



# **Avaya Aura® Contact Center Release 6.4 Service Pack 16**

---

## **Release Notes**

<b>DOCUMENT VERSION</b>	<b>:1.7</b>
<b>DVD BUILD</b>	<b>:</b>
<b>SERVICE PACK BUILD</b>	<b>:SERVICE PACK 16</b>
<b>ISSUE DATE</b>	<b>: 13<sup>ST</sup> DECEMBER 2016</b>

<b>PURPOSE.....</b>	<b>9</b>
PUBLICATION HISTORY .....	9
<b>AVAYA AURA® CONTACT CENTER, RELEASE 6.4 SP16 SOFTWARE .....</b>	<b>10</b>
WHAT'S NEW IN THE AACC 6.4 SP16 RELEASE (THAT WAS NOT PREVIOUSLY AVAILABLE IN AACC 6.4 SP15).....	10
<b>OPERATING SYSTEM &amp; VIRTUALIZATION .....</b>	<b>11</b>
OPERATING SYSTEM SUPPORT.....	11
<i>Microsoft Service Packs</i> .....	11
<i>Microsoft Hotfixes</i> .....	11
VIRTUALIZED ENVIRONMENTS .....	11
<b>SOFTWARE DOWNLOAD .....</b>	<b>12</b>
DVD SOFTWARE .....	12
SERVICE PACK BUNDLE SOFTWARE.....	12
ADDITIONAL CONTACT CENTER UPDATES.....	14
<i>Additional Software in Bundle</i> .....	14
PATCH SCANNER .....	14
AVAYA MEDIA SERVER SOFTWARE.....	15
ADDITIONAL AVAYA MEDIA SERVER UPDATES .....	15
SOFTWARE APPLIANCE SOFTWARE.....	16
<i>Avaya Aura Contact Center OVA Image</i> .....	16
<i>Avaya Media Server OVA Image</i> .....	17
<i>Avaya WebLM OVA Image</i> .....	17
AACC FIREWALL POLICY.....	18
MANDATORY MICROSOFT UPDATES .....	18
IMPORTANT GUIDELINES FOR 3RD PARTY SOFTWARE UPDATES OUTSIDE OF AVAYA SP/PATCH UPDATES .....	19
SUPPORT OF HEADSET CONTROL OF TELEPHONY OPERATIONS IN AAAD.....	19
SUPPORT OF IQ 5.2.6 .....	19
AVAYA AURA CONTACT CENTER CALL NETWORKING COMPATIBILITY ISSUE.....	19
AVAYA GREP .....	21
AVAYA SIP SLEUTH.....	21
<b>THIRD-PARTY SOFTWARE .....</b>	<b>22</b>
THIRD PARTY SOFTWARE FOR NEW INSTALLATIONS.....	22
<i>Intersystems System Management Portal</i> .....	22
THIRD PARTY SOFTWARE FOR PREVIOUS 6.X UPGRADES.....	22
<i>Java Runtime Environment – jre1.6.0_37</i> .....	22
<i>WinPcap</i> .....	22
<i>McAfee Antivirus</i> .....	22
THIRD PARTY SOFTWARE UPGRADES ON WINDOWS DESKTOP SYSTEMS.....	23
THIRD PARTY SOFTWARE UPGRADE UTILITY.....	24
<i>Utility Location</i> .....	24
<i>Fresh Installations</i> .....	24
<i>Fresh Installations – Pre Execution Instructions</i> .....	24
<i>Fresh Installations – Post Execution Instructions</i> .....	25
<i>Fresh Installs – Third Party Software Upgraded</i> .....	25
<i>Upgrades from 6.x</i> .....	26
<i>Upgrades from 6.x – Pre Execution Instructions</i> .....	26
<i>Upgrades from 6.x – Post Execution Instructions</i> .....	26
<i>Third Party Software Upgraded</i> .....	26
<i>Utility Reboot Prompts</i> .....	26
<i>Third Party Software Component Upgrade Failure</i> .....	27

<i>Logging Information</i> .....	27
THIRD PARTY SOFTWARE DOWNGRADE UTILITY .....	28
<i>Utility Location</i> .....	28
<i>Execution Instructions</i> .....	28
<i>Post Execution Instructions</i> .....	29
<i>Third Party Software Downgraded</i> .....	29
<i>Utility Reboot Prompts</i> .....	30
<i>Third Party Software Component Downgrade Failure</i> .....	30
<i>Logging Information</i> .....	30
<i>Important Note</i> .....	30
AVAYA CONTACT CENTER SOFTWARE NOTIFICATION APPLICATION .....	31
<i>Application Behaviour</i> .....	31
<i>Logging Information</i> .....	31
INTERNET EXPLORER COMPATIBILITY ISSUES .....	32
THIRD PARTY SOFTWARE SUPPORT APPLICATIONS .....	33
EQUINOX 3.0 NOT SUPPORTED FOR USE AS AN AGENT SOFTPHONE .....	33
<b>AACC 6.4 SP16 SERVICE PACK SOFTWARE</b> .....	<b>34</b>
NEW INSTALLATIONS .....	34
HOT PATCHING MISSION CRITICAL OR AML WARM STANDBY HA SYSTEMS TO AACC 6.4 SP16 .....	34
DOWNGRADE (AVAYA AURA® CONTACT CENTER 6.4 SP16 TO A PREVIOUS RELEASE) AVAYA AURA CONTACT CENTER .....	35
<i>Avaya Media Server</i> .....	35
<i>Orchestration Designer</i> .....	37
UPGRADING FROM PREVIOUS AVAYA AURA® CONTACT CENTER 6.x RELEASE .....	37
<i>How to Backup/Restore ARConnector Configuration</i> .....	38
<i>How to Upgrade from a Previous Avaya Aura® Contact Center 6.x Release</i> .....	38
<i>Upgrading to a new Service Pack or Restoring a Database backup results in recompile         of all scripts</i> .....	39
<i>Issue Interval Statistics</i> .....	39
<i>Issue with the retention of Configuration of WS Open Interface</i> .....	40
<i>Issue with SMMC starting after upgrading from previous AACC 6.x Release</i> .....	40
<i>HA SOA web services with TLS</i> .....	42
UPGRADING FROM PREVIOUS AVAYA AURA® CONTACT CENTER SERVICE PACK IN A MISSION CRITICAL HA ENVIRONMENT .....	45
UPGRADING FROM SERVICE CREATION ENVIRONMENT (SCE) TO ORCHESTRATION DESIGNER (OD) .....	45
SOA PRESERVATION – DOWNGRADE AND UPGRADE OF AVAYA AURA® CONTACT CENTER COMMON COMPONENTS .....	46
INVALID AGENT AUDIT .....	46
AACC-IQ MODIFIED REPORTING OF QUEUE OUT OF SERVICE .....	47
<b>REMOTE ACCESS</b> .....	<b>48</b>
<b>LOCALIZATION</b> .....	<b>49</b>
OVERVIEW OF AACC 6.4 I18N AND L10N PRODUCTS & COMPONENTS .....	49
SOFTWARE .....	50
<i>Supported operating systems</i> .....	50
<i>Localized Components (CCMA and CCMM)</i> .....	51
LANGUAGE SPECIFIC SUPPORT AND CONFIGURATION .....	51
<i>Support of CCMA Client</i> .....	51
<i>Support of CCMM Client</i> .....	52
<i>Support of CCMM Server and Configuration Notes</i> .....	52
LOGGING ON TO CONTACT CENTER MANAGER ADMINISTRATION .....	55
<i>Enabling languages</i> .....	55
<i>Procedure steps</i> .....	56
START LOCALIZED AAD CLIENT .....	57
<i>Pre-installation steps</i> .....	57
<i>Installing the Agent Desktop Client</i> .....	57

<i>Starting the Agent Desktop Client</i> .....	57
START OCMT CLIENT .....	58
<i>Pre-installation steps</i> .....	58
<i>Logging on to the Outbound Campaign Management Tool</i> .....	58
<i>Prerequisites</i> .....	58
<i>Procedure steps</i> .....	58
DETECTING LATEST LANGUAGE FILES.....	58
<i>Emptying the .Net cache on the client PC running AAD and OCMT</i> .....	59
COMMENTS ON TRANSLATIONS .....	59
<i>French</i> .....	59
<i>German</i> .....	59
<i>Latin American Spanish</i> .....	59
<i>Simplified Chinese</i> .....	59
<i>Brazilian Portuguese</i> .....	59
<i>Russian</i> .....	59
<i>Italian</i> .....	59
CRYSTAL REPORT TEMPLATES.....	60
<i>Localized templates</i> .....	60
KNOWN ISSUES.....	63
<i>For CCMA</i> .....	63
<b>DVD CONTROLLER</b> .....	<b>64</b>
PRE INSTALLATION INSTRUCTIONS .....	64
<i>INSTALLATION OF PRODUCT UPDATES</i> .....	64
INSTALLATION INSTRUCTIONS.....	64
POST INSTALLATION INSTRUCTIONS.....	64
CONFIGURATION ISSUES .....	64
<b>COMMON COMPONENTS</b> .....	<b>65</b>
PRE INSTALLATION INSTRUCTIONS .....	65
INSTALLATION INSTRUCTIONS.....	65
POST INSTALLATION INSTRUCTIONS.....	65
POST UNINSTALL (DOWNGRADE TO 6.2) INSTRUCTIONS .....	65
CONFIGURATION ISSUES .....	65
PVI CHECKER.....	65
<b>CONTACT CENTER UPDATE MANAGER</b> .....	<b>66</b>
<b>UNIFIED COMMUNICATION ENVIRONMENT</b> .....	<b>69</b>
AVAYA CS1000 AML INSTALLATIONS .....	69
<i>Required Patches on CS1000</i> .....	69
AVAYA AURA® INSTALLATIONS .....	71
<i>Required Software &amp; Patches</i> .....	71
<i>Configuration Issues</i> .....	73
<b>CALL REDIRECTION WITH AACC SIP DEPLOYMENTS</b> .....	<b>74</b>
<b>SIP SPECIFIC ISSUES</b> .....	<b>76</b>
CTI BEHAVIOUR FOR TRANSFER AND CONFERENCE.....	76
SIP ENDPOINTS ISSUES .....	76
CALL REDIRECTION WITH MICROSOFT EXCHANGE VOICEMAIL.....	76
DTMF AUDIBLE DURING SUPERVISOR OBSERVE .....	77
CHANGES TO SIP LICENSING.....	77
<i>AMS Instance Licensing</i> .....	77
<i>Changes to Announcement and Dialog Treatment Licensing</i> .....	77
'Transfer Complete' Button Not Available on AAAD When Two Unrelated Calls are Active....	78
<b>SIP HA SPECIFIC ISSUES</b> .....	<b>79</b>

PRE INSTALLATION INSTRUCTIONS .....	79
POST INSTALLATION INSTRUCTIONS.....	80
CONFIGURATION ISSUES .....	80
G.729 CODEC SUPPORT .....	80
VOICE CODEC PACKET SIZE (PTIME) LIMITATIONS .....	81
KNOWN CCMS LIMITATIONS .....	81
<b>AVAYA MEDIA SERVER .....</b>	<b>82</b>
RED HAT ENTERPRISE LINUX SUPPORT.....	82
<i>Support for Security Enhanced Linux (selinux) .....</i>	<i>82</i>
<i>Avaya Media Server Linux Logs .....</i>	<i>82</i>
AVAYA MEDIA SERVER SPECIFICATIONS FOR HIGH AVAILABILITY PAIR .....	83
AMS UPGRADE PROCEDURES .....	83
<i>Upgrading Clustered AMS Servers from SP10 to SP16 .....</i>	<i>83</i>
<i>AMS Windows Upgrade Procedures .....</i>	<i>83</i>
<i>AMS Red Hat Enterprise Linux (RHEL) Upgrade Procedures .....</i>	<i>86</i>
SNMP SUPPORT FOR AMS .....	89
CONFIGURATION ISSUES .....	89
<b>CONTACT CENTER MANAGER SERVER .....</b>	<b>90</b>
INSTALLATION INSTRUCTIONS.....	90
POST INSTALLATION INSTRUCTIONS.....	90
CONFIGURATION ISSUES .....	90
SIP/ACCS CONSULTATION SCENARIOS LIMITATIONS .....	90
REPORTING LIMITATION DURING SYSTEM START-UPS .....	90
EXCHANGING UUI DATA IN AACC.....	91
DATABASE MAINTENANCE UTILITY ONLINE HELP NOT UP TO DATE.....	91
DOCUMENTED NUMBER OF ACTIVITY CODES SUPPORTED .....	91
ALTERNATE CALL ANSWER LIMITATIONS FOR CALL TRANSFER SCENARIOS.....	91
<b>LICENSE MANAGER .....</b>	<b>92</b>
PRE-INSTALLATION INSTRUCTIONS .....	92
INSTALLATION INSTRUCTIONS.....	92
POST INSTALLATION INSTRUCTIONS.....	92
CONFIGURATION ISSUES .....	92
<b>SERVER UTILITY .....</b>	<b>93</b>
PRE INSTALLATION INSTRUCTIONS .....	93
INSTALLATION INSTRUCTIONS.....	93
POST INSTALLATION INSTRUCTIONS.....	93
CONFIGURATION ISSUES .....	93
<b>CONTACT CENTER MANAGER ADMINISTRATION.....</b>	<b>94</b>
PRE INSTALLATION INSTRUCTIONS .....	94
ACTIVE X CONTROLS.MSI FILE UPDATE .....	94
SKILLSET NAMING .....	94
"POP TO FRONT" NO LONGER SUPPORTED ON REAL-TIME DISPLAYS .....	94
CUSTOMER DOCUMENTATION NO LONGER AVAILABLE FROM CCMA HELP MENU .....	95
STORAGE OF HISTORICAL REPORTING STATISTICS LIMITED TO 999 .....	95
INSTALLATION INSTRUCTIONS.....	95
POST INSTALLATION INSTRUCTIONS.....	95
<i>Upgrade Crystal RAS Procedure.....</i>	<i>95</i>
<i>Crystal Reports fail to run after upgrade to SP16 .....</i>	<i>97</i>
POST UNINSTALL (ROLLBACK TO 6.3) INSTRUCTIONS.....	99
CONFIGURATION ISSUES .....	99
<b>COMMUNICATION CONTROL TOOLKIT .....</b>	<b>100</b>

PRE INSTALLATION INSTRUCTIONS .....	100
INSTALLATION INSTRUCTIONS .....	100
POST INSTALLATION INSTRUCTIONS .....	100
CONFIGURATION ISSUES .....	100
<b>CONTACT CENTER WEB STATS.....</b>	<b>103</b>
PRE INSTALLATION INSTRUCTIONS .....	103
INSTALLATION INSTRUCTIONS .....	103
POST INSTALLATION INSTRUCTIONS .....	103
CONFIGURATION ISSUES .....	103
<b>CONTACT CENTER MULTIMEDIA .....</b>	<b>104</b>
PRE INSTALLATION INSTRUCTIONS .....	104
INSTALLATION INSTRUCTIONS .....	104
<i>Avaya Aura Agent Desktop</i> .....	<i>104</i>
POST INSTALLATION INSTRUCTIONS .....	104
CONFIGURATION ISSUES .....	105
<b>ORCHESTRATION DESIGNER .....</b>	<b>107</b>
PRE INSTALLATION INSTRUCTIONS .....	107
INSTALLATION INSTRUCTIONS .....	107
POST INSTALLATION INSTRUCTIONS .....	107
CONFIGURATION ISSUES .....	107
<b>SECURITY FRAMEWORK.....</b>	<b>109</b>
PRE INSTALLATION INSTRUCTIONS .....	109
INSTALLATION INSTRUCTIONS .....	111
POST INSTALLATION INSTRUCTIONS .....	111
CONFIGURATION ISSUES .....	111
<b>FEATURE SPECIFIC: CCT OPEN INTERFACES WEB SERVICES.....</b>	<b>112</b>
CONSTRAINTS ON AGENT COUNT AND CONTACT RATE PER HOUR.....	112
<b>FEATURE SPECIFIC: HIGH AVAILABILITY .....</b>	<b>113</b>
PRE-INSTALLATION INSTRUCTIONS .....	113
INSTALLATION INSTRUCTIONS .....	113
POST INSTALLATION INSTRUCTIONS .....	113
NCC RE-SYNC .....	113
OUTAGE OF AVAYA AURA SESSION MANAGER.....	113
HA INTEROPERATION & AVAYA CONTACT RECORDING (ACR).....	114
NOT-YET ESTABLISHED CALLS – ALERTING/RINGING SCENARIO .....	114
CCMA AD-LDS CONFIGURATION ISSUES / TROUBLE SHOOTING .....	114
CONFIGURATION ISSUES .....	116
<b>FEATURE SPECIFIC: AACC CALL NETWORKING IN A SIP ENVIRONMENT .....</b>	<b>117</b>
MANDATORY HOME LOCATION CODE CONFIGURATION.....	117
<b>FEATURE SPECIFIC: E164 SUPPORT .....</b>	<b>118</b>
TO ENABLE E164 SUPPORT WITHIN SGM FOR CS 1000.....	118
<b>FEATURE SPECIFIC: WORKING WITH AVAYA IQ 5.2.6.....</b>	<b>119</b>
<b>FEATURE SPECIFIC: ONLY TLS 1.0 IS SUPPORTED WITH AACC 6.4.....</b>	<b>120</b>
<b>SDK CHANGES.....</b>	<b>121</b>
CCT SDK CHANGES .....	121
CCMA OPEN INTERFACE SDK CHANGES .....	121
CCMM PHP WEBCHAT SAMPLE APPLICATION .....	122
SOA SDK CHANGES.....	122

<b>APPENDIX A .....</b>	<b>123</b>
SOFTWARE INCLUDED IN THIS LINE-UP .....	123
<i>Previously Released Service Packs .....</i>	<i>123</i>
<i>Previously Released AACC 6.X Contact Center Patches .....</i>	<i>124</i>
ISSUES ADDRESSED IN SERVICE PACK 6.4 LINE-UP .....	126
CCMS, CCMSU, CCCC and CCLM, CCMT, CCWS 6.4 SP16 Listing .....	126
CCMS 6.4.216.1 Patch.....	129
CCMS 6.4.216.2 Patch and CCMS 6.4.216.3 Patch .....	130
CCMS (SGM) 6.4 SP16 Listing .....	130
CMF 6.4 SP16 Listing .....	130
CCCC 6.4.216.1 Patch .....	131
CCCC 6.4.216.2 Patch .....	131
CCMA, SFW 6.4 SP16 Listing.....	131
CCT 6.4 SP16 Listing.....	132
CCMM\AAAD 6.4 SP16 Listing.....	132
CCMM\AAAD 6.4.216.1 Patch .....	134
CCMM\AAAD 6.4.216.2 Patch .....	134
CCMM\AAAD 6.4.216.3 Patch .....	134
Avaya Media Server (AMS) 6.4 SP16 Patches Listing .....	135
Contact Center Services for AMS (CCSA) 6.4 SP16 Patches Listing .....	135
<b>APPENDIX B - KNOWN ISSUES.....</b>	<b>136</b>
HARDWARE APPLIANCE .....	136
<i>Network Configuration.....</i>	<i>136</i>
THIRD-PARTY SOFTWARE .....	137
<i>Third Party Software Upgrade Utility .....</i>	<i>137</i>
<i>Third Party Software Downgrade Utility .....</i>	<i>138</i>
INTERNET EXPLORER COMPATIBILITY ISSUES.....	139
<i>Upgrading from Previous Avaya Aura® Contact Center 6.x Release .....</i>	<i>139</i>
PRE DVD INSTALLATION.....	140
AACC PRODUCT INSTALLATION.....	140
<i>Pre-Requisite Software known issues .....</i>	<i>140</i>
AACC PRODUCT UNINSTALLATION .....	141
DVD CONTROLLER.....	142
<i>Co-Res Installations .....</i>	<i>142</i>
COMMON COMPONENTS .....	142
CONTACT CENTER UPDATE MANAGER .....	146
SIP SPECIFIC ISSUES .....	146
SIP HA SPECIFIC ISSUES .....	148
AURA 7.0 SPECIFIC ISSUES .....	148
KNOWN CCMS LIMITATIONS .....	148
AVAYA MEDIA SERVER.....	149
<i>Linux Issues .....</i>	<i>149</i>
<i>Windows Issues.....</i>	<i>151</i>
CONTACT CENTER MANAGER SERVER .....	153
<i>Installation\Uninstall issues .....</i>	<i>153</i>
<i>Configuration Issues .....</i>	<i>153</i>
<i>Migration from NES 6.0 system .....</i>	<i>153</i>
<i>Known Issues With/Awaiting a Solution .....</i>	<i>153</i>
<i>Limitations.....</i>	<i>158</i>
NETWORK CONTROL CENTER (NCC) .....	160
LICENSE MANAGER.....	160
CONTACT CENTER MANAGER ADMINISTRATION .....	162
<b>SP16: CANNOT LAUNCH CCMA.....</b>	<b>179</b>
<b>AACC 6.4 SP15: PRIMARY SFW UNABLE TO COMPLETE BACKUP .....</b>	<b>180</b>

COMMUNICATION CONTROL TOOLKIT.....	182
CONTACT CENTER MULTIMEDIA .....	183
ORCHESTRATION DESIGNER .....	190
SECURITY FRAMEWORK.....	191
FEATURE SPECIFIC: POM INTEGRATION .....	191
FEATURE SPECIFIC: MULTIPLICITY.....	193
FEATURE SPECIFIC: HIGH AVAILABILITY.....	193
FEATURE SPECIFIC: AML TO SIP MIGRATIONS.....	196



## Purpose

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

## Publication History

Issue	Change Summary	Author(s)	Date
1.0	AACC SP16	Contact Center Release Engineering	April 2016
1.1	Beta Release	Contact Center Release Engineering	22 <sup>nd</sup> April 2016
1.2	GA Release	Contact Center Release Engineering	06 May 2016
1.4	Updating the Required Patches on CS1000 section	Contact Center Release Engineering	28 July 2016
1.5	Equinox 3.0 is not supported as an agent softphone	Contact Center Current Engineering	25 October 2016
1.6	Clarify that Hot Patching is not supported when upgrading to SP16 from any previous line-up	Contact Center Current Engineering	1 December 2016
1.7	Update CC-6354 with available solutions. TLS 1.0 only supported version with AACC 6.4. Updating CCMM known issues	Contact Center Current Engineering	13 December 2016

## **Avaya Aura® Contact Center, Release 6.4 SP16 Software**

**This Service Pack rolls up a number of critical fixes to issues reported by the customers and found in Avaya labs. Please take the following actions:**

- AACC 6.4 SP16 Software is the most up-to-date software line-up. All future patches will only be created on this line-up.
- When upgrading from previous AACC line-ups, please note that hot patching is not supported.

### **What's New in the AACC 6.4 SP16 release (that was not previously available in AACC 6.4 SP15)**

- Jetty – Third Party component upgrade
- Staggered network upgrade support in a Networking environment
- Increase in limit of Agent Skillset Assignments you can create to 1500
- AACC-IQ Modified Reporting of Queue Out Of Service

# Operating System & Virtualization

## Operating System Support

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

- Windows Server 2008 Release 2 Standard 64-bit Edition plus Service Pack 1
- Windows Server 2008 Release 2 Enterprise 64-bit Edition plus Service Pack 1

## Microsoft Service Packs

It is **mandatory** to install Service Pack 1 on top of Windows Server 2008 Release 2.

## Microsoft Hotfixes

Before deploying any new Windows Security Patches and Hotfixes you must confirm that any Windows patches are listed as supported in the Avaya Aura Contact Center Security Hotfixes and Compatibility listing. This is published every month on [support.avaya.com](http://support.avaya.com).

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

## Virtualized Environments

Avaya Aura® Contact Center 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)

In this release Avaya Aura Contact Center will be available in an Open Virtualization Archive (OVA) format and can be deployed using either VMWare vSphere or vCenter.

The deployment Avaya Aura Contact Center requires the following OVA images to be deployed:

- a) Avaya Media Server
- b) Avaya Aura Contact Center
- c) 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 Software** section below.

### IMPORTANT: VMWare Configuration Note

The VMware data store used to store the deployed software appliances must be at VMware Release 5.0, 5.1 or 5.5. 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.

## Software Download

### DVD Software

The supported Avaya Aura® Contact Center Release 6.4 DVD version is available from the support site

<https://support.avaya.com/css/appmanager/css/support/Downloads/P0793>

Please ensure you are using this version for all new software installation. Please contact your Avaya account representative for information on how to obtain the latest DVD.

DVD	MD5 Checksum
6.4.0.0-30.zip	1181f9a881b5a731919d3bcab5f50002

### Service Pack Bundle Software

The Avaya Aura® Contact Center 6.4 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.

**Important Note: Database updates**

During the installation of the service packs the updates to the database schemas may take some time to complete.

The application of the service packs may appear to be unresponsive during this period.

Please wait for the service pack installations to fully complete the database updates and **do not cancel the update process** unless otherwise prompted.

Service Pack Bundle	MD5 Checksum
AACC_64_ServicePack16-1696.zip	c665f64eb75e9b8a99f3e4fc8285bb92

After you have downloaded your software, please verify the MD5 checksum to ensure the file has been downloaded successfully. Please extract its contents to your local hard-disk using a utility such as WinZip.

The following is the layout of the extracted Service Pack bundle:

Software Included in Bundle		Folder Location
<b>Third Party</b>	AACCThirdPartySoftwareUpgradeUtility.exe	..\ThirdParty
<b>Install Software</b>	Avaya Media Server – Windows	..\Install Software\AMS\Windows
	Avaya Media Server – Linux	..\Install Software\AMS\Linux
	Contact Center Services for AMS – Windows	..\Install Software\AMS\Windows
	Contact Center Services for AMS - Linux	..\Install Software\AMS\Linux
	Security Framework	..\Install Software\Security Framework
	ActiveX Controls	..\Install Software\CCMA\ActiveX Controls
	CCMA XML Automated Assignments Service	..\Install Software\CCMA\XMLAutomatedAssignments

	Agent Desktop Client	..\Install Software\CCMM\
	Windows ASG Plugin	..\Install Software\Windows ASG Plugin
<b>Product Updates</b>	AACC Service Pack Software	..\ProductUpdates
<b>AACC Firewall Policy</b>	AACC Firewall Policy	..\AACC FirewallPolicy
<b>Support Applications</b>	AACC Support Applications	..\Support Applications

#### AACC Service Pack Software details

Component	Update Name
CCCC	AvayaAura_CCCC_6.4.216.0-1665_ServicePack
CCLM	AvayaAura_CCLM_6.4.216.0-1665_ServicePack
CCMA	AvayaAura_CCMA_6.4.216.0-1670_ServicePack
CCMM	AvayaAura_CCMM_6.4.216.0-1648_ServicePack
CCMS	AvayaAura_CCMS_6.4.216.0-1665_ServicePack
CCMSU	AvayaAura_CCMSU_6.4.216.0-1614_ServicePack
CCMT	AvayaAura_CCMT_6.4.216.0-1665_ServicePack
CCT	AvayaAura_CCT_6.4.216.0-1644_ServicePack
CCWS	AvayaAura_CCWS_6.4.216.0-1665_ServicePack
SFW	AvayaAura_SFW_6.4.216.0-1670_ServicePack

#### **Important Note:**

For all new systems install-time patching is a **mandatory** part of the installation process. The latest Service Packs for the component(s) being installed should be downloaded to the server and selected as part of the installation process.

Avaya Aura® Contact Center 6.4 SP16 is applicable to all previous Avaya Aura® Contact Center 6.x Releases. After you have installed this Service Pack your system will be running Avaya Aura® Contact Center Release 6.4 SP16 software.

## Additional Contact Center Updates

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

Patches	MD5 Checksum
AACC_64_ServicePack16_Patches-1007.zip	ace3a9738c34942a0b7475134f14fd1a

Please verify the MD5 checksum after download to ensure the file has been downloaded successfully.

This patch is required by sites who have or are planning on configuring Backup Voice Proxy

## Additional Software in Bundle

The following additional software is also delivered in the bundle of patches

Software Included in Bundle	Folder Location
<b>Install Software</b>	ActiveX Controls
	AvayaAuraAgentDesktopClient
	..\Install Software\CCMM\AvayaAura_CCMM_6.4.216.3-1375\

## Patch Scanner

The following is an additional utility Avaya Aura® Contact Center support tool. This patch Scanner utility is released with every ServicePack and Patch bundle from SP13 onwards.

If you are upgrading to a ServicePack or patch lineup – you must use the Patch Scanner version published in the release note of that lineup.

This version of the tool can be used prior to performing upgrades to 6.4 ServicePack 15 regardless of the lineup that one is upgrading from. See readme within application zip file for further information.

Patches	MD5 Checksum
patchscanner_1.0.0.13.zip	2fac4ce9b19b8c769ec6cefea4a9539c

Please verify the MD5 checksum after download to ensure the file has been downloaded successfully.

## Avaya Media Server Software

The following software is available in the Avaya Aura® Contact Center 6.4 SP16 Service Pack bundle.

OS Platform	Install Software	Version	Folder Location
<b>Windows</b>	InstallerMAS.exe		..\Install Software\AMS\Windows
	ContactCenterServicesForAMS.msi		..\Install Software\AMS\Windows
<b>Linux</b>	MediaServer_7.6.0.959_2014.11.27.bin		..\Install Software\AMS\Linux
	ContactCenterServicesForAMS_6.4.0.158.bin		..\Install Software\AMS\Linux

Please see the Section [Avaya Media Server](#) for details on how to install the Avaya Media Server software components. This section discusses both new installations and existing system upgrades for both Windows and Linux.

## Additional Avaya Media Server Updates

File Name	MD5 Checksum
AMS_QFE_ServicePack16-0003.zip	622e81f09b287d40acc727f79cf8ad8c
CCSA_QFE_ServicePack16-0002.zip	8fb3d8413928d41eafc6912ba7f82c3a

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

**Note:** The individual updates included in these packages are known as QFEs and come delivered as a zip file. These zip files should be copied to the Avaya Media Server's QFE folder in zipped form.

Refer to the README.txt files contained within each for installation instructions.

## Software Appliance Software

The following are the files required to deploy Avaya Aura® Contact Center, Release 6.4 SP16 into a virtualization environment. Please ensure you are using this version for all new software installation.

You must deploy the **Avaya Aura Contact Center 6.4 Service Pack 15 Software Appliance** and then perform a software upgrade to Service Pack 16. The following is the link to the software appliance download page: [https://support.avaya.com/downloads/download-details.action?contentId=C20154171843181930\\_9&productId=P0793&releaseId=6.4.x](https://support.avaya.com/downloads/download-details.action?contentId=C20154171843181930_9&productId=P0793&releaseId=6.4.x)

This is applicable to both Avaya Aura Contact Center OVA and the Avaya Media Server OVA

## Avaya Aura Contact Center OVA Image

File Name	MD5 Checksum
AACC_64_DVD30_RB1323_289_20150124_0541.ova	eea7b3cd88eb08a533837b6e1fb26019

Please verify the MD5 checksum after download to ensure the file has been downloaded successfully.

After you have downloaded your software extract the content to your local hard-disk using the utility 7-Zip. The zip file will extract as one OVA file.



## Avaya Media Server OVA Image

File Name	MD5 Checksum
ACC_64_AMS-7.6.0.959_CCSA-6.4.0.158_01_20141222_1616.ova	2af1ea1b67617d6952b6b9039a86aa4f

Please verify the MD5 checksum after download to ensure the file has been downloaded successfully.

## Avaya WebLM OVA Image

The Avaya WebLM software is a required piece of software when deploying the OVAs in a virtualization environment. This software is used for product licensing. Please download the **WebLM 6.3.2**

**Virtualization Enablement (VE) vAppliance** from the Avaya Support Site,

[https://support.avaya.com/downloads/download-details.action?contentId=C2013561630303600\\_5&productId=P0541](https://support.avaya.com/downloads/download-details.action?contentId=C2013561630303600_5&productId=P0541)

Please download and install the latest version of the WebLM software on your OVA deployment. WebLM 6.3.8 can be downloaded from the Avaya Support Site:

[https://support.avaya.com/downloads/download-details.action?contentId=C2014528154813180\\_7&productId=P0541&releaseId=6.3.x](https://support.avaya.com/downloads/download-details.action?contentId=C2014528154813180_7&productId=P0541&releaseId=6.3.x)

This Software can be installed on top of WebLM 6.3.2 or 6.3.3 or 6.3.4 or 6.3.5 or 6.3.7 release. Refer WebLM 6.3.8 Release Notes for instructions on how to install the software.

**File Name** - WebLM\_6.3.8\_r4502368.bin

**MD5 Sum** - e119e92807667c5c1933abe5a4f853d6

The WebLM Release notes can be accessed from:

<https://downloads.avaya.com/css/P8/documents/100180574>

## AACC Firewall Policy

Avaya do not recommend making changes to the Avaya customized Firewall Policy but if changes are made, then it is the responsibility of the customer to manually track/manage their changes. These changes will not be carried forward with a Service Pack upgrade.

The AACC Firewall policy is deployed by Common Components. It is also contained within the Service Pack zip file under the following sub folder:

### AACCFirewallPolicy

File Name	Version
AACC Firewall Policy (Ver 1.19).wfw	1.19

## Mandatory Microsoft 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	File Name	MD5 Checksum
<a href="#">KB2600217</a>	NDP40-KB2600217-x64.exe This patch can be downloaded from from <a href="https://support.microsoft.com">https://support.microsoft.com</a>	0266266553ae18c1088f37a78f8d3ca5

### Important Notes:

1. This update must be applied to your system as a **local administrator**.
2. **KB2600217** is an update to .NET 4. It should be applied after installing AACC 6.4 as .NET 4 is installed as part of AACC 6.4. This patch addresses a memory leak in .NET Framework 4.0 which affects the Log Archiver process on all AACC and ACCS configurations.

Update ID	File Name	MD5 Checksum
<a href="#">KB982638</a>	MicrosoftDotNetFramework4.0LimitedPatch.zip (includes 415512_intl_x64_zip.exe) This patch <b>must</b> be downloaded from <a href="https://support.avaya.com">https://support.avaya.com</a>	deada04a7b12d0342cf14dc0804c0109

Update ID	File Name	MD5 Checksum
<a href="#">KB2742595</a>	NDP40-KB2742595-x64.exe This patch can be downloaded from from <a href="https://support.microsoft.com">https://support.microsoft.com</a>	4d5081f0e6ef496e640537ab0d892e92

### Important Notes:

1. These updates must be applied to your system as a **local administrator**.
2. The MSFT patches should be applied in the following order
  - a. **KB2600217** – available from **Microsoft support website**
  - b. **KB982638** – must be downloaded from <https://support.avaya.com>
  - c. **KB2742595** – available from **Microsoft support website**
3. After installation of the patches a reboot of the server must be performed.

4. These last two patches address a vulnerability in .NET Framework 4.0 which can lead to SMMC crashing affecting AACC MCHA and ACCS BC switcover operation.
5. These patches should be applied to all AACC(SIP, AML) and ACCS systems. This vulnerability exists with all AACC and ACCS releases and the MSFT hot fixes are applicable for all releases. The Microsoft fixes have only been tested on the latest supported AACC and ACCS lineup SP16.

## Important Guidelines for 3rd Party Software Updates Outside of Avaya SP/Patch Updates

The AACC 6.X applications contains a number of 3rd party software applications and components which are utilised by the AACC 6.x application. These 3rd party software applications must never be updated to the manufacturers latest published versions outside of an Avaya AACC 6.X SP/Patch upgrade.

The following 3rd party software applications shall only be updated to a newer version during an Avaya SP/Patch update. Each of these software applications are shown with their version numbers in the SP 15 release.

- Tomcat Release: **7.0.35**
- Java Runtime Environment (JRE) Release: jdk1.6.0\_37
- Microsoft .NET Framework Release: .NET 4.0
- Visual C++ runtime libraries Release: 2005, 2008, 2010 (32 and 64 bit versions)

If there are newer versions of these applications available from the manufacturer, they shall not be installed on the AACC 6.X application without prior consent from Avaya. Upgrading to newer versions will invalidate the current support agreements.

## Support of Headset control of telephony operations in AAAD

This release contains support for headsets controlling telephony operations whilst AAAD is operating in embedded softphone mode. This support is facilitated by installing the AAADHeadsetSupport.msi on all clients PCs that require this functionality. This process is documented in the Fundamentals and Planning Guide. Please note that this has been validated by the verification team with 2.7.0.0 of the Plantronics Spokes Installer only.

File Name	MD5 Checksum
AAADHeadsetSupport.zip	15ed9070fc0baea1863257e66be4d9a0

## Support of IQ 5.2.6

AACC is supported with IQ 5.2.6.

## Avaya Aura Contact Center call networking compatibility issue

An issue has been identified where in a networking AACC contact center – calls are not routed from a CCMS node to other CCMS nodes in the network, if they are on a different SP lineup.

When a networking site upgrades a CCMS node to AACC 6.4 - that site can no longer route calls to another node on their network that is running an earlier lineup –and the node running the earlier lineup cannot route to the AACC 6.4 node (calls cannot be routed either way).

**For example** if the source CCMS node is installed with AACC 6.3 SP 11 and the target node is installed with AACC 6.4 SP 16, the compatibility issue exists and call routing requests will fail.

The following table lists a compatibility matrix between the source node and the target node in the AACC networking configuration:

Source /Target Node Lineup	SP11 (or earlier SP)	SP12	SP13	SP14	SP15	SP 16
SP11 (Or earlier SP)	+	-	-	-	-	
SP12	-	+	+	-	-	
SP13	-	+	+	-	-	
SP14	-	-	-	+	+	
SP15	-	-	-	+	+	
SP 16	-	-	-	+	+	+

+ Means that the Source and Target node lineups are compatible

- Means that the Source and Target node lineups are NOT compatible

This issue affects:

- Networking AACC sites that upgrade a CCMS node to AACC 6.4 (i.e.: SP12, SP13, SP14 or SP15 ) - if they are using Landing pads to route their calls

This issue does not affect:

- ACCS Sites
- Nodal AACC sites
- Networking sites that are not using Landing Pads to route calls
- Networking sites that are using Landing pads to integrate with AAEP
- Sites that use any 3rd party client application that may reserve “Landing Pads” using the CMF web services.

An AACC patch will be created to assist network sites planning to upgrade. This patch must be installed during the upgrade to the SP 16 patch line-up maintenance window.

## Avaya Grep

Avaya Grep is a tool for analyzing and debugging Avaya Aura® Contact Center calls.

Avaya Grep generates a range of reports on a specific call by analyzing the Avaya Aura® Contact Center logs, including a ladder-diagram representation of SIP messages through user-agents and proxies. A search feature is also available for those instances where the user does not know the call ID, but has some other information on the call, e.g. the agent DN number and the approximate time of the call.

More information is included in the application's Help file, and in a user guide bundled with the application (found in the "documentation" directory of the download).

File Name	MD5 Checksum
<b>AvayaGrep_v0.4.2_56.zip</b>	1b9baeea857ddf7eff82f6f8fa9cb193

## Avaya SIP Sleuth

Avaya SIP Sleuth is a tool for viewing, analyzing, filtering and querying SIP message logs.

Supported logs are Avaya Aura® Contact Center Manager Server and Avaya Media Server SIP message logs. SIP Sleuth features a powerful filtering engine, a custom query language for filtering SIP messages and command-line access to enable batch-processing from the shell.

More information is included in the application's Help file, and in a user-guide bundled with the application (found in the "documentation" folder of the download).

File Name	MD5 Checksum
<b>SipSleuth_v0.94.zip</b>	42d5c697e681454e81739ec883545d7d

## Third-Party Software

### Third Party Software for New Installations

For new installations, using the Avaya Aura® Contact Center 6.4 DVD, you must upgrade installed Third Party software. (See section Third Party Software Upgrade Utility).

### Intersystems System Management Portal

Intersystem Cache installs a default Web server. The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

Customer can disable the Windows service “Web Server for CCDSInstance”. This web service is used for cache debugging and admin and is not required for normal operation on AACC.

### Third Party Software for Previous 6.x Upgrades

If you are upgrading from a previous Avaya Aura® Contact Center release you must upgrade installed Third Party software. If you are upgrading software on a server operating system, the Third Party Software Upgrade Utility must be used (see section Third Party Software Upgrade Utility). For Third party software upgrades on Microsoft Windows desktop systems, please see section Third Party Software Upgrades on Windows desktop systems.

### Java Runtime Environment – jre1.6.0\_37

Due to a known Java Issue with jre1.6.0\_37, the system may fail to shutdown successfully if any Java Applications are still running. Please ensure all Applications are closed before Shutting down or Restarting the Server.

### WinPcap

In the Avaya Aura® Contact Center Commissioning document, there are detailed instructions for installing WinPCap in a Mission Critical HA environment. However there are other configurations where WinPCap should be installed.

WinPCap should be installed on the following systems:

- All RnR systems, including AML HA.
- RGN node in a Disaster Recovery configuration.
- Standalone Aura SIP configurations.

The detailed instructions as described for the mission critical HA can be used to deploy WinPCap on all environments.

### McAfee Antivirus

As McAfee can block systems from sending out automatic e-mails, in any system that a switchover are allowed (such as a Mission Critical High Availability system), it's recommend turning off the “Prevent mass mailing worms from sending mail” setting on each machine to ensure notifications will be sent.

## Third Party Software Upgrades on Windows desktop systems

**NOTE: only applicable to those systems on which the Common Components Service Pack will be deployed**

If upgrading Contact Center components for previous 6.x line-ups on Windows desktops e.g. Windows 7 etc. an upgrade of Third Party software is required.

This Third Party software upgrade must be performed manually before you deploy the 6.4 SP16 components.

The Third Party Software Upgrade and Downgrade Utilities should **not** be used on Windows desktop systems.

The 6.4 Common Components Service Pack will fail to install if Third Party software is not upgraded. The 6.4 Common Components Service Pack requires that both .Net Framework 4 and Microsoft Visual C 2010 10.0.40219 Redistributables be installed on all systems (both server and desktop).

To manually install required Third Party software on Windows desktop systems:

1. Browse to the Service Pack Release bundle location ...\\ThirdParty\\ThirdPartySoftware
2. Copy folders DotNetFX40 and MSVC2010Redist\_10.0.40019.1\_x86 to a location on your system
3. From the local MSVC2010Redist\_10.0.40019.1\_x86 folder, execute **setup.exe** and follow the onscreen prompts – wait for completion
4. From the local DotNetFX folder, execute setup.exe and follow the onscreen prompts – wait for completion

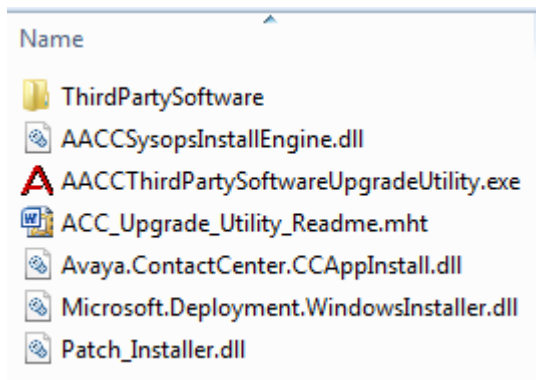
## Third Party Software Upgrade Utility

The Third Party Software Upgrade Utility assists in the upgrade of specific 3<sup>rd</sup> Party software components required by Avaya Aura® Contact Center.

### Utility Location

The utility is included within the Service Pack Release Bundle, available to download from ftp site, details in the Software Download Section of this document.

- The utility should only be launched on Avaya Aura® Contact Center servers. It should not be executed on Avaya Aura® Contact Center clients (e.g. Windows 7/8 desktops)
- The entire utility and supporting files should be copied locally before launching. The utility is contained within folder:  
<ServicePackReleaseBundle\_Root>\ThirdParty
- The utility and supporting files are listed in the below screenshot. All content must be copied locally.



**Important:** Failure to copy and execute the complete utility from a local drive may result in downgrade failure.

### Fresh Installations

It is a **mandatory requirement** to run the Third Party Software Upgrade Utility after deployment of 6.4 Contact Center software using the 6.4 Avaya Aura® Contact Center DVD.\*

\*Please also see section **Contact Center installations without Contact Center Manager Administration (CCMA)**

Although the 6.4 DVD deploys the majority of the Third Party software required to support the Contact Center product, the Third Party Software Upgrade Utility must be launched to verify the current Third Party software and to install any missing Third Party Software components.

The Third Party Software Upgrade Utility must be launched **after** the installation of the Avaya Aura® Contact Center product when performing a fresh install.

### Fresh Installations – Pre Execution Instructions

1. Copy the ACC 6.4 Third Party Software Upgrade Utility locally
2. Shut-down Contact Center
3. Launch AACCThirdPartySoftwareUpgradeUtility.exe from your local folder
4. Click Upgrade on the Third Party Software Upgrade Utility to begin the upgrade process.



## Fresh Installations – Post Execution Instructions

1. After the Third Party software upgrade completes, you must reboot your system to restart Avaya Aura® Contact Center services.
2. If prompted to reboot your system during or after the upgrade of Third Party software, please do so.

## Fresh Installs – Third Party Software Upgraded

The utility will upgrade the following 3<sup>rd</sup> Party Software components:

Software	Platform	Upgrade From Old Version	To New Version
Crystal RAS	x86	2011 SP5	2011 SP8

Table 1 – 3<sup>rd</sup> Party Software Matrix

### Contact Center installations without Contact Center Manager Administration (CCMA)

Crystal RAS will be upgraded only if the Contact Center Manager Administration (CCMA) component is installed.

Crystal RAS is not required for any other Contact Center component therefore if CCMA is not present, the Third Party Upgrade Utility will indicate, when launched, that all Third Party software is at the desired level.

## Upgrades from 6.x

It is a **mandatory requirement** to run the Third Party Software Upgrade Utility when upgrading your system to a 6.4 Service Pack 14 or later line-up.

All installed Service Packs must be removed **before** running the Third Party Software Upgrade Utility. After removal of all installed Service Packs, the Third Party Software Upgrade Utility can be launched and once complete, the 6.4 Service Pack 14 or later line-up can be installed.

## Upgrades from 6.x – Pre Execution Instructions

1. Remove all ACC pre-6.4 SP16 Service Packs from your system
2. Reboot your system if prompted to do so
3. Copy the ACC 6.4 Third Party Software Upgrade Utility locally
4. Shut-down Contact Center
5. Launch AACCThirdPartySoftwareUpgradeUtility.exe from your local folder
6. Click Upgrade on the Third Party Software Upgrade Utility to begin the upgrade process.

## Upgrades from 6.x – Post Execution Instructions

1. After the Third Party software upgrade completes, you must install Avaya Aura® Contact Center 6.4 SP16 Service Packs.
2. If prompted to reboot your system during the upgrade of Third Party software, please do so
3. Install the Common Components Service Pack first.
4. Reboot your system.
5. Continue to install all other Server Packs and patches after the reboot has completed.
6. Reboot your system once the installation of the 6.4 Service Pack 15 line-up is complete

## Third Party Software Upgraded

The utility will upgrade the following 3<sup>rd</sup> Party Software components:

Software	Platform	Upgrade From Old Version	To New Version
Java Runtime Environment	x86	1.6.0 Update 17	1.6.0 Update 37
Java Runtime Environment	x64	1.6.0 Update 21	1.6.0 Update 37
Java Development Kit	x86	1.6.0 Update 17	1.6.0 Update 37
Apache Tomcat	x64	6.0.20 or 6.0.35	7.0.35
VC++ 2010 Redist	x86	n/a	10.0.40219.1
VC++ 2010 Redist	x64	n/a	10.0.40219.1
MS .Net Framework 4	x86\x64	n/a	4.0.30319
Crystal RAS	x86	2008 or 2011 SP5	2011 SP8

Table 2 – 3<sup>rd</sup> Party Software Matrix

**Note:** Not all software is required across all AACC 6.4 SP16 installations. Only that software which is required for the current AACC feature set is installed e.g. Crystal RAS is only installed if CCMA is present.

**Note:** If upgrading from SP14, all third party software required for SP16 should already be installed. In this scenario the Upgrade Utility should still be executed to verify that all required software is present.

## Utility Reboot Prompts

During the course of the upgrade, installation or removal of 3<sup>rd</sup> Party software components may request a system reboot. This request is intercepted by the utility and a mandatory Reboot Request is displayed – please choose the option to reboot your system at this point.

If you do not reboot, your system could be left in an unstable state. After system reboot, the utility should automatically re-launch. If it does not, please browse to the local copy of the utility and re-launch manually.

## Third Party Software Component Upgrade Failure

It is possible that the upgrade of a software component fails. In this instance, the utility will halt the upgrade process.

The failed component will be highlighted on the main utility dialog. The utility log file (accessible via the *View Log* button) may include the failure reason and will detail the location of the 3<sup>rd</sup> Party software component generated log file.

The 3<sup>rd</sup> Party software component generated log file is the most important source of information when trouble-shooting failed component upgrade attempts.

## Logging Information

The utility generates a log file to track overall upgrade progress.

Log file title : ACC – Third Party Software Upgrade Utility.log

Log file location : C:\Avaya\Logs\Sysops\ThirdPartySoftwareUpgradeUtility

In addition to the above log file, each individual Third Party software component that is processed during the upgrade generates a separate log file in the same folder location.

Example: Upgrading to Java Runtime Environment x86 1.6.0 Update 37

- Java Runtime Environment x86 1.6.0 Update 17 is removed, generating log file:  
Remove\_Java Runtime Environment 6\_1.6.0 Update 17\_x86.log
- Java Runtime Environment x86 1.6.0 Update 37 is installed, generating log file:  
Install\_Java Runtime Environment 6\_1.6.0 Update 37\_x86.log

## Third Party Software Downgrade Utility

When upgrading from a previous AACC 6.x installation, before deployment of Avaya Aura® Contact Center 6.4 SP16 Service Packs, it is required that Third Party software be upgraded using the AACC 6.4 Third Party Software Upgrade Utility.

If a user wishes to subsequently **downgrade** their system to a pre-6.4 SP16 Service Pack line-up e.g. Service Pack 11 or 10 etc., the installed Third party software must be downgraded also. The AACC 6.4 Third Party Software Downgrade Utility will assist in this process.

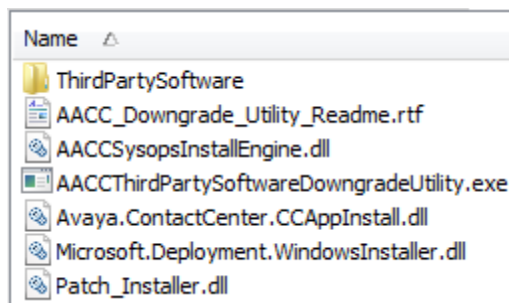
### Utility Location

The utility is available for download from the Avaya Support website, <http://support.avaya.com> in the form of a Zip archive. Please note there has been no updates to Third Party software in this release so the AACC\_64\_ServicePack14\_TPSoftwareDowngradeUtility\_01.zip can be used to downgrade an SP16 system.

File Name	MD5 Checksum
AACC_64_ServicePack14_TPSoftwareDowngradeUtility_01.zip	d241fc71dda07221c0f0fe80688fe9a2

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

- The utility should only be launched on Avaya Aura® Contact Center servers. It should not be executed on Avaya Aura® Contact Center clients (e.g. Windows 7/8 desktops)
- The Zip should be downloaded and extracted locally. The complete Zip file listing can be seen in the below screenshot:



**Important: Failure to copy and execute the complete utility from a local drive may result in downgrade failure.**

### Execution Instructions

1. Copy the AACC 6.4 Third Party Software Downgrade Utility locally
2. Shutdown Avaya Aura® Contact Center
3. Launch AACCThirdPartySoftwareDowngradeUtility.exe from local folder
4. Select a target Service Pack from the utility drop-down list
5. Click Update
6. Follow the prompts displayed by the utility:  
Depending on your chosen target Service Pack, you may be required to either install a complete Service Pack line-up before continuing, or remove all installed Service Packs as follows:
  - a. If your target AACC Service Pack is version 10 or 11, you will be required to install a complete line-up of these Service Packs before installation of Third Party software is possible.  
Please close the Downgrade utility whilst installing the required Service Pack line-up.

After installation of the full AACC Service Pack line-up, repeat steps 2 – 6

- b. If your target Service Pack is anything other than SP10 or 11, you will be asked to remove all installed Service Packs.  
Please close the Downgrade utility while removing installed Service Packs.  
After removal of installed Service Packs, repeat steps 2 – 6.  
At the end of downgrade, you will be informed that you can now install your chosen target Service Pack line-up.

## Post Execution Instructions

If you have installed Third Party software for SP10 or SP11, you must reboot the system to restart Contact Center services.

If you have installed Third Party software for non-SP10\SP11 line-ups, you should now install your chosen target Service Pack line-up.

## Third Party Software Downgraded

The utility will install Third Party Software components to the following versions, based on the target Service Pack line-up:

Software	Platform	Version	6.2 Service Pack				6.3 Service Pack				6.4 Service Pack	
			4	5	6	7	8	9	10	11	12	13 or higher
Java Runtime Environment	x86	1.6.0 U17	✓	✓	✓	✓	✓	✓				
Java Runtime Environment	x64	1.6.0 U21	✓	✓	✓	✓	✓	✓				
Java Runtime Environment	x86	1.6.0 U37							✓	✓	✓	✓
Java Runtime Environment	x64	1.6.0 U37							✓	✓	✓	✓
Java Development Kit	x86	1.6.0 U17	✓	✓	✓	✓	✓	✓				
Java Development Kit	x86	1.6.0 U37							✓	✓	✓	✓
Apache Tomcat	x86	6.0.20	✓	✓	✓	✓	✓	✓				
Apache Tomcat	x64	6.0.35							✓	✓		
Apache Tomcat	x64	7.0.35									✓	✓
Crystal RAS 2008	x86	12.3.0.601	✓									
Crystal RAS 2008	x86	12.4.0.966		✓	✓	✓						
Crystal RAS 2008	x86	12.5.0.1190					✓	✓	✓	✓		
Crystal RAS 2011SP5	x86	14.0.5.882									✓	
Crystal RAS 2011SP8	x86	14.0.8.1229										✓
VC++ 2010 Redist	x86	10.0.40219.1									✓	✓
VC++ 2010 Redist	x64	10.0.40219.1									✓	✓
MS .Net Framework 4	x86\x64	4.0.30319									✓	✓

**Table 3 – Third Party Software Matrix**

**Note:** not all software is required across all Contact Center 6.4 SP16 installations. Only that software which is required for the current Contact Center feature set will be installed e.g. Crystal RAS is only installed if CCMA is present.

