Avaya Contact Center Select

Release 7.1.2.1

Release Notes

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

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 Contact Center Select Installation and Commissioning guides for full installation instructions

PUBLICATION HISTORY

Issue	Change Summary	Author(s)	Date
1.0	ACCS 7.1.2.1 GA Release	ACC Team	31.03.2023
2.0	WS Stuck Agent Clean Up Tool (CC-46529, CC-46923)	ACC Team	25.08.2025

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 Contact Center Select, Release 7.x into a virtualization environment. Please ensure you are using this version for all new software installation.

Avaya Aura Media Server OVA

AACC supports the Avaya Aura Media Server versions 8 and 10.1

File Name	MD5 Checksum
MediaServer_8.0.0.169_A6_2018.10.24_OVF10.ova	eda4b84b51ab9447d78755a3e2d31af8
MediaServer_10.1.0.48_A2_2021.12.17_OVF10.ova	7c2a8e7eb0bb49f5533b36367956f41b

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 Contact Center Select 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 Contact Center Select Workspaces Cluster.

Filename	MD5 Checksum
WSOVAGOLDEN_RB41_71210060.ova	4680cff238c86701e358b289a0680aa6

DVD Product Installation

The following are the files required when deploying Avaya Contact Center Select using the Avaya Contact Center Select 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 Contact Center Select DVD version is outlined below. Please ensure you are using this version for all new software installation.

Filename	MD5 Checksum
ACCS_7.1.2.1-14.iso	b17bd9a5c7d4851df344ea7679127e64

Important Note:
Information on the latest updates available with this release are documented in the **Release Pack Bundle** section below.

Release Pack Bundle

The Avaya Contact Center Select 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_7.1.2.1-41.zip	8961af8f2d14d4a979dfc8231f062224

Additional Required Updates

Avaya Contact Center Select Server

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

File Name	MD5 Checksum
ACC_7.1.2.1_FeaturePack02ServicePack01_GA_Patches-23.zip	7a9aeaecdd53b9737af424e618885562

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

Avaya Contact Center Select Workspaces Cluster

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

File Name	MD5 Checksum
AvayaCC_WS_7.1.2.1.1.9_Patch.zip	44536cdb9daf222ce3d905c4a799c590

Avaya Aura Media Server OVA and Hyper-V Upgrade

The AAMS OVA version is: 8.0.0.169/10.1.0.48. Both need to be upgraded to the latest version. The Media Server needs to be updated to 8.0.0.205/10.1.0.54 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
MediaServer_Update_10.1.0.54_2022.01.12.iso	ed8467e503c4350c2b2348435c7da8b8

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 ACCS deployment guide, SNMP should be installed on the Windows Server prior to deployment of the ACCS 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 Contact Center Select 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

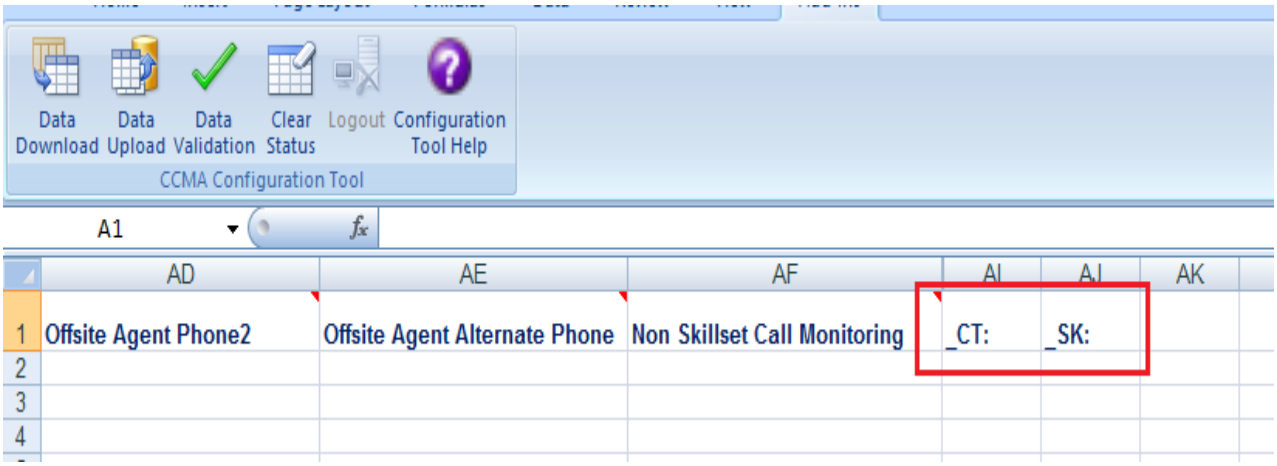
Migration Tool for RCW Generated Reports

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 Service Pack from the ACCS lineup above.

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

SCT's behavior on the "Users" sheet updates in 7.1.2.1 (CC-23193)

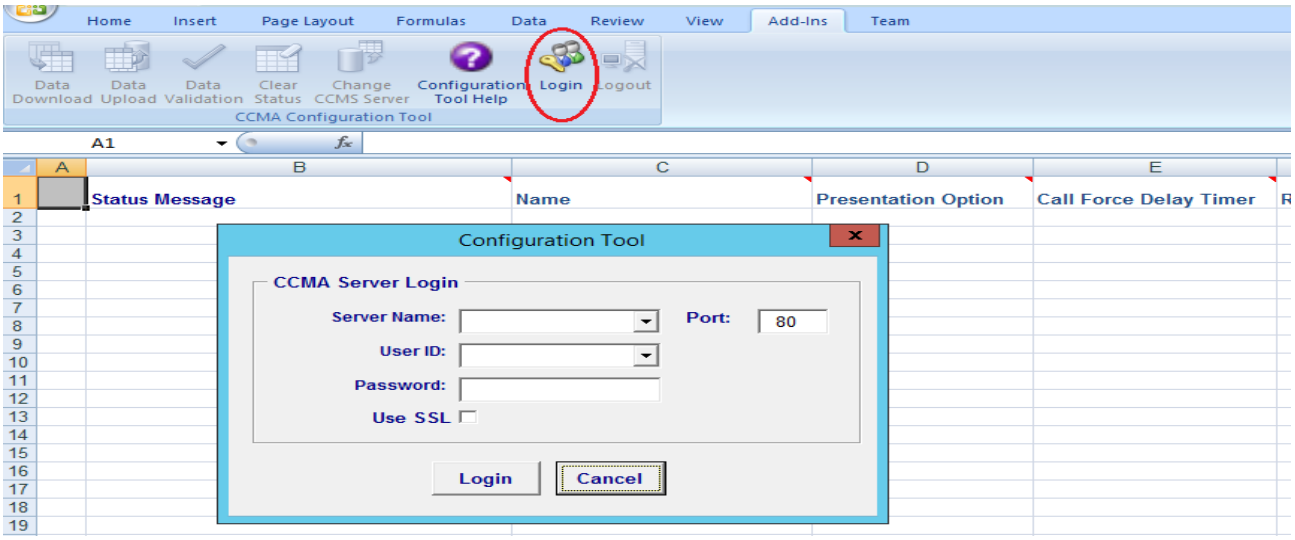
From previous version to 7.1.1: right after user logins to CCMA successfully, the SCT's Users sheet does not have any Contact types or Skillsets columns (please see the image below). It just handles Login action only.



Usually, user will click "Data Download" button to download both headers and data of the selected CCMS. Headers include Contact type names and Skillset names of the selected CCMS. Headers will change if user selects another CCMS (because each CCMS has their different Contact type names and Skillset names). After that, user can use those available headers to upload/update Agents, Sup, or Sup/Agents to that CCMS.

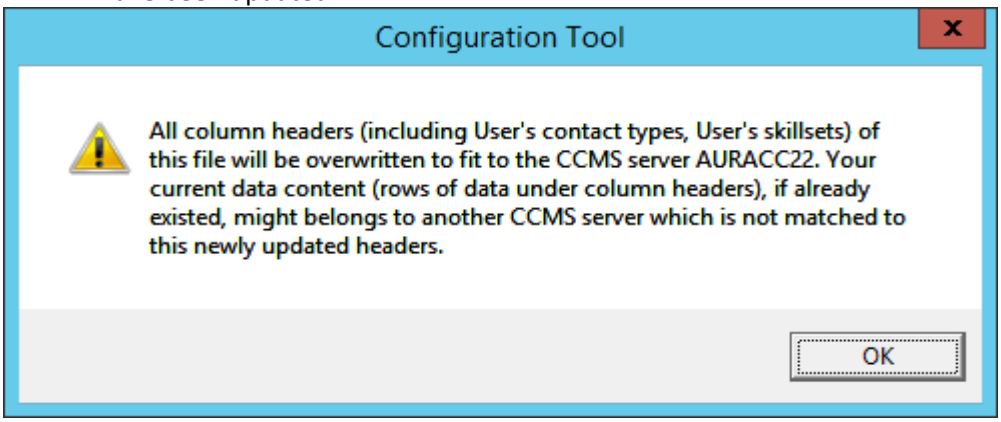
This Jira CC-23193 was raised in 7.1.1. The originator did not click "Data Download" button first, so headers were not available. They had to manually input 2 new columns: "Voice" (as Contact type) and "Default_Skillset" (as Skillset) to test uploading agents. However, two new columns were added after "_CT" & "_SK:" columns which are not correct order. (It should be "Voice", "_CT:", "Default_Skillset", "_SK:"). Therefore, it gets error when uploading user. That is why this Jira was raised.

