Avaya Aura® Contact Center

Simplex Unified Communications Deployment Guide

NN44400-806

Document status: Standard
Document issue: 01.01
Document date: June 2013
Product release: Release 6.3
Job function: Solution
Type: Technical Publication
Language type: English

© 2013 Avaya Inc.

All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://www.avaya.com/support

Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, http://support.avaya.com/LicenseInfo/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

License type(s)

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function(e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.**Heritage Nortel Software**

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise

Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third-party components

“Third Party Components” mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/ThirdPartyLicense/. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://www.avaya.com/support.Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya, the Avaya logo, Avaya one-X® Portal, Avaya Aura® Communication Manager, Avaya Aura® Experience Portal, Avaya Aura® Orchestration Designer, Avaya Aura® Session Manager, Avaya Aura® System Manager, and Application Enablement Services are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading documents

For the most current versions of documentation, see the Avaya Support website:

http://www.avaya.com/support

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product.

For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Introduction 13
Avaya Aura® Contact Center server types 15
Avaya Aura® Contact Center Mission Critical High Availability 15
Switchover 17
Agent experience during a Contact Center switchover 18
Supervisor experience during a Contact Center switchover 18
Administrator experience during a Contact Center switchover 18
Campus High Availability 19
Trusted IP address 21
Database Shadowing 21
High Availability configuration utilities 22
Avaya Media Server 25
Contact Center Manager Administration 26
Switchover Handling Script 32
Campus network requirements 34
Avaya Aura® Unified Communications platform 34
Unified Communications platform integration 36
High Availability Network Timeout optimization 37
High Availability Network Timeout calculation 38
Example solution details 41
Contact Center servers 41
Unified Communications platform servers 43
Domain Administrator requirements 45

Unified Communications Platform integration section 47
Unified Communications – Communication Manager configuration 49
Logging on to Communication Manager 50
Administering IP Node Names 51
Verifying the IP Network Region 52
Configuring a SIP Signaling Group for the Session Manager 53
Configuring a SIP Trunk Group for the Session Manager 55
Configuring a Route Pattern 57
Administering the Dial Plan for routing and extensions 58
Administering the Uniform Dial Plan for routing 59
Administering Automatic Alternate Routing 60
Configuring IP Services for Application Enablement Services 61
Configuring a CTI Link for Application Enablement Services 63
Creating the agent extensions 64
Adding Agent workstations to the numbering tables 67
Enabling Gratuitous Address Resolution Protocol on agent extensions 69

Unified Communications – Session Manager configuration 71
Logging on to the System Manager Web interface 71
Creating a routing domain 73
Creating a routing location 74
Creating a SIP Entity for the Communication Manager 76
Creating a SIP Entity for the Session Manager 78
Creating a SIP Entity Link from the Session Manager to the Communication Manager 81
Creating a routing policy from the Session Manager to Communication Manager 83
Creating a dial pattern to route calls to Communication Manager 84
Creating a SIP Entity for the Voice and Multimedia Contact Server 87
Creating a SIP Entity Link from the Session Manager to the Avaya Aura® Contact Center 90
Creating a routing policy from the Session Manager to Contact Center 92
Creating a dial pattern to route calls to the Contact Center 93
Unified Communications – Application Enablement Services configuration 97
Accessing the AES server management console 98
Adding the Communication Manager switch connection 99
Adding the Communication Manager switch connection CLAN IP 100
Adding a CTI link to the Communication Manager 101
Restarting the AES to Communication Manager connection 103
Enabling TR87 on the AES 104
Configuring security on the AES 105
Adding the Contact Center default certificate CN as a trusted host 106
Restarting the AES Linux server 107
Verifying the AES services are running 108
Verifying the AES connection to the Communication Manager switch 109
Verifying the AES TSAPI connection 110
Debugging the AES server 111

Contact Center server software installation section 113
Voice and Multimedia Contact Server with Avaya Media Server software installation 115
Installing Windows Server 2008 Release 2 116
Installing the most recent operating system service packs 118
Disabling the Remote Access services 119
Adding the server to a domain 122
Downloading the most recent Contact Center patches to the server 123
Disabling unused Network Adapters 124
Enabling Microsoft Remote Desktop connection 124
Configuring Data Execution Prevention 125
Scheduling Weekly Disk Defragmentation 127
Importing the Contact Center Firewall Security policy 129
Downloading the Roles and Features Installer 131

Installing the required Windows roles and features 132
Configuring Windows Server 2008 135
Configuring MIME types to support Microsoft updates 135
Installing the Voice and Multimedia Contact Server with Avaya Media Server software 138
Installing Voice and Multimedia Contact Server software patches 151
Configuring the WebLM license file 154
Confirming that the Contact Center services start 156
Updating the CCMA Administration user password 161
Configuring Internet Explorer on the Voice and Multimedia Contact Server 162
Verifying the Web Services 168
Verifying that Contact Center Multimedia services start 169
Verifying the Multimedia database installation 170
Scheduling Contact Center Manager Administration backups 170
Providing local users with Log on as a service right 174
Configuring the MIME types 175
Configuring Internet Explorer 9.0 for Avaya Media Server Element Manager 177
Logging onto Avaya Media Server Element Manager 177
Patching Avaya Media Server software 178

Contact Center commissioning section 183

Avaya Media Server commissioning 185

Configuring media on the Avaya Media Server 185
Media file formats 185
Media organization 185
Logging onto Avaya Media Server Element Manager 186
Confirming the Contact Center packaged application locale 187
Configuring the SIP port on a co-resident Avaya Media Server 188
Adding Contact Center Manager Server as a trusted node 188
Adding the media content namespace 190
Adding the locale-specific media content group 191
Configuring Avaya Media Server settings for SIP-enabled contact center 193
Uploading a batch zip file 196

Voice and Multimedia Contact Server with Avaya Media Server commissioning 199

Logging on to Contact Center Manager Administration for the first time 199
Adding Communication Control Toolkit to Contact Center Manager Administration 201
Adding the Multimedia server to Contact Center Manager Administration 202
Configuring global settings 204
Adding route points for voice contacts 206
Adding a route point for email contacts 208
Adding the media server 210
Adding media servers to the required media services 211
Editing an activity code 215

Creating a threshold class 217
Creating a call presentation class 219
Enabling Multiplicity 222
Refreshing your servers 223
Creating a Multiplicity Presentation Class 226
Adding a skillset for voice contacts 229
Adding a skillset for email contacts 231
Editing a contact type 233
Adding a supervisor 235
Adding an agent 236
Multimedia commissioning 241
Logging on to the Multimedia Administration tool for the first time 242
Verifying the server settings 243
Configuring the multimedia license type 245
Configuring CCMM administrators 246
Configuring holidays 247
Configuring office hours 248
Applying office hours 249
Configuring the email settings 251
Configuring skillsets for email 253
Creating a keyword group 255
Creating a rule group and a rule 257
Creating an email recipient mailbox 260
Configuring email attachment file locations 264
Selecting the outgoing email address 265
Configuring Agent Desktop Configuration General Settings 267
Controlling access to email message text 269
Viewing real-time traffic reports by contact type 271
Configuring the reporting credentials 272
Updating the System Default Rule 273
Updating the System Delivery Failure Rule 275
Configuring Microsoft Exchange for sending outgoing email 277
Orchestration Designer commissioning 279
Installing the Orchestration Designer client 279
Opening Orchestration Designer 280
Creating a new graphical flow using Orchestration Designer 283
Configuring a graphical flow using Orchestration Designer 286
Configuring the Switchover Handling script 307

Agent Desktop section 315
Agent Desktop – Client software installation 317
Creating Domain users and groups for agents 318
Assigning a group policy for embedded softphone settings 320

Installing the Agent Desktop client software 323
Agent Desktop – Handling voice calls 325
Work item paradigm 325
Top bar 325
Work list window 326
Action bar 328
Starting Agent Desktop 328
Logging on to Agent Desktop when using a desktop phone 329
Changing your status to Ready 331
Accepting a test call 331
Ending the test call 332
Logging off from Agent Desktop 332
Agent Desktop – Handling email messages 335
Accepting an incoming contact 336
Replying to an email message 338
Closing the email contact 339
Agent Desktop – Multiplicity 341
Accepting a route point call 342
Accepting an incoming email contact while handling a voice contact 343
Closing a customer contact 345

Avaya Media Server section 347
Avaya Media Server – Removing Avaya Media Server software 349
Backing up the Locale Specific Media Files on Windows 349
Backing up the batch zip file 350
Removing Avaya Media Server from CCMA 350
Uninstalling Avaya Media Server 355
Avaya Media Server – Primary server software installation 357
Installing the Linux server for Avaya Media Server 358
Installing the required packages on the Linux server 365
Adding a Linux user group and user 367
Preparing the Linux server for Avaya Media Server 368
Configuring Network Time Protocol 370
Installing the Avaya Media Server software 370
Installing the Avaya Media Server patches 373
Securing your Avaya Media Server 374
Avaya Media Server – Backup server software installation 377
Installing the Linux server for Avaya Media Server 378
Installing the required packages on the Linux server 385
Adding a Linux user group and user 388
Preparing the Linux server for Avaya Media Server 388
Configuring Network Time Protocol 390
Installing the Avaya Media Server software 390

Installing the Avaya Media Server patches 393
Securing your Avaya Media Server 395
Avaya Media Server – High Availability commissioning 397
Resolving the Managed name to the Service IP Address 398
Logging on to Avaya Media Server Element Manager 399
Obtaining the Universally Unique Identifier 401
Configuring the High Availability primary Avaya Media Server 401
Configuring the High Availability backup Avaya Media Server 403
Enabling High Availability on the backup server 405
Completing High Availability pair configuration 406
Enabling High Availability on the primary Avaya Media Server 407
Restarting the primary and backup servers 409
Reviewing High Availability configuration and status 410
Avaya Media Server – Commissioning 413
Configuring media on the Avaya Media Server 413
Media file formats 413
Media organization 413
Confirming the Contact Center packaged application locale 414
Adding the Contact Center Manager Server as a trusted node 414
Adding the media content namespace 416
Adding the locale-specific media content group 417
Configuring Avaya Media Server settings for SIP-enabled contact center 418
Restoring the Locale Specific Media Files on Linux 421
Uploading a batch zip file 422
Adding the media server 424
Adding media servers to the required media services 425
Restarting License Manager to push Avaya Media Server licenses 428
Verifying Avaya Media Server licensing 430

Agent Desktop verification section 433
Agent Desktop – Verifying voice calls 435
Starting Agent Desktop 435
Logging on to Agent Desktop when using a desktop phone 436
Changing your status to Ready 437
Accepting a test call 438

High Availability section 439
High Availability – CCMA replication pre-install configuration 441
Adding the domain AD-LDS replication account to the primary administrators and replicator group 443
High Availability – Voice and Multimedia Contact Server standby software installation 459
Installing Windows Server 2008 Release 2 461

Installing the most recent operating system service packs 463
Disabling the Remote Access services 463
Adding the server to a domain 466
Downloading the most recent patches to the server 467
Disabling unused Network Adapters 468
Enabling Microsoft Remote Desktop connection 468
Configuring Data Execution Prevention 469
Scheduling Weekly Disk Defragmentation 471
Importing the Contact Center Firewall Security policy 473
Downloading the Roles and Features Installer 475
Installing the required Windows roles and features 476
Configuring Windows Server 2008 479
Configuring MIME types to support Microsoft updates 479
Adding the domain AD-LDS replication account to the backup administrators and replicator group 482
Installing the standby Voice and Multimedia Contact Server software 496
Installing Voice and Multimedia Contact Server software patches 520
Configuring the WebLM license file 523
Confirming that the Contact Center services start 524
Updating the CCMA Administration user password 530
Configuring Internet Explorer on the Contact Center server 531
Verifying the Web Services 536
Verifying Contact Center Manager Administration replication 538
Verifying the Multimedia database installation 539
Verifying that Contact Center Multimedia services start 540
Providing local users with Log on as a service right 541
Configuring the MIME types 542

High Availability – Voice and Multimedia Contact Server commissioning 545

Resolving the Managed name to the Managed IP Address 549
Installing a third-party utility to support High Availability 550
Configuring CCMM General Administration 552
Verifying services are ready for High Availability 554
Configuring High Availability on the active server 555
Configuring email notification on the active server 558
Backing up the active Contact Center Manager Administration 561
Backing up the database on the active server 569
Restoring the database on the standby server 572
Restoring CCMA data to the standby server 579
Configuring server details on the standby server 582
Configuring High Availability on the standby server 588
Starting High Availability on the active server 591
Starting High Availability on the standby server 595
Verifying High Availability is running on the active server 597

Verifying High Availability is running on the standby server 600
Changing server details in Contact Center Manager Administration 602
Using the Contact Center Manager Administration server Managed name 606
Configuring email attachment file locations 608
Verifying the Managed IP address on the active sever 610
Verifying server communication on the standby server 611
High Availability – Session Manager configuration 613
Updating the Contact Center Manager Server SIP Entity 613
High Availability – Testing 617
Uninstalling Agent Desktop client software 618
Starting Agent Desktop 620
Creating a shortcut to the Agent Desktop 621
Logging on to Agent Desktop when using a desktop phone 622
Changing your status to Ready 623
Generating a test call 624
Generating a test email contact 624
Testing voice and email resiliency by generating a Voice and Multimedia Contact Server switchover 626
Handling multimedia contact refreshes during a switchover 628
Handling loss of desk phone control 629
Handling Server communication issues 630
Handling configuration issues when launching Agent Desktop 630
Replying to the test email message 631
Ending the test call 633
Logging off from Agent Desktop 633
How to reinstate High Availability after a switchover 634

Maintenance section 645
Patching – Voice and Multimedia Contact Server software 647
Installing Voice and Multimedia Contact Server software patches 647

Troubleshooting section 651
Troubleshooting – SIP Contact Center 653
Responding when dialing a Route Point 654
Logging on to Agent Desktop 654
Troubleshooting when hold/unhold causes calls to be dropped after seventy seconds 654
Playing ringback into an active call 655
Call processing fails due to suspected Avaya Media Server failure 655
Handling 486 Busy Here error messages 656
Handling 404 Not Found error messages 656
Handling 480 Temporarily Unavailable error messages 657
Handling 488 error messages 657
Troubleshooting when digits entered for IVR Play and Collect are not recognized 657

Troubleshooting when no terminals or addresses appear in Agent Desktop 658
Handling subscribed Resource Availability error messages 658
Handling TLS server certificate time zone issues 659
Handling missing TLS certificates 659
Troubleshooting CCMS and AES TLS communication issues 659
Troubleshooting when an agent goes not-ready to a presented call 661
Troubleshooting – High Availability 663
Troubleshooting Mission Critical High Availability 663
Troubleshooting when shadowing fails to start 670
Troubleshooting when SMMC fails to start 670
Troubleshooting Licensing issues 671
Troubleshooting when services fail to start 672
Troubleshooting shadowing failures 673
Troubleshooting unnecessary switchovers 674
Troubleshooting switchover failure 674
Troubleshooting when network outages occur in a High Availability Contact Center 675
Troubleshooting contact issues that occur after a switchover 676
Troubleshooting – Avaya Aura platform 679
Troubleshooting AES and CCMS communication issues 679
Troubleshooting Communication Manager stations 680
Troubleshooting treatments when dialing the Contact Center Route Point Address 681
Troubleshooting routing calls from Contact Center to agents on Communication Manager 682
Troubleshooting when agents cannot log on to Agent Desktop 682

Introduction

This guide describes how to initially install and commission a Voice and Multimedia Contact Server with Avaya Media Server, and subsequently configure a voice and multimedia Mission Critical High Availability solution, using the following Avaya Aura® Contact Center Release 6.3 components:

- Two Voice and Multimedia Contact Servers without Avaya Media Server.
- Two Avaya Media Server Linux-based servers, configured as a High Availability pair. Avaya Media Server High Availability is supported only on Linux-based servers.
- One Avaya Aura® Communication Manager (CM) Release 6.2 server.
- One Avaya Aura® Session Manager instance (SM), Release 6.2.
- One Avaya Aura® System Manager, Release 6.2.
- One Avaya Aura® Application Enablement Services (AES) Release 6.2 server.
- A Windows Active Directory Domain Controller and Domain Name System (DNS).

This guide uses a sample solution to describe how to configure Avaya Aura® Contact Center to support basic voice and email contact types. This guide covers only the concepts and procedures required to install and configure a sample Mission Critical High Availability solution based on a simplex Avaya Aura® Unified Communications platform. The examples in this document are specific to this sample solution. To achieve a working solution, you must follow the procedures in the documented order.

This guide describes the initial installation and commissioning tasks required to achieve a working non-HA Contact Center solution that includes a Voice and Multimedia Contact Server with Avaya Media Server. To achieve this working single server solution, follow the procedures in the documented order until the Avaya Media Server section (page 347).

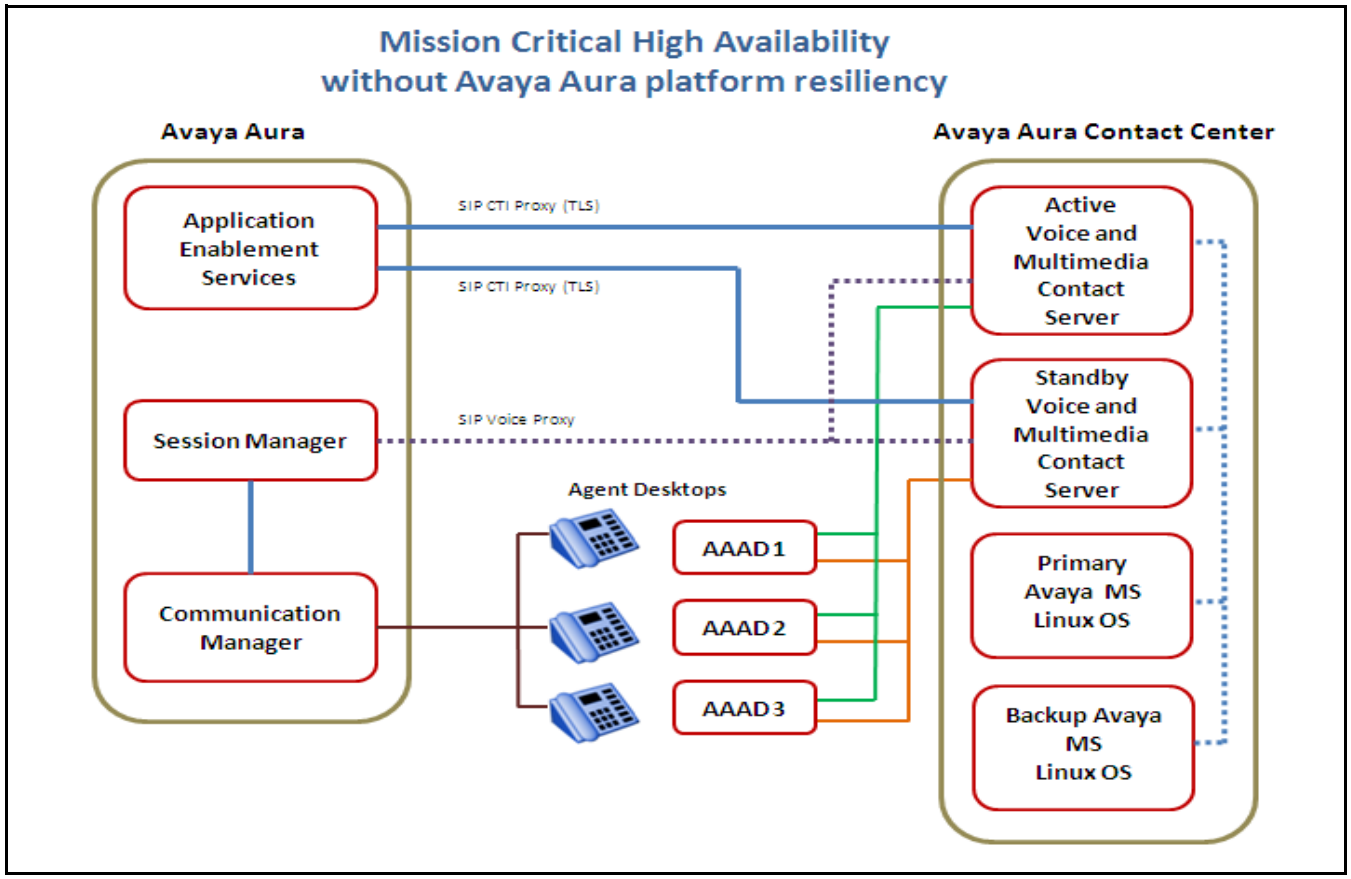
The guide also goes on to describe the procedures required to configure a Mission Critical High Availability solution after you successfully install and commission a Voice and Multimedia Contact Server with Avaya Media Server. In order to achieve a working Mission Critical High Availability solution, you must:

- remove Avaya Media Server from the Windows-based Voice and Multimedia Contact Server
- install and commission Avaya Media Server High Availability on Primary and Backup Linux-based servers
- install a standby Voice and Multimedia Contact Server without Avaya Media Server, and commission both Avaya Aura® Contact Center servers for High Availability.

This guide does not describe other multimedia contact types, Instant Messaging integration, Avaya Aura® Experience Portal integration, or any other integration or solution. For more information about supported integrations and contact types, see the Avaya Aura® Contact Center 6.3 Documentation Collection, available at www.avaya.com/support.

This guide describes how to use Avaya Aura® Agent Desktop to verify basic contact center and High Availability functionality.

Example of a Mission Critical High Availability solution without Avaya Aura® platform resiliency



Attention: This is the least resilient Mission Critical High Availability solution, as there is no platform resiliency. If an outage occurs on any of the Unified Communications components in this solution, the contact center agents can experience downtime, loss of call control or call loss.

Avaya Aura® Contact Center server types

The Avaya Aura® Contact Center Release 6.3 DVD Installer supports a range of new server types. Each new server type installs a combination of Avaya Aura® Contact Center applications suitable for a specific contact center function. Some Contact Center servers support only voice contacts, some Contact Center servers support only multimedia contacts, and some new Contact Center servers support both voice and multimedia.

Avaya Aura® Contact Center Release 6.3 no longer supports the installation of individual Contact Center components or applications.

This deployment guide installs two Voice and Multimedia Contact Servers. The initial server type installed is a Voice and Multimedia Contact Server with Avaya Media Server. Avaya Media Server is then removed from this server before High Availability is configured. A Voice and Multimedia Contact Server provides context sensitive and skill-based routing for customer voice and multimedia contacts. This server provides routed contact support for email messages. A Voice and Multimedia Contact Server includes the following components:

- Contact Center Manager Server (CCMS)
- Contact Center License Manager (LM)
- Contact Center Manager Server Utility (SU)
- Contact Center Manager Administration (CCMA)
- Communication Control Toolkit (CCT)
- Contact Center Multimedia (CCMM)

In a small to medium solution using a Voice and Multimedia Contact Server, agents download and install Avaya Aura® Agent Desktop software from the Voice and Multimedia Contact Server.

Avaya Aura® Contact Center Mission Critical High Availability

Avaya Aura® Contact Center supports Mission Critical High Availability (HA) resiliency for CCMS, CCT and CCMM. Avaya Media Server on the Linux operating system supports High Availability (HA) resiliency. Avaya Media Server High Availability is supported only on Linux-based servers.

All of the Avaya Aura® Contact Center components (CCMS, CCMA, CCT, LM, CCMM, and Avaya Media Server) must be in the same network subnet IP address range. All of the Avaya Aura® Unified Communications components (CM, SM, and AES) must be in the same campus network location as the Avaya Aura® Contact Center components.

All Avaya Aura® Contact Center components (CCMS, CCMA, CCT, and CCMM) must be in the same Windows Active Directory domain. All Avaya Aura® Contact Center servers must be registered with the same Windows Active Directory Domain Controller.

The active and standby Avaya Aura® Contact Center servers must be in the same subnet IP address range for campus High Availability resiliency to work. All Avaya Aura® Agent Desktop client computers must be registered in this domain, or in domains with a two-way trust relationship with this Contact Center server domain.

Contact Center supports High Availability for fault tolerant and mission critical contact centers. In High Availability contact center solutions, the active server actively processes scripts and contacts. A standby server in the same contact center solution monitors and shadows the active server. Each active and standby pair of servers forms a High Availability resilient or replication pair. If the active server fails, the standby server detects the failure and starts processing calls.