## Utility Reboot Prompts

During the course of the downgrade, the installation or removal of 3<sup>rd</sup> Party software components may request a system reboot. This request is intercepted by the utility and a mandatory Reboot Request is displayed – please choose the option to reboot your system at this point.

If you do not reboot, your system could be left in an unstable state.

After system reboot, the utility should automatically re-launch. If it does not, please browse to the local copy of the utility and re-launch manually.

## Third Party Software Component Downgrade Failure

It is possible that the downgrade of a software component fails. In this instance, the utility will halt the downgrade process.

The failed component will be highlighted on the main utility dialog. The utility log file (accessible via the *View Log* button) may include the failure reason and will detail the location of the 3<sup>rd</sup> Party software component generated log file.

The 3<sup>rd</sup> Party software component generated log file is the most important source of information when trouble-shooting failed component downgrade attempts.

## Logging Information

The utility generates a log file to track overall upgrade progress.

Log file title : ACC – Third Party Software Downgrade Utility.log

Log file location : C:\Avaya\Logs\Sysops\ThirdPartySoftwareDowngradeUtility

In addition to the above log file, each individual 3<sup>rd</sup> Party software component that is processed during the downgrade generates a separate log file in the same folder location.

Example: Downgrading to Java Runtime Environment x86 1.6.0 Update 17

- Java Runtime Environment x86 1.6.0 Update 37 is removed, generating log file:  
Remove\_Java Runtime Environment 6\_1.6.0 Update 37\_x86.log
- Java Runtime Environment x86 1.6.0 Update 17 is installed, generating log file:  
Install\_Java Runtime Environment 6\_1.6.0 Update 17\_x86.log

## Important Note

- Avaya Aura® Contact Center Service Pack 6.4 SP16 requires a Third Party software upgrade to support Java dependent product components.

The Communication Control Toolkit NCCT OI Service in AACC 6.4 SP16 (and AACC 6.4 SP12, SP13, SP14 and 6.3 SP10 & SP11) requires JRE 1.6.0 Update 37 (32 bit) to function.

This service requires JRE 1.6.0 Update 17 (32 bit) on pre-AACC 6.3 SP10 systems.

- If, after the upgrade to AACC 6.4 SP16, a user wishes to downgrade to an AACC pre-6.4 SP16 line-up e.g. 6.3 Service Pack 11 (or earlier) they must also downgrade their Third Party software.
- If the Third Party Software Downgrade Utility has not been run before downgrading to 6.3 Service Pack 9, 8, 7 or 6.2 Service 6, 5 etc. the 6.3 Service Pack 9 (or earlier) NCCT OI Service will fail to start.

## Avaya Contact Center Software Notification Application

As part of an AACC 6.4 SP16 deployment, an Avaya Contact Center Software Notification Application is installed.

This application checks the integrity of the Third Party software required by Avaya Aura® Contact Center. If the application detects that necessary Third Party software requires updating, it will prompt the user to run either the Third Party Software Upgrade or Downgrade Utility to check their system and update if necessary.

At each system reboot, an application dialog will be displayed with details of the Third Party software status if an issue is found. This dialog can be dismissed and the application will minimize to the system tray. At intervals, notification messages are displayed in the system tray area in the form of a notification bubble, if action is required. The main application form will be displayed if a user clicks on this notification or on the Avaya system tray icon

The Notification application starts automatically when the Windows Operating System starts. Once running it can be closed by right-clicking on the task tray icon and selecting the option to quit.

This application remains resident on the system after removal of Avaya Aura® Contact Center 6.4 SP16. This allows for the ongoing provision of advice to the user, regarding the Third Party software state.

### Application Behaviour

If AACC 6.4 SP16 is installed but required Third Party software is not present on the system, the Avaya Contact Center Software Notification Application will intermittently (approximately once per hour) notify the user that action is required.

If after deployment of AACC 6.4 SP16, a user chooses to remove all installed Service Packs, the application (after a period) will provide advice to the user in preparation for the installation of the next Service Pack.

The application will also monitor the state of installed Service Packs. If an inconsistent (versions if installed Service Packs differ from each other) or an incomplete Service Pack line-up is installed, the Notification application will warn the user.

### Logging Information

The application generates a log file.

Log file title	: ACC – Software Notification Application.log
Log file location	: C:\Avaya\Logs\Sysops\SoftwareNotificationApplication

This log file is accessible from the main dialog via the View Log button.

The log contains details of the currently installed Service Pack line-up, and in addition, details of the installed or missing Third Party software components.

## Internet Explorer Compatibility issues

Element Manager and CCMA require that Internet Explorer 9.0, Internet Explorer 10.0 and Internet Explorer 11.0 be configured to run the web sites in “Compatibility Mode”.

Microsoft support indicates that some websites might not display correctly in Windows Internet Explorer 9. For example, portions of a webpage might be missing, information in a table might be in the wrong locations, or colors and text might be incorrect. Some Webpages might not display at all. If a portion of the webpage doesn't display correctly, try one or more of the following procedures:

**Note: IE Compatibility Mode must be enabled on IE 9.0, IE 10.0 and IE11.0**

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 7.0 or later **(32 Bit only – 64 Bit not supported)**.



## Third Party Software Support Applications

As part of AACC 6.4 SP16, a Third Party Software “SupportApplications” folder has been added to the release.

This is not a mandatory install.

It contains a Notepad++ installer that can be installed on AACC Servers and used as an alternative text editor to Notepad for reviewing logs.

Location in the release bundle: [\\SupportApplications\npp.6.5.4.Installer.exe](#)

### Notepad++ install instructions

- 1) Double click npp.6.5.4.Installer.exe
- 2) Installer Language: Select your language
- 3) Welcome screen: Click Next:
- 4) License agreement: Click I Agree
- 5) Install Location: Choose your destination folder and click Next
- 6) Choose Components, type of install: Select the Custom option & select the components you require
  - a. Optional components of note
    - i. Context Menu Entry: Ensure this is selected to enable a straightforward way of creating file associations.
    - ii. Auto-Updater: Un-ticking this this will ensure you do not get messages about new versions available. If this is something you do want, then leave this box ticked.

Click Next

- 7) Choose Components: Additional Features: Click Install:  
Installing...
- 8) Click Finish:

### Post install instructions

#### To make Notepad++ the default editor for .log files

- Right click a .log file
- Select “Open with...”
- Browse to the location of notepad++.exe and click “Open”
- Ensure the tick box “Always use the selected program to open this kind of file” is ticked

#### To disable Auto-Updater

If Auto-Updater is enabled, Notepad++ will look for updates each time Notepad++ is started and if available, you will be prompted to update. If you do not want this to happen, and if you didn’t un-tick this option on install, then

- Open Notepad++
- Settings
- Preferences
- MISC
- Un tick Enable Notepad++ auto-updater

## Equinox 3.0 Not Supported for use as an Agent Softphone

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

## AACC 6.4 SP16 Service Pack Software

### New Installations

For all new systems install-time patching is a **mandatory** part of the installation process. The latest Service Packs for the component(s) being installed should be downloaded to the server and selected as part of the installation process.

**Note:** Additional Contact Center Updates must be installed after you have completed the initial installation of your software and reboot of the system performed.

**Note:** Users that install AACC 6.4 SP16 as a fresh install are not supported to downgrade to 6.2.

**Note:** Security Framework must be disabled and re-enabled following an upgrade to this Service Pack if it is in use on the AACC server. (See “Security Framework” section of this document for more details).

### Hot Patching Mission Critical or AML Warm Standby HA Systems to AACC 6.4 SP16

**HOT PATCHING FROM ANY PREVIOUS LINE-UP TO AACC 6.4 SP16 IS NOT SUPPORTED. THIS APPLIES TO BOTH AML AND SIP INSTALLATIONS.**

**PLEASE REFER TO THE PATCHING WHITEPAPERS on [support.avaya.com](http://support.avaya.com) FOR ALTERNATIVE PATCHING PROCEDURES IN A MISSION CRITICAL HA ENVIRONMENT :**

**Avaya Aura® Contact Center R6.4 Mission Critical High Availability:  
Patching Procedure for Least Downtime**

**OR**

**Avaya Aura® Contact Center R6.4 Mission Critical High Availability:  
Patching Procedure for No Data Loss**

#### Known Issues:

##### Interval Statistics

During the Upgrade procedures provided in the whitepapers the Standby Server is not always Shadowing the Active Server, this can result in the latest Interval Statistics being missing from any Backup taken on the Active Server.

The Interval Statistics files will remain on the Active Server until it has been Upgraded and returned to Active Mode, at which time, the Interval Statistics will be correctly written to the Database.

To ensure that all the Interval Statistics are correctly written to the Database a minimum of 15 minutes should elapse between shutting down the Contact Center on the Active Server and Starting the Standby Server in Active Mode.

While the Standby Server is running in Active Mode during the Upgrade it is recommended not to run any Historical Reports against Interval Statistics as the data may not be complete.

**Note:** All Limited Patches support Hot Patching unless otherwise stated in the patch README.

## Downgrade (Avaya Aura® Contact Center 6.4 SP16 to a previous release) Avaya Aura Contact Center

This procedure should be executed in the event that the contact center must be downgraded from Avaya Aura® Contact Center 6.4 SP16 to a previous release.

1. Ensure that the Contact Center database backup scheduled prior to the upgrade to Avaya Aura® Contact Center 6.4 SP16 is available
2. Downgrade 3<sup>rd</sup> Party software using the Third Party Software Downgrade Utility
3. Downgrade the system from Avaya Aura® Contact Center 6.4 SP16 to a previous release via Patch Manager. The 2 step downgrade process is as follows:-
  - a. Remove all Service Packs for Avaya Aura® Contact Center 6.4 SP16
  - b. Install all Service Packs for the previous Avaya Aura® Contact Center release

**Important:** at step 3, the Third Party Software Downgrade Utility may provide instructions regarding the removal of existing Service Packs and installation of others. The sequence indicated by the Downgrade utility should be preferred over step 4.

4. Recover the system and ensure that all services have started via the System Control & Monitoring Utility (SCMU)
5. Restore the database(s) previously backed up prior to upgrading to Avaya Aura® Contact Center 6.4 SP16

## Avaya Media Server

This procedure should be executed on the Avaya Media Server in the event that the contact center must be downgraded from Avaya Aura® Contact Center 6.4 SP16 to a previous release.

### Avaya Media Server on Windows

1. Ensure that the Avaya Media Server database backup scheduled prior to the upgrade to Avaya Aura® Contact Center 6.4 SP16 and the locale specific media files that were backed up are available (only for Voice and Multimedia Contact Server with Avaya Media Server deployments)
2. If this is a standalone AMS primary node using PLIC licensing, take a copy of the license from the Primary AMS Server (*AACC Upgrade and Patches 44400-410*) – this is not required if AACC is using WebLM licensing. Note: Licensing is not preserved in AMS backup
3. Uninstall *Contact Center Services for AMS* via the Windows Control Panel
4. Uninstall Avaya Media Server 7.6 via the Windows Control Panel. When prompted to preserve or remove data, select the 'Remove' option.
5. Locate the **Install Software\AMS\Windows** folder on the AACC Previous Release Bundle, launch the Avaya Media Server installer and proceed through the installation wizard:  
**InstallerMAS.exe**
6. Launch the Contact Center Services for AMS installer and proceed through the installation wizard:  
**ContactCenterServicesForAMS.msi**
7. Download and apply all available AMS and CCSA QFE patches for the previous release.
  - a. Copy all available patch ZIP files to the **%MASHOME%\QFE** folder
  - b. Run the following command:  
**amspatch apply all**

8. If this is an AMS primary node, restore the backups taken in step 1 using Element Manager.
9. Restore the locale specific media files that were backed up in step 1 (if any).
10. If this is an AMS primary node and AMS using PLIC licensing, restore the license copied in step 2 by copying the backed up license file into EM->Licensing->General Settings "Add License Keys". Hit "Display Licenses", "Save" and then "Confirm"
11. Reboot the server

### Avaya Media Server on Linux

1. Ensure that the Avaya Media Server database backup scheduled prior to the upgrade to Avaya Aura® Contact Center 6.4 SP16 and the locale specific media files that were backed up are available (only for Voice and Multimedia Contact Server with Avaya Media Server deployments)
2. If this is a standalone AMS primary node using PLIC licensing, take a copy of the license from the Primary AMS Server (*AACC Upgrade and Patches 44400-410*) – this is not required if AACC is using WebLM licensing. Note: Licensing is not preserved in AMS backup
3. Uninstall *Contact Center Services for AMS 6.4 and Avaya Media Server 7.6*:  
**/opt/orte/UninstallCCSA**
4. Answer 'yes' to '*Also remove Avaya Media Server? y/n [n]:*'
5. Locate the **Install Software\AMS\Linux** folder on the Previous Release Bundle
6. On your Linux server, use the su command to change to the root user account:

```
su -
```

7. Create a temporary folder on Linux server by running command:  
`mkdir /tmp/AvayaMS`
8. Copy the following files from the Previous SP release bundle to the /tmp/AvayaMS folder:
  - `MediaServer_7.x.0.*.bin`
  - `ContactCenterServicesForAMS_6.*.bin`
9. Change to folder: /tmp/AvayaMS and run commands:  
`chmod +x ContactCenterServicesForAMS_6.*.bin`  
`chmod +x MediaServer_7.x.0.*.bin`
10. To Install Avaya Media Server and Contact Center Services for AMS run commands:  
`./MediaServer_7.x.0.*.bin`  
`./ContactCenterServicesForAMS_6.*.bin`
12. Download and apply all available AMS and CCSA QFE patches for the previous release.

- a. Copy all available patch ZIP files to the **%MASHOME%\QFE** folder
- b. Run the following command:  
**amspatch apply all**

13. If this is an AMS primary node, restore the backups taken in step 1 using Element Manager.

14. Restore the locale specific media files that were backed up in step 1 (if any).

15. If this is an AMS primary node and AMS using PLIC licensing, restore the license copied in step 2 by copying the backed up license file into EM->Licensing->General Settings "Add License Keys". Hit "Display Licenses", "Save" and then "Confirm"

16. Reboot the server

## Orchestration Designer

Scripts Modified Prior to downgrading AACC/ACCS to a previous service pack lineup cannot be edited

After the AACC/ACCS has been downgraded

### Procedure

- 1) Right click on the script you are unable to modify and select Export and save the script.
  - o If it's a GUI flow script it ends with .app
  - o Otherwise it ends with .s
- 2) Create a Local View
- 3) Use the Copy To Local View option to copy scripts to your Local View
- 4) Right click on Applications in the Local View and select Import. Import the script you have previously exported. Ensure the option is selected to Overwrite exiting applications without warning and select Finish.
- 5) Synchronize the script on CCMA by right clicking on server and selecting Synchronize in the Local View.
- 6) Upload the script to CCMA by right clicking the script and selecting Update In Contact Center, this will automatically reactivate the script.
- 7) After this you should be able to modify this script.
- 8) If you happen to get an error during the activation stage you will need to fix these errors first before going back to Step 5

## Upgrading from Previous Avaya Aura® Contact Center 6.x Release

The AACC 6.4 SP16 software can be installed on existing systems that were installed using previous versions of the DVD, but it is mandatory that all new installations (including the installation of additional components on an existing system) use the DVD version as outlined in the section DVD Version at the beginning of this document.

- Upgrades from AACC 6.0 that are installed with an 8.0.0.X DVD will be supported
- Upgrades from AACC 6.1 that are installed with an 8.1.0.X DVD will be supported
- Upgrades from AACC 6.2 that are installed with a 6.2.0.41 DVD will be supported

- Upgrades from AACC 6.3 that are installed with a 6.3.0.0-115 DVD will be supported

Before upgrading from a previous AACC 6.x Release, a mandatory Third Party software upgrade is required. Please refer to the section Third-Party Software to ensure all required Third Party software is correctly applied to your system

AACC 6.4 SP16 is applicable to all previous Avaya Aura® Contact Center 6.x Releases. After you have installed this Service Pack your system will be running Avaya Aura® Contact Center, Release 6.4 SP16 software.

**Important:** All previously installed Service Packs and patches for release 6.x must be removed prior to the installation of AACC 6.4 SP16.

**Important:** During an upgrade a certain amount of disc space is required for rebuilding database indexes. Under certain circumstances this can be several Gigabytes. The amount of disc space that is required is determined by the following factors:

- How many Agent Skillset Assignments you have.
- How many Days of Interval Data is kept.

The Space required can be calculated by:

- How many Agent Skillset Assignments you have.
  - The maximum number possible can be checked in CCMA, Configuration, select the CCMS Server, Historical Statistics, check the Measured Value in the Parameters table for both the Skillsets (S) and the Configured Agent IDs (A).
  - Multiply  $S * A = SA$
  - If you don't have every Agent assigned to every Skillset, then you can reduce this value accordingly.
- How many Days of Interval Data is kept.
  - This can be checked in CCMA, Configuration, select the CCMS Server, Historical Statistics, check the Value in the Duration table for the Interval (days) (D).
  - An Interval record is kept every 15 minutes, which means that there are 96 (I) per day.
  - Multiply  $D * I = DI$
- Multiply  $SA * DI = SADI$  to get the number of AgentSkillset Statistics that need to be re-indexed.
  - 1GB of space is required for each 6.5m AgentSkillset Statistics
  - Space required =  $SADI / 6,500,000$
- Example:
  - You have 50 Skillsets
  - You have 400 Agents
  - You keep 20 Days of Interval Data
  - $S * A = SA$ , so  $50 * 400 = 20,000$
  - $D * I = DI$  so  $20 * 96 = 1,920$
  - $SADI = 20,000 * 1920 = 38,400,000$  (AgentSkillset Statistics)
  - Space required =  $38,400,000 / 6,500,000 = 5.9GB$

## How to Backup/Restore ARConnector Configuration

All ARConnector configuration is stored in the folder D:\Avaya\Contact Center\Manager Server\ARConnector\config

Copy all the contents from/to this folder to Backup/Restore

## How to Upgrade from a Previous Avaya Aura® Contact Center 6.x Release

1. Perform a backup of all your Contact Center Databases prior to performing an upgrade

2. Remove all previously installed Service Packs and patches for Avaya Aura® Contact Center 6.x
3. Upgrade the Third Party Software. See section Third-Party Software for more information
4. Install the Common Components Service Pack first
5. Reboot the machine
6. Continue to install all other Service Packs and patches after the reboot has completed

**PLEASE REFER TO THE PATCHING WHITEPAPERS on [support.avaya.com](http://support.avaya.com) FOR ALTERNATIVE PATCHING PROCEDURES IN A MISSION CRITICAL HA ENVIRONMENT :**

**Avaya Aura® Contact Center R6.4 Mission Critical High Availability:  
Patching Procedure for Least Downtime**

**OR**

**Avaya Aura® Contact Center R6.4 Mission Critical High Availability:  
Patching Procedure for No Data Loss**

## **Upgrading to a new Service Pack or Restoring a Database backup results in recompile of all scripts**

When sites are upgrading to a new Service Pack they need to take into consideration that scripts will be recompiled during system startup after the installation this may result in TFE taking longer to report as fully started..

If a Database Restore is performed by the customer they need to take into consideration that scripts will be recompiled during the system startup after completing the restore this may result in TFE taking longer to report as fully started.

### **Known Issues:**

## **Issue Interval Statistics**

During the Upgrade procedures provided in the whitepapers the Standby Server is not always Shadowing the Active Server, this can result in the latest Interval Statistics being missing from any Backup taken on the Active Server.

The Interval Statistics files will remain on the Active Server until it has been Upgraded and returned to Active Mode, at which time, the Interval Statistics will be correctly written to the Database.

To ensure that all the Interval Statistics are correctly written to the Database a minimum of 15 minutes should elapse between shutting down the Contact Center on the Active Server and Starting the Standby Server in Active Mode.

While the Standby Server is running in Active Mode during the Upgrade it is recommended not to run any Historical Reports against Interval Statistics as the data may not be complete.

## Issue with the retention of Configuration of WS Open Interface

When upgrading your system from a previous Avaya Aura® Contact Center 6.x Service Packs please perform the steps outlined below to verify that all configuration information has been successfully retained.

### **Before Upgrade**

On **both** active and standby servers:

- On the server hosting AACC CCT, open the CCT Console  
(Start menu – AVAYA – Contact Center – Communication Control Toolkit – CCT Console)
- Select the CCT Web Services element under Server Configuration
- Take a screenshot of the console screen (see Figure 1 below for an example)
- Keep this for reference after upgrade has completed
- On the server hosting AACC CCMS, open the Server Configuration utility (Start menu – AVAYA – Manager Server)
- Click on the WS Open Interfaces (on left hand side)
- Take a screenshot of the console screen (see Figure 1 below for an example)
- Keep this for reference after upgrade has completed

### **After Upgrade**

On **both** active and standby servers

- Open the CCT Console Utility
- Select the CCT Web Services element under Server Configuration
- Ensure that the settings are the same as those in the screenshot for the CCT Console, saved before the upgrade
- Open the Server Configuration utility
- Click on the WS Open Interfaces (on left hand side)
- Ensure that the settings are the same as those in the screenshot for the Server Configuration, saved before the upgrade

**Note:** The UserPassword does not need to be modified. It is a system password and not stored in a config file

## Issue with SMMC starting after upgrading from previous AACC 6.x Release

When upgrading from a previous release of AACC, SMMC is not automatically started after the patch installation has completed. The user must launch the “SMMC SystemTray” utility from the Avaya shortcut directory located within the Start menu. The user must then right-click the “SMMC SystemTray” icon and select “Start SMMC”.

If the “SMMC SystemTray” icon stays blank (white) for an excessive period of time (more than 5 minutes), a reboot of the system may be required first to proceed with starting AACC.



Figure 1: Sample Screenshot of AACC CCT Console Utility

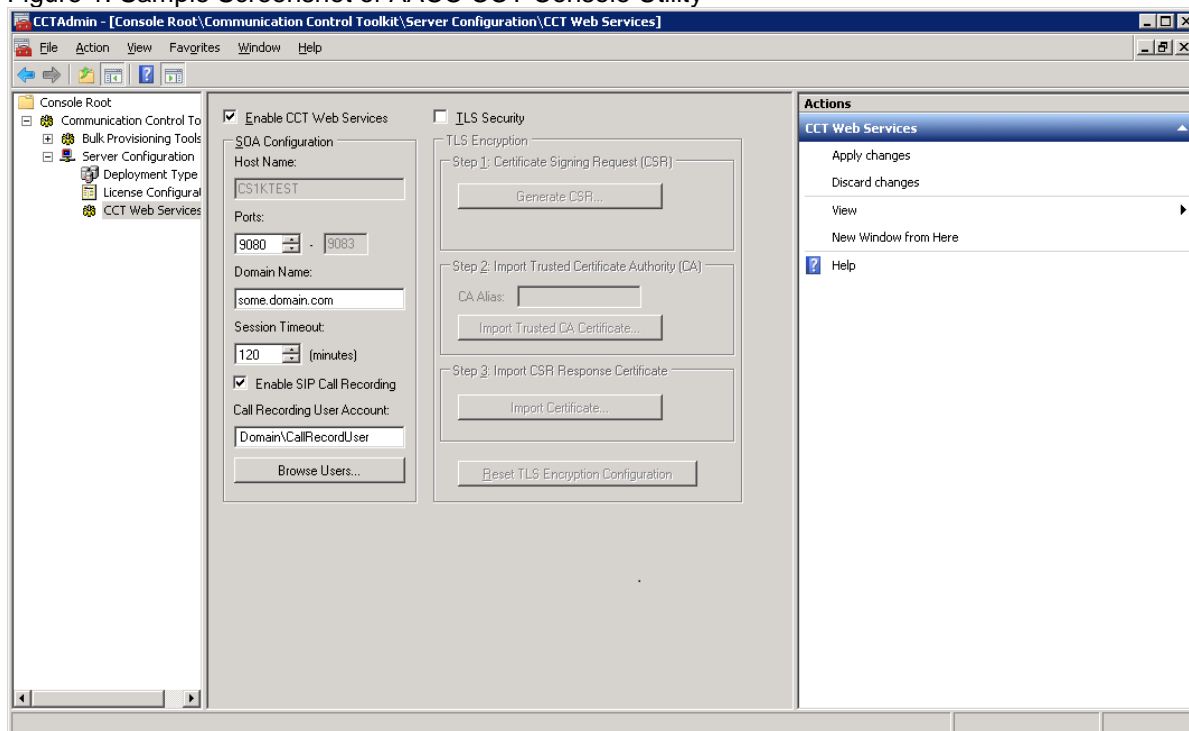
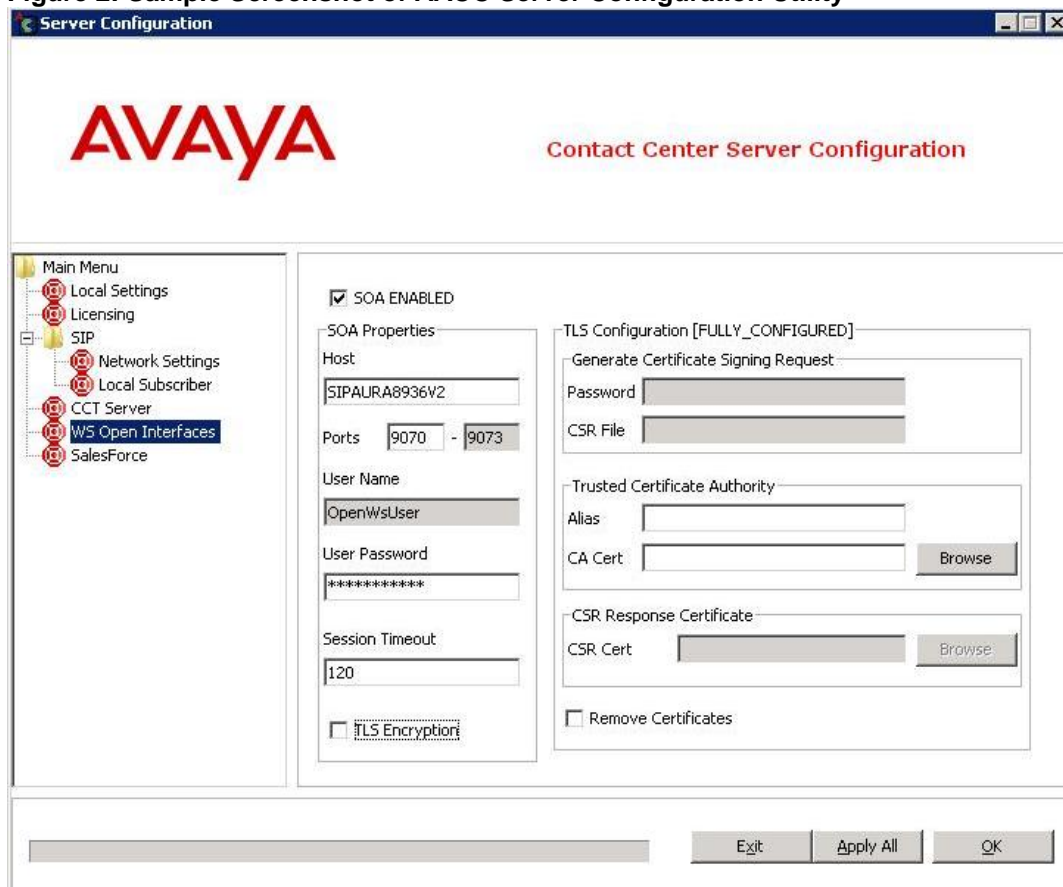


Figure 2: Sample Screenshot of AACC Server Configuration Utility



## HA SOA web services with TLS

AACC 6.3 SP10 introduced support for SOA HA on Mission Critical SIP HA systems. When configuring TLS for SOA OI on HA it needs to be enabled on **both** the active and the standby servers as seamless communication after switchover cannot occur if the transport (http – https and vice versa) changes.

When configuring TLS for SOA OI on HA the host name in the ServerConfig utility **must** be the **managed** server name and must match the managed server name on standby server.

When configuring TLS for SOA OI on HA **exactly** the same information, including case, needs to be specified for CSR generation. In the case where ServerConfig is used to generate the CSR the password is the only field to consider but in the case where CCT console is used to generate the CSR the stipulation applies to the location, company and password fields (note that ServerConfig (CCMS services) and CCT console (CCT services) both use the same security certificate information located in common components\cmf\security i.e. once the security certificate is successfully imported for one, the other will automatically be configured.)

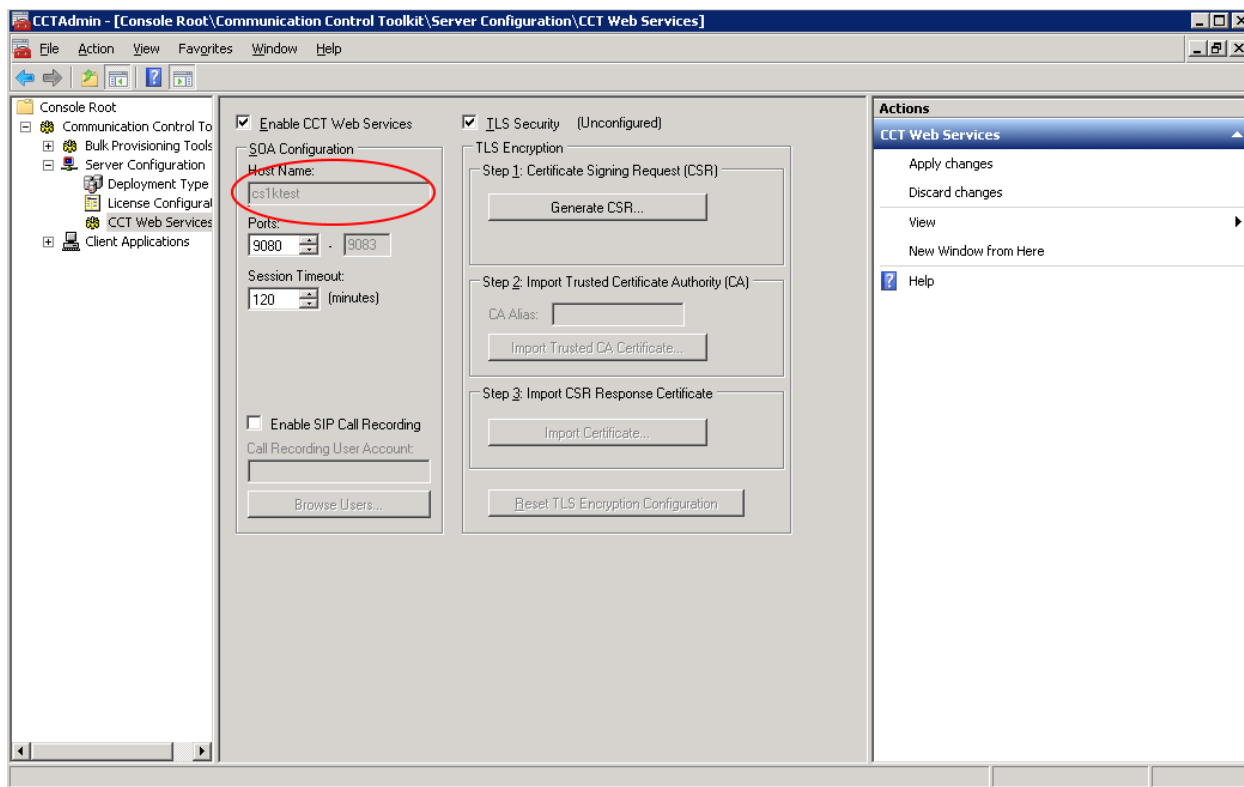
If a mistake is made in configuring TLS for SOA OI on a HA setup the likely error will be that **exactly** the same information was not inputted into the location, company or password fields on both the active and standby servers when the CSR was generated. The result of such a mistake would be a variation in the keystore and/or password files held in the cmf/security directory on each server.

The error would not cause a problem on the individual servers and would only become apparent on a subsequent SOA OI call after a switchover had occurred (due to the client reacting to a change in the server security certificate) and would manifest itself as a drop in the secure connection.

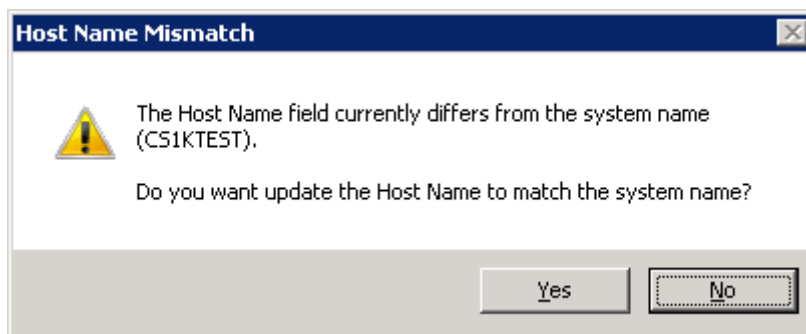
- The easiest way to ensure that the certificate keystore and password files are identical on both servers while eliminating the possibility of the same mistake being made again is to manually copy the keystore and password files from the active to the standby (or vice versa).
- The 2 files that need to be copied across (and hence overwritten) are:
  - D:\Avaya\Contact Center\Common Components\CMF\Security\server.keystore
  - D:\Avaya\Contact Center\Common Components\CMF\Security\lect\_kstore

On HA systems, to configure the managed host name when configuring TLS please follow this procedure:

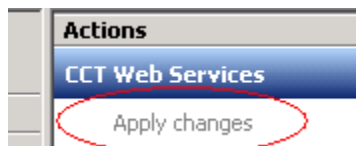
1. Use the Server Configuration Utility web services section to enable SOA and update the host field to the managed host name and click OK. *See figure 2 above.* Also, please note that you cannot change the host name on the CCT console



2. Open the CCT console at the web services section. If you are prompted with the following prompt, select No.



3. Proceed to configure TLS using the CCT console. Select Apply all on the right hand side and close the CCT console.



- Return to the Server Configuration Utility and if using the CCMS web services, enable TLS using the appropriate check box. Please note that the certificates are automatically configured once you do this on either screen.

- Reboot the server and the SOA services will be up after the reboot. This can be checked by opening the OI splash page at <http://localhost:9090>. The services URLs listed should be updated from http to https
- Repeat the above steps on the standby server, or copy the certificate files (server.keystore & ect\_kstore) from the active to the same folder on the standby and ensure the web service settings on the CCT console and server config are matching the active. Restart the Standby for these changes to take effect.

## Upgrading from Previous Avaya Aura® Contact Center Service Pack in a Mission Critical HA Environment

Upgrading to AACC 6.4 SP16 from a previous AACC release in a Mission Critical HA environment requires Contact Center downtime in a planned maintenance window to bring the active and standby servers to a common software release.

**PLEASE REFER TO THE PATCHING WHITEPAPERS on [support.avaya.com](https://support.avaya.com) FOR ALTERNATIVE PATCHING PROCEDURES IN A MISSION CRITICAL HA ENVIRONMENT :**

**Avaya Aura® Contact Center R6.4 Mission Critical High Availability:  
Patching Procedure for Least Downtime**

**OR**

**Avaya Aura® Contact Center R6.4 Mission Critical High Availability:  
Patching Procedure for No Data Loss**

### Known Issues:

#### Interval Statistics

During the Upgrade procedures provided in the whitepapers the Standby Server is not always Shadowing the Active Server, this can result in the latest Interval Statistics being missing from any Backup taken on the Active Server.

The Interval Statistics files will remain on the Active Server until it has been Upgraded and returned to Active Mode, at which time, the Interval Statistics will be correctly written to the Database.

To ensure that all the Interval Statistics are correctly written to the Database a minimum of 15 minutes should elapse between shutting down the Contact Center on the Active Server and Starting the Standby Server in Active Mode.

While the Standby Server is running in Active Mode during the Upgrade it is recommended not to run any Historical Reports against Interval Statistics as the data may not be complete.

## Upgrading from Service Creation Environment (SCE) to Orchestration Designer (OD)

If your upgrade path involves moving from SCE to OD, export all your existing SCE applications using the SCE Export functionality. After the upgrade, import the applications using Import functionality in OD.

## SOA Preservation – Downgrade and Upgrade of Avaya Aura® Contact Center Common Components

Scope: Only pertains to components Communication Control Toolkit (CCT), Contact Center Manager Server (CCMS) and Contact Center Common Components (CC).

In AACC 6.2, Soa configuration data was stored in separate locations for applications CCT and CCMS. An upgrade to 6.4 combines this data into a singular shared location within the Common Components application.

- An upgrade from 6.2 to 6.4 preserves the current 6.2 configuration data without loss of existing settings.
- An upgrade from 6.3 to 6.4 preserves the current 6.3 configuration data without loss of existing settings.
- A downgrade from 6.4 to 6.3 preserves the current 6.4 configuration data without loss of existing settings.
- A downgrade from a **fresh** (clean machine deployment) 6.4 installation to 6.2 results in configuration data loss. The user must recreate their configuration data
- A downgrade from 6.4 to 6.2, on a machine that previously contained a SP5, SP6 or SP7 installation, results in historical 6.2 data being retrieved and used for the current 6.2 installation.
- A downgrade of 6.4 to 6.2, and subsequent re-upgrade to 6.4, results in previous 6.4 configuration data being retrieved and used for the current 6.4 installation.

### Upgrade from 6.2 to 6.4

The 6.4 installation will retrieve previous 6.2 settings used for the CCT and CCMS components, and carry these forward for use in 6.4.

### Downgrade from 6.4, on a machine that had a previous 6.2 installation:

If the machine previously contained an SP5, SP6 or SP7 installation, configuration data from these installations should be present in an archived file. This data will be retrieved and retained as the most suitable configuration data for the current 6.2 deployment.

### Upgrade to 6.4 after prior 6.4 downgrade to 6.2:

Upon removal of 6.4, the current configuration data will be archived for use in an upgrade scenario. As above, downgrade to 6.2 auto-reverts back to previous 6.2 data if it exists, otherwise the user must recreate this manually.

Subsequent re-upgrade to 6.4 will retrieve and retain the archived 6.4 data.

**Note:** In all of the above cases, if further reconfiguration of the SOA data is required, the following tools can be run -

Communication Control Toolkit : CCT Console

Contact Center Manager Server : Service Configuration

## Invalid Agent Audit

AACC 6.4 introduces an automatic database audit feature to identify agents that have an invalid configuration. The audit runs twice a day at 11 AM and 11 PM. An informational event is generated every time the audit completes. If invalid agents exist in the database, a Windows error event is generated.

It is possible that invalid agents exist in the database before the upgrade and will be discovered by the audit after the upgrade. If this occurs, the customer should be advised that a non-critical maintenance window should be organized with Avaya Support to remove the invalid agents.

## AACC-IQ Modified Reporting of Queue Out Of Service

In AACC, when the last agent logs out of a skillset (with queued contacts) the skillset is considered out of service. All contacts queued to the skillset are removed from the skillset. When an agent logs back into the skillset, the skillset is considered in service again. All contacts that were previously queued to the skillset are re-queued to the skillset.

An agent also contains a queue. This allows contacts to be queued directly to the agent. The same behavior described for a skillset going out of service applies to an agent going out of service.

In AACC, when the queue goes out of service no further information is published for the out of service queue. Since the skillset is out of service no skillset reporting is applicable. Out of service skillsets do not appear in the AACC Real-Time Reporting. The contacts that were previously queued to the skillset are still visible in the application level view. The contacts are reported as waiting in the workflow that is managing them in anticipation of the queue coming back into service.

In Avaya IQ, queues are skillsets so the IQ reporting of queues accurately reflects the addition (enqueue) and removal (dequeue) of contacts to the skillset/agent queues. However, Avaya IQ does not have an applications type view of contacts. Therefore, when a skillset goes out of service the contacts that were previously queued disappear from Avaya IQ view.

For some customers the desired behavior (for a skillset/agent going out of service) is that the contacts are allowed to **appear** to be still queued to the skillset/agent when the skillset/agent is out of service. The feature development delivers this behavior.

To enable this feature use the following steps

1. Go to D:\Avaya\Contact Center\Manager Server\ARConnector\config
2. Open seilink.properties in a text editor
3. Modify the last line, "EnhancedQueueOutOfServiceReporting = FALSE" to "TRUE"
  - a. EnhancedQueueOutOfServiceReporting = TRUE
4. Restart the CCMS for the changes to be applied

The feature is disabled by default. If a customer enables the feature, the feature will be disabled if the customer applies any subsequent patch that contains ARC changes. The readme for subsequent AACC patches with ARC content will contain a warning that the feature will need to be re-enabled again.

## Remote Access

The AACC product will be supported using the Remote Desktop Connection (RDC) Microsoft Windows utility.

This utility will allow the Avaya support or design resource to remotely access the customer server from a remote PC and be able to administer the server as if logged in directly to that server.

RDC uses port 3389 so this port should be enabled on all co-resident or standalone servers in the AACC solution installed.

For Linux-based Avaya Media Server installations, Secure Shell (SSH) port 22 should be enabled to allow remote access to the server.



## Localization

Avaya Aura Contact Center 6.4 SP16 UI, Avaya Agent Desktop (AAD), Outbound Campaign Management Tool (OCMT) and Contact Center Manager Administration (CCMA) online Help is localized into French, German, LA Spanish, Simplified Chinese, Brazilian Portuguese, Russian, Japanese, Traditional Chinese, Korean and Italian.

The AACC 6.4 SP16 supports the same level of localization as was previously available in AACC 6.4 SP13 including localization of AACC 6.4 FP2 which is being delivered for the first time as part of this SP.

## Overview of AACC 6.4 I18N and L10N Products & Components

Components that are used by Contact Center agents or by Contact Center supervisors performing non-specialized functions are localized.

Interfaces to support administration or specialized functions (for example, creating routing applications) are not localized.

The following table lists all AACC 6.4 products and components in relation to Internationalization and Localization:

AACC 6.4 Products	Component	International OS Support? Yes/No	Localized? Yes/No	Comments
CCMS	All components	Yes	No	
CCT	All 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	See below for more details.
CCMA	Configuration	Yes	Yes	
CCMA	Emergency Help	Yes	Yes	
CCMA	Outbound	Yes	Yes	
CCMA	Crystal Report Templates	Yes	Yes	
CCMA	NCC Crystal Report Templates	Yes	No	
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.

AACC 6.4 Products	Component	International OS Support? Yes/No	Localized? Yes/No	Comments
CCMA	Configuration Tool	Yes	No	Only administrators use the Configuration Tool.
CCMA	Element Manager	Yes	No	Login page is localized.
CCMM	Server Components	Yes	No	
CCMM	AAD Client	Yes	Yes	
CCMM	AAD online Help	Yes	Yes	
CCMM	OCMT Client	Yes	Yes	
CCMM	OCMT online Help	Yes	Yes	

## Software

### Supported operating systems

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

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

Supported Language OS	Languages									
	ZH-CN	FR	ES	DE	PT-BR	JA	ZH-TW	RU	KO	IT
Windows Server 2008 R2 Standard edition	Y	Y	Y	Y	Y	Y	Y **	Y	Y	Y
Windows Server 2008 R2 Enterprise edition	Y	Y	Y	Y	Y	Y	Y **	Y	Y	Y
Windows Server 2008 R2 Standard edition + SP1	Y	Y	Y	Y	Y	Y	Y **	Y	Y	Y
Windows Server 2008 R2 Enterprise edition + SP1	Y	Y	Y	Y	Y	Y	Y **	Y	Y	Y

**\*\* Windows 2008 R2 for Chinese Taiwan must be used.**

## Localized Components (CCMA and CCMM)

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

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

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

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

## Language specific support and configuration

**NB:** The local language operating system for example French should be a full language operating system (installed from the language DVD/CD) rather than as an OS language patch on top of an English operating system install, for example English Windows 2008 with Microsoft French language patch installed.

## Support of CCMA Client

Language	CCMA Client
French	Supported on Internet Explorer 8, 9, 10 and 11, Browser's Language Preference set to fr-FR. CCMA will be displayed in French if the French language patch is installed on the server, otherwise it will appear in English.
German	Supported on Internet Explorer 8, 9, 10 and 11, Browser's Language Preference set to de-DE. CCMA will be displayed in German if the German language patch is installed on the server, otherwise it will appear in English.
LA Spanish	Supported on Internet Explorer 8, 9, 10 and 11, Browser's Language Preference set to es-CO. CCMA will be displayed in Spanish if the Spanish language patch is installed on the server, otherwise it will appear in English.

Simplified Chinese	Supported on Internet Explorer 8, 9, 10 and 11, Browser's Language Preference set to zh-CN. CCMA will be displayed in Simplified Chinese if the Simplified Chinese language patch is installed on the server, otherwise it will appear in English.
Brazilian Portuguese	Supported on Internet Explorer 8, 9, 10 and 11, Browser's Language Preference set to pt-BR. CCMA will be displayed in Brazilian Portuguese if the Brazilian Portuguese language patch is installed on the server, otherwise it will appear in English.
Russian	Supported on Internet Explorer 8, 9, 10 and 11, Browser's Language Preference set to ru-RU. CCMA will be displayed in Russian if the Russian language patch is installed on the server, otherwise it will appear in English.
Italian	Supported on Internet Explorer 8, 9, 10 and 11, Browser's Language Preference set to it-IT. CCMA will be displayed in Italian if the Italian language patch is installed on the server, otherwise it will appear in English.
Japanese	Supported on Internet Explorer 8, 9, 10 and 11, Browser's Language Preference set to ja-JP. CCMA will be displayed in Japanese if the Japanese language patch is installed on the server, otherwise it will appear in English.
Traditional Chinese	Supported on Internet Explorer 8, 9, 10 and 11, Browser's Language Preference set to zh-tw. CCMA will be displayed in Traditional Chinese if the Traditional Chinese language patch is installed on the server, otherwise it will appear in English.
Korean	Supported on Internet Explorer 8, 9, 10 and 11, Browser's Language Preference set to ko-KR. CCMA will be displayed in Korean if the Korean language patch is installed on the server, otherwise it will appear in English.

## Support of CCMM Client

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

## Support of CCMM Server and Configuration Notes

### CCMM server / Regional Options Configuration

Language	CCMM Server
French	CCMM Server installed on French 2008. Regional option default (French)
German	CCMM Server installed on German 2008. Regional option default (German)
LA Spanish	CCMM Server installed on Spanish 2008. Regional option default (Spanish)
Simplified Chinese	CCMM Server installed on Simplified Chinese 2008. Regional option default (Simplified Chinese)
Brazilian Portuguese	CCMM Server installed on Brazilian Portuguese 2008. Regional option default (Brazilian Portuguese)
Russian	CCMM Server installed on Russian 2008. Regional option default (Russian)
Italian	CCMM Server installed on Italian 2008. Regional option default (Italian)
Japanese	CCMM Server installed on Japanese 2008. Regional option default (Japanese)
Traditional Chinese	CCMM Server installed on Traditional Chinese 2008. Regional option default (Traditional Chinese)
Korean	CCMM Server installed on Korean 2008. Regional option default (Korean)

*Enable email analyzer*

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

See French as an example:

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

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

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

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

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

NB: The following wildcard limitation applies to Asian languages only

Again, using Simplified Chinese is used as an example, but all Asian languages using double byte will apply;

To route a single byte keyword, you must save the keyword as DOUBLE byte on the server.

There is a limitation when enabling the email analyzer to Japanese (CJKAnalyzer).

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 コブタ to a skillset called EM\_Test do the following.

- 1) Create a DOUBLE byte keyword
  - In the Multimedia Administrator, click the plus sign (+) next to Contact Center Multimedia, click the plus sign next to E-mail Administration, and then double-click Keyword Groups.
  - The Keyword Groups window appears.

- To create a new keyword group, click New.
- In the Name box, type a unique name for the keyword group (maximum 64 characters. This NAME must be in English). E.g. “DoubleByteCoputa”
- In the Keyword box, type the word (in DOUBLE byte) you will be searching for. E.g. “コプタ” Click Add.  
The keyword is added to the list, and the keyword group is created. Click Save.

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

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

## 3) Send in an email with the SINGLE byte word コプタ.

The single byte keyword now routes successfully to the EM\_Test skillset.

\*\* Note this also applies when using wildcards in keywords.

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

NB: The following wildcard limitation applies to Asian languages only

Wildcard ‘?’ or ‘\*’ can only be used at the end of a keyword in a Japanese environment.

When using the wildcard ‘\*’ or ‘?’, it can only be used at the end of a string

for example:

たば\* = ok

た\*た = no

Note:

To route the wildcard keyword successfully, the ‘\*’ can be entered in either full-width or half width.

The ‘?’ can be entered in full-width only

## Email Domain Names (Asian)

NB: The following applies to Asian languages only

Using Japanese as an example:

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

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

## CCMM friendly display names

Display names are referred to in the CCMM Server online Help in section **Creating or changing a recipient**, section 99. In the Display Name box, type the friendly name you want to appear in the e-mail From address (for example, Customer Support). You must enter a display name for each mailbox. In response to the case reported above, the Internet Standard IETF RFC 1036, Section 2.1, permits only ASCII characters in the display name.

Some email vendors, such as MS Outlook, included, invalidly permit double-byte display names which are contrary to the Internet Standard. CCMM has always strictly adhered to the Internet Standard and handles only ASCII characters.

## Logging on to Contact Center Manager Administration

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

### Enabling languages

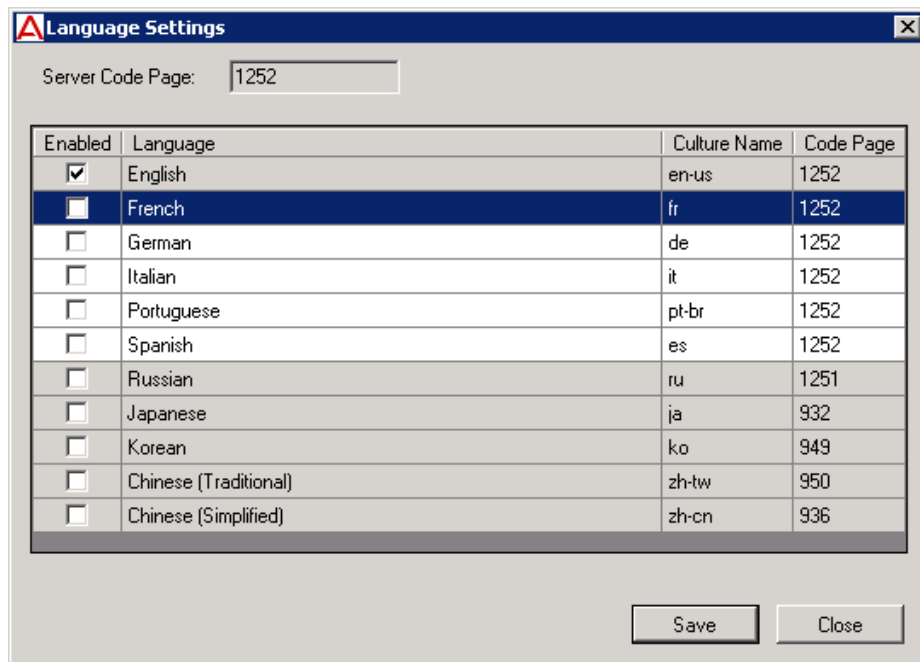
The customer can no longer decide if a language should be installed, a new CCMA Configuration utility was added to enable a language.

The Language Settings utility is accessed from the CCMA Configuration screen.



Once the Service Pack including languages is installed, all localized languages will appear in the CCMA Language Settings application. Only languages matching the current server code page can be enabled, others are disabled. English is always enabled and cannot be disabled.

The utility supports multiple row selection and space bar toggling of enabled checkbox. To quickly enable or disable all supported languages, press [Ctrl] + A, then press space bar.



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

## Procedure steps

Note:

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

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

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

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

1. Launch Internet Explorer.
2. In Internet Explorer, click Tools → Internet Options.  
**Result:** The Internet Options window appears.
3. Click **Languages**.  
**Result:** The Language Preferences window appears.  
Verify that the language you want to use appears in the Language box. E.g. French [France] [fr],
4. If the language does not appear in the box, then you must add it as follows:
  - a. Click **Add**.  
**Result:** The Add Language window appears.
  - b. From the list of languages, click the appropriate language, and then click **OK**.  
**Result:** The language now appears in the Language Preferences window.
  - c. Proceed with the next step to move the language to the top of the box.
5. If the language you want to use appears in the box, then you must move it to the top of the list as follows:
  - a. In the Language box, click the appropriate language.
  - b. Click **Move Up** until the language appears at the top of the box.
  - c. Click **OK** to close the Language Preferences window.
6. Click **OK** to close the Internet Options window.
7. In the Address box, type the URL of the Contact Center Manager Administration server. The default URL is `http://<server name>:81`, where <server name> is the computer name of the Contact Center Manager Administration server.



**Attention:** Do not type the IP address in the Address box. Using the IP address results in problems with Scripting, Historical Reporting, Configuration, Contact Center Management, and Access and Partition Management.

8. In the **User ID** box, type your user ID.
9. In the **Password** box, type your password.
10. Click **Login**.

## Start Localized AAD Client

### Pre-installation steps

Information on how to start AAD (Only when a language patch installed)

NOTE:

To start AAD in a local language (French for example);

- From a French client PC, start AAD.

