Avaya Contact Center Select

Release 7.0 Service Pack 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 Installation and Commissioning guides for full installation instructions

Publication History

Issue	Change Summary	Author(s)	Date
1.0	Release of Service Pack 1	CC Release Engineering	20th July 2016
1.1	Removing references to Agent Greeting which is not supported wih ACCS	CC Release Engineering	28th July 2016
1.2	Updating with support for IP Office 10.0 SP1, phone compatibility and Agent Capacity updates with IP Office 10.0 SP1. ActiveX Controls location and content	CC Current Engineering	1st November 2016

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 7.0 into a virtualization environment. Please ensure you are using this version for all new software installation.

Avaya Aura Media Server OVA

File Name	MD5 Checksum
MediaServer_7.7.0.226_A11_2015.07.02_OVF10.ova	3d476ce8b74efc1bc32e4e45ef1ea141

Avaya WebLM OVA

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

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 AACC lineup above.

The utility is available in:

Install Software\CCMA\RCW_Migration_Utility

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.

DVD Image

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

File Name	MD5 Checksum
ACCS_7.0.0.0-316.iso	c052c95006978a177eeb43be580a7606

Important Note:

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

Service Pack Bundle

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

File Name	MD5 Checksum
ACC_7.0.0.1_ServicePack1-77.1.zip	dde9f8cfba4260392416b319c0d064c2

Additional Required Updates

Avaya Contact Center Select Server

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

File Name	MD5 Checksum
ACC_7.0.0.1_ServicePack01_Patches-261.zip	d8b6204da6d10b6bb5088ed67a1d8dbc

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

Avaya Aura Media Server OVA

The AAMS OVA version is: 7.7.0.226 with System Layer Version 11. Both need to be upgraded to the latest version for the GA installation. The Media Server needs to be updated to 7.7.0.269 and the System layer needs to be updated to 14. This is accomplished by downloading the two ISO files:

MediaServer_Update_7.7.0.269_2015.10.14.iso
MediaServer_System_Update_7.7.0.14_2015.10.26.iso

The procedure: Upgrading GA Avaya Aura Media Server OVA details the steps required to upgrade the AAMS OVA.

File Name	MD5 Checksum
MediaServer_Update_7.7.0.269_2015.10.14.iso	96f5a79bf06d250a051c7440112c9291
MediaServer_System_Update_7.7.0.14_2015.10.26.iso	6c13700de16ea05ed1583a218b1576b7

Additional Optional Updates

Avaya Contact Center Server

The following software update is optional for the Avaya Contact Center.

File Name	MD5 Checksum
ASGPlugin4WindowsX64.zip	76aaa6844a4863a86884d19a0b409558

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

Avaya Contact Center Select Server

The following software update is optional for the Avaya Contact Center.

File Name	MD5 Checksum
ACC_7_0_0_0_SNMP_Trap_File_ver1_0.cnf	3fbc02a8bdf6296fe2c153ced48b0ca9

SNMP Trap Configuration File

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

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

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

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

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

Patch Scanner

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

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

File Name	MD5 Checksum
PatchScanner_1.0.0.16.zip	3f92049e467abca99a9dbd0ef9eefb00

IP Office Software

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

ACCS Release 7.0 and ACCS Release 7.0 SP1 supports integration with

- IP Office 9.1.x, minimum 9.1.4 or later.
- IP Office 10.0 or later.

Agent Capacity

- 250 Agents is the maximum supported capacity for ACCS deployments with IPO 9.x
- 400 Agent support only for ACCS 7.0.x deployments with a minimum release of IP Office 10.0
- Direct Media must be enabled on the SIP Line trunk into IP Office 10.0 to support ACCS 7.0.x deployments of greater than 250 Agents.
- To enable Direct Media support select "Allow Direct Media Path" under VoIP tab for SIP Line Trunk
- New Deployments of ACCS 7.0.x with IP Office must use Direct Media for IP Office SIP line trunk
- Existing deployment of ACCS with IP Office 9.x upgrading to IP Office 10.0 can continue to use Indirect Media on IP Office SIP Line trunk but only up to 250 Agents.
- For ACCS deployments with IP Office 10.0, the maximum supported number of simultaneous call recordings is 400.
- If blanket call recording is required for all 400 Contact Center Agents, then there is no scope to record any other calls.
- IP Office must be configured to ensure that no more than 400 Call Recording resources are consumed concurrently

Phone Compatibility updates with IP Office 10.0 SP1

Phone Compatibility
Digital 5400 series is not supported with IPO 10.0 or later
IP 4610/4620x series and 5600 series is not supported with IPO 10.0 or later

Microsoft Operating System Updates

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

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

Important Notes:

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

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

Important Notes:

1. **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
KB2975719	August 2014 update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2

Important Notes:

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

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

Important Notes:

1. **Important** If you install a language pack after you install this hotfix, you must reinstall this hotfix. Therefore, we recommend that you install any language packs that you need before you install this hotfix. For more information, see Add language packs to Windows.
1. **Important** This KB should only be applied to servers which include Avaya Aura Media Server on Windows Server 2012 R2, i.e. where AACC/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.