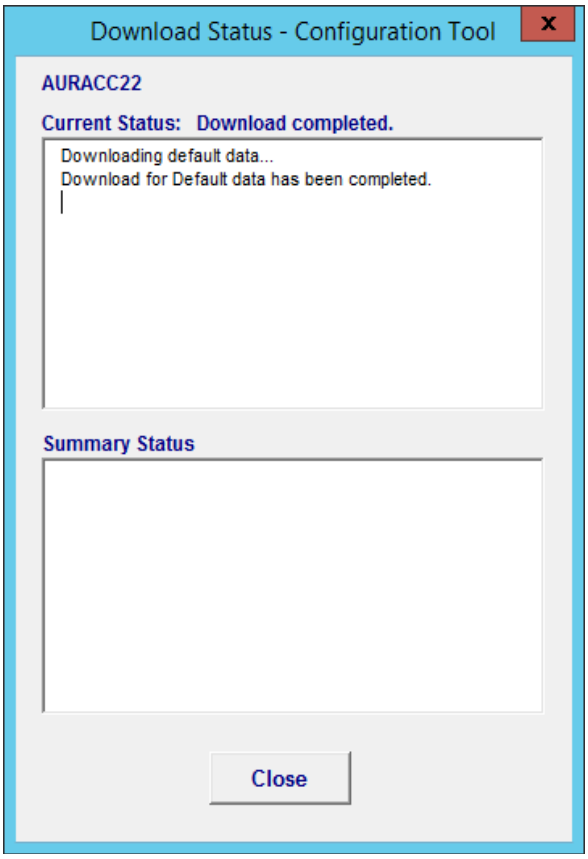
To fix this Jira in 7.1.2.1, we had discussed and agreed that SCT should change its behavior a little bit. Therefore, SCT has added the new task into the "Login" button.



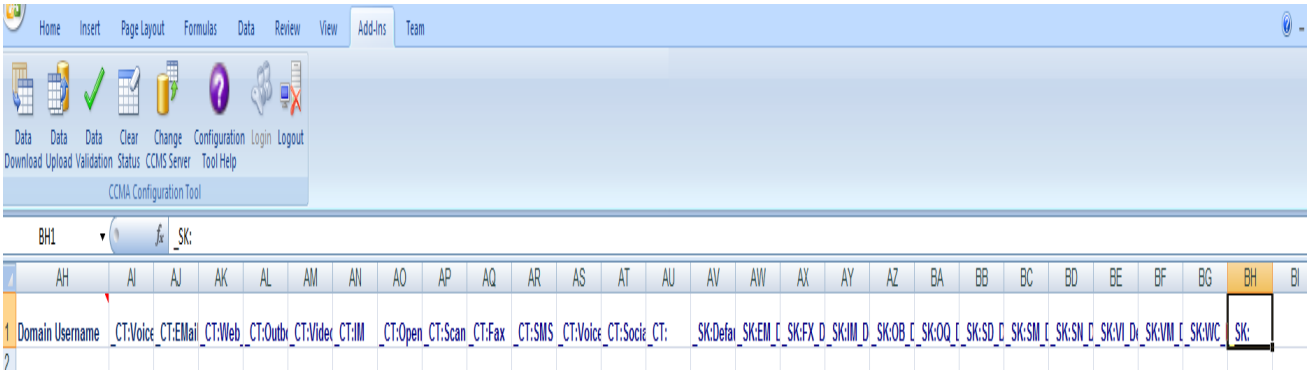
This Login button will do 2 tasks:

1. Login to CCMA Server.
2. Automatically download headers of User sheet (including all Contact type names and Skillset names that the selected CCMS is having). Then, an info message will be shown to inform user that headers have been updated:





That means, after Login successfully, user has all headers available in Users sheet:



Since then, user do not need to manually input headers any more. To test uploading, user just input value under headers as usual.

SWITCH SOFTWARE SUPPORT

Avaya IP Office Software

This section outlines the software requirements for the Avaya IP Office communications infrastructure

Avaya Contact Center Select 7.1 supports integration with the following:

- Avaya IP Office 10.1.7
- Avaya IP Office 11.0 Feature Pack 4
- Avaya IP Office 11.1

Phone Compatibility updates with Avaya IP Office 10.0

Phone Compatibility
Digital 5400 series are not supported with IPO 10.0 or later
Digital 4610/4620x series and 5600 series is not supported with IPO 10.0 or later
IP Phones 1120e and 1220 are supported when running IP Office Release 10.0 or later SIP firmware.

Avaya Session Border Controller for Enterprise support

AACC supports Avaya Session Border Controller for Enterprise(SBCE) 7.2, 7.2.1, 7.2.2, 8.0, 8.1, 8.1.2, 10.1

Secure Access Link support

AACC supports Secure Access Link(SAL) 3.3, 4.0

PLATFORM VENDOR INDEPENDENCE (PVI)

Hardware Requirements

For Single Server deployments of, Voice and Multimedia with Avaya Media Server with/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 with/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 Information

All Avaya Contact Center Select 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 ACCS on a Windows Server platform. A single box solution where ACCS 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 (Feb 2022). Patch Bundle contains a number of critical compatibility fixes and must be applied on all Windows Server 2019 ACCS installations. The Server OS guidelines listed in the ACCS 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

Important: Windows 7 and 8.1 have passed final Extended Security Update Year 3 as of Jan 2023, so they are not supported by AACC 7.1.2.1.

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 Hyper-V installation ships with the most recent RHEL security updates as of GA. Avaya supplied 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.

VMware Horizon View VDI

Avaya Agent Desktop and Workspaces supports the following VDI infrastructure:

- VMware vCenter, Release 5.0 or later
- VMware Horizon View, Release 5.2 or later
- VMware Horizon View Client for Windows, Release 5.2 or later.

Citrix VDI

Agent Desktop and Workspaces is supported only with the following versions of Citrix server:

- Citrix XenApp 6.5
- Citrix ZenApp and XenDesktop 7.x
- Citrix Virtual Apps and Desktops 7.x

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. **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.
2. This KB is contained in KB2975719 (see below)

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 ACCS 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
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 Contact Center Select 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 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 “Deploying Avaya Contact Center Select Software Appliance dated April 2022.
Follow the instructions in Chapter 17: Customizing the solution 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 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" (page 31 – Configure local PCs) or “Internet Explorer mode and Compatibility View configuration on the domain server” (page 35 – Configure domain server for PCs).

The important note is you can disable Internet Explorer 11 browser but cannot remove the Internet Explorer 11 browser from your computer (Windows 10) or your server (Windows 2012, Windows 2016 and Windows 2019) as the IE engine is used by IE mode, otherwise Microsoft Edge cannot launch CCMA.

Windows 11 Pro 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 Contact Center Select 7.1.1.0 is not dependent on a specific version of Microsoft .NET Framework. This release supports Microsoft .NET Framework 4.6.2 through 4.7.x

Windows 11 Pro Support Only

Windows 11 Pro is supported starting from 7.1.2.1 Post GA Patch Bundle (March 2023) 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 Pro also.

VMware Support

Avaya Contact Center Select 7.1.1.0 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 7.1.2.1 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 Contact Center Select 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 to or after the upgrade to 7.1.x.x will result in the loss of functionality, specifically the TAPID link to IPO on Avaya Contact Center Select (if IPO has not been configured to accept TCP connections).

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 IPO, as they will have to be setup to accept the new custom certificates.

Disable Windows Automatic Maintenance

Windows Server 2012 R2

Windows Server 2012 R2and 2016 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 'Enable'

Disable Windows Updates

Windows Server 2012

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 during the Contact Center installation and configuration phase.
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.

Voice & Multimedia Contact Server with Avaya Aura Media Server

Avaya Contact Center Select no longer supports the Avaya Aura Media Server (AAMS) installed co-resident with ACCS on a Windows Server platform. This release achieves a single box solution where ACCS and AMS are running on the same physical server by deploying the AAMS OVA as a virtual server on the Windows Server 2012 or 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 8.0/10.1 is only supported on physical mid-range to high-end servers as defined in Avaya Aura Contact Select Solution Description 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 ACCS 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 ACCS 7.0.2 or earlier, it is necessary to manually backup the AAMS database BEFORE upgrading the ACCS 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 Contact Center Select* user guide.

Orchestration Designer Scripts

Before upgrading you must ensure that all scripts are validated and compile successfully in Orchestration Designer. Default scripts are given as example and must be changed as per customer needs.

Installation

New Installations

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

Install-time Patching

Install-time patching is mandatory for Avaya Contact Center Select 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 ACCS 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 ACCS Release Packs, only ACCS Patches (DPs).

System Backup after Ignition (IMPORTANT)

A full ACCS 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 Contact Center Select Release Pack bundle called the Avaya Release Pack Installer (RPI). This application provides an automated method of updating existing Avaya Contact Center Select 7.x software and must be used when upgrading to this software release.