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

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

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

### Installing the Agent Desktop Client

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

#### Prerequisites

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

#### Procedure steps

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

### Starting the Agent Desktop Client

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

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

#### Procedure steps

1. In Windows Explorer or Internet Explorer, enter the HTTP address (URL). The correct URL format is **http://<Contact Center Multimedia servername>/agentdesktop/LANGUAGE CODE\***  
Using French as an example, the URL is <http://ccmmservername/agentdesktop/fr>  
If using English, URL is **http://<Contact Center Multimedia servername>/agentdesktop**.
2. Click Launch AAD on the web page.  
or  
Click Windows Start, All Programs, Avaya, Avaya Aura Agent Desktop 6.0.

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

## Start OCMT Client

### Pre-installation steps

Information on how to start OCMT (Only when a language patch installed)

NOTE:

To launch CCMM in a local language (French for example);

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

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

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

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

## Logging on to the Outbound Campaign Management Tool

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

### Prerequisites

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

### Procedure steps

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

## Detecting latest Language files

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

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

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

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

1. Close AAD and OCMT.
2. Click Add/Remove Programs.
3. Remove Avaya/Avaya Agent Desktop 6.0.
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.

## Crystal Report templates

### Localized templates

The following table outlines which Historical reports are provided with AACC and identifies those that are localized in French, German, Italian, LA Spanish, Brazilian Portuguese, Korean, Japanese, Russian, Simplified and Traditional Chinese. Additional reports are localized in some regions to maintain consistency with previous localized releases.

CCMA Report Type	Report Template Name	Localized?
Contact Center	Contact Summary	Y
	Originator By Disposition	Y
	Activity Code By Address	Y
	Agent By Address	Y
	Contact Duration	Y
Multimedia	Contacts Closed by Reason Code	Y
	Contacts Closed by Skillset	Y
	Contacts Details	Y
	Contacts Outstanding Detail	Y
	Contacts Outstanding Summary	Y
	Contacts Received by Skillset	Y
Outbound	Campaign Call Details	Y
	Campaign Performance	Y
	Campaign Script Results Details	Y
	Campaign Summary	Y
	Script Summary	Y
Agent Performance	Activity code by agent	Y
	Agent average calls per hour	Y
	Agent average calls per hour – bottom five	Y
	Agent average calls per hour – top five	Y
	Agent by Activity Code	Y
	Agent by Application Performance	Y
	Agent by Skillset Performance	Y
	Agent DN Performance	Y
	Agent DN Performance Calls Answered, Bottom 5	N
	Agent DN Performance Calls Answered, Top 5	N
	Agent Efficiency	Y
	Agent Efficiency By Contact Type	Y
	Agent Efficiency By Skillset	Y
	Agent Login/Logout	Y
	Agent NACD Activity	N
	Agent Performance	Y
	Agent Performance by Supervisor	Y
	Agent Performance Calls Answered, Bottom 5	N
	Agent Performance Calls Answered, Top 5	N
	Agent Short Calls	Y
	Agent Transferred/Conferenced Activity	Y
	Estimated Revenue by Agent	N
	Not Ready Reason Codes by Agent	Y

CCMA Report Type	Report Template Name	Localized?
	Skillset by Agent Performance	Y
Call-by-Call	Call by Call Statistics	Y
Configuration	Config – Activity Code Properties	Y
	Config – Agent By Supervisor Properties	Y
	Config – Agent Properties	Y
	Config – Agent Skillset Assignment	Y
	Config – Agent Skillset Properties	Y
	Config – Agent Supervisor Assignment	Y
	Config – Application Properties	Y
	Config – Application Script Properties	Y
	Config – Application Template Properties	Y
	Config – CDN (Route Point) Properties	Y
	Config – Database View Definitions	Y
	Config – DNIS Properties	Y
	Config – Formula Properties	Y
	Config – Historical and Real Time Statistics Properties	Y
	Config – IVR Queue and Port Properties	Y
	Config – Logged In Agent	Y
	Config – Multimedia	Y
	Config – Route Properties	Y
	Config – Script Variable By Script	Y
	Config – Script Variable Properties	Y
	Config – Skillset Properties	Y
	Config – Supervisor Properties	Y
	Config – Telephone Display Properties	Y
	Config – User Access Privilege	Y
	Config – Real Time Template Properties	N
Networking	Config – Network Site and Application Properties	n/a
	Config – Network Skillset Routing Properties	n/a
	Crosstab – Network Incoming Calls	n/a
	Crosstab – Network Outgoing Calls	n/a
	Network Application Performance	n/a
	Network DNIS Statistics	n/a
	Network Incoming Calls	n/a
	Network Outgoing Calls	n/a
	Network Route Performance	n/a
	Network Skillset Performance	n/a
	Network Skillset Timeline	Y
	Network Skillset Timeline By Contact Type	Y
Contact Summary	Activity Code By Address	Y
	Agent By Address	Y
	Contact Duration	Y
	Contact Duration By Agent	Y
	Contact Summary	Y
	Contacts By Agent	Y
	Originator By Disposition	Y
Others	Activity Code By Application	N

CCMA Report Type	Report Template Name	Localized?
	Application by Activity Code	Y
	Application By Skillset	N
	Application Call Treatment	Y
	Application Delay Before Abandon	Y
	Application Delay Before Answer	Y
	Application Performance	Y
	CDN (Route Point) Statistics	Y
	Crosstab – Application Performance	N
	Crosstab – CDN (Route Point) Statistics	N
	Crosstab – DNIS Statistics	N
	Crosstab – Route Performance	N
	Crosstab – Skillset Performance	N
	Crosstab – Trunk Performance	N
	DNIS Statistics	N
	Music/RAN Route Statistics	N
	Route Performance	N
	Skillset By Application	N
	Skillset Performance	Y
	Skillset Timeline	Y
	Skillset Timeline By Contact Type	Y
	Trunk Performance	N
Predictive Outbound	Agent Productivity	n/a
	Agent Time Summary	n/a
	Predictive Campaign Summary	n/a
	Dialling Statistics	n/a
	Diligence Report By Phone Number	n/a
	Diligence Report by Portfolio & Retrieval Key	n/a
	Management Summary	n/a
Administration	Users	Y
	Report Groups	Y
	User Defined Partitions	Y
	Access Classes	Y

## Known issues

Known issues are listed in this section.

If you encounter a feature issue, review this document and report the issue if it is not listed here.

### For CCMA

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

---

**wi00934076** [All languages] – AACC6.2- CCMA – HR – Hardcode on Selection Criteria

Setup And Actions Performed To Cause The Problem:

1. Login CCMA > Open HR component
2. Choose a CCMS server > Public Report Templates
3. Click on these reports:
  - a. Contact Summary and Multimedia folders: any report
  - b. Agent Performance folder: Agent Efficiency By Contact Type
  - c. Others folder: Skillset Timeline and Timeline By Contact Type
  - d. Networking folder: Network Skillset Timeline and Network Skillset Timeline By Contact Type
4. Expand Selection Criteria link then verify the information at dropdown list

This is design intent

## DVD Controller

## Pre Installation Instructions

### INSTALLATION OF PRODUCT UPDATES

It is mandatory that that you update your system with the latest product updates when setting up your system.

Product Updates should be downloaded to the local system prior to the installation of your AACC software. During the installation you will be prompted to provide the folder where these updates are located.

#### INSTALLING ON A TRADITIONAL CHINESE OPERATING SYSTEM:

If you are performing an installation of Avaya Aura® Contact Center 6.4 SP16 on a Traditional Chinese operating system, please contact your Avaya Account Manager/representative prior to continuing with your installation.

## Installation Instructions

In the 'interview stage' for the CCMM Primary Server tab, a new text box has been introduced to query the UC Server address. For CM, enter the CLAN IP address.

## Post Installation Instructions

After a fresh deployment of Avaya Aura® Contact Center 6.3 Service Pack 11, a Third Party software upgrade is mandatory. Please refer to the section Third-Party Software for more information.

## Configuration Issues



## Common Components

### Pre Installation Instructions

None

### Installation Instructions

None.

### Post Installation Instructions

None.

### Post Uninstall (Downgrade to 6.2) Instructions

---

<b>wi01055139</b>	<b>6.2 SP7- Sysop- Parameter to disabled IPV6 is removed out of registry after downgrade from 6.3 to SP7</b>
-------------------	--

---

I downgraded from 6.3 Service Pack 8 to 6.2 (E.g. Service Pack 7) then Ipv6 must be disabled manually.

This has been fixed in Service Pack 9.

Workaround:

Disabling Internet Protocol version 6

About this task

Disable internet protocol version 6 (Ipv6) to ensure correct operation of the contact center software.

Procedure

1. Search the Microsoft support Web site for instructions to locate the instructions to disable Ipv6 in the Windows Server 2008 registry.
  2. Follow the Microsoft instructions to disable all Ipv6 components.
- Downloading the most recent patches to the server
3. Reboot the server, if required.

## Configuration Issues

### PVI Checker

Please refer to the Fundamentals & Planning Guide (44400-211), for all recommendations regarding the minimum machine specification required. The PVI checker will block installation of AACC 6.4 on any machine that does not meet the minimum specifications.

## Contact Center Update Manager

To ensure you are using the latest version of the Contact Center Update Manager you must follow the upgrade procedure outlined in Downgrade (Avaya Aura® Contact Center 6.4 SP16 to a previous release) Avaya Aura Contact Center

This procedure should be executed in the event that the contact center must be downgraded from Avaya Aura® Contact Center 6.4 SP16 to a previous release.

- Ensure that the Contact Center database backup scheduled prior to the upgrade to Avaya Aura® Contact Center 6.4 SP16 is available
- Downgrade 3rd Party software using the Third Party Software Downgrade Utility

Downgrade the system from Avaya Aura® Contact Center 6.4 SP16 to a previous release via Patch Manager. The 2 step downgrade process is as follows:-

1. Remove all Service Packs for Avaya Aura® Contact Center 6.4 SP16
2. Install all Service Packs for the previous Avaya Aura® Contact Center release

Important: at step 3, the Third Party Software Downgrade Utility may provide instructions regarding the removal of existing Service Packs and installation of others. The sequence indicated by the Downgrade utility **should** be preferred over step 4.

Recover the system and ensure that all services have started via the System Control & Monitoring Utility (SCMU)

Restore the database(s) previously backed up prior to upgrading to Avaya Aura® Contact Center 6.4 SP16

Avaya Media Server

This procedure should be executed on the Avaya Media Server in the event that the contact center must be downgraded from Avaya Aura® Contact Center 6.4 SP16 to a previous release.

Avaya Media Server on Windows

**Ensure that the** Avaya Media Server database backup scheduled prior to the upgrade to Avaya Aura® Contact Center 6.4 SP16 and the locale specific media files that were backed up are available (only for Voice and Multimedia Contact Server with Avaya Media Server deployments)

If this is a standalone AMS primary node using PLIC licensing, take a copy of the license from the Primary AMS Server (AACC Upgrade and Patches 44400-410) – this is not required if AACC is using WebLM licensing. Note: Licensing is not preserved in AMS backup

**Uninstall Contact Center Services for AMS** via the Windows Control Panel

- 1.
2. Uninstall Avaya Media Server 7.6 via the Windows Control Panel. When prompted to preserve or remove data, select the 'Remove' option.
- 3.
4. Locate the Install Software\AMS\Windows folder on the AACC Previous Release Bundle, launch the Avaya Media Server installer and proceed through the installation wizard: **InstallerMAS.exe**
5. Launch the Contact Center Services for AMS installer and proceed through the installation wizard: **ContactCenterServicesForAMS.msi**
- 6.
7. Download and apply all available AMS *and CCSA QFE patches* for the previous release.
- 8.
9. Copy all available patch ZIP files to the %MASHOME%\QFE folder
10. Run the following command:  
**amspatch apply all**
11. If this is an AMS primary node, restore the backups taken in step 1 using Element Manager.

12. Restore the locale specific media files that were backed up in step 1 (if any).
- 13.
- 14.
15. If this is an AMS primary node and AMS using PLIC licensing, restore the license copied in step 2 by copying the backed up license file into EM->Licensing->General Settings "Add License Keys". Hit "Display Licenses", "Save" and then "Confirm"
- 16.
17. Reboot the **server**
- 18.
19. **Avaya Media Server on Linux**
20. Ensure that the Avaya Media Server database backup scheduled prior to the upgrade to Avaya Aura® Contact **Center** 6.4 SP16 and the locale specific media files that were backed up are available (only for Voice and Multimedia Contact Server with Avaya Media Server deployments)
  - a. If this is a standalone AMS primary node using PLIC licensing, take a copy of the license from the Primary AMS Server (*AACC Upgrade and Patches 44400-410*) – this is not required if AACC is using WebLM licensing. Note: Licensing is not preserved in AMS backup
  - b.
  - c. Uninstall Contact Center Services for AMS 6.4 and Avaya Media Server 7.6:  
/opt/ **orte/UninstallCCSA**
  - d.
  - e. Answer 'yes' to 'Also remove Avaya Media Server? y/n [n]:'
  - f.
  - g.
  - h. Locate the Install Software\AMS\Linux folder on the Previous Release Bundle

On your Linux server, use the su command to change to the root user account:

su –

21. Create a temporary folder on Linux server by running command:
22. mkdir /tmp/AvayaMS
- 23.
24. Copy the following files from the Previous SP release bundle to the /tmp/AvayaMS folder:  
MediaServer\_7.x.0.\*.bin  
ContactCenterServicesForAMS\_6.\*.bin
- 25.
26. Change to folder: /tmp/AvayaMS and run commands:
27. chmod +x ContactCenterServicesForAMS\_6.\*.bin
28. chmod +x MediaServer\_7.x.0.\*.bin
- 29.
30. To Install Avaya Media Server and Contact Center Services for AMS run commands:
31. ./MediaServer\_7.x.0.\*.bin
32. ./ContactCenterServicesForAMS\_6.\*.bin
- 33.
34. Download and apply all available AMS and CCSA QFE patches for the previous release.  
Copy all available patch ZIP files to the %MASHOME%\QFE folder  
Run the following command:  
**amspatch apply all**
- 35.
36. If this is an AMS primary node, restore the backups taken in step 1 using Element Manager.

**Restore the locale specific media** files that were backed up in step 1 (if any).

- 1.
- 2.

3. If this is an AMS primary node and AMS using PLIC licensing, restore the license copied in step 2 by copying the backed up license file into EM->Licensing->General Settings "Add License Keys". Hit "Display Licenses", "Save" and then "Confirm"
  - 4.
  5. Reboot the server
  - 6.
  - 7.
  - 8.
  9. Orchestration Designer
  10. Scripts Modified Prior to downgrading AACC/ACCS to a previous service pack lineup cannot be edited
  - 11.
  12. *After the AACC/ACCS has been downgraded*
  - 13.
  14. Procedure
  15. Right click on the script you are unable to modify and select Export and save the script.  
If it's a GUI flow script it ends with .app
  16. *Otherwise it ends with .s*
  17. Create a Local View
  18. Use *the* Copy **To Local View option** to copy scripts to your Local View  
Right click on Applications in the Local View and select Import. Import the script you have previously exported. Ensure the option is selected to Overwrite exiting applications without warning and select Finish.
  19. Synchronize the script on CCMA by right clicking on server and selecting Synchronize in the Local View.  
Upload the script to CCMA by right clicking the script and selecting Update In Contact Center, this will automatically reactivate the script.
  20. After this you should be able to modify this script.
  21. If you happen to get an error during the activation stage you will need to fix these errors first before going back to Step 5
  - 22.
- Upgrading **from Previous Avaya** Aura® Contact Center 6.x Release

## Unified Communication Environment

### Avaya CS1000 AML Installations

#### Required Patches on CS1000

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

CS 1000 R7.5		PI PEP Enabler	Comments
Note that CS 1000 R7.5 is End of Manufacture Support for software since September 2013.			
		MPLR29976	Multimedia contact cannot return to queue while agent is holding a CDN call. <i>Free of charge PI PEP for AACC.</i>
		MPLR30038 Or MPLR32468	New constant required when CCMS pulls call from interruptible IVR & presents to agent. MPLR32468 also available alternatively as merge of MPLR31712, MPLR31870 and MPLR30038. <i>Free of charge PI PEPs for AACC.</i>
		MPLR32646	CS1000 – Different CLID on CCT desktop and acquired phone when DAPC feature is used. PI: MPLR32414 issue – AACC Agent display issue for local calls + merge with MPLR32279/MPLR32495/MPLR32552 <i>Chargeable PI PEP for AACC</i>
		MPLR32439	AACC USM Ringing event is missing if the call goes back to SCR of the original agent /RGNA feature. Only required if agent configured for RGNA, and only applicable for AACC-SIP (not AACC-AML). <i>GEN patch for AACC.</i>
CS 1000 R7.6 SP 7	DepList Patch	PI PEP Enabler	Comments
	MPLR33345		CS1000 doesn't send AML/MLS Transfer Complete message when POM Dialler completes an external transfer MPLR33345 – GEN PEP – included in R7.6 SP6 and higher.
	MPLR33041	MPLR32229	Multimedia contact cannot return to queue while agent is holding a CDN call. Package 411 prevents agent acquired by AACC from going NOT_READY without dropping the active call. MPLR32229 – Free of charge PI PEP for AACC MPLR33041 – GEN PEP – included in R7.6 SP5 and higher.
	MPLR32413	MPLR30038	New constant required when CCMS pulls call from interruptible IVR & presents to agent. <i>Free of charge PI PEP for AACC.</i> MPLR32413 – GEN PEP – included in R7.6 SP5 and higher.
	MPLR33045 (CPPM, CPPL)	MPLR28837	CS1000 – Different CLID on CCT desktop and acquired phone when DAPC feature is used. MPLR28837 –Chargeable PI PEP for AACC

	MPLR33072 (CPP4)		MPLR33045, MPLR33072 – GEN PEP – included in R7.6 SP5 and higher.
	MPLR32439		AACC USM Ringing event is missing if the call goes back to SCR of the original agent /RGNA feature. Only required if agent configured for RGNA, and only applicable for AACC-SIP (not AACC-AML). <i>GEN patch for AACC – included in R7.6 SP5 and higher.</i>

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

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

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

## Avaya Aura® Installations

This section of the release notes deals with the AACC – Avaya Aura 5.2/6.1/6.2/6.3 integrations. For CS1000 details refer to section above. These should be used in conjunction with the Installation Guide.

**Note:** In a situation where AACC and the UC sides need to be upgraded and the upgrades cannot occur in the same maintenance windows, Avaya recommends that AACC is upgraded first and the UC is upgraded as soon as possible afterwards. During this upgrade period, no call flow changes should be made until both UC and AACC are patched.

### Voicemail

The 3 voicemail platforms that are supported are defined in the table below.

Voicemail Platform	Integration Mechanism	
	SIP	QSig
ACM Messaging	Supported	Not Supported
Modular Messaging	Supported	Not Supported
Aura Messaging	Supported	Not Supported

## Required Software & Patches

Product	Release	Software Version
SMGR	7.0	7.0.0.2
SM	7.0	7.0.0.2
CM	7.0	7.0.0.3.1
AES	7.0	7-0-0-0-Patch2
Presence	7.0	7.0.0.1.361

Product	Release	Software Version
SMGR	6.3	6.3.14
SM	6.3	6.3.14
CM	6.3	6.3.11
AES	6.3	6.3.3 Super Patch 4
Presence	6.2	6.2.6.7
System Platform	6.3	6.3.7

**Note:** Everything up to and included in the Software version column is supported

SM is installed on RHEL Kickstart 6.2

Product Release	Initial Software Version	Patch
-----------------	--------------------------	-------

ME 6.2.2.0.1120	System Platform 6.3	SP7
	CM 6.3	SP11
	smgr 6.3	SP14
	aes 6.3.	SP3 with Super Patch 4
	utility_server 6.3.	SP10
	SM 6.3.	SP14
	Presence 6.2.	SP7 Patch 1

**Note:** Everything up to and included in the Software version column is supported

#### Aura 6.2

Product	Release	Patch
SMGR	6.2	SP4_Patch4_r2033
SM	6.2	SP3 patch 6
CM	6.2	6.2.8
AES	6.2	SuperPatch_4
Presence	6.2	7

SMGR, CM, Presence and AES are installed on System Platform version 6.2.1.0.9

SM is installed using ASM 5.6 RedHat Linux Kickstart

Product Release	Initial Software Version	Patch
ME 6.2.0.0.3105	System Platform 6.2	
	CM 6.2	SP8
	SMGR 6.2	SP4_Patch4_r2033
	AES 6.1.2	612_SuperPatch_4
	Utility_Server 6.2	6.2.11
	SM 6.2	SP3 Patch 6
	Presence 6.1	SP5 Patch 7

#### Aura 6.1

Product	Release	Patch
SMGR	6.1	SP8_Patch4
SM	6.1	SP7
CM	6.1	SP11.01
AES	6.1	612_SuperPatch_4
Presence	6.1	SP5 Patch 7

SMGR, CM, AES and Presence are installed on System Platform version 6.0.3.0.3

SM is installed using ASM 5.5 RedHat Linux Kickstart

Product	Release	Patch
SES	5.2	SP7b



CM	5.2	SP18
AES	5.2	

CM, AES and SES are installed as Software Only systems

**MBT versions supported with GA patches in accordance with support.avaya.com**

MBT 5.2.1.3.5
MBT 5.2.1.3.6
MBT 5.2.1.0.7

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

## Configuration Issues

**wi01078943: “183 Session Progress” msg into AACC causes call drop if agent doesn’t answer before 8 seconds**

On page 5 of 22 under trunk-group on Communication Manager (CM), there is a setting Convert 180 to 183 for Early Media?

Please ensure that this is set to **no** for all trunk groups used within AACC.

### Communication Manager Network Call Redirection (NCR)

On the Communication Manager, the Network Call Redirection (NCR) feature must be disabled on the SIP trunk-group between Communication Manager and Session Manager (that is used to target calls at AACC). The Network Call Redirection (NCR) feature may be enabled for other trunk-groups on Communication Manager.

There is one limitation to disabling NCR; for CDN to CDN conference/join, CDN call and Supervisor Barge-In, CDN call and Agent-invoked Emergency, if one party goes on hold then music-on-hold is streamed by Communication Manager into the 3-party conference (provided music-on-hold is provisioned on Communication Manager).

Note:

If disabling NCR at a system level, please ensure that NCR is first disabled on this SIP trunk-group. Otherwise NCR will remain enabled on the SIP trunk-group even though it is disabled at the system level.

## Call Redirection with AACC SIP Deployments

- ▶ There is an updated version of the Redirection Application Note (version 2.0) available that contains information on the improvements made for the AACC 6.4 SP12 release. This should be referred to by any customer interested in deploying AACC with redirection call scenarios.
- ▶ Call Redirection in an Avaya Aura® Contact Center refers to the scenario where a contact center agent transfers an inbound contact center call to an alternative location which subsequently redirects the call back into the Avaya Aura® Contact Center.
- ▶ The alternative location can be one of:
  - Expert (Local to CM or remote)
  - VDN
  - AAEP
- ▶ This redirection can take a number of forms:
  - Coverage on Busy
  - Coverage no Answer
  - Coverage all calls
  - Call Forward all calls
  - Transfer
  - Conference
  - Scripting (Vector / AAEP)

Call Redirection is not enabled by default with AACC 6.4 SP12 upgrades.

If you wish to avail of this feature then you need to download the Application Note from [support.avaya.com](http://support.avaya.com) and confirm that your Avaya Aura Unified Communications stack is updated to the correct version (including patches). You should also note the limitations with this feature as documented in the application note.

Redirection improvements will only apply to AACC SIP with Avaya Aura deployments. The redirection improvements will not apply to AACC SIP CS1k deployments. For AACC SIP CS1k deployments redirection remains an unsupported activity.

### IMPORTANT NOTE:

If you have already enabled redirection on AACC due to an SP9, SP10 / SP11 upgrade – you will need to manually re-enable redirection after installation of AACC 6.4 as the configuration has migrated from the static configuration file (SGM.properties) to CCMA.

The AACC configuration changes for Redirection have been migrated to CCMA -> Configuration -> Global Settings -> Redirection Settings. In order to enable the feature in AACC 6.4 you need to select the “Media Shuffling on transfer” checkbox (this has the same impact as editing the SGM.properties file). Please note that the configuration settings in CCMA now take precedence over any settings in the properties file. The properties file has been updated accordingly to remove any references to the redirection feature. Any references to the redirection feature in this properties file will be ignored in AACC 6.4.

The reason that this configuration has been moved to CCMA is that now:

- No manual configuration file editing is required
- The change is dynamic (no system restart required)
- The change is replicated to the standby server in a HA environment
- The change is persisted on future Service Pack upgrades

### UCID Generation for Call Redirection

A change has been added in AACC 6.4 SP12 to enable AACC to generate its own UCID. This is for the case where calls arrive into AACC without a UCID. This can happen if the call arrives into AACC via a SIP Carrier -> SBC -> SM -> AACC. Note that the ASBCE product will also support the generation of UCID in a future release.

Note that if AACC receives an incoming SIP INVITE with UCID then it will not attempt to generate its own UCID, but instead it will use the UCID as passed in the incoming SIP INVITE.

For calls that arrive into AACC via PSTN -> CM -> SM -> AACC the CM will have appended a UCID and so AACC UCID generation is not necessary.

The configuration entities in CCMA are now explained:

- **UI Mode**  
The options here are Shared UI and Service provider.  
Shared UI should be chosen for AACC UCID generation.
- **UCID Generation check box**  
This allows the administrator to enable / disable UCID generation in AACC. This has the same properties as the “Media Shuffle on Transfer” check box in that it is dynamic, is replicated in a HA environment and is persisted on a system upgrade.
- **UCID Node Id**  
The Node Id is used to ensure that multiple network entities cannot generate UCIDs that would clash. For this reason the UCID node id must be unique within the network. This means that the node Id used by CM/AAEP for UCID generation must be unique. See screen shot below for CM UCID Node Id configuration for reference.

```

display system-parameters features
FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:                Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
  Switch Name:
  Emergency Extension Forwarding (min): 10
  Enable Inter-Gateway Alternate Routing? n
  Enable Dial Plan Transparency in Survivable Mode? n
  COR to Use for DPT: station
  EC500 Routing in Survivable Mode: dpt-then-ec500

MALICIOUS CALL TRACE PARAMETERS
  Apply MCT Warning Tone? n    MCT Voice Recorder Trunk Group:
  Delay Sending RElease (seconds): 0

SEND ALL CALLS OPTIONS
  Send All Calls Applies to: station    Auto Inspect on Send All Calls? n
  Preserve previous AUX Work button states after deactivation? n

UNIVERSAL CALL ID
  Create Universal Call ID (UCID)? y    UCID Network Node ID: 882
  
```

Note: With call redirection, an agent can perform a consult transfer to AAEP. However, there is a limitation in a very specific scenario that if an agent were to initiate a consult transfer to AEP **and** the agent were to select menu options which resulted in AEP sending the call back to AACC **and** the agent does not complete the transfer **before** AEP attempts to send the call back to AACC, there is an issue that the agent doesn't get through to the contact center (on the consult leg of the call). However, the agent can toggle back to the customer leg of the call as the customer is still on hold— so the customer leg is not dropped.

## SIP specific issues

### CTI behaviour for Transfer and Conference

CTI behaviour of Transfer and Conference in AACC SIP installations is not linked to any particular AACC release but depends on CTI Switch used in the solution:

- CS 1000 or Avaya Aura® Application Enablement Services version 6.2 or greater:
  - Consultation Transfer Call can only be completed using CTI as Transfer.
  - Consultation Conference Call can only be completed using CTI as Conference.
- Avaya Aura® Application Enablement Services version 6.1 or earlier:
  - Consultation Transfer Call can be completed using CTI as either Transfer or Conference.

### SIP Endpoints Issues

Following issues were seen when testing with SIP Endpoints as agent stations:

- For a consult originated by an agent, it is observed that TR/87 messaging from AES indicates that there are two calls originated in quick succession. As a result AACC reports this as two calls. The first call is cleared before the second is initiated however the second call originated is created as an unrelated call (based on information received in TR/87 messages) hence agent will not be able to complete the transfer / conference.  
Resolution: This issue is resolved if the connectivity between AACC & SM is changed to TLS.
- Intermittent problems are observed when CTI operations are performed in quick succession.
- TR/87 messaging for a failed call (call to an invalid number) is different in case of SIP endpoint when compared with H.323 endpoint. Based on the TR/87 messages received the failed call is cleared from Agent Desktop even though the call is still up on agent's phoneset playing invalid number tone. This invalid number tone is played for 30 seconds after which the call is cleared from the phone as well. However in this duration, there will be a mismatch in agent state between AACC and the SIP endpoint and can lead to an issue of agent being set to Not Ready if a skillset call was to be presented to him at this time.
- It is not possible to complete a conference if the consult call is not answered by the called party (using SIP endpoint). Thus it is not possible to complete conference on ringing.

---

#### Consult initiated from the SIP phoneset shows up as unrelated call on AAAD

---

An issue has been identified with the use of SIP phones with AACC6.4 against CM 6.3.3 or greater. The issue is only seen when the 3<sup>rd</sup> line is configured.

The issue was introduced by a CM fix to send a 'ServiceInitiatedEvent' as soon as a line is initiated on the SIP phone. However, this 'ServiceInitiatedEvent' includes an incorrect cause value indicating a new call is being initiated, rather than a consult call. The issue only occurs if the agent initiates a consult call from their SIP phone. There is no issue if the consult call is initiated from their Agent Desktop (AAAD).

#### Workaround:

Initiate the consult call from Avaya Aura Agent Desktop (AAAD)

#### Recovery:

If the agent accidentally initiates the consult from their SIP phone, when they notice the 'Complete Consult' option is available on their SIP phone but not on AAAD, they need to drop the consult call and un-hold the customer call. They can then initiate the consult from AAAD.

#### Resolution:

This issue will be addressed in a future SIP phone software up-issue. It is tracked by JIRA ticket SIP96X1-11200.

---

### Call Redirection with Microsoft Exchange VoiceMail

The AACC Call Redirection Application Notes stated incorrectly that Microsoft Exchange VoiceMail is a supported feature of AACC 6.3 SIP installations. The following scenario resulted in Contacts getting stuck in Agent Desktop after call for agent covers to Exchange VoiceMail:

- Agent 1 calls Agent 2 but receives a busy tone.

- Agent 1 leaves a Microsoft Exchange VoiceMail to Agent 2.
- Agent 2's AAAD GUI throws a notification message that there is a voicemail pending.
- Agent 2 attempts to dismiss this notification but is unable.
- Agent 2 has to force terminate AAAD through CTRL+ALT+DEL Task Manager.

Resolution: The documentation has been updated to state that AACC supports Voice Mail Call Redirection to Avaya Messaging (AAM), Communication Manager Messaging (CMM) and Modular Messaging (MM).

## DTMF audible during supervisor Observe

For the Observe functionality (skillset as well as non-skillset Observe), supervisor joins the call as a silent participant i.e. there will be one way speech path for the supervisor. However if the supervisor presses any buttons on his phoneset, the DTMF tones are audible in the conference. CM JIRA CM-2856 has been created for this issue.

## Changes to SIP Licensing

### AMS Instance Licensing

A new feature was delivered to AACC SP12 and SP13 that limits the number of AMS servers that are licensed by AACC when using WebLM licensing. This limit is based on the **VALUE\_CCTR\_AMS\_INSTANCE** count in the WebLM xml license file. An AMS HA pair requires two **AMS\_INSTANCE** licenses. The AACC LM is responsible for controlling this feature. Once an LM is started, it checks the CCMA CONF service in "Media Service and Routes". The AACC LM will then push an AMS Nodal license to each AMS (or to both Primary and Backup AMS in a HA pair if the AMS HA Managed IP Address is specified in CCMA). It will limit the number of AMS servers it will license to **VALUE\_CCTR\_AMS\_INSTANCE**. All AMS Servers encountered over the number of AMS Instance features licenses available will be unlicensed.

Check to make sure the WebLM license has the **VALUE\_CCTR\_AMS\_INSTANCE** equal to the number of AMS servers in your solution.

**Note:** An AMS HA pair will consume two **VALUE\_CCTR\_AMS\_INSTANCE** feature licenses.

If this is not correct then please contact PLDS and request a new WebLM license with the correct **VALUE\_CCTR\_AMS\_INSTANCE** count.

Refer to **PSN004239** for more detailed information.

## Changes to Announcement and Dialog Treatment Licensing

On a SIP Contact Center, customers should always have purchased the required number of ANNC and DIALOG licenses for their Contact Center implementation. Prior to AACC SP12, there was an issue with the consumption of these licenses. AACC SP12 corrected the enforcement of these licenses. All AACC SIP customers MUST check to make sure that they have the required number of ANNC and DIALOG licenses. These licenses are based on **VALUE\_CCTR\_ANNOUNCE\_PORTS** and **VALUE\_CCTR\_DIALOG\_PORTS** counts in the WebLM xml license file or **\_\_sip-annc::sess** and **\_\_sip-dialog::sess** counts in the KRS/PLIC license file.

The following changes have been implemented:

1. AACC CCMS now controls the ANNC and DIALOG licensing.
2. CCMS reads the number of licenses at startup from LM. If a new license file is applied with a change to the ANNC or DIALOG license count, then CCMS needs to be restarted.
3. **GIVE IVR** Orchestration Designer (OD) Script is the only command that consumes ANNC or DIALOG licenses.

4. When the GIVE IVR command completes, it immediately returns the license to the free license pool.
5. GIVE IVR command consumes a DIALOG license if it's playing an announcement **AND** collecting digits.
6. GIVE IVR command consumes an ANNC license if only playing an announcement.
7. The following OD Script commands do not consume ANNC or DIALOG licenses:
  - GIVE RINGBACK
  - GIVE RAN <route>
  - GIVE MUSIC <route>
8. TFE will write the following events to the Windows Event Log:

Category	AMS Dialog
Event	<b>48582</b>
Severity	Critical
Description	AMS Dialog license usage has reached critical condition.

Category	AMS Dialog
Event	<b>48583</b>
Severity	Critical
Description	AMS Dialog license usage has reached major condition

Category	AMS Announcement
Event	<b>48584</b>
Severity	Critical
Description	AMS Announcement license usage has reached critical condition

Category	AMS Announcement
Event	<b>48585</b>
Severity	Critical
Description	AMS Announcement license usage has reached major condition

License thresholds are reported at 80% (major) and 90% (critical) usage condition. Both threshold percentages are configurable via the Windows Registry  
Refer to **PSN004272** for more detailed information.

## 'Transfer Complete' button not available on AAAD when two unrelated calls are active

### 'Transfer Complete' button not available on AAAD when two unrelated calls are active

The 'Transfer Complete' button is not present on Avaya Aura Agent Desktop (AAAD) when two unrelated calls are active. If an Agent who is active on a call initiates a new second call they will not be able to join these calls via the 'Transfer Complete' button on AAAD. There are two workarounds available:

#### Workarounds:

- 1) The second call must be initiated as a 'Transfer Call' in AAAD, and not by initiating a new second unrelated call. The 'Transfer Complete' option will then be available.
- 2) If two unrelated calls are active the Agent can join these calls via the 'Conference/Join' button. If the Agent does not wish to remain in the call they must manually drop from the conference.

## SIP HA Specific Issues

N/A

## Pre Installation Instructions

**HA Installation: AMS Linux upgrades are still supported on Redhat Enterprise 5.x or 6.x 32bit OS, however all new deployments of AMS on Redhat must use Redhat Enterprise 6.x 64bit OS.**

The Linux version of the Avaya Media Server is only supported on the 32bit version of Redhat Enterprise 5.x or 6.x for existing installations. Any new installations of AMS on Linux servers must use Redhat Enterprise 6.x 64 bit OS.3. AMS is only supported on Redhat installed with the Linux **English language pack**.

**HA Installation: Avaya G430 / G450 on same Subnet as Avaya Media Server HA Pair**

If the G430 / G450 are on the same subnet as the Avaya Media Server HA Pair, then ARP Spoofing protection needs to be disabled on the G4x0 to allow for correct operation in the event of an Avaya Media Server Failover. In an Avaya Media Server HA Pair, when the current active AMS fails, the backup AMS will send Gratuitous ARP messages indicating that its MAC address should be used for the Managed IP address of the Avaya Media Server HA pair. The G4x0 is normally configured to enable ARP Spoofing protection which will cause the G4x0 to ignore these GARP messages causing one-way speech path problems when an Avaya Media Server failover occurs. The ARP Spoof protection must be disabled on the G4x0 using the CLI command:

**“no ip arp inspection”**

**HA Installation: Avaya G650 Gateway MedPro boards cannot be on same subnet as Avaya Media Server HA Pair**

Unlike G4x0 gateways, G650 gateways do not allow for ARP Spoofing protection to be turned off at all. Therefore, to avoid the one-way speech path issues indicated above in the event of an AMS HA pair failover, the MedPro boards of any G650 gateways used to communicate with AMS must be homed on a different subnet. This ensures these boards do not need to handle the GARP messages issued by the AMS backup server during a failover.

The management IP address of the gateway itself is not likewise impacted, since there is no media traffic with the AMS servers crossing that network interface. That is, the gateway's own address can be in any required subnet.

**HA Installation: Agent extensions on same subnet as AMS HA Pair require Gratuitous Address Resolution Protocol (GRATARP)**

If the agent extensions (stations/phones) are on the same subnet as the AMS HA Pair then GRATARP must be enabled on the agent extensions. This setting is configured in the 46xxsettings.txt file on the Utility Server. GRATARP must be set to 1:

```
##### GRATUITOUS ARP SETTINGS #####
```

```
##
## GRATARP specifies the phones behavior for handling Gratuitous ARP.
##     In the PE Dup Environment, if the PE DUP server and the phone reside
##     in the same subnet, the user should set this to 1.
## 0 – (Default) ignore all received gratuitous ARP messages.
## 1 – Phones will update an existing ARP cache entry with the MAC address received in a gratuitous
ARP message
##     for that entry's destination IP address.
```

```
SET GRATARP 1
```

```
## NOTE: This feature is available on H.323 release 3.0SP1 for 96xx phones.
##
```

## Post Installation Instructions

### Configuration Issues

Agents URIs need to be unique across all agents and media type. The domain for IM Presence users should be different from the Voice domain e.g. Agent 1 should have a Voice URI of [AgentVoiceURI@voicedomain.com](#) and the presence username should be [AgentIMURI@presencedomain.com](#).

Also an agent should not have the same prefix name if they are configured for Voice and Presence. If they have the same name, then this can cause issues on AAAD where an agent wants to make a call out of the Contact Center. So the following is not supported and will be blocked in CCMA when creating or modifying an agent e.g. [Agent1@voicedomain.com](#) and [Agent1@presencedomain.com](#) are not supported.

Customers migrating from a CS1K/OCS based install should check that Agents names are unique. Otherwise errors may occur when modifying these agents.

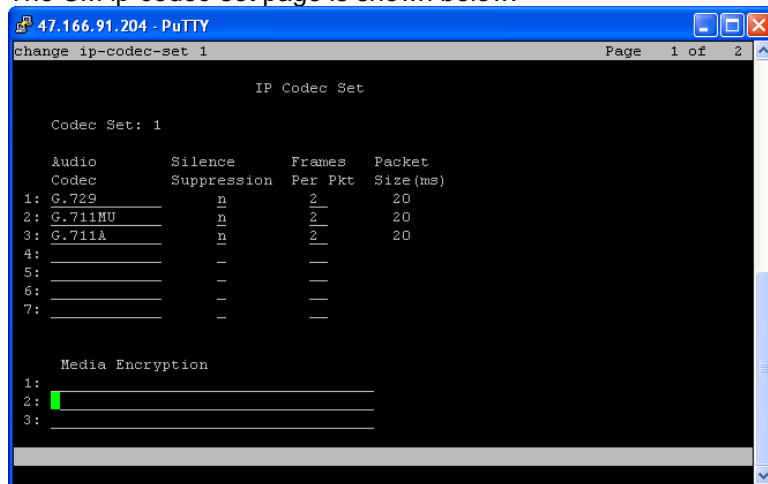
### G.729 Codec Support

In configurations where network bandwidth is limited, G.729 can be used as the Voice codec on either the customer leg **OR** the agent leg of the call. G.729 is **NOT** supported on both legs of the Contact Center call as this could result in voice quality issues.

If G.729 is required, it needs to be configured on both CM and AMS.

CM Network regions should be used to achieve particular codec used on either customer leg or agent leg.

The CM ip-codec-set page is shown below:

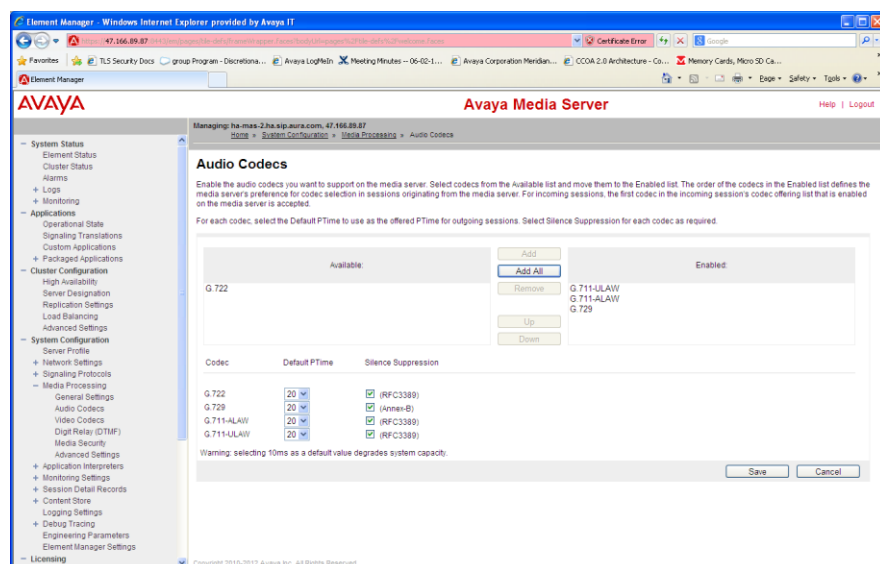


The AMS Audio codecs page is shown below. It is set in:

EM->System Configuration->Media Processing->Audio Codecs

G.729 MUST be in the AMS Audio Codec list if SIP Call Recording is being used as the ACR only uses G.729. Note: As the ACR recording leg is not on the voice path between agent and customer, it will have no impact on voice quality of this call.





## Voice Codec Packet Size (ptime) limitations

Voice codecs MUST use a Packet Size (ptime) of 20ms. Larger Packet sizes are not supported.

## Known CCMS limitations

None

## Avaya Media Server

AACC 6.4 SP16 includes Avaya Media Server 7.6. The process for upgrading an existing installation of AMS 7.5 to 7.6 depends upon the operating system on which AMS is installed and potentially which AACC Service Pack line-up your AMS system is currently installed with. Full procedures for most upgrade scenarios are documented in *44400-410 AACC Upgrade and Patches*, though you should read this in conjunction with the information provided here. If upgrading an AMS cluster (HA or N+1 clusters) from SP10 or earlier then clustering **MUST** be disabled on ALL AMS servers before proceeding with the upgrade. This procedure is detailed in document: **Installing, Upgrading and Patching Avaya Media Server 7.5 June 2013** and AACC PSN: **PSN004175u** which are both available on support.avaya.com.

NOTE: The default media services for AACC have been changed in this release. The “ANNC”, “DIALOG” and “AG” services have been removed. The media services now provided are CONF and XDIALOG. (The XDIALOG service should not be assigned to Avaya Media Server instances in CCMA. This is for use with Avaya Voice Portal or Avaya Aura Experience Portal only.)

## Red Hat Enterprise Linux support

AACC 6.4 SP16 introduces support for AMS 7.6 installations on the 64bit variant of RHEL 6.4, and requires this be used for all new installations. RHEL 5.x and RHEL 6.x 32bit installations continue to be supported for existing customers.

The setup process for RHEL 6.x requires some post-installation configuration steps on Red Hat prior to installing AMS that were not previously necessary when using RHEL 5.x. This is due to AMS having some package dependencies that are not in the default package set for standard installations of RHEL 6.x.

Additional installation steps to cover this are documented in *44400-311 AACC installation Guide* and also *44400-410 AACC Upgrade and Patches Guide*. The following sequence of commands (which should be executed as the *root* user) summarizes the steps needed to apply the correct packages via the ‘yum’ package manager. Ensure the RHEL 6.x DVD is inserted into your system’s DVD drive before completing this procedure:

```
mkdir /mnt/cdrom
mount -t auto /dev/cdrom /mnt/cdrom
cp /mnt/cdrom/media.repo /etc/yum.repos.d/
chmod +rw /etc/yum.repos.d/media.repo
echo -e "baseurl=file:///mnt/cdrom\nenabled=1" >> /etc/yum.repos.d/media.repo
yum install e2fsprogs-libs.i686 glibc.i686 keyutils-lib.i686 krb5-libs.i686 libgcc.i686 libstdc++.i686
zlib.i686 libaio.i686 ncurses-libs.i686 iproute
```

Note that the package dependencies for AMS 7.6 have also changed slightly from AMS 7.5, so customers upgrading from AACC 6.3 should also ensure the correct packages identified above are applied to their systems.

Also note that the use of desktop GUIs such as Gnome or KDE is not supported on RHEL systems operating Avaya Media Server for AACC.

## Support for Security Enhanced Linux (selinux)

AMS 7.6 introduces support for selinux when using RHEL 6.x. This is not supported on RHEL 5.x. Customers currently using AMS on RHEL 5.x are recommended to upgrade to RHEL 6.x.

## Avaya Media Server Linux Logs

AMS logs are logged in UTC time regardless of the Linux time zone configuration. When reviewing AMS logs with AACC logs, the AACC logs are logged in local time and the AMS logs are logged in UTC time. The AMS log timestamps may be different to the AACC log timestamps.

## Avaya Media Server Specifications for High Availability Pair

Avaya Media Server High Availability Pair is only supported on the High-end server specification. Refer to document: *AACC Fundamentals and Planning 44400-211* for details of the high-end server specification.

## AMS Upgrade Procedures

You can upgrade your AMS server from any AACC 6.3 Service Pack to AMS 7.6 for use with AACC 6.4 SP16. It is recommended that you move to Service Pack 11 (AMS 7.5.0.1140 + CCSA 6.3.0.115) before upgrading to AMS 7.6, though this is not mandatory. At a minimum, ensure you have applied all available AMS and CCSA QFE patches for your current Service Pack before upgrading to AMS 7.6.

## Upgrading Clustered AMS Servers from SP10 to SP16

If upgrading AMS clusters (either HA or N+1 Clusters) that are on release SP10 or earlier, then clustering **MUST** be disabled on ALL AMS servers before proceeding with the upgrade. Also all AMS servers **MUST** be upgraded to the same version. Once all AMS servers have been upgraded, clustering must be re-enabled. If the AMS cluster is at SP11 or SP12 (or a later SP) then clusters do not need to be disabled to upgrade to SP16. This procedure is detailed in document: **Installing, Upgrading and Patching Avaya Media Server 7.5 June 2013** and AACC PSN: **PSN004175u** which are both available on support.avaya.com.

## AMS Windows Upgrade Procedures

### New Single Server installations of AACC 6.4 SP16

If performing a new Single Server (AACC + AMS on a single Windows instance) installation of AACC 6.4 SP16 by using the AACC 6.4 DVD in conjunction with the AACC 6.4 SP16 release bundle for install time patching, you must still manually upgrade the versions of AMS and CCSA after completing the installation wizard. This is because the AACC installation wizard does not use the AMS and CCSA installation packages supplied in release bundles in preference to those supplied on the DVD as part of the install time patching process.

To perform this upgrade, simply follow the procedure in the section below.

- 1) Shutdown AACC via the System Control and Monitor Utility.
- 2) Go to Start->Run-> and type "services.msc"
- 3) Stop Service: "CC SMMC Daemon"
- 4) Stop Service: "CC SMMC"
- 5) Uninstall *Contact Center Services for AMS* via the Windows Control Panel
- 6) Locate the **Install Software\AMS\Windows** folder on the SP16 Release Bundle, launch the Avaya Media Server installer and proceed through the installation wizard:  
**InstallerMAS.exe**
- 7) Launch the Contact Center Services for AMS installer and proceed through the installation wizard:  
**ContactCenterServicesForAMS.msi**
- 8) Download and apply all available AMS and CCSA QFE patches.
  - a. Copy all available patch ZIP files to the %MASHOME%\QFE folder
  - b. Run the following command:  
**amspatch apply all**

### Upgrading AMS on AACC Single Server from 6.3 SP10 to 6.4 SP16

This section details the procedure for upgrading AMS and CCSA on existing AACC 6.3 SP10 single server systems to AACC 6.4 SP16.

- 1) Shutdown AACC via the System Control and Monitor Utility.
- 2) Go to Start->Run-> and type "services.msc"
- 3) Stop Service: "CC SMMC Daemon"
- 4) Stop Service: "CC SMMC"
- 5) If this is an AMS primary node, perform a backup of 'System Configuration' and 'Application Content' via the **Tools -> Backup and Restore -> Backup Tasks** page in AMS Element

Manager. Note: The default location for AMS backups is

**%MASHOME%\platdata\EAM\Backups.**

These AMS backup files are preserved during a un-install and re-install, however they should be backed up to another location as a precautionary step.

- 6) If you have deployed any locale specific media files to the AMS file system (as opposed to the Content Store), take a backup of these files. These will have been deployed in the relevant locale sub-folders of **%MASHOME%\platdata\Announcements\contactcenter\default**
- 7) Apply the latest AACC Windows Firewall Policy
  - a. Launch the firewall policy tool – *Start -> Administrative Tools -> Windows Firewall Policy with Advanced Security*
  - b. Click '*Import Policy...*', answer Yes when prompted, and locate the AACC Firewall Policy file on the AACC 6.4 DVD or SP16 Release Bundle:  
**<drive>:\AACCFirewallPolicy\AACC Firewall Policy (Ver 1.xx).wfw**  
 Note: In order to enable Rollback of this policy it is recommended that you export your existing Firewall setting from the "Windows Firewall with Advanced Security" application before you apply this AACC Firewall Policy. If you subsequently need to roll back the policy, you can import your saved policy file and this will remove the new AACC policy settings.
- 8) Uninstall *Contact Center Services for AMS* via the Windows Control Panel
- 9) Uninstall Avaya Media Server 7.5 via the Windows Control Panel. When prompted to preserve or remove data, select the 'Remove' option.
- 10) Locate the **Install Software\AMS\Windows** folder on the AACC 6.4 SP16 Release Bundle, launch the Avaya Media Server installer and proceed through the installation wizard:  
**InstallerMAS.exe**
- 11) Launch the Contact Center Services for AMS installer and proceed through the installation wizard:  
**ContactCenterServicesForAMS.msi**
- 12) Download and apply all available AMS and CCSA QFE patches.
  - a. Copy all available patch ZIP files to the **%MASHOME%\QFE** folder
  - b. Run the following command:  
**amspatch apply all**
- 13) If this is an AMS primary node, upgrade and restore the backups taken in step 1 using the ccsaupgrade command-line tool:  
**ccsaupgrade <system-config-backup> <app-data-backup>**
- 14) Restore the locale specific media files that were backed up in step 2 (if any).
- 15) Reboot the server

## Upgrading AMS on AACC Single Server from 6.3 SP11 or 6.4 SP12 to 6.4 SP16

This section details the procedure for upgrading AMS and CCSA on existing AACC 6.3 SP11 or AACC 6.4 SP12 single server systems to AACC 6.4 SP16.

- 1) Shutdown AACC via the System Control and Monitor Utility.
- 2) Go to Start->Run-> and type "services.msc"
- 3) Stop Service: "CC SMMC Daemon"
- 4) Stop Service: "CC SMMC"
- 5) If this is an AACC 6.3 SP11 system then you need to apply the latest AACC Windows Firewall Policy (Firewall Policy did not change between SP12 and SP16)
  - a. Launch the firewall policy tool – *Start -> Administrative Tools -> Windows Firewall Policy with Advanced Security*
  - b. Click '*Import Policy...*', answer Yes when prompted, and locate the AACC Firewall Policy file on the AACC 6.4 DVD or SP16 Release Bundle:  
**<drive>:\AACCFirewallPolicy\AACC Firewall Policy (Ver 1.xx).wfw**  
 Note: In order to enable Rollback of this policy it is recommended that you export your existing Firewall setting from the "Windows Firewall with Advanced Security" application before you apply this AACC Firewall Policy. If you subsequently need to roll back the policy, you can import your saved policy file and this will remove the new AACC policy settings.
- 6) Uninstall *Contact Center Services for AMS* via the Windows Control Panel
- 7) Locate the **Install Software\AMS\Windows** folder on the SP16 Release Bundle, launch the Avaya Media Server installer and proceed through the installation wizard:  
**InstallerMAS.exe**

- 8) Launch the Contact Center Services for AMS installer and proceed through the installation wizard:  
**ContactCenterServicesForAMS.msi**
- 9) Download and apply all available AMS and CCSA QFE patches.
  - a. Copy all available patch ZIP files to the **%MASHOME%\QFE** folder
  - b. Run the following command:  
**amspatch apply all**

## Upgrading AMS on Windows Standalone Server

Avaya no longer supports standalone deployments of Avaya Media Server on Windows for new AACC customers from version 6.3 onwards. As such, there is no longer an option available on the AACC 6.3 or later DVDs to install only Avaya Media Server onto new systems.

For existing AACC customers already using standalone AMS deployments on Windows, these can be upgraded to AMS 7.6 for use with AACC 6.4 using the procedure below and will be supported. Note that this upgrade process is not documented in the AACC 6.4 user documentation, but is addressed here only.

