Avaya Aura® Contact Center
Release 7.0.2.0

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	**Launch of Avaya Aura Contact Center 7.0.2.0**	Contact Center Release Engineering	**November 20, 2017**
2.0	**Release of Post-GA updates**	Contact Center Release Engineering	**January 12, 2018**
3.0	**Corrected information on Hot Patching support**	Contact Center Release Engineering	**February 28, 2018**
4.0	**Updated with .NET Framework Support.**	Contact Center Current Engineering	**May 22, 2018**
5.0	**Release of Post-GA updates**	Contact Center Current Engineering	**July 2, 2018**
6.0	**Updated JIRA listing**	Contact Center Current Engineering	**November 26, 2018**

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_7.7.0.391_A16_2017.04.13_OVF10.ova	c7a724654bb7c3419fd024290c5045f8

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-7.1.0.0.11-25605-e65-19.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_7.0.2.0-461.iso	9f0bdf43c7801cf81ecd01cbf05f5666

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_7.0.2.0_FeaturePack2-411.zip	14bbba54bbe923738ab8143159fc9f28

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_7.0.2.0_FeaturePack02ServicePack00_GA_Patches-349.zip	342b1b13742bb9c0323f19fbe67c2fe5
ACC_7.0.2.0_FeaturePack02ServicePack00_GA_Patches-325.zip	b556a1c300508e2658716ecb256f652d
ACC_7.0.2.0_FeaturePack02ServicePack00_GA_Patches-330.zip	c7be168269fb9a8ce02954a1e7dd8e32

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

Avaya Aura Media Server OVA

The AAMS OVA version is: 7.7.0.391 with System Layer Version 21. Both need to be upgraded to the latest version. The Media Server needs to be updated to 7.7.0.398 and the System layer needs to be updated to 23. This is accomplished by downloading the two ISO files:

MediaServer_Update_7.7.0.398_2017.05.09.iso
MediaServer_System_Update_7.7.0.23_2017.09.05.iso

The procedure: Upgrading Avaya Aura Media Server 7.0.2.0 OVA from 7.7.0.391 to 7.7.0.398 details the steps required to upgrade the AAMS OVA.

File Name	MD5 Checksum
MediaServer_Update_7.7.0.398_2017.05.09.iso	6d3380b86de275ccce4a357ff0192176
MediaServer_System_Update_7.7.0.23_2017.09.05.iso	137a7643dce281761b03f3d3b22073e1

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_2_0_SNMP_Trap_File_ver1_0.cnf	08a97caf629637aa7f9b4d9cd31beb8e

Patch Scanner

This Patch Scanner utility is released with every Release Pack and Patch bundle from ACCS 6.4 SP13 onwards. If you are moving from an Avaya Aura Contact Center 6.4 lineup to Avaya Contact Center Select 7.x you must use the version of the Patch Scanner published in the 7.x Release Notes document.

This version of the tool can be used prior to moving to Avaya Contact Center Select 7.x. See readme with the application zip file for further information.

File Name	MD5 Checksum
PatchScanner_1.0.0.24.zip	c2e7e7baf70f3f66ed8dbe78f6d883eb

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, 7.1
Avaya Aura Solution for Midsize Enterprise	6.2 FP4
Avaya Aura Communication Manager	6.2 FP4, 7.0, 7.0.1, 7.1
Avaya Aura Application Enablement Services	6.2 FP4, 7.0, 7.0.1, 7.1
Avaya Aura System Manager	6.2 FP4, 7.0, 7.0.1, 7.1
Avaya Aura Session Manager	6.2 FP4, 7.0, 7.0.1, 7.1
Avaya Aura Presence Services	6.2.6, 7.0.1, 7.1

Avaya Communication Server 1000

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

Avaya Aura® Contact Center 7.0.2.0 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 Security 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. From the *Tools* menu select the *Compatibility View settings* option and add the relevant website address to the list of websites

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

NOTE: If Avaya Agent Desktop (AAD) is used on a client desktop then individual websites for CCMA and Element Manager should be added to compatibility view. The "Display all websites in Compatibility View" setting in IE should not be used on these client.

The Avaya Agent Desktop (AAD) embedded browser defaults to IE 10 on clients with IE 10.0 or later.

