CCMM server. A FrenchAnalyzer should be specified for French. The *mailservice.properties* file on the CCMM Server specifies what analyzer is used and lists all supported analyzers in the comments.

Action needed: Update *mailservice.properties* file on the CCMM server to enable the email analyzer for French:

1. Stop the **CCMM Email Manager** service on the server.
2. Navigate to D:\Avaya\Contact Center\Multimedia Server\Server Applications\EMAIL.
3. Open mailservice.properties.
4. Change the properties of the file from read only to write available.
5. In the <box> search for the line mail.analyzer=AlphanumericAnalyzer.
6. Change mail.analyzer=AlphanumericAnalyzer to mail.analyzer=FrenchAnalyzer.
7. Start the CCMM Email Manager service on the server.

The keyword is used correctly for routing email messages with a French string.

Wildcard use (Asian), Limitation 1 – Single Byte Routing

NB: The following wildcard limitation applies to Asian languages only

Again, using Simplified Chinese is used as an example, but all Asian languages using double byte will apply;
To route a single byte keyword, you must save the keyword as DOUBLE byte on the server.

There is a limitation when enabling the email analyzer to Japanese (CJKAnalyser).
This is a limitation of the creator of the analyzer, Lucene.

A problem arises ONLY when using SINGLE BYTE characters in the keyword, double byte routes successfully.
To route a single byte keyword, you must save the keyword as DOUBLE byte on the server.
There are no new files needed for this workaround.
Action: The workaround is to add DOUBLE byte keywords to route both single and double byte successfully.
If you wish to route a single byte keyword to a skillset, you must setup the keyword in DOUBLE byte.
For example to route the single byte keyword コプタ to a skillset called EM_Test do the following.

1) Create a DOUBLE byte keyword

- In the Multimedia Administrator, click the plus sign (+) next to Contact Center Multimedia, click the plus sign next to E-mail Administration, and then double-click Keyword Groups.
- The Keyword Groups window appears.
- To create a new keyword group, click New.
- In the Name box, type a unique name for the keyword group (maximum 64 characters. This NAME must be in English). E.g. “DoubleByteCoputa”
- In the Keyword box, type the word (in DOUBLE byte) you will be searching for. E.g. “コプタ” Click Add.
  The keyword is added to the list, and the keyword group is created. Click Save.

2) Create a Rule to route the keyword to a skillset

- Start the Rule Configuration Wizard.
- On the Rule Configuration Wizard – Input Criteria window, under Available Keyword Groups, select a keyword group you want to use for this rule. E.g. “DoubleByteCoputa”
- Click the black arrow to insert the keyword group name into the selection box.
- Click Next.
- In the Rule box, type the name for your rule. E.g. “DoubleByteCoputaRule”
- In the Skillset box, select a skillset for your rule. . E.g. “EM_Test”
- Click Save.
- Click Finish. Your rule is created with the keyword group.

3) Send in an email with the SINGLE byte word コプタ.
The single byte keyword now routes successfully to the EM_Test skillset.
** Note this also applies when using wildcards in keywords.

*Wildcard use (Asian), Limitation 2 – Wildcard * and ? string position*

NB: The following wildcard limitation applies to Asian languages only

Wildcard ‘?’ or ‘*’ can only be used at the end of a keyword in a Japanese environment.
When using the wildcard ‘*’ or ‘?’, it can only be used at the end of a string
for example:
たば* = ok
た*た = no

Note:
To route the wildcard keyword successfully, the ‘*’ can be entered in either full-width or half width.
The ‘?’ can be entered in full-width only

Email Domain Names (Asian)

NB: The following applies to Asian languages only

Using Japanese as an example:
Internationalized Domain Names are defined by RFC 3490. They can include glyphs from East Asian languages. The take-up on these domain names has been low to date – mostly because of the dangers of 'phishing' sites (an email with a link to www.aib.ie in an email might point you to a site that has the "i" and a "b" in the domain but some other glyph resembling an "a".

W3C have identified a means of using 'punycode' to implement IDNs – this basically provides an ASCII equivalent to the domain name. Normally, the client (web browser or email client) accepts the IDN in native characters and converts it to 'punycode' e.g. xn–jp-cd2fp15c@xn--fsq.com . The receiving client will identify the sender as being a punycode' string and resolve to the native characters. CCMM can support IDNs by having the user enter a punycode' email address directly. The receiving client will be capable of rendering the native characters.

CCMM friendly display names

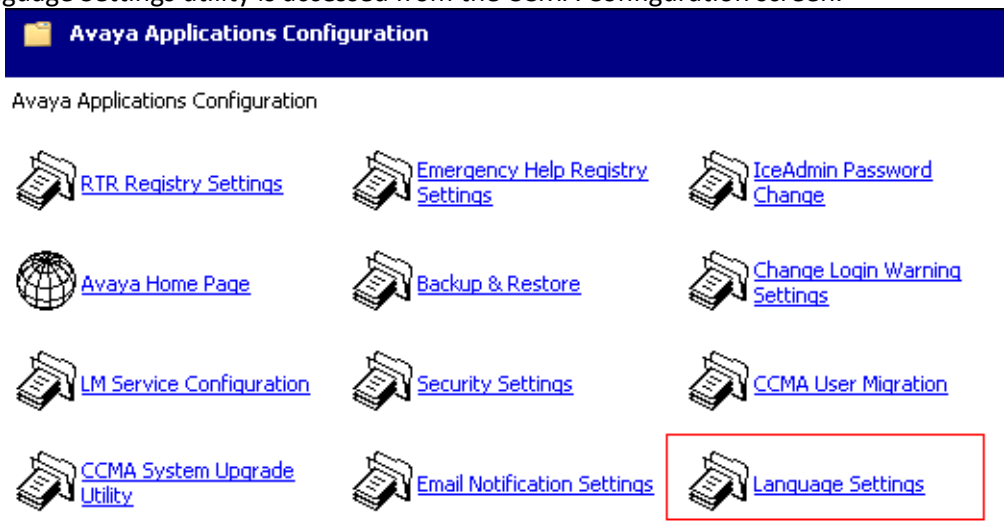
Display names are referred to in the CCMM Server online Help in section **Creating or changing a recipient**, section 99. In the Display Name box, type the friendly name you want to appear in the e-mail From address (for example, Customer Support). You must enter a display name for each mailbox.
In response to the case reported above, the Internet Standard IETF RFC 1036, Section 2.1, permits only ASCII characters in the display name.
Some email vendors, such as MS Outlook, included, invalidly permit double-byte display names which are contrary to the Internet Standard. CCMM has always strictly adhered to the Internet Standard and handles only ASCII characters.