The level of Contact Center application High Availability you achieve depends on your complete enterprise contact center solution, including the underlying network infrastructure. In a Mission Critical High Availability solution, the active and standby servers are constantly communicating with each other and monitoring system components. The High Availability - System Management and Monitoring Component (SMMC) monitors network communications, network latency, and contact center components. If a Contact Center component or network link fails, SMMC detects this failure and takes appropriate action.

If a network communication failure occurs, the active and standby servers use a Trusted IP address to diagnose network connectivity faults. Use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.

If SMMC on the active server cannot communicate with SMMC on the standby server, SMMC pings the Trusted IP address to determine if the network outage is local or remote. If the active server SMMC can communicate with the Trusted IP address, the network outage is remote and the active server continues processing contacts. If the active server SMMC cannot communicate with the Trusted IP address or the standby server, the network outage is local and the active server therefore stops processing contacts.

If SMMC on the standby server cannot communicate with the active server, but can communicate with the Trusted IP address, SMMC enables call processing on the standby server. If SMMC on the standby server cannot communicate with the active server or with the Trusted IP address, the standby server shuts down.

If a critical service on the active Contact Center server fails, a switchover occurs immediately. Critical services are services that are required to route incoming real time calls to the Avaya Aura® Agent Desktop application. The standby Contact Center server becomes active and takes over processing. The remaining services on the crashed server are gracefully halted in order to place the original active in a known state for follow-up analysis of the fault.

Mission Critical HA uses database and in-memory replication to ensure that the standby server is fully synchronized with the active server. If switchovers are not enabled and if the standby server cannot communicate with the active server for a period of time greater than the configured Network Timeout time, the standby server is out of sync and it therefore shuts down.

You must select a value for the Network Timeout tolerance that takes account of the quality of the network between the active and standby Contact Center servers. Avaya Aura® Contact Center provides tools, described in this document, to help you to select a suitable value.

To reinstate High Availability resiliency, after an Avaya Aura® Contact Center switchover, you must ensure the active and standby servers can communicate with each other and then manually restart the standby server (and enable switchovers if required).

.

Switchover

In a Mission Critical High Availability campus solution, a CCMS or CCT service failure, or a CCMS, CCT or CCMM hardware, network, or database failure can initiate a switchover but only in the following situations:

- The active and standby servers are in running state.
- The active server is running. All the critical CCMS and CCT services are monitored and running.
- The servers have Switchover enabled.
- The active server database and standby server database are synchronized. The standby server database is shadowing the active server database.
- The standby server can communicate (ping) with the Trusted IP address.

During normal operation, the (CCMS, CCT, and CCMM) applications on the active server process customer contacts. If a Contact Center active server fails, and if the above switchover conditions are met, all the Contact Center applications and services on the active server are stopped. A complete Contact Center server switchover occurs. All Contact Center applications on the standby server are started and they begin processing customer contacts.

If the Contact Center Administrator uses the Windows Service Control Manager (SCM) to stop a monitored service on an active server, a switchover occurs. If the Contact Center Administrator uses System Control and Monitor Utility (SCMU) to stop a monitored service on an active server, a switchover does not occur.

Agent experience during a Contact Center switchover

If any Avaya Aura® Contact Center application or server fails, the Mission Critical High Availability solution provides a zero-touch Avaya Aura® Agent Desktop experience. Agent Desktop agent contacts in progress continue without interruption, agent login and state are maintained. New contacts that arrive during the switchover are treated and routed without delay.

In a Mission Critical High Availability campus solution Agent Desktop clients are registered with both Communication Control Toolkit servers. In multimedia-enabled systems Agent Desktop clients are launched from the Managed IP address of the Contact Center Multimedia servers.

Supervisor experience during a Contact Center switchover

Agent states such as logged in state and ready state are maintained when the active Avaya Aura® Contact Center server fails, and this is reflected in the Real Time Displays (RTDs) being observed. Not all real-time values such as time in state are maintained however, and the supervisor notices that some RTD items are reset. The supervisor informs IT staff, who receive an automatic email/SNMP switchover notification in parallel, and can then proceed with the Customer's normal follow-up procedure for dealing with a server switchover.

Configure RTDs to use multicast as opposed to unicast in order eliminate the need to manually restart the RTD after an Avaya Aura® Contact Center server switchover.

After a switchover, the supervisor may need to refresh the client Web browser.

During the switchover there is a small interval of time when contact processing is operational but the reporting subsystem is not. During this interval, new contacts entering the contact center are routed correctly but not reported on. Real-time and historical reports do not have an accurate representation of the contacts that enter while the reporting subsystem is unavailable. Customer calls are not impacted, calls are routed to a skilled agent.

Administrator experience during a Contact Center switchover

In a Mission Critical High Availability campus solution, the contact center Administrator launches Contact Center Manager Administration using the Managed name of the pair of campus servers.

If an active Contact Center Manager Server, Communication Control Toolkit, or Contact Center Manager Administration application or server fails, the Contact Center Manager Administration client Web browser continues to use the managed name and the contact center Administrator continues working by refreshing the client Web browser.

Campus High Availability

In a campus High Availability environment the standby and active Avaya Aura® Contact Center servers are in the same location. The active and standby Avaya Aura® Contact Center servers must be in the same subnet IP address range for campus High Availability resiliency to work.

In a campus solution the active and standby server have different static IP addresses, but share a common virtual Managed IP address.

Managed IP address

Avaya Aura® Contact Center supports the active/standby High Availability model. The active server processes contacts. The standby server takes over when the active server fails or is shutdown for maintenance.

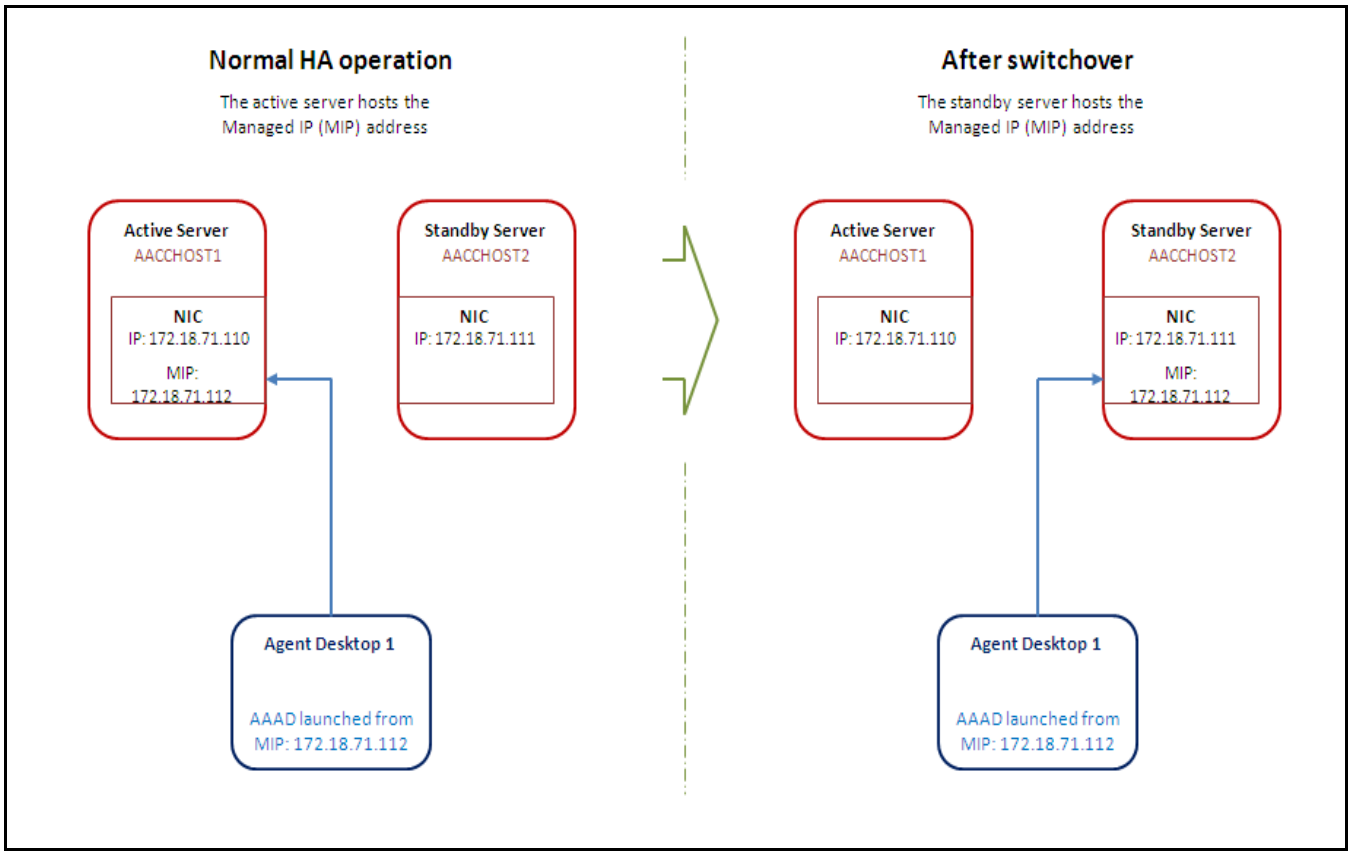
A Managed IP address is a virtual IP address that is attached to a Network Interface Controller (NIC) on the active server.

Each High Availability application server is assigned a static IP address. After the active server in each replication pair is determined, the active server attaches the Managed IP address to its network interface. The Managed IP address is assigned only to the active server. All other contact center applications and clients connect to that application using the Managed IP address. The standby server assumes this same Managed IP address, if it takes over processing and becomes the active application. The active server stops hosting the Managed IP when it stops being the active server. When the standby server starts-up to take over call processing, it attaches the Managed IP address to it's network interface.

The following diagram shows how a Managed IP address is used in High Availability (HA) enabled solutions.

1. In normal HA operation, the active server hosts the Managed IP address. The active server processes Customer phone calls and email messages. Client computers, running Avaya Aura® Agent Desktop, connect to the active server using this Managed IP (MIP) address.
2. If a High Availability switchover occurs, the standby server hosts the Managed IP address by attaching this virtual IP address to its Network Interface Controller (NIC). The standby server then takes over call processing and becomes the active server.
3. The client computers continue using this Managed IP (MIP) address, but now they are communicating with the standby server to process contacts.

Example of a Managed IP address in a High Availability solution



Managed name

A Managed name that maps to the Managed IP address must also be configured. This Managed name may be configured on a Domain Name System (DNS) or in the hosts file on the servers that are connecting to the High Availability (CCMS, CCMA, CCT, and CCMM) servers.

You use the Managed IP address or Managed name when configuring remote IP addresses or server names: do not use the physical name or IP address.

Campus switchover

In a campus environment a switchover from the active to the standby server (using the managed IP address) appears as a server restart to external applications. Connected external applications perceive a link loss, and shortly thereafter a re-connect attempt to the same IP address will succeed (when the standby server has taken over the managed IP).

You can invoke a switchover manually, or have a switchover triggered automatically when communication is lost or if a service fails. For switchover to occur the standby server must be shadowing the active server and switchover must be enabled.

The main advantages of Campus High Availability are:

- Automatic switchover
- Faster switchover time
- Minimal switchover steps
- Third-party applications connect to the Managed IP address

Campus High Availability caters for Contact Center application or server failures and offers resiliency for local network failures.

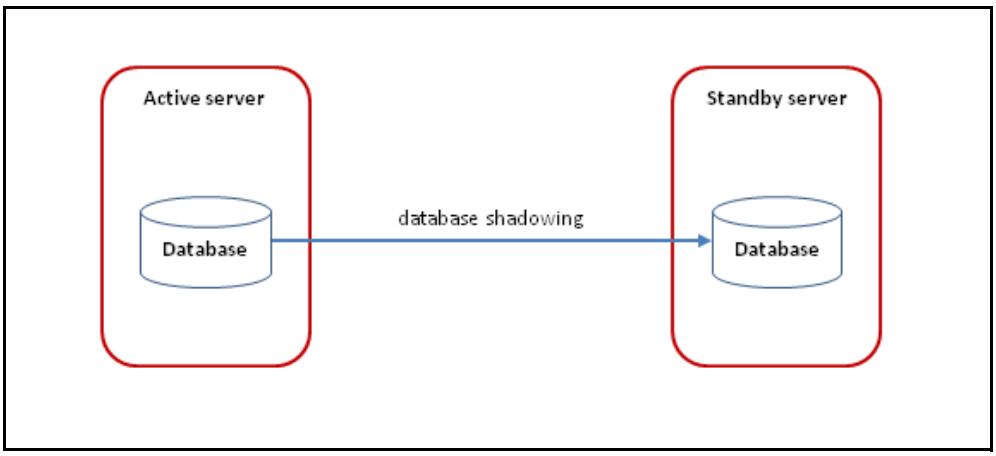
Trusted IP address

The active and standby servers use the Trusted IP address to verify network connectivity. If the active server cannot communicate with the standby server it attempts to communicate with the Trusted IP address. If the active server cannot connect to the Trusted IP address on startup then no Contact Center services start on that server. If the active server cannot communicate with the Trusted IP address, and if shadowing and switchover are enabled, then the active server stops processing contacts and shuts down. The standby server starts processing contacts if it cannot communicate with the active server but can communicate with the Trusted IP address.

Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.

Database Shadowing

Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), and Contact Center Multimedia (CCMM) each store contact center information in a Caché database. This Caché database technology supports database shadowing for fault tolerant and mission critical solutions such as Avaya Aura® Contact Center. To use Caché database shadowing you must have two of each resilient application, an active application server and a corresponding standby application server.



The standby server is constantly retrieving logical records of database updates from the active server so that the standby server always has an “near real-time” copy of the active database. This process is called database shadowing, the standby server is shadowing the active server’s database.

The standby application server shadows the active application server, maintaining a near real-time local copy of the CCMS, CCT, CCMM, and Administration databases. Therefore, the standby server is configured with the most recent data and it can take over from the active server if necessary.

High Availability configuration utilities

The Avaya Aura® Contact Center High Availability feature has the following configuration utilities:

- High Availability Utility (page 22)
- SMMC system tray (page 23)

The Mission Critical High Availability feature uses the High Availability Utility in conjunction with the System Management and Monitoring Component (SMMC) system tray.

High Availability Utility

Configure Mission Critical High Availability resiliency for CCMS, CCT, and CCMM using the High Availability (HA) Utility. The High Availability Utility is used to configure which is the active server and which is the standby server. The HA utility also configures the Managed IP of the active server.

The High Availability Utility on an active server has the following dialog boxes under the Configuration tab:

- Server Mode
  - Configure the IP address for the active and standby servers
  - Configure the IP address for Trusted servers
  - Configure the IP address for the optional Remote Geographic Node
  - Identify if the server is active or standby
  - Enable Switchover
  - Configure the switchover time-out. This is the wait time if a network outage occurs before an automatic switchover occurs
- Notifications
  - Configure an email server for email notifications
  - Configure where and how often to send email notifications
  - Configure the email character set

- System
  - Display information on the system status
  - Verify that database shadowing is running

SMMC system tray

The Contact Center System Management and Monitoring Component (SMMC) system tray gives quick access to action items in your High Availability environment. The SMMC system tray has the following main menu options and action items:

- Start HA System
- Stop HA System
- Disable Switchover
- Enable Switchover
- System Information
- Database Information
- Disable Next Auto Startup
- Select Standby Auto Startup Mode (standby server only)
- Re-enable HA system (this option is available only when the active HA server is running but switchovers are disabled)

To access the SMMC system tray menu, right-click the SMMC icon on the Windows taskbar. The SMMC system tray icon displays the status of the High Availability feature on the server.

In the SMMC system tray, the available menu options depend on the state of the HA System. For example, the Start HA menu option is available only when the High Availability system is in a stopped state. The state of the critical CCT and CCMS services affects the available SMMC system tray menu options. The state of the License Manager, Avaya Media Server, CCMA, and CCMM services does not affect the available SMMC system tray menu options.

The Contact Center System Management and Monitoring Component (SMMC) system tray icons display the status of the High Availability feature on a server, if switchover is enabled or disabled on that server, and if the server can communicate with the High Availability SMMC component on the remote server.

The following table shows the High Availability system status and corresponding SMMC system tray icon.

High Availability status	SMMC icon
Non-HA server in stopped state. High Availability is not configured on this server.	
Non-HA server in starting state. High Availability is not configured on this server.	
Non-HA server in running state. High Availability is not configured on this server.	
Non-HA server in stopping state. High Availability is not configured on this server.	
Active HA server in stopped state. This server is configured as a High Availability active server.	
Active HA server with no connection to remote system. This server is configured as a High Availability active server.	
Active HA server running with connection to remote system, fully HA capable system. A switchover is possible.	
Active HA server running, but switchovers disabled. A switchover is not possible.	
Switchover in progress, the active system is switching over to become a standby system. After the switchover, this server becomes a standby server.	
Standby HA server in stopped state. This server is configured as a High Availability standby server.	
Standby HA server with no connection to remote system. This server is configured as a High Availability standby server.	
Standby HA server running with connection to remote system, fully HA capable system. A switchover is possible.	
Standby HA server running, but switchovers disabled. A switchover is not possible.	
Switchover in progress, the standby system is switching over to become an active system. After the switchover, this server becomes an active server.	

High Availability Utility and SMMC system tray

Use the Mission Critical High Availability Utility to configure High Availability IP addresses and to configure which server is the active server and which is the standby server. Then use the System Management and Monitoring Component (SMMC) system tray to start database shadowing and High Availability functionality.

Avaya Media Server

Avaya Media Server is a software-based media processing platform. All media processing is performed in software on the host CPUs. The Avaya Media Server architecture is uniquely scalable for all core functions of the platform, including media processing, signaling, application execution, and content management.

Avaya Media Server is IP-enabled with a strong focus on Web services and industry standards. The platform is designed for generic multimedia processing and is based on open standards protocols. Avaya Media Server uses standard Session Initiation Protocol (SIP) for signaling and Real-time Transport Protocol (RTP) to transport audio and video, which enables it to work with a wide variety of clients and gateways.

The Avaya Aura® Contact Center DVD contains an enhanced version of Avaya Media Server which contains an additional component—Contact Center Services for Avaya Media Server (CCSM). CCSM provides the Conference, Announcement, and Dialog services required by SIP-enabled Contact Center.

The Avaya Media Server – High Availability feature ensures uninterrupted availability of media processing and reduces loss of processing data when an Avaya Media Server fails. The High Availability feature uses two media servers operating in a standby deployment. Both the servers have identical configuration and provide full media processing capabilities.

The contact center can be scaled up by the addition of more HA pairs of Avaya Media Server servers. You may over-provision media handling capacity if you wish to do so for additional redundancy.

Administrators configure the High Availability feature by designating one server as the primary server and the other as the backup server. Both servers communicate with each other using a heartbeat mechanism.

Interruptions in the heartbeat from the primary server trigger a switchover to the backup server. As both the primary and backup servers are identical in functionality and configuration, the switchover is seamless.

Limitations:

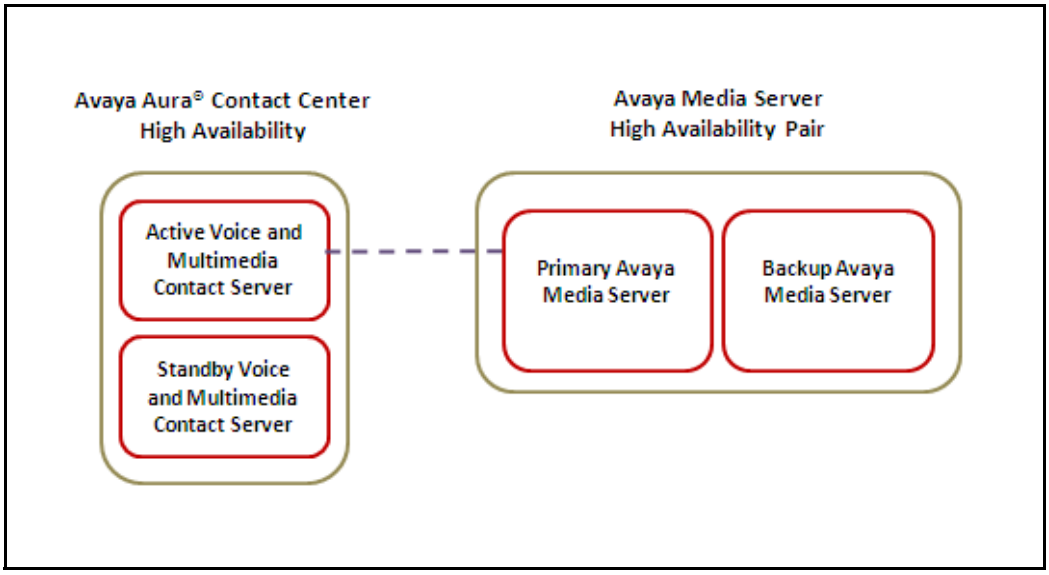
- High Availability can be configured only in 1+1 configuration.
- High Availability is available only if the servers are installed on the Linux operating system.

- Once the backup server becomes active there is no automatic fallback to the primary server.

To restore the primary server the administrator must manually set the backup server status to “Failover”, using Avaya Media Server Element Manager.

Avaya Media Server High Availability Pair

In a High Availability deployment, configure a redundant pair of Avaya Media Server servers. Configure a High Availability primary Avaya Media Server and a High Availability backup Avaya Media Server on two separate servers. In Contact Center Manager Administration, you configure the Avaya Media Server High Availability pair as the media server, using the managed IP address of the cluster, and assign it to handle conference, announcement, and dialog media services. When installed as a High Availability pair, Avaya Media Server uses the Avaya Media Server License Server feature. You install the same license file on the primary server and the secondary Avaya Media Server replicates this license automatically.



Contact Center Manager Administration

Contact Center Manager Administration (CCMA) is a browser-based tool for contact center administrators and supervisors to manipulate the data and reporting for the Contact Center Manager Server database. You can use Contact Center Manager Administration to configure contact center resources, contact flows, components, and activities. You can also use Contact Center Manager Administration to define access levels to data and provide dynamic reporting to fit your enterprise business needs.

Active Directory - Lightweight Directory Services data store

Contact Center Manager Administration uses Active Directory - Lightweight Directory Services (AD-LDS) and other data files to store application data. The following data is stored in AD-LDS:

- user information and details
- access classes
- partitions
- private and graphical real-time reports
- real-time report filters

The following data files are not stored in AD-LDS:

- scheduling data for Contact Center Management assignments
- scheduling data for historical reports
- historical report output files
- user-created historical reports imported into Contact Center Manager Administration
- real-time report exported files
- Emergency Help exported files
- Report Creation Wizard user-created formulas (stored in the file RCW.mdb)
- Report Creation Wizard user-created reports and report definitions
- Audit Trail events

Use the Contact Center Manager Administration Backup and Restore utility to manage the data not stored in AD-LDS.

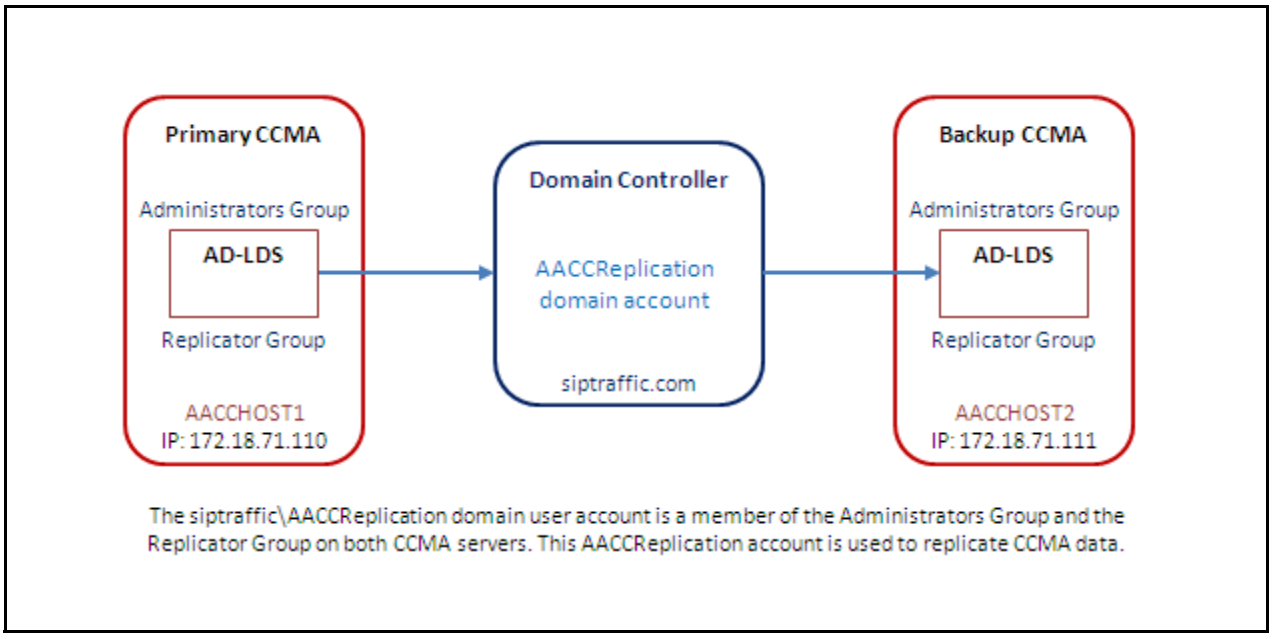
Active Directory Lightweight Directory Services replication

Active Directory Lightweight Directory Services (AD-LDS) supports data replication. AD-LDS replication allows the AD-LDS instance on one server to share data with an AD-LDS instance on another server, ensuring that the replicated data is the same across both servers. AD-LDS replication ensures that when data is added, deleted or modified on either the primary or standby CCMA, that the result is replicated to the other server. If the primary server fails, AD-LDS replication ensures the standby server is configured with the most recent data.