Windows Server 2012 RDS Support

Windows Server 2012 R2 Remote Desktop Services (RDS) is supported from Avaya Aura© Contact Center Release 7.0.1.x. Further details available in "*Avaya Aura© Contact Center – Contact Center Select Windows Server 2012 Remote Desktop Services"* Application Note on support.avaya.com

Microsoft .NET Framework Support

With the introduction of AACC 7.0.2 contact center is no longer dependent on a specific version of .NET. AACC 7.0.2 supports .NET 4.6.2 through 4.7.x

VMware

VMware vSphere 6.5 support added for 7.0.2 release.

ESXi/vCenter 6.5 Limitations

Deploying OVA's to an ESXi 6.5 host using the desktop vSphere Client is not supported by VMware and the vSphere Web Client or Host Client must be used instead. It is recommended that you use vSphere Web Client (https://FQDN-or-IP-Address-of-VC/vsphere–client) when deploying new OVA's since there are known issues with the Host Client (https://FQDN-or-IP-Address-of-ESXi-host/UI).

The following issues exist when using the Host Client to deploy OVA:

 During deployment you are not prompted to select a profile. To work around this you will need to manually edit the VM Virtual Hardware settings before powering the VM on.

 Properties specified when deploying OVA are ignored and they must be re-entered during the first boot process. Drop-down lists are not provided and property defaults are not populated.

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, SP15 or SP16 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, SP15 or SP16 lineup.

Avaya Equinox 3.x is Not Supported for use as an Agent Softphone

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

Hot Patching Support

Hot patching is supported from Avaya Aura© Contact Center Release 7.0.1.x to this Avaya Aura© Contact Center Release 7.0.2.0

POM Support

AACC 7.0.2.0 supports POM 3.0.5 and POM 3.1. No prior version of POM is supported with AACC 7.0.2. If AACC site is operating with POM then site **must upgrade to POM 3.0.5 or POM 3.1 before upgrading to AACC 7.0.2.0 (7.0 Feature Pack 2)**.

Note: Experience Portal (EP) 7.1 SP1 requires POM 3.0.5. POM 3.1 requires EP 7.2.

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

Important: Direct upgrades from 7.0.0.0 and 7.0.0.1 to 7.0.2.0 are not supported. You must upgrade to 7.0.1.x first, before upgrading to 7.0.2.0

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.x software and must be used when upgrading to this software release.

The application will perform the following actions

1. remove all installed Product Updates (Feature Pack/ Service Packs and Patches)
2. remove all unwanted AACC Third Party software
3. install required Third Party Software for the release
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. Please note, the Avaya Release Pack Installer is run via the setup.exe and NOT the AvayaReleasePackInstaller.exe.

Generally Available Patch Bundle Installation

When the setup.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 using the Avaya Release Pack Installer application, the complete ProductUpdates folder from within the GA Patch bundle must be copied locally. The contents of this folder should not be modified e.g. 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 Release Pack Bundle** to your local system and unzip
2. Download all available **GA Patch Bundles for this release** to your local system
3. Unzip each GA Patch bundle separately into a folder reflecting the patch bundle zip name
4. When all individual 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 **setup.exe** from folder 'AvayaReleasePackInstaller' which is located within the **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 AACC 7.0.2.0 Release Pack software. This is due to third party software changes between AACC 7.0.1.0 or 7.0.1.1, and AACC 7.0.2.0.

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 7.0.2.0 OVA from 7.7.0.391 to 7.7.0.398

The AACC 7.0.2.0 AAMS OVA comes with version 7.7.0.391 of the Media Server installed with System Layer Version 21. Both need to be upgraded to the latest version. The Media Server needs to be updated to 7.7.0.398 and the System layer needs to be updated to 23

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_7.7.0.23_2017.09.05.iso
4. Click “Choose File” and select this ISO file to be uploaded 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_7.7.0.398_2017.05.09.iso
7. Click “Choose File” and select this ISO file to be uploaded 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 7.7.0.398 and Appliance version 23.

Upgrading Avaya Aura Media Server for AACC 7.0.1.x to AAMS for AACC 7.0.2

This section details the upgrade steps for all supported AAMS deployments to upgrade the AAMS to the version shipped with AACC 7.0.2.0

Upgrading AAMS OVA from 7.0.1.x to 7.0.2.0

Refer to section: Upgrading Avaya Aura Media Server 7.0.2.0 OVA from 7.7.0.391 to 7.7.0.398 for instructions on how to upgrade the Avaya Aura Media Server OVA to version 7.7.0.398 and System Layer 23.