Logging on to Contact Center Manager Administration

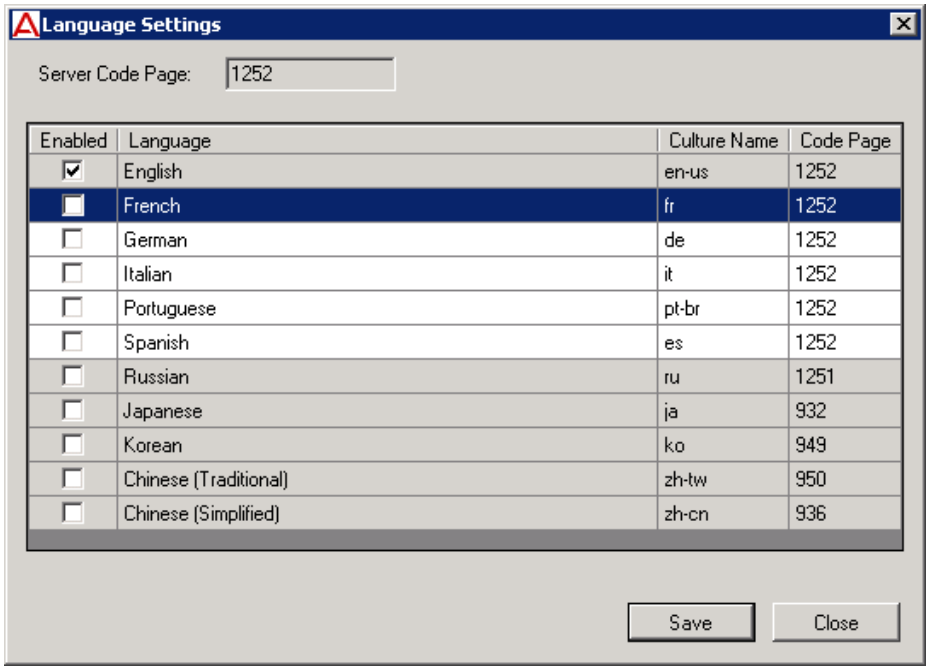
Log on to Contact Center Manager Administration to access the application and administer the contact center.

Enabling languages

The customer can no longer decide if a language should be installed, the CCMA Configuration utility Language Settings should be used to enable a language.
The Language Settings utility is accessed from the CCMA Configuration screen.



Once the Service Pack including languages is installed, all localized languages will appear in the CCMA Language Settings application. Only languages matching the current server code page can be enabled, others are disabled. English is always enabled and cannot be disabled
The utility supports multiple row selection and space bar toggling of enabled checkbox. To quickly enable or disable all supported languages, press [Ctrl] + A, then press space bar.



Note: If server code page changes, previously enabled languages can still be changed. User should disable the languages not supported. CCMA will only use languages if code page matches.

Procedure steps

Note:
To launch CCMA in a local language (French for example):

- Install the Service Pack on the CCMA server and enable French language as described in section 5.1.
- From a French client PC, start Internet Explorer to connect to the CCMA server.

If you wish to launch CCMA in a local language (French for example) BUT THE CLIENT OPERATING SYSTEM IS ENGLISH,

- Install the Service Pack on the CCMA server.
- From a English client PC, change the browser language to French in the internet options, using the following steps.

1. Launch Internet Explorer.
2. In Internet Explorer, click Tools →Internet Options.
   Result: The Internet Options window appears.
3. Click **Languages**.
   Result: The Language Preferences window appears.
   Verify that the language you want to use appears in the Language box. E.g. French [France] [fr],
4. If the language does not appear in the box, then you must add it as follows:
   a. Click **Add**.
   Result: The Add Language window appears.

b. From the list of languages, click the appropriate language, and then click **OK**.
Result: The language now appears in the Language Preferences window.
c. Proceed with the next step to move the language to the top of the box.

5. If the language you want to use appears in the box, then you must move it to the top of the list as follows:
   a. In the Language box, click the appropriate language.
   b. Click **Move Up** until the language appears at the top of the box.
   c. Click **OK** to close the Language Preferences window.
6. Click **OK** to close the Internet Options window.
7. In the Address box, type the URL of the Contact Center Manager Administration server. The default URL is https://<server name>:81, where <server name> is the computer name of the Contact Center Manager Administration server.
   Attention: Do not type the IP address in the Address box. Using the IP address results in problems with Scripting, Historical Reporting, Configuration, Contact Center Management, and Access and Partition Management.
8. In the **User ID** box, type your user ID.
9. In the **Password** box, type your password.
10. Click **Login**.

Start Localized AAD Client

Pre-installation steps

Information on how to start AAD (Only when a language patch installed)
NOTE:
To start AAD in a local language (French for example);

- From a French client PC, start AAD.

If you wish to launch CCMM in a local language (French for example) BUT THE CLIENT OPERATING SYSTEM IS ENGLISH,

- Change the default language in the regional language options to French.

Make sure that no Agent Desktop Client is installed on the desktop and the .Net cache is clear after uninstalling previous versions of Agent Desktop Client. See below, “Emptying the .Net cache on the client PC running AAD and OCMT,” for steps to clear the .Net cache. Procedures such as uninstalling application and flushing out the .Net cache require administrator rights.

Installing the Agent Desktop Client

Install the Agent Desktop if you are launching the application for the first time or if you are launching the application following installation of an upgrade or a patch.

Prerequisites

- Ensure that the administrator has configured your Windows User ID in CCT and that you have a valid User ID, Password, and Domain for use with Contact Center Agent Desktop.

Procedure steps

1. In Windows Explorer or Internet Explorer, enter the HTTP address (URL). The correct URL format is **https://**<Contact Center Multimedia servername>/agentdesktop/LANGUAGE CODE*
   Using French as an example, the URL is https://ccmmservername/agentdesktop/fr
   If using English, URL is **https://**<Contact Center Multimedia servername>/agentdesktop.
2. Click Launch AAD.

3. Click Install.

Starting the Agent Desktop Client

Start the Agent Desktop when you are ready to view the application.

- Ensure that you install Avaya Agent Desktop.
- Ensure that the administrator configures your Windows User ID in CCT and that you have a valid User ID, Password, and Domain for use with Contact Center Agent Desktop.

