Avaya Aura® Contact Center
Release 7.1.2.0

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	AACC 7.1.2.0 GA Release	ACC Team	28-Sep-2021
1.1	AACC 7.1.2.0 GA Security updates	ACC Team	17-Dec-2021
1.2	AACC 7.1.2.0 HA updates	ACC Team	20-Jan-2022
1.3	AACC Post GA patch bundle	ACC Team	09-Mar-2022
1.4	IE out of support updates	ACC Team	16-Jun-2022
1.5	ADD related work-around	ACC Team	23-Jun-2022

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.x 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_8.0.0.169_A6_2018.10.24_OVF10.ova	eda4b84b51ab9447d78755a3e2d31af8

Avaya WebLM OVA

The Avaya WebLM 8 OVA is the required software when deploying the OVA in a virtualisation environment. This software is used for product licensing. Please download this software from http://support.avaya.com

File Name	
WebLM-8.1.0.0.7-32857-e65-9.ova	434706602537e1d57a1e270f4a8cdb2c

Workspaces Cluster

The Avaya Aura® Contact Center Workspaces OVA is required when deploying the workspaces cluster in a virtualization environment. The software provides the base image and software for the deployment of the Avaya Aura® Contact Center Workspaces Cluster.

Filename	MD5 Checksum
WSOVAGOLDEN_RB237_71200275.ova	7e45a2dcc34c910abd15112dc60fec7a

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.

Filename	MD5 Checksum
AACC_7.1.2.0-33.iso	d4231e91b00598292648cb187c4aa257

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.

Filename	MD5 Checksum
ACC_7.1.2.0-237.zip	cdc82d215f0f9c3c4697641f87cbdc1a

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_7.1.2.0_FeaturePack02ServicePack00_GA_Patches-17.zip	b165da9027e276efe4148a7fc2511557
AvayaCC_CCCC_7.1.2.0.4.3_Patch.zip	4b7280348b3e7eb589430195a1ce9c4e
ACC_7.1.2.0_FeaturePack02ServicePack00_GA_Patches-21.zip	905e342dad03ffdc51a85cc7440e853d

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

Avaya Aura Contact Center Workspaces Cluster

The following updates contain critical fixes that must be applied to your Workspaces Cluster

File Name	MD5 Checksum
AvayaCC_WS_7.1.2.0.8.29_Patch.zip	ed61eb1c092ec6b1063829c9d55e68d6

Avaya Aura Media Server OVA and Hyper-V Upgrade

The AAMS OVA version is: 8.0.0.169. Both need to be upgraded to the latest version. The Media Server needs to be updated to 8.0.0.205 and the System layer needs to be updated to 16. This is accomplished by downloading the two ISO files in the table below.
This procedure is detailed in document: “Upgrading and patching Avaya Aura® Contact Center”

File Name	MD5 Checksum
MediaServer_Update_8.0.0.205_2019.04.29.iso	32ff99844e1d40d3c9f0d9341307f829
MediaServer_System_Update_8.0.0.16_2019.04.05.iso	5bd8c1d0ada215088b03571350185924

NOTE: Customers can install AMS version Media Server 8.0.2 and System Update 23 as minumum supported versions but can take later versions available from the support site.

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. 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 and Windows Server 2016 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 prior to deployment of the AACC application.

File Name	MD5 Checksum
ACC_7_1_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
N/A	N/A

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	7.x, 8.x, 10.x
Avaya Aura Communication Manager	7.x, 8.x, 10.x
Avaya Aura Application Enablement Services	7.x, 8.x, 10.x
Avaya Aura System Manager	7.x, 8.x, 10.x
Avaya Aura Session Manager	7.x, 8.x, 10.x
Avaya Aura Presence Services	7.x, 8.x, 10.x

Please note that Avaya Aura 6.4 FP2 is not supported with AACC 7.1. Aura stack must be upgraded to a minimum of version 7.0.1 to align with AACC 7.1.

Avaya Aura® 10.1 Service Observe feature support

AACC supports the Communication Manager 10.1 Service Observing feature as detailed in the Avaya Aura® Communication Manager Feature Description and Implementation documentation. An AACC Agent is on a routed AACC call with the customer.
The Service Observer must not be logged into AACC as either agent or supervisor. The Service Observer uses their phone to initiate the CM Service Observe feature to participate in the Agent-customer call. Observers can monitor calls in listen-only mode or listen-and-talk mode. Observers can leave a monitored call leaving the AACC Agent and customer still in discussion.

Avaya Communication Server 1000

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

Avaya Aura® Contact Center 7.1.2.0 is only supported with CS 1000 R7.6.

Required Packages

The following are the required CS1000 packages

Application	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 of, Voice and Multimedia with Avaya Media Server **without** Workspaces on a physical platform, a Gigabit Network Adapter is required that supports Receive Side Scaling (RSS) with 4 RSS queues.

Single Server deployments of, Voice and Multimedia with Avaya Media Server **without** Workspaces, are supported on physical mid-range to high-end servers only, as defined in Avaya Aura Contact Center Overview and Specification document. Lab and customer deployments must adhere to the minimum RAM requirements. Failure to do so can result in Avaya Aura Media Server being unable to launch.

Single Server deployments of, Voice and Multimedia with Avaya Aura Media Server, now deploy AAMS as a Hyper-V Linux virtual machine. Workspaces is also deployed as a Hyper-V Linux solution.
A hardware requirement is that CPU Virtualization / Virtualization Technology is enabled in the host Windows Server BIOS. The available virtualization settings vary by hardware provider and BIOS version. Read your hardware provider's documents covering virtualization support to determine which settings to configure. This is commonly found in BIOS *System Settings -> Processor settings*.

Refer to document *AACC Overview and Specification* for additional information on Hardware requirements.

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)
- Windows Server 2016 Standard with Desktop Experience
- Windows Server 2016 Standard Datacenter (64-bit Edition)
- Windows Server 2019 Standard
- Windows Server 2019 Datacenter

This release no longer supports the Avaya Aura Media Server (AAMS) installed co-resident with AACC on a Windows Server platform. A single box solution where AACC and AAMS are running on the same physical server is achieved by deploying the AAMS OVA as a virtual server on the Windows Server with Hyper-V manager. This is applied in both fresh installations and upgrades.

AAMS is supported on Red Hat Enterprise Linux (RHEL) 7.x 64-bit OS. It is not supported 32-bit RHEL. It is not supported on any other version of Linux.

Windows Server 2019 is supported starting from 7.1.2 Post GA Patch Bundle (March 2022). Patch Bundle contains a number of critical compatibility fixes and must be applied on all Windows Server 2019 AACC installations. The Server OS guidelines listed in the AACC 7.1.2 Overview & Specification apply to Windows Server 2019 also.

Microsoft Windows Server Updates

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

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

Windows Server 2012 R2

Currently, please do not install **KB4340558** (specifically sub component **KB4338419**) or **KB4340006** (specifically sub component **KB4338605**) on your Avaya Contact Center Select Server. Refer to Avaya Aura® Contact Center Security Hotfixes and Compatibility listing for updates relating to **KB4340558** or **KB4340006**.

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

Windows Server 2016 with Desktop Experience

Please apply all available Microsoft hotfixes as per the Avaya Contact Center Select Security Hotfixes and Compatibility listing

Red Hat Enterprise Linux Updates

AAMS is only supported on Red Hat Enterprise Linux (RHEL) 7.x 64-bit servers.
For an AAMS installed on a customer installed RHEL 7.x 64-bit server, it is mandatory to register the RHEL OS with Red Hat Networks (RHN) and to apply all the latest updates. AAMS is tested regularly against all the latest RHEL updates.

The AAMS VMWare OVA and Hyper-V installations ship with the all the most recent RHEL security updates as of GA. Avaya supplies RHEL updates as an AAMS System Update ISO file that is uploaded and applied using AAMS Element Manager. AAMS System updates are released as part of a Service Pack release. The OVA or Hyper-V AAMS do not need to register with Red Hat Networks.

CentOS Linux Updates

The Workspaces VMWare OVA and Hyper-V installations ship with the all the most recent CentOS security updates as of GA.

Before conducting a yum update of any new CentOS packages you must confirm whether any CentOS package updates are excluded, and not to be installed, by checking the Avaya Aura® Contact Center Security Hotfixes and Compatibility listing – published every month on support.avaya.com.

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.

Windows Server 2012 R2

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.

Update ID	Summary
KB4517298	Addresses an issue in which the following may stop responding and you may receive the error, "Invalid procedure call”: - Applications that were made using Visual Basic 6 (VB6). - Macros that use Visual Basic for Applications (VBA). - Scripts or apps that use Visual Basic Scripting Edition (VBScript).

Update	Summary
Windows Management Framework 5.1	- Windows Management Framework 5.1 includes updates to Windows PowerShell, Windows PowerShell Desired State Configuration (DSC), Windows Remote Management (WinRM), Windows Management Instrumentation (WMI). Release notes: https://go.microsoft.com/fwlink/?linkid=839460 - Download URL: https://www.microsoft.com/en-us/download/details.aspx?id=54616

Windows Server 2016 with Desktop Experience

Install the latest updates available as per the recommendations in the Avaya Aura Contact Center Security Hotfixes and Compatibility listing.

Update ID	Summary
KB4512495	Updates an issue with downloading copyrighted digital media (music, TV shows, movies, and so on) from certain websites using Microsoft Edge and Internet Explorer. Updates an issue that causes File Explorer to intermittently stop working.

Edge Support

Element Manager and CCMA require that Edge be configured to run the web sites in “Compatibility Mode”. Microsoft support indicates that some websites might not display correctly in Microsoft Edge. 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 Edge.

To turn on Compatibility View please refer to the document “Avaya Aura® Contact Center Client Administration” dated April 2022.

Follow the instructions in Chapter 3: Contact Center Manager Administration client operation under “Internet Explorer mode and Compatibility View configuration on the domain server”.

The Avaya Agent Desktop (AAD) uses the Microsoft Edge browser as a rendering engine to display web content. To display sites that are compatible only with Internet Explorer, you must enable IE mode for Agent Desktop using new functionality in Contact Center Multimedia Administration.

CCMA Support with Edge in IE Compatible mode

For all guides and Edge configuration steps, please refer to Avaya Aura® Contact Center Client Administration document, part "Accessing CCMA using Microsoft Edge with Internet Explorer mode".

The important note is you must not delete the Internet Explorer 11 browser from your computer (Windows 10) or your server (Windows 2012, Windows 2016 and Windows 2019) otherwise Microsoft Edge cannot launch CCMA.

Windows 11 does not have Internet Explorer 11 browser. It has Microsoft Edge browser only so users need to configure Microsoft Edge with Internet Explorer mode for CCMA.

Microsoft .NET Framework Support

Avaya Aura® Contact Center 7.1.2.0 is dependent on Microsoft .NET Framework 4.8.
AAAD and some other utilities require .NET Framework 4.8 to be installed.

Windows 11 Support

Windows 11 is supported starting from 7.1.2 Post GA Patch Bundle (March 2022) for Avaya Agent Desktop and Contact Center Manager Administration. The Windows 10 OS guidelines listed in the AACC 7.1.2 Overview & Specification apply to Windows 11 also.