The primary server and the standby replication server must both be in the same Windows domain for AD-LDS replication to work. AD-LDS replication uses a common windows account, used by both servers, to copy or replicate data from the primary CCMA AD-LDS to the standby CCMA AD-LDS.

The following diagram shows a typical CCMA AD-LDS replication situation. The Windows domain account, siptraffic\AACCReplication, is used to replicate data between the two CCMA instances.

Example of AD-LDS replication in action



AD-LDS replication is a real-time operation and can be used in conjunction with CCMA backup and restore. Not all data is replicated with AD-LDS, some manual synchronization is required for all user created reports and wallboards after switchover.

Contact Center Manager Administration – High Availability

The primary server is always the primary server. If the primary server fails, the standby CCMA is still a standby CCMA, they do not switch roles. To restore CCMA solution resiliency, you must repair and reinstate the primary server, or install a new primary server using the same details as the previous primary CCMA. After a primary CCMA failure or shutdown, AD-LDS replication ensures that data stored in AD-LDS is available on the standby server. Data not stored in AD-LDS must be manually restored to the standby CCMA using the CCMA Backup and Restore utility.

A High Availability CCMA replication solution contains a primary CCMA server and a standby CCMA server. You must configure CCMA AD-LDS replication when you are installing CCMA. The primary CCMA server is installed with the Enable CCMA Replication option not selected. The standby CCMA server is installed with the Enable CCMA Replication option selected. The standby CCMA server replicates the primary CCMA server AD-LDS contents.

In a campus solution, the contact center Administrator launches Contact Center Manager Administration using the managed name of the server.

If an active Contact Center Manager Server, Communication Control Toolkit, or Contact Center Manager Administration application or server fails, the Contact Center Manager Administration client Web browser continues to use the Managed name and the contact center Administrator continues working without interruption.

Contact Center Manager Administration – Data backup and restore

You must regularly back up the primary Contact Center Manager Administration (CCMA) server for the following reasons:

- To avoid loss of data in the event of a server failure: schedule backups to back up your CCMA data at least once a day (or more frequently, based on your Contact Center requirements). Schedule backups during periods of low activity.
- To keep data synchronized between CCMA and CCMS: you must back up and restore CCMA data and your CCMS data at the same time to ensure your contact center functions correctly.
- To keep non AD-LDS data synchronized between the primary CCMA and standby CCMA. For example, if you add or modify user-created reports, you must backup and restore the user-created reports to the standby server.

Use the Contact Center Manager Administration Backup and Restore utility to backup and restore the CCMA (AD-LDS and non-AD-LDS) data. Each CCMA backup contains both AD-LDS and non-AD-LDS data. During a data restore, the CCMA Backup and Restore utility handles AD-LDS and non-AD-LDS data differently. To prevent accidently overwriting replicating AD-LDS data, the CCMA Backup and Restore utility enforces the following rules:

- A primary CCMA backup can be fully restored to a primary CCMA. Both AD-LDS and non-AD-LDS data are restored.
- A primary CCMA backup can be partially restored to a standby CCMA. Only non-AD-LDS data is restored.
- A standby CCMA backup can be fully restored to a standby CCMA. Both AD-LDS and non-AD-LDS data are restored.
- A standby CCMA backup can be partially restored to a primary CCMA. Only non-AD-LDS data is restored.

When you backup the CCMS database, you must ensure that you back up the entire server and the associated databases, including CCMA. Complete backups ensure that the data between the two applications is always synchronized. Furthermore, you must store both backups in the same secure location.

If you install a replicating server, you must still perform regular backups. Unlike Active Directory Lightweight Directory Services (AD-LDS) replication, backups provide snapshots of your CCMA data files at moments in time. Backing up data, and not relying on AD-LDS replication as the only method of backing up CCMA data, is important for the following two reasons:

- Not all CCMA data is stored in AD-LDS, and therefore is not replicated.
- You cannot use AD-LDS replication to roll back data to a specific time, which may be required.

In addition to backing up files, you must record your Real-Time Reporting configuration settings and your Emergency Help configuration settings whenever these settings change. During the restoration process, you must manually re-configure these settings.

In High Availability solutions, you must backup the primary CCMA at least once a day and store the backup in secure network location. Do not store the primary CCMA backup on the primary server. If the primary CCMA is offline and if you are using the standby CCMA, then regularly backup the standby server, because this contains the most recent data. Do not store the standby CCMA backup on the standby server. Always store the CCMA backups in a secure network location.

Recovery after the Primary CCMA software fails

In a High Availability solution, the Contact Center Administrator launches Contact Center Manager Administration using the managed name of the CCMS and CCMA. If the primary CCMA instance fails or is shut down, the Contact Center Administrator continues accessing CCMA by pointing Internet Explorer at the managed name of the remaining standby server.

If the primary CCMA instance fails or is shutdown, AD-LDS replication ensures the remaining CCMA contains the most recent AD-LDS data such as agent and partition data. You must restore the most recent primary CCMA data backup onto the standby CCMA. The standby CCMA is then configured with the most recent (AD-LDS and non-AD-LDS) data.

At this point the primary CCMA is offline and the Contact Center Administrator is using the fully configured standby CCMA. CCMA is no longer replicating and it is therefore no longer resilient.

To reinstate Contact Center Manager Administration High Availability resiliency:

- Restart the primary server.
- Ensure all CCMA services are running. Because AD-LDS data replication is bidirectional, the restarted primary CCMA replicates the AD-LDS data from the standby CCMA.
- On the standby CCMA, backup the CCMA (AD-LDS and non AD-LDS) data.

- Restore the standby CCMA backup (AD-LDS and non AD-LDS) data to the primary CCMA.

The primary CCMA is then configured with the most recent (AD-LDS and non-AD-LDS) data. CCMA High Availability resiliency is restored and the Contact Center Administrator can once again use the primary CCMA.

Recovery after the standby CCMA software fails

In a High Availability solution, if the standby CCMA instance fails or is shut down, the Contact Center Administrator continues accessing CCMA by pointing Internet Explorer at the managed name of the primary server. While the standby CCMA is offline, CCMA is no longer replicating and it is therefore no longer resilient.

To reinstate Contact Center Manager Administration High Availability resiliency:

- Restart the standby CCMA
- Restore the most recent primary CCMA backup to the standby CCMA.

Recovery after the Primary server fails

In a High Availability solution, if the primary server fails the Contact Center Administrator continues accessing CCMA by pointing Internet Explorer at the managed name of the remaining server. While the primary server is offline, CCMA is no longer replicating and it is therefore no longer resilient.

To reinstate Contact Center Manager Administration High Availability resiliency:

- Rebuild the primary server. The new primary server must have the exact same name as the previous primary server.
- Reinstall the Operating System and Internet Information Services (IIS). The new primary server must have the exact same disk partitions, workgroup or domain, OS patches and details as the standby server.
- Restore the most recent primary CCMA backup to the new primary server.
- Restart the primary server. Because AD-LDS data replication is bidirectional the restarted primary CCMA replicates the AD-LDS data from the standby CCMA. The primary server is updated with the most recent AD-LDS contact center data.
- On the standby server, backup the CCMA data.
- Restore this backup CCMA data to the primary server.

The primary CCMA is then configured with the most recent (AD-LDS and non-AD-LDS) data. CCMA High Availability resiliency is restored and the Contact Center Administrator can once again use the primary CCMA.

Recovery after the standby server fails

In a High Availability solution, if the standby server fails the Contact Center Administrator continues accessing CCMA by pointing Internet Explorer at the managed name of the primary server. While the standby server is offline, CCMA is no longer replicating and it is therefore no longer resilient.

To reinstate Contact Center Manager Administration High Availability resiliency:

- Rebuild the standby server. The new standby server must have the exact same name as the previous standby server.
- Reinstall the Operating System and Internet Information Services (IIS). The new standby server must have the exact same disk partitions, workgroup or domain, OS patches and details as the primary server.
- On the primary server, remove the obsolete standby server replication entries from the active CCMA database.
- When reinstalling CCMA software on the new standby server, select AD-LDS replication - Enable CCMA Replication.
- On the primary server, backup the CCMA data.
- Restore this backup CCMA data to the standby server.

The standby server is then configured with the most recent (AD-LDS and non-AD-LDS) data. CCMA High Availability resiliency is restored.

Switchover Handling Script

In SIP-enabled contact centers using the High Availability feature, the Switchover Handling Script handles calls in treatment during a switchover.

Under normal operation calls to the Contact Center are routed to the Master script for processing, treatments and queuing to an appropriate skillset. The active CCMS uses the media processing capabilities of Avaya Media Server to provide ringback, conferencing, and other treatments to these calls.

If the active CCMS is shutdown or fails, a switchover occurs, and the standby CCMS starts processing calls. The standby CCMS is now the active CCMS. New calls that arrive after the switchover are presented to the Master script on the currently active CCMS and call processing continues as normal.

Calls that were in treatment on the Avaya Media Server during the switchover cannot be returned to their original active CCMS because it is no longer available, so these calls are routed to the Switchover Handling Script on the currently active CCMS.

The Switchover Handling Script expedites the calls that were in treatment at the time of the active server failure. This means that calls are queued as quickly as possible to an appropriate skillset for that contact type. This can be a default skillset, or a skillset defined by the contact center Administrator.

Calls in treatment during a switchover may contain data, depending on their position in the script on the active server before the switchover occurred. Avaya recommends that you modify the default Switchover Handling Script to check each call for useful data. If the call has useful data or intrinsics, queue it to the most appropriate skillset as normal. If the call does not have useful data, queue the call to the appropriate default skillset.

Attention: After a High Availability switchover, multimedia contacts may be redirected to a different skillset queue. After a switchover, multimedia contacts are requeued to a skillset appropriate to their contact intrinsics. If the multimedia contacts have insufficient intrinsic data or if the appropriate skillset is Out Of Service, the multimedia contacts are queued to the default contact type skillset. Email contacts transferred to agents or Pulled Closed email contacts that are in-queue at switchover time are re-queued to a skillset after switchover. They are not queued to the agent.

The Switchover Handling script does not support commands that delay the handling of calls.

The Switchover Handling Script does not support the following HDX commands:

- SEND INFO
- SEND REQUEST
- GET RESPONSE

The Switchover Handling Script does not support the following commands:

- EXECUTE SCRIPT
- GIVE BUSY
- GIVE MUSIC
- GIVE OVERFLOW
- GIVE RAN
- GIVE RINGBACK
- GIVE SILENCE

A Switchover Handling Script containing these commands does not validate in Contact Center Orchestration Designer.

The Switchover Handling Script is used only in Mission Critical High Availability solutions.

Other applications cannot start the Switchover Handling Script, and the Switchover Handling Script cannot start other applications.

Attention: You must edit the default Switchover Handling Script. For more information about using Contact Center Orchestration Designer to edit the Switchover Handling Script, see Orchestration Designer commissioning (page 279).

Campus network requirements

In a campus High Availability environment the standby and active servers are in the same location.

Campus High Availability supports LAN environments where the round trip delay between the active and standby servers is less than 80ms, with less than 0.5% packet loss.

Use Link Aggregation Control Protocol (LACP) and Network Interface Controller (NIC) Teaming to eliminate network points of failure in the contact center solution.

Link Aggregation Control Protocol

Link Aggregation Control Protocol (LACP) provides a method to control the bundling of several physical ports together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP).

NIC teaming

NIC teaming is the process of grouping together several physical NICs into one single logical NIC, which can be used for network fault tolerance and transmit load balance. The process of grouping NICs is called teaming. By teaming more than one physical NIC to a logical NIC, high availability is maximized. If one NIC fails, the network connection does not cease and continues to operate on other NICs.

Typically, you configure Network Interface Card (NIC) teaming using hardware-specific utilities supplied by your server or hardware manufacturer. For more information about configuring NIC teaming, see your server documentation.

Avaya Aura® Unified Communications platform

Avaya Aura® Contact Center uses industry-standard SIP and CSTA (TR/87 over SIP) interfaces to communicate with other SIP-enabled devices. Avaya Aura® Contact Center uses a SIP Gateway Manager (SGM) component to support SIP. SIP Gateway Manager (SGM) is a Contact Center Manager Server component and a stand-alone SIP element.

The Avaya Aura® Unified Communications platform supports SIP-enabled interfaces. Integrating Avaya Aura® Contact Center with the Avaya Aura® Unified Communications platform using SIP infrastructure supports multi-nodal communication between customers and contact center agents. This integration gives Contact Center access to and control of Avaya Aura® Communication Manager phones. The Avaya Aura® platform benefits from Contact Center skill-based routing, call treatments, reporting, and the graphical Orchestration Designer component. Avaya Aura® Agent Desktop supports Avaya Aura® Communication Manager phones and continues to support voice, email, Instant Messaging (IM), and Web chat contact types.

Avaya Aura® Communication Manager is an IP Telephony platform for enterprises. It delivers centralized call control for resilient and distributed networks, and it supports a wide range of servers, gateways, analog, digital, and IP-based communication devices. Communication Manager has advanced built-in capabilities, including mobility applications, call center features, and conference calling.

Avaya Aura® Session Manager provides connectivity, integration, and a smooth migration path to SIP-based communications. It is used to deploy SIP telephony alongside existing analog, digital, and IP telephones. Multi-vendor telephony can be integrated for greater collaboration and productivity. The software is centrally managed and supports SIP trunking, SIP stations, and other SIP-based applications.

Calls to the Avaya Aura® Unified Communications platform can be redirected to the Contact Center for processing, treatments and routing to appropriate skillsets. To achieve this, the Avaya Aura® Session Manager (SM) server must be configured to trust the Contact Center Manager Server. To determine which calls to the Avaya Aura® platform are redirected to Contact Center Manager Server for processing, you must configure a routing entry and contact details for the Contact Center Manager Server in Session Manager.

Avaya Aura® Application Enablement Services (AES) are a set of enhanced telephony APIs, protocols, and Web services. AES applications support access to the call processing, media, and administrative features available in Communication Manager. AES applications enable off-the-shelf and custom integration with communications and business applications such as Avaya Aura® Contact Center.

The AES server uses Transport Layer Security (TLS) communication channels for the SIP CTI connection with Contact Center. TLS is a public key encryption cryptographic protocol that helps to secure a communications channel, providing privacy and safety. With public key cryptography, two keys are created, one public and one private. Anything encrypted with either key can be decrypted only with the corresponding key. If a message is encrypted with the server's private key, it can be decrypted only using its corresponding public key, ensuring that the data must have come from the server.

Avaya Aura® Contact Center Release 6.3 supplies a set of default certificates for use with Application Enablement Services. If you do not have access to or do not require a third-party Certificate Authority, you can install these Contact Center default certificates

on your Application Enablement Services server to quickly establish a link between the two systems. The sample solution in this guide uses the Avaya Aura® Contact Center default certificates. The Avaya Aura® Contact Center default certificates are installed on the Contact Center Manager Server at install time and they do not require configuration. You must import these default root certificates into the Avaya Aura® Application Enablement Services server so that it can communicate securely with Avaya Aura® Contact Center.

Unified Communications platform integration

To integrate an Avaya Aura® Unified Communications platform with Avaya Aura® Contact Center, perform the following:

- Identify which calls to the Avaya Aura® Unified Communications platform are contact center calls to be handled by Contact Center. The Contact Center suite of applications provides call treatments, skill-based routing, and reporting.
- Identify which Avaya Aura® Unified Communications phones are to become agent phones (controlled by Contact Center) and associated with Agent Desktop clients.
- Configure Avaya Aura® Session Manager to forward calls, based on a dial pattern, to the Contact Center.
  - Add Contact Center as a SIP Entity on the Avaya Aura® Session Manager.
  - Add a dial pattern that resolves to Avaya Aura® Contact Center.
- Configure the Avaya Aura® Application Enablement Services (AES) to support CSTA (TR/87 over SIP) call control by the Avaya Aura® Contact Center using a certified Transport Layer Security (TLS) communication channel.
  - Enable the TR87 port.
  - Apply TLS Certification.
  - Add Contact Center as a trusted host.

The Avaya Aura® Contact Center must then be configured to accept, control, and treat calls originating from the Avaya Aura® Unified Communications platform.

- Detail the voice and CTI proxy addresses and ports.
- Add the route point.

The Avaya Aura® Unified Communications platform can then route calls to Avaya Aura® Contact Center.

High Availability Network Timeout optimization

This section describes how to optimize the Contact Center Mission Critical High Availability feature for your contact center solution network.

Avaya Aura® Contact Center supports High Availability for fault tolerant and mission critical contact centers. In High Availability contact center solutions, the active server actively processes scripts and contacts. A standby server in the same contact center solution monitors and shadows the active server. Each active and standby pair of servers forms a High Availability resilient or replication pair. If the active server fails, the standby server detects the failure and starts processing calls.

The level of Contact Center application High Availability you achieve depends on your complete enterprise contact center solution, including the underlying network infrastructure. In a Mission Critical High Availability solution, the active and standby servers are constantly communicating with each other and monitoring system components. The High Availability - System Management and Monitoring Component (SMMC) monitors network communications, network latency, and contact center components. If a Contact Center component or network link fails, SMMC detects this failure and takes appropriate action.

If a network communication failure occurs, the active and standby servers use a Trusted IP address to diagnose network connectivity faults. Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.

If SMMC on the active server cannot communicate with SMMC on the standby server, SMMC pings the Trusted IP address to determine if the network outage is local or remote. If the active server SMMC can communicate with the Trusted IP address, the network outage is remote and the active server continues processing contacts. If the active server SMMC cannot communicate with the Trusted IP address, the network outage is local. Therefore the active server stops processing contacts, and SMMC on the standby server enables processing calls.

If SMMC on the standby server cannot communicate with the active server, but can communicate with the Trusted IP address, SMMC enables call processing on the standby server.

To support the Mission Critical HA switchover of contact center voice calls, SMMC must quickly determine if communication delays are due to normal network latency or if the delays are indicative of a network outage. SMMC balances the need for a rapid response to network outages with the need to avoid un-necessary switchovers. SMMC uses a network latency threshold (defined in milliseconds) to differentiate between normal network latency and a network outage.

- Network communication delays shorter than the threshold are treated as expected delays.

- Network communication delays longer than the threshold are treated as potential network outages, and SMMC considers corrective action.

You must configure the High Availability SMMC Network Timeout threshold value high enough to be tolerant of normal network latency, but low enough to be responsive if a network failure occurs.

High Availability Network Timeout calculation

The High Availability-System Management and Monitoring Component (SMMC) uses a Network Timeout threshold value to distinguish between normal network latency and a potential network outage. The SMMC Network Timeout is the length of time SMMC network connectivity tests can continue to fail consecutively before corrective action is considered.

SMMC tests network connectivity between High Availability components by default every 100 milliseconds (100ms). The High Availability SMMC Network Timeout value sets the maximum length of time these network connectivity tests can continue to fail consecutively before corrective action is considered. The default Network Timeout is 400ms.

Example:
If SMMC Network Timeout is set to 400ms, High Availability requires 4 consecutive failed network connectivity tests before the remote system is marked as unreachable. In this case, if switchovers are enabled, an attempt to switchover is made.

It is important that you determine the optimum SMMC Network Timeout threshold value for your contact center network. If the threshold is set too high, High Availability may not recognize network outages and switchovers may not occur when necessary. If the Network Timeout threshold is set too low, frequent and unnecessary switchovers may occur. This is basically a matter of determining how long SMMC waits before declaring a network delay as a potential network outage and taking the appropriate action.

SMMC tests network connectivity between High Availability components and it records the details of these connectivity tests in trace log files. The SMMC trace log files contain sufficient statistical data about SMMC communications in your network to characterize the network behavior for a High Availability contact center solution. You can use this SMMC statistical communications data to optimize your solution configuration.

You use the Network Log Analyzer utility (NetworkLogAnalyser.exe) to analyze the SMMC trace log files and determine the optimum Network Timeout value for your network.

The Network Log Analyzer utility (NetworkLogAnalyser.exe) is installed on each CCMS server in the SMMC utility default location:

D:\Avaya\Contact Center\Manager Server\CCSMMC\util

For additional help and instructions about using the Network Log Analyzer utility, open a command prompt in the SMMC utility directory and type "NetworkLogAnalyser.exe -h". The SMMC utility directory also contains a Microsoft Excel spreadsheet "network-analysis.xlsm".

To determine the optimum HA SMMC Network Timeout threshold value:

1 Install the active and standby servers in your enterprise contact center network.

2 Using the HA utility, configure the HA servers using the default Network Timeout value of 400ms.

3 Do not select "Enable Switchover".

4 Leave the servers running for a number of days and do not disturb the network subnet where the HA nodes are installed and running.

5 After a few normal busy days, retrieve the active server SMMC log files from the folder D:\Avaya\Logs\Common Components\SMMC:
—CC_SMMC_NM_X.log

6 Copy the SMMC log files into the same folder as the Network Log Analyzer utility.

7 On the active server, at the command prompt, type:

```
NetworkLogAnalyser.exe CC_SMMC_NM_1.log CC_SMMC_NM_2.log
```

8 The Network Log Analyzer utility processes the SMMC statistical network data in the log file and recommends a Network Timeout value.
For example:

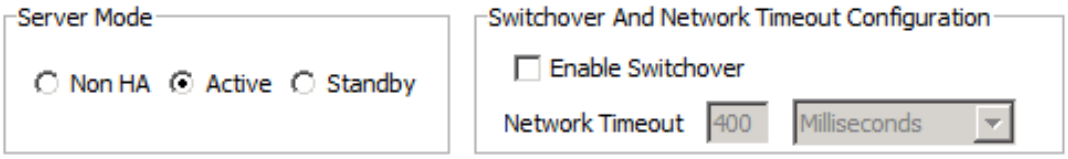
```
$> NetworkLogAnalyser.exe CC_SMMC_NM_1.log
....
....
===== OUTAGES PACKET DATA ANALYSIS END ====
Recommendation:
---------------
Network Timeout= 2x Max(Outage_Duration)= 2x 325ms = 650ms
```

While processing the statistical data, the Network Log Analyzer utility also produces a coma-separated file (network-analysis.csv) that can be imported in to Microsoft Excel using the network-analysis.xlsm spreadsheet.

9 Using the HA utility, re-configure the active server Network Timeout value. In the above example the recommended Network Timeout value is 650 ms, enter this optimized Network Timeout value in the HA configuration utility.

10 Select HA Enable Switchover.

Example of High Availability utility with the default Network Timeout setting



Your High Availability settings are now optimized to your enterprise contact center network. The High Availability - System Management and Monitoring Component (SMMC) is now configured to be responsive to network outages, without causing unnecessary switchovers.

Example solution details

This chapter lists the details of the Avaya Aura® Contact Center servers and Avaya Aura® Unified Communications platform components used in the examples described in the solution description.

Contact Center servers

The following table lists all the values for the Contact Center example servers.