Upgrading AAMS on Customer Install Red Hat Linux 6.x 64 bit Server from 7.0.1.x to 7.0.2.0

This section provides instructions on how to upgrade the Avaya Aura Media Server to version 7.7.0.398 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_7.7.0.398_2017.05.09.bin**. Make sure to choose "Binary" mode of transfer.
3. chmod +x MediaServer_7.7.0.398_2017.05.09.bin
4. Run command: ./MediaServer_7.7.0.398_2017.05.09.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 7.7.0.398.

Upgrading AAMS on Windows 2012 Server (co-resident with AACC) from 7.0.1.x to 7.0.2.0

This section provides instructions on how to upgrade the Avaya Aura Media Server to version 7.7.0.398 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 7.7.0.398.

Downgrades

Important: Direct downgrades from 7.0.2.0 to 7.0.0.0 or 7.0.0.1 are not supported. You must downgrade from 7.0.2.0 to 7.0.1.x first, before downgrading to 7.0.0.x

Avaya Release Pack Installer

To downgrade to an earlier 7.0.1.x release, you must use the Avaya Release Pack Installer which accompanies that target release.
E.g. if the downgrade target is release 7.0.1.1, you must download the complete 7.0.1.1 release bundle from the support site.

Instructions:

Refer to the Release Notes for the target Release for downgrade instructions.

High Availability Maintenance Utility

Following a downgrade certain High Availability and Configuration information is lost. It is therefore necessary to run the High Availability Maintenance Utility to restore this information.

This utility should be run after ARPI has been run for the downgrade, but before the Server has been rebooted.

Application Location:

The High Availability Maintenance Utility is installed with this release of the software and can be found in the following location:

.:\Avaya\Contact Center\Common Components\HighAvailabilityMaintenance\HAMaintenance.exe

Instructions:

1. Launch the HAMaintenance.exe from the above location.
2. Use the Browse button to select the correct file to import.
    a. The correct file will be in the .:\Avaya\Cache\Cachesys folder and will be named SYSDataExport-YYYY-MM-DD-ttttt.xml where “YYYY-MM-DD-ttttt” are a date/time stamp of when the file was created.
    b. If there are multiple files with this naming format then the newest one should be selected.
3. Once a file has been selected, click the Import button.
4. Progress will be indicated on the screen and a message box will be presented to the user when the import has completed. The Import should take no longer than 5 minutes.

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.

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

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 introduced 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.

Server Utility - Users.

All Customer created Desktop Users in Server Utility have their passwords reset during the upgrade. To update the passwords to the correct values use Server Utility to delete and recreate all of the Customer created Users.

Data Integration Wizard (DIW) – Secure Web Services.

Certificate information for Secure Web Services is lost during the upgrade. To ensure Secure Web Services continue to work, Customers should use DIW to delete and then re-import the WSDL and certificate file.

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 to 4.7 are cumulative with 4.0 onwards i.e. 4.5.2 replaces 4.0- 4.5.1 similarly 4.7 replaces 4.0-4.6.2. In other words when you install .Net Framework 4.5.2 you also have 4.0, 4.5 and 4.5.1.

Multimedia Prerequisites for server migration

This is only applicable to users migrating to new 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.

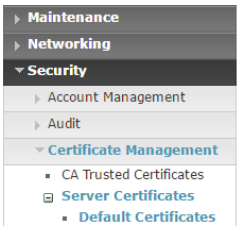
SECURITY INFORMATION

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 7.0.2 fresh installations does not provide the Out of The Box (OTB) security store and AES specific security certificates

From release 7.0.2.0 fresh installations of the solution will not provide the default security store with default security certificates for AACC and the AES.

Fresh installations

For fresh installs the customer will have to create a custom security store for the server during the Ignition Wizard security configuration stage to enable the On by Default and secure the server and services as was provided automatically in previous releases.

If the Ignition Wizard security configuration is not completed fully then upon completion of the Ignition Wizard phase and reboot of the server the services will not be secure and the SIP-CTI link to AES will not be operational as it supports secure connection only.

Ignition Wizard has been enhanced to allow the creation and population of the contact center security store during the configuration phase. If this is skipped then warnings will be given and Security Manager (previously Security Manager) can be used to complete the creation and/or population of the security store.

Upgrades

There is no impact on upgrades, if the OTB store is being used and is on the server, it remains untouched.

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.x 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.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 Security Manager Backup feature.

This will back up the necessary files required to be imported back in on the new system using the Security 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 Security Manager Security Configuration tab

How to change the TLSv1 levels

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

In the Security Configuration Tab of the Security 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 Security 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 Security 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 Security 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 Security 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 Security 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 2 (7.0.2) 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 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.