The application will perform the following actions

1. remove all installed ACCS 7.x.x.x Product Updates (Feature Pack/Service Packs and Patches)
2. remove all unwanted ACCS Third Party software
3. install required Third Party Software for the release
4. install the latest ACCS 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: 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

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

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 Contact Center Select Release Pack bundle called the Update Configurator. This application provides an automated mechanism to deploy and configure the Linux Hyper-V AAMS upgrade and the Avaya Contact Center Select 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

After 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 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 .:\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 MsgBox 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 ACCS 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

Agent Controls Browser Application – Mandatory certificate with IOS 9

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

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 ACCS 7.0 install as contained in Backup. If post install, users migrate a database backup from a previous version of AACS and the Multimedia Database drive defined in the backup does not match the Multimedia Database drive selected during the 7.0 install users will be unable to open attachments that were restored from the backup.

Server Utility - Users.

All customer created desktop users in Contact Center Server Utility have their passwords reset during the upgrade. To update the passwords to the correct values, use Contact Center Server Utility to delete and recreate all of the customer created users.

Avaya Aura Media Server

Avaya Aura Media Server Configuration

The following configuration must be carried out on all AAMS servers (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 >> Network Settings >> General Settings >> SOAP***
5. Add ACCS IP Address into ***SOAP Trusted Nodes***.
6. Hit the "***Save***" button followed by "***Confirm***"
7. Browse to ***System Configuration >> Signalling Protocols >> SIP >> Nodes and Routes***
8. Add ACCs IP Address into ***SIP Trusted Nodes***.
9. 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 ACCS 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

Supporting *Powered by Avaya* Deployment

A new licensing capability is introduced in ACCS 7.0.3.0 to support ACCS deployment in a *Powered by Avaya* cloud environment. *Powered by Avaya* licenses are temporary and expire after 14 days. The licenses are automatically renewed 3 days before the licenses expire. The new licensing capability provides the mechanism to force ACCS License Manager to load the renewed licenses.
A new configuration field is introduced to the configuration tab of **License Manager Configuration Tool**. The *Reload Before Expiry (Hours)* field defines when the license reload will occur. The new configuration field is present for all deployments. The default value in the field is zero. The zero value indicates that the reload is not enabled. To enable the capability, the value in the field must be greater than zero. As licenses are renewed 72 hours before expiry, an appropriate value will be less than 72 hours.

WebLM

WebLM provides Contact Center licensing in an ACCS deployment. A WebLM instance is available as part of ACCS. 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 ACCS deployment platforms and all ACCS 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 Business Continuity deployments, configure the managed IP address lower than both the active and standby IP addresses. Managed IP address configuration is effected using the Business Continuity configuration utility.

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 ACCS 7.1.0.0 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 *Administering ACCS* 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.

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 CONTACT CENTER SELECT

Deployment

This release makes the Workspaces feature available on Avaya Contact Center Select. Workspaces on ACCS is deployed as a Kubernetes single node cluster in virtual deployments, and as a multi node cluster in physical deployments.

Important: At least 1 NTP server is required (maximum 3) starts from 7.1.2.1 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

    Note: Avaya Workspaces HA supplementary server must have Hyper-V feature enabled prior running installation if Hyper-V would be used as virtualization.

- **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 or 255.255.255.192 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

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 7.1.2.1 DVD and verify checksum
4. Download the AACC 7.1.2.1 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. Download the ACCS 7.1.2.1 Release Bundle and verify checksum
2. Extract all 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, if not selected by default choose the option to install Workspaces, providing the required input (if not already selected)
5. Also, while running the Avaya Release Pack Installer, install all 7.1.2.1 GA patch bundles available

6. **Reboot** system when prompted
7. Perform post deployment configuration as detailed in section 'Post-Deployment' and 'Post-Installation Configuration' sections below.

Maintenance – Fresh install

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

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

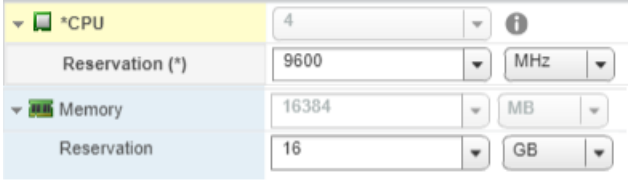
- **Workspaces Cluster Provisioning**
  - For virtual deployments, users must manually deploy a single system using the provided OVA, **prior** to installation or upgrade of Contact Center

  - **Important:** if performing an upgrade from a previously configured Workspaces installation, you must deploy a **new** cluster machine using the OVA which is shipped with this release. The machine created from the OVA 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 the VMWare cluster machine via the provided OVA, the Workspaces 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

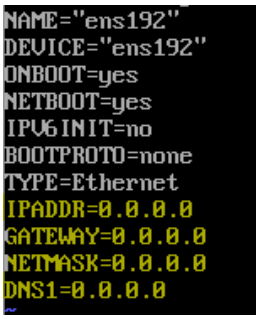
Pre-Installation Steps

1. Review section *Virtual Pre-Install Checks* above
2. Manually Deploy Cluster Machine using provided Workspaces OVA
   - Using you preferred VMWare client (vCenter/ESXi Web Client) deploy the Workspaces OVA
   - As a suggestion (you may choose whatever name you prefer) name the created virtual machine as wsk8master
   - During deployment of the OVA, ensure the 1TB 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:



3. Manually Configure the OVA onto the Network
   - Log into the 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 the wsk8master VM is in a running state and pingable, via IP address, from the Contact Center Windows server

Fresh Install

1. Download the AACC 7.1.2.1 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 7.1.2.1 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 7.1.2.1 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 re-run.

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 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 ACCS 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_7.1.2.1.*.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 ACCS 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 ACCS 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 ACCS 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.

Launching Workspaces

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 ACCS Advanced Administration guides. 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.

Workspaces with ACCS Business Continuity

Avaya Workspaces supports Avaya Contact Center Select Business Continuity for fault tolerant and resilient contact center solutions. To configure Workspaces with Business Continuity, you install and configure Workspaces separately on **both** ACCS servers to provide two independent Workspaces clusters.
Please refer to the customer documentation for further details.

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.

How to restart a Workspaces cluster

Virtual Environment Deployment

- Login to vCenter
- Power down the master node in Workspaces Single Node Cluster
- Power up the master node
- Login to the master node and run the command "kubectl get nodes"

- Verify that the master node is “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.

Troubleshooting Stuck Workspaces Agents Using the Agent Cleanup Tool (CC-46529, CC-46923)

This section outlines the procedure for using the Agent Cleanup Tool to resolve issues where Workspaces agents become stuck during login. The tool enables supervisor agents to remove stale session data, allowing affected agents to log in and resume normal operations.

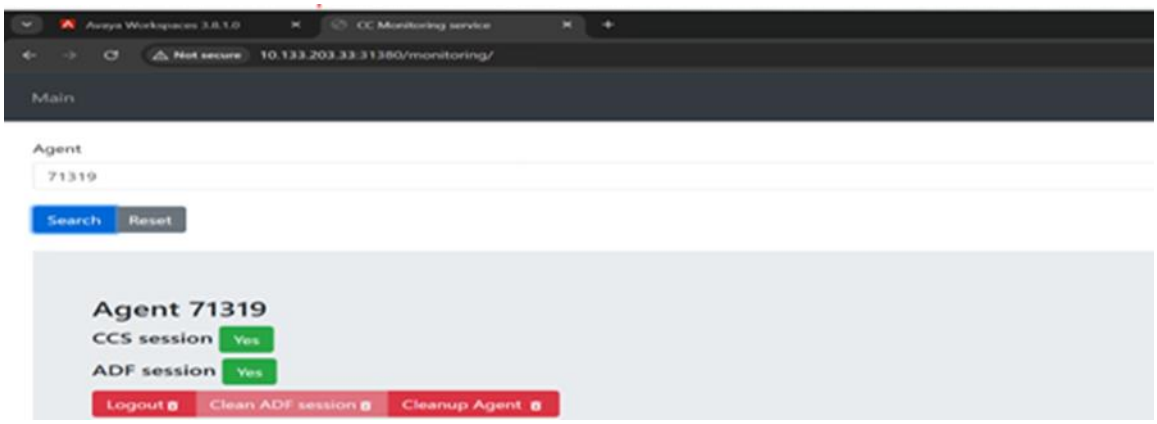
Prerequisites

Before using the Agent Cleanup Tool, the AACC lab administrator must apply the following patches to the AACC server(s) using the hot patching method:

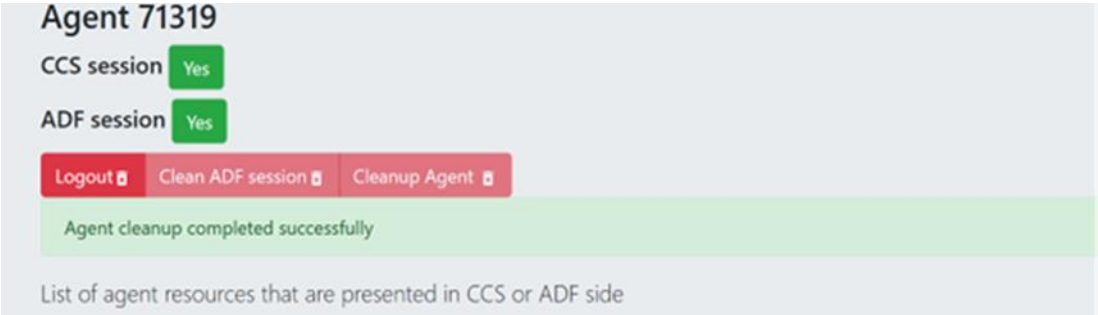
- AvayaCC_CCMM_7.1.2.1.25
- AvayaCC_WS_7.1.2.1.22

Cleanup Procedure

1. **Login and Activation**: Log in to Workspaces using a supervisor agent account responsible for performing the cleanup. Ensure the supervisor agent is activated.
2. **Access Monitoring Service:** Open a new browser tab from the same session and navigate to the Monitoring Service URL: http://<Cluster_IP>:31380/monitoring/



3. **Search for Stuck Agent:** Use the search functionality to locate the affected agent by their Agent ID (e.g., 71319 as shown in the above image). If the agent ID is found, the session details will be displayed along with the **Cleanup Agent** button.
4. **Initiate Cleanup:** Click the **Cleanup Agent** button to begin the cleanup process. The button will be temporarily disabled while the operation is in progress. Upon successful completion, a confirmation message—**"Agent Cleanup completed successfully"**—will appear for 15 seconds. Afterward, the message will disappear and the button will be re-enabled.