Contact Center server installation values

Configuration Item	Example value	Equivalent value for your system
Active Voice and Multimedia Contact Server IP address	172.18.71.110	
Active Voice and Multimedia Contact Server name	AACCHOST1	
Active Voice and Multimedia Contact Server operating system administrator username	Administrator	
Active Voice and Multimedia Contact Server operating system administrator password		
Standby Voice and Multimedia Contact Server IP address	172.18.71.111	
Standby Voice and Multimedia Contact Server name	AACCHOST2	
Standby Voice and Multimedia Contact Server operating system administrator username	Administrator	
Domain administrator password		
Primary Avaya MS server IP address	172.18.71.113	
Primary Avaya MS server name	AMSHOST1	
Backup Avaya MS server IP address	172.18.71.114	

(1 of 2)

Contact Center server installation values

Configuration Item	Example value	Equivalent value for your system
Backup Avaya MS server name	AMSHOST2	
Avaya MS operating system local administrator username	root	
Avaya MS operating system local administrator password		
Avaya MS operating system maintenance user group	amsgroup	
Avaya MS operating system maintenance username	amsuser	
Avaya MS operating system maintenance password		
CCMS Login ID	sysadmin	
CCMS Login password		
(2 of 2)		

Contact Center server configuration values

Configuration Item	Example value	Equivalent value for your system
Local SIP Subscriber MS Locale	en_us	
Local SIP Subscriber domain	siptraffic.com	

Avaya Media Server configuration values

Configuration Item	Example value	Equivalent value for your system
Service IP address	172.18.71.115	

Unified Communications platform servers

The following table lists the values of the Unified Communication platform example components.

Unified Communication server values

Configuration Item	Example value	Equivalent value for your system
Communication Manager server IP address	172.18.66.76	
Communication Manager server name	HCAP6CM	
Communication Manager administrator username		
Communication Manager administrator password		
System Manager server IP address	172.18.66.74	
System Manager server name		
System Manager administrator username	admin	
System Manager administrator password		
Credential name (for TLS connection validation)		
Session Manager server SIP Entity name	Vedupsm1	
Session Manager server SIP Entity IP address	172.18.66.78	
Session Manager server name		
Session Manager administrator username		
Session Manager administrator password		
Local SIP Subscriber MS Locale	en_us	
Local SIP Subscriber domain	siptraffic.com	
Routing location		
Location pattern	172.18.*	
Contact Center SIP entity	AACCHOST1	

(1 of 2)

Unified Communication server values

Configuration Item	Example value	Equivalent value for your system
Dial Pattern	52xxx	
Dial Pattern min.	5	
Dial Pattern max	5	
Application Enablement Services server IP address	172.18.112.40	
Application Enablement Services server name	f81aes4docs	
Application Enablement Services administrator username	craft	
Application Enablement Services administrator password	craft01 (default)	

(2 of 2)

Domain Administrator requirements

The following section describes the solution domain resources required for an Avaya Aura® Contact Center High Availability solution. You may need to ask your Domain Administrator to provide these domain resources.

High Availability and Domain Name System (DNS)

Ask your Domain Administrator to add a Domain Name System (DNS) static entry for the active and standby servers and one additional DNS static entry for each managed name and associated Managed IP address.

The High Availability – Voice and Multimedia Contact Server DNS requirements:

Voice and Multimedia Contact Server details	**Example value**	**Your solution**
Active server name	AACCHOST1	
Active server IP Address	172.18.71.110	
Standby server name	AACCHOST2	
Standby server IP Address	172.18.71.111	
Managed server name	AACCMANHOST	
Managed IP Address	172.18.71.112	

The High Availability – Avaya Media Server server DNS requirements:

AMS server details	**Example value**	**Your solution**
Primary server name	AMSHOST1	
Primary server IP Address	172.18.71.113	
Backup server name	AMSHOST2	
Backup server IP Address	172.18.71.114	
Managed server name	AMSMANHOST	
Managed (Service) IP Address	172.18.71.115	

CCMA Replication account

The primary server and the standby replication server must both be in the same Windows domain for AD-LDS replication to work. CCMA Active Directory - Lightweight Directory Services (AD-LDS) replication uses a common windows account, used by both CCMAs, to copy or replicate data from the primary CCMA to the standby CCMA. Request this CCMA replication account from your Network or Domain Administrator.

CCMA Replication account	**Example value**	**Your solution**
CCMA AD-LDS replication account	AACCReplication	

Agent Desktop – Domain Organizational Unit and Group Policy

Avaya Aura® Contact Center agents use a domain account to log on to a desktop computer and use Agent Desktop. Ask your Domain Administrator to create a domain user account for each Contact Center agent (if they do not already exist). Add the agent desktop computers to the domain, and then add the desktop computers to a Windows domain organizational unit (OU). Avaya Aura® Contact Center supplies a Group Policy – Administrative Template that must be applied to the Agent Desktop domain Organizational Unit.

Ask your Domain Administrator to create a Windows domain Organizational Unit (OU) and to ensure that all Agent Desktop user accounts are a member of this OU. Ask your Domain Administrator to apply the Avaya Aura® Contact Center Group Policy – Administrative Template to this Agent Desktop Organizational Unit (OU).

For more information about the Avaya Aura® Contact Center – Group Policy Administrative Template, see Agent Desktop – Client software installation (page 317).

Unified Communications Platform integration section

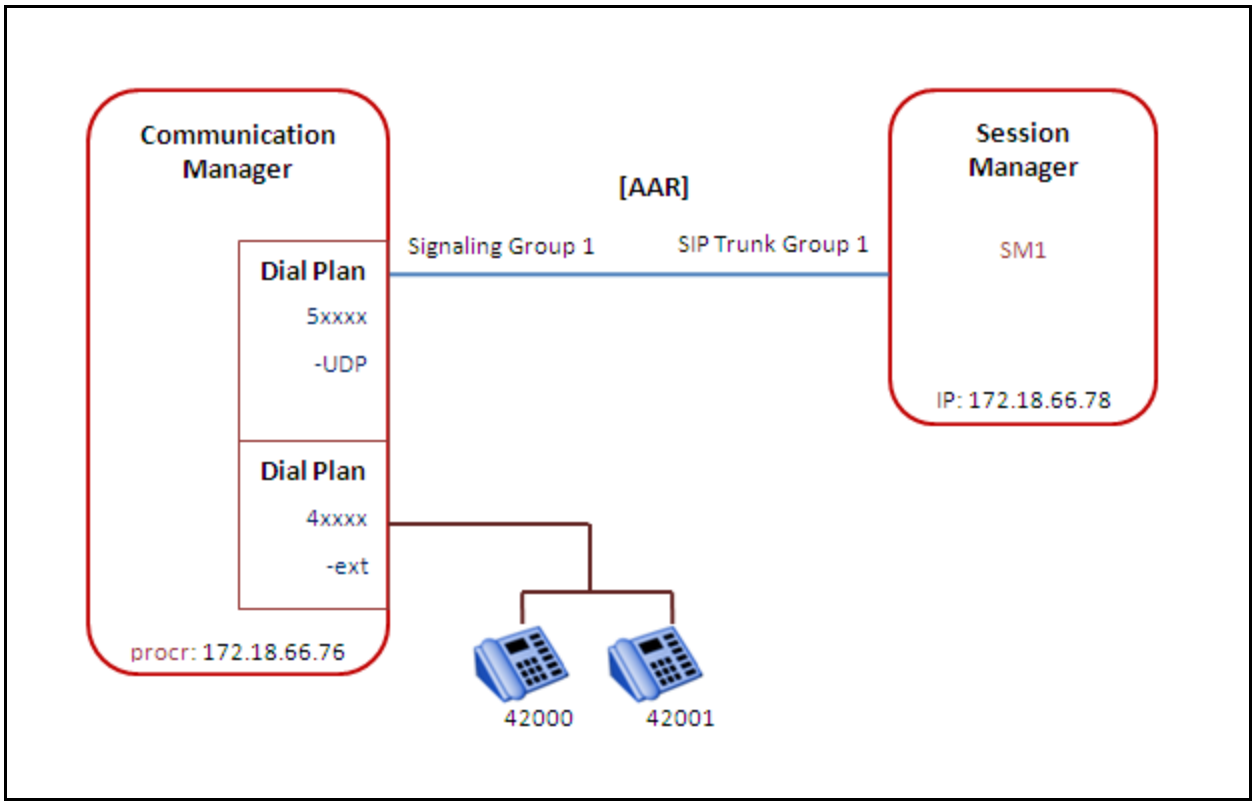
- Unified Communications – Communication Manager configuration (page 49)
- Unified Communications – Session Manager configuration (page 71)
- Unified Communications – Application Enablement Services configuration (page 97)

Unified Communications – Communication Manager configuration

Avaya Aura® Communication Manager delivers centralized call control for resilient and distributed networks. Communication Manager supports a wide range of servers, gateways, analog, digital, and IP-based communication devices.

The following diagram shows a typical Communication Manager deployment and configuration. The procedures and dial plan in this section are based on this diagram.

Example of Communication Manager configuration



Communication Manager phones

To ensure proper integration and Avaya Aura® Contact Center call control, Communication Manager stations (phones) must be configured as follows:

- A maximum of 2 Call Appearance lines per agent station
- Restrict Last Appearance enabled
- Call Forwarding (including Coverage Path) disabled, as it is not supported

- Priority call feature disabled, as it is not supported
- IP Softphone enabled

Communication Manager solution
In addition to the above station configuration, you must configure the Communication Manager to route calls to and from Avaya Aura® Contact Center through SIP using Avaya Aura® Session Manager. You must also configure Communication Manager to communicate with Application Enablement Services (AES) in order to facilitate the station control originating from the Avaya Aura® Contact Center to AES (TR87) communication (CTI Link in Communication Manager).

Communication Manager System Access Terminal (SAT) navigation
Configure Avaya Aura® Communication Manager using the System Access Terminal (SAT) interface.

When using a w2ktt Terminal Emulator, the following shortcuts are available:
—To save information, press Esc followed by e.
—To cancel, press Esc followed by x.
—To move onto next page, press Esc followed by n.
—To go to previous page, press Esc followed by p.
—To erase information, use the spacebar.
—To get help, press Esc followed by h, or type ‘help’.

Logging on to Communication Manager

Log on to Avaya Aura® Communication Manager to configure parameters and resources for integration with Avaya Aura® Contact Center.

Procedure steps

Step	Action
1	Using an SSH client such as PuTTY, begin an SSH session using the Communication Manager IP address. For example, for the IP address of the Communication Manager, type 172.18.66.76.
2	Click **Open**.
3	When prompted enter the user name and password for the Communication Manager.
4	Press return to ignore terminal selection and when prompted for high priority session, enter **n**.
5	To access the System Access Terminal (SAT), type **sat** and enter the same password used above.

6 When prompted, enter a preferred terminal type. For example, select the **w2ktt** Terminal Emulator.

--End--

Administering IP Node Names

The nodes defined in the Avaya Aura® Communication Manager – IP Node Names form are used in other configuration screens to define the SIP signaling groups between Communication Manager and the Avaya Aura® Session Managers.

Procedure steps

Step	Action
1	Use the System Access Terminal (SAT) interface **change node-names ip** command to enter the node name and IP address for the Avaya Aura® Session Manager, for example SM1, 172.18.66.78.

--End--

Procedure job aid

The following example of a Communication Manager – IP Node Names display shows a Session Manager: SM1.

Communication Manager - IP Node Names

```
display node-names ip
                                  IP NODE NAMES
    Name                 IP Address
SM1                   172.18.66.78
SM2                   172.18.66.80
default               0.0.0.0
f81aes4docs           172.18.112.40
procr                 172.18.66.76
procr6                ::
```

```
( 6  of 6    administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

Note the **procr** name, as this is the Avaya Aura® Communication Manager processor interface. The Communication Manager processor (procr) IP address is 172.18.66.76.

In other Avaya configurations such as an Avaya G650 Media Gateway, the C-LAN interface address must be used as the SIP signaling interface to Session Manager, rather than the processor address (node name procr).

Note the Avaya Aura® Application Enablement Services node name and IP address: for example,172.18.112.40.

Verifying the IP Network Region

On the Communication Manager IP Network Region form, verify that the Authoritative Domain name matches the contact center SIP domain name.

Procedure steps

Step	Action
1	Use the System Access Terminal (SAT) interface **display ip-network-region** command to verify that the **Authoritative Domain** names matches the contact center SIP domain name.

--End--

Procedure job aid

The following example of a Communication Manager – IP Network Region form, shows Authoritative Domain configured as siptraffic.com.

Communication Manager - IP Network Region

```
display ip-network-region 1                                   Page   1 of  20
                              IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: siptraffic.com
    Name:
MEDIA PARAMETERS                  Intra-region IP-IP Direct Audio: yes
      Codec Set: 1                Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                        IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Configuring a SIP Signaling Group for the Session Manager

On the Avaya Aura® Communication Manager, configure a SIP Trunk Group for communication between Communication Manager and the Avaya Aura® Session Manager.

Avaya Aura® Communication Manager uses a SIP Signaling Group and an associated SIP Trunk Group to route calls to an Avaya Aura® Session Manager.

Procedure steps

Step	Action
1	Use the System Access Terminal (SAT) interface **add signaling-group <s1>** command to add a signaling group for the Session Manager, where s1 is an un-allocated signaling group.
2	You must disable the IP Multimedia Subsystem (IMS) on the Communication Manager - Signaling Group. Ensure that your signaling group has the IMS Enabled? value set to n.

--End--

Procedure job aid

The Communication Manager – SIP Signaling Group for the Avaya Aura® Session Manager, SIP Signaling Group number 1.

Communication Manager - SIP Signaling Group

```
display signaling-group 1
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tls
       Q-SIP? n                                        SIP Enabled LSP? n
    IP Video? n                                 Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr                 Far-end Node Name: SM1
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                         Far-end Network Region: 1
                                  Far-end Secondary Node Name:
Far-end Domain: siptraffic.com
                                           Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate               RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload         Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                  IP Audio Hairpinning? n
         Enable Layer 3 Test? y                Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n         Alternate Route Timer(sec): 2
```

The following table lists the main SIP Signaling Group variables and appropriate values.

Variable	Value
Group Number	The number of the signaling group. For example, 1.
Group Type	The type of protocol used for this signaling group. For example, enter "sip".
Transport Method	Transport can be accomplished using either TCP or TLS. TLS is set by default.
Near-end Node Name	The node name of the near-end CLAN IP interface used for trunks that use this signaling group which must be already administered. In this example, use the Communication Manager node name (procr).

Variable	Value
Far-end Node Name	The node name of the far-end CLAN IP interface used for trunks that use this signaling group which must be already administered. The Session Manager node-name must be entered here. To match the Session Manager in this worked example, this must be "SM1".
Far-end Domain	The name of the IP domain that is assigned to the far-end of the signaling group. For example "siptraffic.com". This must match the Communication Manager - IP Network Region Authoritative Domain, and the Contact Center SIP domain name.

Configuring a SIP Trunk Group for the Session Manager

On the Avaya Aura® Communication Manager, configure a SIP Trunk Group for communication between Communication Manager and the Avaya Aura® Session Manager. Configure one SIP Trunk Group for each SIP Signaling Group associated with a Session Manager.

Avaya Aura® Communication Manager uses a SIP Signaling Group and an associated SIP Trunk Group to route calls to an Avaya Aura® Session Manager.

Procedure steps

Step	Action
1	Use the System Access Terminal (SAT) interface **add trunk-group <t1>** command to add a SIP Trunk Group for the Session Manager, where t1 is an un-allocated trunk group.

--End--

Procedure job aid

The Communication Manager – SIP Trunk Group for the Avaya Aura® Session Manager, SIP Trunk Group number 1.

Communication Manager – SIP Trunk Group

```
display trunk-group 1                                          Page   1 of  22
                              TRUNK GROUP

Group Number: 1                    Group Type: sip            CDR Reports: y
  Group Name: to SM1                     COR: 1        TN: 1        TAC: *001
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                          Member Assignment Method: auto
                                                    Signaling Group: 1
                                                  Number of Members: 255
```

The following table lists the main SIP Trunk Group variables and appropriate values.

Variable	Value
Group Number	The number of the trunk group. For example, 1.
Group Type	The type of protocol used for this trunk group. For example, enter "sip".
Group Name	A unique name that provides information about this trunk group. Can be up to 27 characters. For example enter "to SM1".
TAC	The TAC (Trunk Access Code) is the number that must be dialed to access the trunk group. A different TAC must be assigned to each trunk group. The characters “*” and “#” can be used as the first character in a TAC and it accepts a one to four digit number. For example, enter “*001”.
Direction	The direction of traffic on this trunk group. Traffic on this trunk group is incoming and outgoing (two-way).

Variable	Value
Service Type	The service for which the trunk group is dedicated. In this case a general purpose service “tie” is used.
Signaling Group	The signaling group to be used in accordance with this trunk group. Since this is created for communication between Communication Manager and the Session Manager “1” is used in this case.

Configuring a Route Pattern

On the Avaya Aura® Communication Manager, configure a route pattern for the Avaya Aura® Session Manager SIP trunk group.

Each Communication Manager route pattern contains a list of trunk groups that can be used to route calls. The maximum number of route patterns and trunk groups allowed depends on the configuration and memory available in your system.

Procedure steps

Step	Action
1	Use the System Access Terminal (SAT) interface **change route-pattern n** command to add a Route Pattern, where n is an available route pattern.

--End--

Procedure job aid

This Communication Manager – Route-pattern (number 1) shows the SIP Trunk Groups for the Session Manager, number 1.

Communication Manager – Route Pattern

```
display route-pattern 1                                          Page   1 of   3
                   Pattern Number: 1   Pattern Name: SM
                                 SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                              DCS/ IXC
    No          Mrk Lmt List Del  Digits                              QSIG
                                  Dgts                                Intw
 1: 1    0                                                            n    user
 2: 2    0                                                            n    user
 3: 7    0                                                            n    user
 4:                                                                   n    user
 5:                                                                   n    user
 6:                                                                   n    user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                   Dgts Format
                                                           Subaddress
 1: y y y y y n  n           rest                                      next
 2: y y y y y n  n           rest                                      next
 3: y y y y y n  n           rest                                      next
 4: y y y y y n  n           rest                                      none
 5: y y y y y n  n           rest                                      none
 6: y y y y y n  n           rest                                      none
```

Administering the Dial Plan for routing and extensions

On the Avaya Aura® Communication Manager edit the Dial Plan to add your routing and the agent extensions (workstations).

The Dial Plan Analysis Table defines the dialing plan for your system. Communication Manager uses dialplans to define how dialed digits are interpreted, and how many digits to expect for each call.

Procedure steps

Step	Action
1	On the Avaya Aura® Communication Manager, use System Access Terminal (SAT) interface to create a dialplan for routing and the agent extensions (workstations) using the **change dialplan analysis** command.

--End--

Procedure job aid

This Communication Manager Dial Plan analysis table shows 5-digit extensions in the 4xxxx range (call type: extension) and 5-digit routing in the 5xxxx range (call type: Uniform Dial Plan (UDP)).

The Call Type column in the Dial Plan Analysis Table indicates what the system does when a user dials the digit or digits indicated in the Dialed String column. The Total Length column indicates how long the dialed string is for each type of call.

For example, this dial plan shows that when users dial a 5-digit number that starts with the digits 4, they are dialing an extension or station.

Communication Manager – dialplan

```
display dialplan analysis                                    Page   1 of  12
                           DIAL PLAN ANALYSIS TABLE
                                 Location: all            Percent Full: 1

   Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
   String   Length Type     String   Length Type     String   Length Type
  1           5    ext
  4           5    ext
  5           5    udp
  *           4    dac
  #           3    fac
```

Administering the Uniform Dial Plan for routing

On the Avaya Aura® Communication Manager create a Uniform Dial Plan for routing.

Uniform Dial Plans (UDPs) are used to share a common dial plan among a group of Communication Manager servers. The UDP provides a common dial plan length – or a combination of extension lengths – that can be shared among a group of media servers or switches. Additionally, UDP can be used singly to provide uniform dialing between two or more private switching systems.

Procedure steps

Step **Action**

1 Use the Communication Manager – System Access Terminal (SAT) interface **change uniform-dialplan n** to update the Uniform Dial Plan for routing.

--End--

Procedure job aid

This Communication Manager – Uniform Dial Plan display shows the 5-digit 5xxxx route to Automatic Alternate Routing (AAR).

Communication Manager – Uniform Dial Plan

```
display uniform-dialplan 1                                    Page   1 of   2
                     UNIFORM DIAL PLAN TABLE
                                                          Percent Full: 0

  Matching                    Insert                Node
  Pattern       Len Del       Digits      Net Conv Num
5                5   0                    aar  n
                                               n
                                               n
                                               n
                                               n
                                               n
                                               n
                                               n
                                               n
                                               n
                                               n
                                               n
                                               n
                                               n
                                               n
                                               n
                                               n
```

Administering Automatic Alternate Routing

On the Avaya Aura® Communication Manager, use Automatic Alternate Routing (AAR) for routing calls with dialed digits 5xxxx to Avaya Aura® Contact Center.

Note: Other methods of routing may be used.

Use Automatic Alternate Routing (AAR) for routing calls with dialed digits 5xxxx to Contact Center. Use the change dialplan analysis command, and add an entry to specify use of AAR for routing of digits 5xxxx.

Automatic Alternative Route (AAR) allows enterprise network calls to originate and terminate at one or many locations without accessing the public network. It routes calls over the private enterprise network.

Procedure steps

Step	Action
1	Use the Communication Manager – System Access Terminal (SAT) interface **change aar analysis n** command to add an entry to specify use of AAR for routing of digits 5xxxx.

--End--

Procedure job aid

This Communication Manager – AAR Digit Analysis table shows the use of AAR for the routing of digits matching 5xxxx to Route Pattern 1.

Communication Manager – Automatic Alternate Routing

```
display aar analysis 1                                      Page   1 of   2
                     AAR DIGIT ANALYSIS TABLE
                               Location: all            Percent Full: 1

      Dialed           Total      Route    Call    Node   ANI
      String          Min  Max   Pattern  Type    Num    Reqd
  2                   7    7     999      aar             n
  3                   7    7     999      aar             n
  4                   7    7     999      aar             n
  5                   5    5     1        aar             n
  6                   7    7     999      aar             n
  7                   7    7     999      aar             n
  8                   7    7     999      aar             n
  9                   7    7     999      aar             n
                                                          n
                                                          n
                                                          n
                                                          n
                                                          n
                                                          n
                                                          n
```

Configuring IP Services for Application Enablement Services

Configure IP Services for the Avaya Aura® Application Enablement Services (AES) transport link.

Procedure steps

Step	Action
1	Use the Communication Manager – System Access Terminal (SAT) interface **change ip-services** command to configure IP services for the AES transport link.

2 On page 1, for **Type**, enter **AESVCS**.

3 Set **Enabled** to **y**.

4 For **Local Node**, enter **procr**.

5 For **Local Port**, select the default port number 8765.

6 On page 3, for **AE Services Server**, enter the name of the AES server.

7 For **Password**, enter the AES administration password.

Attention: The name and password entered for the AE Services Server and Password fields are case sensitive, and must match the name and password on the AES server.

8 Set **Enabled** to **y**.

--End--

Procedure job aid

This Communication Manager – IP services page (1) displays the AESVCS (Application Enablement Services) IP Service type.

Communication Manager – CTI Link

```
change ip-services                                          Page   1 of   3

                                    IP SERVICES
 Service      Enabled      Local        Local        Remote       Remote
   Type                     Node         Port         Node         Port
AESVCS         y        procr          8765
```

This Communication Manager – IP services page (3) displays the Application Enablement Services server name. The administered name for the AES server is created as part of the AES installation, you can obtain it from the AES server by typing `uname -n` at the Linux command prompt.

```
change ip-services                                          Page   3 of   3
                          AE Services Administration

 Server ID    AE Services        Password          Enabled     Status
                 Server
    1:        f81aes4docs                           y
    2:                                              y
    3:                                              y
    4:                                              y
    5:                                              y
    6:                                              y
    7:                                              y
    8:                                              _
    9:                                              _
   10:                                              _
   11:                                              _
   12:                                              _
   13:                                              _
   14:                                              _
   15:                                              _
   16:                                              _
```

Configuring a CTI Link for Application Enablement Services

Add a CTI link from the Communication Manager to the Avaya Aura® Application Enablement Services server.

The other end of this CTI link is configured on the Avaya Aura® Application Enablement Services server. For more information, see Adding a CTI link to the Communication Manager (page 101).