All AACC 7.0.2 products and components support Internationalization (I18n). The following table lists all AACC 7.0.2 products and components that support Localization (L10n):

AACC 7.0.2 Products	Component
CCT	Web Agent Controls
CCT	Web Agent Controls online help
CCMA	Contact Center Management
CCMA	Access and Partition Management
CCMA	Real-Time Reporting
CCMA	Historical Reporting
CCMA	Configuration
CCMA	Emergency Help
CCMA	Outbound
CCMA	Historical Report Templates
CCMA	Agent Desktop Display
CCMA	Online Help
CCMM	AAD Client
CCMM	AAD online Help
CCMM	OCMT Client
CCMM	OCMT online Help

Refer to Chapter 17: Language support fundamentals in the Avaya Aura Contact Center Server Administration guide for supported languages.

Localized Components (CCMA and CCMM)

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

		Supported Languages										
		CCMA										CCMM
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	Y
	Any 1 Latin1 language	Y	Y	Y	Y	Y	N	N	N	N	N	Y
	Simplified Chinese	N	N	N	N	N	Y	N	N	N	N	Y
	Trad. Chinese	N	N	N	N	N	N	Y	N	N	N	Y
	Japanese	N	N	N	N	N	N	N	Y	N	N	Y
	Russian	N	N	N	N	N	N	N	N	Y	N	Y
	Korean	N	N	N	N	N	N	N	N	N	Y	Y

Language specific support and configuration

All languages are supported on Internet Explorer 10 & 11.

Language	CCMA Client	CCMM Client	CCMM Server
	Browser Language Preference	**Client Windows Support**	**Server Windows Support/ Regional Options Configuration***
French	fr-FR	French Windows 7, 8.1 and 10	French Win 2012 R2. Regional option default (French)
German	de-DE	German Windows 7, 8.1 and 10	German Win 2012 R2. Regional option default (German)
LA Spanish	es-CO	LA Spanish Windows 7, 8.1 and 10	Spanish Win 2012 R2. Regional option default (Spanish)
Simplified Chinese	zh-CN	Simplified Chinese Windows 7, 8.1 and 10	Simplified Chinese Win 2012 R2. Regional option default (Simplified Chinese)
Brazilian Portuguese	pt-BR	Brazilian Portuguese Windows 7, 8.1 and 10	Brazilian Portuguese Win 2012 R2. Regional option default (Brazilian Portuguese)
Russian	ru-RU	Russian Windows 7, 8.1 and 10	Russian Win 2012 R2. Regional option default (Russian)
Italian	it-IT	Italian Windows 7, 8.1 and 10	Italian Win 2012 R2. Regional option default (Italian)
Japanese	ja-JP	Japanese Windows 7, 8.1 and 10	Japanese Win 2012 R2 Regional option default (Japanese)
Traditional Chinese	zh-tw	Traditional Chinese Windows 7, 8.1 and 10	Traditional Chinese Win 2012 R2. Regional option default (Traditional Chinese)
Korean	ko-KR	Korean Windows 7, 8.1 and 10	Korean Win 2012 R2. Regional option default (Korean)

* If you wish to launch AAD or OCMT in a local language BUT THE CLIENT OPERATING SYSTEM IS ENGLISH, then change the default language in the regional language options to the local language.

Email Analyzer configuration

An English email analyzer (AlphanumericAnalyzer) is enabled by default for keyword analysis of English Latin-1 character sets on the CCMM server. The email analyzer can be configured based on language specific values specified in the following table:

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

The *mailservice.properties* file on the CCMM Server specifies which analyzer is enabled and lists all supported analyzers in the comments.

This procedure can be used to enable a language specific email analyzer:

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 value to language specific value.
7. Start the CCMM Email Manager service on the server.

Email Analyzer Limitation 1 - Wildcard use (Asian) – Single Byte Routing

There is a limitation when the email analyzer is enabled for Asian languages. A problem arises when routing with SINGLE BYTE characters in the keyword. Double byte keywords route successfully. This limitation also applies for wildcards included in keywords.

To route a single byte keyword to a skillset, you must save the keyword as DOUBLE byte on the server. For example to route the single byte keyword ｺﾌﾟﾀ 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.

Note: This is a limitation of the 3rd party creator of the analyzer, Lucene.

*Email Analyzer Limitation 2 - Wildcard use (Asian) - Wildcard * and ? string position*

There is a limitation when the email analyzer is enabled for Asian languages. Wildcard ‘?’ or ‘*’ can only be used at the end of a keyword.