Platform Vendor Independence (PVI)

Hardware Requirements

For Single Server deployments of ACCS 7.0 (Voice and Multimedia with Avaya Media Server on a physical platform) a Gigabit Network Adapter is required that supports Receive Side Scaling (RSS) with 4 RSS queues.

Network Adapter known issues

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

Recommended Network Adapter

The following RSS capable Gigabit Network adapter has been tested successfully with ACCS 7.0 Single Server deployments
Intel(R) Gigabit 4P I350-t Adapter

Operating System & Virtualization

Operating System

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)

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

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

Microsoft Service Packs

None.

Microsoft Hotfixes

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

Additionally, please install all required Microsoft Operating System update listed in the

Microsoft Operating System Updates section of this document.

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

Red Hat Enterprise Linux Updates

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

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

Internet Explorer Support

Element Manager and CCMA require that Internet Explorer 10.0 and Internet Explorer 11.0 be configured to run the web sites in “Compatibility Mode”.

Microsoft support indicates that some websites might not display correctly in Windows Internet Explorer 10 or Internet Explorer 11. For example, portions of a webpage might be missing, information in a table might be in the wrong locations, or colors and text might be incorrect. Some webpages might not display at all.

If a portion of the webpage doesn't display correctly, try one or more of the following procedures:

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

To turn on Compatibility View

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

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

Virtualization

Avaya Contact Center Select supports the following virtualization environments using the OVA images supplied:

- VMware vSphere Release 5.0 (ESXi)
- VMware vSphere Release 5.1 (ESXi)
- VMware vSphere Release 5.5 (ESXi)

The deployment Avaya Contact Center Select requires that following OVA images to be deployed:

a) Avaya Aura Media Server
b) Avaya WebLM
   This OVA is required for product licensing in a virtualization environment.

Information on the OVA image software is available in the **Software Appliance** section below.

VMWare Configuration Note

Description	The VMware data store used to store the deployed software appliances must be at VMware Release 5.0 or greater. If your data store is not at this release you must either upgrade it to this level or create a new data store location that supports the required VMware release.

Deployment & Configuration Information

Installation

New Installations

Windows Automatic Maintenance

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

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

To disable Automatic Maintenance:

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

After installation is complete you may re-enable Automatic Maintenance

To enable Automatic Maintenance:

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

Install-time Patching

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

Mandatory Execution of Ignition Wizard – Patch Deployments

After deployment of the Contact Center 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 Contact Center Service Packs, only Contact Center 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.

Upgrading from previous ACCS 7.0 Service Pack lineup

All installed Service Packs and Patches must be removed before installing ACCS 7.0 Service Pack 1

Avaya Contact Center 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 7.0/7.0.1

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

The only path available when moving to ACCS 7.0 from ACCS 6.4 is the creation of a new store on the ACCS 7.0 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 7.0

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

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

Name of Server is important

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

Note

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

Migrating Security Certificates to a new system

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

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

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

Note

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

Backing up the Certificate Store

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

Restoring the Certificate Store

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

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

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

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

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

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

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

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

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

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

Upgrading GA Avaya Aura Media Server OVA

This section provides instructions on how to upgrade the Avaya Aura Media Server OVA from version 7.7.0.226 and System Layer 11 to 7.7.0.269 and System Layer 14.

1. Launch AMS Element Manager.
2. Navigate to EM > Tools > Manage Software > Updates > Upload Updates.
3. Locate the System Layer Update ISO (available from the ftp site, please see section: Avaya Aura Media Server OVA):
   MediaServer_System_Update_7.7.0.14_2015.10.26.iso
4. Click Browse to select the software update to upload this file to the AAMS.
5. Click Upload
   Your browser shows a progress spinner until the upload completes.
   The web page refreshes when the update completes and displays the details of the update including the filename of the uploaded file.
6. Using the cust login credentials, open a Linux shell and run the following command to install the update:
   sysTool --install-update
7. Follow the prompts to complete the installation, after which the AAMS will reboot to complete installation.
8. When the system comes up after reboot, open a Linux shell and logon using the cust account. Type in the following command to verify that the System Update has completed successfully:
   sysTool --status
   Output: System Version : 7.7.0.14
   Original Activation Date: 2015-11-03T04:52-0700
   Staged update : MediaServer_System_Update_7.7.0.14_2015.10.26.iso
9. Locate Media Server Update ISO (available from the ftp site, please see section: Avaya Aura Media Server OVA):
   MediaServer_Update_7.7.0.269_2015.10.14.iso
10. Click Browse to select the software update to upload this file to the AAMS.
11. Click Upload
    Your browser shows a progress spinner until the upload completes.
    The web page refreshes when the update completes and displays the details of the update including the filename of the uploaded file.
12. Using the cust login credentials, open a Linux shell and run the following command to install the update:
    InstallMediaServer
13. Follow the prompts to complete the installation.
14. Logon to AAMS Element Manager and go to System Status->Element Status and verify that the AAMS version is 7.7.0.269