5. **Post-Cleanup Validation:** Once cleanup is confirmed, the supervisor agent should instruct the affected agent to log in again and verify that they can perform standard tasks such as login, activation, starting work, and handling interactions.

Important Notes:

- If the above patches are installed, running the **Repair Topics** script is not required, as the patches include cleanup functionality for stuck agents.
- If the issue persists despite using the Agent Cleanup Tool, the administrator should execute the **Repair Topics** script as a final remediation step.

SECURITY INFORMATION

Avaya Contact Center Select security certificate migration considerations

Migrating security custom security certificates has caveats that require planning and consideration before beginning the process.

Migration from 6.4 to 7.x

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

The only path available when moving to ACCS 7.x from ACCS 6.4 is the creation of a new store on the ACCS 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 ACCS 6.4 can be migrated to ACCS 7.x

Migrating ACCS Security Store for ACCS 7.0 to 7.x.x

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

Note: ACCS 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.

Name of Server is important

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

Note

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

Restoring Certificate store to a new system

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

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

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

Note

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

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

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

Upgrades

From 7.0.3.0, 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.

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

For upgrades this new TLS v1.2 default setting may have an impact on any legacy applications that consume ACCS services that cannot support this level of TLSv1. To allow backward compatibility with older releases and applications that consume ACCS 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 ACCS 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 and CTI Traffic

This covers all SIP and CTI traffic to and from the ACCS server. This is configurable via Security Manager Security Configuration tab.

For non-mandatory TLS SIP connections

The servers that can make up the solution may be configured to secure their connection to the ACCS server and so below are the compatibility tables for the different versions that may be used in the solution.

IP Office releases	See Appendix C – IP Office 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 removal

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

Fresh installations

On fresh installations, AACC/ACCS will not install VC++ 2008 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 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 Contact Center Select 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, Korean and Italian.

Overview of I18N and L10N Products & Components

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

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

ACCS 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

Refer to Chapter 24: Language support fundamentals in the Avaya Contact Center Select Advanced 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	JA	RU	KO	
	English	Y	Y	Y	Y	Y	N	N	N	N	Y
	Any 1 Latin1 language	Y	Y	Y	Y	Y	N	N	N	N	Y
	Simplified Chinese	N	N	N	N	N	Y	N	N	N	Y
	Japanese	N	N	N	N	N	N	Y	N	N	Y
	Russian	N	N	N	N	N	N	N	Y	N	Y
	Korean	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	ACCS Server
	Browser Language Preference	**Client Windows Support**	**Server Windows Support/ Regional Options Configuration***
French	fr-FR	French Windows 10 and 11	French Win 2012 R2. Regional option default (French)
German	de-DE	German Windows 10 and 11	German Win 2012 R2. Regional option default (German)
LA Spanish	es-CO	LA Spanish Windows 10 and 11	Spanish Win 2012 R2. Regional option default (Spanish)
Simplified Chinese	zh-CN	Simplified Chinese Windows 10 and 11	Simplified Chinese Win 2012 R2. Regional option default (Simplified Chinese)
Brazilian Portuguese	pt-BR	Brazilian Portuguese Windows 10 and 11	Brazilian Portuguese Win 2012 R2. Regional option default (Brazilian Portuguese)
Russian	ru-RU	Russian Windows 10 and 11	Russian Win 2012 R2. Regional option default (Russian)
Italian	it-IT	Italian Windows 10 and 11	Italian Win 2012 R2. Regional option default (Italian)
Japanese	ja-JP	Japanese Windows 10 and 11	Japanese Win 2012 R2 Regional option default (Japanese)
Korean	ko-KR	Korean Windows 10 and 11	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 ACCS 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 ACCS 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 コプタ to a skillset called EM_Test do the following:

1) Create a DOUBLE byte keyword

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

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

- Start the Rule Configuration Wizard.

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

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.

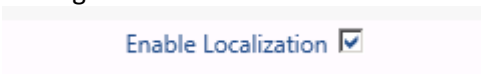
e.g. Wildcard use たば* is correct. Wildcard use た*た is not correct.

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://<Avaya Contact Center Select 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://< Avaya Contact Center Select 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 = i

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.

Start OCMT from CCMA to download the latest OCMT files from the CCMM server.

KNOWN ISSUES

Hardware Appliance

None

Software Appliance

None

Installation

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_7.1.2.1.0.84 Install fails blocking upgrades and new installs of 7.1.1

Tracking Number	CC-22997
Application	Universal installer/ARPI
Description	AvayaCC_CCCC_7.1.2.1.0.84 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

Customer certificates for EmailManager lost after upgrade to AACC 7.1.1.

Tracking Number	CC-23936
Application	Ignition Wizard
Description	The issue observed after upgrade to AACC 7.1.1 since java upgraded as well. During the java upgrade procedure, the old java binaries removed along with the default java Keystore (cacerts) and replaced with a new one. All certificates from the default java Keystore removed as well. It affects only the EmailManager service which can keep customer certificate into the default java Keystore (not mandatory). All other certificates located in the AACC Keystore.
Impact	EmailManager customer certificate can be lost after upgrade to 7.1.1.
Workaround	Need to load EmailManager certificate to the default java key store after upgrade to 7.1.1.

Custom E-mail manager config get overwritten during AACC/ACCS upgrade to another release

Tracking Number	CC-23972
Application	Email Manager
Description	Custom changes in mailservice.properties(D:\Avaya\Contact Center\Multimedia Server\Server Applications\EMAIL\mailservice.properties) file will be lost during AACC/ACCS upgrade to another release or during CCMM patche installation.
Impact	Some Email Manager features may not work as expected
Workaround	Need to backup mailservice.properties(D:\Avaya\Contact Center\Multimedia Server\Server Applications\EMAIL\mailservice.properties) file before upgrade to another release or CCMM patch installation. After upgrade/installation custom changes should be moved to new mailservice.properties manually. Email Manager service should be restarted.

Workspaces Agent security settings are reset on upgrade

Tracking Number	CC-24198
Application	Workspaces
Description	Workspaces Agent Security settings in Kubernetes cluster are reset during every upgrade or after WS HA deployment using WorkspacesHAConfigurator. The problem is that CCMM Database preserves only Agent Security checkbox (enabled/disabled) but not certificate/key. As a result during upgrade, CCMM can't push security settings to K8s cluster together with other settings.
Impact	Workspaces Agent Security settings are lost after upgrade to 7.1.2.
Workaround	Re-apply Agent Security settings

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_7.1.2.1.2.1_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 ACCS

After VHDX failure & Recovery, Agents unusable without intervention

Tracking Number	CC-19714
Application	Workspaces
Description	After VHDX failure & Recovery, agents appear logged in and ready on Workspaces but are unusable. Workspaces displays a red dialog indicating User Authentication required
Impact	Agents unusable without intervention
Workaround	Relaunch browser which brings you to the Authentication page (this may also bring you straight to Ready page). Authenticate agent if required. After authentication you are back at partial ready screen. Eventually this will go to “full ready” (status bar is solid Green). Attempt to toggle state to Not Ready. User Request fails but you will automatically be put back to Start Work Screen. Clicking Start Work will bring you Not Ready. At this point you can toggle to Ready and handle contacts.

Exiting Workspaces when using HTTPS presents error page

Tracking Number	CC-19087
Application	Workspaces
Description	Logout Agent from Workspaces https returns connection error page

Impact	Workspace does not automatically return to login page after agent exits
Workaround	To login, agent need to refresh Workspace https URL from browse

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

Contact represented to agent within 3 seconds

Tracking Number	CC-19080
Application	Workspaces
Description	Contact with same Id not displayed if created within 3 seconds of original contact
Impact	Agent will go not ready and contact will get presented to next available agent
Workaround	None

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.

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.

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
Workaround	RTD can be used instead

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

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	None

The list of agents is truncated in the My Agents widget after the Supervisor observed Agent

Tracking Number	CC-22488
Application	Workspaces
Description	The list of agents is truncated to 10 agents in My Agents widget. It can happen after accepting incoming interaction by the supervisor or after start observing an agent.
Impact	Supervisor cannot see the complete list of agents in the My Agents widget.
Workaround	Restart workspace’s page in browser.