## Upgrading AMS on Windows Standalone Server from AACC 6.3 to 6.4 SP16

- 1) If this is an AMS primary node, perform a backup of 'System Configuration' and 'Application Content' via the **Tools -> Backup and Restore -> Backup Tasks** page in AMS Element Manager. Note: The default location for AMS backups is **%MASHOME%\platdata\EAM\Backups**.  
These AMS backup files are preserved during a un-install and re-install, however they should be backed up to another location as a precautionary step.
- 2) If this is an standalone AMS primary node using PLIC licensing, take a copy of the license from the Primary AMS Server (*AACC Upgrade and Patches 44400-410*) – this is not required if AACC is using WebLM licensing. Note: Licensing is not preserved in AMS backups.
- 3) If you have deployed any locale specific media files to the AMS file system (as opposed to the Content Store), take a backup of these files. These will have been deployed in the relevant locale sub-folders of **%MASHOME%\platdata\Announcements\contactcenter\default**
- 4) Apply the latest AACC Windows Firewall Policy
  - a. Launch the firewall policy tool – *Start -> Administrative Tools -> Windows Firewall Policy with Advanced Security*
  - b. Click *'Import Policy...'*, answer Yes when prompted, and locate the AACC Firewall Policy file on the AACC 6.3 DVD or SP11 Release Bundle:  
**<drive>:\AACCFirewallPolicy\AACC Firewall Policy (Ver 1.xx).wfw**  
Note: In order to enable Rollback of this policy it is recommended that you export your existing Firewall setting from the "Windows Firewall with Advanced Security" application before you apply this AACC Firewall Policy. If you subsequently need to roll back the policy, you can import your saved policy file and this will remove the new AACC policy settings.
- 5) Uninstall *Contact Center Services for AMS* via the Windows Control Panel
- 6) Uninstall *Contact Center Tomcat Instance* via the Windows Control Panel
- 7) Uninstall Avaya Media Server 7.5 via the Windows Control Panel. When prompted to preserve or remove data, select the 'Remove' option.
- 8) Locate the **Install Software\AMS\Windows** folder on the AACC 6.4 SP16 Release Bundle, launch the Avaya Media Server installer and proceed through the installation wizard:  
**InstallerMAS.exe**
- 9) Locate the **ThirdParty\ThirdPartySoftware\jre1.6.0\_<xx>\_x64** folder on the AACC 6.4 SP16 Release Bundle (where <xx> is the specific update number of the JRE supplied) and launch the JRE installer there:  
**jre1.6.0\_<xx>.msi**
- 10) Locate the **ThirdParty\ThirdPartySoftware\Tomcat7.0.<xx>** folder on the AACC 6.4 SP16 Release Bundle (where <xx> is the specific update number of the Tomcat installer supplied) and launch the Tomcat installer there:  
**ContactCenterTomcatInstall.msi**
- 11) Launch the Contact Center Services for AMS installer and proceed through the installation wizard:  
**ContactCenterServicesForAMS.msi**
- 12) Download and apply all available AMS and CCSA QFE patches.
  - a. Copy all available patch ZIP files to the **%MASHOME%\QFE** folder

- b. Run the following command:  
**amspatch apply all**
- 13) If this is an AMS primary node, upgrade and restore the backups taken in step 1 using the ccsaupgrade command-line tool:  
**ccsaupgrade <system-config-backup> <app-data-backup>**
- 14) If this is an AMS primary node and AMS using PLIC licensing, restore the license copied in step 2 by copying the backed up license file into EM->Licensing->General Settings "Add License Keys". Hit "Display Licenses", "Save" and then "Confirm"
- 15) Restore the locale specific media files that were backed up in step 3 (if any).
- 16) Reboot the server

## Upgrading AMS on Windows Standalone Server from AACC 6.4 SP12 (or later) to SP16

- 1) Uninstall *Contact Center Services for AMS* via the Windows Control Panel
- 2) Locate the **Install Software\AMS\Windows** folder on the AACC 6.4 SP16 Release Bundle, launch the Avaya Media Server installer and proceed through the installation wizard:  
**InstallerMAS.exe**
- 3) Launch the Contact Center Services for AMS installer and proceed through the installation wizard:  
**ContactCenterServicesForAMS.msi**
- 4) Download and apply all available AMS and CCSA QFE patches.
  - a. Copy all available patch ZIP files to the %MASHOME%\QFE folder
  - b. Run the following command:  
**amspatch apply all**

## AMS Red Hat Enterprise Linux (RHEL) Upgrade Procedures

### Upgrading AMS on RHEL Servers from AACC 6.4 SP12 (or later) to SP16

AACC 6.4 SP12 (or later SPs) and SP16 support two deployments types of Avaya Media Server: OVA deployed AMS and AMS installed on a physical server with customer supplied Red Hat OS.

Avaya supplies RPM Rollup bundle for OVA deployed AMS servers.

This rollup bundle is built into the ContactCenterServicesForAMS\_6.4.0.158 installer and applies the RPM updates to an AMS OVA.

For Customer purchased Red Hat Installations, the customer is responsible for obtaining the Red Hat updates by registering on the Red Hat Network.

To upgrade AACC 6.4 SP12 (or later) to SP16, run the following procedure:

- 1) Locate the **Install Software\AMS\Linux** folder on the AACC 6.4 SP16 Release Bundle.
- 2) On your Linux server, use the su command to change to the root user account:  
`su -`
- 3) Create a temporary folder on Linux server by running command:  
`mkdir /tmp/AvayaMS`
- 4) Copy the following files from the SP16 release bundle to the /tmp/AvayaMS folder:
  - MediaServer\_7.6.0.959\_2014.11.27.bin
  - ContactCenterServicesForAMS\_6.4.0.158.bin
- 5) Change to folder: /tmp/AvayaMS and run command:  
`chmod +x ContactCenterServicesForAMS_6.4.0.158.bin`
- 6) To Install Avaya Media Server and Contact Center Services for AMS run command:  
`./ContactCenterServicesForAMS_6.4.0.158.bin`

For an AMS OVA installation, this binary will apply all the latest Red Hat RPMs to the OVA to upgrade the Red Hat OS to the same version that is shipped with SP16 OVA.

- 7) Download and apply all available AMS and CCSA QFE patches.
  - a. Copy all available patch ZIP files to the \$MASHOME/qfe folder
  - b. Run the following command:  
**amspatch apply all.**



## Upgrading AMS on RHEL Servers from AACC 6.3 to 6.4 SP16

On Linux servers, AMS can be upgraded to version 7.6 from the 7.5 version supplied with any AACC 6.3 Service Pack, though the procedure for doing so depends upon your current Service Pack level and whether or not you have the SP11 Release Bundle available.

As above, note that for all installation and upgrade procedures, you should use the AMS and CCSA installation packages supplied with the AACC 6.4 SP16 release bundle as opposed to those supplied with the AACC 6.4 DVD as these represent the most recent product versions.

### *Upgrading from Service Pack 11*

- 1) Locate the **Install Software\AMS\Linux** folder on the AACC 6.4 SP16 Release Bundle.
- 2) On your Linux server, use the su command to change to the root user account:  
`su -`
- 3) Create a temporary folder on Linux server by running command:  
`mkdir /tmp/AvayaMS`
- 4) Copy the following files from the SP16 release bundle to the /tmp/AvayaMS folder:
  - `MediaServer_7.6.0.959_2014.11.27.bin`
  - `ContactCenterServicesForAMS_6.4.0.158.bin`
- 5) Change to folder: /tmp/AvayaMS and run command:  
`chmod +x ContactCenterServicesForAMS_6.4.0.158.bin`
- 6) To Install Avaya Media Server and Contact Center Services for AMS run command:  
`./ContactCenterServicesForAMS_6.4.0.158.bin`
- 7) Download and apply all available AMS and CCSA QFE patches.
  - c. Copy all available patch ZIP files to the **\$MASHOME/qfe** folder
  - d. Run the following command:  
**amspatch apply all.**

### *Upgrading from Service Pack 8, 9 or 10 with Service Pack 11 available*

If you are currently using SP8, 9 or 10 and have the Service Pack 11 Release Bundle available to you, use this procedure to upgrade your AMS system:

- 1) Locate the **Install Software\AMS\Linux** folder on the SP11 Release Bundle.
- 2) On your Linux server, use the su command to change to the root user account.  
`Su -`
- 3) Create a temporary folder on Linux server by running command:  
`mkdir /tmp/AvayaMS`
- 4) Copy the `MediaServer_7.5.0.1140_2013.06.13.bin` from the SP11 Release Bundle to /tmp/AvayaMS
- 5) Change directory using command: `cd /tmp/AvayaMS`
- 6) Grant executable permissions to the installation file:  
`chmod +x MediaServer_7.5.0.1140_2013.06.13.bin`
- 7) Start the AMS upgrade from SP8, 9 or 10 to SP11 by running command:  
`./MediaServer_7.5.0.1140_2013.06.13.bin`
- 8) Select 1- Upgrade
- 9) There is no need to install the 7.5.0.1140 QFEs or upgrade the CCSA application.
- 10) Locate the **Install Software\AMS\Linux** folder on the AACC 6.4 SP16 Release Bundle.
- 11) On your Linux server, use the su command to change to the root user account:  
`su -`
- 12) Copy the following files from the SP16 release bundle to the /tmp/AvayaMS folder:
  - `MediaServer_7.6.0.959_2014.11.27.bin`
  - `ContactCenterServicesForAMS_6.4.0.158.bin`
- 13) Change to folder: /tmp/AvayaMS and run command:  
`chmod +x ContactCenterServicesForAMS_6.4.0.158.bin`
- 14) To Install Avaya Media Server and Contact Center Services for AMS run command:  
`./ContactCenterServicesForAMS_6.4.0.158.bin`
- 15) Download and apply all available AMS and CCSA QFE patches.

- a. Copy all available patch ZIP files to the **\$MASHOME/qfe** folder
- b. Run the following command:  
**amspatch apply all.**

### *Upgrading from Service Pack 8, 9 or 10 without Service Pack 11 available*

If you are currently using SP8, 9 or 10 and have not downloaded the Service Pack 11 Release Bundle, you can use this procedure to upgrade your AMS system:

- 1) If this is an AMS primary node, perform a backup of 'System Configuration' and 'Application Content' via the **Tools -> Backup and Restore -> Backup Tasks** page in AMS Element Manager.  
Note: The default location for AMS backups is  
**\$MASHOME/platdata/EAM/Backups.**  
These AMS backup files are preserved during a un-install and re-install, however they should be backed up to another location as a precautionary step.
- 2) If this is an AMS primary node using PLIC licensing, take a copy of the license from the Primary AMS Server (*AACC Upgrade and Patches 44400-410*) – this is not required if AACC is using WebLM licensing. Note: Licensing is not preserved in AMS backups.
- 3) If you have deployed any locale specific media files to the AMS file system (as opposed to the Content Store), take a backup of these files. These will have been deployed in the relevant locale sub-folders of **\$MASHOME/platdata/Announcements/contactcenter/default**
- 4) Uninstall *Contact Center Services for AMS 6.3*:  
**/opt/orte/UninstallCCSM**
- 5) Uninstall Avaya Media Server 7.5:  
**/opt/orte/UninstallMediaServer/UninstallMediaServer**
- 6) Answer 'yes' to 'Do you want to continue?'
- 7) Answer 'no' to 'Do you want to preserve the System Configuration and Application Content?'
- 8) Locate the **Install Software\AMS\Linux** folder on the AACC 6.4 SP16 Release Bundle.
- 9) On your Linux server, use the su command to change to the root user account:  
su -
- 10) Create a temporary folder on Linux server by running command:  
mkdir /tmp/AvayaMS
- 11) Copy the following files from the SP16 release bundle to the /tmp/AvayaMS folder:
  - MediaServer\_7.6.0.959\_2014.11.27.bin
  - ContactCenterServicesForAMS\_6.4.0.158.bin
- 12) Change to folder: /tmp/AvayaMS and run command:  
chmod +x ContactCenterServicesForAMS\_6.4.0.158.bin
- 13) To Install Avaya Media Server and Contact Center Services for AMS run command:  
./ContactCenterServicesForAMS\_6.4.0.158.bin
- 14) Download and apply all available AMS and CCSA QFE patches.
  - a. Copy all available patch ZIP files to the **\$MASHOME/qfe** folder
  - b. Run the following command:  
**amspatch apply all.**
- 15) If this is an AMS primary node, upgrade and restore the backups taken in step 1 using the ccsaupgrade command-line tool:  
**ccsaupgrade <system-config-backup> <app-data-backup>**
- 16) If this is an AMS primary node and AMS using PLIC licensing, restore the license copied in step 2 by copying the backed up license file into EM->Licensing->General Settings "Add License Keys". Hit "Display Licenses", "Save" and then "Confirm"
- 17) Restore the locale specific media files that were backed up in step 3 (if any).
- 18) Reboot the server



## SNMP Support for AMS

The Avaya Media Server versions included in AACC 6.3 SP11 and AACC 6.4, include the AMS MIB file required for SNMP support.

The MIB file is located at:

Windows:	%MASHOME%\MIB\AVMediaServer-smi2.mib
Linux:	\$MASHOME/MIB/AVMediaServer-smi2.mib

## Configuration issues

None.

## Contact Center Manager Server

### Installation Instructions

Install time patching of the AvayaAura\_CCMS\_ServicePack is mandatory.

Depending upon your hardware configuration, these updates may take up to 20 minutes to install.

### Post Installation Instructions

**Important Note:** If upgrading from a prior release, you must run '**Apply All**' in Server Configuration. (wi01013091 & wi01146080)

1. Start Menu > All Programs > Avaya > Contact Center > Manager Server > Server Configuration
2. Click the 'Apply All' button.
3. On the Prompt to restart your server, Click OK

If after a patch installation, System Control and Monitor Utility (SCMU) is run but it displays an error message saying it cannot connect to System Management and Monitoring Component (SMMC), the SMMC service must be restarted. This can be achieved either by rebooting the machine or stopping and restarting "SMMCSERVICE" through Windows. The same procedure needs to be applied if the SMMC SystemTray displays a white icon (this means no connection) even though SMMC service is running.

### Configuration Issues

None.

### SIP/ACCS Consultation scenarios limitations

In AML system architecture consulting a consult leg is not possible. This design principle was adopted by all CCMS core processing engines and it is still enforced strictly for the purpose of providing backward compatibility. In Aura and ACCS systems, when an agent initiates a consult the moment the original leg is disconnected, the consult leg transforms into an individual call. With the existing architecture CCMS core is not able to handle consultation scenarios for these calls. Reporting subsystem is based on the same AML model. Due to this information on these calls on real-time displays and in historical reports is not fully correct.

The described limitation comes into effect in all scenarios based on the following steps:

- An agent receives/originates a call (either internal or customer).
- The agent consults the call to another number.
- Original call is disconnected by any party.
- The agent consults residual consult call to any number.

### Reporting Limitation during system start-ups

During Contact Center startup there is a small window when call processing is operational but the reporting subsystem is not. During the window contacts processed by the system will be routed correctly but not reported on. This includes contacts entering the system and multimedia contacts re-queued during the window. The issue happens on both standalone and HA setups. Contacts are not reflected in any real-time or historical statistics views. Agents handling these contacts are reported as idle. No workaround is available for the issue.

## Exchanging UII data in AACC

**Note:** When exchanging UII data in AACC the data must be hex encoded before being sent and adhere to the following ASAI format:

- Protocol Descriptor + (Application Identifier + Data length + Data) + encoding suffix
  - Protocol Descriptor can be "00" or "04"
  - Application Identifier for ASAI data is "C8"
  - Application Identifier is followed by data length e.g. "08" in example below
  - Data length is followed by Hex encoded data e.g. "5465737431323334" in example below
- Received data will be "00C8085465737431323334<+UCID if enabled via CM>;encoding=hex"

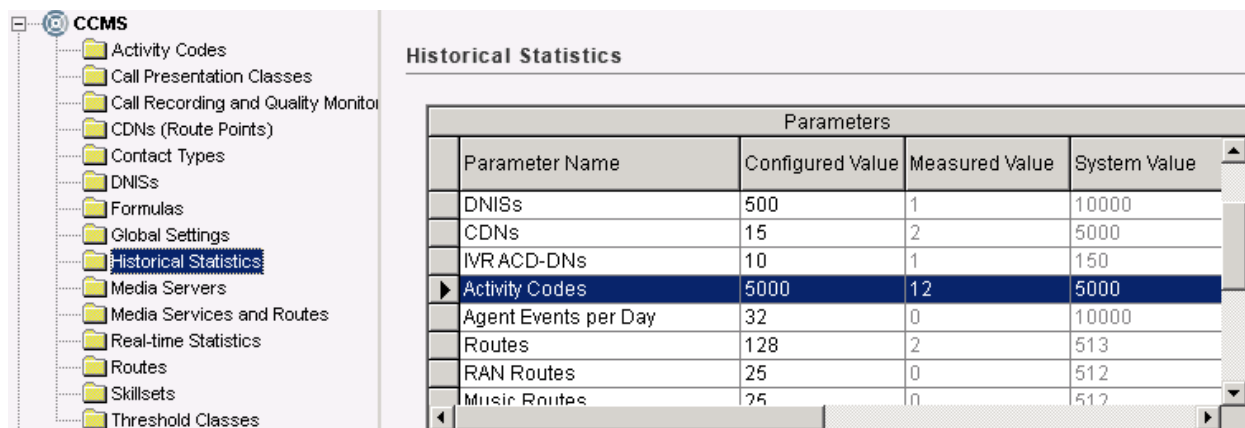
Example: "Test1234" would be encoded as "00C8085465737431323334;encoding=hex"

## Database Maintenance Utility Online help not up to date.

**Note:** The online help in the Database Maintenance Utility is not as up to date as the customer documentation. Please ensure that the customer documentation is used when performing tasks in the Database Maintenance Utility.

## Documented number of Activity Codes supported

**Note:** The existing documentation says that 10,000 Activity Codes are supported in CCMS but the figure is the actual limit displayed in CCMA -> Configuration -> Historical Statistics, as so, which is 5,000:



The screenshot shows the CCMS (Customer Contact Management System) interface. On the left is a navigation tree with various categories like Activity Codes, Call Presentation Classes, etc. The 'Historical Statistics' category is selected. The main area displays a table titled 'Historical Statistics' with a sub-header 'Parameters'. The table has four columns: Parameter Name, Configured Value, Measured Value, and System Value. The 'Activity Codes' row is highlighted, showing a Configured Value of 5000, a Measured Value of 12, and a System Value of 5000.

Parameters			
Parameter Name	Configured Value	Measured Value	System Value
DNISs	500	1	10000
CDNs	15	2	5000
IVR ACD-DNs	10	1	150
Activity Codes	5000	12	5000
Agent Events per Day	32	0	10000
Routes	128	2	513
RAN Routes	25	0	512
Music Routes	25	0	512

## Alternate Call Answer limitations for call transfer scenarios

Alternate Call Answer (ACA) is an AML systems feature that allows an agent to continue receiving CDN calls even if there is a DN call on hold. In order to enable the feature it is required to turn it on both on CS1K and AACC side. On AACC it is configured via CPC field called "Answer by Placing a DN Call on Hold".

The following limitations are applicable for ACA in case of call transfer:

1. Transfer ACA scenarios are not supported by AACC. An agent is not able to receive new CDN calls having a transfer consult call on hold.
2. If Union Break is configured the agent becomes able to receive CDN calls when **both** conditions are met: the Union Break timer after CDN call is expired **AND** transfer call is released. Once the conditions are met the agent becomes able to receive CDN calls immediately.
3. From reporting point of view the agent that has a transfer call leg on hold stays in Break state for a less time than Union Break timer because the Consult state overlays at least some part of Union Break timer.

## License Manager

### Pre-Installation Instructions

None.

### Installation Instructions

None.

### Post Installation Instructions

None.

## Configuration Issues

#### wi00969949 Changing default TOMCAT port to avoid conflicts with third party software

The default HTTP port (8081) of the Tomcat server hosting WebLM can conflict with third party applications. In the case of such conflicts follow these steps to modify the HTTP port used by Tomcat:

- Open the server.xml Tomcat config file located at: D:\Avaya\Contact Center\apache-tomcat\conf\server.xml
- Locate the 'non-SSL HTTP/1.1 Connector' section which defines the connection on port 8081:

```
<!--A "Connector" represents an endpoint by which requests are received
and responses are returned. Documentation at :
Java HTTP Connector: /docs/config/http.html (blocking & non-blocking)
Java AJP Connector: /docs/config/ajp.html
APR (HTTP/AJP) Connector: /docs/apr.html
Define a non-SSL HTTP/1.1 Connector on port 8080
→
<Connector port="8081" protocol="HTTP/1.1" connectionTimeout="20000"
redirectPort="8443"></Connector>
```

- Change the 'port' parameter to a new value eg. 8082

```
<Connector port="8082" protocol="HTTP/1.1" connectionTimeout="20000"
redirectPort="8443"></Connector>
```

- Save the changes to server.xml
- Restart Tomcat
  - o On the Start menu, choose **All Programs > Administrative Tools > Services**.
  - o Right-click the **Contact Center Tomcat Instance** service, and click **Stop**.
  - o Right-click the **Contact Center Tomcat Instance** service, and click **Start**.
  - o Close the services window

## **Server Utility**

### **Pre Installation Instructions**

None.

### **Installation Instructions**

None.

### **Post Installation Instructions**

None.

### **Configuration Issues**

None.

# Contact Center Manager Administration

## Pre Installation Instructions

The Sybase Open Client is only required on the CCMA server if the server is going to be used to manage a pre NES 7.0 CCMS or NCC server.

**NOTE:** The default media services for AACC have been changed in this release. The “ANNC”, “DIALOG” and “AG” services have been removed. The default services now are CONF and XDIALOG.

**NOTE:** It is important that a CCMA backup be taken before the installation begins as this will be required should you need to rollback.

## ActiveX Controls.msi file update

Use the AACC 6.4 SP16 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 located in the \Install Software\CCMA\ActiveX Controls folder within the Service Pack.

## Skillset Naming

AACC uses a naming convention to identify the contact type of skillsets. The convention consists of a two letter prefix followed by an underscore e.g. “EM\_” for email skillsets. Before upgrading from earlier releases of NES or AACC it is important to check that skillset names for voice skillsets on the system will not conflict with this convention as they may be displayed incorrectly after the upgrade. The reserved prefixes are documented in Commissioning guide.

Voice skillsets starting with these reserved prefixes should be renamed prior to upgrading to AACC.

## “Pop to front” No longer supported on Real-time Displays

Prior to SP13, the “Agent Map” and “Billboard” real-time displays provided an option for the display to “pop to front” on a threshold condition. The intent of this feature was that the display window would “pop to the front” of the browser windows that was originally used to launch the display, thus bringing it to the attention of the user.

Due to a change in browser behaviour, the feature now causes the display to appear on top of all open applications on every refresh (i.e. every 5 seconds the display will pop to the front of all open windows). This is considered a serious interruption to the user and the feature has been removed from the product.

## Customer Documentation no longer available from CCMA

### Help menu

As of SP13, the Avaya Aura Contact Center customer documentation links are no longer available from the Help drop down menu in CCMA. The documents are still available to download from [support.avaya.com](http://support.avaya.com).

## Storage of Historical Reporting Statistics Limited to 999

The limit on the number days/weeks/months and Interval (days) for which historical statistics can be stored within AACCC has been reduced to 999 (e.g. "Interval (days)" in the screenshot below). These values are configured within the Configuration – Historical Statistics page of CCMA. An attempt to enter a value greater than 999 will result in an error on the page. Systems upgrading from earlier releases where the limit was higher must now reduce the configured value when changing any value on this page. Once the limit is reduced, data outside the new range will be purged from the statistical database e.g. reducing the value from 9999 to 999 would mean that any records older than 999 days/weeks/months would be deleted.

The data is only deleted from the database once this change is applied. If the older data is still required, the value should not be modified at this time. Customers should also implement a data archival process where the reporting data must be maintained for multiple years.

Duration	
Name	Value
Interval (days)	999
Daily (days)	31
Weekly (weeks)	52
Monthly (months)	36
IVR Voice Port (days)	3
Agent login and logout (days)	3
Length of Business day (hours)	8
Business week contains (days)	5
Call-by-Call (days)	0
Contact Summary (days)	30

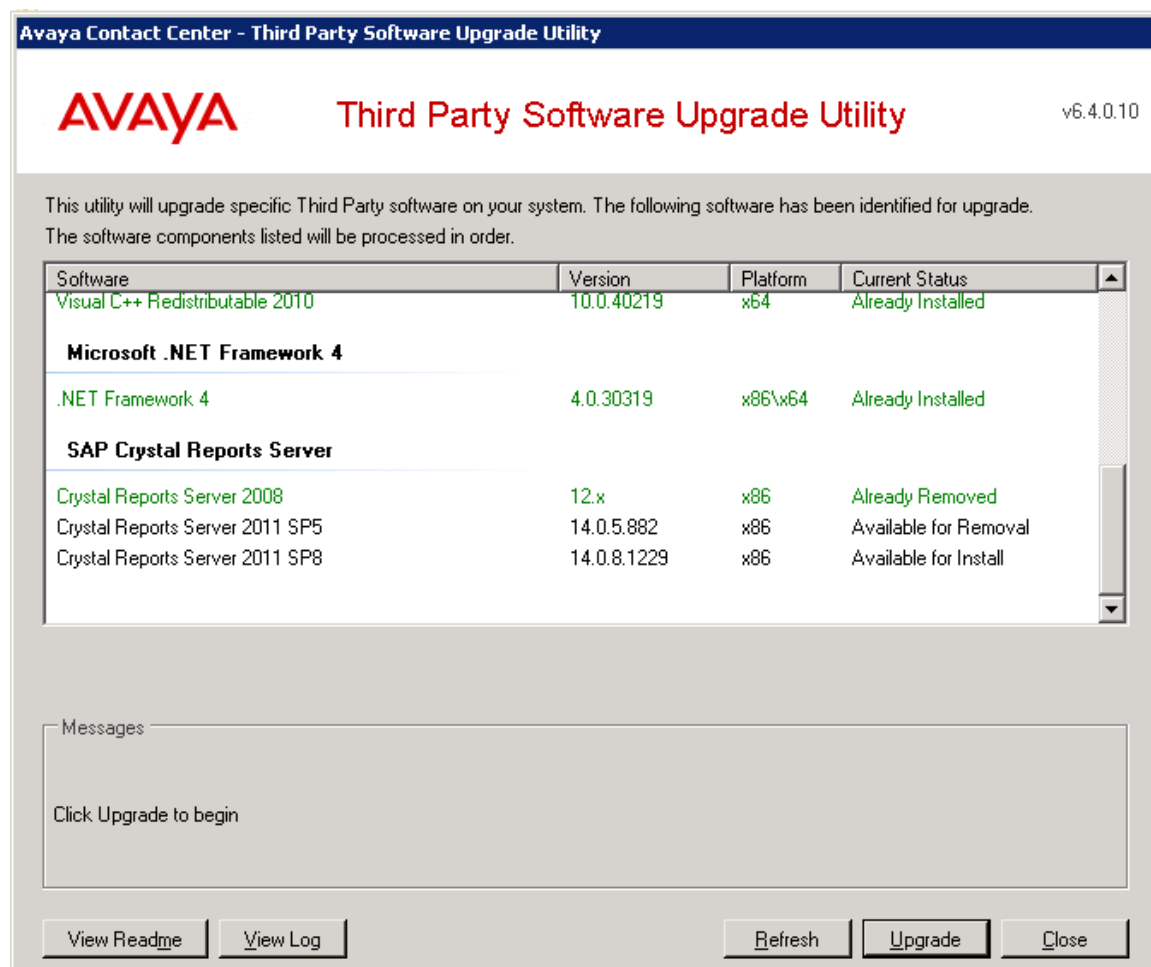
## Installation Instructions

None

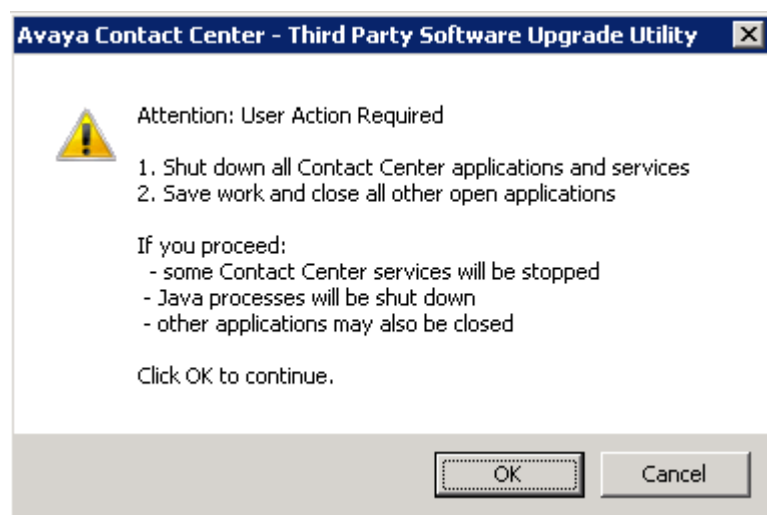
## Post Installation Instructions

### Upgrade Crystal RAS Procedure

- 1 - Make sure there is no Service Pack updates installed on the system.
- 2 - Run the AACCThirdPartySoftwareUpgradeUtility.exe located in the ThirdParty folder of the latest Release Bundle.
- 3 - The utility will run and inform user the list of third-party software will need to be upgraded including Crystal RAS.

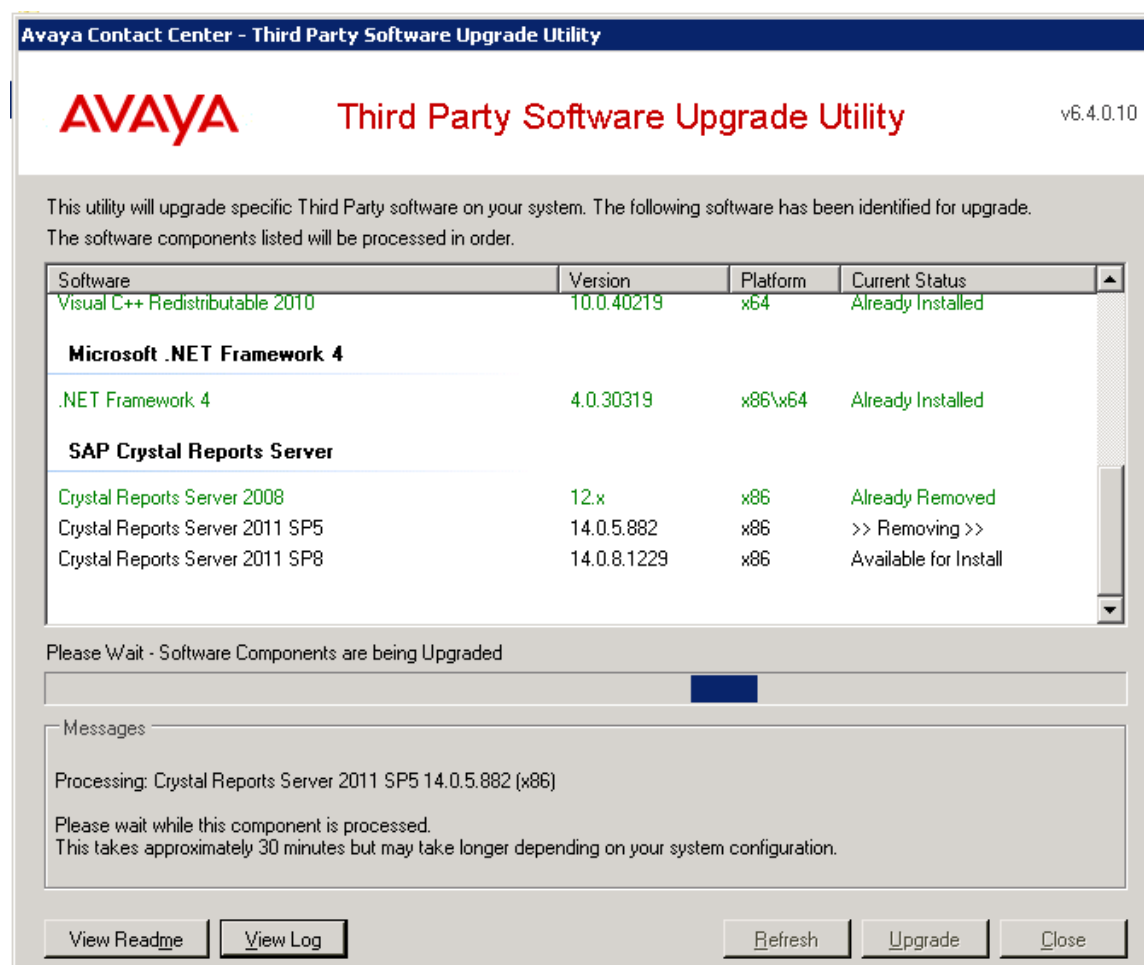


4 - Click on Upgrade button for the utility to upgrade the Crystal RAS software. User is prompted that some Contact Center services will be stopped to proceed:



5 - Click OK to proceed.





6 - Close the dialog after the upgrade completes.

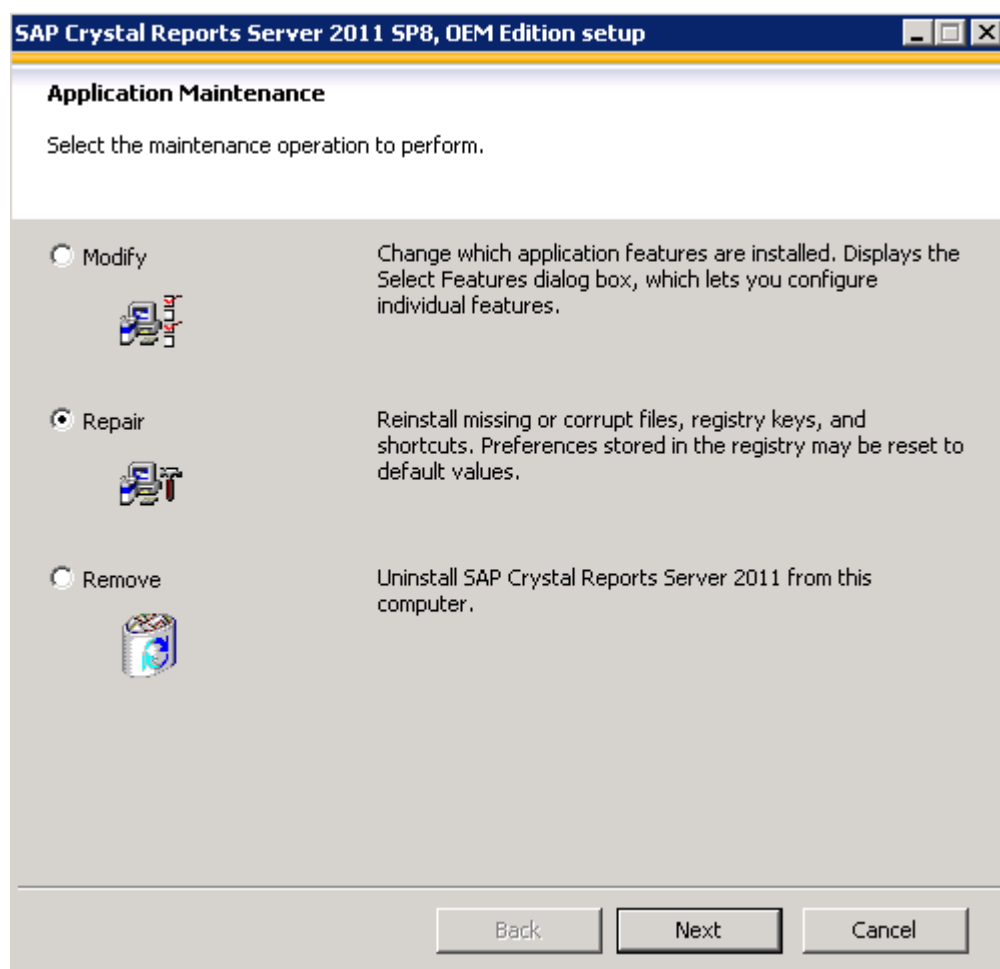
## Crystal Reports fail to run after upgrade to SP16

An intermittent issue exists whereby Crystal Reports may fail to run after an upgrade to SP16. The issue appears when Crystal Reports is removed and then re-installed on the AACC server. The following error may appear when a report is launched within CCMA:



This problem can be resolved by running the following steps:

- Stop the CCMA Reporting Service using "System Control and Monitor Utility"
- Perform an iisreset
- Run the Setup.exe for CrystalRAS2011\_SP8, located in *thirdParty\ThirdPartySoftware\CrystalRAS2011\_SP8* within the Service Pack Release Bundle.
- Choose the "Repair" option.



Once the repair is finished, the CCMA Reporting Service should be restarted.

This process should be carried out on all CCMA servers within the deployment (i.e. Active, Standby and Remote Geographic Node).

## Post Uninstall (Rollback to 6.3) Instructions

The 6.4 release applies several schema changes in the CCMA data store which are not reversed when the software is uninstalled. For this reason, it is required that a CCMA backup be taken prior to upgrading to 6.4. This backup must be restored should a rollback to a pre-6.4 release be required. Note that any CCMA data changes made while the system was on the 6.4 software line-up will be lost when the pre 6.4 data is restored.

## Configuration Issues

### **Custom Historical Reports created with pre 9.0 Crystal Designer may not work correctly:**

Custom historical report templates that were created using a version of Crystal designer prior to 9.0 may not display correctly when run through this release. Certain fields on the reports are no longer supported by the Crystal Reports 2011 runtime. The reports must be updated to replace these fields. Please contact the CCMA team if this issue arises.

# Communication Control Toolkit

## Pre Installation Instructions

### Custom changes to CCT Server “RestrictedSessionAppNames” will not be maintained

Any custom changes to the “RestrictedSessionAppNames” section of the “Nortel.CCT.Service.exe.config” file will not be maintained following an AACC 6.4 upgrade.

To maintain any custom changes please back-up these changes prior to uninstalling the software. Following the Service Pack installation these custom changes must be made again, but this time using the CCT Console as these settings are no longer stored in the Nortel.CCT.Service.exe.config file.

The “RestrictedSessionAppNames” feature limits the maximum number of resources that can be allocated to a particular CCT client application regardless of the configuration settings within CCT.

## Installation Instructions

None.

## Post Installation Instructions

None.

## Configuration Issues

### wi00969949 Changing default TOMCAT port to avoid conflicts with third party software

The default HTTP port (8081) of the Tomcat server hosting CCT WebAdmin can conflict with third party applications. In the case of such conflicts follow these steps to modify the HTTP port used by Tomcat:

- Open the server.xml Tomcat config file located at: D:\Avaya\Contact Center\apache-tomcat\conf\server.xml
- Locate the ‘non-SSL HTTP/1.1 Connector’ section which defines the connection on port 8081:

<!--A “Connector” represents an endpoint by which requests are received and responses are returned. Documentation at :

Java HTTP Connector: /docs/config/http.html (blocking & non-blocking)

Java AJP Connector: /docs/config/ajp.html

APR (HTTP/AJP) Connector: /docs/apr.html

Define a non-SSL HTTP/1.1 Connector on port 8080

→

```
<Connector port="8081" protocol="HTTP/1.1" connectionTimeout="20000"
redirectPort="8443"></Connector>
```

- Change the ‘port’ parameter to a new value e.g. 8082

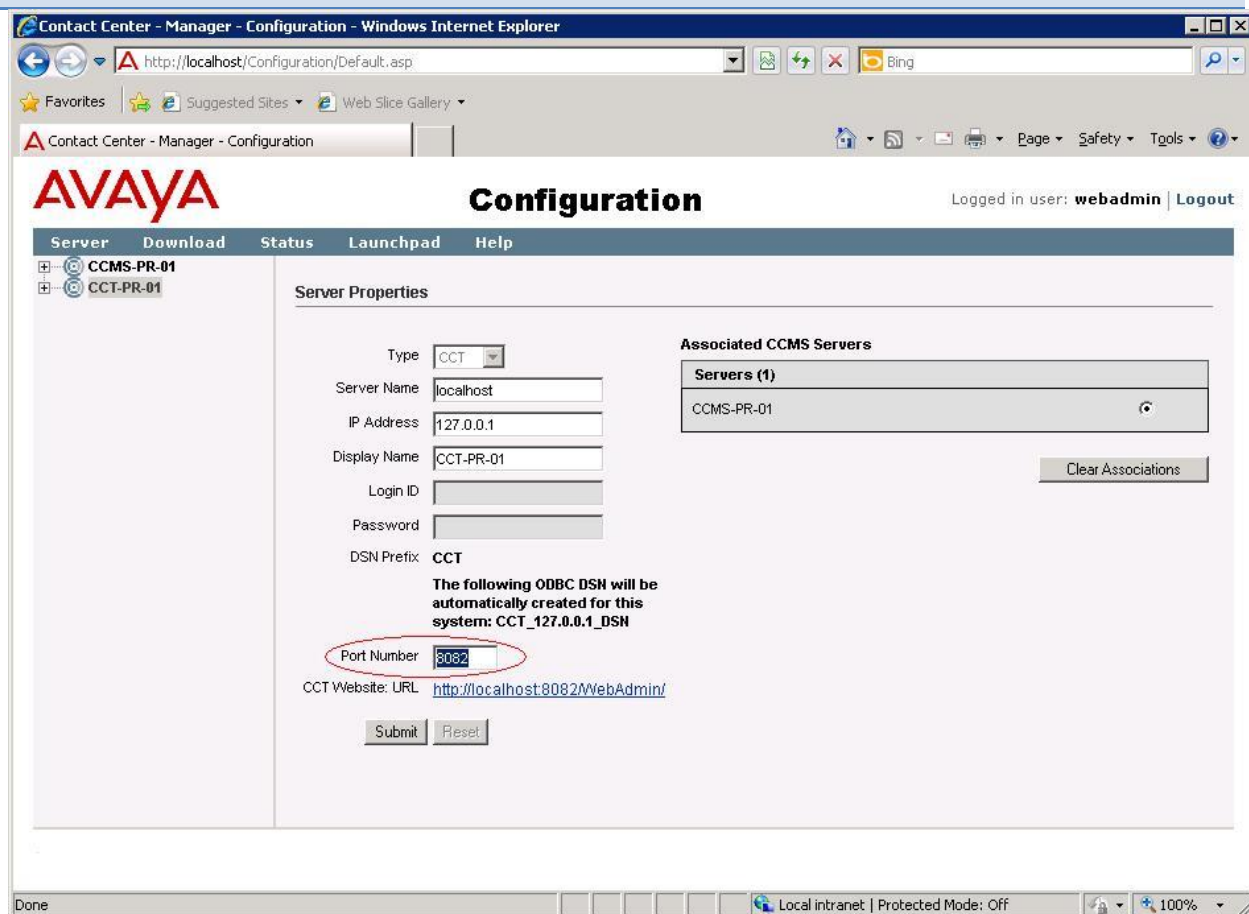
```
<Connector port="8082" protocol="HTTP/1.1" connectionTimeout="20000"
redirectPort="8443"></Connector>
```

- Save the changes to server.xml
- Restart Tomcat
  - o On the Start menu, choose All Programs > Administrative Tools > Services.
  - o Right-click the Contact Center Tomcat Instance service, and click Stop.

- Right-click the Contact Center Tomcat Instance service, and click Start.
- Close the services window

In non-KnowledgeWorker environments, the CCT WebAdmin URL needs to be updated in CCMA once the default HTTP port has been modified in Tomcat. This ensures the CCT WebAdmin can be successfully launched from CCMA.

- Open CCMA and navigate to the Configuration page
- Highlight the CCT server in question on the left hand tree view
- Select Server->Edit Properties (or alternatively right-click the selected CCT server and select Edit Properties)
- Update the port number entry to match the port number configured in the Tomcat WebAdmin, e.g. 8082 from the example above
- Click the Submit button



### CCT web service Session Timeout value impacts memory consumption

Large session timeout will increase the period before a session is destroyed automatically after session timer expires. Each session consumes a small amount of memory, a high rate of session creation with long session timeouts can negatively impact memory consumption resulting in a slowdown and potentially out of memory exceptions. To avoid these problems reduce the value of the CCT WS Session Timeout value.

- If using Avaya Contact Recording (ACR) / Workforce Optimization (WFO) with or without CCT SOA Open Interfaces clients, the default timeout value can be increased only if site deployment conditions require it and to the lowest possible value to maintain the session during idle periods. Increasing this value impacts memory consumption which will need to be monitored.

- If using the CCT SOA Open Interfaces interface only, then the session timeout value should be set to the default value of 120min or less.

**Background Information:**

Refer to the SDK documentation for these interfaces which contain rules/requirements that must be implemented by client's that use the interface, Third-party developers must be familiar with, and comply with SDK documentation in order to prevent failure in the contact centre environments.

---

## **Contact Center Web Stats**

### **Pre Installation Instructions**

None.

### **Installation Instructions**

None.

### **Post Installation Instructions**

None.

## **Configuration Issues**

None.

# Contact Center Multimedia

## Pre Installation Instructions

Ensure that you have accurately completed the Section 'Installing operating system components for Contact Center Manager Administration' from the Avaya Aura® Contact Center Installation document 44400-311. Failure to correctly install the required Operating System roles before installing the Contact Center Software will result in a failed installation.

### Wi01029680 AACC 6.2 SP6 – Default welcome message overwritten during SP uninstall

The Default Welcome Message for webchat is overwritten by the default Avaya message after a SP install. The message is updated by the base install after one SP is removed and before next SP is installed.

Note: this issue does not occur for Welcome Messages configured per skillset. Issue is specific to the Default Welcome Message when no Welcome Message is configured for a skillset.

Workaround: After the SP install update the default welcome message to the desired text.

## Installation Instructions

Install time patching of the AvayaAura\_CCMM\_\_ServicePack is mandatory.

## Avaya Aura Agent Desktop

**Note:** AAAD web page can state that "This machine has the correct version of the .NET Framework 3.5 installed." When it is not installed as on an Agent Desktop PC if the Microsoft .NET 3.5 framework is installed and then uninstalled from the PC the Microsoft Internet Explorer browser sometimes does not pick up on the uninstall and sends the incorrect information to the CCMM Server. This does not affect install or launch functionality of the web page.

**Note:** In AACC 6.4, AAAD has migrated to using .NET framework 4.0. This means desktops running AAAD will need to be updated to .NET framework 4.0 before the 6.4 version of AAAD can operate. The updated pre-reqs must be installed prior to launching the AACC 6.4 version of AAAD. This can be achieved by pressing the "Install prerequisites" option on the AAAD launch page or by installing the pre-requisites manually.

Once an SP/DP is installed on the server with a new version of the AAAD, the next time an Agent launches the AAAD the new software is pushed out to them i.e. automatically installed on their PC. If you subsequently uninstall the SP/DP on the CCMM/CCT server and revert back to the earlier version of software, you must uninstall the later version from the client PCs manually. This is because the AAAD will not run against a CCMM/CCT server where an earlier version is installed.

## Post Installation Instructions

### AAAD Minimum Version check

Avaya Aura Agent Desktop (AAAD) implements a minimum version requirement which ensures that the latest version is automatically downloaded onto Agent PCs, via ClickOnce deployment, the next time it is launched after CCMM/CCT with a new version of the AAAD is upgraded.

NB: If a site rolls back to an earlier version of CCMM (such as removing a DP, for example), this feature will require Agents to manually remove Avaya Aura Agent Desktop (AAAD) from their PCs using the Windows Control Panel "Programs and Features" tool.



## RGN patching

On an RGN configuration the Secondary CCMM has a dependency on the Campus Primary LM being up. After the patch install, the CCMM services may not come up and may become disabled. If this happens, make sure that the license manager is started and then the CCMM services will recover.

## AAAD robustness feature in an AVAYA Aura Offsite Agent configuration

AAAD has introduced a new robustness feature in an Offsite Agent configuration whereby if an Offsite Agent logs out of AAAD but fails to shutdown the application, the application will begin a self shutdown if the following criteria are met

1. The agent has been logged out for the defined period and
2. No calls have been active for the defined period and
3. The agent has not cancelled a previous shutdown request for the defined period:

This feature is enabled by default. The ability to enable/disable this robustness feature is contained within the “InactivityShutdown” value with the “CCADUserSettings.xml” file. A value of “true” enables the feature, while a value of “false” disables the feature. Please note AAAD must be restarted once these changes are made to take effect.

## Configuration Issues

### AAAD HA SSL Environment

In a HA environment where SSL is configured, the CCMM backup server should be configured EXACTLY matching the value for the “Issued To:” from your CCMM cert. This step should be performed using the CCMM admin tool. After making this change, the administrator should check the CCADAppSettings.XML <CCMMBackupServer> tag contains the correct value.

### AAAD embedded Softphone in “My Computer” mode Guidelines

When the embedded phone in AAAD is operational in my-computer mode ( in Elite adjunct mode of operation or AAAD operating in SIP on Aura platform mode), the following guidelines apply:

- 1) On a certain machine with multiple core/processor, AAAD may exhibit heavy jitter while playing the voice of other end. This may happen due to a known issue on certain machines where the hardware abstraction layer is not able to provide correct value for the high performance counters. This can be resolved by using the steps mentioned in the KB at:  
<http://support.microsoft.com/kb/895980>  
 Note: This is Windows wide setting and one should undo the change if it does not resolve the problem.
- 2) Intermittent one-way talk path has been observed on the Windows 7 machine where the AAAD user could not hear the remote party. In such scenario, it is mandatory to have the Service Pack1 of Windows 7 to be installed due to a known issue on Windows 7.

### AAAD operation in Citrix environment

When AAAD is operating in a Citrix environment, CCAD.exe should be excluded from the Memory Optimization Management Program. Major stability issues for AAAD in a Citrix Environment have been seen to stop happening when this step is performed.

### Logging into Aura Presence Services in AAAD 6.4

Higher domain-based security is mandated for the XMPP protocol in core .Net and third-party libraries as a result of the upgrade to .Net 4.0 in AAAD 6.4. This means that an Agent logging into Aura Presence Services (APS) using AAAD 6.4 must specify a resolvable server name in the Presence tab i.e. use of the APS server's IP address is not supported.

---

**CCMM cannot authenticate to any mailbox from a provider that requires DH parameters of larger than 1024 bits**

---

AACC does not support email providers that require DH parameters of larger than 1024 bits. This issue is caused by an incompatibility with Java 6u37 which AACC 6.4 uses.

**Solution**

Upgrade to AACC 7.x which uses Java 1.8

## Orchestration Designer

### Pre Installation Instructions

None.

### Installation Instructions

None.

### Post Installation Instructions

None.

## Configuration Issues

---

#### **wi01100902 Issue launching Orchestration Designer**

It has been reported that on some deployments of the orchestration designer that the download and installation of the orchestration designer application from the CCMA web interface is not successful. This issue occurs when there is a corruption in the registry entry for the component on the system.

The symptoms visible to the user are:

- They are asked to continually download and install the orchestration designer component when they click on the Launch Orchestration Designer link in CCMA

A **work-around** for the problem has been identified for the problem:

- 1) In the CCMA web interface
  - 2) Go to the Scripting Section
  - 3) On the top, click on Orchestration Designer – Launch Orchestration Designer
    - You will receive an information message indicating that you need to download the component installation.
    - Click OK on the dialog box
  - 4) Following the instruction in the browser, download and run the executable
  - 5) Perform the installation following the instructions provided.
  - 6) After the installation completes you go to the Star Menu – All Programs – Avaya – Contact Center – Orchestration Designer
  - 7) Click on Orchestration Designer application shortcut.
  - 8) This will launch the Orchestration Designer application.
- 

---

#### **Backward compatibility concerns arising from AMS Zoning feature in AACC 6.4**

AMS Zoning introduces a new flow called Media\_Server\_Selection. To facilitate this new flow, a new flow type has been introduced and a new Media Server block has been introduced.

If reverting back to AACC 6.3 from AACC 6.4, delete Local Views of the AACC 6.4 server as these views will still be present in the AACC 6.3 OD local views however they will not be loadable as they contain the above elements that are not available or compatible with

---

---

**wi01171201 Time stamp in CCMA audit trail versus OD one hour different.**

---

OD timestamps are 1 hour ahead when compared to CCMA server time and Audit Trail timestamps. Database timestamps in ccms.NITaskFlow table are consistent with the OD timestamps.

Root cause of this problem is that jdk 1.5.0\_22 does not have proper timezone updates.

**Workaround:**

A workaround for this issue is to manually update the Java timezone information using the Oracle provided TimeZone Updater Tool for updating jdk. This tool is also known as TZUpdater

**Instructions**

The Oracle update should be applied to all AACC servers. The following are the instructions to install this update.

Stop any running instances of the JDK/JRE software to be operated upon before you run the TZUpdater tool on that installed JDK/JRE software image.