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

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

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

AMS to AAMS Upgrades

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

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

Scripts for Migrations and Upgrades

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

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

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

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

1. Launch ssh session to RHEL server, logon as root user and create a directory:
   mkdir /tmp/AvayaMS
2. Copy the script using a file transfer utility (e.g. WinSCP) to the RHEL server. Make sure that the script is transferred in "Text mode".
3. Make script executable by running command: (example prepareForAAMS77migration.py):
   cd /tmp/AvayaMS
   chmod +x prepareForAAMS77Migration.py
4. Run the script by running command (example shows prepareForAAMS77migration.py):
   ./prepareForAAMS77Migration.py

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

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

1. Copy and run the ***prepareForAAMS77Migration.py*** script to the AMS 7.6 RHEL server using procedure: Scripts for Migrations and Upgrades
2. At the "**Please Enter ACC SIP Domain"** prompt, enter the AACC SIP domain name.
3. Uninstall CCSA by running commands:
   cd /opt/avaya
   ./UninstallCCSA
4. At the **"Also remove Avaya Media Server"** prompt, answer '**n**'. Do not uninstall AMS software.
5. Locate the AAMS 7.7 Linux binary on the AACC 7.0 DVD: ***MediaServer_7.7.0.269_2015.10.14.bin***
6. Copy this binary to the /tmp/AvayaMS directory on the RHEL server using WinSCP or equivalent. Make sure transfer is in Binary mode.
7. Run the binary by running commands:
   cd /tmp/AvayaMS
   ./MediaServer_7.7.0.269_2015.10.14.bin
8. At the **Upgrade** prompt, press Enter to accept the default selection.
9. Answer **y** to the License agreement and press Enter at the next **Upgrade** prompt.

The software upgrades to AAMS 7.7.0.269

10. Copy and run utility: ***completeAAMS77Migration.py*** to the RHEL server using procedure: Scripts for Migrations and Upgrades
    The upgrade is complete and the AAMS Content Store now has the required content for AACC 7.0 operation.

AMS 7.5 or 7.6 Migrations to AAMS 7.7

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

AAMS 7.7 supports the following Application Content migrations:

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

The following procedure should be used for all migrations:

1. Locate and run script: prepareForAAMS77Migration.py (or .exe for windows) on the AMS 7.5 or AMS 7.6 RHEL or Windows Server 2008 R2.
2. On AMS Element Manager go to section: **Tools>>Backup and Restore>>Backup Tasks** and click **Add**.
3. Enter a name for this backup task.
4. Select "**Application Content**".
5. Clear "**System Configuration**".
6. Select "**Manually as needed"** and click "**Save**".
7. In the Backup Tasks window, select the task and click "**Run Now**"
8. The **History Log** window appears. Wait until you see confirmation that backup task has completed.
9. The Content Store will be backed up to a zip file at location:
   Windows: *%MASHOME%platdata\EAM\Backups*
   Linux: *$MASHOME/platdata/EAM/Backups*
10. Copy this zip file to the new AAMS 7.7 server.
11. Open a terminal session (ssh for Linux and cmd prompt for windows) and run the following command (shown with example filename) to migrate the Content Store data to the AAMS 7.7 server:
    amsupgrade taskname_hostname__2015_11_26_8_41_48.zip
12. On AMS Element Manager, go to section: **Tools>>Media Management** and verify that a **streamsource** namespace exists with the music content groups and the **SIP domain** namespace exists with the locale, tones, prompts and music content groups.
13. Copy the ***completeAAMS77Migration (.py or .exe)*** to the AAMS 7.7 server and run this script. This script simply deletes any duplicate music content groups from the SIP domain namespace if they are already under the **streamsource** namespace.

14. Add this AAMS to CCMA Media Servers and services. If this AAMS is the Master Content Store, then tick this box in the Media Servers page. This will push down any default media files to the AAMS Content Store that are missing from the migration.
15. Carry out Post-Installation Configuration on AAMS 7.7 server.

Post-Installation Configuration

Avaya Aura Media Server Installation

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

1. Launch AAMS Element Manager and browse to ***System Configuration >> Network Settings >> General Settings >> Connection Security***
2. Un-tick "***Verify Host Name***" setting and hit the "***Save***" button followed by "***Confirm***".
3. Browse to ***System Configuration >> Network Settings >> General Settings >> SOAP***
4. Add AACC IP Address into ***SOAP Trusted Nodes***. If HA, add AACC Active, Standby and Managed IP Address.
5. Hit the "***Save***" button followed by "***Confirm***"
6. Browse to ***System Configuration >> Signalling Protocols >> SIP >> Nodes and Routes***
7. Add AACC IP Address into ***SIP Trusted Nodes***. If HA, add AACC Active, Standby and Managed IP Address.
8. Verify that AAMS can resolve AACC FQDN.

Avaya Aura Media Installed on Red Hat Enterprise Linux Servers

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

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

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

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

CCMM Administration

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

ActiveX Controls.msi file update

Use the ACCS 7.0 ActiveXControls.msi to distribute the CCMA ActiveX Controls to CCMA Client machines where the local user does not have permission to download ActiveX controls within Internet Explorer.

You only need to use this file if your contact center security policy does not allow all users to log on to the client PCs with administrator privileges. In this scenario, the automatic download process for the Contact Center Manager Administration controls will not function.