Workspaces - Agents can close the OB contact when the call is not released

Tracking Number	CC-22634
Application	Workspaces
Description	Agents can close the Outbound contact whithot making a voice call to the client or close the OB contact while the call is in progress.
Impact	Agents can close the OB contact when the voice call is not released in the Workspaces.
Workaround	None

Workspaces - Historical Report is displayed incorrect data when the Outbound contact working on Workspaces

Tracking Number	CC-22308
Application	Workspaces
Description	The statistics about voice calls in Outbound campaign contains incorrect data in some cases.
Impact	The Historical Report contains incorrect data about voice call parameters (DialTime, TalkTime, etc.)

Workaround	None

Workspaces - The “No results found” message overlaps both buttons “Search” and “Add more search parameters” in Multimedia Contact Search.

Tracking Number	CC-22628
Application	Workspaces
Description	When Multimedia Contact Search widget gives no result and “No results found” message is displayed, both buttons “Search” and “Add more search parameters” are not working.
Impact	Impossible to push “Search” and “Add more search parameters” buttons
Workaround	“Search” and “Add more search parameters” buttons are active only in their upper part.

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 ACCS 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 ACCS 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.

When a consult call is initiated from AAD, call first presents to the consulting agent. Only when answered, the consult call is finally initiated

Tracking Number	CC-17612
Application	SGM
Description	When a consult call is initiated from AAD by an agent using SIP endpoint (hard phone or Equinox), the call first presents to the agent that initiated the consult. Only when that call is answered, is the consult call presented to the target agent / CDN.
Impact	There does not seem to be any impact to any of the applications, just that this behavior of consulting agent having to answer the call first leads to confusion for the agent.
Workaround	Initiate the consult call directly from the phone set.

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 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

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. 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	Users already configure SSO and enable SSO. When they upgrade their system to 7.x.x GA and they do not need to have any further configuration for SSO after the upgrade, Workspaces, SCT, ADD and OD will fail to connect CCMA (Fail to active agent in Workspaces)
Impact	SCT, ADD and OD are failed to connect CCMA or Fail to active agent in Workspaces
Workaround	The workaround is to disable SSO and 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	User does not understand the guideline of 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 on 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 Windows 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

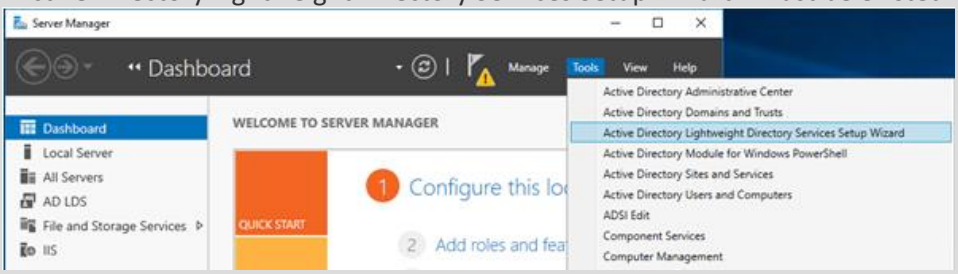
After migrating from NES 6.0 or NES7 to AACC SIP 7.1 Windows 2016, cannot find "IceInstallADAM.vbs" when upgrading CCMA data

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

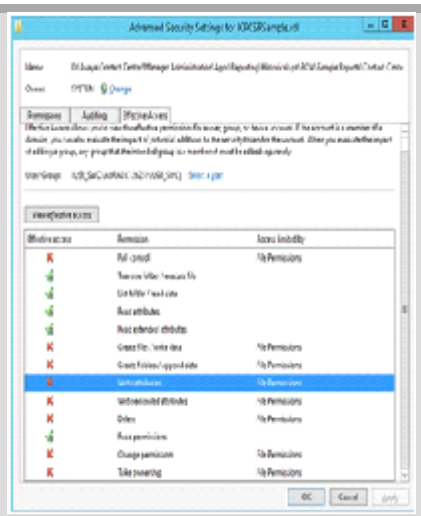
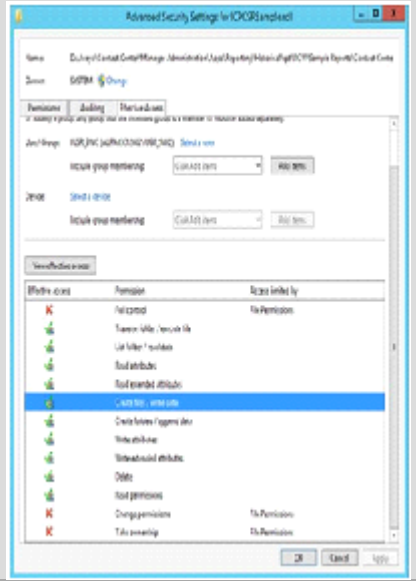
Tracking Number	CC-18904
Application	Contact Center Manager Administration
Description	Users cannot add a Media server name with FQDN name that its length is larger than 30 characters into CCMA Media Servers Configuration
Impact	Prompt Management
Workaround	Add Avaya Aura® Media Server to CCMA Media 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 issue.

	 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) 

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 to 7.1

Tracking Number	CC-20517
Application	Contact Center Manager Administration

Description	Private reports and scheduled jobs are not migrated from 6.4 to 7.1. 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 brower, 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
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	KB5012643 (OS Build 22000.652) Preview - Windows 11

CCMA ERROR Could not get text Table = A Index = N for many labels

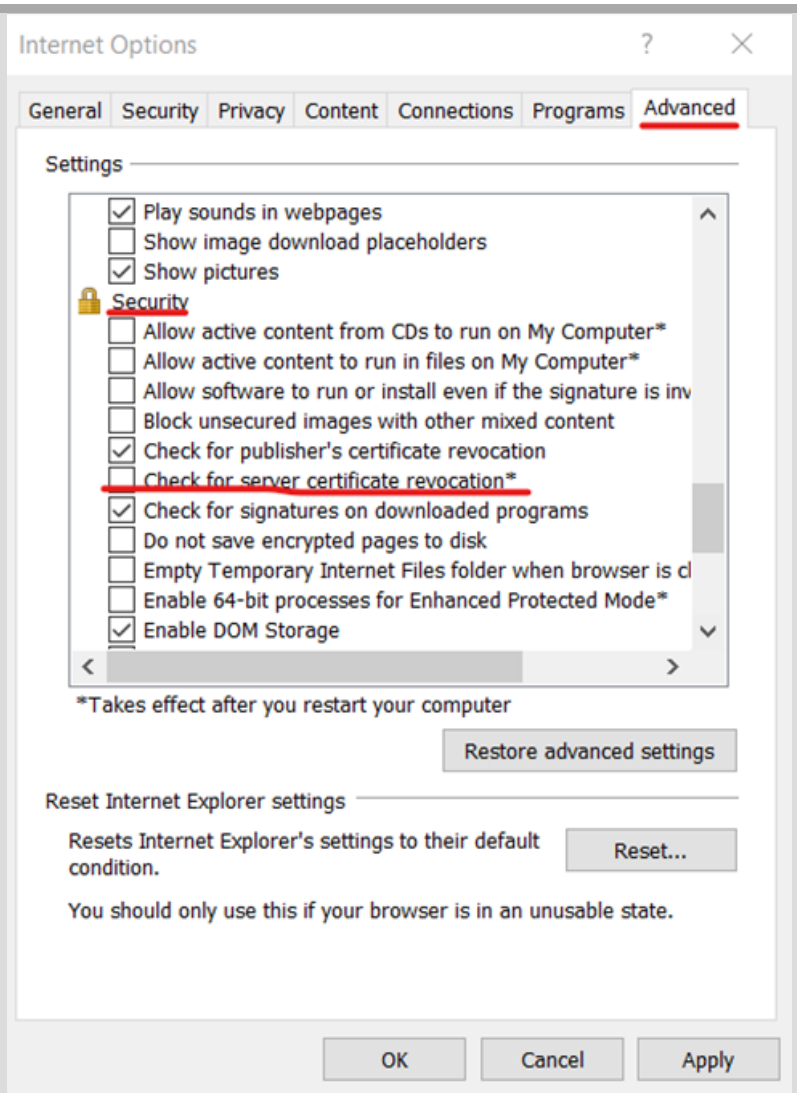
Tracking Number	CC-26193
Application	Contact Center Manager Administration
Description	Issue "CCMA ERROR Could not get text Table = A Index = N, Language = L" appears whenever we try to access the CCMA webpage
Impact	CCMA web pages
Workaround	Try the following command. The command will clear all indexes and install them again: 1. Make sure AllText.mdb file exists at <ccmainstalldrive>\Avaya\Contact Center\Manager Administration\Server\TextXlater 2. Open command line and navigate to <ccmainstalldrive>\Avaya\Contact Center\Manager Administration\Server\bin\ 3. Run command as follows : AccessToInterSystems -install ALLTEXT 4. Stop/Start CCMA services and test the issue again.

CCMA Administrator password reset after upgrade

Tracking Number	CC-26180
Application	Contact Center Manager Administration
Description	ACCS server is upgraded from 7.1.2 or older releases, the password is changed from Administrator password to webadmin but the issue cannot be duplicated at CCMA lab
Impact	CCMA Login
	Run the following SQLs (the password is webadmin) update APM.ccmUser set Password='5767142366101EB6' where UserID=10000

The setup.exe file from CCMM Outbound or Multimedia is failed to launch

Tracking Number	CC-26425
Application	Contact Center Manager Administration
Description	The setup.exe file from CCMM Outbound or Multimedia is failed to launch when security is on (https)
Impact	CCMA Outbound and Multimedia
Workaround	The work-around is to disable the following property from Internet browser: Internet options -> Advanced -> Security Settings -> Check for server certificate revocation (Do not select “Check for server certificate revocation”)



For RGN server, please open a windows cmd and run the following commands at target folders on RGN server. Replace <RGNservername> with your RGN server.