From the Oracle support site, locate and download the appropriate tzupdater tool for the installed version of JRE/JDK

If "C:\Program Files (x86)\Java\jre6\bin" directory exists on the server

- Launch Command Prompt
- CD to "C:\Program Files (x86)\Java\jre6\bin" directory
- Copy the tzupdater.jar you downloaded from the Oracle website into this directory
- Run the following "java -jar tzupdater.jar -u -bc"

If "C:\Program Files\Java\jre6\bin" directory exists on the server

- Launch Command Prompt
- CD to "C:\Program Files\Java\jre6\bin" directory
- Copy the tzupdater.jar you downloaded from the Oracle website into this directory
- Run the following "java -jar tzupdater.jar -u -bc"

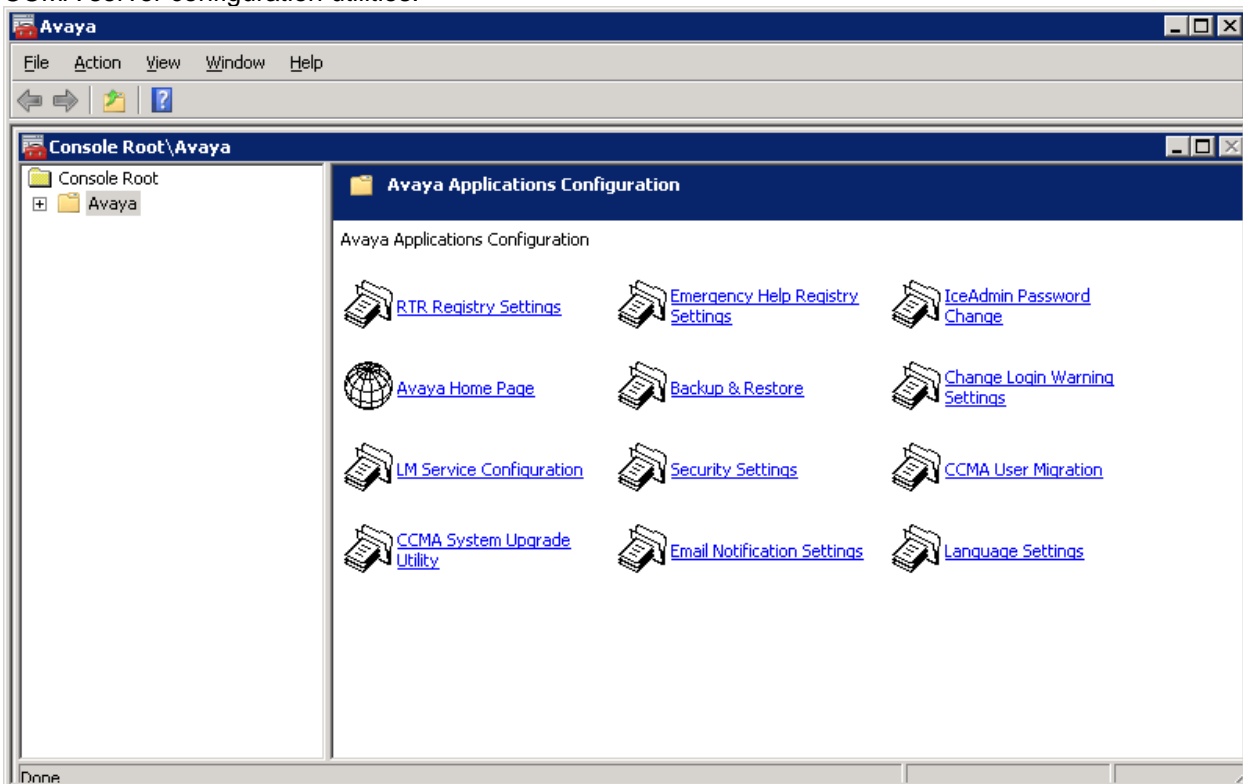
## Security Framework

See section “Feature Specific: High Availability” for information on Security Framework in High Availability environments.

New installations of security framework are not supported as of AACC 6.4 release. It is now recommended that CCMA be configured to use System Manager as the security server. Existing installations can continue to use the current deployment. The Security Framework installation is no longer available on the AACC 6.4 DVD.

**Note 1:** ACCCM cannot be used to configure AACC Agents or Skillsets if Security Framework is enabled for CCMA. To use ACCCM, Security Framework must be disabled for CCMA.

**Note 2:** If the enhanced security is enabled for CCMA prior to an upgrade to SP16, it should be disabled and re-enabled once the upgrade is complete using the Security Settings MMC snapin which is part of the CCMA server configuration utilities.



## Pre Installation Instructions

**Warning:** If upgrading from AACC 6.0 or AACC 6.1 you must have the latest Security Framework patch DP\_SFW\_6.1.203.0 installed before you start that upgrade.

Verify that the security framework services are running prior to commencing an upgrade. If the Jboss service is not running the backup will fail and all security framework data will be overwritten at the end of the install.

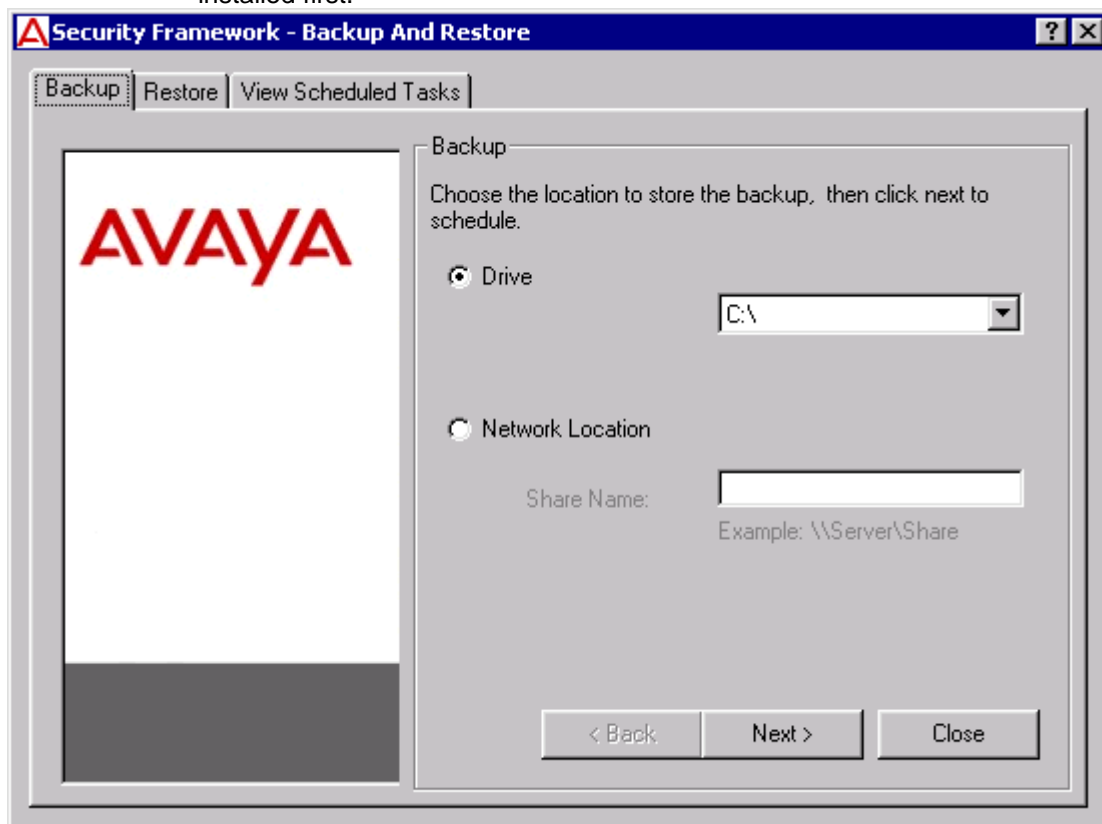
### Upgrading from AACC 6.0 or AACC 6.1

To upgrade security framework run **setup.exe** from the \Install Software\Security Framework\ folder from the patch bundle. DO NOT attempt to install the security framework by running the ContactCenterSecurityFramework.msi as this will overwrite the configured data.

**Warning:** do not run **setup.exe** if Security Framework with AACC 6.3 is installed.

Before commencing a security framework upgrade,

1. Take a backup using the “Security Framework Backup & Restore” utility rather than the CCMA backup and restore tool.
2. Make sure that you have latest Contact Center Common Components (CCCC) line-up installed first.



### **Warning**

If a “File In Use” dialog is displayed during the upgrade select the “Do not close applications. (A reboot will be required)” radio button and continue with the installation.



If you do not select this option the security framework will be installed but your configured data will be lost.

Note: When you launch the CCMA Configuration MMC console after a SFW upgrade (co-res only) a dialog window appears saying to “Please wait until Windows configures Avaya Security Framework”. When this completes the Configuration console window will be displayed.

**NOTE:**

If the Security Framework backup may fail with a message stating “Errors found during backup. Error details are stored in d:\Avaya\Logs\SFW\SFWBackupRestore.log”. This is a known issue. To workaround this issue do the following:

1. Launch Regedit
2. Backup the existing registry configuration before making any changes to the machine.
3. Locate the following entry
  - a. HKLM\SOFTWARE\Wow6432Node\JavaSoft\Pers\com\avaya\cnd
  - b. Change the is/Running key from “true” to “false”
4. Restart the Security Framework
5. Run the backup.

## Installation Instructions

None.

## Post Installation Instructions

None.

## Configuration Issues

None

## Feature Specific: CCT Open Interfaces Web Services

### Constraints on Agent Count and Contact Rate per Hour

The CCT SOA Open Interface SDK provides a mechanism for CTI using SOAP/XML based Web Services.

There are differences in the underlying architecture between the CCT OI and the alternative AACC .Net CTI SDK which lead to limits on:

1. The supported number of concurrent logged in agents
2. The contact-rate (measured in contacts per hour) that the CCT OI SDK can support.

The limits are given below for (i) SIP-based and (ii) CS1K-based AACC deployments.

#### SIP-Based

- Maximum count of logged in Agents: 1000
- Maximum contact rate: 10,000 contacts per hour

#### CS1K-Based

- Maximum count of logged in Agents: 1500
- Maximum contact rate: 15,000 contacts per hour

Where a CTI application interacting with the AACC is being developed with requirements that exceed either, (1) the supported agent count or (2) the contact rate, then the CCT OI SDK is not a suitable choice.

This is also true if the requirements come within a minimum of 20% of these limits and the CTI application is expected to scale up to greater numbers in the near future.

In either of the cases above, it is recommended that the CTI application should be designed to use the CCT.Net SDK which supports the full AACC capacity for agents and contact rate per hour.



## Feature Specific: High Availability

### Pre-Installation Instructions

Full instructions on the setup of AD-LDS replication at the install time of CCMA is included in the Commissioning guide. However, users should also be aware that prior to setting up AD-LDS replication, both the active and standby AACC servers should be joined to the Windows domain.

### Installation Instructions

When using the Mission Critical HA feature, and in order for the Avaya Aura Agent Desktop application to be able to continue to exercise call control over the Communication Manager telset endpoints following either an AACC switchover or an AES switchover, the latest GA patch lineup of AES 6.1.1 is required. This was released by AES in June 2011.

The version of Session Manager used should be at least SM 6.1 SP4. This is because the SM 6.1 SP4 baseline, and associated changes in System Manager, contains changes that enable the SM to react correctly to an AACC switchover. Within System Manager, under Routing -> Entity Links, the Connection Policy selected for the SM's link to the AACC HA pair should be "Trusted HA". If an earlier version of SM is used, then following an AACC switchover, it will take SM approximately 60 seconds to clean up its half-open TCP sockets and begin using the new active AACC. An alternative to upgrading the SM is to disable the firewall on AACC, which may be acceptable for certain limited deployments.

### Post Installation Instructions

Please refer to Mandatory Microsoft Updates section of Release Notes for mandatory Microsoft patches required to avoid an SMMC crash vulnerability.

### NCC Re-Sync

This note applies to customers using the "mission critical" campus HA feature at the same time as the networking feature. For example, a number of contact center sites, each with "mission critical" campus HA, and participating in a networking environment configured by the NCC. In such a scenario, the NCC automatically re-syncs with the newly active AACC following a campus HA switchover at one of the sites. Please note if there are several AACCs on the NCC, it can take up to 30 minutes for the automatic re-sync to complete.

### Outage of Avaya Aura Session Manager

The Session Manager (SM) uses "record-route" and from a SIP protocol perspective acts as a stateful proxy for all incoming and outgoing sessions with AACC. The second SM (SM-2) is available for service continuity, but it does not maintain real time call state information with the primary SM. This means that, following loss of the primary SM, the signaling path for all existing SIP Sessions to/from AACC is broken. This should not have an immediate impact on calls due to the fact that media streaming continues between AMS and the agent/customer User Agents (Uas).

Problems arise however when further signaling is attempted for the calls that were in progress at the time of the SM outage. For example, a BYE (disconnect) sent by either customer or agent will not be propagated because there is no knowledge of this SIP dialog in SM-2. The agent and customer will have to separately disconnect to clear their sessions. Furthermore, any Re-INVITEs associated with existing sessions cannot be processed by SM-2 because it has no knowledge of the setup of these sessions, and, in accordance with RFC 3261 section 14.1, this will cause the session to be terminated. An example of when Re-INVITEs are used is to modify the media/SDP when participants are put on hold, or if RFC 4028 is in use.

In SM 6.2, a Call Preservation feature has been introduced. This allows SM peer SIP elements (for example M3K gateway, CM, VP/ACC) to send back responses and in-dialog requests to an alternate SM when the primary SM fails in middle of a dialog. AACC 6.4 has no corresponding feature to take advantage of this functionality.

## HA Interoperation & Avaya Contact Recording (ACR)

The ACR application uses polling to ensure that the AACC from which it is receiving events is in operational state. The rate of polling is set in an ACR property file setting called “cct.pollinterval” with a default setting of 30 sec. The ACR performs a new login to AACC/CCT if a poll fails. Due to the rapid nature of the switchover of an AACC Mission Critical HA pair, it is possible for an AACC switchover to complete without the ACR being aware. Using a lower ACR poll interval reduces the likelihood of an issue being seen.

If the ACR is unaware that an AACC switchover has occurred, the ACR does not re-establish its listeners and web services session after the AACC switchover, meaning that ACR may cease to record calls. To resolve this problem, restart the ACR application, which takes approximately 10-15 seconds. Go to the Windows Service Control Manager, select the “Avaya Contact Recorder” service and select “Restart”. Call recording should recommence immediately.

## Not-Yet Established Calls – Alerting/Ringing Scenario

The Mission Critical HA feature is designed to maintain calls that are in progress at the time of an outage of the active AACC server. Once the agent and customer are speaking, such stable calls are maintained following an AACC outage, and the call can be ended normally when the conversation is complete.

There is a short timeframe when a call is ringing at the agent position, before the call is stable, which is an ‘edge case’ requiring special handling in AACC. Because this is not a stable call, the standby does not have the necessary information to effect a normal answer following a switchover. If an AACC switchover occurs while a call is alerting on AAAD, then after the switchover the customer remains in the treatment (e.g. ringing). The agent will answer AAAD and hear silence. When the agent disconnects the customer call is taken out of treatment, presented to the agent, and can be answered normally.

This scenario only applies for calls that happen to be in the alerting/ringing state at the time of an active AACC outage. The vast majority of calls will not be in this state, because they will be either connected to an agent, or in-queue (in-treatment), and the above does not apply.

## CCMA AD-LDS configuration issues / Trouble shooting

### Choosing Managed IP addresses

For both AML HA (Campus HA) and Mission Critical HA (Campus HA) the Managed IP must be in the same network subnet IP address range as Active and Standby IP Addresses. It can be lower or higher than the physical IP Addresses of Active and Standby servers.

Example 1:

|          |           |
|----------|-----------|
| Active:  | 10.0.0.20 |
| Standby: | 10.0.0.30 |
| Managed: | 10.0.0.10 |

Example 2:

|          |           |
|----------|-----------|
| Active:  | 10.0.0.20 |
| Standby: | 10.0.0.30 |
| Managed: | 10.0.0.50 |

## Verify that AD-LDS replication is operational

The following outline steps to verify that CCMA replication is functioning as expected:

Ensure both servers, primary and secondary are configured and installed as detailed in the Avaya installation guides.

Login to the Primary CCMA server as the default “webadmin” account.

Choose “Access & Partition Management” from the main Launchpad

Choose “Add”, “New Access”, specify a name and save details.

**Note:** This information will now be saved in the local AD-LDS instance and also replicated to the Secondary AD-LDS instance.

Login to the secondary CCMA server as the default “webadmin” account.

Choose “Access & Partition Management” from the Launchpad and click on Access Classes.

A list of access classes should appear on the left hand side tree menu. The access class created on the primary CCMA should be listed.

Repeat this test by creating a new access class on the standby server and check that it is replicated to the primary CCMA.

## CCMA AD-LDS replication issues – Delays between replication servers OR replication occurring in one direction only.

If delays occur between replication servers, the following errors may be logged to the AD-LDS instance event viewer and also displayed when running the following diagnostic test on a replicating CCMA server.

**Diagnostic Test Example:** (Note this should be done on primary and secondary servers)

```
C:\Windows\ADAM>repadmin /replsummary CCMA Server2.Test.Avaya.com:389
```

```
Replication Summary Start Time: 2011-07-06 05:13:26
```

Beginning data collection for replication summary, this may take a while:

....

```
Source DSA          largest delta  fails/total %%  error
CCMA Server1$SymposiumWC 41d.03h:54m:48s  3 /  3 100 (2148074274) The target principal name
is incorrect.
```

```
Destination DSA      largest delta  fails/total %%  error
CCMA Server2$SymposiumWC 41d.03h:54m:48s  3 /  3 100 (2148074274) The target principal name
is incorrect.
```

Event viewer Log Example: AD-LDS log, Warning message.

Access is denied.

00002098: SecErr: DSID-03150BB9, problem 4003 (INSUFF\_ACCESS\_RIGHTS)

myDomain\CCMAReplication

**Message Details:** The directory server has failed to update the AD LDS serviceConnectionPoint object in Active Directory Lightweight Directory Services. This operation will be retried. Additional Data SCP object DN: CN={7387157e-92fe-466a-99c6-

04cf7d63bc8a},CN=CCMA Server1,OU=Servers,OU=Test,DC=test,DC=orte,DC=com Error value: 5

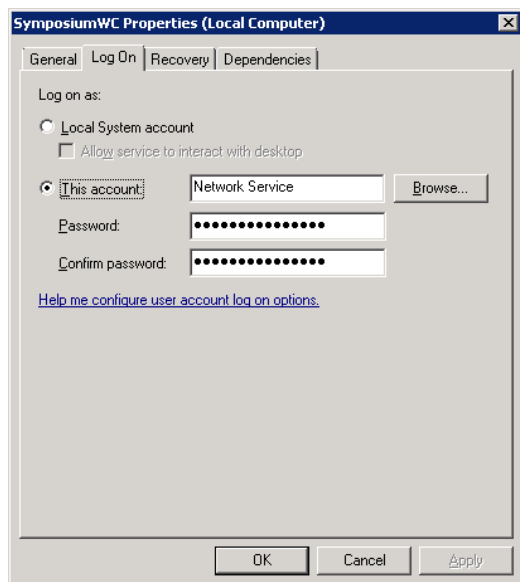
Access is denied. Server error: 00002098: SecErr: DSID-03150BB9, problem 4003

(INSUFF\_ACCESS\_RIGHTS), data 0 Internal ID: 3390390 AD LDS service account:

myDomain\CCMAReplication User Action If AD LDS is running under a local service account, it will be unable to update the data in Active Directory Lightweight Directory Services. Consider changing the AD

LDS service account to either NetworkService or a domain account. If AD LDS is running under a domain user account, make sure this account has sufficient rights to update the serviceConnectionPoint object. ServiceConnectionPoint object publication can be disabled for this instance by setting msDS-DisableForInstances attribute on the SCP publication configuration object.

**Resolution:** If these errors are logged, modify the AD-LDS instance on the Primary server to also run under the default “Network Service” account. This can be done from Start -> Administrative Tools -> Services.



**Note:**

It will be necessary to restart the SymposiumWC in order to make this change. During this time CCMA will be unavailable.

The password field can be left blank when re-setting to Network Service account.

## Configuration Issues

For customers using the Disaster Recovery site, it is recommended that after a period of operation of the RGN (Remote Geographic Node) that a backup and restore be used as part of bringing the campus HA pair on the primary site back online. On a campus HA pair, following a switchover a backup and restore is required before bringing the originally active back online.

## Feature Specific: AACC Call Networking in a SIP Environment

### Mandatory Home Location Code Configuration

The AACC Call Ids that is used by AACC components is made up of a Home Location Code (HLOC) and a local Call ID. The HLOCs must be unique on each node in a AACC SIP network.

To ensure this it is necessary to configure each node with a unique HLOC. Each node reserves HLOC to HLOC+9 for its own local use. For example if a node has a HLOC of 570 then this particular node may create call ids with a HLOC of 570 to 579. Therefore it is recommended that each nodes HLOC is configured with an increment of 10. e.g.

1. Node 1 = 570 (decimal) = HLOC1
2. Node 2 = 580 = HLOC1+10
3. Node 3 = 590 = HLOC1+20

To change the HLOC open Regedit to find and modify accordingly the following registry entry:

Registry Location:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\CCMS\_SIP\_Service\Parameters\JVMOptio  
ns\

Entry:

Dcom.nortel.contactcenter.sgm.HLOC (Default Value: 570)

The changed HLOC will take effect after AACC is restarted.

The minimum HLOC value is 10 and the maximum value is 65525.

In a HA environment it is necessary to perform the above configuration in both the active and the standby AACC server ensuring the HLOC is the same on both.

## Feature Specific: E164 support

If the E164 dialing plan is configured to allow customer to dial a 15 digits CDN number (for example CDN number is 9123459 but configured in 15 digits format 353123459123459 by prefixing 35312345) then the CDN number in CCMA->Configuration->CDNs (Route Points) and in Orchestration Designer Script also should be configured with the same 15 digits format,

Otherwise the CDN call is treated as DN call when agent receives the CDN call from customer who dials 15 digits E164 format.

## To enable E164 support within SGM for CS 1000

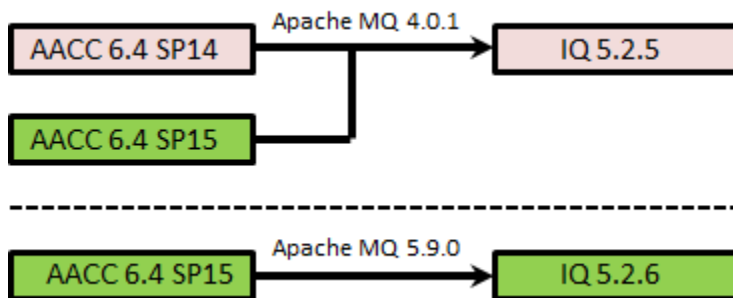
To enable E164 support within SGM for CS 1000, a configuration file on the AACC machine must be updated. This change only affects the behavior of this machine. All machines in a HA environment must be updated individually.

To update the configuration file:

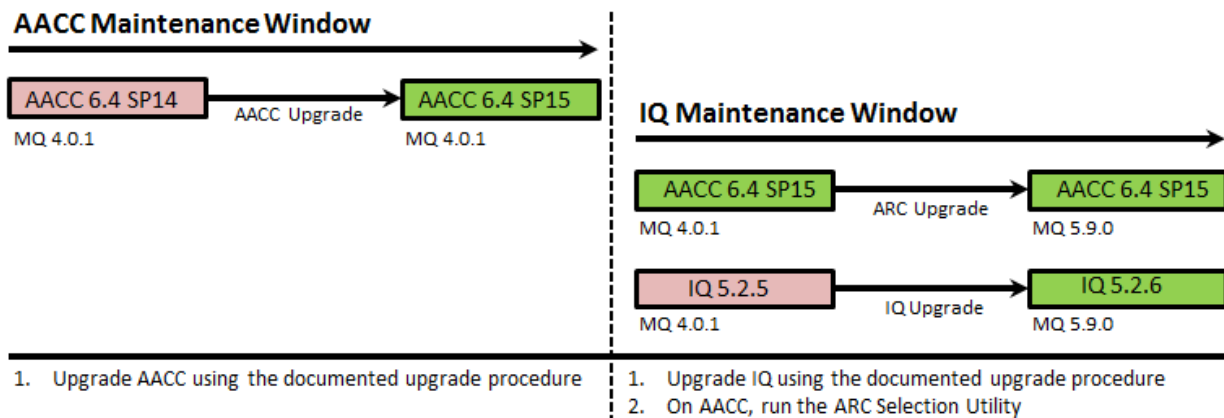
1. Stop AACC
2. Navigate to "D:\Avaya\Contact Center\Manager Server\licm\sgm\config\"
3. Backup the "SGM.properties" file
4. Edit the "SGM.properties" file
5. Add the following `com.nortel.ccms.sip.MaintainE164CharsForCS1K=true`
6. Save the "SGM.properties" file
7. Start AACC.

## Feature Specific: Working with Avaya IQ 5.2.6

AACC 6.4 SP16 will work with Avaya IQ 5.2.5 and IQ 5.2.6. However, a custom action (called ARC upgrade) must be completed on AACC 6.4 SP16 to allow successful interworking with IQ 5.2.6. No action is needed if AACC 6.4 SP16 is connected to IQ 5.2.5.



The process for upgrading to AACC 6.4 SP16 and Avaya IQ 5.2.6 involves an AACC maintenance window to upgrade to AACC 6.4 SP16 and an IQ maintenance window to upgrade to IQ 5.2.6.



The ARC upgrade process is facilitated by a new utility called ArcSelectionUtility (ASU) which is part of the AACC 6.4 SP16 software. ARC upgrade is performed during the IQ maintenance window.

1. Using File Explorer, navigate to `D:\Avaya\Contact Center\Manager Server\ArcSelectionUtility`. Launch `ArcSelectionUtility`.
2. The action button will identify the action (upgrade or downgrade) that is possible based on the configuration that is currently in effect. After upgrading to AACC 6.4 SP16, the expected action is Upgrade.
3. The ASU password must be entered before the action can be executed. Contact Avaya support for the password. Enter the password.
4. Click the button to perform the action. The action will be performed. Progress is reported in the message area of ASU.
5. When complete, exit ASU using the Exit button.

## **Feature Specific: Only TLS 1.0 is supported with AACC 6.4**

TLS 1.0 is the only supported version of TLS with AACC 6.4



## SDK Changes

### CCT SDK changes

The 6.4 FP2 release of the Communication Control Toolkit (CCT) introduces support for the Avaya Contact Center Select (ACCS) product.

Below is a brief list of the new features found in the Release 6.4 FP2 version of the CCT SDK:

- For a CS1K AML CCT client application the size of the destination address parameter for a number of API calls has been limited to 30 digits.  
This change does not apply to SIP based CCT client applications.  
Should a CCT client application attempt to call the affected CCT API with a destination address greater than 30 digits an `InvalidPartyException` will be thrown.
- New APIs have been added that provide support for the ability to observe or barge-in on non-skillset contacts. Previously these functions were restricted to contacts that arrived at the Contact Center via skillset queues. The ability to observe and/or barge-in on non-skillset contacts is controlled through permissions granted to individual agent supervisors. To make it easier for client applications to determine when it is possible to observe or barge-in on a contact, new **CanObserveFrom** and **CanBargeInFrom** methods have been added to the **IContactCapabilities** interface. The new methods take into account the class of the contact (skillset vs non-skillset), the permissions assigned to the supervisor associated with the specified terminal, and the logged-in status of the supervisor.  
**Note: The observe and barge-in operations now require the supervisor to be logged in to the Contact Center for them to succeed. This applies to skillset and non-skillset calls and is enforced to ensure that reporting of the observe and/or barge-in features is correct.**
- Associated with this change is a new **IsMonitored** property that indicates if there are any supervisors currently observing or barged-in on the contact. The intent of this new property is to provide a visual indication to agents that the conversation is being monitored in some way by one or more supervisors.

More detailed information regarding changes in the Communication Control Toolkit for this release can be found in the CCT SDK Programmer's Reference Guide included with the SDK.

### CCMA Open Interface SDK changes

The 6.4 FP2 release of the CCMA Open Interface SDK introduces the following changes to the API's and Data Structures:

- The `UserDetails` object contains the following additional properties:

| Type    | Name                       | Description  |
|---------|----------------------------|--|
| Boolean | <b>DNBargeInEnabled</b>    | Allow a Supervisor/Agent to barge into a reporting agents DN call. |
| Boolean | <b>DNObserveEnabled</b>    | Allow a Supervisor/Agent to observe a reporting agents DN call.    |
| Boolean | <b>SIPSoftPhoneEnabled</b> | Reserved for future use  |

The `DNBargeInEnabled` and `DNObserveEnabled` fields are only applicable to Supervisor/Agents.

More detailed information regarding changes in the CCMA Open Interface for this release can be found in the CCMA Open Interface SDK Guide included with the SDK.

## **CCMM PHP Webchat sample application**

An updated version of the PHP Webchat sample application has been released that addresses some security issues. Please contact DevConnect for more information on the changes and details on how to receive the latest Webchat sample application.

## **SOA SDK changes**

The 6.4 Service Pack 16 the embedded Jetty server on the AACC server that is used to host the SOA interface has been upgraded to version . An updated version of the SOA SDK has been released including this upgraded Jetty server. Backward compatibility with the previous Jetty server has been maintained.

## APPENDIX A

### Software Included in this line-up

#### Previously Released Service Packs

Avaya Aura® Center 6.4 Service Pack contains updates and fixes for problems delivered in the following previously released Service Packs

#### Avaya Aura® Contact Center Software

| Release    | Service Pack   |
|------------|--|
| <b>6.0</b> | Service Pack 1   |
|            | Service Pack 2   |
| <b>6.1</b> | Service Pack 2   |
|            | Service Pack 3   |
| <b>6.2</b> | Service Pack 4 & Patch .10 & Patch .11 (RU01)          |
|            | Service Pack 5 & RU01 & RU02 & RU03 & Critical Patches |
|            | Service Pack 6 & Patches                               |
|            | Service Pack 7 & Patches                               |
| <b>6.3</b> | Service Pack 8 & Patches                               |
|            | Service Pack 9 & Patches                               |
|            | Service Pack 10 & Patches                              |
|            | Service Pack 11 & Patches                              |
| <b>6.4</b> | Service Pack 12 & Patches                              |
|            | Service Pack 13 & Patches                              |
|            | Service Pack 14 & Patches                              |
|            | Service Pack 15 & Patches                              |

#### Previous Contact Center Releases:

| Release                             | Service Update (SU)\Service Update Supplement (SUS) |
|-------------------------------------|---|
| <b>Avaya NES Contact Center 6.0</b> | SU08  |
|                                     | SUS0801   |
|                                     | CCMS Release Patches: RP08010801 through RP08010808 |
| <b>Avaya NES Contact Center 7.0</b> | SU03  |
|                                     | SUS0301   |
|                                     | Additional for CCMS:                                |
|                                     | SUS0302, SUS0303                                    |
|                                     | SUS0304 & SUS0305                                   |

This section provides information on patches that have been included in Service Pack 115.

#### Avaya NES 6.0 Contact Center Patches

| CCCC & CCMS | CCMA | CCMM | CCT |
|-------------|------|------|-----|
| n/a         | n/a  | n/a  | n/a |

## Avaya NES 7.0 Contact Center Patches

| CCCC & CCMS | CCMA | CCMM | CCT |
|-------------|------|------|-----|
| n/a         | n/a  | n/a  | n/a |

## Previously Released AACC 6.X Contact Center Patches

For information on patches that have been included in the Avaya Aura® Contact Center 6.4 Service Pack SP16 (AACC\_6.4.216.0) Lineup, please run the Patch Scanner Utility, bundled with this Service Pack, as per the instructions in the Customer Documentation.

The Patch Scanner Utility references a Catalog file (bundled with the Service Pack software) that compares the patch lineup, currently installed on your solution, against the patches that have been included in the AACC\_6.4.216.0 software build.

If any patches installed on your system are **not** included in the AACC\_6.4.216.0 software, then this will be identified and reported, via the tool.

Examples of patches that will not have been included in the AACC\_6.4.216.0 build are :

- Diagnostic patches (as these are usually built to identify a specific issue for a specific customer reported problem).
- LTD patches (on any AACC 6.X software lineup) that were built and provided to a customer site, after the design close of AACC\_6.4.216.0.
- AACC 7.X patches – as these are specific to the AACC 7.X release of software and do not apply to AACC 6.x customers.

If a patch on your AACC system is not included in AACC\_6.4.216.0 Service pack build, then you must contact the Avaya support organization to request an updated version of this LTD patch that can then be installed on top of the AACC\_6.4.216.0 Service Pack. ***This should be done in advance of installing the AACC\_6.4.216.0 software on your AACC solution.***

## CCMA ActiveX Control MSI – Content and Versions

| File Name              | File Size     | Version            |
|------------------------|---------------|--------------------|
| ChartWrapperCtrl.ocx   | 65104         | 1.0.0.1            |
| DTPWrapperCtrl.ocx     | 97872         | 8.0.0.0            |
| RICHTX32.OCX           | 212240        | 6.0.88.4           |
| riched32.dll           | 3856          | 5.0.2134.1         |
| iceemhlpcontrol.dll    | 130640        | 8.0.0.2            |
| icertdcontrol.dll      | 855624        | 8.4.12.21          |
| iemenu.ocx             | 65648         | 4.71.115.0         |
| LCIDTable.xml          | 3404          | None               |
| ntzlib.dll             | 65080         | 1.1.4.0            |
| todg8.ocx              | 1101824       | 8.0.20042.329      |
| todgub8.dll            | 249856        | 8.0.20041.18       |
| tdbgpp8.dll            | 507904        | 8.0.20042.15       |
| rope.dll               | 249400        | 1.0.0.4            |
| SSPng2.dll             | 61440         | 1.0.1.1            |
| sstree.ocx             | 337120        | 1.0.4.20           |
| comcat.dll             | 22288         | 4.71.1460.1        |
| mscomct2.ocx           | 647872        | 6.0.88.4           |
| asycfilt.dll           | 147728        | 2.40.4275.1        |
| oleaut32.dll           | 598288        | 2.40.4275.1        |
| olepro32.dll           | 164112        | 5.0.4275.1         |
| stdole2.tlb            | 17920         | 2.40.4275.1        |
| msvbvm60.dll           | 1388544       | 6.0.89.64          |
| msvcrt.dll             | 278581        | 6.0.8797.0         |
| hrctrl.dll             | 114240        | 8.0.0.3            |
| olch2x8.ocx            | 2102448       | 8.0.20051.51       |
| WSEColorText.ocx       | 179784        | 6.0.0.15           |
| PrintControl.dll       | 548776        | 12.5.0.1190        |
| PrintControl2011.dll   | <b>505808</b> | <b>14.0.8.1229</b> |
| csprintdlg.dll         | 263632        | 12.5.0.1190        |
| Csprintdlg2011.dll     | <b>260544</b> | <b>14.0.8.1229</b> |
| Pvlocale-1-0.dll       | 497056        | 12.5.0.1190        |
| pvlocale1_0_2011.dll   | <b>473496</b> | <b>14.0.8.1229</b> |
| Rsclientprint.dll      | 594443        | 11.0.3128.0        |
| rsclientprint_1028.rll | 19432         | None               |
| rsclientprint_1031.rll | 20968         | None               |
| rsclientprint_1033.rll | 20480         | None               |
| rsclientprint_1036.rll | 21504         | None               |
| rsclientprint_1040.rll | 20992         | None               |
| rsclientprint_1041.rll | 19944         | None               |
| rsclientprint_1042.rll | 19944         | None               |
| rsclientprint_1046.rll | 20968         | None               |

|                        |         |               |
|------------------------|---------|---------------|
| rsclientprint_1049.rll | 20968   | None          |
| rsclientprint_2052.rll | 19432   | None          |
| rsclientprint_3082.rll | 20968   | None          |
| RSClientPrint-x86.inf  | 1216    | None          |
| xerces_2_7.dll         | 1893832 | 12.5.0.1190   |
| msvcr80.dll            | 632656  | 8.0.50727.762 |
| msvcm80.dll            | 479232  | 8.0.50727.762 |
| msvcpr80.dll           | 554832  | 8.0.50727.762 |

## Issues Addressed in Service Pack 6.4 Line-up

This section of the release notes provides information on customer issues that have been addressed in this Service Pack since the release of Avaya Aura® Contact Center 6.4 Service Pack 14.

## CCMS, CCMSU, CCCC and CCLM, CCMT, CCWS 6.4 SP16 Listing

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

| WI ID      | JIRA ID | Description  |
|------------|---------|--|
| wi01215497 | N/A     | 6.4 SP15 ACCS – CCMS – PCP time does not peg for CDN call in Contact Summary report while agent is active on MM contact and CDN call                           |
| wi01213074 | N/A     | 6.4 SP15 ACCS – Agent is stuck on Busy status after releasing OB contact and consultation call   |
| wi01208005 | N/A     | 6.4 SP15 – AML Networking – Local Agent is updated to Busy without DN out after completing supervised transfer to remote Agent                                 |
| wi01221253 | N/A     | Login/logout report pegs data incorrectly for MM only agent setting NotReady while active on a contact.  |
| wi01220807 | N/A     | Non-multiplicity capable Supervisor stuck in Busy state after release of pulled contact and WC Observe   |
| wi01228657 | N/A     | ASM is moving blended agent to Idle instead of Break when DN call is released, if a multimedia contact was released previously but after DN call was initiated |
| wi01226092 | N/A     | Longest Idle Agent does not receive a call if the CDN call that queued to network skillset is abandoned before being answered                                  |
| wi01230800 | N/A     | VSM_Service sets up state before configuration is complete.  |
| wi01232101 | N/A     | NINOAM_dwNtwkSkillsetStatusListGet NOAM API is not being passed a valid SiteID value   |
| wi01231960 | N/A     | CCMS fails to install on SP16  |
| wi01233307 | N/A     | CBC at Source shows Abandon CBC at Target shows Disconnect   |
| wi01199107 | N/A     | Agent state is updated incorrectly after transfer call while active on 3 calls from Communicator   |
| wi01201634 | N/A     | RTD updates Idle in contact status after releasing mm contact even though agent is Busy on outbound call   |
| wi01203595 | N/A     | [6.4FP2] ASM_RTD does not update Busy for DN ringing if the Voice Mail and DN are ringing and the Voice Mail is accepted                                       |
| wi01214281 | N/A     | 6.4-CCMS-Supervisor agent with MPC off can pull MM contact when he is on observer/barge in contact   |
| wi01131095 | N/A     | Able to assign many POM skillset with a numerical priority for an agent via Assignment   |
| wi01199236 | N/A     | CCMS 6.4.2 – Agent status back to Idle during Break time when changing MPC value   |

|            |         |   |
|------------|---------|---|
| wi01215309 | N/A     | [Intermittently] SP15_ASM_RTD updates Idle instead of Busy when agent actives on DN call and hold call in the Not Ready state then changes to Ready |
| wi01212188 | N/A     | Resource leak in CMF due to JMX connection not being closed by MSM in cmfServiceNotAvailable  |
| wi01199080 | N/A     | ASM does not update phoneset display on the transfer complete in LNI case   |
| wi01203630 | N/A     | AACC6.4 FP2 ASM– The MM contact is not presented to agent while he is consulting IM to other agent  |
| 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   |
| wi01196285 | N/A     | Changes to CBC Applications or Historica1 statistics setttings are not updating   |
| wi01207924 | N/A     | AACC SP14 Pull fails when agent goes NRDY on phone leading to long ring time in HR  |
| wi01206192 | N/A     | Scheduled backup runs immediately after the switchover  |
| wi01210359 | N/A     | Call Arrived date and time on CBC reports are incorrect when the call ID is reused  |
| wi01209714 | N/A     | Exception thrown when creating a new Queue Block in OD  |
| wi01210470 | N/A     | Skillset calls not presenting in order they are received when agent priority and call priority are equal  |
| wi01212628 | N/A     | CP_CONNECTED event received for previous GiveBroadcast request destroyed the SR timer and then the service request was hanging without any action   |
| wi01216404 | N/A     | TFE - ROUTE Call CONTROLLED Results in Phantom Call where messages take greater than 12 seconds to respond  |
| wi01216019 | N/A     | Voice segments fail to be played to caller  |
| wi01212635 | N/A     | VSM experiences 1.5 seconds delay if agent completes transfer to CDN while consult call is ringing on voice port                                    |
| wi01215533 | N/A     | DIW test results in error 51514 - SQLCODE: 99 Privilege Violation   |
| wi01218948 | N/A     | Heap corruption and access violation exceptions in HDC leading to a crash   |
| wi01216747 | N/A     | TFE generates Event ID 48510 Call already exists for wrong scenario   |
| wi01220885 | N/A     | Intermittent calls are presented in AAAD without skillset   |
| wi01222476 | N/A     | MLSM sends ApplicationRegistration_Resp containing ALREADY_EXISTS to incorrect application  |
| wi01222773 | N/A     | FirstEventTimestamp populated with value of previous instance of callid   |
| wi01224277 | N/A     | IVR transferred calls to CDN are defaulting to ACD DN intermittently  |
| wi01221782 | N/A     | Agents are intermittently presented two email or two WC contacts although the MPC value is set to 2: 1 email and 1 WC.                              |
| wi01225389 | N/A     | FirstEventTimestamp populated with value of previous instance of callid   |
| wi01224728 | N/A     | SP15 NCC DB restore fail with error on switch type  |
| wi01224287 | N/A     | Database Restore Failure due to DataSafeGuard exception.  |
| wi01224537 | N/A     | Unable to login Agent created that was earlier deleted.   |
| wi01222070 | N/A     | HDM terminating when Purging CSRIntrinsic Stats resulting in roll-back and excess CSR and no daily consolidation                                    |
| wi01224782 | N/A     | The Agent stuck in Consultation state on RTD  |
| wi01227134 | N/A     | AACC Mission Critical Standby generating Licensing alarm (Event ID 61150) every 6 hours   |

|            |     |   |
|------------|-----|---|
| wi01227250 | N/A | ASM treated the idle agent as active on DN call - resulted in agent unable to pull Emails   |
| wi01226270 | N/A | RTD showing Agent in busy state when agt is ready after OB scenario   |
| wi01230007 | N/A | AACC SP13 Voice and Multimedia contacts fail to be created when only the Standby AACC is restarted  |
| wi01225426 | N/A | After AACC reboot VSM requires to be restart for access ports to work   |
| wi01230936 | N/A | Database Migration fails when Actual Number of agents exceeds Configured number of agents   |
| wi01229984 | N/A | ASM did not send agent reservation to NCP after reserving an agent  |
| wi01228134 | N/A | Agents reported Idle on RTD but they are not getting presented calls from the queue   |
| wi01226176 | N/A | HDM hang HDM not processing stat files  |
| wi01229543 | N/A | AACC - Call being pegged as abandoned in CBC report if the call return to network skillset  |
| wi01230322 | N/A | Application Threshold not working as expected   |
| wi01232218 | N/A | TFE termination due to CounterInformation utility   |
| wi01232313 | N/A | agent using reject button - incorrect call abandon at source node   |
| wi01231472 | N/A | second activity code missing contact id results in reporting error  |
| wi01231325 | N/A | Reply Email from customer does not present to other agents and does not escalate  |
| wi01229785 | N/A | uniqueDeviceIdToTn Hashtable entries are never being deleted leading to CMF Out of Memory over a long period                              |
| wi01217993 | N/A | HDC Termination   |
| wi01219930 | N/A | Traps are not generated properly for Cache SNMP events  |
| wi01232311 | N/A | In case of RESPONSE Failure the NCP should not filter the target node for this generic failure  |
| wi01232297 | N/A | Agents stuck and not moving to Idle after agent rejected the incoming network call by going NRD   |
| wi01233212 | N/A | Emails cannot be pulled following MCHA Switchover   |
| wi01232760 | N/A | Real agent is getting stuck when a call transfer is being completed just after a ITR Route is being issued but before ITS is received     |
| wi01232710 | N/A | Managed IP does not move from Active to Standby after CCMM HA failover  |
| wi01232693 | N/A | AnswerData notified to source ASM but not passed to source EB leads to inject abandon in CBC  |
| wi01232506 | N/A | CBC at Source shows Abandon CBC at Target shows Disconnect  |
| wi01230483 | N/A | When importing WSDL using DIW throws error saying already exists  |
| wi01233611 | N/A | CCMS ASM_Service terminated unexpectedly for customer   |
| wi01233903 | N/A | LNI call abandoned causes stuck agent   |
| wi01232902 | N/A | AACC SP15 - AML to SIP networking calls showing abandoned on AML site   |
| wi01233953 | N/A | TFE is resuming script execution when a pull request is performed on a contact that is being already handled                              |
| wi01221256 | N/A | Time for NRR and ACW codes is not pegged correctly in case agent sets NotReady while active on MM contact.                                |
| wi01212280 | N/A | Race condition on CAB on Voice port in VSM causes incorrect events for all calls on broadcast port  |
| wi01223288 | N/A | 11th call in SR isn't added to broadcast session if some call is abandoned between ITR and ITS Listen Add-on requested for first 10 calls |
| wi01222242 | N/A | Agent incorrect state due to logout event missing in EB   |
| wi01226110 | N/A | TSM issue with Access ports (Dead Air)  |
| wi01218239 | N/A | Historical statistics is not pegged correctly for dynamic skillsets in AgtBySkillsetStat  |



|            |         |   |
|------------|---------|---|
|            |         | view.   |
| wi01218723 | N/A     | ASM in SIP CC models call as ACD call   |
| wi01221624 | N/A     | Intermittent failure on attached data using UNE   |
| wi01220996 | N/A     | Agent displayed as Not Ready on RTD when Logged Out during UnionBreak time  |
| wi01223705 | N/A     | AACC 6.4 SP14 - intrinsic after transfer is empty   |
| wi01223159 | N/A     | AACC 6.3 SP11 ASM termination   |
| wi01202706 | N/A     | HDM service intermittently gets into a hung state   |
| wi01205104 | N/A     | ASM should allow the Queue to Agent as long as agent has the matching contact type  |
| wi01212676 | N/A     | AACC - AML to SIP networking calls showing abandoned on AML site  |
| wi01233228 | N/A     | Clickjacking Security flaw in Tomcat instance on AACC   |
| 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 EXTSELECT^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"  |
| wi01206964 | N/A     | Invalid archive namespace initiates switchover  |
| wi01217248 | N/A     | ROUTE CALL to AAM has ringback from AMS continues to be heard after AAM answers   |
| wi01218418 | N/A     | TFE logs generation has stopped   |
| wi01233372 | CC-6210 | Change NCC OAM Sync Site call timeout from 30 seconds to five minutes   |
| wi01233617 | CC-6212 | AACC SP15: NComSetup changes to not delete NCC site in Standby mode when called with no parameters                                    |
| CC-3199    | CC-3199 | MCHA: RTD displays agent state incorrectly while agent is active on MM contact and standby is startup after switchover                |
| CC-4215    | CC-4215 | Cannot migrate database from NES 7 to ACCS 7  |
| wi01235236 | CC-6254 | AACC 6.4 SP15 ASM Request failed messages seen in Windows events  |
| CC-6315    | CC-6315 | ASM does not reset the PRIORITY IN NETWORK QUEUE to zero on All trunks busy   |
| CC-6358    | CC-6358 | Error response "Target Agent Blocked" the agent will end up receiving two calls   |
| CC-6365    | CC-6365 | Network call is not re-queued as ASM does not notify TFE to reset PRIORITY IN NETWORK QUEUE when the call is not yet queued at target |
| wi01162063 | N/A     | AACC-IQ Modified Reporting of Queue Out Of Service  |
| CC-6351    | CC-6351 | Restore of CCMS delayed by CSR Table reindex before and after restore   |
| CC-6553    | CC-6553 | ASM_Service terminated unexpectedly after pull contact scenario   |
| CC-6654    | 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    | CC-6780 | AACC SP15 - ASM did not send the dialed number to EB in Call Transferred message  |
| CC-3529    | CC-3529 | ServerConfig: Changing the case of Site Name causes the NBConfig address table to be deleted  |

## CCMS 6.4.216.1 Patch

| WI ID   | JIRA ID | Description   |
|---------|---------|---|
| CC-7265 | CC-7265 | [ACCS SP16] Migration from AML 6.4 SP15 to ACCS SP16 fails with error "No devices mapped to this session" |

|         |         |   |
|---------|---------|---|
| CC-7326 | CC-7326 | ACCS 6.4 SP16 _ Agent does not pick the call in skillset with SLR enabled and EWT exceeds TSL |
|---------|---------|---|

## CCMS 6.4.216.2 Patch and CCMS 6.4.216.3 Patch

| WI ID   | JIRA ID | Description  |
|---------|---------|--|
| CC-2471 | CC-2471 | Application still shows in Activate status after DeActivate the application  |
| CC-4010 | CC-4010 | The Contact Summary Report is not pegged ACW time when agent releases MM contact working with a DN call and logout agent |
| CC-7811 | CC-7811 | AACC6.4 SP16 - MasterService did not auto start up after fresh install Elite system                                      |
| CC-8099 | CC-8099 | SP16 – ASM does not reset priority in network queue on all trunk busy in case network skillset method setup LIA or ASA   |

## CCMS (SGM) 6.4 SP16 Listing

| WI ID      | JIRA ID | Description  |
|------------|---------|--|
| wi01207701 | N/A     | IM URI on standby server being created as an extra session on the AES                                      |
| wi01232317 | CC-6198 | queue call to skillset fails as call is locked - caller abandons   |
| wi01205685 | N/A     | SGM - ROUTE Call CONTROLLED Results in Phantom Call where messages take greater than 12 seconds to respond |
| wi01227171 | N/A     | SGM does not process agent LogOut request while a call is being routed to the agent.                       |
| wi01231701 | N/A     | SGM on Standby server attempts to register IM URI with AES.  |
| wi01232646 | N/A     | Answered Call being pegged incorrectly as abandoned in CBC report  |
| wi01233843 | N/A     | Calls are intermittently not being routed to the correct CDN   |
| wi01231035 | N/A     | exception when failed DN call blocks agent while on skillset call  |
| CC-6324    | CC-6324 | after SIP Agent NRDY scenario ASM didn't perform RTQ for call  |

## CMF 6.4 SP16 Listing

| WI ID      | JIRA ID | Description  |
|------------|---------|--|
| wi01233052 | N/A     | Universal Networking calls between 6.4 SP15 & AACC 7.0 DVD 271 not working                         |
| wi01225427 | N/A     | Unable to network calls from SP11 to SP15 node, CMF unavailable at target                          |
| wi01225186 | CC-6258 | CCT_OI should not remove OIOpenQ user upon startup   |
| wi01221170 | CC-6739 | Exception in RefClient after call transfer - RefClient can't show intrinsics                       |
| CC-6451    | CC-6451 | ACR generates unexpected alarm in case Agent holds CDN call or Agent stops CDN call by AIM         |
| CC-6464    | CC-6464 | case sensitivity in IM URI impacts wi01231701 causing stby SGM to consume all csta sessions on AES |
| wi01234663 | CC-6235 | Web Service blocking OI Clients  |
| wi01230132 | CC-6258 | CCT web service responses are greater than 10 seconds intermittently - leads to screenpop failure  |
| wi01232703 | N/A     | AACC SP15 - Issues logging into a SOA refclient when 400 terminal groups                           |

|            |     |   |
|------------|-----|---|
|            |     | assigned to user                                |
| wi01221624 | N/A | Intermittent failure on attached data using UNE |

## CCCC 6.4.216.1 Patch

| WI ID   | JIRA ID | Description   |
|---------|---------|---|
| CC-7890 | CC-7890 | AACC6.4SP16_ Unable to login SA after changing from Agent to SA - No Termial Assigned to this agent |

## CCCC 6.4.216.2 Patch

| WI ID | JIRA ID | Description  |
|-------|---------|--|
| N/A   | CC-8752 | AACC6.4SP16_ ACC Dashboard displays the lineup version is unrecognized |

## CCMA, SFW 6.4 SP16 Listing

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

| WI ID      | JIRA ID | Description  |
|------------|---------|--|
| wi01226400 | N/A     | AACC6.4 SP15 CCMA– Error to save user mapping from CCMA User migration                                   |
| wi01234130 | CC-6220 | AACC 6.4 SP15 Real Time Display failure - SOAPICERTdService down   |
| wi01227557 | CC-6175 | Elements not displayed for ContactSubType in Contact Summary Originator By Disposition                   |
| wi01231422 | CC-6190 | Failure to open reports due to 'Not enough memory' exceptions.   |
| wi01232232 | N/A     | AACC - ASP.NET unhandled exceptions in the windows event log   |
| wi01221872 | N/A     | Webadmin LogIn fails after CCMA reboot post SP14 upgrade   |
| wi01208091 | N/A     | CCMA not displaying available agents in CCM skillset view  |
| wi01217709 | N/A     | AACC 6.4 AML: DisconnectSource field is not available when creating a simplified report within RCW       |
| wi01218422 | N/A     | signature for iemenu.cab is expired  |
| wi01222714 | CC-6163 | Real-Time public or private Billboard Collection layout is not saving from client with Hebrew language   |
| wi01224141 | N/A     | Prompt Management UI does not show local time  |
| wi01225367 | N/A     | Unable to add assignment with skillset expression to Logic block in OD                                   |
| wi01225463 | N/A     | CCMA 6.3 SP11 - The command "wcApplyChanges" required after patch install                                |
| wi01226180 | N/A     | With SFW SSO enabled, media file pull by AMS from CCMA fails during prompt management                    |
| wi01226715 | N/A     | AACC6.4 SP14 - ICERTD service crash  |
| wi01228503 | N/A     | Intermittent CCMA Web Admin LogIn failure  |
| wi01228994 | N/A     | Content Group deletion by user   |
| wi01229646 | N/A     | Monthly Historical reports scheduled for last month contains data for 2 months                           |
| wi01230616 | N/A     | AACC6.4 SP14 - ICERTD service crash Aug 2015   |
| wi01231015 | N/A     | [NCC] Site filter and skillset filer in the Network Communication Parameters displays status incorrectly |
| wi01232075 | N/A     | CCMA Internet Explorer Enhanced Security Configuration (IE ESC) Setting Causes Message Text truncation   |

|            |         |  |
|------------|---------|--|
| wi01232234 | N/A     | Generic OAM Error event - ProcessActivityCodeAdd   |
| wi01232669 | N/A     | CCMA SP15 - Limit the number of Agent skillset assignment to 1500  |
| wi01233820 | N/A     | Cannot edit/open CCMM RCW reports  |
| wi01235165 | CC-6253 | AACC 6.4 SP15 - CCMA - unable to select Skillset ID in historical reproting                                |
| wi01226400 | CC-6290 | wi01226400 - AACC6.4 SP15 CCMA– Error to save user mapping from CCMA User migration                        |
| CC-6352    | CC-6352 | AACC 7.0 CCMA – RCW- All reports saved in custom folder from previous release are not migrated to AACC 7.0 |
| CC-6392    | CC-6392 | AACC 6.4 SP15: Graphic in Skillset Timeline report incorrect in Report Viewer                              |
| CC-6814    | 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 6.4 SP16 Listing