Avaya Workplace Support

Avaya Aura® Contact Center 7.1.2.0 supports Avaya Workplace client as a softphone for Voice/Video.
But recent versions of Avaya Workplace is supported ONLY on Windows 10 and they won't be installed on Windows clients supported by AAAD (Windows 7, 8.1).
So if the agents are going to use AAAD together with Avaya Workplace, then only Windows 10 is supported.

VMware

Avaya Aura® Contact Center 7.1.2.0 supports VMware vSphere 6.5, 6.7 and 7.0.

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 Firewall Service

Windows Firewall service have to be started and enabled on automatic startup before installation or upgrade of 7.1.2.0 release started. You can turn off and disable Windows Firewall Service after successful installation. In case of using own firewall software please configure with Port Matrix accordingly.

Tools for extracting software

It is advised that you utilize the latest versions of your preferred tools for unpacking the Avaya Aura® Contact Center software.

Important - Default Out-of-Box Certificate Removal

Removal of Default Out-of-box Certificates

Default out-of-box certificates will be removed during the installation of the Contact Center 7.1.x.x Release. Custom certificates **must** be applied to your system before upgrade begins, or after upgrade completion, using the Security Manager application.

Failure to create custom security certificates prior or during the upgrade to 7.1.x.x will result in the loss of functionality, specifically the SIP-CTI link to AES on Avaya Aura Contact Center.

As well as the loss of functionality any previously secure connections will now not be secure until custom security certificates are put in place.

Removal of default certificates from the Contact Center server will result in additional configuration on other services that make up the solution, such as AES, as they will have to be setup to accept the new custom certificates.

Disable Windows Automatic Maintenance

Windows Server 2012 R2

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'

Disable Windows Updates

Windows Server 2012 R2

The download and installation of Windows Updates, during the installation and configuration of Contact Center software, can severely impact the fresh install and upgrade processes.
Microsoft Updates must be disabled before the Contact Center installation and configuration phase, however only after all applicable windows updates have been applied.
To disable Microsoft Updates:

1. Launch the Windows *Control Panel*
2. Click *System and Security*
3. Click *Windows Update*
4. Click *Change settings*
5. In the available drop down, choose the option to *Never check for updates (not recommended)*

Windows Server 2016 with Desktop Experience

The download and installation of Windows Updates, during the installation and configuration of Contact Center software, can severely impact the fresh install and upgrade processes.
Microsoft Updates must be disabled before the Contact Center installation and configuration phase, however only after all applicable windows updates have been applied.
To disable Microsoft Updates:

1. Start – Run *gpedit.msc*
2. Browse to Computer Configuration \ Administrative Updates \ Windows Components \ Windows Update
3. Locate the *Configure Automatic Updates* setting
4. Note the current setting so that it can be reverted to later
5. Double-click on *Configure Automatic Updates* and select the *Disabled* radio button option
6. Click Apply
7. Click OK
8. Exit gpedit.msc

After installation and configuration of Contact Center software is complete, you may revert this setting to its original value.

PEM certificates with DIW

PEM certificates do not work with DIW. PEM certs must be renamed as .CER for adding to DIW.

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.

Hot Patching Support

Upgrading

Hot Patching is **NOT SUPPORTED** when upgrading to Avaya Aura© Contact Center Release 7.1.2.0.

AACC Patches

If you have deployment Avaya Aura© Contact Center Release 7.1.x.x and need to apply patches to your evironmment Hot Patching **IS SUPPORTED** for these patches.

Workspaces Patches

Hot Patching is **NOT SUPPORTED** when deploying Workspaces patches on to your system. The outage associated with the patch will affect all logged in Agents. During the maintenance window for the deployment of a workspaces patch the Agent Desktop application can be used. Therefore, customers with Workspaces can continue to Hot Patch their servers with Traditional AACC component patch bundles but will require downtime to patch Workspaces containers as most patches will require container removal, replace and restart.

POM Support

AACC 7.1.2.0 supports POM 3.1.3 or later. No prior version of POM is supported with AACC 7.1.2.0. If AACC site is operating with POM then site **must upgrade to POM 3.1.3 or later before upgrading to AACC 7.1.2.0**.

Note: POM 3.1.3 requires Experience Portal (EP) 7.2.x.
Note: POM 4.0.x requires Experience Portal (EP) 8.x.

Voice & Multimedia Contact Server with Avaya Aura Media Server

Avaya Aura® Contact Center no longer supports the Avaya Aura Media Server (AAMS) installed co-resident with AACC on a Windows Server platform. This release achieves a single box solution where AACC and AMS are running on the same physical server by deploying the AAMS OVA as a virtual server on the Windows Server 2012 and 2016 Hyper-V Manager. This is applied in both fresh installations and upgrades scenarios.

Hardware considerations:

- CPU Virtualization / Virtualization Technology must be enabled in the host Windows Server BIOS. The available virtualization settings vary by hardware provider and BIOS version. Read your hardware provider's documents covering virtualization support to determine which settings to configure. This is commonly found in BIOS System Settings -> Processor settings
- The Hyper-V deployment of Linux AAMS 8.0 is only supported on physical mid-range to high-end servers as defined in Avaya Aura Contact Center Overview and Specification document. Lab & site deployments must adhere to the minimum RAM requirements

Software considerations:

- As in previous releases, you cannot deploy a Voice and Multimedia Contact Server with AAMS in a virtual environment. This will be blocked by the Universal Installer and Avaya Release Pack Installer applications
- The AAMS should be upgraded or patched following the AAMS procedures for virtual deployments as outlined in product documentation. For AACC 7.0.3 and later releases, the co-resident Linux based AAMS Hyper-V image will not be upgraded or downgraded using the Avaya Release Pack Installer.
- If upgrading from AACC 7.0.2 or earlier, it is necessary to manually backup the AAMS database BEFORE upgrading the AACC and restore the AAMS database post upgrade to ensure that all media files are preserved. Detailed steps are documented in the *Backing up the Avaya Aura® Media Server database and Restoring the Avaya Aura® Media Server database sections of the Upgrading and patching Avaya Aura® Contact Center* user guide.

Orchestration Designer Scripts

Before upgrading you must ensure that all scripts are validated and compile successfully in Orchestration Designer.

Removing Reserved Skillset Prefixes

Before upgrading you must ensure that none of your created skillsets are using prefixes reserved by AACC. The list of reserved prefixes are EM_, PO_, OB_, WC_, SN_, SM_, IM_ and VM_. If you are using any of these you need to rename them before upgrading.

Installation

New Installations

Update Manager is missing CCMS patches after fresh installation. Please review known issues section for CC-25452

Install-time Patching

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

Reboot required before Ignition Wizard

After the Universal installer has completed, a reboot is required before launching the Ignition Wizard. If a reboot prompt is not displayed, please reboot the system anyway before launching the Ignition Wizard. Failure to do so may result in an Ignition Wizard failure.

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.

Security configuration during Ignition Wizard (IMPORTANT)

During the import of P7 chained certificate, Ignition Wizard may display the message "Import of the security certificate has failed". In this case, skip the security configuration step and after Ignition Wizard finishes and the server restarts, use Security Manager.
Please also see Known Issues (Installation) section for more details.

Upgrades

Direct upgrades from 7.0.0.0 and 7.0.0.1 to 7.1.x.x are not supported. You must first upgrade to 7.0.1.x before upgrading to 7.1.x.x

If you applied a license file on 7.1.1.0 release manually, then AvayaCC_CCLM_7.1.1.0.4.5_Patch must be installed prior to upgrade. Otherwise, license file will be lost during upgrade. You will have to re-apply the license manually after the upgrade is completed.

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 AACC 7.x.x.x 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
5. install GA Patches from any available GA Patch 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.

Reboot Prompts

Before running the Avaya Release Pack Installer application, if the operating system or other installed software display prompts for a reboot, please reboot your system.
If additional reboots are required during execution of the Avaya Release Pack Installer application, a prompt will be displayed to the user.
All reboot prompts should be actioned – failure to reboot when requested will adversely affect the installation of software.

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.

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

Note: If upgrading, the Avaya Contact Center Select Update Manager application resident on the system will fail to install the ACCS 7.1.x.x Release Pack software. This is due to third party software changes between ACCS 7.0.x.x and ACCS 7.1.x.x

Update Manager

Use the Contact Center Update Manager to view the patches currently on a Contact Center server. You can use Update Manager to install and uninstall patch bundles in the correct order.
You must install patches for each server application in order of patch number, for example; 01, 02, 03.
You cannot use Update Manager to install Release Packs, Feature Packs, or Service Packs; you must use the Contact Center Release Pack Installer (ARPI).

Update Configurator

A new application is provided within the Avaya Aura® Contact Center Release Pack bundle called the Update Configurator. This application is applicable provides an automated mechanism to deploy and configure the Linux Hyper-V AAMS upgrade and the Avaya Aura® Contact Center Workspaces Cluster. This application will launch automatically after the Avaya Release Pack Installer reboot has completed.

Downgrades

Important: Direct downgrades from 7.1.x.x to 7.0.0.0 or 7.0.0.1 are not supported. You must downgrade from 7.1.x.x to 7.0.1.x first, before downgrading to 7.0.0.x

If local WebLM is used then turn off security using Security Manager before downgrade to 7.0.x. Security can be re-enabled after downgrade is finished.

Avaya Release Pack Installer

To downgrade to an earlier 7.0.3.x, 7.0.2.x, 7.0.1.x, or 7.1.0.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 and completed the down 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:

D:\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 D:\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.

Avaya Aura Media Server

For co-resident Voice and Multimedia Contact Center with AAMS it is not possible to downgrade the Linux Hyper-V AAMS once it has been deployed and configured. The newly upgraded Hyper-V AAMS 8.0 can be maintained and is supported with AACC 7.0.2 onwards.

Support for 1500 applications (scripts) in ACCS/AACC

The downgrade will not support systems having greater than 1000 active scripts. After the downgrade, TFE will be explicitly limited 1000 active scripts, and the database will contain more than 1000 active scripts. The customers who downgrade will need to reduce their active scripts back to 1000 before downgrade to 7.1.0.x or earlier releases.

Post-Installation Configuration

Avaya Aura Media Server

Avaya Aura Media Server Configuration

The following configuration must be carried out on all AAMS servers (PVI Linux, VMWare OVA and Hyper-V).

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 pinging the CCMA hostname and 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 and Hyper-V deployments do 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 hostname and FQDN name resolution of the CCMA server.
    - On PVI AAMS running on customer supplied Red Hat servers, EM does not provide Name Resolution functionality. Host and FQDN resolution need to be added to **/etc/hosts** file on Red Hat server.

Avaya Aura Media Server - Upgrade - License

If the AAMS *Element Manager -> Element Status* is displaying *"Media Server instance is not licensed"* then the following configuration steps must be carried out to update the AAMS license:

1. On AACC launch SCMU and navigate to LM tab
2. Shut down License Manager
3. Start License Manager

Avaya Aura Media Server - Upgrade - Service Status

If the AAMS *Element Manager -> Element Status -> Service Status* is displaying *Stopped* state, and it is not possible to Start AAMS via Element Manager then the following configuration steps must be carried out to update the Service Status:

1. Open an SSH session to the AAMS e.g. using putty
2. Login with cust and <custpw> entered during configuration.
3. At the prompt enter 'reboot' and 'y' to confirm

4. Allow time for the AAMS to restart and verify the state is Started in Element Manager -> Element Status -> Service Status

PVI AAMS 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 or Hyper-V.