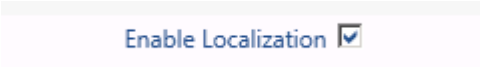
e.g. Wildcard use たば* is correct. Wildcard use た*た is not correct.

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.

Start Localized AAD Client

Pre-installation steps

- Ensure that Localization is enabled in CCMM Administration -> Agent Desktop Configuration -> User Settings



- If you wish to launch AAD in a local language but the client operating system is ENGLISH, then change the default language in the regional language options to the local language.

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) using format:
   https://<Contact Center Multimedia servername>/agentdesktop/LANGUAGE CODE*
2. Click Launch AAD.
3. Click Install.

Starting the Agent Desktop Client

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

Prerequisites

- Ensure that you install Avaya Agent Desktop.

Procedure steps

1. In Windows Explorer or Internet Explorer, enter the HTTP address (URL) using format:
   https://<Contact Center Multimedia servername>/agentdesktop/LANGUAGE CODE*
2. Click Launch AAD.

Alternative Procedure steps

1. 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 CODE**s to be used are:

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

Troubleshooting

Detecting latest Language files

In case that client runs the English AAD and OCMT applications and does not pick up the language files, then 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.

KNOWN ISSUES

Hardware Appliance

None

Software Appliance

None

Application\Features

AML AACC not being prompted for a reboot upon installation of Patch Bundle

Tracking Number	CC-13839
Application	Contact Center Update Manager
Description	During the installation of Contact Center patches, Contact Center services will be shutdown. On AML systems, after installation of GA Patch Bundle content using the Update Manager application, a notification indicating a reboot is required will not be presented to the user. On SIP systems users are notified of a reboot requirement as expected.
Impact	Contact Center services will remain in a stopped state unless a reboot is undertaken.
Workaround	After using Update Manager to install Generally Available patch content, manually restart the system.

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

Agent greetings and Voice recording not working "A Serious Error has occurred – Exiting"

Tracking Number	CC-13218
Application	Contact Center Manager Administration
Description	When security is ON, CCMA Authentication web service just supports HTTPS request, not HTTP request from clients. If the client requests HTTP, it will return an error code 403 (HTTP 403) to the client. However in the case of CC-13218 issue, the client requests HTTP, CCMA Authentication web service still works when security is ON.
Impact	Agent greetings and Voice recording do not work. CCMA Authentication is not secure.
Workaround	The following Authentication web service configuration is added into IIS config file, applicationHost.config located at C:\Windows\System32\inetsrv\config folder. <location path="Default Web Site/WebServices/Authentication/Service.asmx"> <system.webServer> <security> <access sslFlags="None" />

	</security> </system.webServer> </location> That configuration makes IIS support both http and https for Authentication service. We need to remove that configuration.

Install wrong .NET Framework version from installing pre-requisites on CCMA Dashboard

Tracking Number	CC-13274 (CC-9825)
Application	Contact Center Manager Administration
Description	Cannot launch Dashboard report from Real-Time Report page
Impact	Unable to use CCMA Dashboard
Workaround	1. Install .NET FW 4.5.2 from FP2 DVD for the client machine. 2. Apply "SchUseStrongCrypto" value for the client machine. Create a text file named strongcrypto35-enable.reg that contains the following text: Windows Registry Editor Version 5.00 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319] "SchUseStrongCrypto"=dword:00000001 [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319] "SchUseStrongCrypto"=dword:00000001 Run regedit.exe In Registry Editor, click the File menu and then click Import. Navigate to and select the strongcrypto35-enable.reg file that you created in the first step. Click Open and then click OK Exit Registry Editor. 3. For Windows 7 SP1, the client needs to install the update https://support.microsoft.com/en-us/kb/3140245 4. Restart the client.

With SSO enabled prior to upgrade, SCT Tool and OD are failed to connect CCMA after upgrading to new release

Tracking Number	CC-13655
Application	Contact Center Manager Administration
Description	For users who have already configured SSO and enabled SSO - When they upgrade their system to 7.0.2 GA, SCT and OD will fail to connect CCMA
Impact	SCT and OD fail to connect CCMA

Workaround	The workaround is to disable SSO and re-enable SSO from Security Details dialog. Steps: - Open Manager Administrator Configuration - Open Security Settings - Click Disable button - Click Yes button from the confirmation dialog - Click OK button from the information dialog - Click Enable button - Click Yes button from the confirmation dialog - Click OK button from the information dialog

With SSO enabled, POM client fails to retrieve skillsets

Tracking Number	CC-13683
Application	Contact Center Manager Administration
Description	With SSO enabled, POM client fails to retrieve skillsets. The issue lies with POM (OUTREACH-8526)
Impact	POM client fails with SSO enabled in CCMA
Workaround	The workaround is to disable SSO.