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

| WI ID      | JIRA ID | Description  |
|------------|---------|--|
| wi01215682 | N/A     | AACC 7.0 DAL service can't start on SP14 when the domain is absent in LoginName                      |
| wi01226832 | N/A     | CCT socket connection timeout when using high numbers of activity codes                              |
| wi01232045 | N/A     | AACC - missing events on CDN to CDN route  |
| wi01232316 | N/A     | Intermittently calls from AAEP are not being set to Controlled                                       |
| wi01232727 | N/A     | TAPIC termination function did not recover   |
| wi01233394 | CC-6211 | Incorrect Calling Number Displayed on Refclient after completion of transfer                         |
| CC-5168    | CC-5168 | Incorrect parsing of CallerID with CS1K 7.6.3  |
| Wi01235091 | CC-6249 | CCT SP15 - TAPI hangs on lineUnholdCall  |
| CC-3703    | CC-3703 | AML DVD193 – CCT – Need to restart CCT services to acquire new CDN Route Point or re-enable terminal |
| CC-6664    | CC-6664 | TAPISRV crash due to copying 32 bytes + a null byte (33 bytes ) into 32 byte integer                 |

## CCMM\AAAD 6.4 SP16 Listing

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

| WI ID      | JIRA ID | Description  |
|------------|---------|--|
| wi01234025 | CC-6918 | Customer scheduled backup did not complete as expected   |
| wi01198796 | N/A     | RB1238 - AAAD can be closed by X button while Agent is active on contact   |
| wi01213090 | N/A     | AAAD SP15 – AAAD still able to exit when working on contacts   |
| wi01201571 | N/A     | [6.4FP2] [I18N] AAAD_Observer button is gray out when supagent chooses the agent name to filter with I18N characters |
| 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                   |

|            |         |   |
|------------|---------|---|
| wi01229312 | N/A     | Activity Code button can be clicked in AACC SP15 for Elite when agent has no 'work-code' option enabled                                 |
| wi01229855 | CC-6183 | Standby skillsets are displayed in Contact Search depending on the "Show All E-mail Skillsets" option                                   |
| wi01234194 | CC-6222 | AAAD has no limit on the length of MailTo when sending emails   |
| wi01233734 | CC-6216 | Number of contacts return by ReadBlockOfContacts functions is incorrect   |
| wi01233732 | CC-6215 | Exception thrown when trying to read a block of contacts with Fax contact type  |
| wi01221147 | N/A     | Custom Fields Text is visible even if isVisible = 0   |
| wi01221271 | N/A     | Selected skillset on "Transfer to" changes when selecting activity code with keyboard   |
| wi01221417 | N/A     | Selected skillset on "Transfer to" changes when agent switches around the tabs  |
| wi01221516 | N/A     | The list of skillsets displayed while composing the email depends on the "Show All E-mail Skillsets" option                             |
| wi01223531 | N/A     | [I18N DU] [6.4FP2] Customer details are incorrect when the WC customer uses the Dutch characters  |
| wi01223783 | N/A     | AAAD invokes CCMMWeb Service on Voice only deployment   |
| wi01224000 | N/A     | AACC Data Management - Change to clean up schedule when clean up is running does not save   |
| wi01224400 | N/A     | MCMC incorrectly creating CCMS Contact  |
| wi01224827 | N/A     | Agents are dropped from AAAD with Critical Error message  |
| wi01224829 | N/A     | AAAD Presence issue - AAAD hang and XMPP user disconnect  |
| wi01225919 | N/A     | Phone from Agent to customer record is missing from AAAD contact history  |
| wi01226804 | N/A     | The Take Ownership button is greyed out for all users   |
| wi01227370 | N/A     | AAAD email reply-all to multiple recipients fails sends email to one recipient  |
| wi01193272 | N/A     | AAAD slow to draw when Java client is running side by side on the client  |
| wi01194958 | N/A     | ACC 6.4 RB1206 - Observe window - The skillset call in observe window of supervisor is flashed when supervisor clicks on observe button |
| wi01205299 | N/A     | CC contact tab not populated correctly  |
| wi01218002 | N/A     | Agent Name not shown in AAAD window title   |
| wi01219478 | N/A     | The words 'withs', 'withe', 'withes' and 'withing' are not flagged by AAAD spellcheck   |
| wi01221058 | N/A     | Skillset call in the observe window of a supervisor is flashed when the supervisor clicks on observe button                             |
| wi01226601 | N/A     | AAAD is allowing agent to close OB contact while DN call is still open  |
| wi01227026 | N/A     | unable to create call backs on a German locale / time zone system   |
| wi01227668 | N/A     | AACC 6.4 SP13 AAAD Contact Search Failure When Contact Search Interrupted   |
| wi01227887 | N/A     | AAAD is unable to transfer an email contact due to the dropdown list being blank  |
| wi01229167 | N/A     | "Created by" record in contact's history depends on the type of logged in agent   |
| wi01229659 | N/A     | AACC - New Multimedia contacts stop routing after restart with mails to unacquired Route Point  |
| wi01230512 | N/A     | Originating a Call in wrapup will not auto-select highlighted number  |
| wi01232105 | N/A     | CCADIntrinsicSettings.xml are truncated when modified via CCADConfigurator  |
| wi01232244 | CC-6196 | Contact gets stuck in open state when AAAD crashes  |
| wi01232318 | N/A     | Sometimes Schedule Callback skillset list is not populated and shows "Retrieving Skillsets..."  |
| wi01232528 | N/A     | Agent Desktop - Critical Error Reported to agent  |
| wi01232577 | N/A     | Supervisor shows no contacts to observe, approx 2 minutes later, he shows up  |

|            |         |  |
|------------|---------|--|
|            |         | observable (Same Call)   |
| wi01233603 | N/A     | Auto Phrases not loading for first contact in an IM chat   |
| wi01234857 | CC-6243 | MM barred email addresses case sensitive   |
| wi01234638 | N/A     | newer uccapi.dll replaced by AAAD on install   |
| CC-3689    | CC-3689 | ACCS- CCMM- AAAD- Cannot login agent after changing from voice only to blended agent because missing account info under multimedia tab |
| wi01175181 | CC-6033 | AACC SP11: AAOA: Offsite Agent Gets Stuck Cotnact upon Network Issues - Login Issues After the Fact                                    |
| wi01233831 | CC-6218 | AACC 6.4 CS1K SIP: Cannot initiate call on AAAD after two DN calls placed to agent.  |
| wi01235324 | CC-6257 | Agents can extend ACW multiple times   |
| wi01235031 | CC-6248 | ReadBlockOfContacts Methods from CIClientWS returns wrong amount of contacts remaining   |
| wi01235030 | CC-6247 | When given startContactID not in DB to ReadNextBlockOfContacts in CIClientWS it returns wrong contacts                                 |
| CC-5221    | CC-5221 | Allow hot desking to be enabled on an AML platform   |
| CC-6693    | CC-6693 | Callback expiry date not set correctly for expiry having tomorrows date  |
| CC-7522    | CC-7522 | [SP16] AAAD is stuck if agent actives on CDN call and maximum MM contact then tries set AC and NRD code                                |
| wi01229157 | N/A     | Update CCT Assemblies for AAAD to include wi01226832   |
| wi01231523 | CC-6191 | Contacts Outstanding Summary report slow after upgrade to sp15   |
| wi01234538 | CC-4876 | Request to disable the COM registration of the Microsoft Lync dll "Uccapi.dll".  |

## CCMM/AAAD 6.4.216.1 Patch

| WI ID   | JIRA ID | Description  |
|---------|---------|--|
| CC-7522 | CC-7522 | AAAD is stuck if agent actives on CDN call and maximum MM contact then tries set AC and NRD code   |
| CC-7315 | CC-7315 | POM Preview/Predictive contacts - AAAD not reflecting correct POM Wrap up timers<br>AAAD denies any ACW time when ACW Extensions is 0 or not defined |
| CC-5193 | CC-5193 | AAAD hangs when logging in Presence ID   |

## CCMM/AAAD 6.4.216.2 Patch

| WI ID   | JIRA ID | Description  |
|---------|---------|--|
| CC-7888 | 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 | 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 | 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 |

## CCMM/AAAD 6.4.216.3 Patch

| WI ID   | JIRA ID | Description  |
|---------|---------|--|
| CC-8377 | CC-8377 | Launch AAAD and login agent who currently logged in, AAAD topmost is auto active |

## Avaya Media Server (AMS) 6.4 SP16 Patches Listing

This list contains defects addressed for the Avaya Media Server components of Avaya Aura® Contact Center.

**AMS: 7.6.0.959**

**AND**

**QFE-EMLite-7.6.0.959-0001**

**AND**

**QFE-platform-7.6.0.959-0001**

| CR/WI/JIRA | Summary  |
|------------|--|
| AMS-876:   | Conference session attempts following MSML interpreter crashes can fail due to port collisions between FntMP and IvMP. |
| AMS-883:   | The MSML interpreter crashes when a termination dialog specifies a repeat forever iteration on a CStore resource.      |

**QFE-platform-7.6.0.959-0002**

| CR/WI/JIRA | Summary  |
|------------|--|
| AMS-1136:  | A JRE TZData update is required for insertion of the 2015 leap second. |

**QFE-platform-7.6.0.959-0003**

| CR/WI/JIRA | Summary  |
|------------|--|
| AMS-1411:  | The voice of a conference participant can be distorted when the G.729 codec is used. |

## Contact Center Services for AMS (CCSA) 6.4 SP16 Patches Listing

**CCSA: 6.5.0.158**

**And**

**QFE-\_\_sip-conf-6.4.0.158-0001**

| CR/WI      | Summary   |
|------------|---|
| wi01210954 | AACC6.4 SP16: The zip tone is not play when agent answers call using de_de locale |

**QFE-\_\_sip-conf-6.4.0.158-0002**

| CR/WI   | Summary  |
|---------|--|
| CC-6742 | Create CCSA QFE to apply all the latest RHEL updates to SP15 OVA for SP16 release. |

## APPENDIX B - Known Issues

### Hardware Appliance

---

**wi01175733** AACC Hardware Appliance requires manual NIC Adapter "Receive Side Scaling" (RSS) configuration.

---

AACC Hardware Appliance does not have Receive Side Scaling (RSS) fully configured to minimize the chances of CPU saturation when processing inbound RTP streams.

This is only applicable when Avaya Media Server is installed on Windows.

**Impact:**

Individual CPU cores may become saturated processing inbound RTP stream leading to potential degradation in speech quality.

**Workaround:**

Carry out the following configuration changes to all NIC Adapters:

Configure the following NIC settings under:

Control Panel >> Network and Internet >> Network and Sharing Center >> Change adapter settings

- i. Set "Receive Side Scaling" to Enabled.
- ii. Set "Maximum Number of RSS Queues" to 4.
- iii. Set "Receive Buffers" to "Maximum".

### Network Configuration

---

**wi01175369** Prior to joining a Windows Domain, ensure the times of the Domain Controller and AACC Server is within the same day.

---

Cache will not start up, and will show in the taskbar as greyed out. This only happens if your current Server Time in your system clock is ahead of the system clock configured on the Domain controller and the Server time is prior to 12am (Day Boundary) and the Domain Time is post 12am (Day Boundary).

This is caused by the journal files of cache getting corrupted by an incorrect chronological sequence in the timestamps of the files.

In the event of this occurring, contact Design Support to provide assistance in Journal Recovery.

---



## Third-Party Software

### Third Party Software Upgrade Utility

#### **wi01086965 Third Party Software Upgrade Utility 'Reboot' message may become hidden**

After the completion of the upgrade task, the user is prompted to reboot their system via a warning dialog. Sometimes this reboot prompt may become hidden behind the main application dialog. To reveal the warning dialog use the Alt-Tab key combination to bring the dialog into the foreground.

#### **wi01097093 Removal of WebLM license (plservrc.xml) on install of Tomcat 7.0.35 may prevent License Manager from starting**

When upgrading to AACC 6.4 from an earlier Service Pack line-up e.g. SP11, SP10, SP9 etc. an upgrade of Third Party software is mandatory.

The Third Party Software Upgrade Utility is provided to perform the Third Party software upgrade.

The Upgrade utility upgrades Tomcat from versions 6.0.20 or 6.0.35 to Tomcat v7.0.35 if one of these versions is detected on the system. If no versions pre-exist, Tomcat 7.0.35 is cleanly installed.

During the installation of Tomcat 7.0.35, an attempt is made to remove the following folder:

<ContactCenterInstallDirectory>apache-tomcat\webapps\WebLM

If a WebLM License file is in use in this directory prior to Tomcat installation, it will be backed up as:

<ContactCenterInstallDirectory>License Manager\bin\plservrc\_Tomcat\_backup.xml

It can occur prior to or during the install of Tomcat 7.0.35, that folder <ContactCenterInstallDirectory>apache-tomcat\webapps\WebLM becomes locked by the operating system or other process, thus preventing deletion. In this instance, Tomcat will complete its installation but there may be a loss of WebLM functionality and license data.

If this occurs the following steps must be taken to recover License Manager functionality:

1. Stop the Tomcat service (Contact Center Tomcat Instance) if it is running via services.msc
2. Manually delete the folder <ContactCenterInstallDirectory>apache-tomcat\webapps\WebLM and all contents
3. Start the Tomcat service (Contact Center Tomcat Instance) via services.msc. This will recreate the WebLM directory deleted on install of Tomcat 7.0.35
4. Launch AACC License Manager Configuration
5. Browse for a valid XML. You may browse to the earlier license backup of  
<ContactCenterInstallDirectory>License Manager\bin\plservrc\_Tomcat\_backup.xml
6. Click Apply
7. Restart the Tomcat service via services.msc

#### **wi01216527 Third Party Upgrade Utility cannot detect Crystal Reports installation status**

**DESCRIPTION** : The vendor install routine for Crystal RAS 2011 does not accurately report success or error status messages when run silently.

When Crystal fails internally, and returns a success code of '0', this is taken as a successful installation by the Upgrade Utility - which is a false positive. The next launch of the Upgrade Utility does not find that Crystal is actually installed, therefore indicates that Crystal should be installed again. This can result in a cyclical process, when each attempt to install Crystal fails but is not reported accurately, and each re-launch of the Upgrade Utility prompts for the reinstallation of same.

**WORKAROUND** : As a first check, ensure that the complete file set for the Third Party Software Upgrade Utility is available. If complete sources are available and the issue still reoccurs, please contact your local support representative for assistance.

## Third Party Software Downgrade Utility

### **wi01101812 LM fails to start when applying WebLM license after test bed is downgraded from SP10**

If downgrading from AACC 6.4 to a previous Service Pack line-up e.g. SP11, SP10, SP9 etc. a Third Party software downgrade is mandatory.

The Third Party Software Downgrade Utility is provided to perform the Third Party software downgrade.

The Downgrade utility removes Tomcat 7.0.35 before installing Tomcat 6.0.35 or 6.0.20 (version differs depending on the chosen target Service Pack line-up).

During the removal of Tomcat 7.0.35, an attempt is made to remove the following folder:

<ContactCenterInstallDirectory>apache-tomcat\webapps\WebLM

It can occur during the removal of Tomcat 7.0.35, that this folder becomes locked by the operating system or other process, thus preventing deletion. This can result in a partial WebLM directory remaining on the system after downgrade.

Note: The following procedure should be followed after you have:

- i. Downgraded your Third Party Software
- ii. Installed your Service Pack 7 Software Line-up

If the folder is not deleted, please perform the following steps:

1. Ensure you have a copy of your WebLM license file
2. Stop the Tomcat service (Contact Center Tomcat Instance) via services.msc
3. Go the folder <ContactCenterInstallDirectory>apache-tomcat\webapps
4. Manually delete the folder WebLM
5. Start the Tomcat service (Contact Center Tomcat Instance) if it has not already started, via services.msc. Wait for completion.
6. Validate that WebLM directory is available
7. Restore WebLM license file as outlined in the procedure below

#### Restore WebLM License File

During the downgrade procedure, the WebLM License file will be backed up as follows:

<ContactCenterInstallDirectory>License Manager\bin\plservrc\_Tomcat\_backup.xml

On downgrade, this license file backup can be re-used as per the following process or an alternative user copy can be used:

1. Start the Tomcat service (Contact Center Tomcat Instance) if it has not already started, via services.msc. Wait for completion.
2. Stop the Tomcat service (Contact Center Tomcat Instance) via services.msc
3. Launch AACC License Manager Configuration
4. Browse to the <ContactCenterInstallDirectory>License Manager\bin\ plservrc\_Tomcat\_backup.xml license file - click Apply (alternatively, browse for a valid license XML of your choosing)
5. Restart the Tomcat service via services.msc

## Internet Explorer Compatibility issues

### wi00808468 Memory leaks on IE8 when opening several RTDs

A memory leak happens with IE8 (iexplore.exe) when running many real-time displays. This can cause serious issues if this browser is running on the AACC server.

Microsoft provided a fix for this issue in the Internet Explorer Update released on 30/March/2010. This update should be installed to resolve this issue. It can be found at the following location (<http://technet.microsoft.com/en-us/security/bulletin/MS10-018>)

## Upgrading from Previous Avaya Aura® Contact Center 6.x Release

### wi01014200 Excessive time to uninstall SP5 RU01, RU02, RU03

The time required to remove Service Pack 05 with Rollup Patches 1, 2, 3 plus all Patches that have been generally released, could be take up to approximately 5½ hours depending on the hardware specification of your system and the number of patches that have been installed.

### wi01014041 SIP SM AACC6.Critical problem when migrating an Aura 5.2 MBT system to Aura 6.1 SM system

**Note # 1:** Migration or upgrade from Aura 5.2 MBT system to Aura 6.1 SM system requires database restore from Aura 5.2 database backup. **Only "Data"** part of the database needs to be restored for the application databases. **Do not restore the "Code"** part of the database because it will overwrite the code and routines (source code) of the Aura 6.1 SM system database with 5.2 MBT system database code, making the system unstable and unrecoverable.

**Note # 2: Do not restore the ADMIN database** when migrating or upgrading from Aura 5.2 MBT system to Aura 6.1 SM system.

### wi00928172 Server Config: Configuration of WS Open Interfaces is reset to default setting when removing/applying SP

This applies to upgrades from 6.2 SP4 (or earlier), and covers issues pertaining to a loss of both WS Open Interfaces & CCT Open Interfaces configuration settings. These settings are stored within individual xml files (SOAPProperties.xml) which are not retained upon removal of 6.2 SP4 (or earlier), resulting in a loss of configuration data on upgrade.

### Custom changes to CCT Server "RestrictedSessionAppNames" will not be maintained

Any custom changes to the "RestrictedSessionAppNames" section of the "Nortel.CCT.Service.exe.config" file will not be maintained following an AACC 6.4 upgrade.

To maintain any custom changes please back-up these changes prior to uninstalling the software. Following the Service Pack installation these custom changes must be made again, but this time using the CCT Console as these settings are no longer stored in the Nortel.CCT.Service.exe.config file.

The "RestrictedSessionAppNames" feature limits the maximum number of resources that can be allocated to a particular CCT client application regardless of the configuration settings within CCT.

The "RestrictedSessionAppNames" feature limits the maximum number of resources that can be allocated to a particular CCT client application regardless of the configuration settings within CCT.

## Pre DVD Installation

**wi01175369      Prior to joining a Windows Domain, ensure the times of the Domain Controller and AACC Server is within the same day.**

Cache will not start up, and will show in the taskbar as greyed out. This only happens if your current Server Time in your system clock is ahead of the system clock configured on the Domain controller and the Server time is prior to 12am (Day Boundary) and the Domain Time is post 12am (Day Boundary).

This is caused by the journal files of cache getting corrupted by an incorrect chronological sequence in the timestamps of the files.

In the event of this occurring, contact Design Support to provide assistance in Journal Recovery.

## AACC Product Installation

**wi01149567      An exception was reported during the CCMS Service Pack install**

An exception was reported during a CCMS Service Pack install.

ERROR #5368: Objects of class 'RS.CacheSql9' are instantiated in 1 process(es)  
> ERROR #6084: Unknown errors detected, but no error code reported

**Workaround:**

If this error message appears, reboot the server and install CCMS SP again.

**wi01191563      AMS upgrade reports locked file during upgrade**

On an AMS-AACC co-resident system, the AMS upgrade reported a locked file during the upgrade. The AMS file mysqld.exe was locked by SMMC so could not be updated by the AMS installer. The message reported is:

**Impact:**

The upgrade of AMS runs to completion however the file mysqld.exe will not have been updated. The AMS Install displays the following error message:

"The installation of Avaya Media Server is finished, but some errors occurred during the installation. After you exit the installer, provide the log files in C:\\MA\_Logs to your next level of support."

To ensure that the mysqld.exe file is updated during the upgrade, shutdown AACC using the shutdown procedure outlined in the workaround below.

**Workaround:**

Prior to upgrading AMS, perform a complete AACC shutdown using the following steps:

1. Shutdown Contact Center using SCMU.
2. Shutdown the service **CC SMMC Daemon** using the Services applet.
3. Shutdown the service **CC SMMC** using the Services applet

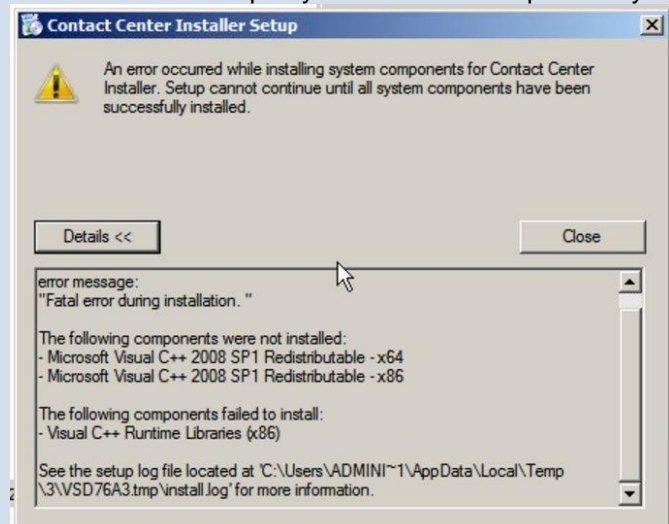
## Pre-Requisite Software known issues

**Pre-Requisite Software does not install successfully**

If performing a fresh install using the DVD media, the included setup.exe will install a number of pre-requisite software components on your system. These components enable the successful installation of your AACC software.

A problem could be encountered with the installation of the Microsoft Visual C++ Runtime Libraries (x86)

Redistributable Setup. If you encounter this problem you will receive the following error message:



This issue is a known problem and is caused by an unsuccessful install of prior Windows Updates OR Custom MSI packages that could have left faulty registry keys under HKEY\_LOCAL\_MACHINE\COMPONENTS. The Microsoft knowledge base article, KB 970652, (<http://support.microsoft.com/kb/970652/en-us>) outlines the problem and provide a link to a resolution.

To address the problem please follow the steps as outlined in the Microsoft article <http://support.microsoft.com/default.aspx?scid=kb;EN-US;946414>

## AACC Product Uninstallation

### wi01154042 Removing CCMM Primary on Single Server impacts remaining component services

When removing the Contact Center product, if the option to "Remove Multimedia Contact Center Software" is selected (if available), the uninstaller will remove the Contact Center Multimedia Service Pack (if present) and the Contact Center Multimedia base software.

Uninstallation of the base software will remove registry data that is required for licensing purposes. The undesired removal of licensing information will impact the start-up of other Contact Center component services.

#### Workaround:

After removal of "CCMM Primary Server", please run the Server Configuration utility located at Start Menu\Programs\Avaya\Contact Center\Manager Server\Server Configuration and click Apply All. This will restore the missing license data.

## DVD Controller

Please ensure that the system is in a stable condition at the time of installation. This means that all services should be fully started or stopped and the system is not in a transitional state. Otherwise the installation may fail or return errors.

---

### **wi01071276 CCMM HA UI throws Cache error after hot patching (Sp8 to SP9)**

---

Workaround:

1. Click OK on the dialogue box presented.
  2. Close the HA UI.
  3. Ensure that the HA UI is fully closed and not just minimized to the System Tray.
  4. Re-Open the HA UI.
- 

## Co-Res Installations

---

### **Updating IPs or Site Name in Server Configuration when Co-Res with Multimedia**

---

Server Configuration - When changing an IP or Site Name in Server Configuration, a message is displayed if the CCMS services are running, informing users that they must stop all CCMS services prior to making these changes. Due to link of CCMS Naming Service to Multimedia, users may not be able to make the update by stopping CCMS services alone.

Work Around:

To avoid ensure all AACC services are stopped prior to making IP or Site Name updates in the Server Configuration application. There is a possibility that the naming service will still be running even though all services appear to be shutdown. If this is the case the naming service must be killed via the task manager.

---

## Common Components

---

### **SMMC Crashes affecting AACC MCHA switchovers**

---

A vulnerability in .NET Framework 4.0 can cause SMMC to crash affecting AACC MCHA and ACCS BC switchover operation. The SMMC service is used in the operation and control of switchovers in an AACC MCHA and ACCS BC environment. The SMMC service will recover but the crash can lead to a switchover in an AACC MCHA and ACCS BC configurations.

On Standalone AACC SIP and Standalone ACCS systems the SMMC will crash and subsequently recover with no other impact to AACC/ACCS operation

#### **Solution**

Please refer to the Mandatory Microsoft Updates section of the Release Notes for Microsoft updates which must be installed to address this issue

---



**Note:** Database updates were not successfully applied due to an “error during call class method compile ‘Compile’ on class ‘%SYSTEM.OBJ’” error.

In the unlikely event that one receives that following exact error (please ignore the specified CCC patch version) on a Common Components patch install.



Workaround:

Reboot the server and attempt to install the Common Components patch again.

---

**Backup / Restore Running while installing/uninstalling Software**

User cannot create or edit Scheduled Backup tasks on Database Maintenance after upgrade from SP4 to SP6. This issue is most likely to happen when more than one Database Maintenance application is open at the same time.

Workaround:

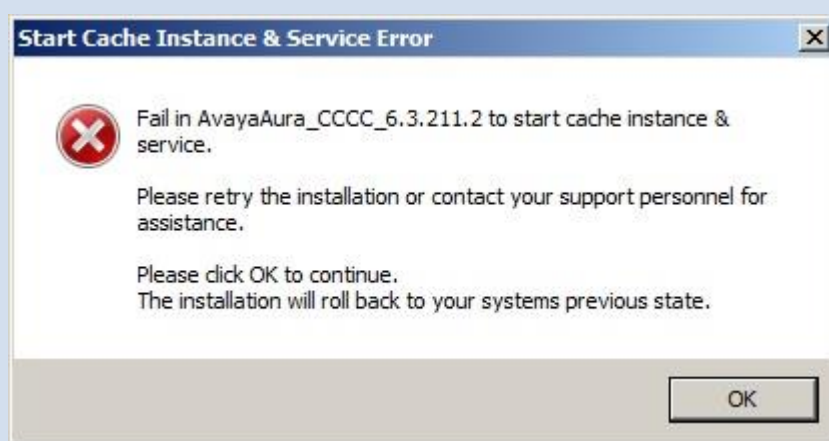
Do not perform software installation or un-installation while a backup or restore operation is running.

---

---

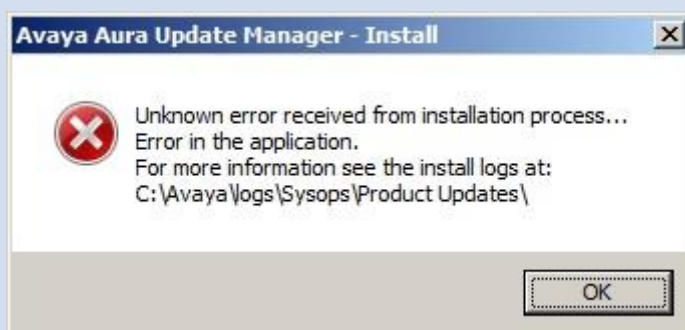
**Failure in Avaya\_Aura\_CCCC\_6.3.211.? to start cache instance...**

During the install it is possible that the user will be presented with the following error:



Workaround:

Click ok to perform the rollback. You may be presented with an additional error screen:



Click ok to continue. Once the rollback has completed, use the Blue Caché Cube in the system tray to Stop Caché, when prompted select the Restart Caché option and click ok.

---



**wi01128749 Log Archiver: Archive location reverts to default.**

**Issue:** After installing the Service Pack the archive location reverts back to the default location  
*D:\Avaya\Logs\Archive*

**Workaround:**

If the customer wants to use an alternative to the default archive location, the customer should use Log Archiver to select the alternative location. The change applies automatically when the Log Archiver is saved.

**Archiving log files to DVD**

The AACC 6.3 Log Archiver provides a feature where archives can be copied (or mirrored) to a DVD. There is, however, a limitation in a Microsoft API that is used by this feature to communicate with the DVD drive hardware. As a result, certain DVD drives will not work. Microsoft does not provide a list of compatible drives so it is possible to identify drives that will not work.

The following is the hardware that was tested in the Avaya test labs.

1. Supported drives: LG GSA-2164D, LG GCC-4482B, LG GCC-T10N, LG GCC-T20N, Optiarc AD-5560A, TEAC DV-W28EAW, TSST SH-S182M
2. Unsupported drives: TSST TS-L463A

It is expected that most drives will not exhibit the problem. To check if your drive is supported, open the Log Archiver configuration window, click the Settings tab, click the Mirror Settings button, select the Disc tab and click on the Detect Media button. If you see the error message below, your drive is not supported.

**wi01232257 Automatic switchover occurs when Active server has AACC shutdown and is rebooted.**

**Issue:** After shutting down AACC on an Active Server, if the Server is then rebooted an Automatic Switchover can occur.

This only occurs in an AML HA environment.

**Workaround:**

If, during a maintenance window, there is a requirement to reboot the Active Service the following steps should be taken to prevent an automatic switchover.

1. Stop AACC on the Active Server.
2. Using the High Availability Application, Disable Switchovers.
3. Reboot the Active Server.
4. Using the High Availability Application, Enable Switchovers.

**Notes:**

The code is working as designed, the Standby Server is monitoring the Active Server, if the Active Server is not reachable on the Network the Standby Server will take over and become the Active Server.

## Contact Center Update Manager

### Patching while backup / restore is running

Cache might fail to shut down if backup / restore is running while the patching process is running.

Workaround: Do not perform patching while a backup or restore is in progress.

### Wi01148358 Update Manager License Agreement buttons truncated on Japanese language system

In Contact Center 6.4, Update Manager has been modified and introduces a new License Agreement dialog. This dialog shows the standard Avaya license text and this must be agreed to before the installation of Service Packs and Patches can proceed.

On some language systems e.g. Japanese, the buttons at the bottom of this form can become truncated and hidden from view. A user cannot then continue with the installation.

#### Workaround

On the License Agreement screen, select the option to accept the license, and then press the return key. The default action of the return key is to continue the installation after license acceptance.

## SIP Specific Issues

### wi01207335 - RTD does not update Emergency status for Agent when Supervisor is not logged in and answers an emergency call

When a Supervisor is not logged into the contact center, and they answer an Emergency call, the RTD may display the 'In Contacts Status' as 'Active' instead of 'Emergency'.

#### Steps to reproduce:

1. Launch AAAD, login AgentA
2. Launch OneX with extension is Supervisor' Voice URI.  
Supervisor can launch CTI (AAAD/RefClient) but not login agent or no need to launch AAAD/RefClient
3. Customer make CDN call to AgentA.
4. Check RTD, 'In Contacts Status' of AgentA is Active.
5. AgentA make Emergency call,
6. Supervisor answers the call.
7. Check RTD, 'In Contacts Status' of AgentA is Emergency.

#### Expected result:

At step 7: 'In Contacts Status' of AgentA is Emergency.

#### Actual result:

At step 7: 'In Contacts Status' of AgentA still is Active

### wi01178035 The agent greeting is not played if we transfer/conference call before whisper skillset is finished

Agent1 answers call, while whisper skillset is playing then agent1 initiates transfer/conference to CDN number and completes it. Agent2 answers call then the agent greeting of agent2 is not played.

The issue only occurs with blind transfer/conference call. It does not happen if we use supervisor transfer/conference call.

The issue does not occur if Agent1 initiates transfer/conference call after whisper skillset is finished

#### Workaround:

Wait until whisper skillset completes before initiating a conference/transfer

**wi01178597: Ringback is still played if consulted agent drop call while the whisper skillset is playing**

Agent1 completes conference call, then Agent2 answers the call then drops it while the whisper skillset is playing, we see that the ringback tone is still played to customer and agent1 although they can talk to each other.

The issue happens when Agent1 completes conference call before call is presented to Agent2.

The issue does not happen if Agent1 completes conference call after call is presented to Agent2. The issue does not occur if Agent2 waits until it's whisper Skillset is complete before dropping the call

**Workaround:**

Conferenced Agent should wait until whisper skillset completes before dropping the call.

**wi01212974 Call is dropped on AAAD/RefClient and completing a transfer of a POM contact to a non POM agent**

When a POM contact is transferred to another non POM agent in an AACC environment the call is lost on AAAD/RefClient once transfer has been completed.

**CM-9955 From header changed to AACC number for the new INVITE after REFER from AACC when the original call's calling number is anonymous**

INVITE from Communication Manager (CM) contains incorrect 'From' address when 'anonymous' CDN call is routed out and back into AACC. For the scenario where a CDN call, with 'anonymous' 'From' address, is routed out of AACC via a REFER and then back into AACC the 'From' address of the INVITE incorrectly contains the CDN number instead of the expected 'anonymous'. In addition, CM maintains the same UCID which results in AACC treating this as a redirection scenario and attempts to match this call to an existing call, but fails.

**Workaround:**

REFER to a vector in CM which routes via PSTN back into the network with a default UCID. This will ensure the second call is treated as a new unrelated call, and AACC will not attempt to match to existing call.

**Solution:**

The CM team addressed this issue in CM patch 22740 which is available from CM support team.

## SIP HA Specific Issues

### **wi01007880 After manual interchange of SPHA AES, DMCC and TR/87 ports were not listening AES MR for this issue is wi01009436**

On AES 6.2, during a manual interchange on SP HA AES and in one interchange, port 4721, 4722 and 4723 were not listening and all the registration went into idle mode. For AACC, after an AES switchover, AACC cannot reestablish a TCP connection with AES.

#### Work Around:

The system recovered after restarting AES Services which does not initiate a switchover.

#### **Solution**

The AES team has a hotfix/patch for this issue: AES Patch 2 which is available from the AES Support team. - AES 6.2.0 Hotfixes and it is Hotfix No.2

### **wi01132066 6.4 [SIP HA]: Active - Active scenario observed if SMMCSERVICE.exe\*32 is killed via Task Manager**

If the SMMCSERVICE.exe crashes on the Active system, the system will recover by restarting said service. Depending on the system, this might be performed quickly, which the current system will stay Active, or else a switchover might occur. If this were to happen, the old Active may enter into Active Stopped state, which means all services, will be shut down. The HA system is now in Active-Active however, only one system is processing calls so the Contact Center can still function correctly.

#### **Solution**

To recover the HA system, the user must reconfigure the stopped Active (old Active) via HA UI to be a Standby system. Then the user must perform the necessary database backup of the current Active and restore onto the now Standby system. Once this is performed, the user can start the system via SMMC SystemTray and shadow the Active machine.

## Aura 7.0 Specific Issues

### **wi01206383 AACC 6.4 FP2 - SIP Entity Link between AACC and SM fluctuation under traffic**

During a traffic run with Aura 7.0 the SM-AACC link was dropped for 15s then recovered. This issue causes calls to AACC getting failures during this time frame.

### **Non-skillset monitoring - Customer still hears observe tone after observed agent**

Enhancements added as part of 'wi01185209 - Enhance TR/87 call control to allow dropping of unmonitored extension' also required AES updates which were delivered in AES 6.3.3. These changes were not migrated to AES 7.0.

Reference AES-14222 for inclusion in AES 7.x

## Known CCMS limitations

### **wi01098874 AACC6.3 Transfer / Conference Number appearing as DIALED#:N/A in CBC report**

In SIP Contact Center, the dialed number information is now available and pegged correctly in CBC reports. CallConsultInit event in CBC reports will show correct dialed number in case of transfer/conference to both external DN or CDN.

This feature is not supported on AML Contact Center and therefore the dialed number information does not peg. For example, DIALED#:N/A will appear in the Event data column of CallConsultInit event in CBC reports.

# Avaya Media Server

## Linux Issues

### Linux Issue with Broadcom NIC driver

During traffic testing, an issue was experienced where the NIC interface on the AMS Linux server became unresponsive. The issue was only seen on systems with the following version of Broadcom bnx2 NIC card driver: **Version 1.9.3**

This driver was released as part of Redhat Enterprise 5.4. If a more recent version of Redhat is used then a more recent version of this driver will probably be installed.

To check the version of NIC driver on the Linux Server:

Run the command **ethtool -i eth0**

The version information for the Broadcom driver with the issue is:

**driver: bnx2**

**version: 1.9.3**

**firmware-version: 5.2.3 NCSI 2.0.11**

To update the driver install the latest Redhat Linux updates and run the **ethtool -i eth0** command to verify that the NIC driver has been upgraded.

### Security Enhanced Linux (selinux) not supported on RHEL5.x

Avaya Media Server 7.6 only supports selinux on RHEL 6.x installations. selinux is not supported on RHEL 5.x systems.

#### wi01199874 AMS RHEL 32bit Linux: AMS Server failed due to memory issue.

AMS running on Red Hat 32bit Operating System sometimes experiences issues where critical AMS components are killed by the Red Hat OS due to "Out of Memory" issue. This issue is caused by a known limitation of the Red Hat 32bit architecture known as "**lowmem starvation**". This issue cannot be addressed in 32bit Installations. The AMS Server will have to be upgraded to Red Hat 6.x 64Bit OS. A complete Server rebuild is required

PSN004375u has been published detailing this issue.

To check if your system has experienced this issue. Check the following:

1. Search file: /var/log/messages for the following string: "**Out of Memory: kill**".  
Note: Other processes as well as AMS processes may be killed by the kernel, so there could potentially be other failures in the Linux Server that are unrelated to AMS.  
Examples (sipmc is a AMS critical component, audiospd and portserve are OS applications): In this example one AMS process is killed and two non-AMS processes are killed (audiospd and portserve).  
  

```
Sep  9 08:42:41 ams1.pkgappslab.com kernel: Out of memory: Kill process 8756 (sipmc) score 14 or sacrifice child
Sep  9 08:43:21 ams1.pkgappslab.com kernel: Out of memory: Kill process 2234 (audiospd) score 1 or sacrifice child
Sep  9 08:43:23 ams1.pkgappslab.com kernel: Out of memory: Kill process 2251 (portreserve) score 1 or sacrifice child
```
2. The amount of **LowMem** can be checked in **/proc/meminfo**. If the LowFree falls below 50Mb it may be cause for concern. However this does not always indicate a problem as the kernel will try to use the entire LowMem zone and it may be able to reclaim some of the cache
3. Check AMS Element Manager Event Logs for critical component restarts.
4. If the AMS servers are configured as a HA pair, check for HA failovers due to component restarts.

#### Resolution:

This issue is caused by a known limitation of the Red Hat 32bit architecture known as "**lowmem starvation**". This issue cannot be addressed in 32bit Installations. The AMS Server will have to be upgraded to Red Hat 6.x 64Bit OS. A complete Server rebuild is required.

A full description of this condition can be found in the following documentation:

<https://access.redhat.com/solutions/16995>

This is covered in the “**LowMem Starvation**” subsection of this article.

The steps for rebuilding an AMS Server from RHEL 5.x or 6.x 32bit to RHEL 6.x 64bit are as follows:

**Note:** If this is an AMS HA Pair configuration then ALL of these steps MUST be carried out on both the **Primary** and the **Backup** AMS Servers (with the exception of step 3, backing up PLIC license from Primary AMS Server).

- 1) Perform a backup of ‘System Configuration’ and ‘Application Content’ via the **Tools -> Backup and Restore -> Backup Tasks** page in AMS Element Manager.  
Note: The backup is stored as two zip files in the default location for AMS backups:  
**\$MASHOME/platdata/EAM/Backups.**
- 2) Copy these backup files to an external location as this Server will be rebuilt and these files will be deleted during the rebuild.
- 3) If this is an AMS primary node using PLIC licensing, take a copy of the license from the Primary AMS Server (*AACC Upgrade and Patches 44400-410*) – this is not required if is AACC is using WebLM licensing.
- 4) If you have deployed any locale specific media files to the AMS file system (as opposed to the Content Store), take a backup of these files and save them to an external location. These will have been deployed in the relevant locale sub-folders of  
**\$MASHOME/platdata/Announcements/contactcenter/default**
- 5) Install Red Hat Linux 6.x 64bit OS on this server. This requires a full rebuild as Red Hat do not support upgrades of a 32bit Server to a 64bit server. Note: The Network settings and Fully Qualified Domain Name of the newly installed 6.x 64bit Server **MUST** be the same as the old Red Hat 32bit Server.
- 6) Locate the **Install Software\AMS\Linux** folder on the AACC 6.4 SP16 Release Bundle.
- 7) On your newly built 6.x 64 bit Linux server, use the su command to change to the root user account:  
su –
- 8) Create a temporary folder on Linux server by running command:  
mkdir /tmp/AvayaMS
- 9) Copy the following files from the SP16 release bundle to the /tmp/AvayaMS folder:
  - MediaServer\_7.6.0.959\_2014.11.27.bin
  - ContactCenterServicesForAMS\_6.4.0.158.bin
- 10) Change to folder: /tmp/AvayaMS and run command:  
chmod +x ContactCenterServicesForAMS\_6.4.0.158.bin
- 11) To Install Avaya Media Server and Contact Center Services for AMS run command:  
./ ContactCenterServicesForAMS\_6.4.0.158.bin
- 12) Download and apply all available AMS and CCSA QFE patches.
  - Copy all available patch ZIP files to the **\$MASHOME/qfe** folder
  - Run the following command: **amspatch apply all**
- 13) If this is an AMS primary node and AMS using PLIC licensing, restore the license copied in step 3 by copying the backed up license file into EM->Licensing->General Settings “Add License Keys”. Hit “Display Licenses”, “Save” and then “Confirm”
- 14) Copy the Backup files taken in step 2 to the AMS Linux server location:  
\$MASHOME/platdata/EAM/Backups/ and restore using AMS Element Manager:  
**Home>>Tools>>Backup And Restore>>Restore:** Select both Application Content and System Configuration and click “Restore Now” button, If this was an AMS HA pair
- 15) Restore the locale specific media files that were backed up in step 4 (if any)
- 16) Reboot the server.

**wi01226926: AMS N+1 clusters using plic licensing reporting alarm: "License Server Redundancy Connection Failure"**

The workaround is as follows (this is for linux AMS servers only.)

The issue is caused by TCP port: 1027 not being allowed through the firewall.

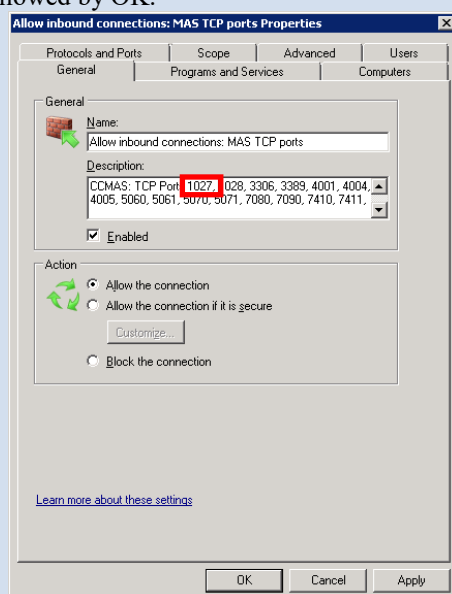
The workaround is to add a rule to allow TCP port 1027 through the firewall on both the Primary and Secondary AMS server:

**Linux:** Carry out these steps on both the Primary and Secondary AMS

1. Open putty session and logon with root access.
2. Make a copy of /etc/iptables by running command:  
cp /etc/iptables /etc/iptables.orig
3. edit /etc/iptables
4. Add lines:  
-A INPUT -m state --state NEW -m tcp -p tcp --dport 1027 -j ACCEPT  
-A OUTPUT -m state --state NEW -m tcp -p tcp --dport 1027 -j ACCEPT
5. Save /etc/iptables
6. Restart iptables by running command: **service iptables restart**

**Windows:** Carry out these steps on both the Primary and Secondary AMS

1. Launch "Windows Firewall with Advanced Security"
2. Add port 1027 into Inbound Rule: "Allow inbound connections: "MAS TCP ports"
3. Click "Apply" followed by OK.



## Windows Issues

### Upgrading AMS on a Windows Single Server Installation

This section details an AMS upgrade issue on a Windows Single Server (AACC + AMS on a single Windows instance) system.

**wi01191563 Error encountered during AMS Upgrade on an AACC/AMS co-resident Windows server.**

1. Have SIP server AACC co-resident system (single server with AACC and AMS installed)
2. Upgrade AACC to 6.4 FP2
3. Upgrade AMS from 6.4 FP2
  - i. Shutdown Contact Center services

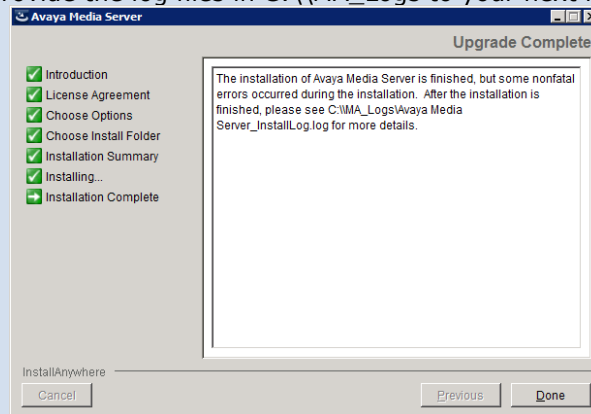


- ii. Remove CCSA ContactCenterServicesForAMS
- iii. Run InstallAMS.exe from 6.4 FP2 to upgrade AMS

Expected results: The AMS upgrade completes without errors

Actual results: The AMS upgrade completes but displays the following error message:

"The installation of Avaya Media Server is finished, but some errors occurred during the installation. After you exit the installer, provide the log files in C:\\MA\_Logs to your next level of support":



AMS has not successfully upgraded. This should be a "fatal" error and not "non-fatal".

**Workaround:** After upgrading AACC (Step 2 above) run the following steps before upgrading AMS:

1. Go to Start->Run-> and type "services.msc"
2. Stop Service: "CC SMMC Daemon"
3. Stop Service: "CC SMMC"
4. Upgrade AMS.
5. Start Service: "CC SMMC Daemon". This will automatically start "CC SMMC" service and all other AACC services.



## Contact Center Manager Server

### Installation\Uninstall issues

N/A

### Configuration Issues

In a HA environment, for calls that are up before switchover, post switchover INFO messages related to this call are being sent on the local IP to AMS. In order to avoid any problems with these calls, the user must add Managed IP, Active IP and Standby IP as trusted nodes on the AMS as per documentation.

#### wi01093311 SIP HA Voice Only-CCMS-Agent RTD shows busy while agent is on CDN call

1. Have SIP HA Voice Only system + ADTT
2. Login agent on ADTT and make him Ready
3. Agent accepts CDN call.
4. Make an auto switchover by killing service which occurs switchover (ex: TFE service)
5. After switchover completed > backup database on new active and restore database on new standby.
6. Make an auto switchover by killing NITSM by services.msc
7. Monitor the Agent RTD.

Expected results: At the step 6, Agent RTD shows active with skillset name

Actual results: Agent RTD shows Busy or Not Ready.

*Note:* I refreshed RTD but it does not update new status. The issue only happened on SIP HA Voice Only but not AML and SIP non-HA.

### Migration from NES 6.0 system

Migration from a NES CC6.0 system using the Avaya migration tool does not support the migration of Nordic characters. Please contact Avaya support if you have this character set.

### Known Issues With/Awaiting a Solution

#### CC-6354 AACC SP15: Network MCHA start-up prevents ASM from accessing all available nodes

When a switchover occurs on an MCHA node within an AACC Networking environment there is a race condition which can occur leading to the new Active Nodes ASM being unable to retrieve all relevant information relating to all the nodes in the network. This can lead to some calls being unable to route to successfully to target nodes from this new Active Node.

##### Workaround

On the NCC select the new Active Node and perform a Site Synch

##### Solution

Install designer patch AvayaAura\_CCMS\_6.4.215.302 for Service Pack 15 or AvayaAura\_CCMS\_6.4.216.4 on Service Pack 16

#### wi01222511 Event ID 41552 generating critical alarm against "nbbkp" service which no longer exists

Event ID 41552 for the "nbbkp" service is being generated as a critical error. It is a legacy service from NES CCMS 6.0 for the MAS Backup/Restore service. The "nbbkp" service no longer exists in AACC 6.4, so no events should be generated against it. But the NBSM service continues to query a non-existent service.

##### Workaround

Customers can remove the key manually from registry to avoid irrelevant alarms in NMS system.

Steps to remove the key:

1. Open Registry Editor ( "regedit") and press Enter or click/tap OK.
2. Go to the branch HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\
3. Find the key "nbbkp"
4. Delete it by a command in context menu.

#### **wi01093311 SIP HA Voice Only-CCMS-Agent RTD shows busy while agent is on CDN call**

1. Have SIP HA Voice Only system + ADTT
2. Login agent on ADTT and make him Ready
3. Agent accepts CDN call.
4. Make an auto switchover by killing service which occurs switchover (ex: TFE service)
5. After switchover completed > backup database on new active and restore database on new standby.
6. Make an auto switchover by killing NITSM by services.msc
7. Monitor the Agent RTD.

Expected results: At the step 6, Agent RTD shows active with skillset name

Actual results: Agent RTD shows Busy or Not Ready.

*Note:* I refreshed RTD but it does not update new status. The issue only happened on SIP HA Voice Only but not AML and SIP non-HA.

#### **wi01089091 AML HA– Email notification about switchover time is not sent to intended recipient when switchover initiated by unplug CLAN, power down Active or Manual switchover**

1. Have the system configured HA and working well.
2. The switchover Notifications is configured and working well.
3. Enable auto switchover on Active & Standby servers.
4. Power down Active server
5. Switchover
6. Check the Email notifications about switchover are sent to intended recipient.

Expected result: At step 6: The intended recipients will receive the emails notified reason caused switchover, the time when switchover occurs.

Actual result: At step 6: The intended recipients do not receive the emails notified reason caused switchover, the time when switchover occurs. They only receive the email notification about the time when switchover is completed.

#### **wi01101419 Not Ready time is not consistent across reports for multiplicity agents.**

The inconsistency between Agent Performance and NRRC reports is intentional.

When agent is working on a MM contact and is in NotReady state in AAAD, the time is not pegged as NotReady time in Agent Performance reports (because agent is not in Not Ready state in general).

But NRRC reports deal with Real agent only and look at his state so calculate Not Ready time.

#### **wi01082595 AML HA - RTD shows Idle agents to be Not Ready post switchover.**

1. AML HA system
2. Login blended agent. RTD shows him as Idle (agent has to login via Ref or AAAD)
4. Perform an auto switchover by killing NCCT OI service on Active
4. Switchover is completed
5. RTD displays agents as Not Ready.

### SDMCA stuck starting

On a SIP based system, a rare race condition can occur when the communication to WebLM is slow. The race condition can result in SDMCA stuck starting as it waits for NDLOAM which is stopped.

Workaround: Launch SCMU and click Start CCMS.

### First system start-up post install, TFE stuck in starting

After the first start-up following an installation, TFE can be seen stuck in a starting state. This is caused by a script activation failure. This can happen if the licensing is not correct at the time of the first start-up of the server.

Workaround: Launch OD and activate all scripts. Multimedia Script first, followed by all other scripts and Master script last

### wi01050669 AAAD logs in to DeskPhone Mode even when Hardphone(SIP) is not logged in

AAAD allows user to Login to Deskphone mode even when there is no SIP Endpoint logged in. AES does not know if the SIP Endpoint is logged in and therefore SGM does not know – so login is allowed to continue. This is not an issue with H.323 stations.

Workaround: Ensure phone set is logged in.

### Possible AACC Backup error when Backup operation completes

Possible error message displayed at completion of an AACC backup:

Error displayed at the end of a backup operation and the following is logged to the `\Common Components\CC_DBMaintenance.log` file:

*ERROR #5001: could not move directory 'O:\Backups\ccms\_conf\data\Backup.log' to: 'O:\Backups\BACKUP\_1\CCMS\_CONF\DATA'. The folder may be in use by another application. Close explorer windows and try again.*

Workaround: Ensure there are no open File Explorer sessions to the backup folder and that the location is not in use OR if the issue persists, backup to an empty folder location.

### wi01088835 SP10 – CCMS SGM – CLID of CC agent is updated T3683 when Elite agent receives VDN call from customer and Elite agent makes a transfer DN to CC agent

1. Remote customer makes a VDN call to Elite agent
2. Elite agent answers then makes a blind transfer to DN of CC agent
3. CC agent answers call

The CLID is displayed on AAAD of CC agent as T3683#`

### wi01176769 SMMC Startup: Message broker port (61616) can be taken by other application leading to SMMC startup failure

#### Steps to reproduce:

SMMC service, which starts Systemcontroller, can sometimes fail to startup correctly if the port 61616 is already taken by other SMMC message broker clients. Such clients can be SCMU, SystemTray and NCCT Service (whatever CCT service uses the MQ). It is required then for the user to shutdown these processes/services for SMMC to start up correctly. The usual culprit is SystemTray which will continually try to reconnect to the message broker thus blocking systemcontroller from taking the port.