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)

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.x, 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 with EWC installed. 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.

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.x 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.x install users will be unable to open attachments that were restored from the backup.

WebLM

WebLM provides Contact Center licensing in an Aura deployment. A WebLM instance is available as part of AACC. This instance is called **Local WebLM**. Alternatively, an independent WebLM can be deployed using the WebLM OVA. The independent WebLM is called **Remote WebLM**. Local WebLM and Remote WebLM are supported on all AACC deployment platforms and all AACC deployment configurations.
WebLM generate a unique ID to identify the WebLM instance. The ID is called **Host ID**. The Host ID is used to lock a license file to the customer deployment. The Host ID is generated by WebLM and is published as a server property in the Web License Manager web application. For Local WebLM, the web application can be accessed from https://localhost:8444/WebLM. For Remote WebLM, the web application can be accessed from https://[HOST]:52233/WebLM.
The Host ID generated by WebLM for a virtualized deployment is a function of the IP address and the VMware UUID. To guarantee a constant Host ID is generated by WebLM in High Availability deployments, configure the managed IP address lower than both the active and standby IP addresses. Managed IP address configuration is effected using the High Availability configuration utility.

CCMA SSO via SMGR

In case SAM usernames is different from UPN usernames (CC-14196). User needs run CCMA User Migration tool to update UPN usernames for CCMA DB.

1. A new button ("Auto Update UPN") is already added to CCMA User Migration tool. It is used to automatically update UPN usernames for many SAM accounts which are already mapped to domain users in case SSO for CCMA is enabled. User needs to use CCMA User Migration tool and click "Auto

Update UPN" new button. It will search CCMA users who need to update their own UPNs then click Save button to save changes to database. If user does not use that new button "Auto Update UPN", user can map one by one user and save it as the previous behavior.

2. In case SSO is enabled user can log in to CCMA through SMGR using both SAM and UPN. If using SAM, user needs to input SAM usernames and its password. If using UPN usernames, user needs to input UPN usernames with format "UPN@domain.com" and its password

Disable IIS Rapid-Fail Protection for CCMA_DefaultAppPool to avoid intermittent w3wp.exe crashes

When IIS Rapid-Fail Protection is enabled for CCMA_DefaultAppPool it may lead to intermittent w3wp.exe crashes. To protect against this issue perform the following steps

1. On AACC server, please open Internet Information Server (IIS) Manager application
2. Click Application Pools then right click on CCMA_DefaultAppPool then select Advanced Settings…
3. Go to Rapid-Fail Protection then select False for Enabled then click OK button.
4. Perform iisreset command from a Windows cmd

WORKSPACES ON AVAYA AURA® CONTACT CENTER

Deployment

This release makes the Workspaces feature available on Avaya Aura® Contact Center. Workspaces is deployed as a Kubernetes three node cluster.

Important: At least 1 NTP server is required (maximum 3) starts from 7.1.2.0 release for time and date synchronization at Workspaces Nodes.

Workspaces can be deployed in the following environments:

1. Physical machine; Hyper-V Workspaces cluster co-resident with Contact Center software
2. Virtual deployment; VMWare hosted Workspaces cluster

Physical Machine Deployments

Physical Pre-Install Checks

- **Microsoft Updates**
  - All applicable MS Updates must be applied to the Contact Center system **before** installation of Contact Center software.
    Both the download **and** install of MS Updates must be turned **off** for the duration of the Contact Center installation and configuration phases

- **Additional Hard Drive/Partition**
  - For Workspaces deployments, additional disk space is required as defined in *AACC Overview and Specification* document available on support.avaya.com
  - The additional disk space must be accessible via a single drive letter e.g. W:
  - During deployment, users will be prompted to choose a drive which will be used for the storage of cluster data
  - This drive will be used to store cluster data in Network File System (NFS) shared folders

- **Workspaces Cluster Provisioning**
  - For physical deployments, all required Workspaces machines will be created automatically during the configuration phase

Engineering requirement for AACC 7.1.2.0 Workspaces

To support more than 1000 agents simultaneously it's required to increase vCPU value to be equal "8" for Workspaces Worker Nodes VMs in MultiNode or HA setups. Shutdown and reconfigure accordingly Workspaces Worker Nodes VMs settings in Hyper-V Manager after successful deployment. Power on VMs on completion.

- **IP Addressing**
  - IP addresses must be supplied during Workspaces configuration
  - IP addresses provided must not already be allocated to existing systems on the network
  - All cluster IP addresses must reside within the **same subnet** as the Contact Center server
  - It is expected that the Subnet Mask IP is 255.255.255.0 and Gateway IP Subnet matches the user entered IPs e.g. GW 192.168.10.xxx and user entered IPs 192.168.10.xxx

Fresh Install

1. Review section *Physical Pre-Install Checks* above
2. Review the additional disk space requirement as defined in *AACC Overview and Specification*
3. Download the AACC 7.1.2.0 DVD and verify checksum
4. Download the AACC 7.1.2.0 Release Bundle and verify checksum
5. Extract all downloaded content locally
6. Launch the Universal Installer application from the DVD
7. To deploy Workspaces, choose the option to configure Workspaces
8. Progress through the Universal Installer application providing required input (Release Bundle location, drive selections etc.)
9. Reboot system if/when prompted
10. After reboot, configure the system using the Ignition Wizard application
11. Complete required Ignition Wizard fields providing appropriate input on the Workspaces tab
12. Reboot system after Ignition Wizard completion

Upgrades

1. Shutdown all of your Workspaces Virtual Machines on all hosts in case of HA setup.
2. Download the AACC 7.1.2.0 Release Bundle and verify checksum
3. Extract all downloaded content locally
4. From the extracted Release Bundle content, launch the Avaya Release Pack Installer application to upgrade Contact Center and Third Party software
5. Also, while running the Avaya Release Pack Installer, choose the option to install Workspaces, providing the required input
6. Also, while running the Avaya Release Pack Installer, install all 7.1.2.0 GA patch bundles available
7. **Reboot** system when prompted

Maintenance – Fresh install

If it is necessary to repair a Workspaces fresh install the Ignition Wizard application can be re-launched. For physical deployments the Ignition Wizard will remove and re-deploy the required Hyper-V virtual switch and virtual machines:

1. Launch the Ignition Wizard by double clicking desktop shortcut
2. Enter the required data and follow the onscreen instructions

Maintenance - Upgrades

If it is necessary to repair a Workspaces upgrade following script failure the Update Configurator application can be re-run. For physical deployments the Update Configurator will remove and re-deploy the required Hyper-V virtual switch and virtual machines:

1. Launch the Update Configurator by double clicking D:\Avaya\Contact Center\Update Configurator\Update Configurator.exe
2. Enter the required data and follow the onscreen instructions

Uninstall

Uninstall process

Follow these steps to uninstall the product:

1. Remove all installed patches via Update Manager
2. Go to C:\Program Files (x86)\Avaya\UniversalInstaller

3. Run UniversalInstaller.exe

Virtual Environment Deployments

Virtual Pre-Install Checks

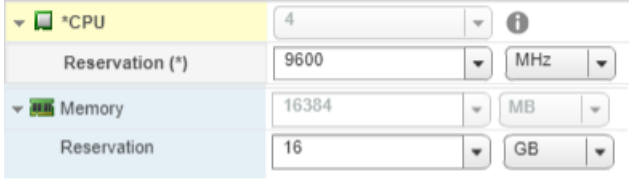
- **Microsoft Updates**
  - All applicable MS Updates must be applied to the Contact Center system **before** installation of Contact Center software.
    Both the download **and** install of MS Updates must be turned **off** for the duration of the Contact Center installation and configuration phases

- **Workspaces Cluster Provisioning**
  - For virtual deployments, users must manually deploy three separate systems using the provided OVA, **prior** to installation or upgrade of Contact Center
  - **Important:** if performing an upgrade from a previously configured Workspaces installation, you must deploy **new** cluster machines using the OVA which is shipped with this release. Machines created from OVAs of the previous release cannot be re-used and should be removed.

- **IP Addressing**
  - IP addresses must be supplied during Workspaces configuration
  - During creation of VMWare cluster machines via the provided OVA, each node/machine must be allocated an IP address and readily accessible on the network
  - All Workspaces cluster IP addresses must reside within the **same subnet** as the Contact Center server
  - It is expected that the Subnet Mask IP is 255.255.255.0 and Gateway IP Subnet matches the user entered IPs e.g. GW 192.168.10.xxx and user entered IPs 192.168.10.xxx
  - Workspaces Cluster IP is the same as Master IP address for Single-Node deployment type

Pre-Installation Steps

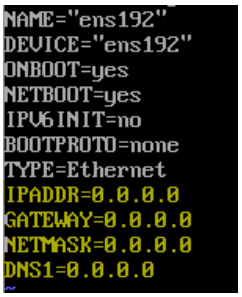
1. Review section *Virtual Pre-Install Checks* above
2. Manually Deploy Cluster Machines using provided Workspaces OVA
   - Using your preferred VMWare client (vCenter/ESXi Web Client) deploy the Workspaces OVA **three** times
   - As a suggestion (you may choose whatever names you prefer) name each of the created virtual machine as:
     - wsk8master
     - wsk8node1
     - wsk8node2
   - During deployment of the OVA, ensure the disk of each virtual machine is configured as **thin**
   - DISABLE guest time synchronization for virtual machine in "VM Options/VMware tools" settings
   - Turn on CPU and Memory reservation for Workspaces VMs according to specification:



Engineering requirement for AACC 7.1.2.0 Workspaces

To support more than 1000 agents simultaneously it's required to increase vCPU value to be equal "8" for Workspaces virtual machines in MultiNode or HA setups.

3. Manually Configure the OVAs onto the Network
    - Log into each deployed virtual machine with username *root* and password *root01*
    - Using the following command, open the CentOS network config script: *vi /etc/sysconfig/network-scripts/ifcfg-ens192*
    - Select the <*Insert*> key on the keyboard to enter edit mode
    - Add/modify the *IPADDR*, *GATEWAY*, *NETMASK* & *DNS* entries as required



    - To save changes select the Esc key then type :*wq!* followed by Enter
    - To exit without saving, select the Esc key then type q! followed by Enter
    - A restart of the network service is required to enable the changes. Enter the following command: *systemctl restart network*

4. Ensure all 3 x VMs are in running state and pingable, via IP address, from the Contact Center Windows server

Fresh Install

1. Download the AACC 7.1.2.0 DVD and verify checksum
2. Download the AACC 7.1.2.0 Release Bundle and verify checksum
3. Extract all downloaded content locally
4. Launch the Universal Installer application from the DVD
5. To deploy Workspaces, choose the option to configure Workspaces
6. Progress through the Universal Installer application providing required input (Release Bundle location, drive selections etc.)
7. Reboot system if/when prompted
8. After reboot, configure the system using the Ignition Wizard application
9. Complete required Ignition Wizard fields providing appropriate input on the Workspaces tab
10. Reboot system after Ignition Wizard completion

Upgrades

1. Download the AACC 7.1.2.0 Release Bundle and verify checksum
2. Extract the downloaded content locally
3. From the extracted Release Bundle content, launch the Avaya Release Pack Installer application to upgrade Contact Center and Third Party software
4. Also, while running the Avaya Release Pack Installer, choose the option to install Workspaces, providing the required input
5. Also, while running the Avaya Release Pack Installer, install all 7.1.2.0 GA patch bundles available
6. **Reboot** system when prompted
7. Perform any post deployment configuration as detailed in section ‘Post-Deployment’ and ‘Post-Installation Configuration’ sections below.