For those users who have a central management tool in their network, such as a Systems Management Server (SMS), Avaya bundled the required controls into a single file called ActiveX Controls.msi. The SMS server can be used to run this file and silently install all the required controls on all the SMS clients, regardless of the level of user who logs on to the PC.

The ActiveXControls.msi file can be found on the DVD at the following folder location
\Install Software\CCMA\ActiveX Controls

Agent Desktop

The Agent Desktop application is no longer available as part of the Service Pack bundle file set.

The Agent Desktop Client application can be deployed as a click-once application. Alternatively, the Agent Desktop Client application installer can be located in the following folder on your ACC server: <Application Drive>:\Avaya\Contact Center\Multimedia Server\Agent Desktop\Client

Agent Desktop Prerequisites

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

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

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

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

Agent Desktop and desktop virtualization

To support Agent Desktop on Citrix and desktop virtualization environment, users must select the "Enable Unsupported Client OS" through CCMM Administrations. Refer to documentation; Avaya Contact Center Select Advanced Administration - Agent Desktop configuration - Configuring User Settings, for further details.

Multimedia Prerequisites for server migration

This is only applicable to users migrating to new ACCS 7.0 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.

Localization

Avaya Contact Center Select 7.0 Microsoft SSRS, Avaya Agent Desktop (AAD), Outbound Campaign Management Tool (OCMT) and 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, Italian, Japanese and Korean.

New features introduced in Avaya Contact Center Select 7.0 are localized in this release for the first time.

Overview of ACCS 7.0 I18N and L10N Products & Components

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

The following table lists all ACCS 7.0 products and components in relation to Internationalization and Localization:

ACCS 7.0 Products	Component	International OS Support? Yes/ No	Localized? Yes/No	Comments
CCMS	All components	Yes	No	
CCT	Web Agent Controls	Yes	Yes	
	Web Agent Controls online Help	Yes	Yes	
	All other components	Yes	No	
Server Utility	All components	Yes	No	
License Manager	All components	Yes	No	
Web Collaboration	All components	Yes	n/a	
CCMA	Server Components	Yes	No	Only Administration users work with Server Components.
CCMA	Contact Center Management	Yes	Yes	
CCMA	Access and Partition Management	Yes	Yes	
CCMA	Real-Time Reporting	Yes	Yes	
CCMA	Historical Reporting	Yes	Yes	
CCMA	Configuration	Yes	Yes	
CCMA	Emergency Help	Yes	Yes	
CCMA	Outbound	Yes	Yes	

CCMA	Historical Report Templates	Yes	Yes	
CCMA	Agent Desktop Display	Yes	Yes	
CCMA	Online Help	Yes	Yes	
CCMA	Orchestration Designer (OD)	Yes	No	The target audience of the Localization effort (call center agents and supervisors) do not use the OD tool.
CCMA	Configuration Tool	Yes	No	Only administrators use the Configuration Tool.
CCMA	Element Manager	Yes	No	Login page is localized.
CCMM	Server Components	Yes	No	
CCMM	AAD Client	Yes	Yes	
CCMM	AAD online Help	Yes	Yes	
CCMM	OCMT Client	Yes	Yes	
CCMM	OCMT online Help	Yes	Yes	

Support of CCMM Server and Configuration Notes

Enable email analyzer

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

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

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

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

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

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

NB: The following wildcard limitation applies to Asian languages only

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

There is a limitation when enabling the email analyzer to Japanese (CJKAnalyser).
This is a limitation of the creator of the analyzer, Lucene.
A problem arises ONLY when using SINGLE BYTE characters in the keyword, double byte routes successfully.
To route a single byte keyword, you must save the keyword as DOUBLE byte on the server.
There are no new files needed for this workaround.

Action: The workaround is to add DOUBLE byte keywords to route both single and double byte successfully.
If you wish to route a single byte keyword to a skillset, you must setup the keyword in DOUBLE byte.
For example to route the single byte keyword コプタ to a skillset called EM_Test do the following.

1) Create a DOUBLE byte keyword

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

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

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

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

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

NB: The following wildcard limitation applies to Asian languages only

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

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

Email Domain Names (Asian)

NB: The following applies to Asian languages only

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

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

CCMM friendly display names

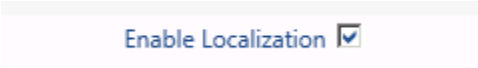
Display names are referred to in the CCMM server online Help in section **Creating or changing a recipient**, section 99. In the Display Name box, type the friendly name you want to appear in the e-mail From address (for example, Customer Support). You must enter a display name for each mailbox.
In response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

Start Localized AAD Client

Pre-installation steps

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

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



- From a French client PC, start AAD.

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

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

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

Installing the Agent Desktop Client

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

Prerequisites

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

Procedure steps

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

Starting the Agent Desktop Client

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

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

Procedure steps

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

Click Windows Start, All Programs, Avaya, Avaya Agent Desktop 7.0.
The Agent Desktop toolbar appears. If a CCT Connection Failure message appears, your Windows User ID is not configured on CCT. Click Retry to enter valid User Credentials or click Cancel to exit the application.