Procedure steps

Step	Action
1	Use the Communication Manager – System Access Terminal (SAT) interface **add cti-link** command to add a CTI link for the Avaya Aura® Application Enablement Services server.
2	Type **add cti-link n,** where n is an available CTI link number.
3	In the **Extension** field, enter an available extension number.
4	For **Type**, enter **ADJ-IP**.
5	For **Name**, enter a descriptive name for this CTI link to the Avaya Aura® Application Enablement Services server. For example, type Link to AES.

--End--

Procedure job aid

This Communication Manager – CTI link page displays an ADJ-IP link type. The ADJ-IP link type is for Adjunct Switch Application Interface (ASAI) links administered by Avaya CTI applications, such as Avaya Aura® Application Enablement Services.

Communication Manager – CTI Link of type ADJ-IP

```
display cti-link 1                                          Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 19999
     Type: ADJ-IP
                                                                   COR: 1
     Name: Link to AES
```

Creating the agent extensions

On the Avaya Aura® Communication Manager create the agent extensions.

Procedure steps

Step	Action
1	On the Avaya Aura® Communication Manager, use the System Access Terminal (SAT) interface to create an agent extension (workstation) using the **add station n** command. For example, enter **add station 42000**.
2	Use the SAT interface to create the another agent extension (workstation) using the **add station n** command. For example, enter **add station 42001**.
3	Repeat the SAT **add station n** command for each additional agent phone (extension) required.

--End--

Procedure job aid

To ensure proper integration and Avaya Aura® Contact Center call control, Communication Manager stations (phones) must be configured as follows:

- A maximum of 2 Call Appearance lines per agent station
- Restrict Last Appearance enabled
- Call Forwarding (including Coverage Path) disabled, as it is not supported
- Priority call feature disabled, as it is not supported
- IP Softphone enabled

When you are finished configuring the Avaya Aura® Communication Manager, use the **save translation** command to save your changes.

Shuffling (Direct IP - IP Audio Connections)

If you are using an Avaya Aura® Unified Communications platform PABX, Avaya recommends that you enable the shuffling feature to avoid unnecessary DSP usage. Avaya Aura® Shuffling (Direct IP-IP Audio Connections) attempts to renegotiate the media on an established SIP call, to update the anchor point of the media processor, thereby reducing the total number of Digital Signal Processor (DSP) channels required.

On your Avaya Aura® Communication Manager, configure “Direct IP-IP Audio Connections? y” on every agent station, and on the SIP Signaling group configuration screens.

Attention: Communication Manager consumes DSPs if shuffling is turned off on either the SIP Signaling groups, or any of the agent IP stations. So Avaya recommends that you enable shuffling on all agent stations (phones) and on the SIP signaling group.

Call Appearance lines on agent stations

Avaya Aura® Contact Center supports Communication Manager stations (phones) with a maximum of 2 Call Appearance lines per agent station. New Communication Manager stations are automatically created with three Call Appearance lines, so if a station is to be used by an Avaya Aura® Contact Center agent, you must configure the new station to have a maximum of two Call Appearance lines.

The following Communication Manager station displays show one of the extensions (agent phones) configured to support Avaya Aura® Contact Center. The extension number is 42000 and the phone is an Avaya IP Deskphone 9640.

Communication Manager – station 42000

```
display station 42000                                    Page   1 of   5
                                    STATION

Extension: 42000                      Lock Messages? n                BCC: 0
     Type: 9640                       Security Code:                   TN: 1
     Port: S00025                   Coverage Path 1:                  COR: 1
     Name: Agent one                Coverage Path 2:                  COS: 1
                                    Hunt-to Station:

STATION OPTIONS
                                         Time of Day Lock Table:
             Loss Group: 19        Personalized Ringing Pattern: 1
                                           Message Lamp Ext: 42000
          Speakerphone: 2-way           Mute Button Enabled? y
       Display Language: english             Button Modules: 0
 Survivable GK Node Name:
           Survivable COR: internal          Media Complex Ext:
   Survivable Trunk Dest? y                      IP SoftPhone? y

                                        IP Video Softphone? n
                                 Short/Prefixed Registration Allowed: default

                                        Customizable Labels? y
```

Communication Manager – station 42000 continued

```
display station 42000                                    Page   2 of   5
                                    STATION
FEATURE OPTIONS
          LWC Reception: spe              Auto Select Any Idle Appearance? n
          LWC Activation? y                       Coverage Msg Retrieval? y
  LWC Log External Calls? n                             Auto Answer: none
            CDR Privacy? n                          Data Restriction? n
   Redirect Notification? y                 Idle Appearance Preference? n
 Per Button Ring Control? n               Bridged Idle Line Preference? n
   Bridged Call Alerting? n                   Restrict Last Appearance? y
 Active Station Ringing: single
                                                     EMU Login Allowed? n
       H.320 Conversion? n          Per Station CPN - Send Calling Number?
      Service Link Mode: as-needed                    EC500 State: enabled
        Multimedia Mode: enhanced               Audible Message Waiting? n
    MWI Served User Type:                     Display Client Redirection? n
            AUDIX Name:                       Select Last Used Appearance? n
                                               Coverage After Forwarding? s
                                                 Multimedia Early Answer? n
 Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? y
  Emergency Location Ext: 42000        Always Use? n IP Audio Hairpinning? n
    Precedence Call Waiting? y
```

Communication Manager – station 42000 continued

```
display station 42000                                    Page   4 of   5
                                    STATION
 SITE DATA
       Room:                                          Headset? n
       Jack:                                          Speaker? n
      Cable:                                         Mounting: d
      Floor:                                     Cord Length: 0
   Building:                                       Set Color:

ABBREVIATED DIALING
     List1:                  List2:                    List3:



BUTTON ASSIGNMENTS
 1: call-appr                          5:
 2: call-appr                          6:
 3:                                    7:
 4:                                    8:

    voice-mail
```

Adding Agent workstations to the numbering tables

Avaya Aura® Contact Center agents use Communication Manager workstations to handle customer calls. Add the Avaya Aura® Contact Center controlled workstations to the numbering tables to create caller identifications and calling numbers for locally originated Contact Center agent calls.

Adding agent workstations to the numbering tables ensures that the incoming SIP requests contain "From" headers that contain the agent's Uniform Resource Identifier (URI).

Attention: If a table entry applies to a SIP connection to Avaya Aura® Session Manager, the resulting number must be a complete E.164 number.

Procedure steps

Step	Action
1	Using the Communication Manager – System Access Terminal, enter **change public-unknown-numbering x**, where x is the public number table to change.
2	In the **Ext Len** field, type your extension length.
3	In the **Ext Code** field, type the starting digit(s) of the extension, such as the country code.

4 Leave the **Trk Grp(s)** field blank to apply to all trunks in the system.

5 In the **CPN Len** field, type the number of digits in your calling number.

6 Press Enter to save your changes.

7 Enter **change private-numbering y**, where y is the private number table to change.

8 In the **Ext Len** field, type your extension length.

9 In the **Ext Code** field, type the starting digit(s) of the extension, such as the country code.

10 Leave the **Trk Grp(s)** field blank to apply to all trunks in the system.

11 In the **CPN Len** field, type the number of digits in your calling number.

12 Press Enter to save your changes.

--End--

Procedure job aid

This Communication Manager numbering table shows the agents workstations added to a numbering table.

Communication Manager – Automatic Alternate Routing

```
display public-unknown-numbering 1                          Page   1 of   2
                     NUMBERING - PUBLIC/UNKNOWN FORMAT
                                          Total
Ext  Ext             Trk        CPN       CPN
Len  Code            Grp(s)     Prefix    Len
                                                Total Administered: 2
 5   2                                     5        Maximum Entries: 9999
 5   4                                     5
                                                Note: If an entry applies to
                                                a SIP connection to Avaya
                                                Aura(R) Session Manager,
                                                the resulting number must
                                                be a complete E.164 number.
```

Enabling Gratuitous Address Resolution Protocol on agent extensions

If your Avaya Media Servers are installed on the Linux operating system, and if they are installed on the same network subnet as the H.323 phones, then you must configure your Avaya Aura® Communication Manager - Utility Server to allow the phones and Avaya Media Server to support the High Availability feature. You must enable Gratuitous Address Resolution Protocol (GRATARP) for your agent extensions (stations/phones).

The Utility Server - Utility Admin IP Phone Settings Editor provides a web based tool for configuring the IP phone settings file. This significantly simplifies the process of making changes to the IP phone settings file and provides enhanced validation to help avoid mis-configurations. The Utility Admin IP Phone Settings Editor also provides IP Phone firmware management, enabling you to upload new phone firmware to the file server.

Procedure steps

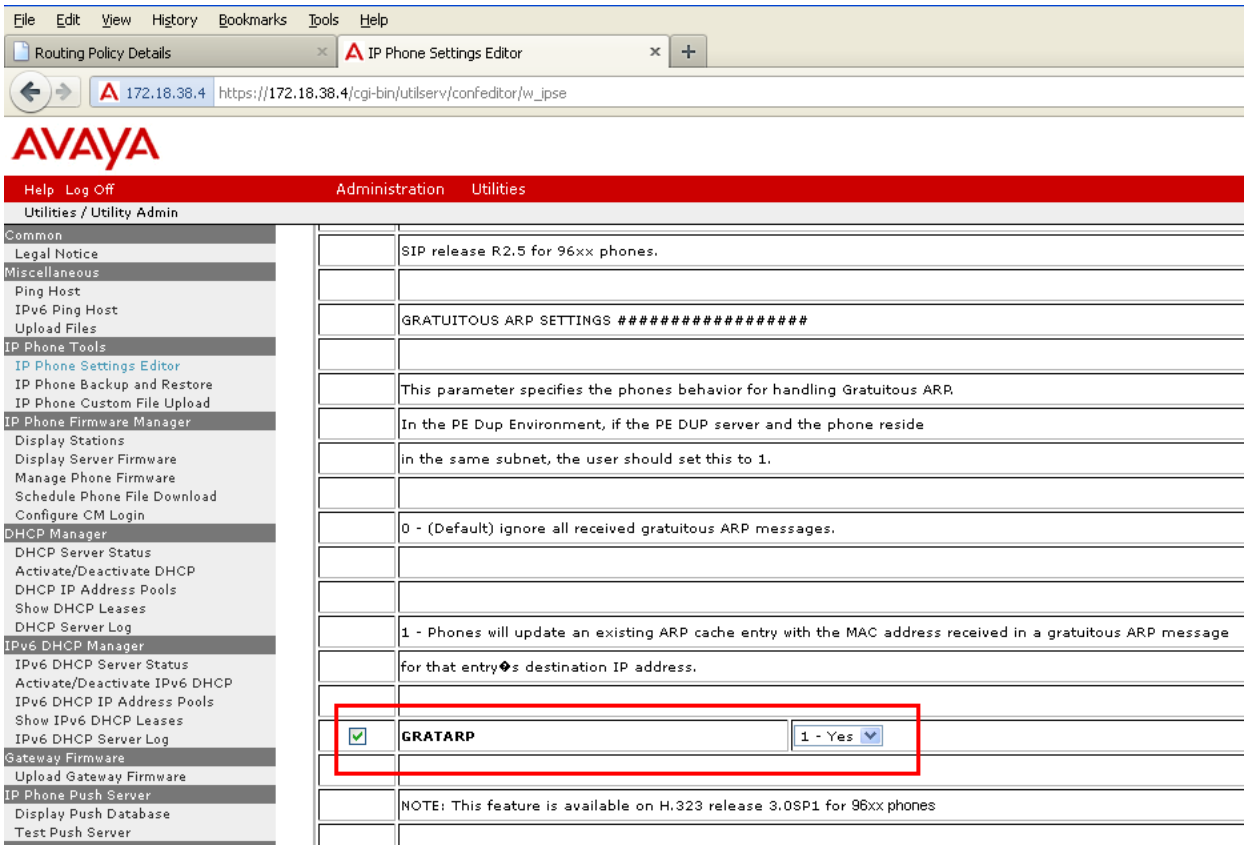
Step	Action
1	Start Internet Explorer.
2	In the Internet Explorer address box, type http://<Utility Server IP address>. For example, type http://172.18.38.4
3	On the Utility Server Web console, click **Utilities**.
4	Click **Utility Admin**.
5	Enter your Utility Server user name.
6	Click **Logon**.
7	Enter your Utility Server password.
8	Click **Logon**. *The system displays the Utility Server Utility Admin menu.*
9	On the Utility Server Web console, click **Utilities**.
10	Click **Utility Admin**.
11	From the left navigation menu, select **IP Phone Settings Editor**.
12	Click **Proceed with selected values**.
13	For your Contact Center phone types, set **GRATARP** to **Yes**. This configures the phones to process Gratuitous Address Resolution Protocol (ARP) requests and provides duplicate IP address detection. This enables the phones to work with Linux-based Avaya Media Server in a High Availability resilient solution.

--End--

Procedure job aid

Enabling Gratuitous Address Resolution Protocol (ARP) on agent extensions with 9640 phones.

Avaya Aura® Communication Manager - Utility Server, with GRATARP enabled



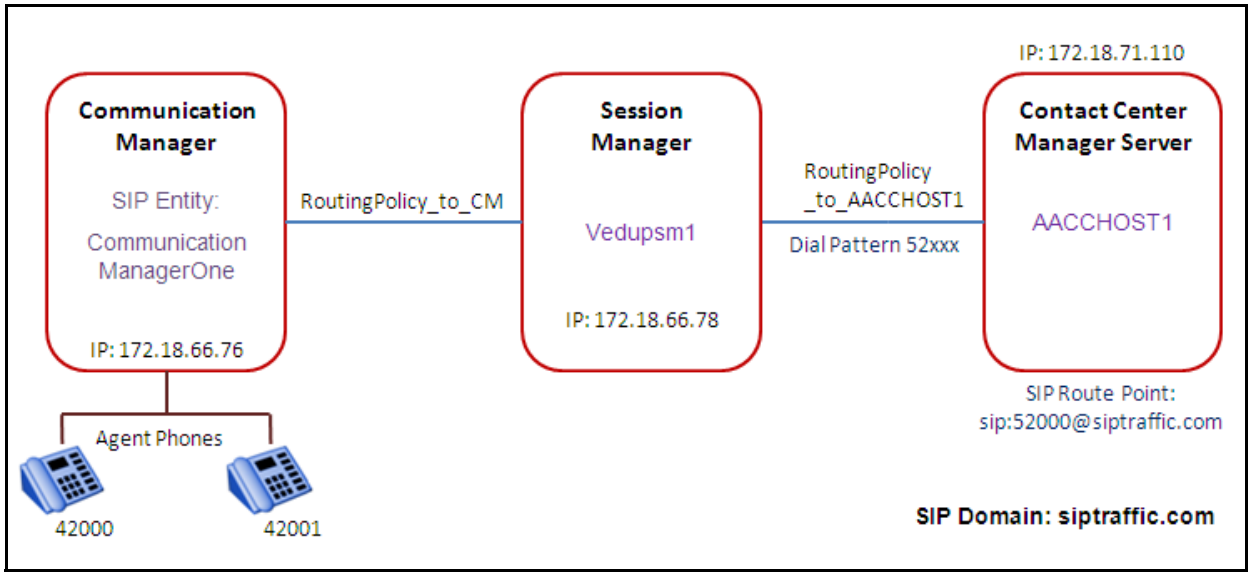
Unified Communications – Session Manager configuration

This section describes how to configure Avaya Aura® Session Manager Release 6.2 for use with Avaya Aura® Contact Center Release 6.3.

Avaya Aura® Session Manager is a SIP routing and integration tool. It integrates all the SIP entities across the entire enterprise network within a company. Session Manager provides a core communication service that builds on existing equipment but adds a SIP-based architecture. Session Manager connects to and acts as a system-wide dial plan for call processing applications such as Avaya Aura® Communication Manager using direct SIP connections.

The following diagram shows a typical Session Manager deployment and configuration. The procedures and SIP Entity names in this section are based on this typical routing configuration.

Example of a typical Session Manager routing solution



Logging on to the System Manager Web interface

Log on to the System Manager Web interface to configure the Session Manager.

You use Avaya Aura® System Manager to configure Avaya Aura® Session Manager. Avaya Aura® System Manager delivers a set of shared, secure management services, and a common console across multiple products. System Manager includes the following central management services:

- User Management: administer users and user groups.
- Communication System Management: administer individual and group stations, and mailboxes.
- Routing: administer routing policies for all Session Manager instances within an enterprise.
- Alarm Management Service: Supports alarm monitoring, acknowledgement, configuration, clearing, and retiring.
- Logging Service: Receive log events formatted in the common log format.

A central database that resides on the System Manager server stores all the System Manager central data, the Session Manager administration data, and the Central Data Distribution Service information. The Central Data Distribution Service detects changes to the System Manager central database and distributes these changes to the Session Manager instances. All communication between System Manager and Session Manager instances is performed over secure links.

Procedure steps

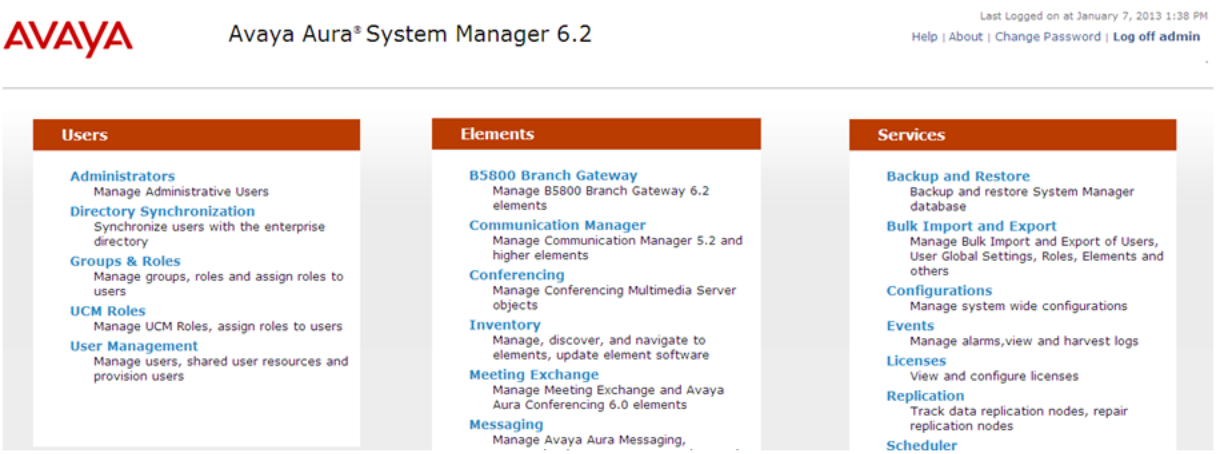
Step	Action
1	On the browser, type <Avaya Aura® System Manager IP address>/SMGR. For example, type; https://172.18.66.74/SMGR
2	In the **User ID** box, type the Avaya Aura® System Manager user name.
3	In the **Password** box, type the Avaya Aura® System Manager password.
4	Click **Log On**.

--End--

Procedure job aid

The System Manager home page displays the main navigation menu. The tasks you can perform using System Manager depends on your user role.

Example of the System Manager Web page



Creating a routing domain

Routing domains determine whether the Session Manager dial plan routes a particular call. Typically, in a contact center, the routing domain name matches the Windows Active Directory domain name.

Procedure steps

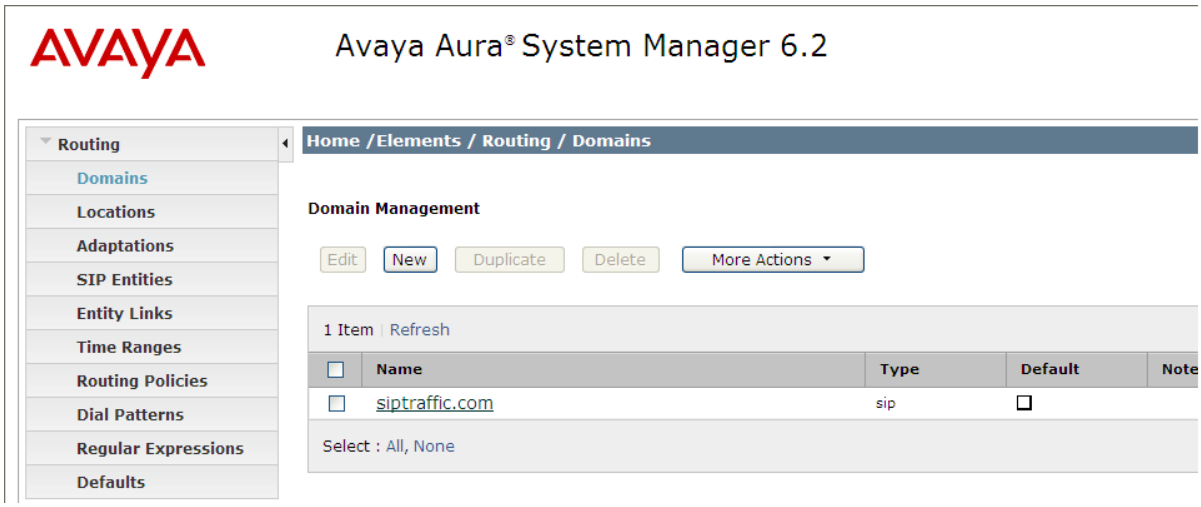
Step	Action
1	On the System Manager console, select **Routing**, **Domains**.
2	Click **New**.
3	On the **Domain Management** page, in the **Name** box, type the new contact center solution domain name. For example, type siptraffic.com.
4	From the **Type** list, select **sip**.
5	In the **Notes** box, type your notes about this domain, for example siptraffic.com.
6	Click **Commit**.

--End--

Procedure job aid

Example of a Session Manager domain, siptraffic.com.

Example of configuring a routing domain



Creating a routing location

Configure the location of your Session Manager. Session Manager uses the origination location to determine which dial pattern to use when routing calls. Locations are also used to limit the number of calls coming out of or going to a physical location.

Procedure steps

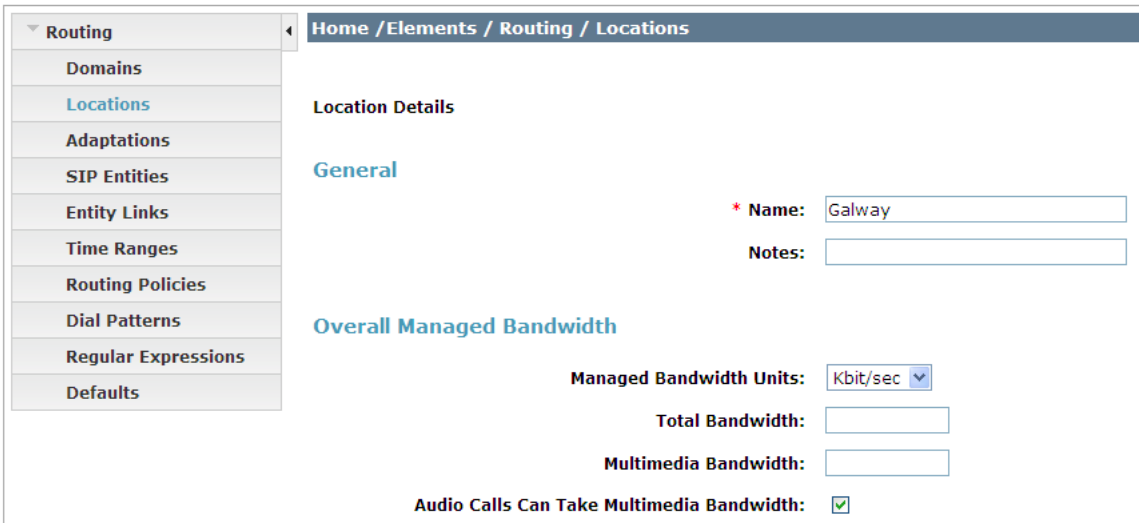
Step	Action
1	On the System Manager console, select **Routing**, **Locations**.
2	Click **New**.
3	In the **Name** box, type the location name. Avaya recommends that you type a descriptive name for your location, for example Galway.
4	In the **Notes** box, type your notes about this location.
5	From the **Managed Bandwidth Units** list, select **kbit/sec**.
6	In the **Total Bandwidth** box, type your required bandwidth.
7	To add a location pattern, click **Add** under **Location Pattern**.
8	In the **IP Address Pattern** box, type the pattern string to match your system. For example: 172.18.*
9	In the **Location Pattern** section, in the **Notes** box, type your notes about this pattern, for example "Location is the campus network".
10	Click **Commit**.