8. Optional - remove Workspaces cluster drive (e.g. W:\) on Contact Center server.
   This drive is no longer required from 7.1.0.3 Workspaces deployments in virtual environments.

Maintenance – Fresh install

If it is necessary to repair a Workspaces fresh install the Ignition Wizard application can be re-run.

Important: The Workspaces OVAs must be re-deployed and configured on the network before the Ignition Wizard is started.

1. Launch the Ignition Wizard by double clicking the desktop shortcut
2. Enter the required data and follow the onscreen instructions

Maintenance - Upgrades

If it is necessary to repair a Workspaces upgrade following script failure the Update Configurator application can be re-run.

Important: The Workspaces OVAs must be re-deployed and configured on the network before the Update Configurator is re-run.

1. Launch the Update Configurator by double clicking D:\Avaya\Contact Center\Update Configurator\Update Configurator.exe
2. Enter the required data and follow the onscreen instructions

Uninstall

Uninstall process

Follow these steps to uninstall the product:
1. Remove all installed patches via Update Manager
2. Go to C:\Program Files (x86)\Avaya\UniversalInstaller
3. Run UniversalInstaller.exe

Post-Deployment Configuration

Please also review the Known Issues - Workspaces on AACC section

Workspaces Patches

After successful Workspaces deployment please install the latest Avaya Workspaces Patch at your system:
- Log on to the Active Contact Center server as Administrator.
- Extract the downloaded Avaya Workspaces Patch to a local folder from a AvayaCC_WS_7.1.2.0.*.zip archive.
- From the WorkspacesPatchInstaller folder, launch the WorkspacesPatchInstaller.exe file.
- Enter Workspaces cluster administration password to establish SSH connection to the Workspaces cluster and click Connect.
- Click Next.
- When the license agreement screen appears, click I ACCEPT THE LICENSE TERMS. The installation process starts.
- When the installation finishes, click Close.

Email handling – Closed Reason Code

Email reply will not send if a closed reason code was never created on the AACC/ACCS system.
Check if Closed reason Code exists

1. Run CCMM Administration
2. Check under Agent Desktop Configuration -> Resources → Closed Reason Codes
3. If no Closed Reason code exists then create one

Workspaces and Domain Server

NOTE: Workspaces Agents must be Domain users

Add the Workspaces and Workspaces Domain servers to the CCMM admin

- Launch CCMA and select multimedia.
- Launch the CCMM admin
- Navigate to Workspaces Configuration
- Add "Workspaces server IP" using the Cluster IP
- Add "Domain Server IP"
- Leave the ports as the default

Workspaces operating with Security ON

Similar to existing clients, if your AACC is operating with Security ON you must copy the root certificate from each CA to all Workspaces clients in your contact center. Note: Enterprise Web Chat will not operate on Workspaces if required root certificate is not present.

Re-applying Agent Security settings after AACC upgrade

Agent Security certificate and key are not pushed to Workspaces nodes at deployment time. If you use Agent Security, you must re-apply Agent Security settings after you have upgraded AACC to 7.1.2 and deployed a new Workspaces cluster.

1. Open CCMM Administraton, go to Workspaces – General Settings.
2. Uncheck the Enable Agent Security checkbox, and click Save.
3. Wait for 5 minutes for the new Agent Security settings to propagate.
4. Check the Enable Agent Security checkbox, enter the Hostname, load the certificate, load the key, and click Save.
5. Wait for 5 minutes for the new Agent Security settings to propagate.

Workspaces Troubleshooting

There may be a requirement to restart a Workspaces Cluster node or container in the event of a failure scenario. Detailed procedures are provided in this section. However, restart procedures should only be executed where it's clear that this is the appropriate recovery action.

NOTE: Please save all container logs via Avaya Workspaces Service Utility befor performing any action.

How to restart a Workspaces cluster

Virtual Environment Deployment

- Login to vCenter
- Power down the three nodes in Workspaces Cluster (i.e master, node1 and node2)
- Power up the master node
- Login to the master node and run the command "kubectl get nodes"
- Verify that the master node is "ready"
- Power up node1 and node2
- From the master node, run the command "kubectl get nodes" and verify all nodes are "ready"

Physical Server Deployment

- Login to hyperv manager
- Power down the three nodes in Workspaces Cluster (i.e master, node1 and node2)
- Power up the master node
- Login to the master node and run the command "kubectl get nodes"
- Verify that the master node is "ready"
- Power up node1 and node2
- From the master node, run the command "kubectl get nodes" and verify all nodes are "ready"

How to restart a Workspaces container in the event of a failure

Virtual Environment Deployment

- Login to vCenter
- Login to the master node and run the command "kubectl get pods"

- Verify the pod name and execute “kubectl delete pod <pod name>”
- From the master node, run the command “kubectl get pods” and verify the pod has restarted

Physical Server Deployment

- Login to hyperv manager
- Login to the master node and run the command “kubectl get pods”
- Verify the pod name and execute “kubectl delete pod <pod name>”
- From the master node, run the command “kubectl get pods” and verify the pod has restarted

How to collect logs for the relevant containers

You can collect the Workspaces logs via Workspaces service utility or:

Virtual Environment Deployment

- Login to vCenter
- Login to the master node and run the command “kubectl logs <pod name>”
- Login to the master node and run the command “kubectl logs <pod name> -p” for previous container logs.

Physical Server Deployment

- Login to hyperv manager
- Login to the master node and run the command “kubectl logs <pod name>”
- Login to the master node and run the command “kubectl logs <pod name> -p” for previous container logs.

Web Statistics widget work on the clients without internet connection

As part of the features parity between AAAD and Workspaces, Web Statistics feature was added to Workspaces as a separate widget. But Web statistic widget used the 'Google Charts' to render the charts and bars and the Google library is dynamically loading from Google services on widget initialization. Google Chart API is not permitted to work offline since it is against their Terms Of Service.

Now Web Statistics widget use another library mdbootstrap to render charts which can work offline.

As a result Web Statistics widget works as expected even on the clients that don’t have an access to internet.

Workspaces and High Availability

Avaya Workspaces supports High Availability for fault tolerant and resilient contact center solutions in both physical and virtual (VMware) environments.
You can configure Avaya Workspaces High Availability only on those Contact Center server types that support both Mission Critical High Availability and Avaya Workspaces. Such servers are:

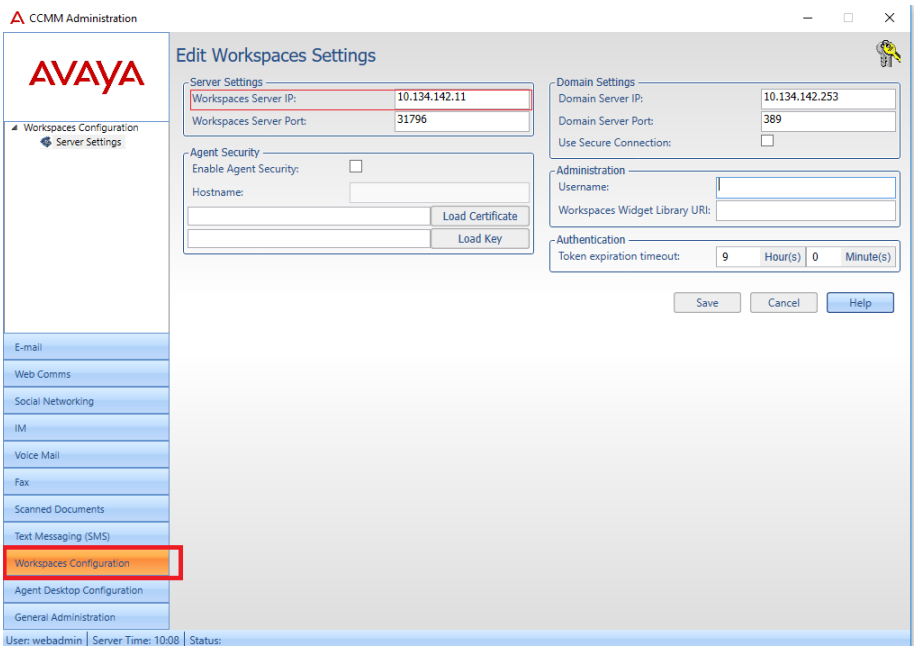
- Voice and Multimedia Contact Server without Avaya Aura® Media Server
- Multimedia Contact Server Only

You can deploy Avaya Workspaces High Availability only if Mission Critical High Availability is configured. Please refer to the customer documentation for further details.

Post-Configuration Instructions

After the cluster has been configured you must perform the following:

1. Update the *Workspaces Server IP* address to the IP address of your cluster (cluster_ip)



2. The workspaces interface will be accessible using http or https from:

   http://<CLUSTER_VIRTUAL_IP>:31380/services/UnifiedAgentController/workspaces/
   http://<FQDN>:31380/services/UnifiedAgentController/workspaces/

   https://<CLUSTER_VIRTUAL_IP>:31390/services/UnifiedAgentController/workspaces/
   https://<FQDN>:31390/services/UnifiedAgentController/workspaces/

   Note:

- HTTPS support will require security configuration as documented in section *Enabling Agent Security for Avaya IX Workspaces* in the AACC Server Administration. The certificate should be created with the FQDN or Cluster
- Virtual IP Address that will be used in the launch URL.
  The port number changes to 31390 for HTTPS.
- An FQDN can be used if a DNS server is setup with Hostname mapped to the Cluster Virtual IP Address.

Remote Geographic Node High Availability with Workspaces

RGN commissioning procedure described in the “AACC Commissioning for Avaya Aura Unified Communications” requires additional steps during the initial configuration.
During the first the database restore from Campus active server to RGN, the following settings are overwritten on RGN server with the Campus ones and need to be corrected.

- the server elements on CCMM is overridden
  It is required to check and re-configure server elements in CCMM Administration -> General Settings -> Server Settings from Campus to RGN addresses if necessary
- Workspaces Agent Security settings
  It is required to check and re-setup Workspaces Agent Security in CCMM Administration -> Workspaces Configuration -> General Settings from Campus to RGN if necessary

The settings above will be preserved during the subsequent database restores

The procedure "How to revert to a campus site after running the RGN" is missing the optional step (step 11) if Workspaces is in the solution.

11. **(Optional)** If you use Avaya Workspaces, when revering to the campus site, you must configure the Avaya Workspaces settings on the active server:
    a. On the active server, log on to CCMM Administration.
    b. On the left pane, select Workspaces Configuration > General Settings.
    c. In the Cluster Settings section, in the Workspaces Cluster IP/FQDN field, enter the campus Avaya Workspaces cluster IP address or FQDN.
    d. In the Workspaces Cluster Port field, enter the campus Avaya Workspaces cluster port number.
    e. Click Save.