Procedure steps

1. In Windows Explorer or Internet Explorer, enter the HTTP address (URL). The correct URL format is **https://**<Contact Center Multimedia servername>/agentdesktop/LANGUAGE CODE*
   Using French as an example, the URL is https://ccmmservername/agentdesktop/fr
   If using English, URL is **https://**<Contact Center Multimedia servername>/agentdesktop.
2. Click Launch AAD on the web page.
   or
   Click Windows Start, All Programs, Avaya, Avaya Aura Agent Desktop.
   The Agent Desktop toolbar appears. If a CCT Connection Failure message appears, your Windows User ID is not configured on CCT. Click Retry to enter valid User Credentials or click Cancel to exit the application.

   * Applicable LANGUAGE CODEs to be used are:

- French = fr
- German = de
- LA Spanish = es
- Simplified Chinese = zh-cn
- Brazilian Portuguese = pt-br
- Russian = ru
- Italian = it

Start OCMT Client

Pre-installation steps

Information on how to start OCMT (Only when a language patch installed)
NOTE:
To launch CCMM in a local language (French for example);

- Install the French language patch on the CCMM server.
- From a French client PC, launch OCMT.

If you wish to start OCMT in a local language (French for example) BUT THE CLIENT OPERATING SYSTEM IS ENGLISH,

- Install the French language patch on the CCMM server.
- Change the default language, in the regional language options, to French.

Make sure that no OCMT Client is installed on the desktop and the .Net cache is clear after uninstalling previous versions of OCMT Client. See section, “Emptying the .Net cache on the client PC running AAD and OCMT,” for steps to clear the .Net cache. Procedures such as uninstalling application and emptying the .Net cache require administrator rights.

Logging on to the Outbound Campaign Management Tool

Log on to the Outbound Campaign Management Tool in the Contact Center Manager Administration application to open the application to configure, monitor, and maintain an outbound contact campaign.

Prerequisites

- Ensure that your contact center is licensed for outbound campaigns.
- Ensure that you have a Contact Center Manager Administration user name and password.

Procedure steps

1. Log on to Contact Center Manager Administration.
2. On the Launchpad, click Outbound.
3. In the left pane, select a Contact Center Multimedia server.
   The translated Outbound Campaign Management Tool window appears.

Detecting latest Language files

In case that client runs the English AAD and OCMT applications and does not pick up the language files. The client has previously launched English-only AAD and OCMT applications from the server and these files are now stored in the GAC (.Net cache) on the client PC. The .Net cache (GAC) therefore, needs to be emptied on the client PC so the latest English and language files can be taken from the server.

Note: If you install an updated Service pack or Design patch, the client still runs applications with cached language files. The .Net cache (GAC) must be emptied, so the latest language files can be taken from the server.

Emptying the .Net cache on the client PC running AAD and OCMT

Procedures such as uninstalling application and emptying the .Net cache require administrator rights.

1. Close AAD and OCMT.
2. Click Add/Remove Programs.
3. Remove Avaya/Avaya Agent Desktop.
4. Navigate to *C:\Documents and Setting\USERNAME\local settings\apps* .
5. Delete the 2.0 folder.
6. *Note:* This folder may be hidden. If so, open Windows Explorer and click on Tools, Folder options. Choose the View tab. Under Files and folders or Hidden files and folders, choose to show hidden files and folders. Click Apply and click OK.
7. Start AAD to download the latest AAD files from the CCMM server.
8. Start OCMT from CCMA to download the latest OCMT files from the CCMM server.

Comments on Translations

French

Translation of the software attempts to find terms that are acceptable to both Canadian and European French speakers. Some translations are different from the terms usually used in your region.

German

No special comments.

Latin American Spanish

Translation of the Software attempts to find terms that will be acceptable to both Latin American and European Spanish speakers. This may result in some translations being different from the terms usually used in your region.

Simplified Chinese

No special comments.

Brazilian Portuguese

No special comments.

Russian

No special comments.

Italian

No special comments.

KNOWN ISSUES

Hardware Appliance

None

Software Appliance

None

Application\Features

Remote desktop connection fails due to service stuck in starting

Tracking Number	CC-2435
Application	Windows Server 2012 R2
Description	Under certain error conditions, i.e. misconfiguration, some AACC services will not complete startup. While in this error state remote desktop connection logins and local console logins can fail with a “please wait” message.
Impact	Inability to login through RDC of local console to AACC server.
Workaround	If this error condition is experienced a connection to the console should be attempted. In the case of a physical sever deployment this would be the physical keyboard and monitor connection to the server. In the case of virtualized environments the equivalent to the physical console should be used. If a connection is successful on the console the service which is stuck in starting should be identified and normal trouble shooting performed to determine why the service is not completing startup. If the connection to the console is not successful a power cycle of the server will be required. A connection should be attempted, either through the console or through RDC, as soon as possible after the power cycle is performed.
Solution	This issue is resolved by applying the following Microsoft fix (KB3100956) mentioned in the Microsoft Operating System Updates section.

Agent Greeting not working on AACC due to Apache Tomcat 8081 port conflict

Tracking Number	CC-9938
Application	Agent Greeting and CCT Console
Description	Installing Avaya Aura Contact Center installs Apache Tomcat Server. The default port number for Apache Tomcat is 8081. If you need to change the port number to avoid conflicts with third-party software, see your Apache Tomcat documentation. If the Tomcat port is changed then refer to section: “**Adding Communication Control Toolkit to CCMA**” in the commissioning guide to change the CCT Console port used. **McAfee Agent Common Services** (macmnsvc.exe) or **McAfee Framework Service** (FrameworkService.exe) are the services that can use port 8081. If these services are required, then the Apache Tomcat port must be changed. Refer to If these services are not required then they can be stopped and

	configured not to run on startup in Windows Services.
Impact	If a conflict occurs, then both AACC **Agent Greeting** and **CCT Console** will be impacted. McAfee Anti-Virus could potentially be one of the third party applications that conflicts with port 8081.
Workaround	If you need to change the port number to avoid conflicts with third-party software, see your Apache Tomcat documentation. If the Tomcat port is changed then refer to section: "**Adding Communication Control Toolkit to CCMA**" in the commissioning guide to change the CCT Console port used.