--End--

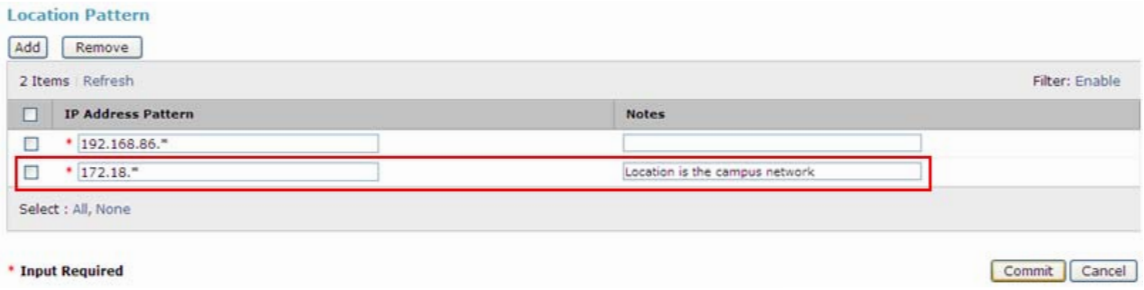
Procedure job aid

Example of a Session Manager routing location. If your Avaya Aura® Communication Manager has an IP address of 172.18.66.76 and if your Session Manager has an IP address of 172.18.66.78, then your IP Address Patterns may be 172.18.*. This pattern must cover the addresses that you deem part of this routing location.

Example of creating a routing location



Example of creating a routing location continued



Creating a SIP Entity for the Communication Manager

Create a SIP Entity for the Communication Manager. To administer minimal routing using Session Manager, you must configure a SIP Entity of type Communication Manager and the Session Manager.

Procedure steps

Step	Action
1	On the System Manager console, select **Routing**, **SIP Entities**.
2	Click **New**.
3	In the **Name** box, type the name of the Communication Manager SIP Entity, for example CommunicationManagerOne.
4	In the **FQDN or IP address** box, type the IP address of the Communication Manager, for example 172.18.66.76.
5	From the **Type** list, select **CM**.
6	If you need to specify an Adaptation Module for the Communication Manager SIP entity, from the **Adaptation** list, select an adaptation value.
7	From the **Location** list, select the location for this Communication Manager. For example, select Galway.
8	In the **Credential name** box, enter a regular expression string. The **Credential name** is used for TLS connection validation by searching for this string in the SIP entity identity certificate.
9	From the **SIP Link Monitoring** list, select for example **Use Session Manager Configuration**.
10	If you need to specify the **Port** parameters, under **Port** click **Add**. When Session Manager receives a request where the host-part of the request-URI is the IP address of the Session Manager, it associates one of the administered domains with the port on which the request was received.
11	Enter the necessary **Port** and **Protocol** parameters.
12	Click **Commit**.

--End--

Variable definitions

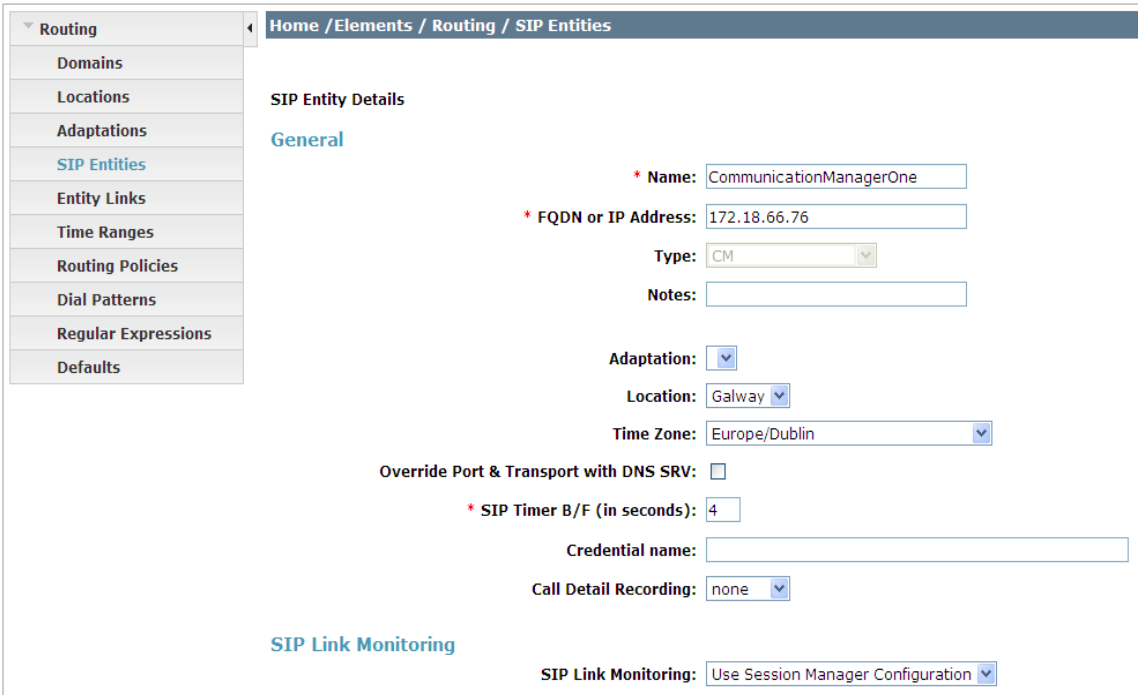
Variable	Value
Name	SIP entity name. This name must be unique and can have between 3 and 64 characters.
FQDN or IP Address	Fully qualified domain name or IP address of the Communication Manager.
Type	SIP entity type, such as a Communication Manager.
Notes	Additional notes about the SIP entity.
Adaptation	Adaptation to be used for the SIP entity. Select from already defined adaptations.
Location	Communication Manager SIP entity location. Select from previously defined locations.
Time Zone	Time zone for the SIP entity.
Override Port & Transport with DNS SRV	Specify if you wish to use DNS routing. SIP uses DNS procedures to allow a client to resolve a SIP URI into the IP address, port, and transport protocol of the next hop to contact. It also uses DNS routing to allow a server to send a response to a backup client if the primary client fails.
SIP Timer B/F (in seconds)	Amount of time the Session Manager waits for a response from the SIP entity.
Credential name	Enter a regular expression string in the Credential name. Credential name is used for TLS connection validation by searching this string in the SIP entity identity certificate.
Call Detail Recording	Select or clear the check box to turn SIP monitoring on or off.
Proactive cycle time (Seconds)	Enter a value between 120 and 9000 seconds. The default is 900. This specifies how often the entity is monitored when the link to the entity is up or active.
Reactive cycle time (Seconds)	Enter a value between 30 and 900 seconds. The default is 120. This specifies how often the entity is monitored when a link to the entity is down or inactive.
Number of retries	Enter a value between 0 and 15. The default is 1. This specifies the number of times Session Manager tries to ping or reach the SIP entity before marking it as down or unavailable.
Port	Add a listening port for the SIP entity.
Protocol	Protocol that the SIP entity uses.

Variable	Value
SIP Domain	The domain of the SIP entity.
Notes	Additional notes about the port and port parameters.

Procedure job aid

The SIP Entity for the Communication Manager.

Example of configuring the Communication Manager SIP Entity



Creating a SIP Entity for the Session Manager

Create a SIP Entity for the Avaya Aura® Session Manager. To administer minimal routing using Session Manager, you must configure two SIP Entities, a SIP Entity of type Communication Manager and a SIP Entity of type Session Manager.

Procedure steps

Step	Action
1	On the System Manager console, select **Routing**, **SIP Entities**.

2 Click **New**.

3 In the **Name** box, type the name of the Session Manager SIP Entity, for example Vedupsm1.

4 In the **FQDN or IP address** box, type the IP address of the Session Manager, for example 172.18.66.78.

5 From the **Type** list, select **Session Manager**.

6 From the **Location** list, select the location for this Session Manager. For example, select siptraffic.

7 If the SIP entity type is **Session Manager** and you need to specify an Outbound Proxy for the SIP entity, click the drop-down selector for the **Outbound Proxy** box.

8 In the **Credential name** box, enter a regular expression string. The **Credential name** is used for TLS connection validation by searching for this string in the SIP entity identity certificate.

9 From the **SIP Link Monitoring** list, select, for example; **Use Session Manager Configuration**.

10 If you need to specify the **Port** parameters, under **Port** click **Add**. When Session Manager receives a request where the host-part of the request-URI is the IP address of the Session Manager, it associates one of the administered domains with the port on which the request was received.

11 Enter the necessary **Port** and **Protocol** parameters.

12 Click **Commit**.

--End--

Variable definitions

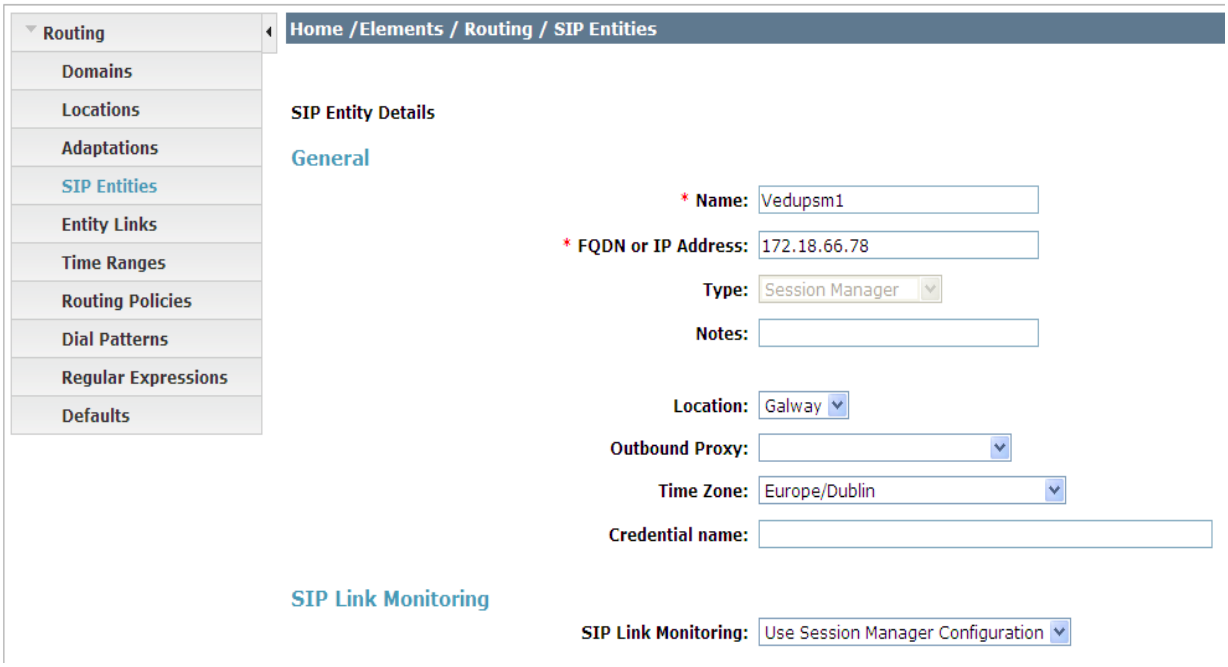
Variable	Value
Name	SIP entity name. This name must be unique and can have between 3 and 64 characters.
FQDN or IP Address	Fully qualified domain name or IP address of the Session Manager SIP Entity.
Type	SIP entity type, such as a Session Manager.
Notes	Additional notes about the SIP entity.
Location	SIP entity location. Select from previously defined locations.
Outbound Proxy	Outbound proxy if the entity type is Session Manager, and you wish to specify a proxy.
Time Zone	Time zone for the SIP entity.
Override Port & Transport with DNS SRV	Specify if you wish to use DNS routing. SIP uses DNS procedures to allow a client to resolve a SIP URI into the IP address, port, and transport protocol of the next hop to contact. It also uses DNS routing to allow a server to send a response to a backup client if the primary client fails.
SIP Timer B/F (in seconds)	Amount of time the Session Manager waits for a response from the SIP entity.
Credential name	Enter a regular expression string in the Credential name. Credential name is used for TLS connection validation by searching this string in the SIP entity identity certificate.
Call Detail Recording	Select or clear the check box to turn SIP monitoring on or off.
Proactive cycle time (Seconds)	Enter a value between 120 and 9000 seconds. The default is 900. This specifies how often the entity is monitored when the link to the entity is up or active.
Reactive cycle time (Seconds)	Enter a value between 30 and 900 seconds. The default is 120. This specifies how often the entity is monitored when a link to the entity is down or inactive.
Number of retries	Enter a value between 0 and 15. The default is 1. This specifies the number of times Session Manager tries to ping or reach the SIP entity before marking it as down or unavailable.
Port	Add a listening port for the SIP entity.
Protocol	Protocol that the SIP entity uses.

Variable	Value
SIP Domain	The domain of the SIP entity.

Procedure job aid

The SIP Entity for the Avaya Aura® Session Manager, 172.18.66.78.

Example of configuring the Session Manager SIP Entity



Creating a SIP Entity Link from the Session Manager to the Communication Manager

Create a SIP entity link from the Avaya Aura® Session Manager to the Communication Manager. You must configure an entity link to allow Session Manager to be able to send messages to, or receive messages from, that entity directly. To be able to communicate with other SIP entities, each Session Manager instance must know the port and the transport protocol of its entity link to the SIP entities in the network.

Procedure steps

Step	Action
1	On the System Manager console, select **Routing**, **Entity Links**.

2 Click **New**.

3 In the **Name** box, type the name for this SIP Entity Link, for example SM1_CM_Entity_Link.

4 Under **SIP Entity 1**, select the Session Manager SIP entity, and provide the port type and number; for example Vedupsm1, TLS, 5061.

5 Under **SIP Entity 2**, select the Communication Manager SIP entity, and provide the port type and number; for example CommunicationManagerOne, 5061.

6 For the **Connection Policy**, select **Trusted**. Session Manager does not accept SIP connection requests or SIP packets from untrusted SIP entities.

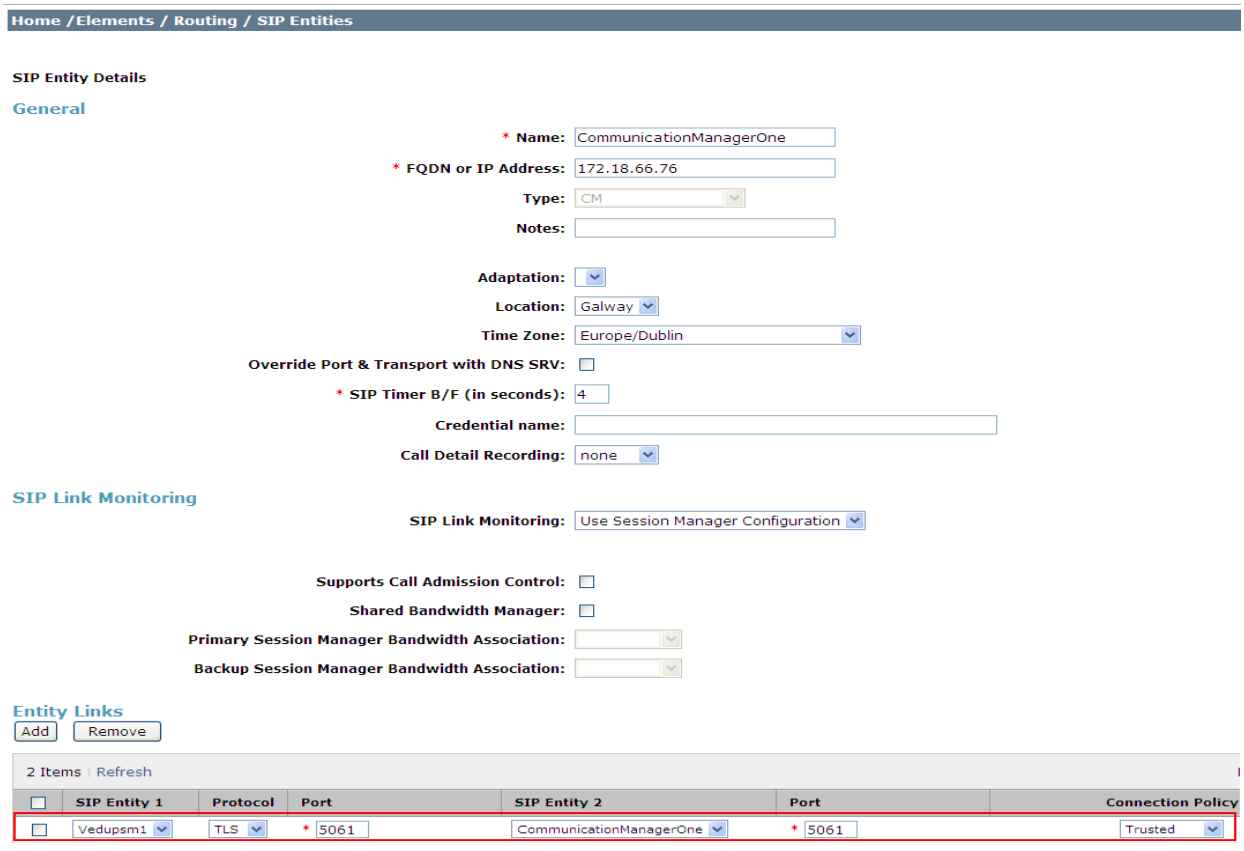
7 Click **Commit**.

--End--

Procedure job aid

The Avaya Aura® Communication Manager SIP Entity details showing one link to the Session Manager SIP Entity (SM1_CM_Entity_Link).

Example of configuring Communication Manager SIP entity links



Creating a routing policy from the Session Manager to Communication Manager

Create a routing policy from the Avaya Aura® Session Manager to Avaya Aura® Communication Manager.

Session Manager uses the data configured in the Routing Policy to find the best match against the number (or address) of the called party.

Procedure steps

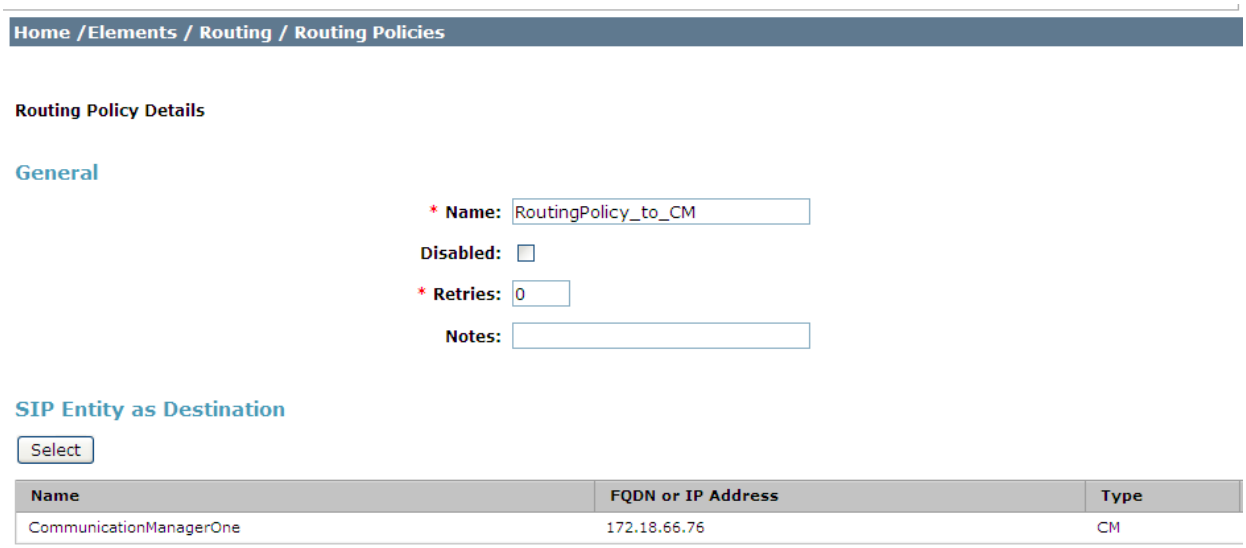
Step	Action
1	On the System Manager console, select **Routing**, **Routing Policies**.
2	Click **New**. *The Routing Policy Details screen is displayed.*
3	In the **General** section, in the **Name** box, type the name for the Routing Policy. Avaya recommends that you type a descriptive name for your Routing Policy, for example RoutingPolicy_to_CM.
4	In the **Notes** box, type your notes about this Routing Policy.
5	In the **SIP Entities as Destination** section, click **Select**.
6	From the list of SIP Entities, select the SIP Entity for your Avaya Aura® Communication Manager, for example CommunicationManagerOne.
7	Click **Select**.
8	If you need to associate the Time of Day routing parameters with this Routing Policy, click **Add** from the **Time of Day** section.
9	Select the Time of Day patterns that you want to associate with this routing pattern and click **Select**.
10	Click **Commit**.

--End--

Procedure job aid

The routing policy from the Session Manager (SM) to Avaya Aura® Communication Manager (CM).

Example of configuring routing policy from SM to CM



Creating a dial pattern to route calls to Communication Manager

Create a dial pattern using the Session Manager to Avaya Aura® Communication Manager routing policy. Session Manager uses this dial pattern to route calls to Avaya Aura® Communication Manager.

A dial pattern specifies which routing policy or routing policies are used to route a call based on the digits dialed by a user which match that pattern. The originating location of the call and the domain in the request-URI also determine how the call gets routed.

Procedure steps

Step	Action
1	On the System Manager console, select **Routing**, **Dial Patterns**.
2	Click **New**. *The Dial Pattern Details screen is displayed.*
3	In the **Pattern** box, type the dial pattern for voice calls to Avaya Aura® Communication Manager, for example 4xxxx.
4	In the **Min** box, type the minimum number of digits from the dial pattern to match, for example 5.
5	In the **Max** box, type the maximum number of digits from the dial pattern to match, for example 5.

6 From **SIP Domain**, select the SIP domain for this dial pattern, for example siptraffic.com, or select all domains.

7 Under the **Originating Locations and Routing Policies** section, click **Add**.

8 Select the check box for the location. For example, select Galway.

9 From **Routing Policies** list, select the Session Manager to Avaya Aura® Communication Manager Routing Policy, for example RoutingPolicy_to_CM.

10 Click **Select** to indicate that you have completed your selections.

11 Click **Commit**.

--End--

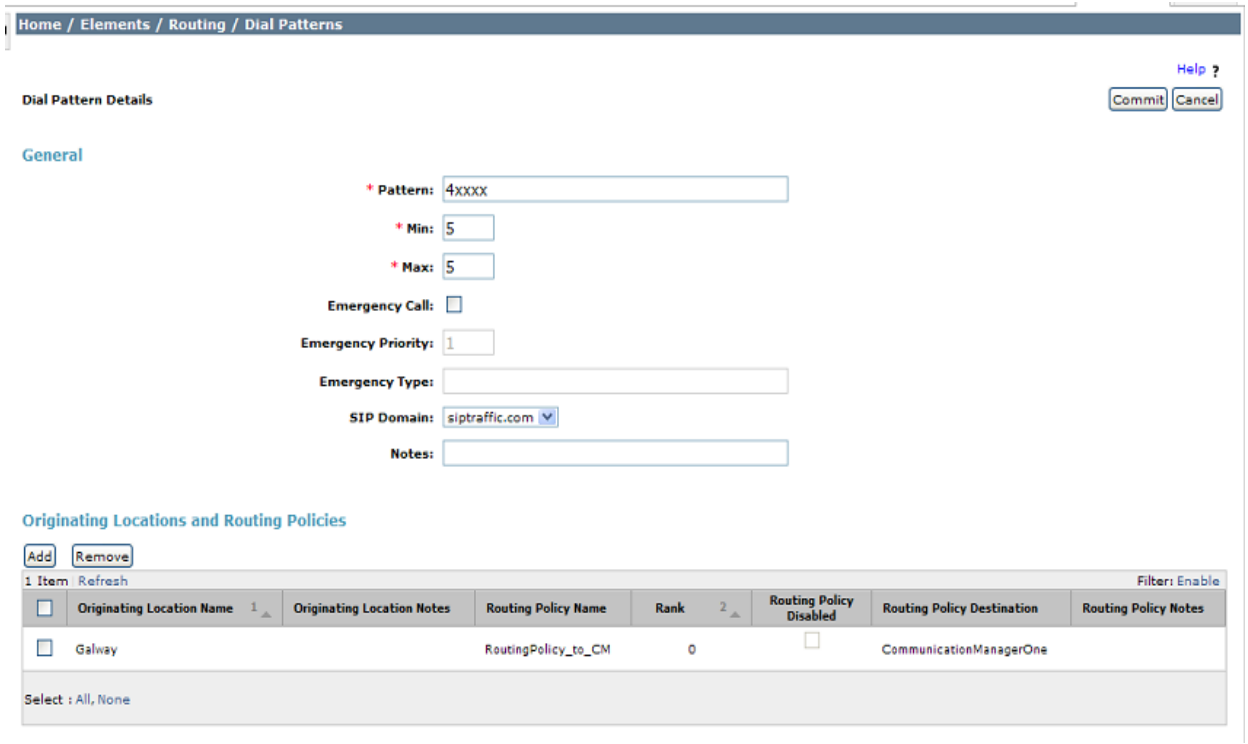
Variable definitions

Variable	Value
Pattern	Dial pattern to match. The pattern can have between 1 and 36 characters.
Min	Minimum number of digits to be matched.
Max	Maximum number of digits to be matched.
Emergency Call	Indicate if it is an emergency call. Note: Some of the important constraints on the use of this feature are as follows — Each location must be assigned to only one emergency dial number. — This emergency dial number must match the emergency dial number in the 96xx Deskphone settings file for all SIP phones in the identified location.
SIP Domain	Domain for which you want to restrict the dial pattern.
Notes	Other details that you wish to add.
Select check box	Use this check box to select and use the digit conversion for the incoming calls.
Location Name	Name of the location to be associated to the dial pattern.
Location Notes	Notes about the selected location.
Routing Policy Name	Name of the routing policy to be associated to the dial pattern.
Routing Policy Disabled	Name of the disabled routing policy.
Routing Policy Destination	Destination of the routing policy.
Routing Policy Notes	Any other notes about the routing policy that you wish to add.