This leads to a failed SMMC start up and it's not clear to the user why.

**Workaround:** SMMC Service should shutdown SystemTray before starting SystemController and re-open it afterwards. This guarantees that it will not block the port. All SMMC service needs to do is launch systemtray with the argument "-c" to shut down all instances. This could also be applied to SCMU and NCCTService potentially, kill all instances of these processes first before starting SystemController.

#### **wi01197653      'ARC Service should not be started automatically on Stdbby server after running ARC Selection Utility**

##### **Steps to reproduce:**

SMMC service, which starts Systemcontroller, can sometimes fail to startup correctly if the port 61616 is already taken by other SMMC message broker clients. Such clients can be SCMU, SystemTray and NCCT Service (whatever CCT service uses the MQ). It is required then for the user to shutdown these processes/services for SMMC to start up correctly. The usual culprit is SystemTray which will continually try to reconnect to the message broker thus blocking systemcontroller from taking the port.

This leads to a failed SMMC start up and it's not clear to the user why.

**Workaround:** SMMC Service should shutdown SystemTray before starting SystemController and re-open it afterwards. This guarantees that it will not block the port. All SMMC service needs to do is launch systemtray with the argument "-c" to shut down all instances. This could also be applied to SCMU and NCCTService potentially, kill all instances of these processes first before starting SystemController.

#### **wi01213074      Agent is stuck on Busy status after releasing OB contact and consultation call**

##### **Steps to reproduce:**

1. Login agent 1, 1000 and 8001 on AAAD or Ref
2. Set agent 1 Not Ready -> Pull an outbound contact and makes DN out to agent 1000 also
3. Agent 1000 accepts the DN call
4. Agent 1 initiates a supervised transfer the DN call to agent 8001 by DN call -> Agent 8001 accepts it -> Agent 1 have not completed transfer yet
5. Agent 1000 releases the DN call -> Take a look on RTR
6. Agent 1 releases the OB contact -> Change agent1 to Ready -> Take a look on RTR
7. Agent 1 releases DN call -> Take a look on RTR

##### **Expected result:**

At step 5: Agent 1 updates blank on DN out column

At step 6: Agent 1 updates Busy in Contact Status column

At step 7: Agent 1 updates Idle

##### **Actual result:**

At step 5: Agent 1 updates blank on DN out column

At step 6: Agent 1 updates Busy in Contact Status column

At step 7: Agent 1 is stuck on Busy status

##### **Note:**

- The issue does not happen if agent 1 changes to Ready then release OB and DN contact.
- The issue does not happen if agent 1 makes DN out at step2 without pulling OB contact
- The issue does not happen with another MM contact
- The issue has gone after set Not Ready then Ready agent 1
- The issue does not happen if agent accepts OB contact and changes to Not Ready automatically due to MPC
- ContactID: 53. Timestamp: 3:15 pm -> 3:21 pm

**Workaround:** The issue has gone after settin Not Ready then Ready for Agent 1

**wi01227109 RGN Server Monitoring during Campus Switchover.**

During a switchover on the Campus Servers it's possible the RGN Server will not automatically continue Shadowing.

- This is expected behavior as under certain circumstances the RGN Server will not be able to continue shadowing from the new Active Server.
- The RGN Server after about 10 minutes will raise a Windows Event and report the problem through the High Availability Application. But if no one is monitoring the RGN Server then this information can be missed with the result that the RGN Server is not Shadowing.
- If the RGN Server is unable to start Shadowing it will request that a Backup and Restore is required before starting Shadowing. Users should perform a Backup and Restore in this situation in order to enable Shadowing on the RGN Server.

**wi01225184 Site Name change deletes NCC from nbconfig - nbconfig crashes****Steps to reproduce:**

On AACC-NCC SP16, modifying the "Site Name" to all lowercase or uppercase in "Server Configuration" deletes NCC server from "nbconfig -admin" utility. Afterwards, one may not add the NCC server back into "nbconfig -admin." Running "Force Synchronization" afterwards causes "nbconfig -admin" to crash..

**Workaround:** Do not change the "Site Name" to the same in upper or lower case.

**wi01226163 4 Party Conference RTD shows incorrect state for all agents**

Scenario:

1. OOP call CDN1 which routes to agent 1
2. Agent 1 makes a conference call to CDN2
3. Agent 2 gets the conference invite but does not accept it immediately
4. Agent 1 finishes the conference
5. Agent 1 makes a conference to CDN1
6. Agent 3 gets the call but does not answer it
7. Agent 1 finishes the conference again
8. Agents 2 & 3 answer the call

Actual results: Call is running fine but two agents show as Busy and one agent shows as Idle and Ans Skiset column is empty in RTD because the current design limits the number of active conferences per agent to one only.

**Workaround:** complete the first conference before initiating the second one.

**wi01230951 CCMS Event Codes**

The following Event Codes do not have proper description in the Server Utility tool:

- **49403** is the memory allocation failure event. Usually it is accompanied by some WARN message in MLSM logs. Check if the machine hardware meets the system requirements. If yes, please note any error codes / messages and contact your Customer Support Representative.
- **49447**. Bad MLINK message received. These messages are ignored on AACC side.
- **41294**. "Info Not Found" TSM event. SPI Monitor Start response is received from the switch but no

corresponding session is found in the table. Please note any error codes / messages and contact your Customer Support Representative.

## Limitations

### **Scripts already saved to disk can't be opened in OD if saved with Windows reserved file extensions**

If scripts are saved to disk with Windows reserved file extensions you will not be able to open them within OD unless they are renamed first.

The following are the list of extensions Windows has reserved.

CON, PRN, AUX, CLOCK\$, NUL, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8, and LPT9.

### **The temp agent is changed to Not Ready state after he initiates IM CDN contact**

The agent can be put in NotReady state without ability to handle MM contacts if he initiates IM CDN contact which is presented to him again.

- If there is only one agent logged in and ready on the system and at the same time he initiates IM CDN contact.
- If a blended agent is enabled with multiplicity and initiates IM contact to CDN then this outgoing IM contact will be connected with the real agent while the temporary agent will remain in Idle state.

So the same agent can be selected for that IM CDN contact by ASM but in turn SGM will fail the routing because the agent already has active IM session. In this case upon receiving failed routing response ASM will force the temporary agent to NotReady state so the blended agent won't be able to handle MM contacts until IM CDN contact is released by the agent or handled by another agent.

### **wi01107848 AACC6.3 SP10 using close to 16GB while under max traffic in a CoRes system**

At very large active agent numbers, the RAM consumption can approach the physical limit of the server. Therefore, 32 GB is recommended for configurations where the number of active agents is 4000 or greater.



## Network Control Center (NCC)

### CC-8050 Adding Site can disappear or Removed Site can reappear on NCC

If you are Adding or Removing a Site on the NCC it is critical to restart the NCC to avoid a mismatch of Nodal data between the NCC and the sites networked nodes.

## License Manager

### After a full un-install of Corporate License setup, CCMM LM starts up as Nodal

After the reboot following a full un-install of Corporate License setup, CCMM LM starts up as Nodal license.

Workaround: Run the Server Configuration utility after the patches have been re-installed.

### Standby CCMM did not get the MMP license on switchover

CCMM does not check its license state until cache is up and running, but the problem is that the LM client is getting initialized beforehand (when the CCMM LM Service starts).

This is ok most of the time, as it initializes and connects to a running LM, but in this co-res campus standby scenario it points to a bogus LM so it looks for the grace license and can't get it from the db.

The licensing component does not recover from the first failure to connect to the db.

Workaround: A CCMM restart will bring everything up.

### wi01104823 HA - SDMCA gets stuck in starting state after License change to add Networking feature and performing switchover without rebooting Standby first

Description: When users enable Networking on the Active server, this change will be synchronized automatically to the Standby server. But there is a mismatch between the Active & Standby about enabling NDLOAM service. It's enabled on the Active, but not on the Standby. SDMCA will get stuck due to NDLOAM disabled on the Standby if switchover is initiated.

To prevent this issue, after the Active Server has been rebooted you must also reboot the Standby server for it to pick up the updated information correctly.

### Networking versus non-Networking license features in WebLM

When using a WebLM licensing mechanism, If the networking feature/license is defined, License Manager will only make available agent licenses of type "NET" (networking) and not of type "LOC" (local) for consumption by other AACC components i.e. it will not be possible to unselect the "Networking" package in Server Configuration and expect the previously created "NET" agent licenses to work likewise.

Workaround: Produce a non-Networking WebLM license file when non-Networking operations are required.

### wi01147885 LM is not started after Upgrade\_6.3 SP 11 to RB447 AACC6.4\_SIP\_Cores with AMS

Description: License Manager will not start because it finds an incompatible library when it is loading its dependent libraries.

#### Workaround:

Copy libeay32.dll from D:\Avaya\Contact Center\Manager Server\iccm\bin to D:\Avaya\Contact Center\License Manager\bin.

### wi01205140 License type may change from remote to local WebLM after upgrading to SP16 from SP10/11

This is not an issue with the SP16 installation but rather an issue with SP10/11 removals. On removal, these Service Packs will not retain remote WebLM settings and will revert to a state of local WebLM



usage.

On SP16 install, existing licensing settings will not be modified i.e.local WebLM settings will be retained

Workaround:

1. Launch LMconfig
2. Configure WebLM port and IP accordingly
3. Press apply.
4. Relaunch LMconfig to verify details are correct (this step is optional)

## Contact Center Manager Administration

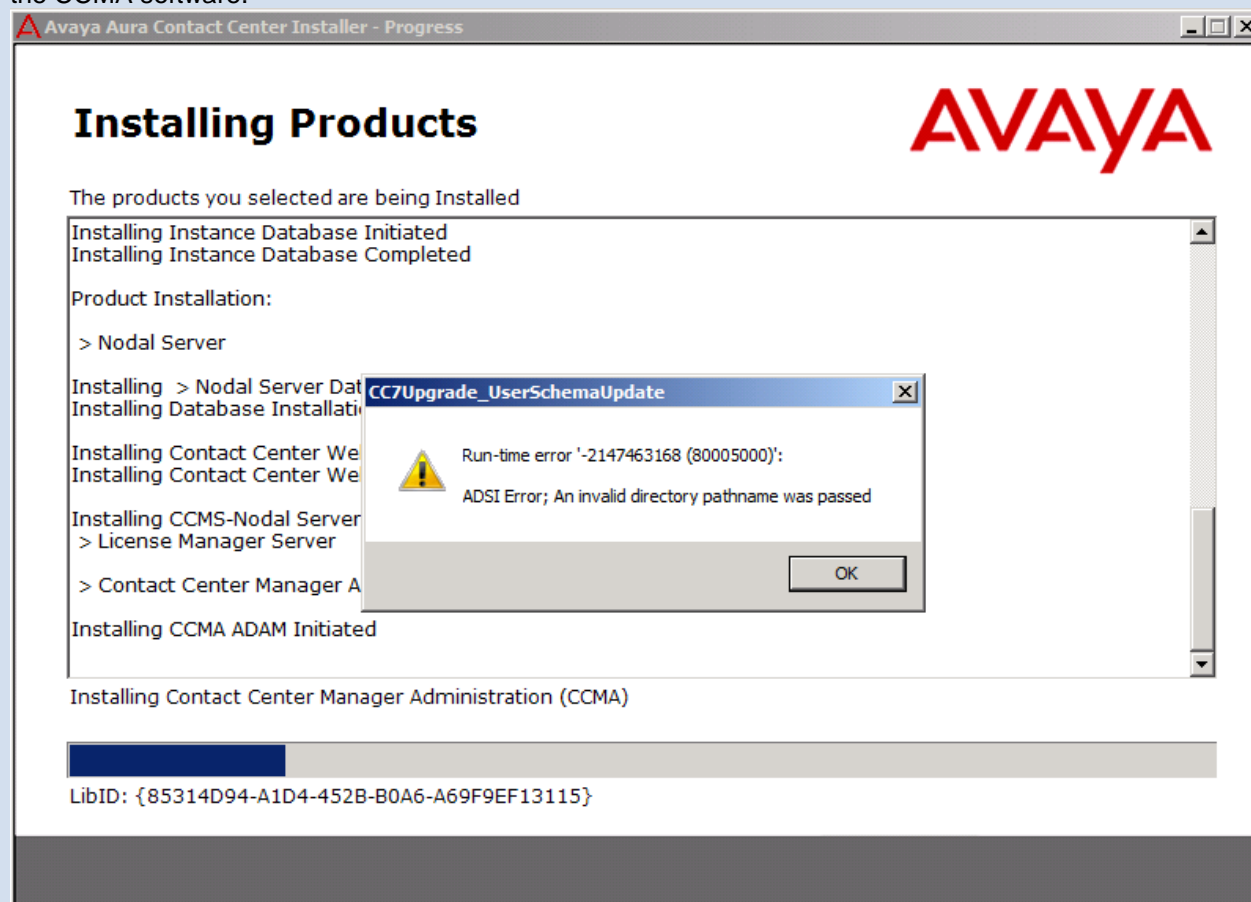
### CC-5054 Should have blank value in Agent to skillset assignment

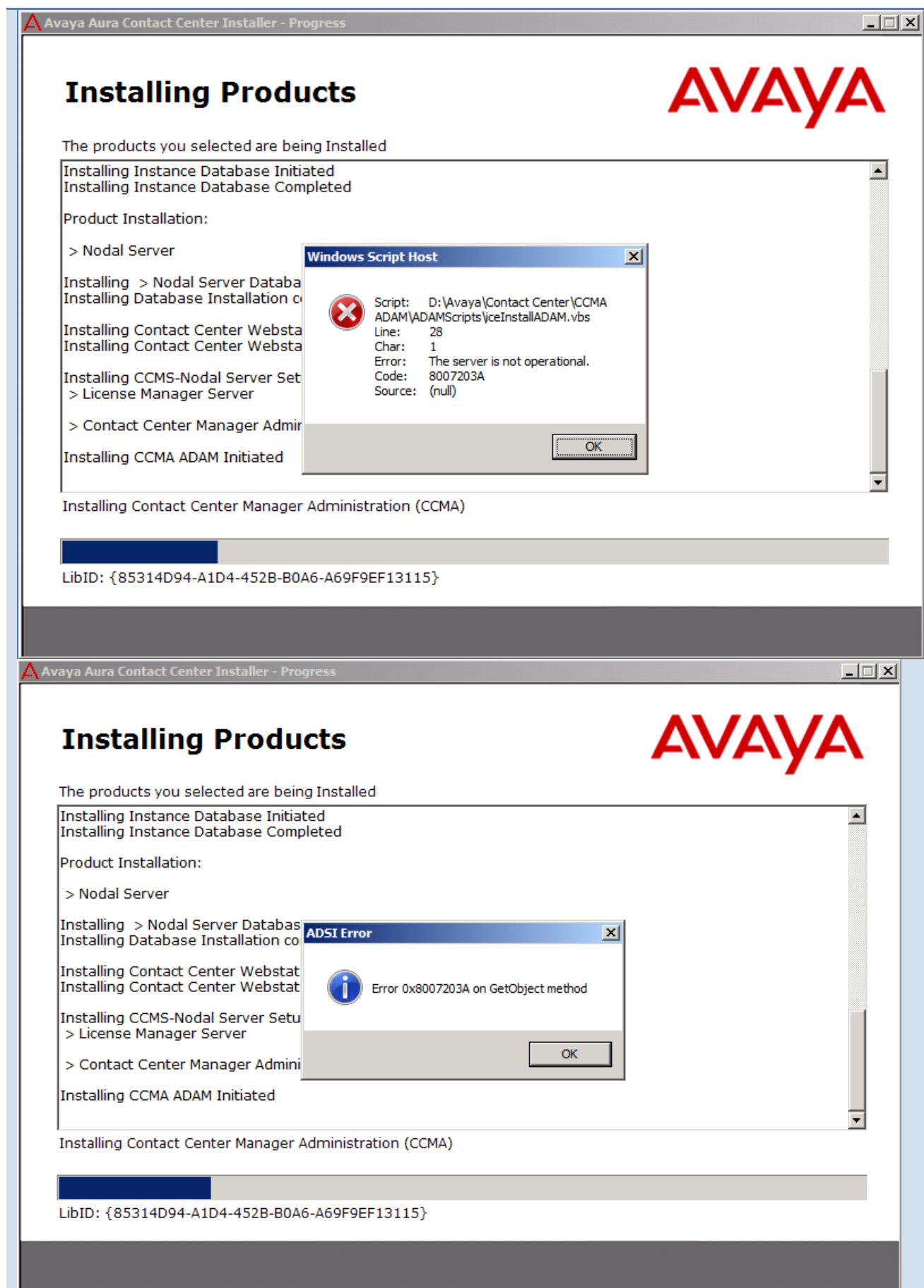
The 'blank' option is no longer selectable from the grid drop down list and the 'Update all agent...' priority drop down list in Agent to Skillset Assignment.

### AD-LDS errors appear during install but installation completes and reports success

In circumstances where a server which was on a domain has been restored from a virtual image or a ghost image, AD-LDS may fail to install correctly during the CCMA install. Several popup errors will appear during the install, but the CCMA install will continue and report success.

The errors are as a result of broken trust between the server and the domain due to the fact that it was restored from an image. The machine needs to be removed from the domain then re-added before installing the CCMA software.





---

**CCMA pages fail to load on some client machines but work ok on the server**

Certain CCMA pages appear to freeze while loading on some client PC's while the same pages work correctly when loaded on the CCMA server. This issue can be caused as a result of configuration settings on the network interface card, in particular certain Broadcom Gigabit Ethernet cards. This is a documented problem at the operating system and a workaround is available from Microsoft.

<http://support.microsoft.com/kb/951037>

---



---

**wi00822957 Update OpenInterfaces Web Services and SCE Web Services to support https/SSL**

The CCMA WCF Web Services need to be updated to support HTTPS/SSL.

WCF web services are limited in relation to SSL/nonSSL support. A single web.config cannot support both (This is a Microsoft limitation). CCMA has 2 WCF web services - SCE and Open Interfaces and it installs only the nonSSL versions by default. Therefore SCE/Open Interfaces fail if SSL is enabled.

In order to work around this limitation and allow SCE and Open Interfaces to work with SSL, you must do the following procedure:

1. Open a command prompt (DOS window)
2. Navigate to \avaya\contact center\Manager administration\server
3. Run `wcApplyChanges -i`

Note: if you ever need to revert back to a nonSSL setup, you will need to re-run the steps performed above.

---



---

**Migrating data between 6.x releases**

In the case where data from an earlier 6.x Service Pack is being migrated to a 6.4 CCMA server, the following command should be run to update the database: <installdrive>:\ Avaya\Contact Center \ Manager Administration\Apps\Sysops\RunCCMADataMigration.exe HROnly

---



---

**Unable to restore CCMA backup from server with multiple drives to a server that only has a single disk**

The CCMA restore utility does not allow the user to restore a CCMA backup taken from a server that has more than one disk drive (e.g. C:\ and D:\). A similar hardware configuration is required on the new server in order to support this restore.

---



---

**wi00785816 Agent Map only shows a single block for agents in a multiplicity environment**

Agent Map does not currently support reporting multiple contacts. It will correctly report on the primary contact (i.e. the equivalent of the agent's collapsed row in a Standard Agent tabular display)

---



---

**wi01058428 Internet Explorer terminates intermittently when downloading updated ActiveX controls**

The first time that Internet Explorer accesses CCMA after an upgrade it will download the updated ActiveX controls. In some cases IE may terminate immediately after the download. Restarting the browser fixes the problem and it will work correctly thereafter.

---

**wi01079087 CCMA unclear message cannot add users greater than Configured value for “Configured Agent IDs” in Historical statistics**

If the user attempts to add an agent when the maximum value for "Configured Agent IDs" or "Agent Positions" has been reached, a generic error message is returned. For example if the value for "Configured Agent IDs" in the Historical Statistics page is set to 900. Once this limit is reached, if the user then tries to create agent 901, the error message will be displayed. The same behavior is also true for the "Agent Positions" field. The user needs to increase the value of the "Configured Agent IDs" and "Agent Positions" in the Historical Statistics page, but this is not evident from the error message (see screenshots below).

The error message is as follows:

Error: Unable to save the users details.-2147220475:The number of items you are adding exceeds the currently configured maximum value. Increase the configured value on the Parameters page of the Historical Statistics Configuration window, and then try again.

| Parameters                          |                      |                  |                |              |
|-------------------------------------|----------------------|------------------|----------------|--------------|
|                                     | Parameter Name       | Configured Value | Measured Value | System Value |
| <input checked="" type="checkbox"/> | Agent Positions      | 500              | N/A            | 10050        |
| <input type="checkbox"/>            | Skillsets            | 150              | 25             | 1500         |
| <input type="checkbox"/>            | Calls per Hour       | 100              | 0              | 35000        |
| <input type="checkbox"/>            | DNISs                | 500              | 4              | 10000        |
| <input type="checkbox"/>            | CDNs                 | 15               | 5              | 2000         |
| <input type="checkbox"/>            | IVR ACD-DNs          | 10               | 2              | 150          |
| <input type="checkbox"/>            | Activity Codes       | 250              | 5              | 5000         |
| <input type="checkbox"/>            | Agent Events per Day | 32               | 0              | 10000        |

**Historical Statistics**

| Parameters                          |                       |                  |                |              |
|-------------------------------------|-----------------------|------------------|----------------|--------------|
|                                     | Parameter Name        | Configured Value | Measured Value | System Value |
| <input type="checkbox"/>            | Trunks                | 300              | 0              | 3000         |
| <input type="checkbox"/>            | Applications          | 100              | 15             | 1005         |
| <input type="checkbox"/>            | Nodes                 | 30               | 0              | 30           |
| <input type="checkbox"/>            | IVR Ports             | 0                | 0              | 1000         |
| <input checked="" type="checkbox"/> | Active Agents         | 500              | N/A            | 5000         |
| <input checked="" type="checkbox"/> | Configured Agents IDs | 200              | 17             | 10050        |
| <input type="checkbox"/>            | Supervisors           | 600              | 9              | 600          |

**wi01117618 Skillsets with special characters from NES 7 could not be searched on APM**

On NES7 there are some skillset names with special characters like: ß1, oan3&\_SK:land, oan3 & \_SK:land,... then migrated to AACCC 6.4. The skillsets are able to view correctly in Configuration -> Skillsets but they cannot be viewed at APM (Access and Partition Management) by searching agents by Skillsets. The list of skillsets is empty and you cannot search skillsets. CCMA 6.4 does not allow inputting those special characters. You need to manually delete those special characters at CCMA configuration when migrating NES7 to AACCC 6.4.

**wi01180065: Error on launching OCMT application from CCMA server with CGI (Common Gateway Interface) installed.**

The following error may appear when launching OCMT application from CCMA server.

## Server Error in Application "DEFAULT WEB SITE/OUTBOUND"

Internet Information Services 7.5

**Error Summary**

**HTTP Error 404.0 - Not Found**  
The resource you are looking for has been removed, had its name changed, or is temporarily unavailable.

**Detailed Error Information**

|                               |  |
|-------------------------------|--|
| ModuleIIS Web Core            | Requested URLhttp://ccmm-hoth:80/outbound/ocmt.application |
| NotificationMapRequestHandler | Physical PathD:\Avaya\Contact Center\Manager               |
| HandlerStaticFile             | Administration\Apps\Outbound\ocmt.application              |
| Error Code0x80070002          | Ligon MethodAnonymous                                      |
|                               | Ligon UserAnonymous  |

**Most likely causes:**

- The directory or file specified does not exist on the Web server.
- The URL contains a typographical error.
- A custom filter or module, such as URLScan, restricts access to the file.

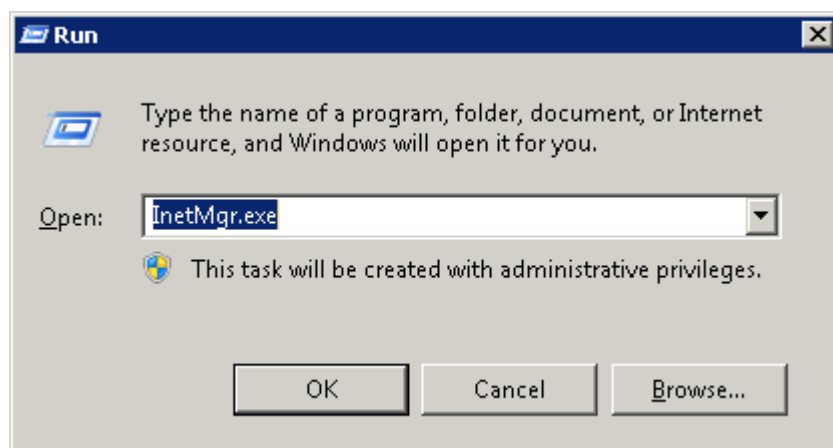
**Things you can try:**

- Create the content on the Web server.
- Review the browser URL.
- Create a tracing rule to track failed requests for this HTTP status code and see which module is calling SetStatus. For more information about creating a

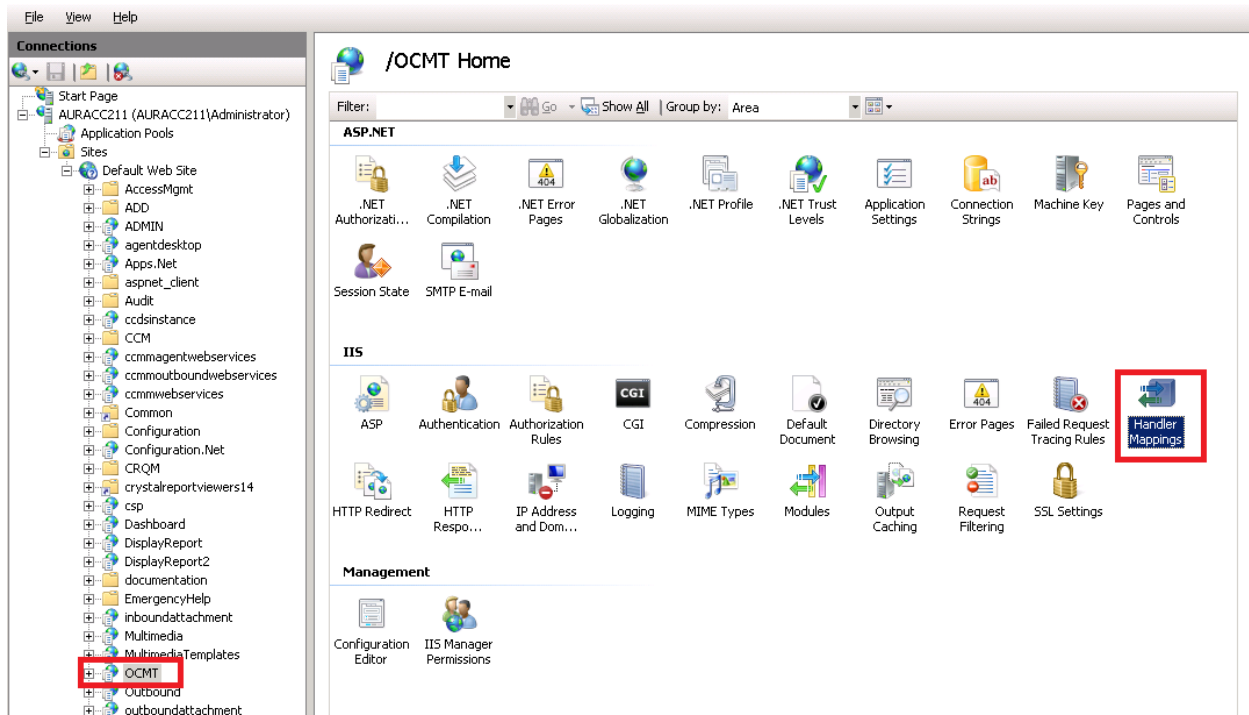
The root cause is the CGI is installed and enabled for the OCMT application in IIS. Disable the CGI resolve the issue.

Follow the steps below to disable the CGI

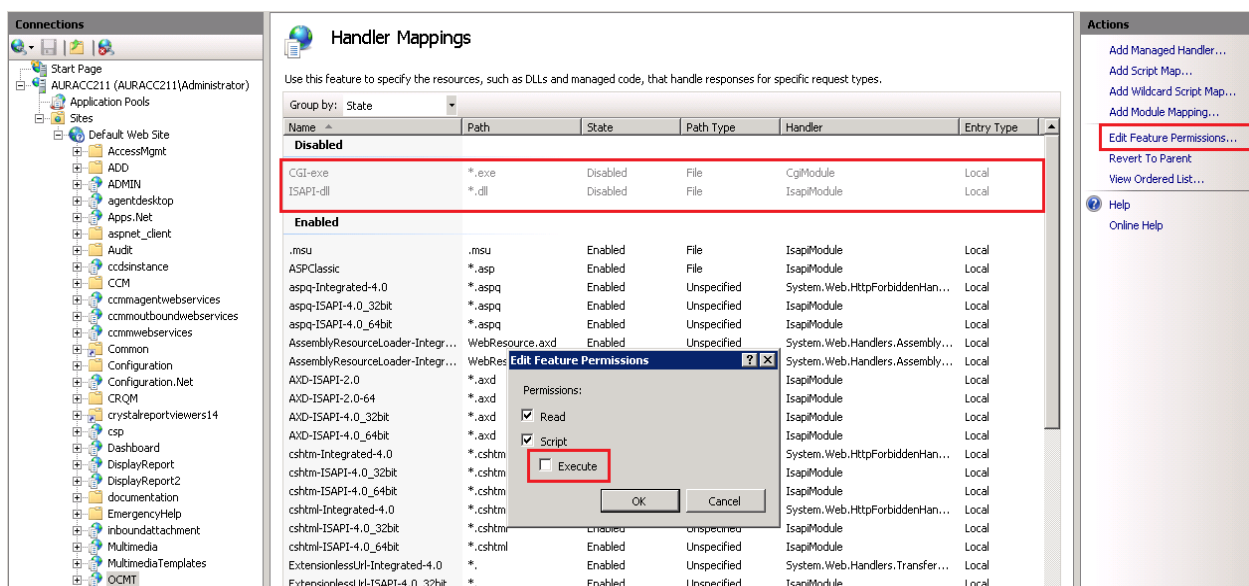
1. Open IIS management



2. Browse to OCMT application and open Handler Mappings



3. Select Edit Feature Permissions and un-check the Execute option.



### wi01181185 Reports failing to export or print when SSL is enabled on IIS

The issue happens on IE8, it does not happen on IE9 and IE10.

The cause is the IE checks if the file can be downloaded to the local Cache folder when user clicks to download a file. The report viewer window returns the headers that are failed by IE browser. Therefore the error appears.

Adding the new registry key is to notify the browser not to check caching when the file is downloaded.

The steps is to add the new registry key as followed:

- key value name: BypassSSLNoCacheCheck
- key value data: 1
- type: DWORD



- path:  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet  
Settings]

#### wi01185545 CCMA Prompt Partitioning shows all prompts after an AMS RGN switchover

CCMA users who have access to a limited set of prompts via the prompt management partitioning feature are able to see all prompts following a switchover to the RGN AMS.

This is the intended functionality as it is not possible to enforce prompt partitioning on the RGN node. Any changes made to prompt partitions will have to be re-applied following a switch back to the Active server.

#### wi01192964 Excel formula appears as text in Configuration Tool

When attempting to use a formula to populate fields in the Excel Configuration Tool, the formula appears as text within the cells rather than being evaluated.

This is due to the default formatting of the cells within the workbook which is "Text". The format can be changed to "General" on cells where formulae are required.

NOTE: Changing the format on cells where a formula is not being used is not recommended as it may lead to issues with configuration data e.g. leading zero's will be lost.

#### wi01207957 Accessing CCMA from Standby server returns HTTP error 500

When upgrading CCMA from SP10 to SP14(or higher) then rolling back to SP10 again, accessing CCM got the HTTP error 500. The root cause is .NET FW 4.0 has been installed on that server and SP10 does not work with .NET 4.0

Solution: Changing the version .NET FW 4.0 back to .NET FW 2.0 for CCMA Application Pools.

The screenshot shows the 'Application Pools' management console. On the left is a tree view with 'Application Pools' selected. The main area displays a table of application pools. A red box highlights the 'CCMA\_DefaultAppPool' row.

| Name                   | Status  | .NET Frame... | Managed Pipeli... | Identity               | Applications |
|------------------------|---------|---------------|-------------------|------------------------|--------------|
| CCMA_DefaultAppPool    | Started | v2.0          | Classic           | IUSR_SWC               | 7            |
| CCMA_ReportingPool     | Started | v2.0          | Classic           | IUSR_SWC               | 2            |
| CCMA_ReportViewersPool | Started | v2.0          | Classic           | IUSR_SWC               | 1            |
| Classic .NET AppPool   | Started | v2.0          | Classic           | ApplicationPoolIden... | 0            |
| DefaultAppPool         | Started | v2.0          | Integrated        | ApplicationPoolIden... | 4            |
| NT_WebServicesPool     | Started | v2.0          | Classic           | IUSR_SWC               | 29           |
| OI_WebServicesPool     | Started | v2.0          | Classic           | IUSR_SWC               | 1            |
| SCE_WebServicesPool    | Started | v2.0          | Classic           | IUSR_SWC               | 1            |

#### wi01201810 Historical Statistics duration need to increase to value of 1825

We have changed the limit from 999 days to 1825 (5 years) for historical stats in Duration section except two fields, "Length of Business day" and "Business week contains" because some customers may be impacted. If users have data which is older than 1825 days, it will be purged when the change is made. The following warning message will be shown if users input a value which is less than the old value:

"Reducing the duration for which historical statistics are stored will result in data older than <parameter> being deleted from the system. A CCMS backup should be taken before reducing the storage duration value. An offline data archiving solution should be considered where there are legal or regulatory requirements to retain data."



| Duration                       |       |
|--------------------------------|-------|
| Name                           | Value |
| Interval (days)                | 20    |
| Daily (days)                   | 31    |
| Weekly (weeks)                 | 26    |
| Monthly (months)               | 36    |
| IVR Voice Port (days)          | 3     |
| Agent login and logout (days)  | 3     |
| Length of Business day (hours) | 2     |
| Business week contains (days)  | 4     |
| Call-by-Call (days)            | 5     |
| Contact Success (days)         | 5     |

#### wi01222429 Document the difference of Service level value between RTD and HR

A customer site has requested to change the service level of RTD Application from 100% to 0%. They based on the document of Historical Report. However there is no that value in RTD documents. In CCMA SP16, the Service Level of RTD Application 100% needs to be documented in RTD documents when the calls answered and calls abandoned is 0.

#### wi01226405 Not able to create Private RTDs following recovery of AD-LDS replication

Create private copy of a public RTD on the two CCMA servers at a time that replication is not working (network disconnected or other cause).

The entries are created for each server, and while replication is down, and after replication is recovered, a renamed entry is replicated to the target server that has invalid characters. DisList.asp is unable to process the actions correctly because of the invalid characters, and RTD creation fails.

Remove the entries with “CNF---” in their name to resolve this issue. On CCMA server (Primary and Secondary), open ADSI Edit tool and find the “CNF” entries right click to delete them.

ADSI Edit

File Action View Help

Default naming context [localhost:389]

- DC=NortelNetworks;dc=com
  - CN=LostAndFound
  - O=NortelNetworks
    - OU=ICE
      - OU=AccessClasses
      - OU=AccessPartitions
      - OU=AccessStandardPartitions
      - OU=Charts
      - OU=Configuration
      - OU=Groups
      - OU=LicenseInfo
      - OU=RTDViews
      - OU=Servers
      - OU=StandardReportGroups
      - OU=Templates
    - OU=Users
      - CN=USER20110706221953069
        - OU=Servers
          - L=100.30.4.236
            - OU=RTDViews
              - OU=ServersCNF:53330dd1-677c-4fb8-b4af-b21d8afd09e2
            - OU=Templates
              - OU=RTDTemplates
                - OU=TemplatesCNF:1b9582bc-604e-4fd6-9505-e0aace1bc83c
          - CN=USER20150618101447403
          - CN=USER20150619144726839
          - CN=webadmin
        - CN=NTDS Quotas
        - CN=Roles

Configuration [localhost:389]

| Name  | Class      | Distinguished Name                                 |
|---|------------|--|
| CN=Display4                                       | iceRTDView | CN=Display4,OU=RTDViews,L=100.30.4.236,OU=Servers, |
| CN=Display5                                       | iceRTDView | CN=Display5,OU=RTDViews,L=100.30.4.236,OU=Servers, |
| CN=Display6                                       | iceRTDView | CN=Display6,OU=RTDViews,L=100.30.4.236,OU=Servers, |
| CN=Display6CNF:1ab0093a-af17-44ff-84cf-9f6e51e95c | iceRTDView | CN=Display6CNF:1ab0093a-af17-44ff-84cf-9f6e51e95c, |
| CN=HA_AURACC_Standard_Agent_...                   | iceRTDView | CN=HA_AURACC_Standard_Agent_Display,OU=RTDViews,   |
| CN=HA_AURACC_Standard_Applica...                  | iceRTDView | CN=HA_AURACC_Standard_Application_Display,OU=RTDV, |
| CN=KHoa_123                                       | iceRTDView | CN=KHoa_123,OU=RTDViews,L=100.30.4.236,OU=Server   |

#### After installing CCMA patch, the sites who are using HTTPS cannot launch OD, force logout Agent

Some CCMA patches install all CCMA webservises including web.config files. This causes the current

web.config files on CCMA server overwritten and lost all SSL settings.  
The sites who are using HTTPS cannot launch OD, use Force Logout feature,...

**Workaround:**

Run **wcApplyChanges -i** after installing the CCMA patch.  
(Open CMD, type **wcApplyChanges -i** and run).

---

**wi01222657    Slow CCMA**

AACC 6.4 SP13 German has slow response from standalone CCMA after SP13 upgrade, APM is slow to list all CCMA users as well as Orchestration Designer fails to load intermittently.

w3wp.exe dump file is collected and analyzed, it is found that the IIS AppDomain is forced to be restarted due to the file properties changes in the CCMA Application, therefore CCMA does not work properly and gets slow to response.

Suggest checking the Anti Virus scan on the customer server to see if the scan is performed on the file set of CCMA Application. Anti Virus scan is able to modify the file properties when scanning and it leads to CCMA AppDomain restart.

**Workaround:**

Exclude the CCMA file set from the Anti Virus scan, CCMA file properties will not be changed and the AppDomain is not restarted, CCMA is back to work normally.

---

**wi01225390    Not able to manage media prompts via CCMA Prompt management. Conversion failed for Account Type**

Unable to add any new content namespace and media content via CCMA Prompt management. Message "The system was unable to connect to the media server. Please contact your administrator" is displayed in CCMA.

**Workaround:**

Add managed IP, active IP and standby IP into AMS SOAP trusted node list.

---

**wi01234619                    Unable to login to OD since enabling SSL**

Users could not log on to OD after enabling SSL on CCMA server. The following error message appeared: "Unable to connect to Contact Center: Could not send message".

**Workaround:**

Make sure SCE web service works. Try the following link and no error is shown on IE.

<https://<managedFQDN>/WebServices/SceService/service.svc> or  
<https://<CCMAserver>/WebServices/SceService/service.svc>

There is a known issue. If that CCMA server is using SSL 3.0 (SSL v3.0 in the registry), OD will NOT work with SSL 3.0. The work-around is to remove SSL3.0 registry keys:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\  
Remove : **SSL 3.0\Client**

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\  
Remove: **SSL 3.0\Server**

---

**CC-6682 Prompt cannot be downloaded in Prompt Management page**

---

A prompt cannot be downloaded in CCMA Prompt Management page, the error is displayed stating that 'An error occurred. Please contact your Administrator'.

When a prompt is downloaded on the Prompt Management page, firstly the media file is copied to the TempMediaStorage folder on the CCMA server (D:\Avaya\Contact Center\Manager Administration\Apps\Configuration\PromptManagement) before it is posted back to the client browser for user to save it anywhere else. The root cause is The Prompt Management is unable to overwrite an existing media file in the folder when a prompt is downloaded, therefore an error message is displayed (It should be more detailed error message instead of a generic message).

In a working server, an existing media file can be overwritten multiple times but if the existing media file is damaged somehow on a server, it cannot be overwritten by Prompt Management. There may be reasons for this failure: the file attributes are changed by Anti-Virus application, the newly changed policy in computer domain or the media file is just corrupted.

**Workaround:**

The TempMediaStorage folder must be cleaned up for the download to work normally.

---

---

**CC-7182 Supervisors show no agent lists in CCM**

---

In CCM, when a supervisor is selected, CCMA fails to display the two lists of agents.

Error message: "No agents have been assigned to the selected supervisor" and "There are currently no agents available to assign" are displayed when selecting a supervisor in Contact Center Management.

Issue could happen on some supervisors only, not all the supervisors.

**Workaround:**

The CCMS database field "ExternalServer" of the ccms.NIUser table contains some invalid characters which can be caused by migration from 6.1 or 6.2 release. Workaround is to re-set the value to empty for the "ExternalServer" field and no more problem going forward.

---

---

**CC-6779 Unable to login to CCMA after migrating the NES6 data**

---

When migrating from NES6 to 6.4 SP15 ACCS, the migration process will rename the user "webadmin" to "Administrator" in AD LDS. However, if the NES6 backup database also has another user named "administrator", the rename function will be failed. It said that "The object already exists.". It results in the ACCS default "Administrator" user is not converted completely. So, after migration finishes, user cannot log in to CCMA by default Administrator.

**Workaround:**

Users need to modify the legacy administrator account prior to taking the NES CCMA backup. That step prevents conflict when ACCS administrator account is installed during the migration.

Users need to check their accounts with the following account names. If they are existed, their names need to be modified before taking the NES CCMA backup.

1. "Administrator"
2. "reporting1"
3. "reporting2"

4. "accsync"
5. "webadmin"
6. "AgentGreeting"

## CC-6234 high w3wp CPU at time of congestion causing defaulted calls

The high workload of ADD's client requests causes CPU usage 100% at a time.

### Workaround:

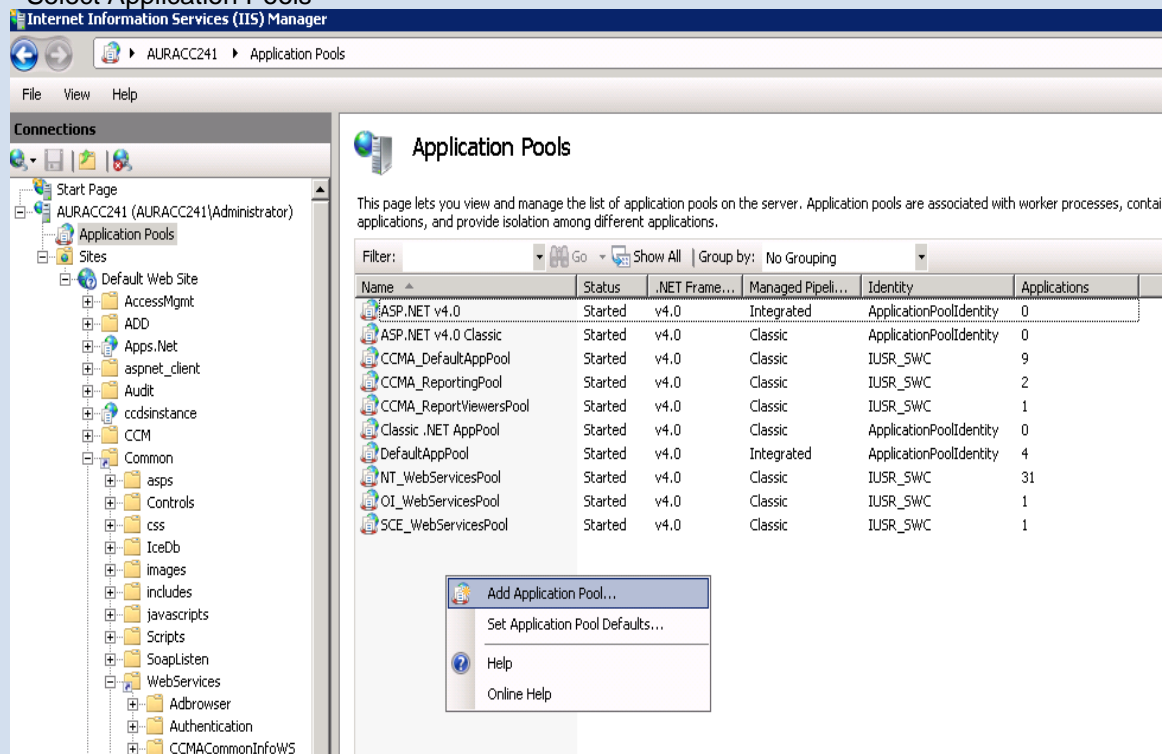
ADD applications will use a new web service pool which is separate from NT\_WebServicesPool that CCMA users are using. Users also can change the "cacheTimeoutMinutes" value from 1 minute (default value) to 2 minutes. This configuration file, web.config file is located at D:\Avaya\Contact Center\Manager Administration\Apps\Common\WebServices\SOAPADD.

The "cacheTimeoutMinutes" value is used to refresh the list of agent skillsets and the list of agent status in the web service cache. The data of ADD applications will be queried from this cache instead of getting it from DB.

The following steps show how to create a new ADD Pool and move ADD's webservices from NT\_WebServicesPool to this new pool. It also shows how to set Processor Affinity to limit CPU usage for ADD requests so that all ADD's just use 2 processor cores. Other processors will not take high CPU usage when there are a huge number of ADD client requests.

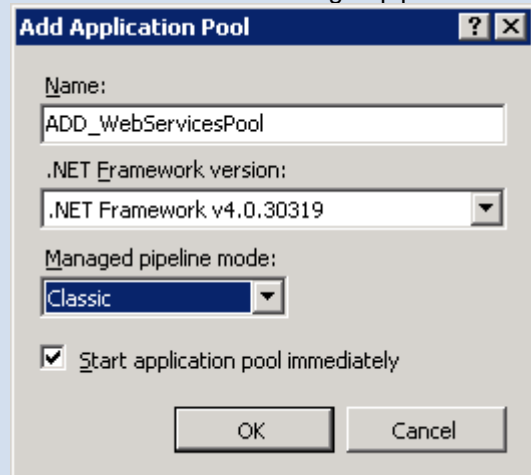
1. From Windows, open "Internet Information Services (IIS) Manager"

- Select Application Pools



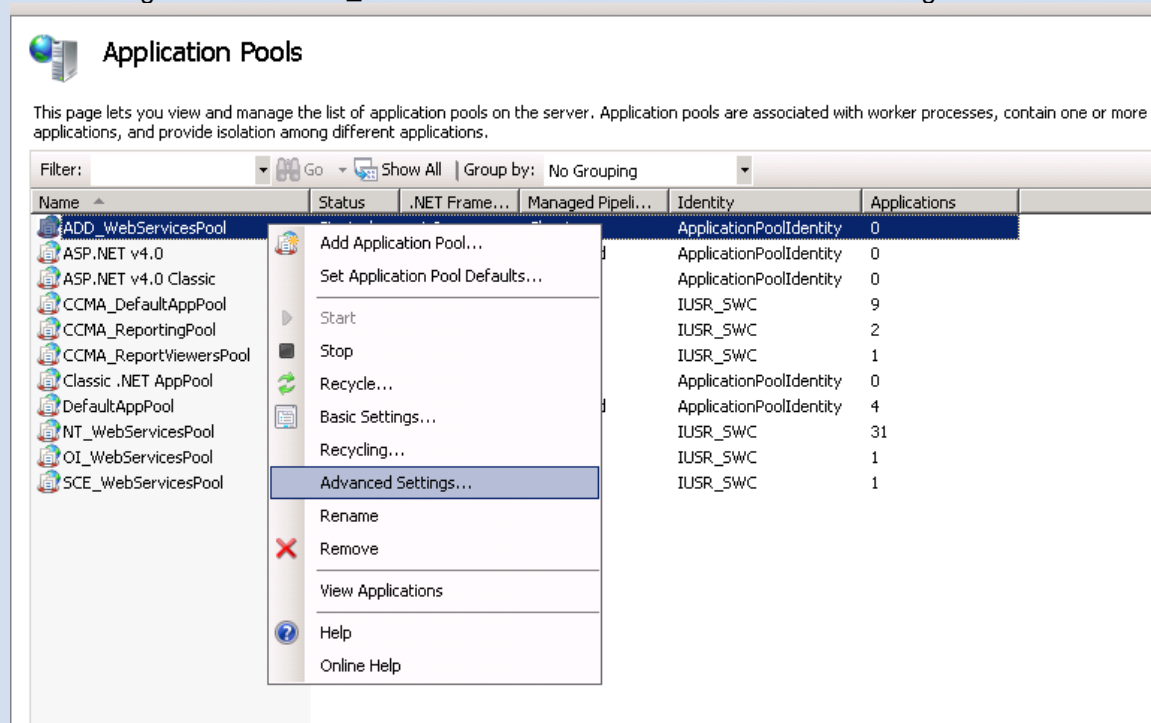
- Right click on the right hand side and select "Add Application Pool..."
- Input ADD\_WebServicesPool into the Name field
- Select .NET FW v4.0

- Select Classic from Managed pipeline mode



- Click OK

After that right click on "ADD\_WebServicesPool" and select "Advanced Settings..."



- Set True for Enable 32-Bit Applications

**Advanced Settings**

**(General)**

|                            |                     |
|----------------------------|---------------------|
| .NET Framework Version     | v4.0                |
| Enable 32-Bit Applications | True                |
| Managed Pipeline Mode      | Classic             |
| Name                       | ADD_WebServicesPool |
| Queue Length               | 1000                |
| Start Automatically        | True                |

**CPU**

|                            |            |
|----------------------------|------------|
| Limit                      | 0          |
| Limit Action               | NoAction   |
| Limit Interval (minutes)   | 5          |
| Processor Affinity Enabled | False      |
| Processor Affinity Mask    | 4294967295 |

**Process Model**

|                                      |                         |
|--------------------------------------|-------------------------|
| Identity                             | ApplicationPoolIdentity |
| Idle Time-out (minutes)              | 20                      |
| Load User Profile                    | False                   |
| Maximum Worker Processes             | 1                       |
| Ping Enabled                         | True                    |
| Ping Maximum Response Time (seconds) | 90                      |
| Ping Period (seconds)                | 30                      |
| Shutdown Time Limit (seconds)        | 90                      |
| Startup Time Limit (seconds)         | 90                      |

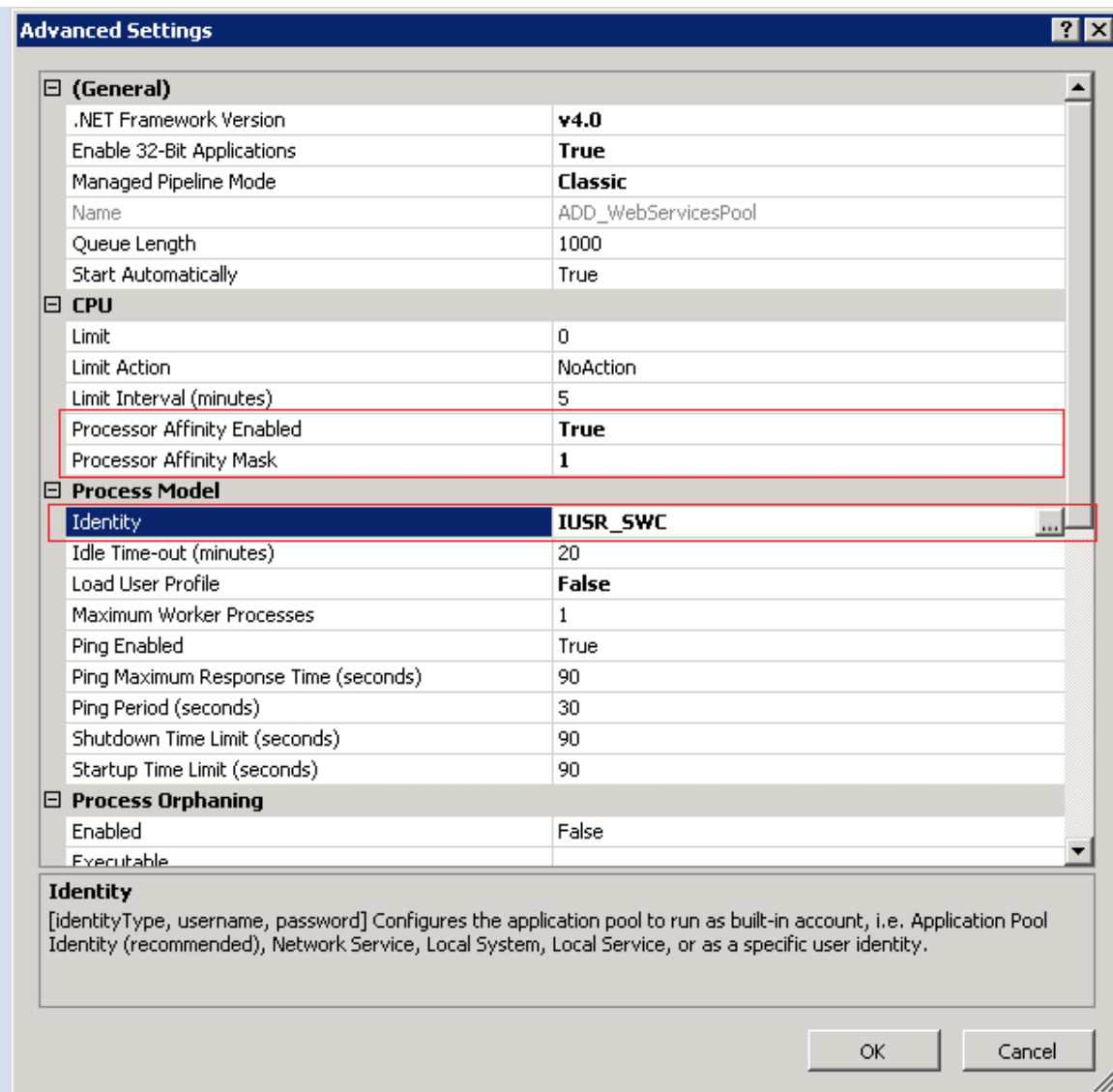
**Process Orphaning**

|            |       |
|------------|-------|
| Enabled    | False |
| Executable |       |

**Enable 32-Bit Applications**  
 [enable32BitAppOnWin64] If set to true for an application pool on a 64-bit operating system, the worker process(es) serving the application pool will be in WOW64 (Windows on Windows64) mode. Processes in WOW64 mode are 32-bit processes that load only 32-bit applications.