CCMA- All texts in Attribute in JSON variables showed "ERROR: Could not get text: Index = 9040, Language = en-us!" for upgraded lab from 7.0.1

Tracking Number	CC-13468
Application	Contact Center Manager Administration
Description	From Scripting, open JSON variable (JSON Object, JSON String, JSON Pair), the text string shows the error "ERROR: Could not get text: Index = 9040, Language = en-us!"
Impact	Text does not explain the guidelines around JSON variable
Workaround	We need to run the command "AccessToInterSystems.exe -install ALLTEXT" at D:\Avaya\Contact Center\Manager Administration\Server\bin folder. Steps: - Open a cmd - Change the folder to D:\Avaya\Contact Center\Manager Administration\Server\bin - D:\Avaya\Contact Center\Manager Administration\Server\bin > AccessToInterSystems.exe -install ALLTEXT

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

Avaya Agent Desktop slow to launch

Tracking Number	CC-11982
Application	Avaya Agent Desktop
Description	Avaya Agent Desktop is slow to launch due to issue with embedded browser version. This is caused by IE forcing AAD to use older version of IE due to Compatibility setting (Display all websites in Compatibility View**)**.
Impact	Agent Desktop is slow to launch and remains in initializing state for several minutes.
Workaround	Remove/deselect the "Display all websites in Compatibility View" setting under Compatibility View Settings in IE

Agent Greeting not working when extended characters used in Username or Skillset name.

Tracking Number	CC-12067, CC-12057.
Application	Agent Greeting
Description	Agent Greeting experiences the following issues when extended characters (non-US-ASCII) used in: Username (CC-12067): "Agent Greeting Recorded" is not ticked in CCMA when user records Agent Greeting. Greeting will still play. Skillset (CC-12057): Agent Greeting Recorder will drop the call when trying to record an Agent Greeting for a Skillset with extended characters.
Impact	CC-12067: CCMA does not display ticked box in "AG Recorded" when Agent Greeting is recorded. AG is not affected. CC-12057: Agent cannot record an Agent Greeting for Skillset with non-ASCII characters.
Workaround	None

Music On Hold And Announcements do not play when extended characters used in Music Content Group or Announcement name.

Tracking Number	CC-12090, CC-12017.
Application	Music On Hold and Announcements
Description	Music On Hold and Announcements do not play when extended characters (non-US-ASCII) used in the names.
Impact	Music On Hold by design will not allow Extended character set. CCMA will be changed to not allow non-ASCII characters. Announcements do not play if extended character used in Announcement name.
Workaround	Rename MOH and Announcement to use ASCII character set.

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 CS1000 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.

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 installed
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

Agent Controls not working in Firefox Browser

Tracking Number	CC-11673
Application	Agent Controls Application
Description	The agent controls application will not connect to the Integration Portal web socket when launched from Mozilla Firefox browser.
Impact	It is not possible to use Agent Controls Application with Mozilla Firefox browser.
Workaround	Use another browser, for example Internet Explorer.

On one particular deployment CCMS IS_Service fails to start

Tracking Number	CC-13554
Application	Contact Center Manager Server
Description	On one particular deployment CCMS IS_Service fails to start.
Impact	Intrinsics in scripting do not have valid data.
Solution	There is no workaround. However, the problem usually disappears after a server restart.

AAD does not display Agent Statistics when security is on

Tracking Number	CC-13431
Application	Agent Desktop
Description	AAD will fail to display Agent Statistics if the following conditions exist: 1) Security is turned on in Security Manager (formerly known as Certificate Manager) 2) The server signed cert has SAN's configured, ie for MCHA deployments the managed name should be configured as a SAN 3) The hostname configured within CCMM Administration for CC Web Stats matches one of these SAN names. Ie in MCHA the managed name is configured
Impact	If the conditions described above exist then Agent Statistics will not display in AAD
Solution	The work around is to configure (Agent Statistics) CC Web Stats to use an IP address instead of a hostname or FQDN. 1) Through CCMA launch the CCMM Administration client 2) Navigate to: General Administration -> Server Settings 3) With Server Settings selected on the left hand pane, a list of host names should be present on the right hand pane. 4) Under Server Type find an entry called CC Web Stats and change the Hostname entry to use the relevant IP address instead of a hostname or FQDN 5) In HA environments this should be the managed IP address, in all other environments this should be the CCMS server IP address