* Applicable LANGUAGE CODEs to be used are:

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

Start OCMT Client

Pre-installation steps

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

- From a French client PC, launch OCMT.

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

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

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

Logging on to the Outbound Campaign Management Tool

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

Prerequisites

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

Procedure steps

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

Detecting latest Language files

In case that client runs the English AAD and OCMT applications and does not pick up the language files. The client has previously launched English-only AAD and OCMT applications from the server and these files are now stored in the GAC (.Net cache) on the client PC. The .Net cache (GAC) therefore, needs to be emptied on the client PC so the latest English and language files can be taken from the server.
Note: If you install an updated Service pack or design patch, the client still runs applications with cached language files. The .Net cache (GAC) must be emptied, so the latest language files can be taken from the server.

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

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

1. Close AAD and OCMT.
2. Click Add/Remove Programs.
3. Remove Avaya/Avaya Agent Desktop 7.0.
4. Navigate to *C:\Documents and Setting\USERNAME\local settings\apps* .

5. Delete the 2.0 folder.
6. *Note:* This folder may be hidden. If so, open Windows Explorer and click on Tools, Folder options. Choose the View tab. Under Files and folders or Hidden files and folders, choose to show hidden files and folders. Click Apply and click OK.
7. Start AAD to download the latest AAD files from the CCMM server.
8. Start OCMT from CCMA to download the latest OCMT files from the CCMM server.

Comments on Translations

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

German
No special comments.

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

Simplified Chinese
No special comments.

Brazilian Portuguese
No special comments.

Russian
No special comments.

Italian
No special comments.

Japanese
No special comments.

Korean
No special comments.

Known Issues

Hardware Appliance

None

Software Appliance

None

Application\Features

Potential for Agents to be prompted multiple times with security warnings when viewing inline attachments in an email with out of the box certificates

Tracking Number	CC-3686
Application	Agent Desktop
Description	If a customer site has security enabled but has not yet substituted an official certificate with the out of the box certificate, then for the first email received by an Agent which contains inline images, the Agent will be prompted with a security warning for each image, prompting the Agent to install the certificate.
Impact	For the first email received by the Agent with inline attachments the Agent will be forced to accept a server certificate for each image. The Agent will not be prompted for subsequent emails unless Agent Desktop is restarted.
Workaround	Navigate to the Start Menu->Control Panel and open “Internet Options” under “Network and Internet”. Click on the Advanced tab and scroll down to the setting “Warn about certificate address mismatch”. Uncheck this checkbox

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.

CCT Console not working on ACCS due to Apache Tomcat 8081 port conflict

Tracking Number	CC-9938
Application	CCT Console
Description	Installing Avaya Aura Contact Center installs Apache Tomcat Server. The default port number for Apache Tomcat is 8081. If you need to change the port number to avoid conflicts with third-party software, see your Apache Tomcat documentation. If the Tomcat port is changed then refer to section: "**Adding Communication Control Toolkit to CCMA**" in the commissioning guide to change the CCT Console port used. **McAfee Agent Common Services** (macmnsvc.exe) or **McAfee Framework Service** (FrameworkService.exe) are the services that can use port 8081. If these services are required, then the Apache Tomcat port must be changed. Refer to If these services are not required then they can be stopped and configured not to run on startup in Windows Services.
Impact	If a conflict occurs, then ACCS **CCT Console** will be impacted. McAfee Anti-Virus could potentially be one of the third party applications that conflicts with port 8081.
Workaround	If you need to change the port number to avoid conflicts with third-party software, see your Apache Tomcat documentation. If the Tomcat port is changed then refer to section: "**Adding Communication Control Toolkit to CCMA**" in the commissioning guide to change the CCT Console port used.

AMS 7.5 Linux Migration: prepareForAAMS77Migration does not run on AACC 6.3 (AMS 7.5) systems

Tracking Number	CC-5117
Application	AAMS
Description	**prepareForAAMS77Migration.py** (7.0.0.4) python script does not run on AACC 6.3 AMS 7.5 Linux Systems. It reports the error: **"ERROR: AMS Version is . This Utility can only be run on 7.5 or 7.6 AMS systems. Exiting."**
Impact	AMS 7.5 Application content will not have been prepared for AAMS77 migration meaning the music content in the content groups will not have been copied to the streamsource namespace and the canned prompts in the file system would not have been copied to the AMS Content Store.
Workaround	The GA Patch bundle contains a working version of this utility in directory

	(7.0.0.5): \\Install Software\AMS\Windows \\Install Software\AMS \AMS\Linux

Rebuild Report Creation Wizard reports created with Beta 2 software

Tracking Number	
Application	Contact Center Manager Administration – Report Creation Wizard
Description	Reports created during Beta should be rebuilt with this version to fix issues in the base templates.
Impact	It is recommended that reports that were created in Beta version of Report Creation Wizard using the "Simplified Report" option should be re-built with this version of the application in order pick up fixes to the underlying report definitions.
Workaround	