Some fields are not aligned when Agent Performance report exported to .pdf file,

Tracking Number	CC-3856
Application	Contact Center Manager Administration
Description	AACC7.0 HR- Export Agent Performance report to .pdf file, some fields are not aligned
Impact	A number of reports within AACC are larger than a standard A4 page and as a result appear misaligned when exported to pdf. They also span pages when printed.
Workaround	None

Report Creation Wizard – Some sample reports do not work

Tracking Number	CC-5035
Application	Contact Center Manager Administration
Description	The following sample reports do not work in this release: BillingByAddress SkillsetOutboundDetails Voice Skillset Name ID Mapping Network Consolidated Skillset Performance ICPCSRSample MMCSRStat
Impact	These samples cannot be used as a starting point for new reports
Workaround	None

Report Creation Wizard – Column headers do not repeat on every page

Tracking Number	CC-4854
Application	Contact Center Manager Administration
Description	Column headers do not repeat on new page unless the first row of data is the start of a group.
Impact	Column headers may be missing from pages.
Workaround	None

Unable to login to CCMA using System Manager with TLS 1.1 or TLS 1.2 enabled

Tracking Number	CC-9923
Application	Contact Center Manager Administration
Description	Unable to login to CCMA using System Manager 7.0 or earlier when TLS 1.1 or TLS 1.2 is enabled. System Manager 7.0 and earlier versions do not support TLS 1.1 or 1.2
Impact	Unable to login to CCMA
Workaround	1. System Manager 7.0.1 supports TLS 1.1 and TLS 1.2

Unable to login to CCMA Configuration Tool when Security is enabled using System Manager

Tracking Number	CC-10124
Application	Contact Center Manager Administration
Description	Login to the CCMA Configuration Tool fails when the CCMA Security Settings are configured and enabled to use System Manager
Impact	Unable to use CCMA Configuration Tool under these circumstances
Workaround	1. Disable CCMA Security temporarily using the Manager Administration Security Settings snap-in 2. Use CCMA Configuration Tool as normal 3. Enable CCMA Security using the Manager Administration Security Settings snap-in

CCMA- Run time error displays during schema upgrade for NES 6 database migration

Tracking Number	CC-11429
Application	Contact Center Manager Administration
Description	While running the CCMA System Upgrade Utility, a run-time error may appear as follows: “Run-time error ‘-2147016656 (80072030). There is no such object on the server.” This error can be ignored and the migration will continue successfully to completion
Impact	There is no impact. This error can be ignored and the migration will continue successfully to completion
Workaround	No workaround required. This error can be ignored and the migration will continue successfully to completion

A CCMA standard user is unable to import a report

Tracking Number	CC-11537
Application	Contact Center Manager Administration
Description	A CCMA standard user (i.e. a non-administrator user) is unable to import a customized report from the Historical Reporting component. When the user selects the Import option in Historical Reporting they are instead presented with the CCMA Login screen
Impact	Non Administrator CCMA users are unable to import reports into the CCMA Historical Reporting component
Workaround	1. Login to CCMA as an Administrator user 2. Go to the Access and Partition Management component 3. Edit the details of the user who is unable to import reports. 4. Under the *Launchpad Options* section tick the *Contact Center Management* checkbox 5. Click Submit 6. If the user is currently logged in to CCMA then they will need to logout and then log back in again in order for the changes to be applied

A CCMA standard user is unable to save an imported report in Historical Reporting

Tracking Number	CC-11546
Application	Contact Center Manager Administration
Description	A CCMA standard user (i.e. a non-administrator user) is unable to save a scheduled report that has been imported to the Historical Reporting component. This is applicable only to reports that have been imported by a CCMA standard user and are scheduled
Impact	Non Administrator CCMA users cannot save user imported reports that are scheduled
Workaround	1. If the report is a public report i.e. the user saved it to a public Report Group then the workaround is for an administrator user to make the required modification and save the report. The user can then run the report as normal or it will run as scheduled 2. If the report is a private report i.e. the user saved it to their Private reports group then there is no workaround as admin users do not have access to users private reports

CCMA private HR reports and private Realtime displays are not migrated to 7.0.1 from AML NES 6 database

Tracking Number	CC-11504
Application	Contact Center Manager Administration
Description	When migrating from an AML NES 6 system to AACC 7.0.1 then users private historical reports and private realtime displays are not migrated
Impact	Users private historical reports and private realtime displays are not migrated
Workaround	Before performing the migration add the user *iceAdmin* to the Administrators group as follows 1. Launch the *Computer Management* application 2. Under *Local Users and Groups* click on the *Groups* node 3. Locate the *Administrator* group and view its properties 4. Add the user *iceAdmin* to this group 5. Perform the migration 6. Once the migration has completed then remove the *iceAdmin* user from the Administrator group

Installing CCMS Patch on a very large database can take 20+ minutes

Tracking Number	CC-5140
Application	Contact Center Manager Server
Description	Installing a CCMS database patch on very large databases can take 20+ minutes. This is due to re-indexing of the CCMS database tables with volume of data in the order of few million rows.
Impact	Longer CCMS patch install time.
Workaround	None

Enterprise Web Chat – Sessions closed while sending messages may not close

Tracking Number	CC-8344
Application	Tomcat & Enterprise Web Chat
Description	When a WebSocket connection is closed while the Agent Controller or Customer Controller is processing a message, the controller may not be notified that the connection has been closed. This issue could be seen if the customer application OR agent application (Custom Desktop) terminates unexpectedly, immediately after an 'agent Login' request OR 'Queue Status' request is sent. Other requests are less likely to produce this issue.
Impact	The Agent Controller / Customer Controller will not detect that the session has closed. An affected agent may not be able to login until Tomcat is restarted. There is a small memory leak associated with this issue.
Workaround	None

Enterprise Web Chat – HA: Agent can type and send messages for a brief window at start of a manual switchover of CCMM

Tracking Number	CC-8334
Application	Agent Desktop Reference Client & High Availability
Description	When performing a manual switchover on the Multimedia AACC server, there is a 20 second window in which the Agent can continue to type and attempt to send messages. When the Agent tries to send the message, a dialog box is displayed stating; "500 - Internal server error".
Impact	This does not have an effect on the overall chat. Once the switchover is complete the chat can continue as normal.
Workaround	None

Avaya Agent Desktop Embedded browser not rendering page correctly

Tracking Number	CC-11331
Application	Avaya Agent Desktop
Description	On the first launch of AAD after install/update to 7.0.1 the embedded browser in AAD for screen pops can default to IE7 instead of the latest version of IE installed on the client.
Impact	Screen pop page may render incorrectly.
Workaround	Restart Avaya Agent Desktop

Agent Controls Browser Application – Online help not available when using Chrome browser

Tracking Number	CC-9849
Application	Agent Controls Browser Application
Description	Online help feature is not working when using Chrome browser.
Impact	Online documentation not available with this browser type.
Workaround	Online help may be accessed using another browser.