Scale

The supported agent count upper limit is 3000 agents with Avaya Aura® Contact Center 7.1 Service Pack 3

Workspaces HA Troubleshooting

1. Run Workspaces Service Utility tool at AACC host and save all container logs - .
2. Run in command line at AACC host (replace “**mm-dd-yy-hh-mm”** with appropriate date and time):

kubectl get pod -owide > "D:\Avaya\Logs\kubectl-get-pod_mm-dd-yy-hh-mm.txt"

3. Repeat step 2 after ten minutes.
4. Inspect collected log files. You have a problem with pod if:
   - Value in ‘STATUS’ column is different from ‘Running’ state, for example ‘OOMKilled’ or ‘CrashLoopBackOff’.
   - Amount of pod restarts in ‘RESTARTS’ column increases over time.
   - Value in ‘READY’ column is differnet from ‘1/1’ or ‘2/2’.

NOTE: In other cases you don’t have to follow the current procedure.

5. Perform for affected pods in command line at AACC host (replace “**<pod name>”** and **<container name>** with appropriate values):

kubectl describe pod <pod name> > "D:\Avaya\Logs\kubectl-describe-pod_<pod name>.txt"
kubectl logs <pod name> <container name> -p > "D:\Avaya\Logs\kubectl-logss-pod_<pod name>.txt"

example: kubectl logs adp-broadcast-service-59df8f788f-wmhtp adp-broadcast-service –p > "D:\Avaya\Logs\kubectl-logs-pod_ adp-broadcast-service-59df8f788f-wmhtp.txt"

6. Run Avaya Workspaces HA Configurator tool, enter ‘Cluster password’ and press ‘Reconfigure’. Cluster repair procedure will take approximately ~20 minutes.
7. Check cluster state via Workspaces Service Utility tool after redeployment.

NOTE: Do not reboot Master Nodes.

Workspaces HA recovery

When operating in the 6 Node (3 x Master, 3 x Worker) Workspaces HA configuration, on failure of a Master Node the Workspaces clients will lose call / contact control for up to 2 minutes while the system rebalances. Active voice calls however, remain up.

The loss of a Worker Node can take up to 10 minutes to rebalance, during which time all Workspaces clients call / contact control will be unavailable. Active voice calls however, remain up.

Upon restoration of these Master or Worker Nodes, they will be added back to the cluster without impact to the Workspaces Agents. It should be noted that the above recovery times are only a guide as to what to expect under these conditions. Timings may vary depending on each unique customer environment deployed.

In cases of an AACC or CCMM switchover there is no impact to Workspaces users.

SECURITY INFORMATION

From Avaya Aura® Contact Center release 7.0.2 fresh installations, Out of The Box (OTB) security store and AES specific security certificates are no longer provided.

From release 7.0.3.0 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.

From Avaya Aura® Contact Center release 7.0.3, upgrades to 7.0.3 or higher will remove OTB or default store if detected.

Upgrades

In 7.0.3, if the OTB store is being used and is on the server it will be actively removed by the installer. From 7.0.3.0 all existing deployments will be required to have implemented custom security configuration.

Prior to upgrading to 7.0.3.0 or higher please put in place custom security certificates and security store via the Security Manager, this is the application on the server to create a custom security store.

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 releases prior to 7.0.3 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 reusing 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
8.0	No	No	Yes	

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

Microsoft VC++ Redistributables 2008/2010 removal

AACC/ACCS don't depend on old Microsoft VC++ 2008/2010 Redistributable packages anymore.

Fresh installations

On fresh installations, AACC/ACCS will not install VC++ 2008/2010 Redistributables packages at all

Upgrades

On an upgrade where the feature pack is applied on an existing 7.1.0.x release, Microsoft VC++ 2008/2010 Redistributables packages will NOT be uninstalled by ARPI automatically. It is expected behavior. The customers can remove them after upgrade manually due to security constraints.

Downgrades

If Microsoft VC++ 2008 Redistributable packages are removed manually after upgrade then it will impact subsequent downgrades to 7.1.0.x or older releases. So before downgrade the customers will need to install Microsoft VC++ Redistributable 2008 x86 9.0.30729.6161 manually located in Release bundle package in \ThirdPartySoftware\Microsoft VC++ Redistributables\2008 - x86 9.0.30729.6161 folder

Log4j 2.x vulnerabilities

Starting from 7.1.2 Post GA Patch Bundle (Feb 2022) the log4j 2.x has been upgraded to the version 2.17.1 to resolve all known vulnerabilities.
Note that during an upgrade the previous versions of log4j 2.x libraries are moved to the backup folders to support downgrades but they will not be used any longer after the upgrade.
So the vulnerabities detected by any scanners for log4j 2.x libraries located in the backup folders should be treated as false positive.

LOCALIZATION

Avaya Aura Contact Center 7.1 (7.1) Avaya Agent Desktop (AAD), Outbound Campaign Management Tool (OCMT), Contact Center Manager Administration (CCMA), and Web Agent Controls UI and online Help is localized into French, German, LA Spanish, Simplified Chinese, Brazilian Portuguese, Russian, Japanese, Traditional Chinese, Korean and Italian. Workspaces on Avaya Aura Contact Center UI and online Help is localized into French, German, LA Spanish, Simplified Chinese, Brazilian Portuguese, Russian, Japanese, Korean, Italian and Hebrew.

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 7.1 products and components support Internationalization (I18n). The following table lists all AACC 7.1 products and components that support Localization (L10n):

AACC 7.1 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
Workspaces	Workspaces UI
Workspaces	Workspaces 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 Edge.

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. “ｺﾌﾟﾀ” 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.

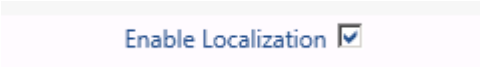
e.g. Wildcard use たば* is correct. Wildcard use た*た is not correct.

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 Edge, 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 Edge, 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

Installation

MCHA AACC Workspace HA deployment fail by using WS HA configuration tool

Tracking Number	CC-19658
Application	Workspaces HA Configurator Tool
Description	Workspaces HA cluster fails to be configured on system where latest version of powershell is 4.0
Impact	Failure to install Workspaces HA cluster
Workaround	Upgrade to Windows Management Framework 5.1 (containing Powershell 5.1 - found at https://www.microsoft.com/en-us/download/details.aspx?id=54616.

Ignition Wizard - Fail to add the chained certificate to Ignition Wizard with error message

Tracking Number	CC-22675
Application	Ignition Wizard
Description	Fail to add the chained certificate to Ignition Wizard with error message: “Import of the security certificate has failed.”
Impact	Security fails during configuration and CCMM services not all starting on a fresh install
Workaround	Do not set security on in Ignition Wizard. Security can be applied via the "Security Manager" application after install has completed.

AvayaCC_CCCC_7.1.2.0.0.84 Install fails blocking upgrades and new installs of 7.1.1

Tracking Number	CC-22997
Application	Universal installer/ARPI
Description	AvayaCC_CCCC_7.1.2.0.0.84 Install fails blocking upgrades and new installs of 7.1.1
Impact	Installation or upgrade cannot be completed.
Workaround	Turn on Windows Firewall service and enable on startup. Execute in command line with Administrator access rights: C:\Windows\SysWOW64\netsh.exe advfirewall import "D:\Avaya\Contact Center\System Configuration\AACCFirewallPolicy\AACC_Firewall_Policy.wfw" Run Universal installer or ARPI in Repair mode

Update Manager is missing CCMS patch during GA patch bundle installation

Tracking Number	CC-25452
Application	Update Manager
Description	Update Manager is missing CCMS patch during GA patch bundle installation.
Impact	CCMS patches cannot be installed.
Solution	1. Install AvayaCC_CCCC_7.1.2.0.2.1_Patch. 2. Install missing CCMS patch from GA patch bundle via Update Manager.
Workaround	1. Apply CCMS base values for the client machine. Create a text file named CCMS.reg that contains the following text: Windows Registry Editor Version 5.00 [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Avaya\Contact Center\Product Installation\CCMS] "ProductVersion"="7.0.0.0" "Build"="7.0.0.0" "CCVersionExt"="7.0.0.0.0.377" Run regedit.exe In Registry Editor, click the File menu and then click Import. Navigate to and select the CCMS.reg file that you created in the first step. Click Open and then click OK Exit Registry Editor. 2. Install GA patch bundle/CCMS patch via Update Manager.

Workspaces on AACC

Incorrect Time Zone in Logs

Tracking Number	CC-17638
Application	Workspaces
Description	The timestamp in the log files was incorrect. It was GMT instead of the relevant time zone
Impact	Troubleshooting
Workaround	Manually apply time zone offset from GMT

Agents Cannot Start Work in Ready State

Tracking Number	CC-18154
Application	Workspaces
Description	Agents are not automatically set to Ready on login to AACC if option selected in Agents Workspace Preferences. Default is Not Ready
Impact	Agents Workspace Preferences not picked up for Starting Work Ready
Workaround	Agents can manually go ready

Agents able to Close Emails without Replying

Tracking Number	CC-17930
Application	Workspaces - Email
Description	It is possible to close the email interaction without replying
Impact	Behavior change between AAD flow and workspaces flow
Workaround	None

WS agent with MPC going back ready, toast popups state going not ready

Tracking Number	CC-19735
Application	Workspaces
Description	When an agent with Multiplicity that is active on a contact and in Not Ready Pending state releases the contact and goes back to Ready state, the WS toast popups incorrectly state agent channels are going to not ready state.
Impact	Agent displayed incorrect information.
Workaround	None

An in-progress ad-hoc email won't Send after switchover

Tracking Number	CC-19697
Application	Workspaces
Description	An ad-hoc email which was initiated before switchover will not be sent successfully after switchover. After switchover, a new ad-hoc email works fine and can be sent successfully

Impact	Agent unable to send an ad-hoc email that was initiated prior to switchover.
Workaround	End existing email and create a new ad-hoc email.

Agent profile activation failed since its failed to load configuration

Tracking Number	CC-20861
Application	Workspaces
Description	Agent profile activation failed due to continuesly restart of adp-cis-service pods. None of any request to "/session", "/configuration" web links could be proceded due to high memory consuming of cis-service.
Impact	Agent unable to be activated.
Workaround	Increase existed memory limits from 1Gb to 4Gb for "adp-cis-service" deployment on Workspaces cluster via "kubectl edit deployment adp-cis-service" from AACC server.

After switchback, RTD is displayed Busy state for agent MPC OFF is working on EWC contact

Tracking Number	CC-21169
Application	Workspaces
Description	After switchback, RTD is displayed Busy state for agent MPC OFF is working on EWC contact.
Impact	RTD displays incorrectly information
Workaround	N/A

Supervisor cannot change Agent status to Ready

Tracking Number	CC-22079
Application	Workspaces
Description	Supervisor cannot change Agent status to Ready
Impact	Supervisor cannot change Agent status to Ready brecause it is not a supported scenario.
Workaround	RTD can be used instead

Supervisor, in addition to his agents, also monitors his primary supervisor's agents.