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

Page Range not supported when saving historical reports in PDF format

Tracking Number	CC-5051
Application	Contact Center Manager Administration
Description	When saving a historical report to a pdf file, it was previously possible to save a range of pages. This functionality is no longer available with the AACC 7.0 reporting solution.
Impact	All pages will be saved to the pdf file.
Workaround	None

Report Creation Wizard – Some sample reports do not work

Tracking Number	CC-5035
Application	Contact Center Manager Administration
Description	The following sample reports do not work in this release: BillingByAddress SkillsetOutboundDetails Voice Skillset Name ID Mapping Network Consolidated Skillset Performance ICPCSRSample

	MMCSRStat
Impact	These samples cannot be used as a starting point for new reports
Workaround	None

Report Creation Wizard – Migrated reports show white space where custom formulas previously existed

Tracking Number	CC-4903
Application	Contact Center Manager Administration
Description	When RCW generated reports are migrated from a previous release, custom formulas will be lost as these cannot be automatically migrated. This results in blank space on the reports.
Impact	The custom formula definition is missing from the report
Workaround	Create the missing formula in RCW and add it to the report.

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

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

Popup window appears when launching OD for first time on server

Tracking Number	CC-4916
Application	Contact Center Manager Administration
Description	An information window appears with details about the “ComponentOne TrueDB Grid Pro 8” software the first time Orchestration Designer is launched on the server.
Impact	This window can be closed and ignored.
Workaround	Close the popup window.

Failure to upload modified agent via Configuration Tool

Tracking Number	CC-5045
Application	Contact Center Manager Administration
Description	Under certain circumstances the upload of modified agent data from the Excel configuration tool fails with an error “An error occurred adding agent to CCMS …”. This only happens when the names of the configured servers are in a certain alphabetical order.
Impact	Agents cannot be updated using excel configuration tool.
Workaround	Contact Avaya support.

Agent data does not sync with IP Office

Tracking Number	CC-4988

Application	Contact Center Manager Administration
Description	Under certain circumstances the synchronization of agents with ACCS fails. This only happens when the names of the configured servers are in a certain alphabetical order.
Impact	Agent data is not synchronized between ACCS and IPOffice.
Workaround	Contact Avaya support.

CCT server memory leak under heavy traffic

Tracking Number	CC-4772
Application	Communication Control Toolkit
Description	In lab environments running high levels of traffic a CCT server memory leak has been observed.
Impact	High memory usage observed in task manager. Possibility of CCT server termination after several days at a very high traffic rate.
Workaround	Patch available from design: AvayaCC_CCT_7.0.0.0.1

ACCS sample thresholds not automatically assigned to sample applications and skillsets by ACCS Ignition Wizard

Tracking Number	CC-5132
Application	Contact Center Manager Administration (CCMA) & Contact Center Manager Server (CCMS)
Description	ACCS 6.x and 7.0 ship with a sample application threshold class called “application” and a sample skillset threshold class called “skillset”. These sample threshold classes are not assigned to any of the sample applications or skillsets. Instead the default threshold classess of Application and Skillset are automatically assigned to all default applications and skillsets. The affects of this is this all of the sample RTD particulary the CC_Status collection will not have the correct colour changes for statistics exceeding or falling below their values in the sample thresholds
Impact	Anyone running the sample RTD’s will not see the correct threshold colour changes or service level changes in these displays. Sample skills which are skill1, skill2, EM_Skill1, WC_Skill2 and OB_Skill1 will not show a proper service level indication. All other custom displays created by an Administrator are not affected by this issue.
Workaround	There is a simple workaround. Using existing documented procedures, go into CCMA, Scripting, Application thresholds and assign the sample threshold class “application” to any/all of the existing applications. Then go into CCMA, Configuration, Skillsets, and replace the default Skillset Threshold class value with the sample value “skillset” . The sample agents threshold class is automatically assigned so there is no need to edit any of the sample agents injected by the ignition wizard.

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

The Historical Statistics value for Configured Agent IDs is changed during migration from AML to ACCS

Tracking Number	CC-9804
Application	Contact Center Manager Server
Description	After migration the limit of configured agents is set to 400
Impact	Reduction of the limit configured before the migration
Workaround	Set back to the old value in CCMA configuration

Max Open Duration setting cannot function longer than 2 hours

Tracking Number	CC-6289
Application	Contact Center Manager Server
Description	Steps to reproduce: 1. Launch CCMM Admin/Agent Desktop Configuration/General Settings, set Open Duration to value greater than 2 hours. 2. Launch AAD, login an agent, accept some MM contacts (VM, Fax …) and wait more than 2hours Expected result: Agent is able to active the contacts for the length of time set in step 1 without any problem Actual Result: After having been active on the contact for more than 2hrs, the agent is auto logged out with the message “You have been logged out of Agent Desktop while a contact is Open. Please finish this contact before you login again”
Impact	Unable to have a max open duration function longer than 2 hours.
Workaround	The following two files need to be updated: D:\Avaya\Contact Center\Common Components\CMF\CmfProperties.xml D:\Avaya\Contact Center\Common Components\CMF\CmfProperties.xml.ftl This value in each file: <AgentFailureAfterAnswerTimeout>7500000</AgentFailureAfterAnswerTimeout> Should be updated to: <AgentFailureAfterAnswerTimeout>86400000</AgentFailureAfterAnswerTimeout> After making this update a restart of Contact Center is required. If the workaround above has been applied it may need to be applied again after installing or removing a CCCC patch or service pack.