AAMS Configuration of RSS and SHOUTcast not preserved during AACC 7.0 to 7.0.1 upgrade

Tracking Number	CC-9854
Application	Contact Center Music Treatments
Description	AAMS version used in AACC 7.0.1 (7.7.0.348 or later) has enhanced its Music Streaming feature. This has resulted in a different procedure for configuring AMS for RSS or SHOUTcast streaming.
Impact	All Music treatment using RSS or SHOUTcast will not be operational.
Workaround	Before updating, note down the current RSS / SHOUTcast settings. After the upgrade go to **EM->System Configuration->Media Processing->Music->Stream Provisioning** and add the RSS/SHOUTcast configuration.

CCT services keep restarting if no resources configured on CS1k platform

Tracking Number	CC-11144
Application	Communication Control Toolkit
Description	In CS1K voice only deployments which do not use CCT clients, AAAD or custom CCT clients, it is possible to not have any CCT terminals configured. This leads to a scenario where some CCT services will restart continually, these being ACDPROXYService and NCCT TAPI Connector Service.
Impact	Some CCT services will restart continually, these being ACDPROXYService and NCCT TAPI Connector Service. AACC server operation may become negatively impacted if the services are allowed to keep restarting. It is therefore recommended to make the configuration changes outlined below as soon as possible.
Workaround	To avoid the CCT services from continually restarting it is necessary to have at least one CCT terminal configured. To avoid warnings being logged a valid address should also be created and mapped to the terminal.

	Ensure CCT has been started as the NCCTDALS service is required for configuration. Following the steps documented in "Avaya Aura® Contact Center Client Administration": 1. section "Adding an address" to add a valid address 2. section "Adding a terminal" to add a valid terminal. 3. While creating the new terminal a mapping to the address/addresses created in the first step should be added. This is done by using the "Address assignments" section of the “Update Terminal” screen. The "Update Terminal" screen is available when creating or editing a terminal. When the address and terminal, with address terminal mappings, has been successfully saved a restart of CCT is required. The restart should be performed as follows: 1. Using SCMU "Shut down CCT" button 2. Wait for all of the services to successfully stop 3. Using SCMU "Start CCT" button 4. All of the CCT service should now start successfully and stay running.

Supervisor cannot invoke whisper to agent1 after agent1 completes CDN - DN conference with agent2

Tracking Number	CC-11394
Application	SIP Gateway Manager (SGM)
Description	If the supervisor invokes observe and whisper after the CDN to DN conference is completed, he is not able to invoke whisper. The user experience is that when whisper button is pressed, an error message is displayed saying “Whisper failed: Feature error, Can’t coach as call type not supported”. There is no other breakage or impact.
Impact	Whisper functionality for that particular agent
Workaround	There is no workaround. Issue however is not seen if the observe and whisper is invoked before the CDN-to-DN conference is completed. Also issue is not seen for CDN-to-CDN conference whether the whisper feature is invoked before or after the conference is completed.

CCCC patch install failure due to locked database

Tracking Number	CC-11375
Application	Common Component Database
Description	CCCC patch failing to install and cache console.log reporting that “Database

	is locked by another instance.
Impact	CCCC patch cannot be installer
Workaround	To allow the patch to install perform following steps: 1. Stop Cache 2. Delete the file: d:\avaya\cache\cachesys\mgr\cachelib\cache.lck 3. Start Cache 4. Run install again

Localization issues

Internationalization issues or common across all languages and require a base fix

The installation UI is in English instead of localized version

Tracking Number	CC-6323
Application	Avaya Agent Desktop
Description	Steps to reproduce: 1. Open AAAD installer link: https://aacc70zt.prgloc.avaya.com/agentdesktop/zh-tw/ 2. Click on Launch > Check the installation window Expected result: Installer is Traditional Chinese Actual Result: Installer in English
Impact	Agent may not understand installation.
Workaround	Agent needs to install application using English installation wizard.

APPENDIX

Appendix A – Issues Addressed in this release

This section of the release notes provides information on customer issues that have been addressed in this Feature Pack.

CCMS, CCSU, CCCC and CCLM Defect Listing

This list contains defects addressed for the Manager Server, Common Components and License Manager Components

WI/JIRA	Summary
CC-6189	Not Ready times differ from one report to another for same time period/interval
CC-6210	Change NCC OAM Sync Site call timeout from 30 seconds to five minutes
CC-6228	TFE fires Windows event 48458 when agent goes on hold following completion of conference.
CC-6230	Terminal port addresses from 100.x.x.x not set to null during aml to sip migration
CC-6246	Answer Delay Time not pegged correctly
CC-6354	AACC SP15: Network MCHA start-up prevents ASM from accessing all available nodes
CC-6384	Changing HA mode deletes RGN configuration
CC-6420	AACC 6.4 SP15: Abandoned calls not showing in Crosstab Skillset report
CC-6555	AACC 6.4 SP15 - SCMU Crashed
CC-6564	Multimedia offline database is included Backup Database List
CC-7286	Phantom call hung in Standard App display after SIP Call Join
CC-7340	GIVE IVR Combining Messages not working
CC-7455	AACC is unexpectedly receiving the expired UCID during call join
CC-7603	Standby server OAM Termination
CC-7774	FirstEventTimestamp in CBC populated with value of previous instance of callid
CC-7821	Misspelling in the NCCT error event log
CC-8047	EWT doesn't calculate as expected before queue to skillset
CC-8053	The call Abandoned Data does not match on RTD & Cross Tab report
CC-8057	CCMM backup Move Older Backup Folders Files Does Not Include OFFLINE Folder
CC-8059	nicmfjvm termination
CC-8103	SP15 - TFE Termination following script changes
CC-8142	Webstats contains extra file with cross-domain scripting vulnerability
CC-8155	SMMC Service Termination
CC-8165	ASM - Voice and emails are not routing to agents
CC-8453	ASM Service Termination
CC-8996	AACC 7.0 DTMF fails on upgrade due to notypeahead = false as default
CC-9049	NCCT Server service terminated unexpectedly on HA standby co-resident AACC server.
CC-9435	AACC CCMS Code Cache DB growing
CC-9442	After switchover, RTDs do not correctly display currently queued contacts
CC-9716	call routed to two agents after rtq scenario
CC-9830	Misspelling in CMF_OAM log