OK Cancel

- Set True for Processor Affinity Enabled
- Set 48 for Processor Affinity Mask (5th & 6th processor will be used by pool.)  
 '48 is a hexadecimal 0x110000 mask 5th and 6th bit
- Set IUSR\_SWC user for Identity. It will require the password of iceadmin when we input this user.  
 Requirement: to know the password for the iceadmin user. If password is not known, set the password to a known value using the iceadmin password change procedure in CCMA Configuration.














- Click OK from Advanced Setting
- The ADD\_WebServicesPool is created as the following picture



## Application Pools

This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

| Filter:  |         | Go            | Show All          | Group by: No Grouping   |              |
|--|---------|---------------|-------------------|-------------------------|--------------|
| Name   | Status  | .NET Frame... | Managed Pipeli... | Identity                | Applications |
|  ADD_WebServicesPool    | Started | v4.0          | Classic           | IUSR_SWC                | 0            |
|  ASP.NET v4.0           | Started | v4.0          | Integrated        | ApplicationPoolIdentity | 0            |
|  ASP.NET v4.0 Classic   | Started | v4.0          | Classic           | ApplicationPoolIdentity | 0            |
|  CCMA_DefaultAppPool    | Started | v4.0          | Classic           | IUSR_SWC                | 9            |
|  CCMA_ReportingPool     | Started | v4.0          | Classic           | IUSR_SWC                | 2            |
|  CCMA_ReportViewersPool | Started | v4.0          | Classic           | IUSR_SWC                | 1            |
|  Classic .NET AppPool   | Started | v4.0          | Classic           | ApplicationPoolIdentity | 0            |
|  DefaultAppPool         | Started | v4.0          | Integrated        | ApplicationPoolIdentity | 4            |
|  NT_WebServicesPool     | Started | v4.0          | Classic           | IUSR_SWC                | 31           |
|  OI_WebServicesPool     | Started | v4.0          | Classic           | IUSR_SWC                | 1            |
|  SCE_WebServicesPool    | Started | v4.0          | Classic           | IUSR_SWC                | 1            |

2. Move ADD's Webservices from NT\_WebServicesPool to ADD\_WebServicePool
- Right click on NT\_WebServicePool and select View Applications



## Application Pools

This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

| Filter:  Go  Show All   Group by: No Grouping |         |               |                   |                         |              |  |
|---|---------|---------------|-------------------|-------------------------|--------------|--|
| Name  | Status  | .NET Frame... | Managed Pipeli... | Identity                | Applications |  |
| ADD_WebServicesPool                           | Started | v4.0          | Classic           | IUSR_SWC                | 0            |  |
| ASP.NET v4.0                                  | Started | v4.0          | Integrated        | ApplicationPoolIdentity | 0            |  |
| ASP.NET v4.0 Classic                          | Started | v4.0          | Classic           | ApplicationPoolIdentity | 0            |  |
| CCMA_DefaultAppPool                           | Started | v4.0          | Classic           | IUSR_SWC                | 9            |  |
| CCMA_ReportingPool                            | Started | v4.0          | Classic           | IUSR_SWC                | 2            |  |
| CCMA_ReportViewersPool                        | Started | v4.0          | Classic           | IUSR_SWC                | 1            |  |
| Classic .NET AppPool                          | Started | v4.0          | Classic           | ApplicationPoolIdentity | 0            |  |
| DefaultAppPool                                | Started | v4.0          | Integrated        | ApplicationPoolIdentity | 4            |  |
| NT_WebServicesPool                            |         |               |                   | IUSR_SWC                | 31           |  |
| OI_WebServicesPool                            |         |               |                   | IUSR_SWC                | 1            |  |
| SCE_WebServicesPool                           |         |               |                   | IUSR_SWC                | 1            |  |

- Add Application Pool...
- Set Application Pool Defaults...
- Start
- Stop
- Recycle...
- Basic Settings...
- Recycling...
- Advanced Settings...
- Rename
- Remove
- View Applications
- Help
- Online Help

- Right click on "/Common/WebServices/SOAPADD" and select "Change Application Pool"



**Applications**

This page lets you view and manage the list of applications. Applications contain content and code.

The applications have been filtered by the NT\_WebServicesPool application pool.

[Remove filter](#)

Filter:  Go  Group by: No Grouping

| Virtual Path                        | Physical Path                            | Site             | Application Pool    |
|-------------------------------------|--|------------------|---------------------|
| /Common/WebServices/SOAPADD         | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /Dashboard                          | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /Multimedia                         | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /Outbound                           | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /SWCCommon/WebServices/CCMA...      | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/Adbrowser              | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/Authentication         | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/CCMMProxyInterfaces    | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/CCTProxyInterfaces     | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/CMFProxyInterfaces     | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/DataManagerWs          | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/IPOfficeWSRestClient   | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/MPCWS                  | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/RealtimeDashboardWS    | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/SOAPCCMANXML           | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/SOAPFltFuncs           | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/SOAPICertdService      | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/SOAPParameterRPT       | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/SOAPRepAgents          | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/SOAPReportOAMWrapper30 | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/SOAPRptFuncs           | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/SOAPSCCSAgToSk30       | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/SOAPSCCSAgToSup30      | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/SOAPSCCSRDScheduler30  | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/SOAPSCcsRDSUsers30     | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/SOAPScriptingWrapper   | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/SOAPWrapper            | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/SOAPWrapperCommon      | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/SOAPWrapperSites       | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/SOAPWrapperUsers       | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/SOAPWSEScriptBasicCOM  | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |

- Select ADD\_WebServicePool and click OK

**Applications**

This page lets you view and manage the list of applications. Applications contain content and code.

The applications have been filtered by the NT\_WebServicesPool application pool.

[Remove filter](#)

Filter:  Go  Group by: No Grouping

| Virtual Path                      | Physical Path                            | Site             | Application Pool    |
|-----------------------------------|--|------------------|---------------------|
| /Common/WebServices/SOAPADD       | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /Dashboard                        | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /Multimedia                       | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /Outbound                         | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /SWCCommon/WebServices/CCMA...    | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/Adbrowser            | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/Authentication       | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/CCMMProxyInterfaces  | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/CCTProxyInterfaces   | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/CMFProxyInterfaces   | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/DataManagerWs        | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/IPOfficeWSRestClient | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/MPCWS                | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/RealtimeDashboardWS  | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/SOAPCCMANXML         | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |
| /WebServices/SOAPFltFuncs         | D:\Avaya\Contact Center\Manager Admin... | Default Web Site | NT_WebServicesPo... |

**Select Application Pool**

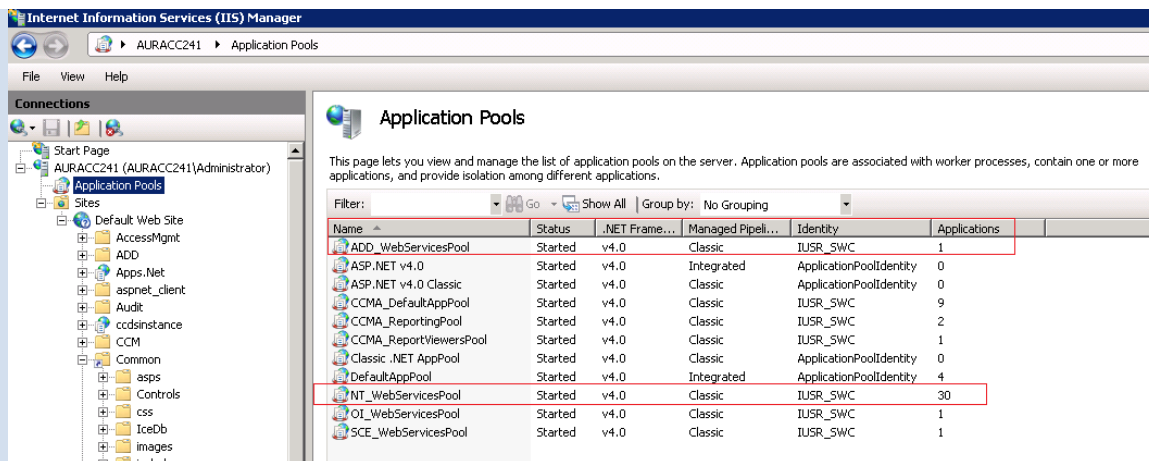
Application pool: **ADD\_WebServicesPool**

Properties:

.Net Framework Version: 4.0  
Pipeline mode: Classic

OK Cancel

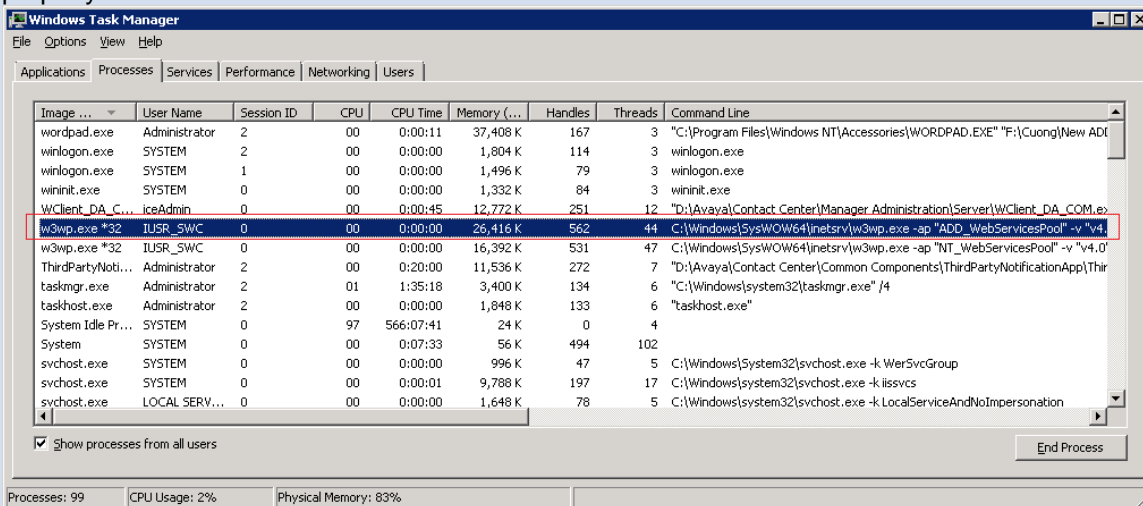
- Select Application Pool. We will see ADD\_WebServicePool has 1 application and NT\_WebServicesPool has 30 applications



- In IIS, select the ADD\_WebServicePool. Right click on that pool and select Stop.
- Start ADD to test the new Pool to make sure ADD works properly



- Open Windows Task Manager and see the ADD\_WebServicesPool is started and used by ADDs properly.



If the ADD\_WebServicesPool is not started automatically, right click the pool and press Start.

### 3. How to change the "cacheTimeoutMinutes" value.

- Open web.config file located at D:\Avaya\Contact Center\Manager Administration\Apps\Common\WebServices\SOAPADD folder
- Change the value 1 to 2.

For example:

```
<add key="cacheTimeoutMinutes" value="2"/>
```

### **Event ID 4353 intermittently appears in the Windows Application Event Log.**

Event 4353 is logged in the Windows Application Event Log intermittently, the event message is: 'The keycode assembly, BusinessObjects.Licensing.KeycodeDecoder.dll, cannot be loaded.' Customers are concerned there is an issue with the product since the message appears has an error in the Windows Event Log.

SAP Crystal Reports contains references to the BusinessObjects.Licensing.KeycodeDecoder.dll file which is no longer shipped with the product. The file is no longer required; however, the references cause this error to appear in the Application Event Log.

#### **Workaround:**

The issue has been escalated to SAP; it is a known issue and does not cause any impacts in the Crystal Reports product.

### **Sometimes, users cannot login CCMA. CCMA displays error that an invalid User ID/Password combination has been entered**

Sometimes, users cannot login in CCMA. Even though users input correct User ID and Password, CCMA displays an error that an invalid User ID/Password combination has been entered.

The root cause is that in Windows Server 2008 the User Profile Service will force the unloading of a user profile when that user logs off. DCOM objects in CCMA are run using a specific account. When this account is logged off, its user profile is unloaded and DCOM processes may not function properly. For more details, please refer to Microsoft link <http://support.microsoft.com/kb/2287297>.

#### **Workaround:**

The resolution is to modify the default behavior of the User Profile service. This is done by enabling the policy setting "Do not forcefully unload the user registry at user logoff". When enabled, the User Profile Service will not forcefully unload the registry. Instead it waits until no other processes are using the user registry before it unloads it. The policy can be found in the group policy editor (gpedit.msc). The policy is located under:

Computer Configuration->Administrative Templates->System-> User Profiles  
'Do not forcefully unload the user registry at user logoff'

Change the setting from "Not Configured" to "Enabled" which disables the new User Profile Service feature.

Reboot CCMA.server after this change has been made.

### **CC-10975**

#### **SP16: Cannot launch CCMA**

The issue has been recently seen at customer site where after SP16 upgrade, CCMA was inaccessible due to a HTTP 500 Internal Server error. IIS logs showed numerous instances of the following error:

```
2016-10-05 15:38:18 172.29.24.78 GET /
[26]800a0030|Error_in_loading_DLL: '_nbcmdObj.LoadNBComd' 80 - 172.29.24.78
```

Mozilla/5.0+(compatible;+MSIE+9.0;+Windows+NT+6.1;+WOW64;+Trident/5.0) 500 0 0 682

#### **Workaround:**

Register nbcom\_loader.dll by opening a cmd and running the following command:

```
> regsvr32 "D:\Avaya\Contact Center\Manager Administration\Server\nbcom_loader.dll"
```

### **CC-10331**

#### **AACC 6.4 SP15: Primary SFW unable to complete backup**

Co-resident CCMA and SFW server is unable to complete either an immediate SFW backup or a SFW scheduled backup. CCMA backups were completing without error, but now are generating the same error during both scheduled and ad hoc backups as SFW. However, the ad hoc CCMA backup creates what seems to be a viable backup as the file size matches previously successful backup file sizes. The scheduled backup truly fails as the output file size is only 1 KB. The SFW user interface returns the following message:

"Error found during backup. Error details are stored in D:\Avaya\Logs\SFW\SFWBackupRestore.log"

A SFW database backup file is created, but is only 1 KB large.

#### **Workarounds:**

##### **SFW workaround**

1. Set is/Running to false. (HKLM\SOFTWARE\Wow6432Node\JavaSoft\Pers\com\avaya\cnd)
2. Stop all of SFW services and re-start them.
3. Wait for 5 to 10 minutes.
4. Open a cmd that runs as administrator and input the following commands:  
D:>cd "D:\Avaya\Contact Center\Security Framework\bin"  
D:\Avaya\Contact Center\Security Framework\bin > "C:\Program Files (x86)\Java\jre6\bin\java" -DHTTP\_TLS\_PORT="8443" -jar "backupRestoreQuantum.jar" -b "D:\Avaya\Contact Center\Security Framework\QuantumBackup.zip"
5. Wait for 30 minutes and the command result is OK.
6. Rename sfwBku.exe to sfwBku.exe\_org and rename the updated file sfwBku.exe\_update got from CC-10331 to sfwBku.exe and copy it into "D:\Avaya\Contact Center\Security Framework\Backup" folder.
7. Run the application "Backup and Restore" from Security Framework and backup SFW.

##### **CCMA workaround**

1. Rename ccmaBk.exe to ccmaBk.exe\_org. It is located at "D:\Avaya\Contact Center\Manager Administration\Apps\SupportUtil" folder.
2. Rename the file (ccmaBk.exe\_update) got from CC-10331 to ccmaBk.exe and copy it into "D:\Avaya\Contact Center\Manager Administration\Apps\SupportUtil" folder.

3. Run the CCMA backup again using the Backup and Restore utility.

The CCMA workaround was necessary because when you back up CCMA, a SFW backup is also created. The workaround ensures the SFW backup is not taken again – it uses the SFW backup file that existed before.

## Communication Control Toolkit

### **wi00795012 Blank address appears after launching CCT WebAdmin**

After launching the CCT WebAdmin using IE, the browser flags a dialog asking to add a blank URL <http://> even if the CCT server address has been added as a trusted site.

Workaround: Click the cancel button to continue or selection the option to not present the dialog in future and continue.

### **wi01075843 AACC6.2\_AML\_SP9\_CS1K7.65P RefClient is hold automatically after complete 4 parties with CDN call**

1. Agent 1 makes call CDN call to Agent 2 by RefClient
2. Agent 2 answers the call
3. Agent 1 makes a conference call to Agent 3 and completes conference
4. Agent 1 makes a conference call to Agent 4 and completes the conference on RefClient, but the info on contact is showed held in RefClient of Agent 1

Workaround: There is no workaround for this issue, a "ConferenceComplete" event is not being sent by the CS1000. A CS1000 WI01074653 has been raised.

### **AML agent state reported incorrectly**

If an AML agent attempts to logout of AACC while on a Posn ID call, CCT will display the agent as "Logged Out" while the CS 1k reports the agent as in a Pending Logged Out until the Posn ID call drops at which stage the agent gets logged out automatically.

The Pending Logged Out stage can be cancelled by an agent by clearing the Make Set Busy request. After this step CCT is out of synch with the CS 1k. To resolve this issue the Agent must manually logout of the phone set and log back in via the CCT client.

### **wi01212881 AACC6.4 SP16 Ref– The Error Exception is thrown if supervisor un-tick observed agent while agent is logout then login**

1. Login agent1 and agent/sup2 onto Ref-client.
2. Agent/sup2 open observe window then tick agent check box. Do not close this window.
3. We logout agent1.
4. We re-login agent1.
5. Back to observed window on agent/sup2, we un-tick agent check box.
6. Agent/sup2 click x button to close observed window. there is error exception and we cannot close observed window.

Workaround: Click Quit button to close the Ref client and associated Observe window.

## Contact Center Multimedia

### Multimedia Only Install

In a multimedia only install, the outbound contact is still visible and can be assigned to an agent. This will cause an issue on login as Outbound license is not available on Multimedia only install. Do not assign the Outbound contact type to agents on a multimedia only install.

### WI00783464 CCMM8: Agent browser incorrect after uninstall of .NET 3.5

After uninstalling the Microsoft .NET 3.5 framework on an Agent desktop. Launching Agent Desktop does not detect that .NET 3.5 isn't on the client. This is due to Internet Explorer passing incorrect information about its environment to CCMM server. This is a core Microsoft issue.

### WI00784615 AAAD performance in a high latency network

Running AAAD over a network with high latency will adversely impact its performance. AAAD should run over a network with sufficient speed and bandwidth. Minimum requirements for the network are specified in the P&E guide.

### WI00793563 CCMM: MCMC Service restarting after service shutdown on SIP/CoRes Systems

The MCMC service restarts intermittently after getting shutdown. This is due to the service recovery settings in Windows Service Control. By default these are set to restart the service after 1 minute if it terminates. On shutting down the MCMC service there is an intermittent issue where the service terminates instead of shutting down cleanly hence the service is restarted by service recovery.

Workaround(to get MCMC service to remain shutdown):

Switch off the failure recovery in Windows Service manager using the following steps:

1. Launch Start->Run
2. Enter "services.msc" and enter
3. Select the service "CCMM Multimedia Contact Manager", Right click and select properties.
4. Select the "Recovery" tab.
5. Change the settings under First, Second and Subsequent failures from "Restart the Service" to "Take no Action"

Note: Setting should be changed back to "Restart the Service" when system operational.

### wi00932192 AACC services not starting after patching a full Multimedia cores system

On a system where CCMM is co-resident with AACC, an important registry key may get overwritten during patching. In order to install a new Service Pack, any older Service Pack has to be removed, so, for a time only the base software is on the machine. If the base CCMM services start, the LSHost registry key can be updated to an incorrect value for the co-resident system, causing start-up problems for the AACC after patching is complete.

Workaround: After installing the new Service Pack, run Server Config to fix the LSHost registry key.

### wi00891414 Mail Attachments do not backup when path/filename exceeds 255 characters

Note: A fix for this issue was delivered in SP6 to prevent new attachments exceeding 255 characters. However, workaround information is still required for customers upgrading from prior releases.

Mail Attachments do not get backed up if path/filename is over 255 characters. This is due to a limitation of NTFS. The following error will be reported in logs when attempting a backup ERROR #5001: xcopy - Initialization error (not enough memory or disk space, invalid drive, or syntax error)  
This error does not indicate a failure of the database backup rather a failure to back up the attachment folders.

Workaround: Copy the attachment files directly out of the subfolder to the location you require the files stored.



**wi00992664 AAAD doesn't display status of agent on Web Comm. when customer is typing message from Firefox Browser.**

In Webcomms SDK customer user typing notification is disabled in Firefox because of Firefox's inability to handle user-typing updates without losing displayed characters.

If desired functionality is required recommend customers use IE or Chrome

**wi01011000 SIP CS1K - AACC6.2 SP6 – IM - Presence tab is disappeared on login page of Agent after upgrading from an older SP**

When upgrading your CCMM server from an older SP to AACC 6.3, you first must remove the old SP software. This action will remove the settings on your CCMM Administrator that were newly introduced in the AACC 6.1/6.2. These settings should be recorded before this process is started and will need to be manually reset in the CCMM Administration tool after the upgrade to 6.3 is finished.

**wi01029680 AACC 6.2 SP6 - Default welcome message overwritten during SP uninstall**

The Default Welcome Message for webchat is overwritten by the default Avaya message after SP install. The message is updated by the base install after one SP is removed and before next SP is installed.

Note: this issue does not occur for Welcome Messages configured per skillset. Issue is specific to the Default Welcome Message when no Welcome Message is configured for a skillset.

Workaround: After the SP install update the default welcome message to the desired text.

**wi00851137 CCMM overwriting licensing LSHost & Type values**

Upgrading from one CCMM patch level to another may cause LM registry key to be incorrectly updated. The LSHost & Type keys located at HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Nortel\LM may be overwritten.

This means CCMS services do not start after the CCMM patch has been installed

Workaround: To stop this issue occurring, once the CCMM patches have been applied, if CCMS ServerConfig is run, it will set the LS\_Hosts registry key to the correct value.

**wi01048027 AAAD uses ctrl-home macro in email handling operation.**

AAAD uses ctrl-home macro when it is handling emails. If 3<sup>rd</sup> party applications are deployed on the same PC as AAAD, agents should not be using the ctrl-home macro to access this application as this short cut could be invoked inadvertently using AAAD.

Workaround: Use different macros instead of ctrl-home.

**wi01089067 WK [FR][SP10 RB536] AAAD\_Hardcode of warning message is not localized**

Currently some warning messages for AAAD client connection failures are not Localized. These will be localized in a later release.

**wi01121387 Email Manager memory spikes when running AML multiplicity traffic**

Email Manager memory may spikes intermittently under high traffic if system has a large number of customers.

Workaround: Archive out customers from the system.



### Scroll Bar does not work on an AAAD 'filtered' autocomplete list.

When an autocomplete list is presented on AAAD, the user can type a character to filter the autocomplete list. If the resulting filtered list is greater than 16 items, there will be a scroll bar, but the scroll bar will not work.

This is caused by a known defect in Microsoft .Net.

Workaround: The Microsoft position is that users should use the keyboard to navigate this "autocomplete" (filtered) list i.e. arrow buttons to move, and Enter to select.

### AAAD ClickOnce update fails.

Occasionally an AAAD ClickOnce update will fail if the client has had multiple updates without a re-boot. The error displayed will be "Cannot start the application. Contact the application vendor for assistance". Clicking on the 'Details' button will reveal the following failure message:

***"The process cannot access the file because it is being used by another process"***

This is a Windows issue. The problem is in the interaction between the particular PC and the Microsoft ClickOnce publishing platform.

Workaround: Reboot the client machine to release the locked file and re-launch the clickOnce AAAD.

### Web Communications Max Open Duration

The AAAD implementation of Max Open Duration has been disabled for Web Communications Contacts. Web Communications contacts should be treated like Voice Contacts as they are a real-time customer interaction, so it does not make sense to have a MaxOpenDuration valid for these contact types. The CMF implementation of Max Open Duration has changed to 24 hours in AACC 6.4 SP12.

### wi01135544 AAAD installation still named as Version 6

When installing or upgrading AAAD by clicking 'Launch AAAD' button, the Agent Desktop version shown is '6.0'. This version needs to be 6.0 as otherwise we could end up with two click-once installs on the same PC— one say from AACC 6.2 and one from AACC 6.4. The full currently operational version of AAAD appears in the "About AAAD" window.

### Installation of AAAD pre-requisites fail intermittently

Occasionally the pre-requisites for AAAD will fail to install and return a message box with an error code of 1935.

This is caused by a damaged installation of Microsoft .Net.

Workaround: (Note: backup the registry before making any changes)

1. In Windows, click Start > Run...
2. In the Run window, type 'regedit'. In the Registry Editor window, navigate to HKEY\_LOCAL\_MACHINE > SYSTEM > CurrentControlSet > Control.
3. If a Value with the name 'RegistrySizeLimit' does not exist in this key, right-click and select New-> DWORD (32-bit) Value and name it 'RegistrySizeLimit'.
4. In the 'Registry Editor' dialog box, double-click on 'RegistrySizeLimit'. This opens the 'Edit DWORD Value' dialog box.
5. In the 'Edit DWORD Value' dialog box, enter ffffffff as the 'Hexadecimal' value. Click on the 'Decimal' radio button, and enter 4294967295 as the 'Decimal' value. Click OK.
6. Reboot the machine.

7. Log in as an Administrator and open a Command Prompt and run 'SFC /SCANNOW'.

Taken from [http://answers.microsoft.com/en-us/windows/forum/windows\\_7-windows\\_programs/microsoft-visual-c-2005-redistributable-error-1935/9b245369-5053-e011-8dfc-68b599b31bf5](http://answers.microsoft.com/en-us/windows/forum/windows_7-windows_programs/microsoft-visual-c-2005-redistributable-error-1935/9b245369-5053-e011-8dfc-68b599b31bf5)

#### **AAAD reports missing or incorrect installation of .NET framework**

Intermittently when AAAD is launched after installing all pre-requisites, it will display a message to the user indicating a missing .NET framework/ CLR install

This is a Microsoft bootstrapper install issue. The .NET framework 4.0 will appear in the list of installed applications but the install is damaged.

Workaround: (Note: Administrative privileges are required to perform the following steps)

1. Copy the .Net 4.0 installer from the Multimedia Server onto the client pc at D:\Avaya\Contact Center\Multimedia Server\Agent Desktop\DotNetFx40
2. Run the installer and select the option to repair the install

#### **AAAD may hang due to IE stability issue**

Intermittently when AAAD is launched, it will display a message to the user that "CCAD main has stopped working". Investigating the eventlog indicated the AAAD application hung because of a problem in jscript9.dll – "Faulting application name: CCAD.exe, version: 8.4.0.225, time stamp: 0x52ab14b2  
Faulting module name: jscript9.dll, version: 9.0.8112.16545, time stamp: 0x531a521b.....  
Faulting module path: C:\Windows\SysWOW64\jscript9.dll"  
Installing the latest version of IE was found to rectify this problem. ( Note this was seen in one lab environment).

#### **wi01199007 [6.4FP2] AAAD\_IM\_The history tab shows Loading Contacts when agent completes the IM transfer**

1. Log in 2 blended agents into AAAD with IM contact.
2. Agent1 accepts the IM CDN from customer.
3. Agent1 consults to agent2 and agent2 rejects the IM consult
4. Then agent1 consults to agent2 again
5. Agent1 completes the IM transferred
6. Have a look the History tab on AAAD of the agent2

Expected result:

At step 6: It should be " No Contacts Found"

Actual result:

At step 6: It shows " Loading Contacts"

#### **wi01195447 ACCS RB1206 – AAAD – Enable "Highlight DN during transfer call" does not work on Supervisor call**

1. Launch CCMM Administration and navigate to Agent Desktop Configuration
2. At User Setting, tick to option "Highlight DN call during transfer"
3. Launch AAAD and login Agent 1101
4. Caller 7788 makes CDN call to Agent 1101
5. Agent 1101 answers CDN call
6. Agent 1101 makes Supervisor call to consult supervisor 90101
7. Check which call is highlighted on AAAD

Expected result:

At step 7: The consult call should be highlighted as option “Highlight DN call during transfer” is enabled

Actual result:

At step 7: The main call from Caller is highlighted instead of consult call

#### **wi01194198    AAAD 6.4.2 - Search on AAAD throw out some strange error message**

1. AAAD launched before
2. Attempt to search contact with closed or new status
3. Press Search again

\*\*\*\*Actual Result\*\*\*\*

Intermittently you may see the following messages:

- You may only attempt one Search at a time. Please wait for your initial search to complete before proceeding with another.
- The current Search has Timed Out. Please redefine your search criteria.

#### **wi01210081    Attachments in AgentEmailWS aren't worked**

1. Send email to CC
2. Using AgentEmailWS reply this email with attachmets(set file contents and display file name)

Expected Result:

Email reply should be received with attachment

Actual Result:

AgentEmailWS didn't return any errors but email wasn't sent.

#### **wi01202954    6.4 PB697 - WC cleanup – The barge in WC contacts are not closed automatically after restarting system**

1. Have an agent that is assigned to asupervisor
2. Login supervisor and agent with MPC enabled
3. Send some WC contacts to agent
4. Agent answers the WC contact
5. Supervisor observes, then barges in the web chat from agent
6. Perform system reboot
7. Look at CCMM Dashboard and search open contact on AAAD

Expected result:

At step 7: The WC contacts in “Open” status are closed

The WC contacts are not stuck on observe window

Actual result:

At step 7: The WC contacts are still in “Open” state

The WC contacts are stuck on observe window

#### **wi01196648    AAAD\_Webcom\_Supagent can observe and barge in the webcom contact if the agent releases the webcom incompletely.**

1. Login a blended Agent, the Agent is associated with an AgentSupervisor Supagent
2. The Agent accepts a Webcom contact from a customer and begins to chat
3. The Agent presses “Close” button on AAAD. Please make sure the Note window is not closed i.e. The webcom contact is active on AAAD (both work item and content window)
4. On Supagent, have a look at the Observer button and the Barge in button

**Expected result:** On the Supagent client, the Observe and Barge in button are grayed out as the agent had closed the web chat

**Actual result:** The Observe and Barge in button are not grayed out.

#### **CC-7495      AAAD\_Unable to observe Agent initiated CC calls**

##### **Steps to reproduce:**

1. Agent1 makes a CDN call
2. Agent2 answers the call
3. Launch AAAD login the Supervisor of Agent2, open Supervisor Observer tab
4. Select to the row that displays the CDN call
5. Try to observe this call.

##### **Expected result:**

Supervisor can observe the CDN out call

##### **Actual result:**

The observe button is grayed out, unable to observe the CDN out call

#### **CC-7502      Tabs in the screen Pop-up is not closing after Supervised call transfer releases**

##### **Configuration:**

##### **In CCMM Admin, Basic Screenpops, General Settings Tab:**

- i) Ensure "Close Screenpop when Consult/Transfer is Completed" isn't selected
- ii) Ensure "Launch Screenpop in a tab inside AAAD" is selected
- iii) Ensure "Auto Close Screenpop tab(s) on Work Item Release" is selected
- iv) Choose "Launch State" as "Alerting"

##### **In CCMM Admin, Basic Screenpops, Basic Screenpop (Shortcut) Tab:**

- i) Add a new "Screenpop Application Shortcut"
- ii) Ensure "Always on screenpop" is selected

##### **In CCMM Admin, Basic Screenpops, Basic Filters (Launch Types) Tab:**

- iii) Ensure the "Voice" checkbox is selected

##### **Steps to reproduce:**

1. Make CDN call to agent 1
2. Agent 1 accepts the call
3. Agent 1 initiates Supervised call transfer to CDN
4. Agent 2 answers the call. Make sure screen pops are displayed on AAAD of Agent 2.
5. Agent 1 completes transfer.
6. Agent 2 releases the call
7. Observe AAAD for Agent 2

##### **Expected result:**

At step 7: The screen pops disappear after call is released on agent 2.

##### **Actual result:**

At step 7: The screen pops still display after call is released on agent 2.

#### **CC-8356      SP16\_AAAD Incorrect telephone number displays when user type is changed from SA to Agent and via versa**

##### **Steps to reproduce:**

1. Create a blended Agent with IM uri and IM contact are included, login AAAD and logout
2. Change the Agent user type to a Supervisor Agent
3. Monitor the dialog boxes displayed on AAAD

**Expected result:**

All dialog boxes relate to the IM uri.

**Actual result:**

A dialog box may appear listing an incorrect IM uri. This dialog is displayed in error and does not effect the behavior of AAAD.

---

**CC-8068      AACC6.4SP16\_AAD\_Unable to login PO Agent after POM\_Outbound contact and PO skillset are unassigned and re-assigned**

---

**Steps to reproduce:**

1. Create a blended POM Agent(s)
2. Login the Agent and ensure the nail-up contact is presented
3. Logout the Agent
4. Login CCMA/CCM, un-assign the POM\_Outbound contact type from the Agent
5. Re-assign the POM\_Outbound contact type and assign a POM skillset
6. Attempt to re-login the Agent

**Expected result:**

Agent is able to successfully log in without any problem.

**Actual result:**

The zone name is displayed twice and the Agent fails to login. After shutting down and re-launching AAAD the Agent is able to Login again.

---

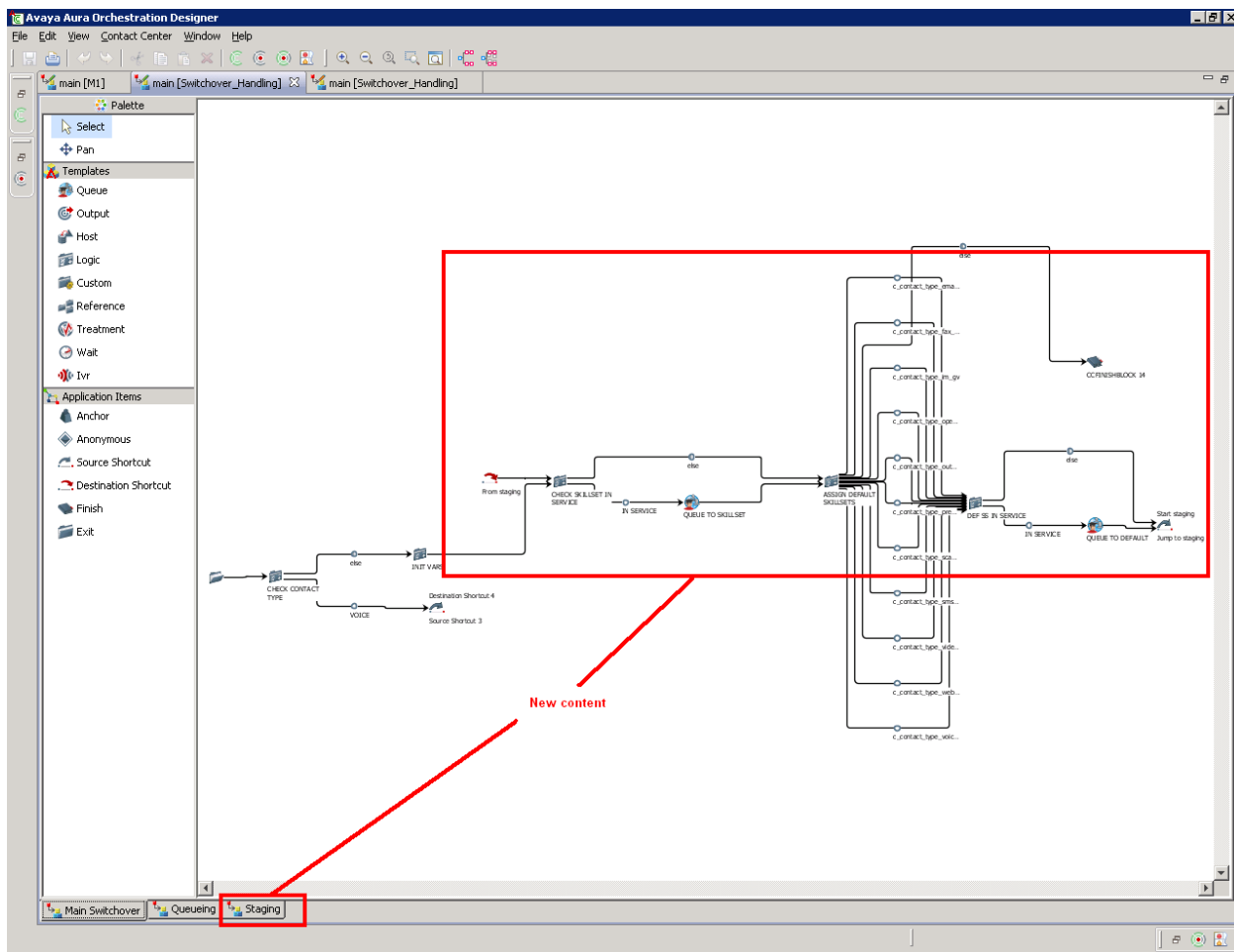
## Orchestration Designer

### wi00957924 Switchover handling script - updates will not apply if script edited previously

If the Switchover Handling flow has been updated by the customer prior to installing AACC 6.3 SP(or higher), then the AACC 6.3 SP(or higher) version of the flow will not be deployed during the install. The version that was updated by the customer will continue to be in use. Customers have to manually merge the changes to the Switchover Handling flow into the AACC 6.3 SP version supplied by Avaya.

Procedure to Deploy the AACC 6.3 SP(or higher) Switchover Handling flow:

- 1) Install AACC 6.3 SP(or higher)
- 2) Open Orchestration Designer.
- 3) Create a new CCMA in the Local View.
- 4) Copy the CCMS from the Contact Center view to the Local view.
- 5) In the Local view, rename the Switchover Handling flow to something else.
- 6) Import the Switchover Handling flow. The location of the flow is dependent on the installation of OD. The default locations are:
  - a. 64-bit: %ProgramFiles(x86)%\Avaya\Contact Center\SCE\8.2.2239\Samples\Flows\SIP\Update
  - b. 32-bit: %ProgramFiles%\Avaya\Contact Center\SCE\8.2.2239\Samples\Flows\SIP\Update
- 7) Open the flow just imported. The new areas of the flow are highlighted in the screenshot below.
- 8) Copy all the custom changes to the Switchover Handling flow to the Switchover Handling flow provided by Avaya. All the changes are expected to be located in the "Queueing" tab.
- 9) Right click on the CCMS and select "Synchronise". When the Synchronisation View appears on screen, right click on the new Switchover Handling flow and select "Update in Contact Center"
- 10) To test the new Switchover Handling flow, execute a switchover followed by a switchback. However, please be aware that this procedure can be time consuming.



## Security Framework

### wi01008566 Uninstall of base SFW does not remove all data, breaking the next re-install

If the security framework is uninstalled from a server and then re-installed CND does not install correctly. The result is that SFW cannot be configured. This has been reproduced with the SFW base install that is bundled with AACC SP5.

CND remains in Add/Remove programs after SFW has been uninstalled. It cannot be removed from Add/Remove programs.

Workaround: The CND registry information must be manually removed from the registry after the SFW has been removed.

- Launch Regedit
- Search for "Common Network Directory"
- Delete the registry key that contains this information.

At this point the SFW can be re-installed.

## Feature Specific: POM Integration

AACC FP2 POM integration is supported with the following line-up:

- ☐ POM 3.0 Service Pack 3
- ☐ CS1000 7.6 SP7 and Patch **MPLR33345, MPLR32229, MPLR33041** or later equivalent
- ☐ CS1000 needs to be configured to use ADS block rather than SCB block.
- ☐ CM – No specific restrictions.

### Configuration Items for AML and SIP

To ensure that the Agent Desktop operates correctly, observe the following differences of configuration for AML vs. SIP environments:

- AML:
  - o Ensure the P-Asserted Identity value is set in AAEP and that this number is set to a unique value that does not overlap with any other numbers on the CS1000 numbering plan.
  - o Ensure the nail-up CLID in CCMM Administration is set to match the P-Asserted Identity.
  - o Ensure that the Nailup Call CLID under Agent Settings in the Manage Global Configuration page on POM is also set to match the P-Asserted Identity.
  - o Ensure that 'Override PAI for External Consult calls' is TICKED.
  - o Ensure that 'ANI for external consult calls' is set to 'Agent Extension'.
  - o Under System Configuration -> Applications. Edit POMDriverApp and Nailer applications and set 'Generate UCID:' to YES.
- SIP :
  - o Ensure the P-Asserted Identity value is set in AAEP and that this number is set to a unique value that does not overlap with any other numbers on the CM numbering plan.
  - o Ensure the nail-up CLID in CCMM Administration is set to match the P-Asserted Identity.
  - o Ensure that the Nailup Call CLID under Agent Settings in the Manage Global Configuration page on POM is also set to match the P-Asserted Identity.
  - o Ensure that 'Override PAI for External Consult calls' is NOT TICKED.
  - o Ensure that 'ANI for external consult calls' is set to 'Nailup call CLID'.
  - o Under System Configuration -> Applications. Edit POMDriverApp and Nailer applications and set 'Generate UCID:' to YES.

**wi01172853    Need to restart POMProxy after restarting POM**

After a restart of POM Services, you will need to restart POMProxy Service on AACC to continue normal agent operation. Your maintenance window should restart both.

**wi01168899    POM Agents will be blended to inbound although no inbound contacts are waiting when using the Average\_Answer\_Dely\_S as a blend threshold**

You may observe agents being blended from Outbound to Inbound even though there are no waiting inbound contacts if the Average\_Answer\_Dely\_S is selected as the blend criteria. This is due to the answer delay initially being zero.

Workaround: Do not use the Average\_Answer\_Dely\_S as blend criteria. Use any of the other criteria for blending agents.

**wi01196648    POM zoning – Can login POM Agent but cannot Ready when POM zone is not the same AACC zone**

As part of the development of the fix for this issue; two POM issues have been raised “wi01199380” and “wi01199383”. For a complete solution all three wi must be fixed.

**wi01211877    AML POM traffic - time delay in wrap up**

During a POM traffic run agents experienced a delay during the wrap up time handling a POM contact.

**wi01210134    PO – Successfully make Standard schedule callback when it is disabled in campaign strategy**

1. Login a PO Agent into AAAD
2. Have the Agent active an PO contact
3. Press Release button and then press Schedule while in ACW time, input a valid type, press OK button and verify if the Agent is able to make Standard Schedule while it is disabled in campaign strategy.

**Actual result:**

The Agent successfully make Standard Schedule callback and the callback is routed to the Agent at the schedule time.

**Expected result:**

Either Standard type callback is not selected by default when General Callback is disabled in Campaign Strategy or an informative message is displayed to inform the Agent to select another option because current option is not enabled at this time.



## Feature Specific: Multiplicity

### **wi00794149 [M&I] Agent By Skillset Post Call Processing stat not working with Multiplicity**

Post Call Processing (also known as After Call Work) is the time the agent spends performing activities relating to the contact that has just been completed. The agent signals the start of PCP by entering the Not Ready state. When the agent is working on multiple contacts PCP is not pegged until the last contact is released.

Workaround: No workaround currently available.

## Feature Specific: High Availability

### **wi00895527 AACC HA: Following a Switchover and then a Switchback, Agents that have been logged in for all this time will have incorrect RTDs until the next call/contact**

1. Agent has (for example) multiplicity, with 1 email and 1 voice.
2. Switchover
3. Follow procedure for Switchback (backup & restore etc)
4. Switchback
5. Assume agent has remained logged in, and is still working on the call and email.
6. Examine RTD for the agent
7. The voice line for the agent shows “busy” not “active”, and the skillset is not shown.
8. The MM contact(s) are summarized in one line, with “busy”, or “idle” if no MM contacts are active. The skillset is not shown.
9. RTD corrects automatically with next new call, new email.

This limitation applies to situations where the standby AACC is started after there has been agent/call/contact activity on the active AACC. A switchover and switchback is a prime example, but could also occur during commissioning.

Note that the standby AACC is not tracking every nuance of contact processing that is taking place in the active. The key preserved elements are agent login state and ready state. Some RTD items such as time in state will revert to zero and start counting again upon the outage of the active AACC.

Workaround: No workaround. RTDs automatically recover, but will be incorrect until next new call/contact. For customers that choose to perform steps 3 & 4 as out of hours maintenance this problem will not arise, because after step 2 the agents will have logged out and they will log in again as part of step 5.

### **wi00926067 AACC HA: Call Disconnects Can be Lost While AACC is Switching Over**

The AACC takes between 200msec and 5 sec to complete a switchover. During this time it is possible that a BYE may originate from the Session Manager. While the AACC HA pair is in transition, this BYE cannot be processed or acknowledged, and it will not be resent by the SM.

Therefore, it is possible for example that when a customer goes on-hook, the customer leg of a call will be properly cleared, but the associated agent leg will not automatically be taken down. The agent will also have to disconnect (i.e. separately disconnect his/her leg of the session).

Workaround: Agent clicks “release” button on AACC at the end of the conversation with the customer.

#### Re-Attempting INVITEs

Note that, similar to BYE, INVITE call setup sequences could conceivably be in progress when AACC switches over (i.e. before the call dialog is stable / established). Depending on when the AACC switchover occurs relative to the progress the SIP dialog setup, the agent may be set to NRdy. The

agent can go Rdy again to work around if this occurs. In SM/SMGR 6.1, there is no specific config item to make the SM retry an INVITE when Timer B expires (i.e. when the INVITE request times out), plans are underway to include such an option in SM 6.2.

#### **wi00953109    Disabling NIC on Active crashes SMMC**

For an SMMC based HA system, if the NIC is disabled it can cause SMMC to crash. The crash can result in an indeterminate state of HA system

Workaround: There is no workaround. In an SMMC based HA system, do not disable the NIC on the active server.

#### **wi00947429    On switchover Presenting contacts' Call Presentation timeout has not worked correctly**

Set the system to have a Return To Queue of, for example, 30 seconds (set in CCMA, Configuration, Call Presentation Classes).

Log in an agent, set to NRdy

Send in a CDN call or webcom or email (depending on which contact type is appropriate for the agent you are using)

Set the agent ready & once the contact is presenting/alerting, don't answer, pull the CAT 5 cable(s) out of the active AACC, causing a switchover.

The presenting contact will not timeout after 30 sec. In general, it will remain alerting until answered. In the case of a voice call, a separate SIP timeout will occur and the call will be taken back and requeued.

There is no loss of customer contacts or calls; there is no loss of agent state.

The absence of Call Pres timing is only visible for the subset of contacts that happen to be alerting on AAAC at the time of the active AACC outage.

Workaround: None. Call Pres timing operates normally for all contacts routed post-switchover.

#### **wi01073764    [SP10]AML-6.3-The Migration button is always disabled with the system time zone is not on DST**

To Prevent the corruption of the database and keep its consistency when doing a Database Migration, the above work item was created.

When attempting to migrate in Database maintenance, if you have Daylight Saving Time (DST) Turned on, the migrate will not continue as it causes severe inconsistencies to the database thus affecting other components.

It has been observed that if you do not have the latest Hot fixes for countries DST, Database maintenance gets inaccurate readings from your Windows settings as your system is out of date, thus allowing migrations when it shouldn't, or blocking migrations when it should.

Workaround: Install the latest Hot fixes for DST that apply to your Time zone and system.

#### **wi00972300    SIP HA - Post switchover with an email backlog (<4000), RTD's are incorrect**

In a very rare instance, it has been observed that after a switchover the number of contacts reported by the RTD is not the same as reported prior to the switchover. All real contacts are correctly routed and processed by agents.

Workaround: The root cause of the reporting discrepancy is the contact processing sub-system can be operational before the reporting sub-system is available. There is currently no workaround.

### wi01076997 AACC 6.3 SP10 HA: could not start HA system after daylight saving time changes due to mixed dates in the journal files

When testing Daylight Savings Time (DST) changes in a Lab setting it is sometimes necessary to move the Servers Date backwards. This is something that would not happen in the real world and is not supported. If you do need to adjust the Date backwards, it is possible that the Caché Database will not Start Up, this is due to the fact that there will be Journal Files on the system with Future Dates. It is possible to recover from this situation by following these steps:

- Ensure Caché is stopped.
- Set the Date/Time back to where you need it to be.
- Delete all the Journal Files in the X:\Avaya\Contact Center\Databases\Journal folder.
- Reboot the Server.
- Perform a Backup and Restore of the Databases.

This should also preserve the integrity of the Database in that no data will be lost, but it should be noted that any data that contains Date/Time information could potentially have data marked as being in the future, this would be particularly evident for the Historical Statistics for example.

It should be stressed that this cannot happen in Live running, as Dates are never moved backwards, even with a DST change; it is only the Time that changes.

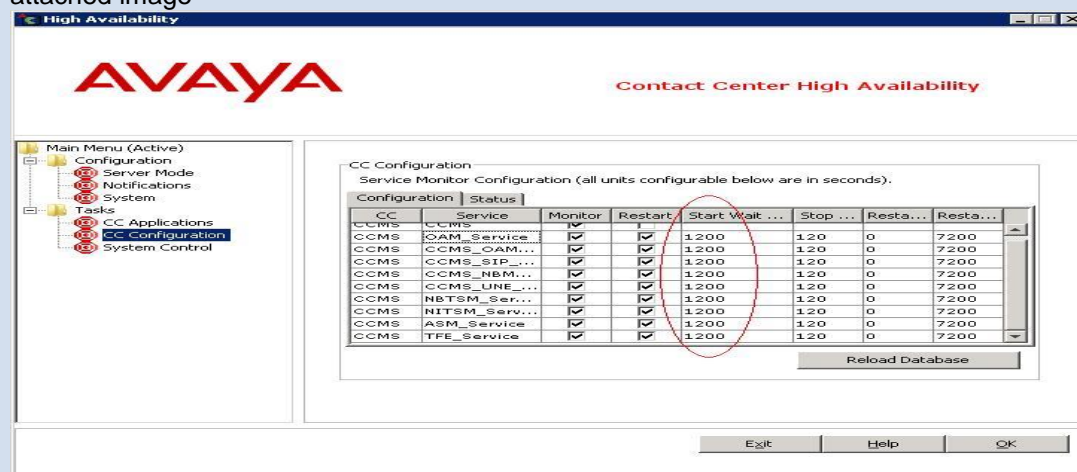
### During CCMS start up, an automatic switchover or CCMS monitored services can be restarted if service start up takes longer than configured monitor time

Systems affected: Some AML / SIP CS1k CCMS systems with large amount of task flow scripts/applications e.g. > 300 scripts/applications.

Pre-conditions: Automatic Switchover is Enabled and Service Monitoring is ON.

Background: During CCMS services start up e.g. post reboot or manual startup of services, if monitored services "OAM\_Service, NBTSM\_Service, NITSM\_Service, ASM\_Service, TFE\_Service, CCMS\_OAM\_CMF\_Service, CCMS\_SIP\_Service, CCMS\_NBMSM\_Service, or CCMS\_UNE\_Service" take longer than 8 minutes to start, CCMS service triggers an automatic switchover

Workaround: Configure 1200 seconds for StartWaitTime under High Availability-CC Configuration. See attached image



Note: If for any reason, monitored services takes longer than 1200 seconds (20 minutes), turn off Service monitoring by un-checking the "Monitor" checkbox before or during the start up. Once the CCMS services fully started, Monitoring can be turned on with default configuration or other custom configuration.

### CC-10956 SGM rejects calls from Communicator v3.0 with 'SIP 403 forbidden' due to 'Microsoft' in UA header

Call CDN using from a station controlled by a user(not an agent) with the Equinox 3.0 softphone. AACC rejects the call.

A solution for this will be delivered in AACC 7.0.1

## Feature Specific: AML to SIP Migrations

### **wi01207905 AML to SIP Migration: Updated information needed for Event 64145**

A data integrity check is run as part of an AML to SIP migration. One purpose of this check is to highlight any duplicate URIs that may exist on the system as a result of the migration process and system generated URIs. Example: By default, the unique agent ID will be used to set the URI for an agent as part of the migration. It is possible for a conflict to arise between the newly generated agent URI and another resources that requires a URI (CDN or DNIS). These URI conflicts will be logged to the Windows Event viewer during the migration as event code 64145.

The resolution information contained in these events does not provide enough information to remove the conflict.

Workaround:

More detailed resolution steps are detailed here:

1. Compile a list of resources flagged as having duplicate URIs. This can include Agents, Supervisor/Agents, CDN's (Route Points) or DNIS.
2. Ensure that the migration procedure is complete, including all documented steps to migrate CCMA, CCMM etc.
3. Ensure that all AACC services are running and login to CCMA.
4. Modify the Agent OR Supervisor/Agent URI to a new value removing the conflict (i.e. a value other than that already in use by a CDN or DNIS resource). This can be done via the CCMA Contact Center Management component – Agent Properties.
5. If a large number of conflicts exist, the CCMA Configuration Tool (Excel based) can be used to update agent URI fields in bulk.

Note: It is also possible to change the URI of a CDN or DNIS and resolve the conflict in this way. CDN and DNIS URIs can be updated using the CCMA Configuration Tool (SIP Spreadsheet) only. They cannot be modified using the CCMA UI.

6. Restart AACC for changes to take effect.