Tracking Number	CC-22164
Application	Workspaces
Description	Supervisor, in addition to his agents, also monitors his primary supervisor's agents.
Impact	Supervisor can monitor not only his agents.
Workaround	N/A

Supervisor cannot observe the observing/ barging voice contact

Tracking Number	CC-22294
Application	Workspaces
Description	Supervisor cannot observe the observing/ barging voice contact
Impact	Supervisor cannot observe the observing/ barging voice contact

Workaround	Supervisor who needs such functionality should use AAAD instead of Workspaces

Supervisor cannot change Agent's status to Not ready when Agent is in ACW state

Tracking Number	CC-22325
Application	Workspaces
Description	Supervisor has no possibility to set NotReady with NRR code, as the reasult the supervisor cannot force Not ready Agent when Agent is in ACW state.
Impact	Supervisor cannot change Agent's status to Not ready when Agent is in ACW state
Workaround	RTD can be used instead

AACC widgets are not translated in Admin WS page in non-English language

Tracking Number	CC-21912
Application	Workspaces
Description	AACC widgets are not translated in Admin WS page in non-English language
Impact	AACC widget names are presented in English
Workaround	None

Sup/Agent, Agent and customer can hear and speak to each other after Sup/Agent observes

Tracking Number	CC-23402
Application	Workspaces
Description	Sup/Agent, Agent and customer can hear and speak to each other after Sup/Agent observes a DN call, click Hold and then Un-hold
Impact	Customer can hear supervisor when supervisor pressed hold-unhold or after auto-hold due to parallel call to supervisor
Workaround	The supervisor should not use hold-unhold while observing. But there is no way to bypass auto-hold when DN-calling the supervisor in parallel during supervision.

Application\Features

AMS VHDX does not allow a subnet mask different from 255.255.255.0

Tracking Number	CC-17121
Application	AAMS VHDX Deployment
Description	There is a network restriction when installing the AMS VHDX where the customer must use 255.255.255.0 as the Subnet Mask IP
Impact	Customer networks may not conform to this so these restrictions need to be removed
Workaround	The network configuration of the underlying physical NIC card must have a Subnet Mask IP of 255.255.255.0.

AAMS Media Services displayed incorrectly as not started in EM after AACC licenses AAMS

Tracking Number	CC-14420
Application	Avaya Aura Media Server
Description	If an AAMS is not licensed and AACC licenses the AAMS then the AAMS Element Manager can sometimes display the AAMS Media Services as "Not Running" when it is up and running. The **Start** Button in AAMS EM Element Status will be selectable and the **Stop** button will be grayed out.
Impact	There is no impact on AACC as AAMS is up and running fully. The AAMS is displaying the wrong state in EM.
Workaround	Reboot the AAMS by logging into ssh terminal and running "reboot"

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.

AAMS Element Manager may display incorrect FQDN of AAMS VHDX server after deployment AAMS SP

Tracking Number	CC-16955
Application	AAMS VHDX Deployment
Description	After deployment AAMS SP, Element Manager may display invalid FQDN of AAMS server. EM may display the following instead of FQDN: • hostname without domain name; • FQDN with default domain name (“accdev.lab”); • two IP addresses of AAMS.
Impact	Element Manager displays incorrect FQDN
Workaround	Log into AAMS VHDX Linux. Look at a content of the **/etc/sysconfig/network-scripts/ifcfg-eth0** file. It must contains IPADDR and NETWORK entries only once. If necessary, edit that file removing duplicated entries and reboot AAMS VHDX server.

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

Unable to login to CCMA using System Manager 7.0 or earlier 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

One instance of 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 only 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, 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 was found in 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 incorrectly makes IIS support both http and https for Authentication service. We need to remove that incorrect 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 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, Workspaces, SCT Tool, ADD and OD are failed to connect CCMA after upgrading to new release

Tracking Number	CC-13655/CC-21831/CC-26220
Application	Contact Center Manager Administration
Description	For users who have already configured SSO and enabled SSO - When they upgrade their system to 7.x.x GA or, Workspaces, SCT, ADD and OD will fail to connect CCMA (Failed to active agent in Workspaces).
Impact	SCT, ADD and OD fail to connect CCMA or Fail to active agent in Workspaces
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

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

Unable to access CCMA component intermittently after enabling SSO

Tracking Number	CC-14606
Application	Contact Center Manager Administration
Description	After enabling SSO via Security Settings snap-in, unable to access CCMA component intermittently, the page is stuck at loading…
Impact	Customer Impact: Cannot configure data from CCMA
Workaround	The workaround is to restart IIS service using Manager Administration Configuration -> Security Settings -> Advanced -> Restart Service.

Document the use case for UnInstallADLDS.bat

Tracking Number	CC-14620
Application	Contact Center Manager Administration
Description	Customers migrating from AACC 6.x to CC7 will restore the ADLDS instance but it is not always auto removed.
Impact	Customer Impact: ADLDS exists on the system and some Windows ADLDS events are displayed
Workaround	Users need to manually remove the ADLDS instance by running the following bat file:

	UnInstallADLDS.bat located in D:\Avaya\Contact Center\Manager Administration\Apps\Sysops\NESRestore

AAD launch fails from IE on some clients

Tracking Number	CC-14738
Application	Contact Center Manager Administration
Description	The launch address of AAD doesn't seem to work correctly. For example, if the user enters https://<FQDN>/agentdesktop/ where FQDN is the AACC server, the user cannot launch AAD
Impact	AAD
Workaround	User needs to clear IE browsing history and try it again or use the MSI to install AAD

CCMA Launchpad shows more items which should be hidden. This backslash issue happens with IE o both client and server

Tracking Number	CC-17167
Application	Contact Center Manager Administration
Description	CCMA Launchpad displays more items which should be hidden on AACC/ ACCS 7.0.3 and 7.1. This backslash issue happens with IE on both client and server.
Impact	Launchpad Page
Workaround	KB4491113 fixed IE backslash issue. KB4491113 resolves this issue on Windov 2012 server. KB4487011 – Window 10 1703 (https://support.microsoft.com/en-us/help/4487011/windows-10-update-kb4487011) KB4482887 – Window 10 1809 (https://support.microsoft.com/en-us/help/4482887/windows-10-update-kb4482887 If the issue still shows, please also check the following things for IE: a) Internet Options -> Advanced and uncheck "Always expand ALT text for images". Click Apply button. b) Go to Multimedia and check "Show pictures". Click Apply button c) Close IE and Open IE and try CCMA URL again

After migrating from NES 6.0 or NES7 to AACC SIP 7.1 Windows 2016, cannot find "IceInstallADAM.vbs" when upgrading CCMA data

Tracking Number	CC-18121
Application	Contact Center Manager Administration
Description	After migrating from NES 6.0 or NES7 to AACC SIP 7.1 Windows 2016, a message showing that the file "C:\Windows\system32\ADAMScripts\IceInstallADAM.vbs" cannot be found when upgrading CCMA data.
Impact	Migrating NES6 or NES7 to AACC 7.1 on Windows 2016
Workaround	We will use CCMA 6.4 as a middle layer. NES6/7 backup data will be restored on CCMA 6.4, then backup it as 6.4 backup data, then migrating this new 6.4 backup data on Windows 2016. Here are steps: 1. Migrate NES6/7 to 6.4 SP16

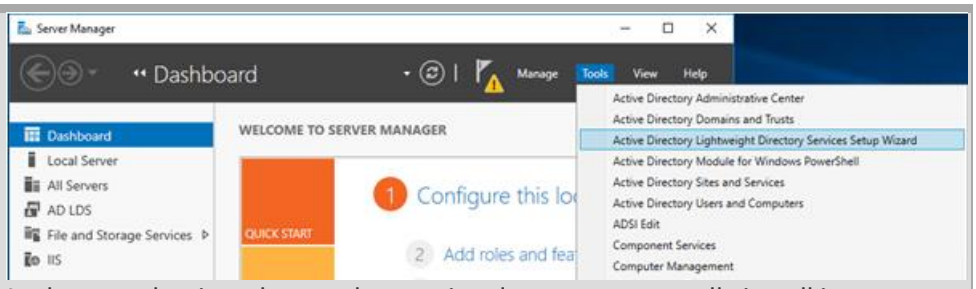
	a) On CCMA 6.4 SP16, we delete all of CCMS servers, Users, Partitions and Access Class b) On 6.4 SP16, on drive D:, create a folder NES67 then copy the following files from a 7.0 machine - ntbackup.exe - ntmsapi.dll - vssapi.dll c) Copy NES67 backup file (.bkf file) to NES67 folder d) Run ntbackup.exe and select the backup file of NES67 (bkf file) then only select "Program Files" to restore CCMA files e) Run CCMA System Upgrade Utility f) Run CCMA backup&Restore to take a CCMA backup file on 6.4 SP15. This file is used for migration on Windows 2016 For more details, please refer to [NES67 workaround pictures.docx] file from the JIRA

CCMA - Users cannot input FQDN name for AMS server name and FQDN name's length is longer than 30 characters

Tracking Number	CC-18904
Application	Contact Center Manager Administration
Description	Users cannot add a Media server name with FQDN name that its length is larger than 30 characters into CCMA Media Servers Configuration
Impact	Prompt Management
Workaround	Add Avaya Aura® Media Server to CCMA Media Servers Configuration as the trusted host name (AMS server name, not FQDN name). The trusted host name is the Avaya Aura® Media Server name that is used to sign the certificate. Note: If you are using AMS HA, please use the AMS managed name (short name, not FQDN name) already signed in the certificate. For more information, please refer to CC-16818/CC-18621 - 7.1 Document update for Media Server hostname to be added to CCMA as trusted name.

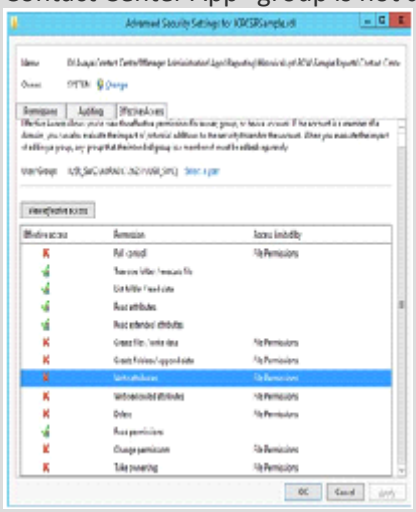
Document - ACCS_7_1_AML_ACCS_Migration - missing Instruction note to require ADLDS installed before starting Migration process

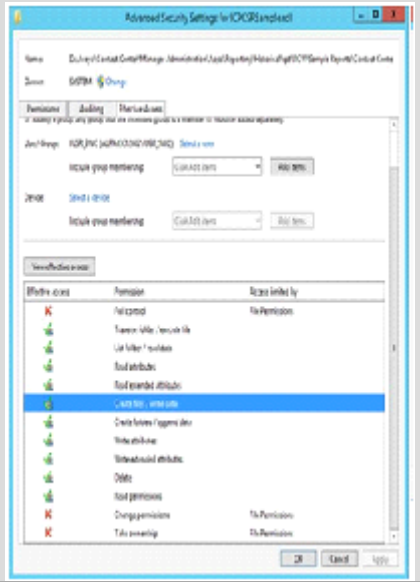
Tracking Number	CC-18861
Application	Contact Center Manager Administration
Description	After migrating from CCMA 6.4 to AACC/ACCS 7.1, a message showing that “Unable to locate CCMA ADAM instance data from a previous installation….” on Windows 2016 or Windows 2012 server.
Impact	Migrating Contact Center Management Administration (CCMA) data
Workaround	Restoring process of CCMA data requires ADLDS existed in the system. User needs to check ADLDS installation on Windows 2012/2016 server. To check if ADLDS is existed or not, they can check as follow: + Launch the "Server Manager" utility, selects the Tools menu item, the item "Active Directory Lightweight Directory Services Setup Wizard" must be existed.