CC-9839	CCT client looses control of call from external number after conference
CC-10066	OAM Termination on passing 10240 bytes of data
CC-10067	OAM delay in processing sync
CC-10128	AACC 6.4 SP16: Metrics files being generated constantly
CC-10149	HDM not processing data
CC-10243	Historical statistics consolidation fails
CC-10288	AAAD losed Intrinsics Data if Call was waiting longer then 10 Minutes in Queue
CC-10414	RTDs not matching AAAD search for contacts waiting
CC-10521	Voice and emails were not routing to the agents after CCMS switch over for few minutes
CC-10642	AACC 6.4 SP15/16: DN talk Time incorrect after patch install
CC-10654	AACC 6.4 SP16: Call not releasing on RTD and Agent stuck, not receiving any calls
CC-10657	OAM service in starting state in standby AACC server
CC-10678	AACC 6.4 Ringback tone heard during conference
CC-10715	HDX variable length too long causing crash of TFA and TFE
CC-10716	Not Ready time is not pegging correctly in iAgentPerformanceStat table when agent supervisor is changed
CC-10973	AACC 7.0 SP1: Same call presented to 2 agents
CC-11131	Agents are not getting calls, stuck in NRD in RTDs after network glitch
CC-6223	ACVT flagging agent URIs assigned to CDNs but such CDNs are deleted, also the database incorrectly generates event 64141 and 64140

CCMA Defect Listing

This list contains defects addressed for the Manager Administration components

WI/JIRA	Summary
CC-6779	Unable to login to CCMA after migrating the NES6 data
CC-7033	SCT not using LogoutToken method causes failure at subsequent login
CC-7344	Agent to skillset scheduled assignments generating runAssign error in App log
CC-8051	AACC 6.4 SP15: Skillset Crosstab missing intervals when contact count is zero
CC-8450	CCMA User Migration SnapIn should encode & characters
CC-8711	AACC 7.0 - Unable to import report from RCW as server is missing in CCMA
CC-8810	AACC 6.4 SP15: After switchover, calls presented to agents for old skillsets
CC-9112	error code -119 seen on Historical Reporting web page
CC-9123	ACCS 7.0 - Unable to change Real-time reporting default Public Graphical Displays
CC-9686	Add media buttons on CCMA prompt management are not visible on Internet Explorer 11 with SP16
CC-9992	ACCS 7.0: CCMA migration fails
CC-10245	7.0.1 AML HA- Unable to launch RCW imported into HR after switchover
CC-10297	AACC 6.4 SP15: Cannot add Activity Codes with Russian characters on a Russian OS
CC-10487	CCMA latency with large count of RTD hits from many RTD clients
CC-11093	Existing agent deleted while creating a copy of an agent in CCMA

CCT Defect Listing

This list contains defects addressed for the Communication Control Toolkit components of Avaya Aura® Contact Center Select.

WI/JIRA	Summary
CC-7821	Misspelling in the NCCT error event log
CC-9049	NCCT Server service terminated unexpectedly on HA standby co-resident AACC server.
CC-9839	CCT client looses control of call from external number after conference

CCMM/AAD Defect Listing

This list contains defects addressed for the Multimedia\Outbound Server and Avaya Agent Desktop components

WI/JIRA	Summary
CC-11841	Unable to pull contacts in any language other than English
CC-11741	Email buttons truncated on PT-BR L10N AAD
CC-3647	POM calls pegged as DN In and Busy
CC-6345	AAAD_Call Log_There is 1 missed call in call log window of agent 2 after agent1 blind conference or blind transfer the call to agent2
CC-7075	AAAD shows wrong email ID on POM contact
CC-7195	code for the view vw_campaignContacts selects from the wrong fields
CC-7565	Outbound Campaign Scheduler not processing campaign at Campaign Start time causes no OB contacts to queue
CC-8913	AACC Outbound - Transferred call leg shows in outbound report
CC-9867	POM Agent showing IDLE in RTD after logging out
CC-9905	OCMT fails to export campaigns
CC-10044	AACC7 Default email analyzer not working with simplified Chinese keyword
CC-10264	OCMT not updating existing customers with second items
CC-10843	GetUsersBySkillsetId returns the incorrect result since the change to improve skillset assignment performance

Install Defect Listing

This list contains Installation defects addressed for in this release

WI/JIRA	Summary
CC-10950	ACCS 7.0.0.1 Dashboard shows a mismatch between current and expected patch versions

CCMA ActiveX Control MSI – Content and Versions

File Name	File Size (bytes)	Version
ChartWrapperCtrl.ocx	64312	1.0.0.1
DTPWrapperCtrl.ocx	97080	8.0.0.0
hrctrl.dll	113464	8.0.0.4
iceemhlpcontrol.dll	129848	8.0.0.2
icertdcontrol.dll	854840	9.0.0.2
iemenu.ocx	65648	4.71.115.0
ntzlib.dll	65080	1.1.4.0
olch2x8.ocx	2102448	8.0.20051.51
rope.dll	248632	1.0.0.4
rsclientprint.dll	594432	2011.110.3128.0
sstree.ocx	337120	1.0.4.20
WSEColorText.ocx	179000	6.0.0.15
xerces-c_2_7.dll	1893832	12.5.0.1190

Appendix B – Avaya Media server 7.x Migrations To 7.7

This section details all of the procedures required to migrate an AAMS used in AACC 6.x to the AAMS version used in AACC 7.0.1.

AMS (7.5 and 7.6) Upgrade and Migrations to AAMS 7.7

This section details all of the procedures required to upgrade or migrate previous version of Avaya Media Server to Avaya Aura Media Server 7.7.

Note: AMS refers to Avaya Media Server versions 7.5 and 7.6 used by AACC 6.3 and 6.4. AAMS refers to Avaya Aura Media Server 7.7 used by AACC 7.0 and AACC 7.0.1.

AMS to AAMS Upgrades

The only AMS to AAMS in-place upgrade that is supported is an upgrade from an AMS 7.6 server that has been installed on a customer-supplied Red Hat Enterprise Linux (RHEL) 6.x 64bit server. In place upgrades are not supported and migration procedure must be used if your AMS is:

- Installed on Windows Server 2008 R2
- Installed on RHEL 5.x
- Installed on RHEL 6.x 32bit
- Deployed from the AMS7.6 OVA supplied with AACC 6.4

Scripts for Migrations and Upgrades

Two scripts are provided for use in preparing and completion of AMS to AAMS server migrations:

- prepareForAAMS77Migration.py (Linux) / prepareForAAMS77Migration.exe (Windows)
- completeAAMS77Migration.py (Linux) / completeAAMS77Migration.py (Windows)

The scripts are available on the DVD at location: /Install Software/AMS/Linux and /Install Software/AMS/Windows. Note: the Service pack or patch bundle may have a more recent version of these scripts.

The following procedure details how to copy and run these scripts on RHEL servers.