For CCMM Outbound:
D:\Avaya\Contact Center\Multimedia Server\Outbound Client>setup.exe -url=https://<RGNservername>/ocmt

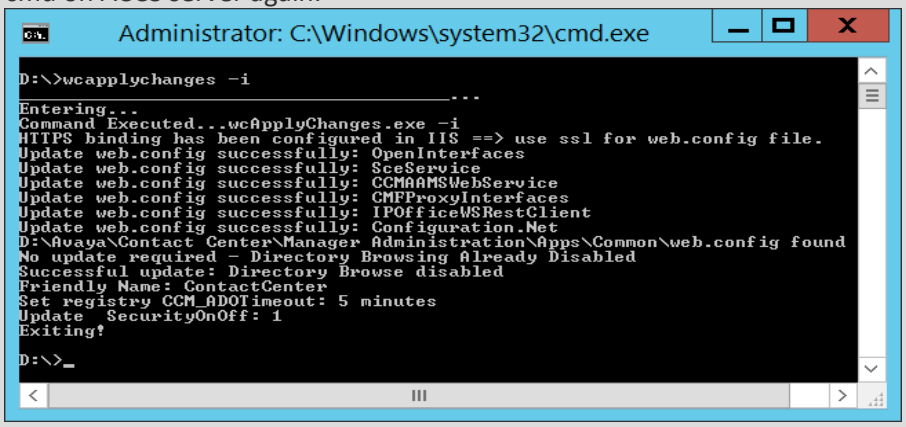
For Multimedia:
D:\Avaya\Contact Center\Multimedia Server\Server Applications\WEBADMIN>setup.exe -url=https://<RGNservername>/admin

For Data Management:
D:\Avaya\Contact Center\Multimedia Server\Server Applications\ARCHIVE>setup.exe -url=https://<RGNservername>/ccmmarchive

Agents not visible under supervisor filter

Tracking Number	CC-26368
Application	Contact Center Manager Administration
Description	Standard Agent Display shows 4 agents instead of 9 agents after applying the supervisor filter
Impact	CCMA RealTime Agent Displays
Workaround	The root cause is the RTD cache does not match with DB because OAM Agent supervisor channel with icertdservice had problems and OAM Toolkit could not notify agent changes to CCMA icertdservice. The workaround is to restart icertdservice from SCMU.

CCMA- User cannot deploy Master Content Store after change security

Tracking Number	CC-44524
Application	Contact Center Manager Administration
Description	User cannot deploy Master Content Store
Impact	Prompt Management
Workaround	The workaround is to run the command "wcapplychanges -i" from Windows cmd on ACCS server again.  Make sure AMS FQDN name and short name have been added into the ACCS Windows hosts file.

CCMA logs out user with Access Denied session is invalid

Tracking Number	CC-44480
Application	Contact Center Manager Administration
Description	This issue that only happens when Standby is either fully started or just shadowing (cause of HA startup is unknown at time being), CCMA starts producing "Access Denied. Your session is invalid. This account has been logged in on other client. Please logout and login again." It happens intermittently when user is browsing CCMA pages and user gets kicked CCMA with above error and is not able log back in.
Impact	CCMA Login
Workaround	The root cause is DB returned the last login date which was different the “LastLog field from the security token. The “LastLoginDate” field is not changed until the user logs in to CCMA again (the second login). Applying the solution from https://support.avaya.com/ext/index?page=content&id=SOLN373472&viewlocale fixed the issue.

Date time in left tree and in the content of Historical report are inconsistent fomat.

Tracking Number	CC-26330
Application	Contact Center Manager Administration
Description	If the client user changes the windows date-time default format to 24 hours (AM/PM). The report content will show 24 hours format (AM/PM) but the report tree date-time format on the left hand side always shows the client date-time default format (not AM/PM).
Impact	CCMA Historical Report
Workaround	In this case, printing reports or exporting reports are still OK because the tree is not printed or exported out. The work-around is client PCs need to use the default date-time format (please should not make a custom of date-time format).

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

Tracking Number	CC-5140
Application	Contact Center Manager Server
Description	Installing CCMS Database Patch on a very large database can take up to 23 minutes. This is due to re-indexing of the CCMS database tables with large volume of data in the order of few million rows.
Impact	Longer CCMS patch install time.
Workaround	None

AAD does not display Agent Statistics when security is on

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

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

Tracking Number	CC-13860
Application	Contact Center Manager Administration

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

Loading of agent from database failed

Tracking Number	CC-13265
Application	Contact Center Manager Server
Description	Issue observed on one test server. OAM bridge on startup logs SQL exception and fails to add agents to CMF space. This caused "no devices mapped to session" error in RefClient, similar may be observed in AAAD.
Impact	Agents unable to login or process calls
Solution	Work around applied: 1) Create new agent using CCMA 2) Restart contact center

Main call gets disconnected when a transfer/conference is initiated to another agent using phonebook (for a setup using IPO 11.x & ACW)

Tracking Number	CC-14785
Application	IPO 11.x, ACW, SIP Gateway Manager
Description	On a setup with IPO 11.x with agent using Avaya Communicator for Windows as agent station, the main call gets disconnected when a transfer or conference is completed to agent number selected from AAD's phonebook entry. This issue is not seen when IPO 10.x is used. The issue is not seen when agent uses his phone to initiate the consult call. Also, issue does not occur for ACW on Windows 10.
Impact	The customer call is dropped for the specific case mentioned above.
Workaround	Workaround is for the agent to not use the phonebook entry to initiate the call and instead dial the number manually in AAD or to use his phone to initiate the consult.

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

AAAD – Agent cannot make a DN call out to another agent successfully while the CDN call routed to Agent is ringing

Tracking Number	CC-21748
Application	Workspaces
Description	Agent is unable to initiate an outgoing call from AAAD while CDN call is ringing if the agent uses Avaya IX Workplace as an endpoint
Impact	Agent is unable to initiate an outgoing call from AAAD while CDN call is ringing if the agent uses Avaya IX Workplace as an endpoint
Workaround	As a workaround, the agent can initiate an outgoing call directly from Avaya IX Workplace or use Avaya Communicator as an endpoint

AAEP – Voice Outbound proxy or CTI proxy is sometimes disconnected when attached string data between 355 and 370 chars

Tracking Number	CC-22363
Application	Workspaces
Description	The Voice and CTI links are disconnected to IP Office if AAEP attaches big data (more than 355 characters).

Impact	The Voice and CTI links are disconnected to IP Office if AAEP attaches big data (more than 355 characters). The issue happens only with IP Office 11.1 SP1
Workaround	None

AAEP Bridge transfer, call remains at customer after all agents release a call

Tracking Number	CC-22373
Application	Workspaces
Description	In the scenario where AAEP is used as FrontEnd IVR and performs a bridged transfer to ACCS, when the agent answers and releases the call, the customer is not dropped automatically and remains on the active call.
Impact	The customer appears active on the call even when the agents releases the call. The issue happens only with IP Office 11.1 SP1
Workaround	None The customer needs to release a call manually

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.

Agent unable to terminate an OB campaign call presented

Tracking Number	CC-26470
Application	Agent Desktop
Description	Agent unable to terminate an OB campaign call presented.
Impact	Agent unable to close outbound contact and continue work with next one.
Workaround	Need to enable using E.164 number format on CM.

Agent cannot login to SOA Reference Client

Tracking Number	CC-44495
Application	Contact Center OI Ref Client
Description	With MD5withRSA signature algorithm being deprecated by Java, Digest-MD5 authentication method is not supported
Impact	Agent cannot login to OI Ref Client
Workaround	Replace the following line in D:\Avaya\Contact Center\Common Components\CMF\Config\Soaproperties.xml <AuthMech>Digest-MD5</AuthMech> With the one below <AuthMech>SIMPLE</AuthMech> Then restart Contact Center.

Define configuration Workspaces Log Upload URI at CCMM

Tracking Number	CC-44570
Application	Contact Center Multimedia Administration
Description	It is not clear how to configure Workspaces Log Upload URI at CCMM Admin
Impact	Unable to collect Workspaces Agents' logs centrally
Workaround	Use one of the following value for property CCMM Admin => Workspaces Configuration => General Settings => Log Upload URI. To uload logs to folder D:\Avaya\Logs\CCMM\AADS: https://<CCMM IP or CCMM Managed IP>/agentdesktop/UploadFile.aspx?AgentID=WS&ContactID=ClientLogs&OutboundLocation=D%3A%5CAvaya%5CLogs%5CCCMM%5CAADS To uload logs to folder G:\Avaya\Contact Center\Email Attachments\Outbound: https://<CCMM IP or CCMM Managed IP>/agentdesktop/UploadFile.aspx?AgentID=WS&ContactID=ClientLogs&OutboundLocation=G%3A%5CAvaya%5CContact+Center%5CEmail+Attachments%5COutbound

Agent unable to terminate an OB campaign call presented

Tracking Number	CC-26470
Application	Workspaces
Description	If disposition code configured in OCMT doesn't require outgoing call to the customer then agent should be able to close outbound contact without call.
Impact	Agents are not able to terminate outbound contact without outgoing call
Solution	This issue will be fixed in the next release 7.1.2.2

Preview Outbound call issues solving the error - No outbound call has been attempted if agent changes the dialled number

Tracking Number	CC-26633
Application	Workspaces
Description	Agent should be able to change customer's number in Workspaces after receiving outbound contact and use that number for outgoing call. Analysis
Impact	Agents are not able to change customer's number in Workspaces after receiving outbound contact and use that number for outgoing call. Analysis
Solution	This issue will be fixed in the next release 7.1.2.2

Tool to flush stuck agent session in workspaces

Tracking Number	CC-46529, CC-46923
Application	Workspaces, CCMM
Description	Introduce a dedicated tool within Workspaces for supervisor agents to selectively terminate sessions of agents who are unable to perform any activity due to being stuck. A common scenario includes agents becoming unresponsive following the installation of a new Workspaces patch.