Ignition Wizard – Error message setting click-once launch URL

Tracking Number	CC-13608
Application	Installer / Ignition Wizard
Description	The install tries to set the launch URL on the boot-strap setup.exe for the click-once applications; AAAD, OCMT and CCMM Admin. A permissions problem intermittently causes an exception message to pop up indicating that the setup file is in use.
Impact	The setup.exe is not signed properly so the launch with prerequisites from CCMA will install the prerequisites but will not locate and launch the OCMT or CCMM Admin click once application.
Workaround	Save the CCMM server name in the MM dashboard to reapply the launch URL

Contact Center Agent Browser application - cannot login if Contact Center SSO (CCMA SSO) enabled

Tracking Number	CC-13682
Application	Contact Center Agent Browser application Contact Control Service – Java SDK Contact Control Service – JavaScript SDK
Description	Contact Control Service based applications, which includes the Contact Center Agent Browser application, will fail to establish a web socket connection when Contact Center SSO (CCMA SSO) is enabled.

Impact	Contact Center Agent Browser application cannot login agent. Contact Control Service – Java SDK and Contact Control Service – JavaScript SDK based application will fail to establish a web socket with the Contact Center.
Workaround	Do not use Contact Center SSO (CCMA SSO) when using Contact Control Service SDK based applications, including Contact Center Agent Browser application.

Release Bundle number missing from Update Manager in some systems

Tracking Number	CC-13633
Application	Update Manager
Description	Steps to reproduce: 1. Deploy a fresh install system 2. Launch Update Manager 3. Check Release Bundle Build number Expected result: Check Release Bundle Build number Actual Result: Release Bundle Build number is “not found”
Impact	Cannot check Release Bundle Build number
Workaround	User can see Release Bundle Build number in Registry

Update Manager installing and installed screens missing progress information

Tracking Number	CC-13714
Application	Update Manager
Description	Steps to reproduce: 1. Open Update Manager 2. Click on Install to open the "Update Manager - Install" screen. Note the message informing the user to update Contact Center Feature Packs or Service Packs using the Avaya Release Pack Installer 3. Click on Browse and browse to the location of the GA patches 4. Click on Scan. Applicable patches should appear 5. Select a patch or patches and click on "Install Patch(es)" 6. Click Yes on the dialog box, asking you to confirm the patch(es) to be installed 7. Confirm that you understand the Terms and Conditions by clicking Yes on the next screen Expected result: The patch(es) get installed. The lower part of the window displays progress information in a Summary group box Actual Result: The patch(es) get installed. The lower part of the window is blank
Impact	Agent may not have understanding of how much longer left in install.
Workaround	Agent still getting information on whether patch is installing or installed.

Context Menu not working in HTML Email control

Tracking Number	CC-13694
Application	Agent Desktop
Description	Steps to reproduce: 1. Launch AAD and login agent with email capabilities 2. Click create email button 3. Check that email format is HTML 4. Copy text from an external application e.g. word 5. Right-click on the email control Expected Result: Context menu is displayed and agent can paste text into email Actual Result: Context menu does not appear to allow agent to paste text into email
Impact Workaround	
Workaround	Agent can still paste to email using keyboard shortcuts

For large Contact Centers, Agent RTD may fail to load agents

Tracking Number	CC-13860
Application	Contact Center Manager Administration
Description	For a Contact Center with a very large number of configured agents, the time to load the agent records from the database may exceed the configured timeout. If the timeout is exceeded, the Agent RTD will not display the agents.
Impact Workaround	
Workaround	Increase the OAM Timeout to allow more time to load the agent records from the database. 1. From Start Menu, launch Manager Administration Configuration. 2. Select RTR Registry Settings. 3. Change OAM Timeout to 300000 milliseconds. 4. Accept the ICERtdService restart.