1. Launch ssh session to RHEL server, logon as root user and create a directory:
   mkdir /tmp/AvayaMS

2. Copy the script using a file transfer utility (e.g. WinSCP) to the RHEL server. Make sure that the script is transferred in “Text mode”.
3. Make script executable by running command: (example prepareForAAMS77migration.py):
   cd /tmp/AvayaMS
   chmod +x prepareForAAMS77Migration.py

4. Run the script by running command (example shows prepareForAAMS77migration.py):
   ./prepareForAAMS77Migration.py

Upgrading AMS 7.6 to AAMS 7.7 in-place on RHEL 6.x 64bit

This section details the procedure required to complete an in-place upgrade of an AMS 7.6 on RHEL 6.x 64bit OS to AAMS 7.7.

1. Copy and run the ***prepareForAAMS77Migration.py*** script to the AMS 7.6 RHEL server using procedure: Scripts for Migrations and Upgrades
2. At the "**Please Enter ACC SIP Domain"** prompt, enter the AACC SIP domain name.
3. Uninstall CCSA by running commands:
   cd /opt/avaya
   ./UninstallCCSA
4. At the **"Also remove Avaya Media Server"** prompt, answer '**n'**. Do not uninstall AMS software.
5. Locate the AAMS 7.7 Linux binary on the AACC 7.0.1 DVD: ***MediaServer_7.7.0.359_2016.07.20.bin***
6. Copy this binary to the /tmp/AvayaMS directory on the RHEL server using WinSCP or equivalent. Make sure transfer is in Binary mode.
7. Run the binary by running commands:
   cd /tmp/AvayaMS
   ./MediaServer_7.7.0.359_2016.07.20.bin
8. At the **Upgrade** prompt, press Enter to accept the default selection.
9. Answer **y** to the License agreement and press Enter at the next **Upgrade** prompt.
   The software upgrades to AAMS 7.7.0.359
10. Copy and run utility: ***completeAAMS77Migration.py*** to the RHEL server using procedure: Scripts for Migrations and Upgrades
    The upgrade is complete and the AAMS Content Store now has the required content for AACC 7.0.1 operation.

AMS 7.5 or 7.6 Migrations to AAMS 7.7

AAMS 7.7 migration from previous AMS releases only supports migrations of the "**Application Content**" of the AMS database. It does not support "**System Configuration**". Application Content refers to the Content Store contents of the AMS server. This includes all announcements and music.

AAMS 7.7 supports the following Application Content migrations:

- AMS 7.5 or 7.6 installed on RHEL 5.x or 6.x to AAMS 7.7 installed on RHEL 6.x 64bit OS (including AAMS 7.7 OVA).
- AMS 7.5 or 7.6 installed on Windows Server 2008 R2 to AAMS 7.7 installed on Windows Server 2012 R2.
- AMS 7.5 or 7.6 installed on Windows Server 2008 R2 to AAMS 7.7 installed on RHEL 6.x 64bit OS (including AAMS 7.7 OVA).
- AACC 6.4 AMS 7.6 OVA to AMS 7.7 OVA
- AACC 6.4 AMS 7.6 OVA to AMS 7.7 installed on RHEL 6.x 64bit OS (including AAMS 7.7 OVA).

The following procedure should be used for all migrations:

1. Locate and run script: prepareForAAMS77Migration.py (or .exe for windows) on the AMS 7.5 or AMS 7.6 RHEL or Windows Server 2008 R2.
2. On AMS Element Manager go to section: **Tools>>Backup and Restore>>Backup Tasks** and click **Add**.
3. Enter a name for this backup task.
4. Select "**Application Content**".
5. Clear "**System Configuration**".

6. Select "**Manually as needed"** and click "**Save**".
7. In the Backup Tasks window, select the task and click "**Run Now**"
8. The **History Log** window appears. Wait until you see confirmation that backup task has completed.
9. The Content Store will be backed up to a zip file at location:
   Windows: *%MASHOME%platdata\EAM\Backups*
   Linux: *$MASHOME/platdata/EAM/Backups*
10. Copy this zip file to the new AAMS 7.7 server.
11. Open a terminal session (ssh for Linux and cmd prompt for windows) and run the following command (shown with example filename) to migrate the Content Store data to the AAMS 7.7 server:
    amsupgrade taskname_hostname__2015_11_26_8_41_48.zip
12. On AAMS Element Manager, go to section: **Tools>>Media Management** and verify that a **streamsource** namespace exists with the music content groups and the **SIP domain** namespace exists with the locale, tones, prompts and music content groups.
13. Copy the ***completeAAMS77Migration (.py or .exe)*** to the AAMS 7.7 server and run this script. This script simply deletes any duplicate music content groups from the SIP domain namespace if they are already under the **streamsource** namespace.
14. Add this AAMS to CCMA Media Servers and services. If this AAMS is the Master Content Store, then tick this box in the Media Servers page. This will push down any default media files to the AAMS Content Store that are missing from the migration.
15. Carry out Post-Installation Configuration on AAMS 7.7 server.

Avaya Aura Media Server Clustering

Avaya Aura Media Server supports two types of clustering:

- Standard AAMS cluster (N+1 Cluster)
- High Availability AAMS Cluster Pair

These two cluster types are different configurations and cannot be combined.

Content Store Replication can be configured between clusters of the same type by selecting a Primary AMS server as the “Master Cluster Primary” and then configuring this IP Address into the “**Master Cluster Primary Node Address**” in Element Manager in Cluster Configuration >> Replication Settings.

Standard AAMS Cluster

A standard N+1 AAMS Cluster is a collection of up to eight AAMS servers. AACC will carry out Round Robin load balancing between all the AAMS servers in the cluster. Each AAMS server’s IP Address in the cluster must be added to the Media Servers List and associated with the ACC_APP_ID service in CCMA.
The Standard AAMS cluster must consist of a Primary and Secondary AAMS Server. Optionally up to six Standard AAMS servers can be added to the cluster. In an AACC environment, the only benefit of configuring this Cluster type over using stand-alone AAMS servers with Content Store Replication is that you also get Configuration replication.

High Availability AAMS Cluster Pair

A High Availability AAMS cluster is a collection of two AAMS servers consisting of a Red Hat Linux Primary and Backup AAMS server. This configuration provides uninterrupted availability of media processing in cases where a media server fails (also known as “Active Call Protection”). The HA cluster has a Service (Managed) IP Address that is entered into Media Servers List and associated with the ACC_APP_ID service in CCMA. An AAMS HA cluster must not span a geographical location. Both Primary and Backup AAMS in a HA Cluster pair must be on the same local network.