	Executing the "repair topics" script following the installation of a new Workspaces patch results in approximately 90 minutes of system downtime, as it performs a comprehensive cleanup of all agent sessions. This targeted solution eliminates the need to run the broader "repair topics" script across all agents, ensuring that only the affected agents are addressed while preserving the integrity of active sessions for others.
Impact	Workspaces agents may encounter issues that cause them to become stuck during various operations, such as agent login, activation, starting work, and other core functionalities within the Workspaces environment.
Solution	Add a **"Cleanup Agent"** button to the **Monitoring Service** within the **Workspaces UI**, enabling supervisor agents to clean-up session details of stuck agents from the Workspaces data store. To perform the cleanup: • The supervisor agent searches for the stuck agent using their **Agent ID** in the Monitoring Service. • Once the agent is located, the supervisor clicks the **"Cleanup Agent"** button to initiate the session cleanup process.

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-26315	Call was showing in waiting in source site RTD while it was already been abandon
CC-26281	nieb Discarded NIEB_clReturnedFromIVR and call is defaulted in reports during eb audit
CC-26191	relocate the TfeRest logs to the standardized CCMS logs folder
CC-26138	With CC-24906 TfeRestConfigurator is not sending parameters in uri query
CC-26121	Add HAI number of worker threads control to CCMS Serviceability Control Panel
CC-26100	Agent becomes idle when the Break time expires and receive new call, but should remain NOT ready
CC-25994	active calls <30 seconds with agent dropped on AMS switchover
CC-25721	Agents have Multiplicity, but Web Chats are still queueing, despite Agents not reaching Max Multiplicity capacity
CC-26286	AACC 7.1.2 - JQuery vulnerabilities
CC-26168	Workspaces display custom field with question marks(???) when the character is set to Korean
CC-26338	Acquisition fails after agent URI is changed and reverted
CC-25726	7.1.2 - Migrate – Error "Unable to connect to database" display when running file Workflow Application
CC-26190	include the CCMS_HAIW_ODBC log into the Log Archiver
CC-26139	TFE REST parameters lost during CCMS patching
CC-25392	Cache.key missed during installation 7.1.2
CC-26066	Workspaces cluster certificate expiry warning
CC-26110	move renew_certs script
CC-26113	Include renew certs csripts to installer
CC-25452	Fix base versions of CCMS registry
CC-26065	AACC7.1.2 UNE log not archive
CC-26262	ccms.NIServerConfig should contain only supported values of SIPServerType field
CC-26487	ACCS Dashboard - 7.1.2.1 - Status of OpenJDK is missing on ACCS dashboard

CCMA Defect Listing

This list contains defects addressed for the Manager Administration components

WI/JIRA	Summary
CC-25443	CCMA HR- Taking a list of CCMA users should be improved in Historical Reporting
CC-25454	Unable to add CCT data when last name contains special character
CC-25913	WClient_DA_COM's logs shows errors ""Mapping failed"" - EXCEPTION: ElementName

CC-25897	Remove codes of checking RTD cache for loading agents from partitions in case of cores system
CC-25969	RepAgents - Insufficient memory to continue the execution of the program
CC-25985	7.1.2 HR – Username and User ID field in criteria is not displayed in User report of Historical Report"
CC-26048	CCMA 7.1.2 can create new APM user with empty password
CC-26033	Getting Error in the report for Date Field
CC-26003	After AACC was migrated from 7.0.3 to 7.1.2 on new Servers, CCMA-> Historical Reporting -> Scheduled Events is slow to open. Takes 1-2 mins
CC-26082	CCMA - SMGR cannot redirect to CCMA after logging out of CCMA
CC-26142	CCMA Script Variables modified timestamp wrong by 1 hour (after DST change)
CC-25065	Increase Call Request Queue Size Threshold value in CCMA UI
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-26128	CCMA - Multimedia Administration URL is still HTTP
CC-26129	CCMA - Outbound Administration URL is still HTTP
CC-26131	CCMA - Data Management Administration URL is still HTTP
CC-26145	CCMA - Scripting successfully creates a script variable with ACD type in SIP system
CC-25595	CCMA - Password has been expired in Web GUI but user still can login and use SCT
CC-26114	7.1.1 – Section 508 – Cannot use keyboard to select Media's prompts in Prompt Management
CC-26023	7.1.1 - CCMA RepAgent - User ID missing Source
CC-25868	CCMA - 7.1.2 - JAWS tool cannot access to the RTD tree
CC-25980	CCMA - HR - An error log is shown in CCMA_SOAPRptFuncs_1.log file when opening the Users report
CC-24908	7.1.1 – Section 508 – Cannot accessible check/uncheck User Defined Partitions in Prompt Management
CC-24983	7.1.2 CCMA - Logged in user field display previous user name when login CCMA after disabling SSO
CC-25093	7.1.2 CCMA - User Type should not be changed when changes password CCMA from CCM page
CC-25775	7.1.2 CCMA SSRS – Config - Network Site and Application Properties – Network site in GMT -x is displayed as #Error on report
CC-26182	AACC - 7.1.2 Configuration Tool uploads incorrect agent type if the bulk upload has both Supervisor, Agent only and SupAgent
CC-26196	SSO - XML automated assignments not working for AACC German locale on Windows 2012
CC-26219	CCMA - AllText needs to update the text due to IE is officially stopped support
CC-26223	CCMA - About window should update the time
CC-26203	"CCMA IceAssignment" service has issues when AACC reboots because it always starts before Cache service starts
CC-23954	7.1.2 CCMA Administrator user should be able to create Programmatic account
CC-23663	Administrator user should be able to unlock inactive CCMA user
CC-23193	AACC AML 7.1.1 – SCT tool – Unable to upload new users if Contact types and Skillsets headers are not displayed in order
CC-21587	CCMA – CCMA User’s password should not allow change to the same with previous one.

CC-21310	AC/ACW/NNRC displays inconsistently between RTD and Historical Report.
CC-21221	SCT – When uploading an user with MPC_ON for POM contact type, there should be an upload status notifying that it is automatically changed to OFF.
CC-25860	7.1.2 – CCMA – HR – Missing tooltip for properties toolbar in Report Viewer on client Windows 11
CC-25769	7.1.2 – CCMA– RCW – Missing tooltip for properties toolbar on client Windows 11
CC-25737	7.1.2 – RTD – Skillsets are truncated on Skillset chart (choose skillset per statistic) report
CC-26250	When changing Historical Statistics, CCMA page references AACC 6.3 and older document Planning_and_Engineering Guide
CC-25851	7.1.2 - I18N - CCMA User Migration Tool – There is no data displayed on Unassigned CMMA User panel
CC-26198	Historical Reporting - Scheduled Events is slow to open - takes 1-2 mins
CC-26233	Scheduled Events are slow to load in CCMA
CC-26257	CCMA - Outbound/Multimedia/Data Management pages should update the text of Internet Explorer
CC-26282	CCMA Vulnerability: Path-relative stylesheet import (PRSSI) vulnerability
CC-26283	CCMA Vulnerability: Insecure Transport
CC-26352	Bulk Upload tool fails validation if domain contains dot
CC-26252	Contact summary changed to 12h format at 7.1.2 VS 7.1.1
CC-25830	ConfigurationTool shows incorrect Skilset priority when downloading user who has Standby skillset
CC-26112	CCMA - Configuration Tool omits the first record when checking the combo of Windows Password, Domain and Domain Username
CC-26477	CCMA - Increase Call Request Queue Size Threshold value in Configuration Tool
CC-26437	CCMA RTDs stopped working (Increase the cache time out value of SOAPICERtdService to 5 minutes)
CC-26497	CCMA - CCTProxyInterface web service gets ERROR "The operation has timed out" when there is a big number of CCT Users (>5000 users)
CC-26502	CCTProxyInterfaces should be improved to prevent AAAD auto login failing for high agent counts
CC-26549	7.1.2.1 CCMA GA patch bundle 1 is created to include some critical fixes
CC-26553	7.1.2.1 - Need to remove jquery-1.10.2.js from PwdMain.asp
CC-26556	After AACC was migrated from 7.0.3 to 7.1.2 on new Servers, CCMA-> Contact Center - Manager ->Assignments -> Scheduled Events is slow to open. Takes 1-2 mins