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-11441	License Manager GUI displays incorrect number of AMS instances used
CC-11670	Access ports terminating calls
CC-11862	AACC 6.4 SP16: ASM ignores activity code entered on a consult call
CC-11879	Detection of NBTSM_Service state 'Link Status=UNKNOWN' Initiated Switchover
CC-11930	ASM Executor thread crashed after switchover while processing multiplicityClearEvent
CC-12020	Presentation Denied Time or Not Ready time is showing wrongly in agent performance table. PDT+NRD time cannot be greater than 900 seconds for an interval.
CC-12029	AACC 7.0.1: Cannot restore Active server backup to Standby post-migration
CC-12083	skillset priority from dynamic assignment being applied to other agent skillsets
CC-12229	HDX Get response intermittently a blank value
CC-12232	Emails are not presenting based on Oldest age preference for few skillsets
CC-12239	ASM Termination on STBY while processing call answer
CC-12276	AACC 6.4 SP16: Agent getting stuck in idle state after call routing failure in ASM
CC-12317	AACC 6.4 SP16: Huge number of calls showing as offered in real time statistics
CC-12318	ACTIV ASM race condition in MultiplicityTimeOutTransaction results in ASM restart
CC-12468	MAS Event Scheduler (NBSCH) repeatedly terminates after start-up [DB changes]
CC-12485	ASM service termination asm xmlWrp::operator
CC-12728	ASM Service termination when an agent logged out
CC-13044	TFE crash when processing TSM event CP_CLEAR for three party conference
CC-13070	ASM fails to process agent logout for logout during RTQNA scenario - agent logins fails thereafter
CC-13167	calls stuck in the PSCAN tool
CC-13252	bad sequence to TFE after ROUTE CALL causing routed calls to peg as Defaulted
CC-13363	Agents losing assignments from multiplicity skillsets
CC-13430	no idle to ASM after call rejected at telset leaves Agent Stuck Idle not getting calls
CC-13432	Two agents received the same call at the same time
CC-13647	Agents appear as logged out on switchover
CC-9509	AACC Agent Validation source is not listed in the Event-to-Trap Translator utility (evntwin.exe) on the 6.4.215 RGN
CC-14579	Failure to load Master_Script after migration
CC-14602	TFE crashes in case of OAM timeout while compiling scripts
CC-13708	Avoid sending ITR Music and ITR SBR to SGM in the same split second
CC-14462	WHERE-EQUALS is not processing contacts correctly
CC-12205	getSPAgentAddressForIm not found generates exception causing no MonitorStop from STBY AACC to AES

CCMA Defect Listing

This list contains defects addressed for the Manager Administration components

WI/JIRA	Summary
CC-11837	RCW report failing after upgraded from AACC 6.4 SP15 to AACC 7.0 SP1
CC-12236	CCMA - when copying an agent the partition is not copied
CC-12275	AACC 7.0.1: w3wp wClient_DA_COM termination stopped Agent RTDs
CC-12397	Unable to configure call-by-call in Historical Statistics
CC-12639	AACC 7.0.1.1: Scheduled MM reports do not run if selection criteria applied
CC-12741	CDN name “NOT IN USE” in historical reporting
CC-13557	CCMA - Billboard Private Collection showing in wrong order when launching a private collection
CC-13705	7.0.1.1 - CCMA migration from 6.4 SP15 to 7.x fails

CCT Defect Listing

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

WI/JIRA	Summary
	NONE

CCMM/AAD Defect Listing

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

WI/JIRA	Summary
CC-11012	AAD 7.0.1 - POM - Selecting external number for callback does not result in number being presented when callback arrives
CC-11120	[RB689] AAAD_There is no Not Ready Reason Code name when agent changes Not Ready state with Reason Code
CC-11445	Display text only configuration on CCMM configuration not working
CC-11649	Email templates inserting at top instead of cursor position
CC-11940	Receiving an email with the MailTo field greater than 4096 characters can cause emails to stop downloading
CC-12278	SMS text body not visible
CC-12316	Failed to create chat controller - UnknownXmppException No response to stanza
CC-12430	CCMM agents not able to pull from all assigned skillsets
CC-12484	AAAD consult/Transfer made by agent on a web chat contact not each time displaying the agent list to consult
CC-12603	AAD not ready state not updated correctly after changing it to another not-ready code
CC-12615	agents unable to receive EWC chats
CC-12638	AAD - Print option doesn't print all search contacts
CC-12643	When an agent is not assigned to a skillsets upon login and attempts to pull a contact, nothing is displayed
CC-12997	ADD inserting template appears to add padding around blank lines in template

Install Defect Listing

This list contains Installation defects addressed for in this release

WI/JIRA	Summary
CC-13047	Local Administrator gets black screen on RDC with AACC / ACCS

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 – Additional Security Information

Store Maintenance – backup and restore

Backing up the Certificate Store

1) Ensure all services are stopped
2) Launch Security 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 Security 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 Security Manager
7) Open Security 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 Security 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 Security 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 Security 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 Security Manager
15) Open Security 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 Security 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 Security 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 Security 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