Appendix C – Additional Security Information

Store Maintenance – backup and restore

Backing up the Certificate Store

1) Ensure all services are stopped
2) Launch Certificate Manager
3) Go to Store Maintenance Tab
4) In the Backup and Restore Certificate Store section choose a location in which to create the backups. **NOTE:** do not choose a Contact Center directory structure
5) Press the Backup button to back up the store and its associated files
6) Check your chosen backup location and verify the following files are present in the directory: CCKeyStore.jks, signme.csr (optional), storeInformation.txt ,storePwdEncrypt.txt

Restoring the Certificate Store

1) Ensure all service are stopped
2) Launch Certificate Manager
3) Go to Store Maintenance Tab
4) Select the location where your backups are stored, in the Backup and Restore Certificate Store section
5) Press Restore button to restore the store and associated files
6) Close Certificate Manager
7) Open Certificate Manager and confirm store has the correct content
8) Start Services

After restoring Certificate Store – Reset Security Level if previously set to ON

If the certificate store has been restored onto a system that contained another store and had the security level set to ON then the following steps have to be followed to apply the new stores certificates to the various web servers otherwise the previous stores certificates will remain in effect.

This procedure is only if the previous security setting was set to ON while using the previous store and the store has been restored.

1) Ensure all services are stopped.
2) Launch Certificate Manager.
3) Go to Security Configuration Tab.
4) Check Security level – If ON then turn OFF and then ON again.
5) Hit Apply button.

This effectively will remove the previous configuration settings on the various web servers and apply the contents of the new store to web servers.

Failure to follow this step will result in the various web servers using the certificates from the previous store regardless of the restore procedure.

Restoring a certificate store whose contents have been signed by another Certificate Authority

If the certificate store has been restored to a system that used another certificate authority (CA) to sign the contents of the store used previously then, if not done already, the root certificate authority certificate will have to be deployed to the various clients that communicate with the server.

If the restored certificate store has been signed by the same certificate authority then this is not required since the root CA certificates should have already been distributed.

Backing up the Certificate Store

1) Ensure all services are stopped
2) Launch Certificate Manager
3) Go to Store Maintenance Tab
4) In the Backup and Restore Certificate Store section choose a location in which to create the backups. **NOTE:** do not choose a Contact Center directory structure
5) Press the Backup button to back up the store and its associated files
6) Check your chosen backup location and verify the following files are present in the directory: CCKeyStore.jks, signme.csr (optional), storeInformation.txt ,storePwdEncrypt.txt

Restoring the Certificate Store

9) Ensure all service are stopped
10) Launch Certificate Manager
11) Go to Store Maintenance Tab
12) Select the location where your backups are stored, in the Backup and Restore Certificate Store section
13) Press Restore button to restore the store and associated files
14) Close Certificate Manager
15) Open Certificate Manager and confirm store has the correct content
16) Start Services

After restoring Certificate Store – Reset Security Level if previously set to ON

If the certificate store has been restored onto a system that contained another store and had the security level set to ON then the following steps have to be followed to apply the new stores certificates to the various web servers otherwise the previous stores certificates will remain in effect.

This procedure is only if the previous security setting was set to ON while using the previous store and the store has been restored.

1) Ensure all services are stopped.
2) Launch Certificate Manager.
3) Go to Security Configuration Tab.
4) Check Security level – If ON then turn OFF and then ON again.
5) Hit Apply button.

This effectively will remove the previous configuration settings on the various web servers and apply the contents of the new store to web servers.

Failure to follow this step will result in the various web servers using the certificates from the previous store regardless of the restore procedure.

Restoring a certificate store whose contents have been signed by another Certificate Authority

If the certificate store has been restored to a system that used another certificate authority (CA) to sign the contents of the store used previously then, if not done already, the root certificate authority certificate will have to be deployed to the various clients that communicate with the server.

If the restored certificate store has been signed by the same certificate authority then this is not required since the root CA certificates should have already been distributed.

TLS Information

Non-mandatory TLS SIP connections

Session Manager releases TLSv1 support

SM Release	TLS v1.0 support	TLS v1.1 support	TLS v1.2 support	Options
7.0.1	Yes	Yes	Yes	
7.1	No	No	Yes (Greenfield sites only)	Minimum TLS version in SM R7.1 will be inherited from the release upgrading from The 7.1 SM EM running on SMGR will set the network global default to TLS 1.2 if it sees no SMs administered in the DB

Avaya Aura Media Server releases and TLSv1 support

AAMS Release	TLS v1.0 support	TLS v1.1 support	TLS v1.2 support	Options
AAMS 7.7.1.1 FP1 SP1	No	No	Yes	Configurable (via Element Manager) TLSv1.0 or TLSv1.1 can be set instead if required

Known applications and services that cannot support TLS v1.2

HDX / DIW connection to databases

HDX / DIW can be used to connect to customer databases. HDX / DIW connect to a remote database using an ODBC Data Source Name (DSN). The DSN for the database connection must be manually created on AACC using the ODBC Data Source Administrator.

If connecting to older versions of Microsoft SQL Server, the DSN created will not connect successfully if TLS is set to higher than TLS v1.0. In this scenario, enable TLS v1.0 on Certificate Manager Security Configuration field "CCMA – Multimedia Web Service Level".

Remote desktop

Remote desktop connections can also be impacted on some client machines and requires a Microsoft KB required to remote into AACC server when TLS v1.1 or higher is set due to RDC only supporting TLS v1.0. Disabling TLS 1.0 on the CCMA- Multimedia web services setting in Certificate manager will break RDP under default settings on Windows 7 clients and Windows 2008 R2 Server.

This setting covers the entire AACC server and not only CCMA-MM WS and thus causes remote desktop connections to fail from Windows 7 and Windows 2008 R2 server due to the fact it cannot support TLS v1.1 or TLS v1.2.

Please apply the following KB from Microsoft on your CLIENT or machine wishing to connect to CC server.

This update provides support for Transport Layer Security (TLS) 1.1 and TLS 1.2 in Windows 7 Service Pack 1 (SP1) or Windows Server 2008 R2 SP1 for Remote Desktop Services (RDS).

https://support.microsoft.com/en-us/kb/3080079

System Manager 7.0

System Manager 7.0 and earlier releases do not support TLS 1.1 and TLS 1.2
If implementing a Single Sign-On configuration using System Manager to login to CCMA then if TLS 1.1 or TLS 1.2 is enabled the System Manager login page will not be presented.
System Manager 7.0.1 includes support for TLS 1.1 and TLS 1.2