Procedure job aid

Example of creating a dial pattern using the Session Manager to Avaya Aura® Communication Manager routing policy.

Example of configuring a dial pattern to route calls to the Communication Manager



Creating a SIP Entity for the Voice and Multimedia Contact Server

Create a SIP Entity for the Contact Center Manager Server. Contact Center Manager Server is installed on the Avaya Aura® Contact Center Voice and Multimedia Contact Server with Avaya Media Server, for example AACCHOST1, 172.18.71.110.

Procedure steps

Step	Action
1	On the System Manager console, select **Routing**, **SIP Entities**.
2	Click **New**.
3	In the **Name** box, type the name of the Contact Center Manager Server SIP Entity, for example AACCHOST1.
4	In the **FQDN or IP address** box, type the IP address of the Contact Center Manager Server, for example 172.18.71.110.

5 From the **Type** list, select **Other**.

6 If you need to specify an Adaptation Module for the Contact Center SIP entity, from the **Adaptation** list, select an adaptation value.

7 From the **Location** list, select the location for this Session Manager. For example, select Galway.

8 In the **Credential name** box, enter a regular expression string. The **Credential name** is used for TLS connection validation by searching for this string in the SIP entity identity certificate.

9 From the **SIP Link Monitoring** list, select **Use Session Manager Configuration**.

10 If you need to specify the **Port** parameters, under **Port** click **Add**. When Session Manager receives a request where the host-part of the request-URI is the IP address of the Session Manager, it associates one of the administered domains with the port on which the request was received.

11 Enter the necessary **Port** and **Protocol** parameters.

12 Click **Commit**.

--End--

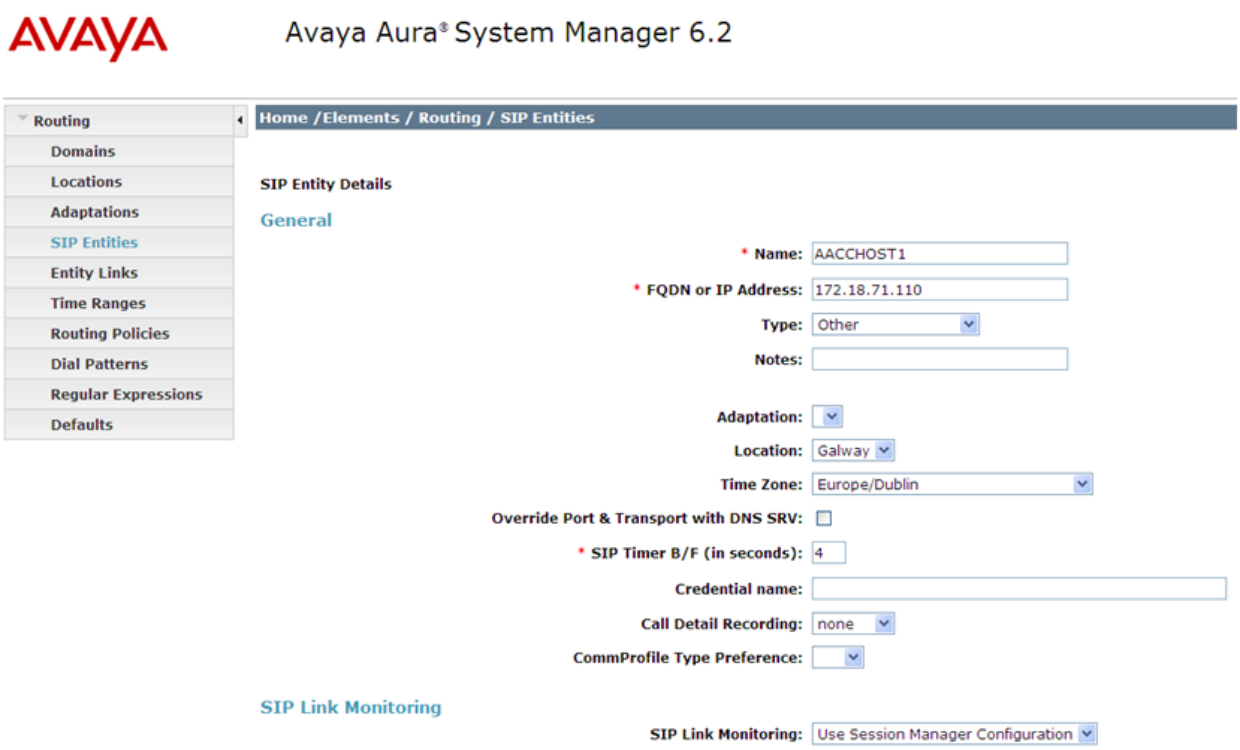
Variable definitions

Variable	Value
Name	SIP entity name. This name must be unique and can have between 3 and 64 characters.
FQDN or IP Address	Fully qualified domain name or IP address of the Avaya Aura® Contact Center SIP entity.
Type	SIP entity type, such as Other.
Notes	Additional notes about the SIP entity.
Adaptation	Adaptation to be used for the SIP entity. Select from already defined adaptations.
Location	SIP entity location. Select from previously defined locations.
Outbound Proxy	Outbound proxy if the entity type is Session Manager, and you wish to specify a proxy.
Time Zone	Time zone for the SIP entity.
Override Port & Transport with DNS SRV	Specify if you wish to use DNS routing. SIP uses DNS procedures to allow a client to resolve a SIP URI into the IP address, port, and transport protocol of the next hop to contact. It also uses DNS routing to allow a server to send a response to a backup client if the primary client fails.
SIP Timer B/F (Seconds)	Amount of time the Session Manager waits for a response from the SIP entity.
Credential name	Enter a regular expression string in the Credential name. Credential name is used for TLS connection validation by searching this string in the SIP entity identity certificate.
Call Detail Recording	Select or clear the check box to turn SIP monitoring on or off.
Proactive cycle time (Seconds)	Enter a value between 120 and 9000 seconds. The default is 900. This specifies how often the entity is monitored when the link to the entity is up or active.
Reactive cycle time (Seconds)	Enter a value between 30 and 900 seconds. The default is 120. This specifies how often the entity is monitored when a link to the entity is down or inactive.
Number of retries	Enter a value between 0 and 15. The default is 1. This specifies the number of times Session Manager tries to ping or reach the SIP entity before marking it as down or unavailable.
Port	Add a listening port for the SIP entity.

Variable	Value
Protocol	Protocol that the SIP entity uses.
SIP Domain	The domain of the SIP entity.
Notes	Additional notes about the port and port parameters.

Procedure job aid

The SIP Entity for the Contact Center Manager Server.



Creating a SIP Entity Link from the Session Manager to the Avaya Aura® Contact Center

Create a SIP entity link from the Avaya Aura® Session Manager to the Avaya Aura® Contact Center. Session Manager enables you to create an entity link between the Session Manager and any other administered SIP entity. You must configure an entity link between a Session Manager and any entity that you have administered if you want Session Manager to be able to send or receive

messages from that entity directly. To be able to communicate with other SIP entities, each Session Manager instance must know the port and the transport protocol of its entity link to these SIP entities in the network.

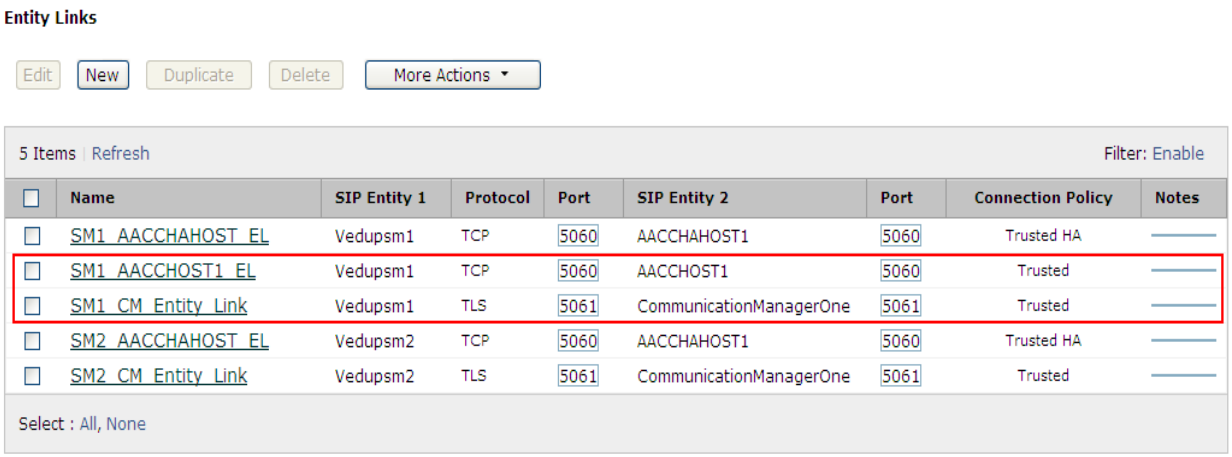
Procedure steps

Step	Action
1	On the System Manager console, select **Routing**, **Entity Links**.
2	Click **New**.
3	In the **Name** box, type the name for this SIP Entity Link, for example SM1_AACCHOST1_EL.
4	Under **SIP Entity 1**, select the Session Manager SIP entity, and provide the port type and number; for example Vedupsm1, TCP, 5060.
5	Under **SIP Entity 2**, select the Contact Center Manager Server SIP entity, and provide the port type and number; for example AACCHOST1, TCP, 5060.
6	For the **Connection Policy**, select **Trusted**. Session Manager does not accept SIP connection requests or SIP packets from untrusted SIP entities.
7	Click **Commit**.

--End--

Procedure job aid

Avaya Aura® Session Manager SIP entity showing SIP Entity links to Avaya Aura® Contact Center (AACCHOST1) and Avaya Aura® Communication Manager (CommunicationManagerOne).



Creating a routing policy from the Session Manager to Contact Center

Create a routing policy from Avaya Aura® Session Manager to Avaya Aura® Contact Center. Routing policies can include the "Origination of the caller", the "dialed digits" of the called party, the "domain" of the called party, and the actual time the call occurs. Optionally, instead of "dialed digits" of the called party and the "domain" of the called party a "regular expression" can be defined.

Session Manager uses the data configured in the Routing Policy to find the best match against the number (or address) of the called party.

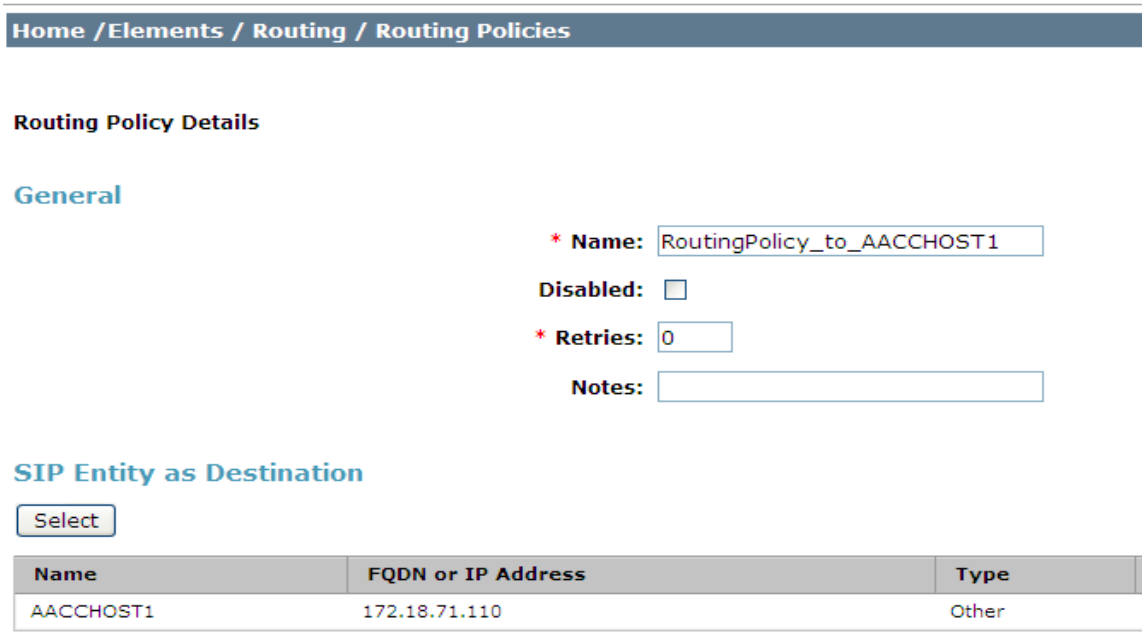
Procedure steps

Step	Action
1	On the System Manager console, select **Routing**, **Routing Policies**.
2	Click **New**. *The Routing Policy Details screen is displayed.*
3	In the **General** section, in the **Name** box, type a name for the routing policy, for example RoutingPolicy_to_AACCHOST1.
4	In the **Notes** box, type your notes about this Routing Policy.
5	In the **SIP Entities as Destination** section, click **Select**.
6	From the list of **SIP Entities**, choose the SIP Entity for your Avaya Aura® Contact Center, for example AACCHOST1.
7	Click **Select**.
8	If you need to associate the Time of Day routing parameters with this Routing Policy, click **Add** from the **Time of Day** section.
9	Select the Time of Day patterns that you want to associate with this routing pattern and click **Select**.
10	Click **Commit**.

--End--

Procedure job aid

The routing policy from Session Manager to Avaya Aura® Contact Center.



Creating a dial pattern to route calls to the Contact Center

Create a dial pattern using the Session Manager to Avaya Aura® Contact Center Routing Policy. Session Manager uses this dial pattern to route calls to the Contact Center for processing.

A dial pattern specifies which routing policy or routing policies are used to route a call based on the digits dialed by a user which match that pattern. The originating location of the call and the domain in the request-URI also determine how the call gets routed.

Procedure steps

Step	Action
1	On the System Manager console, select **Routing**, **Dial Patterns**.
2	Click **New**. *The Dial Pattern Details screen is displayed.*
3	In the **Pattern** box, type the dial pattern for voice calls to the contact center, for example 52xxx.
4	In the **Min** box, type the minimum number of digits from the dial pattern to match, for example 5.

5 In the **Max** box, type the maximum number of digits from the dial pattern to match, for example 5.

6 From **SIP Domain**, select the SIP domain for this dial pattern, for example siptraffic.com.

7 Under the **Originating Locations and Routing Policies** section, click **Add**.

8 Select the check box for the location. Select Galway.

9 From **Routing Policies** list, select the Session Manager to Avaya Aura® Contact Center Routing Policy, for example RoutingPolicy_to_AACCHOST1.

10 Click **Select** to indicate that you have completed your selections.

11 Click **Commit**.

--End--

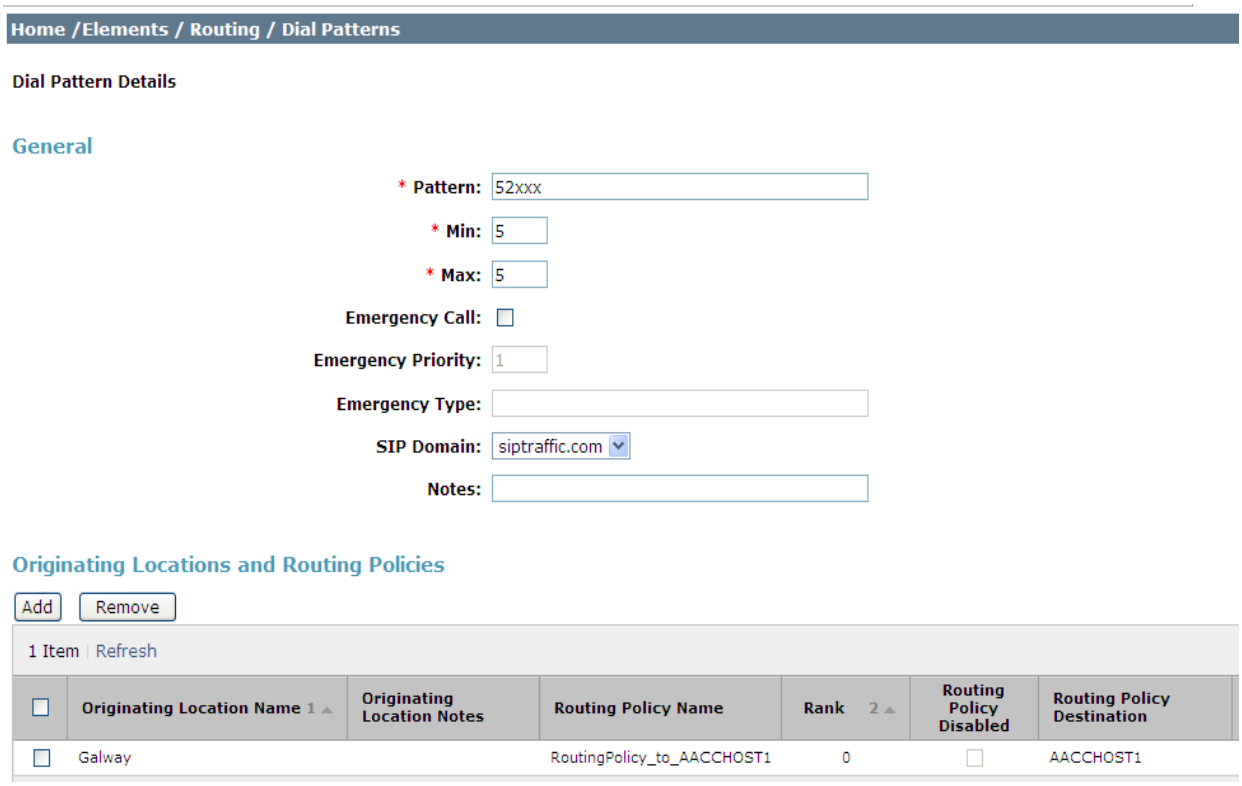
Variable definitions

Variable	Value
Pattern	Dial pattern to match. The pattern can have between 1 and 36 characters.
Min	Minimum number of digits to be matched.
Max	Maximum number of digits to be matched.
Emergency Call	Indicate if it is an emergency call. Note: Some of the important constraints on the use of this feature are as follows — Each location must be assigned to only one emergency dial number. — This emergency dial number must match the emergency dial number in the 96xx Deskphone settings file for all SIP phones in the identified location.
SIP Domain	Domain for which you want to restrict the dial pattern.
Notes	Other details that you wish to add.
Select check box	Use this check box to select and use the digit conversion for the incoming calls.
Location Name	Name of the location to be associated to the dial pattern.
Location Notes	Notes about the selected location.
Routing Policy Name	Name of the routing policy to be associated to the dial pattern.
Routing Policy Disabled	Name of the disabled routing policy.
Routing Policy Destination	Destination of the routing policy.
Routing Policy Notes	Any other notes about the routing policy that you wish to add.

Procedure job aid

Example of creating a dial pattern using the Session Manager to Avaya Aura® Contact Center routing policy.

Example of configuring a dial pattern to route calls to the Contact Center



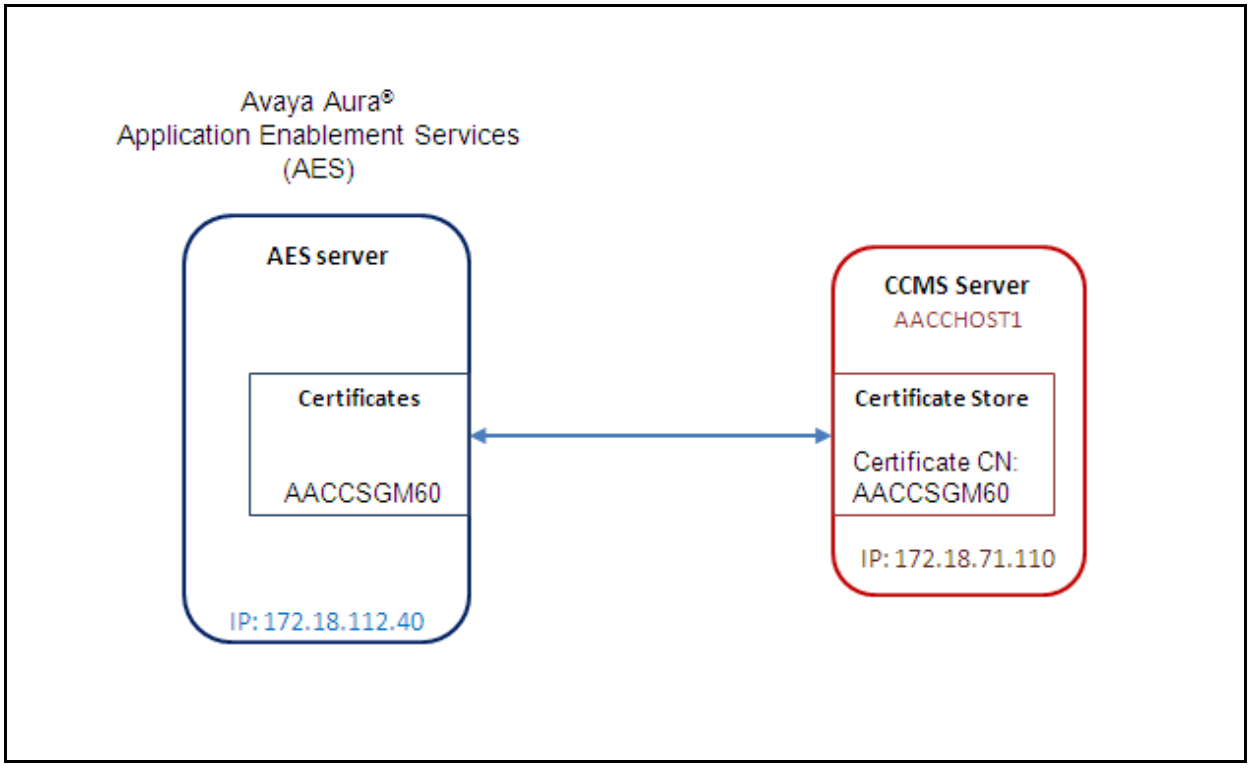
Unified Communications – Application Enablement Services configuration

Avaya Aura® Application Enablement Services (AES) is a set of enhanced telephony APIs, protocols, and Web services. These applications support access to the call processing, media, and administrative features available in Avaya Aura® Communication Manager. AES enables off-the-shelf and custom integration with communications applications such as Avaya Aura® Contact Center.

The Avaya Device, Media, and Call Control (DMCC) APIs provided by Application Enablement Services enable Avaya Aura® Contact Center to access the physical device, media, and basic third-party call control capabilities of Communication Manager.