Cannot send SNMP Traps to NMS server because SNMP Service is not running

Tracking Number	CC-7163

Application	Events & SNMP Service
Description	A manual configuration procedure must be executed on an Avaya Aura Contact Center (AACC) 7.0 or Avaya Contact Center Select (ACCS) 7.0 server after installing the windows 2012 operating system software but BEFORE installing the AACC 7.0 or ACCS 7.0 application software. The manual procedure will install and start the SNMP Service service and must be executed if the customer wants SNMP traps to be sent to the Network Management System (NMS) to report failure and/or notification events.
Impact	Failure to execute this manual procedure before installing the AACC 7.0 or ACCS 7.0 application software will result in an inability to forward installation related SNMP traps to the NMS server.
Workaround	Manual Procedure 1. Log on to the AACC 7.0 or ACCS 7.0 Microsoft Windows 2012 server as Administrator. 2. Launch the Server Manager. 3. Select ***Manage*** menu & click ***Add Roles and Features***. 4. Add Roles and Features Wizard is launched 5. On ***Before You Begin*** tab, click ***Next***. 6. On ***Installation Type*** tab, click ***Next***. 7. On ***Server Selection*** tab, select the AACC 7.0 server from the server pool & click ***Next***. 8. On ***Server Roles*** tab, accept the default settings & click ***Next***. 9. On ***Features*** tab, select the SNMP Service feature check box. 10. On ***Add features that are required for SNMP Service*** window, click ***Add Features*** to add the SNMP Tools required to manage the SNMP service. 11. On ***Features*** tab, click ***Next***. 12. On ***Confirmation*** tab, click ***Install*** after confirming that SNMP Service and SNMP Tools are listed for installation. 13. On ***Results*** tab, click ***Close*** once the installation has completed successfully. 14. Verify the ***SNMP Service*** service is running on the Services Administrative Tool. 15. Proceed with the AACC 7.0 or ACCS 7.0 application software deployment. Repeat this procedure on all other AACC 7.0 or ACCS 7.0 Microsoft Windows 2012 servers.

RTDs are not showing any data after switchback from RGN to Primary

Tracking Number	CC-9787
Application	Contact Center Manager Administration
Description	Seen in one ACCS Business Continuity test lab : RTDs not showing any data after switchback from RGN to Primary. Not reproducible. 1. Perform a switchback from RGN to Primary site.

	2. Reinstate Geographic Business Continuity. 3. Once all services are up, launch RTDs.
Impact	RTDs not showing data after switchback from RGN to Primary.
Workaround	Manual Procedure 1. Go to the Start menu on ACC and select Run 2. Enter services.msc 3. Scroll down to the service 'CCMA IceRTDService' 4. Right click and select the 'restart' option The only impact is this service restart – no other functionality affected

Localization issues

For CCMM

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

The installation UI is in English instead of localised version

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

Appendix A

Issues Addressed in Service Pack 0 and Patches Line-up

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

CCMS, CCSU, CCCC and CCLM 7.0 SP1 Listing

This list contains defects addressed for the Manager Server, Common Components and License Manager components of Avaya Aura® Contact Center

WI/JIRA	Summary
wi01234356/CC-6224	AACC CCMS SP15 Disable LM check for Multiplicity in Control Service when CORPORATE
wi01234594/CC-6231	Call Abandoned at target node but no clear call message returned to source node
wi01234508/CC-6227	remote note filtered by ASM following SGM ITS ROUTE Failure with reason 34
wi01234135/CC-6221	AACC 6.4 SP15 AML HA The SDP service is crashing intermittently
wi01232883/CC-6204	AACC SP15 LM port number invalid after running Server Configuration
wi01232294/CC-6197	FirstEventTimestamp populated with value of previous instance of callid
wi01227393/CC-6174	AACC - Event Handler call processing change between SP10 and SP13
wi01233204/CC-6207	Database Integration Wizard (nihaiw.exe) has stopped working when trying to click Next to Configure Database Connections