In the case that item has not been existed, user can manually install it as below:
+ In the Server Manager, selects the Manage menu item, then clicks "Add Roles and Features".
+ An "Add Roles and Features Wizard" dialog is shown, then clicks "Server Selection" item.
+ Clicks the "Server Roles" item on the left pane of the dialog, then select the "Active Directory Lightweight Directory Services" item.
+ Click Install button to start installing ADLDS. After this installation completes, user can see its item existed in the Tools menu as mentioned above.
After ADLDS is installed successfully, user can start the Restoring process of CCMA data.

7.1 – RCW - Cannot import Sample Reports from Contact Center Summary folder to HR

Tracking Number	CC-18920/CCRELEASETEAM-9919
Application	Contact Center Manager Administration
Description	Login CCMA with Administrator account, launch RCW and choose some reports under Contact Center Summary(ex:MMCSRStat.rdl). Then import this one into HR, but the message shows that “mscorlib : Access to the path ‘D:\Avaya\Contact Center\Manager Administration\Apps\Reporting\Historical\rpt\RCW\Sample Reports\Contact Center Summary\MMCSRStat.rdl’ is denied “.
Impact	Historical Report cannot import Sample reports
Workaround	Insufficient permission causes import failure. The permission for “Avaya – Contact Center App” group is not applied on the rdl files that caused this issu  The "Avaya – Contact Center App" should have below permissions on sample templates (D:\Avaya\Contact Center\Manager

	Administration\Apps\Reporting\Historical\rpt\RCW\Sample Reports): (Modify, Read & execute, List folder contents, Read, Write) 

RGN SSO Failures - Check FailoverSMGR during PrimarySMGR is down

Tracking Number	CC-17629
Application	Contact Center Manager Administration
Description	The Campus has worked successfully, however, when testing feature of the Failover SMGR (Campus is down, PrimarySMGR is down), user could not log in to the RGN server.
Impact	CCMALogin
Workaround	Suppose that we have the following GR system. Primary SMGR information: IP: 10.128.200.177 FQDN: smgr81177.ccsdc2016.com Virtual FQDN: vsmgr8117.ccsdc2016.com Secondary SMGR information: IP: 10.128.200.178 FQDN: smgr81178.ccsdc2016.com Virtual FQDN: vsmgr8117.ccsdc2016.com When the primary SMGR server is off and the secondary SMGR server is activ In order that CCMA can work with SSO, please apply the following work-arou for your system (RGN server is active). The first work-around: 1) Open Security Setting (we do not need to change SMGR primary server wh it is off) Go to Primary Security Server Details Security Server FQDN is primary SMGR IP (smgr81177.ccsdc2016.com) 2) At CCMA server, open hosts file and update the primary SMGR which point to secondary SMGR IP 10.128.200.178 smgr81177.ccsdc2016.com then save the hosts file or

	the second work-around: 1) Open Security Setting (we change SMGR primary server to the secondary SMGR) Go to Primary Security Server Details Security Server FQDN is the second SMGR IP (smgr81178.ccsdc2016.com) 2) From Security Details, click Advanced to open File Editor and modify cookie name and cookie reset from smgr81178.ccsdc2016.com to smgr81177.ccsdc2016.com (see SecurityDetails.png) then click Save button and Restart Service button 3) Update SSOCookieName in APM.ccmGlobalSettings table from smgr81178.ccsdc2016.com to smgr81177.ccsdc2016.com by running the SQL as SQL_Update_Cache.png (see SQL_Update_Cache.png and APM.ccmGlobalSettings.png) For the pictures and more information, please refer to CC-17629.

IceAdmin password tool get errors because McAfee is blocking Windows machinekeys folder

Tracking Number	CC-20521
Application	Contact Center Manager Administration
Description	IceAdmin password tool get errors when running Ignition Wizard
Impact	Ignition Wizard
Workaround	Antivirus software (McAfee) blocks Windows machinekeys folder that iceAdmin password tool needs to update so the antivirus software (McAfee) need to be disabled before running Ignition Wizard

Private and scheduled reports are not migrating from 6.4 AML to 7.1 SIP system

Tracking Number	CC-20517
Application	Contact Center Manager Administration
Description	Private reports and scheduled jobs are not migrated from AACC 6.4 AML to AACC 7.1 SIP. The executable file "AccessToInterSystems.exe" has been crashed due to it gets exception when reading the corrupted data in CCMA backup file. The backup process has collected all files in the folder "D:\Avaya\Contact Center\Manager Administration\Apps\Common\IceDb" from the 6.4 server which contains the corrupt file, "ICELog.mdb".
Impact	CCMA migration
Workaround	In order to prevent from corrupted access files, we should not use CCMA while taking CCMA backup. All of *.ldb files should be removed before taking CCMA backup.

7.2 – Citrix – Nothing happen when run Outbound and CCMMAdmin tool

Tracking Number	CC-20844
Application	Contact Center Manager Administration
Description	Cannot launch the Outbound and CCMMAdmin on client via citrix
Impact	Outbound and CCMMAdmin tool
Workaround	After saved file download from URL of application, open view download in browser, select it and right click to open it in the folder download and run it manually there.

CCMA - After migration completes, error 503 is shown, reboot CCMA server, the system works fine

Tracking Number	CC-21819
Application	Contact Center Manager Administration
Description	After migration completes, error 503 is shown when accessing CCMA
Impact	CCMA Login page
Workaround	When the error 503 is shown on the Web page, we can see DefaultAppPool has been stopped. Just reboot the CCMA server, the issue will be gone.

RCW formula time format in report preview shows hh:mm:ss when mm or ss is selected

Tracking Number	CC-11894/1-13985295951
Application	Contact Center Manager Administration
Description	7.0's formula format is not updated by RCW as 6.4's formula format. RCW formula time format in report preview shows hh:mm:ss when mm or ss is selected
Impact	CCMA RCW and Historical Report
Workaround	Customers can use below workaround if they want to change output format: 1/ In RCW, click on Formulas button on menu bar to open Formula Editor. 2/ Select Standard Formula > RCW_AverageWorkTime from the Formulas list on the left pane. 3/ Copy Formula Text of this formula. 4/ Click New button. 5/ Paste copied text to Formula Text and fill Formula Name (Ex: Custom_AverageWorkTime). =Code.RCWFunctions.ElapsedTimeFormatter(Code.RCWFunctions.DivideOrDefaultOnZero((Sum(Fields!iAgentByApplicationStat__TalkTime.Value) + Sum(Fields!iAgentByApplicationStat__PostCallProcessingTime.Value)), Sum(Fields!iAgentByApplicationStat__CallsAnswered.Value), (Sum(Fields!iAgentByApplicationStat__TalkTime.Value) + Sum(Fields!iAgentByApplicationStat__PostCallProcessingTime.Value))), "1", False) 6/ Change the highlighted text in Formula Text to get desired elapsed time format: =Code.RCWFunctions.ElapsedTimeFormatter(Code.RCWFunctions.DivideOrDefaultOnZero((Sum(Fields!iAgentByApplicationStat__TalkTime.Value) + Sum(Fields!iAgentByApplicationStat__PostCallProcessingTime.Value)), Sum(Fields!iAgentByApplicationStat__CallsAnswered.Value), (Sum(Fields!iAgentByApplicationStat__TalkTime.Value) + Sum(Fields!iAgentByApplicationStat__PostCallProcessingTime.Value))), "1", False) Available values:

	HH:MM:SS = 1 HH:MM = 2 MM:SS = 3 HH = 4 MM = 5 SS = 6 Ex: If we want the format is HH:MM then the formula text will look like below. =Code.RCWFunctions.ElapsedTimeFormatter(Code.RCWFunctions.DivideOrDefaultOnZero((Sum(Fields!iAgentByApplicationStat__TalkTime.Value) + Sum(Fields!iAgentByApplicationStat__PostCallProcessingTime.Value)), Sum(Fields!iAgentByApplicationStat__CallsAnswered.Value), (Sum(Fields!iAgentByApplicationStat__TalkTime.Value) + Sum(Fields!iAgentByApplicationStat__PostCallProcessingTime.Value))), "2", False) 7/ Save and close Formula Editor 8/ In Report Layout, use Custom_AverageWorkTime instead of RCW_AverageWorkTime. 9/ Done

CCMA failed installation during install-uninstall-install scenario

Tracking Number	CC-25014
Application	Contact Center Manager Administration
Description	If uninstalling AACC/ACCS from Windows OS (Remove the whole 7.1.2 and Base), re-installing AACC/ACCS will be failed. Steps 1/ Fresh install of AACC/ACCS 7.1.2 DVD32 + RB 237 2/ Uninstall AACC/ACCS (Remove 7.1.2 SP + Base) 3/ Install AACC/ACCS 7.1.2 once again. It is failed at step 3
Impact	AACC/ACCS installation
Workaround	The work-around is to take a snapshot of Windows fresh OS. If we want to do the step 2, we just restore that snapshot of a fresh OS again then can install DVD32 + 7.1.2 RB237 properly.

CCMA– RCW – Missing tooltip for properties toolbar on client Windows 11

Tracking Number	CC-25769
Application	Contact Center Manager Administration
Description	Users cannot see tooltip from RCW's toolbar on Windows 11 when moving mouse over buttons from the toolbar. It may make users confused when selecting a button from RCW's toolbar. This issue does not happen on Windows 10 and other Windows OS.
Impact	RCW Application
Workaround	None

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

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.

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.

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	The Agent RTD will not display the agents.
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.

In some lab upgrades with a Local WebLM configuration, AACC was found to be operating with grace licensing after the upgrade

Tracking Number	CC-17177
Application	Upgrade
Description	In some lab upgrades with a Local WebLM configuration, AACC was found to be operating with grace licensing after the upgrade.
Impact	The system is operating with grace licensing. Grace licensing is allowed to be in effect for 30 days.
Solution	The XML license file must be re-applied using **License Manager Configuration Utility**.

CCMM Services not all starting on a fresh install, where Security has failed to be applied via Ignition Wizard

Tracking Number	CC-18286
Application	Ignition Wizard
Description	When a user imports certificate in Security Store Ignition Wizard can create broken certificate with alias URIName.
Impact	Security fails during configuration and CCMM services not all starting on a fresh install
Workaround	Do not set security on in Ignition Wizard. Security can be applied via the "Security Manager" application after install has completed.

Local WebLM may have issues after downgrade to 7.0.x with Security ON

Tracking Number	CC-18589
Application	License Manager
Description	There may be issues with Local WebLM after downgrade from 7.1.0.1 to 7.0.x with security ON. The problem will happen if after downgrade, the security is disabled and the keystore is deleted - local WebLM won't start and manual modification of Tomcat's server.xml will be required.
Impact	Local WebLM fails to start so the product will have issue with licensing
Workaround	If local WebLM is used then turn off the security using Security Manager before downgrade to 7.0.x. The security can be re-enabled after downgrade is finished

Can not login on Offsite or POM Agent with ACCS/AACC Windows 7/8.1/10 without latest .NET framework updates

Tracking Number	CC-24975
Application	AgentDesktop (AAAD)
Description	Can not login on Offsite or POM Agent with ACCS/AACC Windows 7/8.1/10 without latest .NET framework updates
Impact	For agents that have configured Offsite mode or have POM skillset there is no way to login. For offsite agents: when agent is logging with AAAD client, AAAD is freezing before selecting Other Phone in Telephony tab. For POM agent: when agent is logging with AAAD client, AAAD is freezing after client clicked to CCMM tab.
Workaround	Please install August 10, 2021 Update (or later) for .NET Framework 4.8 for appropriate windows version. This version should be greater or equal than v4.8.4410.0. To detect .NET version please execute command in PowerShell (with Administration rights) [System.Runtime.InteropServices.RuntimeInformation]::get_FrameworkDescription() Note: for Windows 7 there is need to follow "Procedure to continue receiving security updates after extended support ends on January 14, 2020". Extended Security Updates (ESU).