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
CC-25939	AACC WS duplicated agent in supervisor My Agents widget
CC-25855	F12 key issue in the new AAAD 7.1.2 with edge as embedded browse
CC-26062	AAAD Deafult tab stuck in "Details"
CC-25468	Email template was disappeared when reload CCMM
CC-25967	Issue with AgentEmailWS.ForwardWithAttachmentsHtml
CC-26060	FindContactsByCustomField SOAP query fails (Outbound Contact Web Service)
CC-26059	CCMM OI error occurred trying to analyse customer wsdl
CC-26012	AACC Duplicate emails
CC-26042	Outbound email is not send after updating to AACC 7.1.2
CC-26092	Unsent emails intermittently stop sending
CC-26101	AAD not connecting after failover to RGN
CC-26106	Avaya Aura Agent Desktop (AAAD) client will not install if pre-requisite WebView2 version 100 or greater installed
CC-26122	Function keys not working @AAD 7.1.2 at advanced screenpops as it was working at 7.1.1
CC-26126	Webchat transcript in plaintext not showing hyperlink
CC-26125	Emails not sent when Friendly Name contains a comma
CC-26123	AAAD client have CRM page as home and its not working since its failed on silent authentication
CC-26151	Home page tab can not be closed or reloaded after right click on tab
CC-26164	Shortcut keys are not working when agent is focus on the Home page
CC-26215	Unable to see signature content on Email signature Editor
CC-26197	Emails not being downloaded, not persisted to the database
CC-26229	scheduled callbacks not dialing automatically
CC-26184	Percent sign (%) at middle of recipient E-mail address, cause E-mail manager to stop sending outgoing E-mails
CC-26222	Emailmanager starts using TLS for server even no encryption set for that in CCMM Admin
CC-26216	ProviderContactID case sensitive issue
CC-26260	CCMM admin url ca not to be changed to https
CC-26235	Problem with linking the URL to image in AAAD's signature editor
CC-26280	ReplyTo field ignored and field from used when MS Graph is enabled
CC-25954	Log4Net CVE-2018-1285 vulnerability at AAAD
CC-26127	AAD CallBack missing Re-Schedule button after a OB Call. Ok after restart of AAD
CC-26178	Checkmark Chat session to survive a webpage refresh do not work as suppose to

CC-26306	MS graph CCMM component has only error log level, which is not enough for troubleshooting
CC-26120	tomcat application possible memory leak at CCMM server
CC-26346	Cache should change URL in setup.exe after enabling/disabling security
CC-26372	Outbound SMTP server with STARTTLS doesn't work
CC-26354	AAD History tab launches attachment links in IE, regardless of user's default browser
CC-26389	OCMT is unable to start if HTTP port 80 is unavailable
CC-26363	Unable to unhold the chat
CC-26376	Percent character in TO field causes all outgoing email to stop
CC-26355	inbound email stops due to java.lang.OutOfMemoryError: unable to create new native thread
CC-26423	mailboxes O365 not functioning EMM terminations and EMM blocked threads detected
CC-26447	implement MSGraph for Voice mail, fax, SMS, SN contact types
CC-26462	EMM blocked thread detected Caused by: java.lang.NullPointerException at getNestedMessageAsText
CC-26463	EMM blocked thread detected - ErrorInvalidRecipients caused by recipient having SPACE character Open
CC-26446	E-mail managers exception causing to stop processing e-mails
CC-26453	E-mail attachment can't be retrieved and stored due to Exception: java.lang.StringIndexOutOfBoundsException
CC-26398	EMM Add proxy configuration for the Microsoft Graph client
CC-26481	AACC is not initiating connection to certain mailboxes if the handle is duplicated
CC-26398	EMM Add proxy configuration for the Microsoft Graph client
CC-26473	AAAD appears to hang on text email with URL when spellcheck Always run before sending is enabled
CC-26491	AAD auto login to CCMM fails
CC-26503	Outbound e-mail stopped after CCMM_7.1.2.0.63 was installed
CC-26546	Unable to load web chat transcriptions
CC-26493	Possible to remove proxy server which associated with OAuth2.0 credentials
CC-26478	Screenpop External applications cannot open when agent receives a contact
CC-24749	Custom Field of OCMT
CC-26563	Customer original email address is not showing in mail body in History tab
CC-23354	Workspaces – Multimedia contact search - Missing data on content of closed OB contact when view contact history

CCT Defect Listing

This list contains defects addressed for the Communication Control Toolkit components

WI/JIRA	Summary
CC-25259	Subscriptions to EWC notifications leak out
CC-25009	7.0.2.0.11 code propagation
CC-25068	Workspaces webchat input textbox disabled after 3 minutes inactivity
CC-25150	Garble char in Thai and Chinese message
CC-23538	The activity code is not updated while call

CC-25816	request to make configurable monitoring for LogoutVoiceOnlyAgentWithUnregisteredDevice
CC-26116	Agent is able to login to web agentcontrol with incorrect password
CC-26179	IIS memory usage consumption by IntegrationPortal App Pool
CC-26210	Workspaces agent cannot change status after switchback until standby is started
CC-26205	Workspaces agent cannot change status after standby was started at switchback
CC-26289	Webchat contact will stuck at routing state then agent PC loose
CC-26456	Configuration of OI webservice with TLS 12 fails due to TLS handshake inconsistency
CC-26545	CCS Clients reporting wrong password as network error

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-25794	Log4j Vulnerability CVE-2021-44228
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"
CC-25936	WS Monitoring Service is not functional to remove stuck interactions
CC-26010	7.1.1 Workspaces Section 508 Agent is not notified on Jaws tool and cannot use scrollbar when opening the Notification list on Agent Toolbar
CC-26069	the screen reader reads all the content in the window or it reads About tab when that is not what is focused
CC-26071	all the contents of the modal are spoken by the screen reader
CC-26073	Workspaces Accessibility - Tooltip should be shown per element focusing
CC-26074	7.1.1_Workspaces_sestion 508_ The Jaws pronounce card info with double speech
CC-26075	Setting Panel-- Panel name is "About" instead of "Settings"
CC-26077	Sidebar Active Button Indication using Color
CC-25585	Workspaces – Section 508 – Jaws should read out the information of record and focus on the redial button to make call from Interaction Log
CC-25870	Workspaces - Section 508 – JAWS should read out meaningful the action of Expand/Collapse button when press Enter
CC-25644	Workspaces – Section 508 – Jaws should read out the status of channels, time in state on Agent state summary
CC-25912	JAWS pronounses Customer Details instead of Work card label

CC-25889	Workspaces - Section 508_ Jaws tool doesn't focus correctly on the position of keys on DTMF
CC-25805	Workspaces_sestion 508_ The Jaws tool does not read action status when using shortcut key
CC-25847	WORKSPACES UI - Double speech on Tablist (outer div)
CC-25922	Section 508 – There is no alerting for incoming Email or EWC contact and cannot use Enter key to accept them while JAWS is opening
CC-25925	Tooltip displays incorrect role on Team widget
CC-25932	Section 508 - Jaws read User Menu by English instead of selected language
CC-25931	Workspaces – Section 508 – Jaws tool does not read action status on Email or EWC contact when using shortcut key
CC-25924	Session 508 - JAWS read both the previous select tab and ABOUT tab after navigate to Settings widget again using ctrl+alt+, shortcut
CC-25988	Workspaces shortcut key mismatch between Help page and Help Menu for Open Address Book key
CC-25926	Section 508 - Jaws should read out a notification when user sign in failed Workspaces
CC-25846	WORKSPACES UI - JAWS does not convey collapsed/expanded on User Menu
CC-25933	Table header has no association when focus was in the table cell in My Agents Widget
CC-26078	There are two attribute - aria-expanded and aria-label - giving the state which will be confusing for blind users
CC-26094	Multistate components reveal their current status (state/value)
CC-26095	Collapsed state of the control, on initial focus, is not announced
CC-26096	When multiple nested tables are open, they all are named
CC-26097	Ready is not announced when tabbing to the control
CC-26085	Workspaces Suggested content Widget for email not present/not working
CC-26133	My Agent view shows only 10 Agents for Supervisors
CC-26150	Email templates for plain text reply inserting at top instead of cursor position
CC-26143	Agents unable to log in or control workspaces
CC-26171	Email arrival time incorrectly changed to the open time in Workspaces
CC-26074	Sestion 508 - The Jaws pronounce card info with double speech
CC-26162	Sestion 508 - Workspaces Keyboard navigation not working as expected
CC-26163	Sestion 508 - Workspaces - Tab key must read items that are read only
CC-26157	Sestion 508 - Duplicate labels when more than one similar key on workspaces
CC-26161	Sestion 508 - Workspaces Call interaction card - Agent cannot confirm time in any state
CC-26159	Sestion 508 - Consult shown as Conference button is confusing or misleading
CC-26183	Sestion 508 - Filter by State always reads as checked
CC-26325	Workspaces upgrade to HA failing
CC-26323	Double work cards when supervisor barge in contacts.
CC-26324	Workspaces - Missing icon transfer when agent transfer to service
CC-24758	7.1.2 WORKSPACES- Workcard display incorrectly when agent join in a conference after end observe
CC-26480	istio-ingressgateway increase resource limit memory from 200Mi to 1000Mi

CC-25487	An unclear message displays when agent try to send a suggest phrase after session chat between agent and customer is disconnected
CC-26499	WS Worker node ran out of space due to logging - WS Outage

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

For non-mandatory TLS SIP connections

IP Office releases TLSv1 support

All supported IP Office releases currently provide support for TLSv1.0, TLSv1.1 and TLSv1.2.

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
10.1	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 ACCS 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”.

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