wi01227025/CC-6170	Database Restore fails with ERROR #5001 Unknown EXTSELCT^DBREST error code 1
wi01234674/CC-6237	CBC reports are empty
wi01234797/CC-6240	AACC windows event logs throwing warning NCCT DAL An attempt to purge a failed cached query
wi01233372/CC-6210	Change NCC OAM Sync Site call timeout from 30 seconds to five minutes
wi01233617/CC-6212	AACC SP15 NIComSetup changes to not delete NCC site in Standby mode when called with no parameters
wi01231523/CC-6191	Contacts Outstanding Summary report slow after upgrade to sp15
CC-6315	ASM does not reset the PRIORITY IN NETWORK QUEUE to zero on All trunks busy
CC-6358	Error responce Target Agent Blocked the agent will end up receiving two calls
CC-6365	Network call is not re-queued as ASM does not notify TFE to reset PRIORTIY IN NETWORK QUEUE when the call is not yet queued at target
CC-6351	Restore of CCMS delayed by CSR Table reindex before and after restore
CC-6324	after SIP Agent NRDY scenario ASM didn't perform RTQ for call
CC-6553	ASM_Service terminated unexpectedly after pull contact scenario
CC-6654	SP15 ASM Request failed Event seen in Windows Application
wi01231637/CC-6193	AACC SP14 ApplicationListGet Toolkit client-side call failing in ICERTD
CC-6780	AACC SP15 - ASM did not send the dialed number to EB in Call Transferred message
CC-7890	AACC6.4SP16_Unable to login SA after changing from Agent to SA - No Terminal Assigned to this agent
CC-7265	[ACCS SP16] Migration from AML 6.4 SP15 to ACCS SP16 fails with error No devices mapped to this session
CC-7326	ACCS 6.4 SP16 _ Agent does not pick the call in skillset with SLR enabled and EWT exceeds TSL
CC-2471	Application still shows in Activate status after DeActivate the application

CCMA 7.0 SP1 Listing

This list contains defects addressed for the Manager Administration components of Avaya Aura® Contact Center.

WI/JIRA	Summary
wi01234130/CC-6220	AACC 6.4 SP15 Real Time Display failure - SOAPICERtdService down
wi01222714/CC-6163	Real-Time public or private Billboard Collection layout is not saving from client with Hebrew language
wi01235165/CC-6253	AACC 6.4 SP15 - CCMA - unable to select Skuillset ID in historical reproting
CC-6814	Remove XSS Vulnerability from MsgBox.asp and Connect.asp in CCMA
wi01234841/CC-6242	Unable to modify flow in OD undefined variable

CCT 7.0 SP1 Listing

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

WI/JIRA	Summary
wi01235091/CC-6249	CCT SP15 - TAPI hangs on lineUnholdCall
CC-6664	TAPISRV crash due to copying 32 bytes + a null byte (33 bytes) into 32 byte integer

CCMM/AAD 7.0 SP1 Listing

This list contains defects addressed for the Multimedia\Outbound Server and Avaya Agent Desktop components of Avaya Aura® Contact Center.

WI/JIRA	Summary
wi01233238/CC-6208	AAAD disables login menu after logging out POM agent
wi01234912/CC-6245	CCMMOAM process on CCMM Server shows high number of handle count and keeps growing
wi01233203/CC-6206	for mailto list exceeding 255 chars the list of addresses is truncated to 255 causing send failure
wi01234194/CC-6222	AAAD has no limit on the length of MailTo when sending emails
wi01233734/CC-6216	Number of contacts return by by ReadBlockOfContacts functions is incorrect
wi01233732/CC-6215	Exception thrown when trying to read a block of contacts with Fax contact type
wi01232244/CC-6196	Contact gets stuck in open state when AAAD crashes
wi01234857/CC-6243	MM barred email addresses case sensitive
wi01175181/CC-6033	AACC SP11 AAOA Offsite Agent Gets Stuck Cotnact upon Network Issues - Login Issues After the Fact
wi01235324/CC-6257	Agents can extend ACW multiple times
wi01235031/CC-6248	ReadBlockOfContacts Methods from CICustomerWS returns wrong amount of contacts remaining
wi01235030/CC-6247	When given startContactID not in DB to ReadNextBlockOfContacts in CICustomerWS it returns wrong contacts
CC-7522	AAAD is stuck if agent actives on CDN call and maximum MM contact then tries set AC and NRD code
CC-7315	POM PreivewPredictive contacts - AAAD not reflecting correct POM Wrap up timers AAAD denies any ACW time when ACW Extensions is 0 or not defined
CC-5193	AAAD hangs when logging in Presence ID
CC-7888	[SP16] AAAD_The observer button is enabled on supagent when the agent is active on WC contact isn't belong to him
CC-3513	AACC 7.0 DVD174 - AAD - Contact item in Observe window is disappeared when supervisor selects filter with agent that is not active on CDN or Webcomm contact
CC-8106	ACCS 6.4 SP16 Drop2 _ Unable to observe the agent CDN call because observe and barge in buttons are grey out if sup agent accepts and releases the

	Emergency call some times
CC-8377	Launch AAAD and login agent who currently logged in, AAAD topmost is auto active

Software included in this line-up

CCMA ActiveX Control MSI – Content and Versions

File Name	File Size (bytes)	Version
ChartWrapperCtrl.ocx	63752	1.0.0.1
DTPWrapperCtrl.ocx	96520	8.0.0.0
hrctrl.dll	112904	8.0.0.4
iceemhlpcontrol.dll	129288	8.0.0.2
icertdcontrol.dll	854280	8.4.12.21
iemenu.ocx	65648	4.71.115.0
ntzlib.dll	65080	1.1.4.0
olch2x8.ocx	2102448	8.0.20051.51
rope.dll	248072	1.0.0.4
rsclientprint.dll	594432	2011.110.3128.0
sstree.ocx	337120	1.0.4.20
WSEColorText.ocx	178440	6.0.0.15
xerces-c_2_7.dll	1893832	12.5.0.1190