All MS Edge browsers are closed automatically after user clicks on Launch button to launch AAAD by using MS Edge on Windows 7 client

Tracking Number	CC-24974
Application	AgentDesktop (AAAD)
Description	All MS Edge browsers are closed automatically after user clicks on Launch button to launch AAAD by using MS Edge on Windows 7 client
Impact	Run AAAD from MS EDGE browsers. (Click Launch to install AAAD) AAAD can be launched successfully but all MS Edge browsers are closed automatically.
Workaround	Please install August 10, 2021 Update (or later) for .NET Framework 4.8 for appropriate windows version. This version should be greater or equals than v4.8.4410.0.

	To detect .NET version please execute command in PowerShell (with Administration rights) [System.Runtime.InteropServices.RuntimeInformation]::get_FrameworkDescription() Note: for Windows 7 there is need to follow "Procedure to continue receiving security updates after extended support ends on January 14, 2020". Extended Security Updates (ESU).

Tomcat security off port is change back to default one post upgrade

Tracking Number	CC-24886
Application	Security Manager
Description	Tomcat security off port is change back to default one post upgrade in Security Manager.
Impact	If the customer set a custom port in the security manager for the security off option, the port changed back to default 8081 after the upgrade.
Workaround	Need to verify the port number in Security manager after an upgrade and change it to custom if required.

Hot patching is broken after Gigaspaces upgrade

Tracking Number	CC-24523
Application	Contact Center Manager Server
Description	Hot Patching is broken in AACC 7.1.2 due to Gigaspaces upgrade to 15.8. As per Gigaspaces support, the upgrade between major versions is not supported for Active-Active topology (used in AACC MCHA deployments).
Impact	The customer sites will have a down time during an upgrade of MCHA systems to AACC 7.1.2.
Solution	There is no workaround

The agents are unable to login into Agent Desktop/Workspaces after adding voice chanel to No Switch Configured

Tracking Number	CC-24228
Application	AgentDesktop (AAAD) and Workspaces
Description	The agents are unable to login into Agent Desktop/Workspaces after adding voice chanel to No Switch Configured
Impact	The agents are unable to login into Agent Desktop/Workspaces after adding voice chanel to No Switch Configured due to incorrect swith subtype being set in the database
Solution	Please contact Avaya Support to change the switch subtype in the database manually

Localization issues

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

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-25794	Log4j Vulnerability CVE-2021-44228
CC-23302	MCHA switchover causes network call to fail to route successfully
CC-24893	Abandoned calls
CC-24906	TFE REST not accepting raw json body
CC-24710	Problems working with JSON TFERest interface
CC-24656	Agent swap ready/notready state in a extremely short time which cause agent state stuck in ready in ASM, but not ready in CMF
CC-25047	AACC Networking reporting inconsistencies
CC-25089	Universal Networking: Race condition between NCP and SIP NOTIFY causes Give Default on Source AACC
CC-25451	HeteroNetworkDisconnect is missing when CAB comes before PCI on target node
CC-25650	Universal Networking: Source agents are stuck in ICCMnotAvailable state after target agent rejected three networking calls in a row
CC-25580	Agents lost call control on AACC
CC-25541	Agents able to log into vice skill without a voice endpoint / phone logged in
CC-25940	Upgrade log4j2 to the latest version
CC-25853	Schema ccms not visible after CCC patch install

CCMA Defect Listing

This list contains defects addressed for the Manager Administration components

WI/JIRA	Summary
CC-25787	CCMA GA patch bundle 2 is created to include some critical fixes for Windows 2019 and Windows 11
CC-25738	CCMA Edge with client Windows 11– There are some pages are not loaded when launch CCMA by FQDN
CC-25753	Window 2019 - CCMA SSO – Cannot launch CCMA with MS Edge when SSO is enabled on client window 11
CC-25777	Intermittently incorrect document mode in IE mode of Microsoft Edge
CC-25843	SupportUtil pages are running with the incorrect document mode in Microsoft Edge - Windows 11
CC-25024	7.1.2 [I18N] CCMA- Supervisor view, agent view and skillset view showed blank page when login with a CCMA user containing I18N characters
CC-25152	CCMA - ERROR "The operation has timed out" when there are many requests to the CCTProxyInterface web service
CC-25261	CCMA APM - Taking a list of CCMA users should be improved in RepAgents's function GetUserDetailsRecordset
CC-25115	SSA: CCMA intermittently slow to respond for all users

CC-25480	APM should define Max Limit of number of UDPs per each user and Max Limit of number of Agents in each UDP
CC-25578	CCMA - RTD - Following the RegAgent log file that the StdDisplay.asp page called GetUsersAvailableElements_rs 2 times
CC-25745	Keep nbcomd.dll loaded in memory for CCMA_RealTimeReportingPool
CC-25741	Bug in SIP Configuration Tool Excel Sheet

CCMM/AAD Defect Listing

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

WI/JIRA	Summary
CC-25151	Anonymous calls are always showing the same number for the agents
CC-25140	Display out of Service Aquisition failure message
CC-25587	AACC 7.1.2: No Font style and Font size on the AAAD client for the multimedia agent
CC-25626	Inserting a picture in AAAD not showing the picture in email
CC-25499	AAAD is showing email body blank when agent replies to it
CC-25123	POM outbound agents looses nailup periodically
CC-25390	Agent make logout, the session is immediately re-created for further quick login or exit from the system
CC-25850	Outbound webservices unable to get getcontactsby phone number through SOAP UI
CC-25902	Voice – The observed Workcard on Supervisor is not auto accepted
CC-24746	On scheduled callback contacts close/reschedule button is missing sometimes while finishing the contact
CC-25915	TabPage not opening when agent get contact
CC-25011	On AAAD of Station A the caller is still shown as Station B instead of Station C
CC-25069	Intermittent issue that AAAD CLient dont show the POM Zone

CCT Defect Listing

This list contains defects addressed for the Communication Control Toolkit components

WI/JIRA	Summary
CC-25543	Issue related to NCC network call
CC-25259	Subscriptions to EWC notifications leak out
CC-25009	7.0.2.0.11 code propagation

Install Defect Listing

This list contains Installation defects addressed for in this release

WI/JIRA	Summary

Workspaces Defect Listing

This list contains defects addressed for the Workspaces components

WI/JIRA	Summary
CC-25074	Workspaces - update workspaces_content_service to new version
CC-25354	Workspaces - update workspaces_content_service to new version
CC-25068	Workspaces webchat input text box disabled
CC-25440	Need to update Keyboard shortcuts page for AACC OLH for 7.1.1 and 7.1.2
CC-25794	Log4j Vulnerability CVE-2021-44228
CC-25354	Workspaces - update workspaces_content_service to new version
CC-25440	Need to update Keyboard shortcuts page for AACC OLH
CC-25068	Workspaces webchat input text box disabled
CC-25403	Workspaces shortcut key should update description to Open transfer menu instead of Blind transfer an interaction
CC-25517	Workspaces – Section 508 – Sup_Agent cannot use keyboard to click to call agent
CC-25523	Workspaces - Section 508 - Agent cannot use keyboard to move down the list transferred skillset
CC-25526	Section 508 - Workspaces Accessibility should work for My Agent widget at status dropdown list and focus on call record
CC-25539	Section 508 - Workspaces Accessibility - Jaws read out all agent info again when focus on Status or Click to call at My Agent widget
CC-25544	Workspaces Accessibility - User Menu not working with JAWS
CC-25545	Need to add a hotkey for transfer button (AACC) + update documentation
CC-25546	Need to update aria-label for checkboxes of General Settings tabs
CC-25547	Checkboxes label in Notification Settings speak two to three times with the screen reader
CC-25548	Jaws should pronounce workspaces toasts
CC-25558	Workspaces – Should focus on interaction card when unholding the chat interaction with keyboard
CC-25582	Workspaces – Section 508 – The content of Suggested Phrases should be read out by Jaws
CC-25644	Workspaces – Section 508 – Jaws should read out the status of channels, time in state on Agent state summary
CC-25798	Workspaces – Cannot switch menu on interaction card using shortcut key after 2 times
CC-25799	Section 508 - Workspaces Accessibility - Jaws read Redial button not correct when it is enabled
CC-25800	Workspaces – Section 508 – Address book area should be focused exactly when using shortcut key
CC-25801	Workspace – Section 508 – The order of members in the team’s menu is read out incorrectly when trying to transfer the call to another member
CC-25803	[Accessibility defect Chrome/Edge] - More Menu - Jaws skips 1st work/disposition code
CC-25804	JAWS pronounses Checkboxes labels in Settings -> Audio three times
CC-25806	Workspaces - Section 508 – Datepicker can not open choose date when using keyboard in Customer History Search
CC-25807	[Accessibility defect Chrome/FF/Edge] - More Menu - Work Codes Menu Needs To Be Read by Jaws
CC-25808	WORKSPACES UI - Sidebar Expand button should say "Expand sidebar navigation"
CC-25809	UAC_3.8.1.0.12 UI issues after Consult

CC-25810	Need to update aria-label for channel icon of Interaction table in My Agents widget
CC-25811	Workspaces Accessibility – Agents is not notified on Jaws tool for new alerting contact on Workspaces
CC-25812	Workspaces shortcut key mismatch between Help page and Help Menu for key Emergency exit
CC-25846	WORKSPACES UI - JAWS does not convey collapsed/expanded on User Menu
CC-25847	WORKSPACES UI - Double speech on Tablist (outer div)
CC-25849	WORKSPACES UI - Unlabeled "For Button"

CCMA ActiveX Control MSI – Content and Versions

File Name	File Size (bytes)	Version
ChartWrapperCtrl.ocx	64360	1.0.0.1
DTPWrapperCtrl.ocx	97128	8.0.0.1
hrctrl.dll	113512	8.0.0.4
iceemhlpcontrol.dll	129896	8.0.0.2
icertdcontrol.dll	854888	9.0.0.3
iemenu.ocx	65648	4.71.115.0
ntzlib.dll	65080	1.1.4.0
olch2x8.ocx	2102448	8.0.20051.51
rope.dll	248680	1.0.0.4
rsclientprint.dll	594432	2011.110.3128.0
sstree.ocx	337120	1.0.4.20
WSEColorText.ocx	179048	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
8.0	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

CCT Toolkit

CCT Webservices works based on what we select protocol version in CCT Console:

- select TLSv1.0 in CCT Webservices it accepts connections from other Applications with TLSv1.0 only
- select TLSv1.1 in CCT Webservices it accepts connections from other Applications with TLSv1.1 only
- select TLSv1.2 in CCT Webservices it accepts connections from other Applications with TLSv1.2 only