The AES server uses Transport Layer Security (TLS) communication channels for the SIP CTI connection with Avaya Aura® Contact Center.

Example of using the CCMS default certificates with AES



Avaya Aura® Contact Center Release 6.3 includes a set of default certificates for use with Application Enablement Services. If you do not have access to or require a third-party Certificate Authority, you can install these Contact Center default certificates on your Application Enablement Services server to quickly establish a link between the two systems.

The sample solution in this guide uses the Avaya Aura® Contact Center default certificates. The Avaya Aura® Contact Center default certificates are installed on the Contact Center Manager Server at install time and they do not require configuration. You must import these default root certificates into the Avaya Aura® Application Enablement Services server so that it can communicate securely with Avaya Aura® Contact Center.

Adding the Avaya Aura® Contact Center default certificate as a trusted host on the Application Enablement Services server configures AES to communicate securely with one or more Contact Center Manager Server (CCMS) servers.

Attention: The Contact Center default certificates for AES may not meet your organization's security requirements. Avaya recommends the you use a third party Certificate Authority or follow your organization's security policies and procedures to better secure the TLS link between Avaya Aura® Contact Center and the Avaya Aura® Application Enablement Services server.

Accessing the AES server management console

Use the Avaya System Platform to access the Avaya Aura® Application Enablement Services (AES) server management console. You can log on to Application Enablement Services directly or you can log on using the System Platform.

Procedure steps

Step	Action
1	Start a Web browser.
2	In the **Address** box, type the secure URL for the Application Enablement Services server. For example, type **https://172.18.112.40** *A welcome page appears.*
3	Click **Continue To Login**.

A Logon dialog box appears.

4 In the **Username** box, type the administrator user name.

5 In the **Password** box, type the administrator user password.

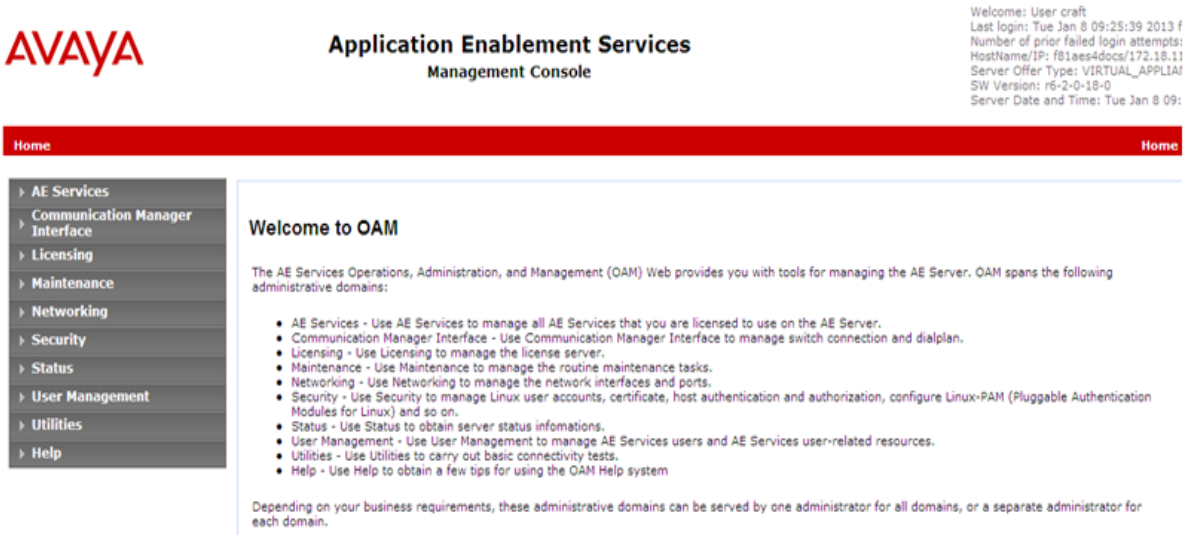
6 Click **Login**.

The Application Enablement Services Management Console appears.

--End--

Procedure job aid

The Application Enablement Services Management Console.



Adding the Communication Manager switch connection

Add the Communication Manager switch connection to the Application Enablement Services (AES).

Procedure steps

Step	Action
1	In the left pane of the AES management console, click **Communication Manager Interface**.
2	Select **Switch Connections**.
3	Under **Switch Connections**, type the host name of your Communication Manager. For example, type CM.
4	Click **Add Connection**.

5 In the **Switch Password** box, type the Communication Manager switch password.

6 In the **Confirm Switch Password** box, type the Communication Manager switch password again.

7 In the **Msg Period** box, accept the default (30 minutes).

8 Select the **SSL** check box.

9 Clear **Processor Ethernet**. By default this check box is not selected. Accept the default setting if you are administering a connection to a Communication Manager media server that uses a CLAN connection to AE Services.

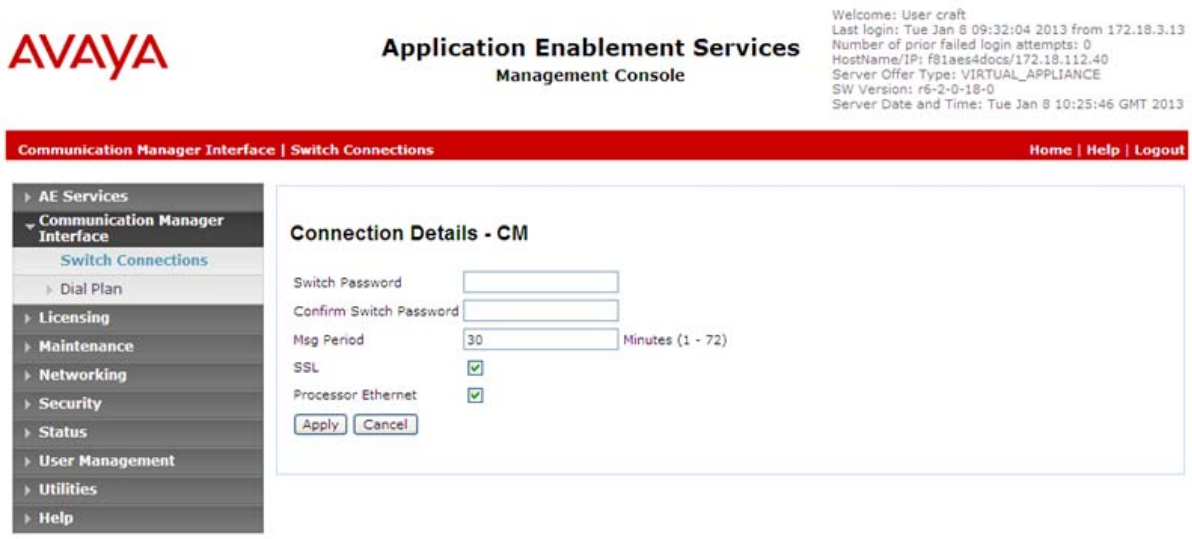
10 Click **Apply**.

The system adds the new Communication Manager switch connection to the list of switch connections.

--End--

Procedure job aid

The Communication Manager switch connection.



Adding the Communication Manager switch connection CLAN IP

Add the switch connection CLAN IP so Application Enablement Services (AES) can communicate with the Communication Manager. After you add a switch connection, you must associate the switch connection name with a CLAN host

name or IP address. Use this procedure when you are setting up a switch connection with a Communication Manager media server that uses a CLAN connection to AES.

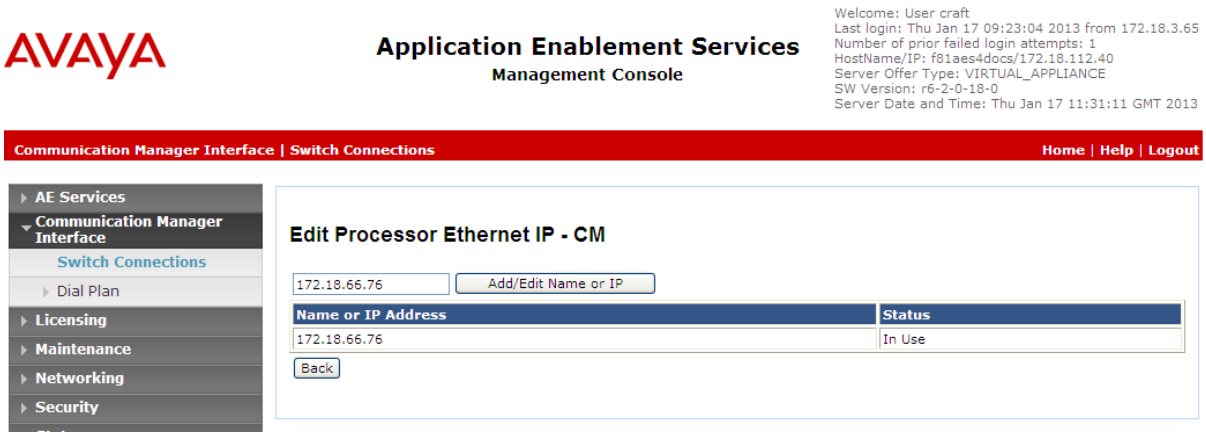
Procedure steps

Step	Action
1	In the left pane of the AES management console, click **Communication Manager Interface**.
2	Select **Switch Connections**.
3	From the list of **Switch Connections**, identify the switch connection to the Communication Manager.
4	Under your switch connection, click **Edit PE/CLAN IPs**.
5	In the **Edit CLAN IPs** box, type the IP address of your Communication Manager server. For example, type 172.18.66.76.
6	Click **Add Name or IP**.

--End--

Procedure job aid

The Communication Manager switch connection CLAN IP address.



Adding a CTI link to the Communication Manager

Add a CTI (TSAPI) link between Application Enablement Services (AES) and the Communication Manager.

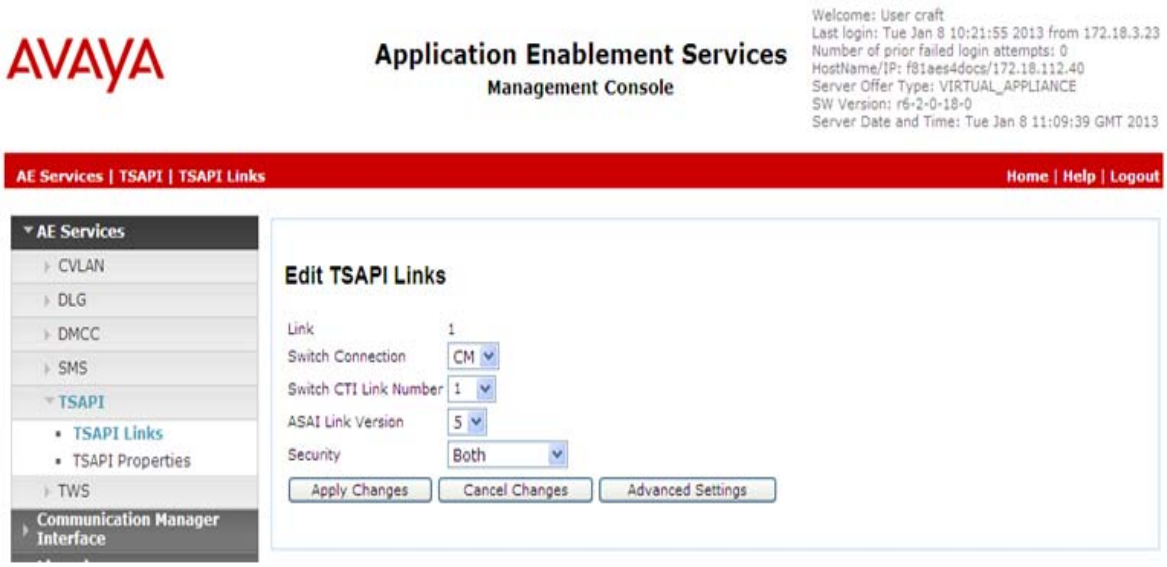
Procedure steps

Step	Action
1	In the left pane of the AES management console, click **AE Services**.
2	Select **TSAPI**, **TSAPI Links**.
3	Under **TSAPI Links**, click **Add Link**.
4	From the **Link** list, select the link number.
5	From the **Switch Connection** list, select the Communication Manager.
6	From the **Switch CTI Link Number** list, select the link number. The switch CTI link number must match that of the IP Services Server ID for AES as configured in Communication Manager. See Configuring a CTI Link for Application Enablement Services (page 63).
7	From the **ASAI Link Version** list, select **5**.
8	From the **Security** list, select **Both**.
9	Click **Apply Changes**.

--End--

Procedure job aid

The a CTI (TSAPI) link between Application Enablement Services (AES) and the Communication Manager.



When adding a CTI (TSAPI) link between Application Enablement Services (AES) and the Communication Manager, the switch CTI link number on the AES must match that of the IP Services Server ID for AES as configured in Communication Manager.

To add a CTI link on the Communication Manager, use “add cti-link n”, where “n” is an available CTI link number.

Restarting the AES to Communication Manager connection

Restart the TSAPI connection between Application Enablement Services (AES) and the Communication Manager. You must restart the TSAPI Service for changes to the CTI link between the AES and the Communication Manager to take effect.

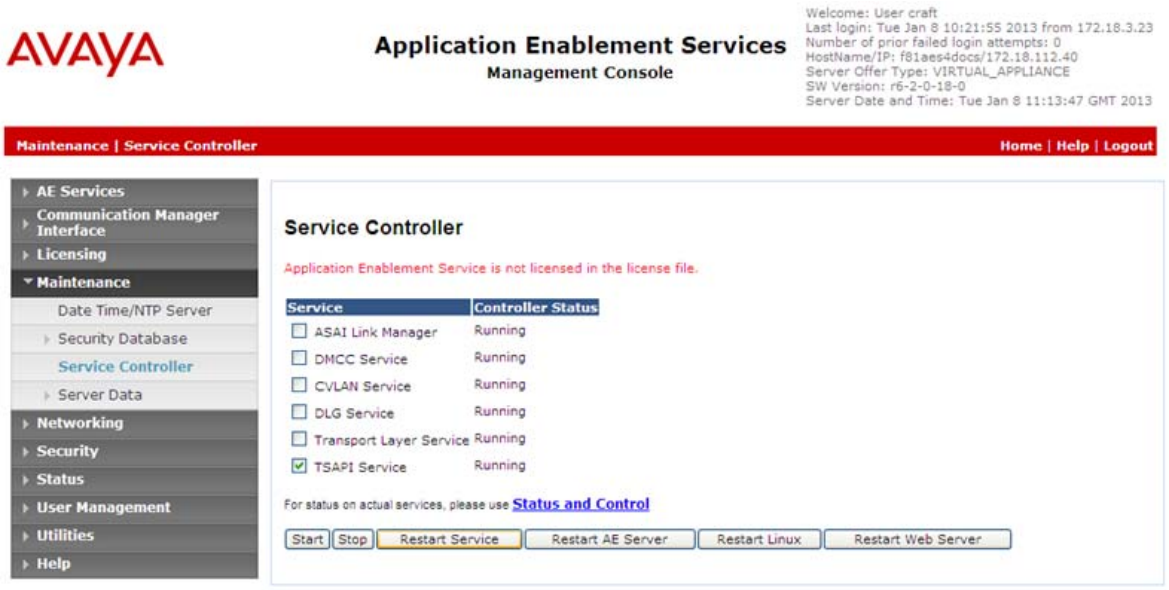
Procedure steps

Step	Action
1	In the left pane of the AES management console, click **Maintenance**.
2	Select **Service Controller**.
3	Under the Service Controller list of services, select **TSAPI Service**.
4	Ensure none of the other services are selected.
5	Click **Restart Services**.

--End--

Procedure job aid

The Avaya Aura® Application Enablement Services server maintenance service controller menu.



Enabling TR87 on the AES

Enable TR87 SIP CTI call control on the Avaya Aura® Application Enablement Services (AES) server. TR87 can be used over a SIP session to control and observe SIP user agents.

The TR87 interface on the AES is used by Avaya Aura® Contact Center to control and monitor agent stations on Avaya Aura® Communication Manager.

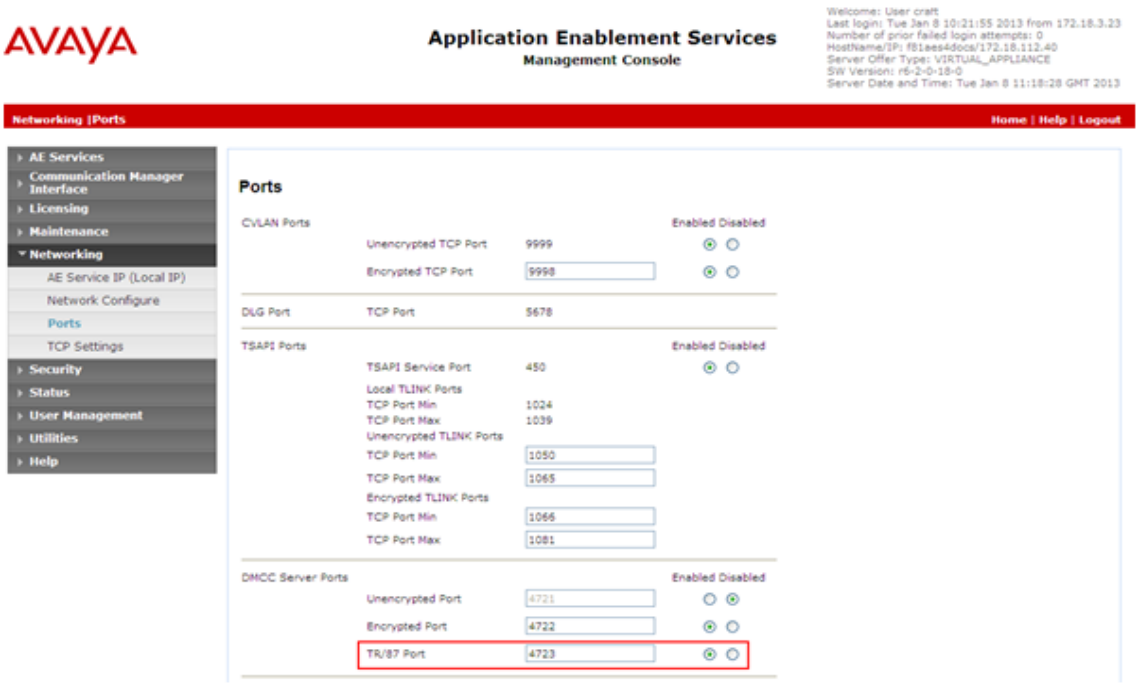
Procedure steps

Step	Action
1	In the left pane of the AES management console, click **Networking**.
2	Click **Ports**.
3	Scroll down to the DMCC Server Ports section.
4	In the **DMCC Server Ports** section, select the **Enabled** check box to the right of **TR/87 Port**.
5	Confirm that the **TR/87 Port** number is 4723.
6	Click **Apply Changes**.
7	Click **Apply**.

--End--

Procedure job aid

Enabling TR87 on the Avaya Aura® Application Enablement Services server.



Configuring security on the AES

Configure security on the Avaya Aura® Application Enablement Services server to require authorized host connections with the required client certification.

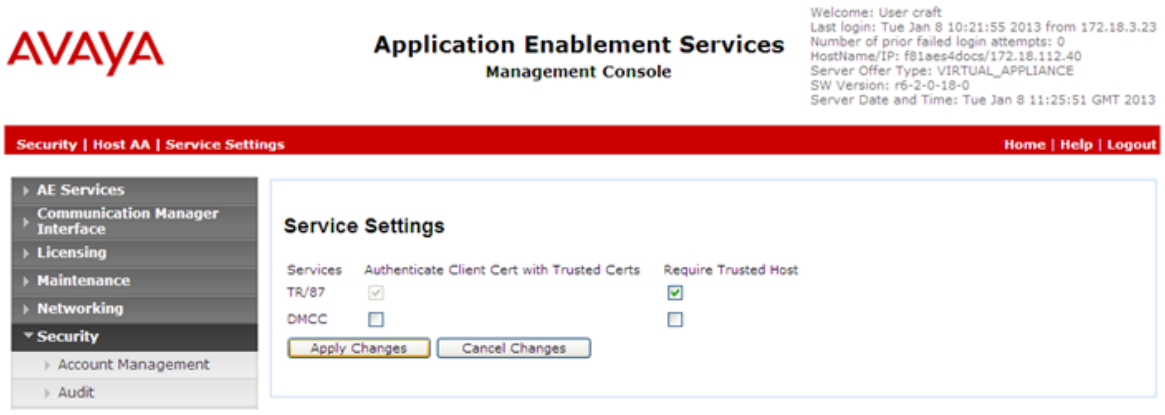
Procedure steps

Step	Action
1	In the left pane of the AES management console, click **Security**.
2	Click **Host AA**. *The system displays the Host Authentication and Authorization page.*
3	Click **Service Settings**.
4	Select the **TR/87**, **Require Trusted Host Entry** check box. *When you select this setting, the DMCC service verifies the Common Name (CN) in the client certificate and verifies that it matches one of the administered authorized hosts.*
5	Click **Apply Changes**.
6	On the **Apply Changes to Host AA** service page, click **Apply**.

--End--

Procedure job aid

Configuring security on the Avaya Aura® Application Enablement Services server.



Adding the Contact Center default certificate CN as a trusted host

Add the Avaya Aura® Contact Center default certificate Common Name (Certificate CN) as a trusted host on the Application Enablement Services server. The Avaya Aura® Contact Center default certificate Common Name (Certificate CN) is AACCSGM60.

Adding the Avaya Aura® Contact Center default certificate as a trusted host on the Application Enablement Services server configures AES to communicate securely with one or more Contact Center Manager Server (CCMS) servers.

Procedure steps

Step	Action
1	In the left pane of the AES management console, click **Security**.
2	Click **Host AA**.
3	Click **Trusted Hosts**.
4	Click **Add**.
	An Add Trusted host page appears.
5	In the **Certificate CN or SubAltName** box, type **AACCSGM60**.
6	From the **Service Type** list, select **TR/87**.
7	From the **Authentication Policy** list, select **Not Required**.
8	From the **Authorization Policy** list, select **Unrestricted Host**.

9 Click **Apply Changes**.

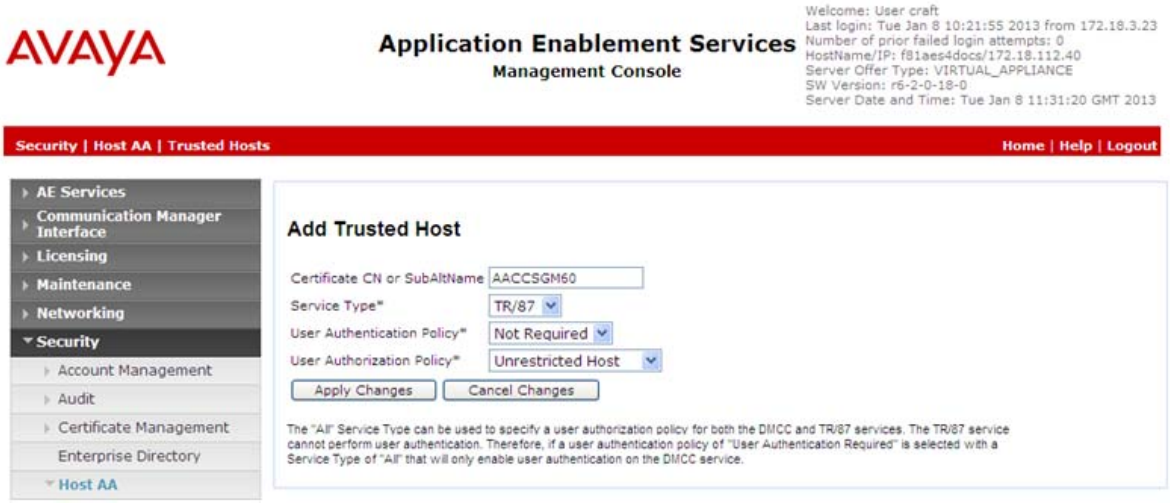
The system displays a confirmation page.

10 Click **Apply**.

--End--

Procedure job aid

Using the Avaya Aura® Contact Center default certificate Common Name (Certificate CN) as a trusted host on the Application Enablement Services server. The Avaya Aura® Contact Center default certificate Common Name (Certificate CN) is AACCSGM60.



Restarting the AES Linux server

Restart the Application Enablement Services (AES) Linux server to apply system configuration changes.

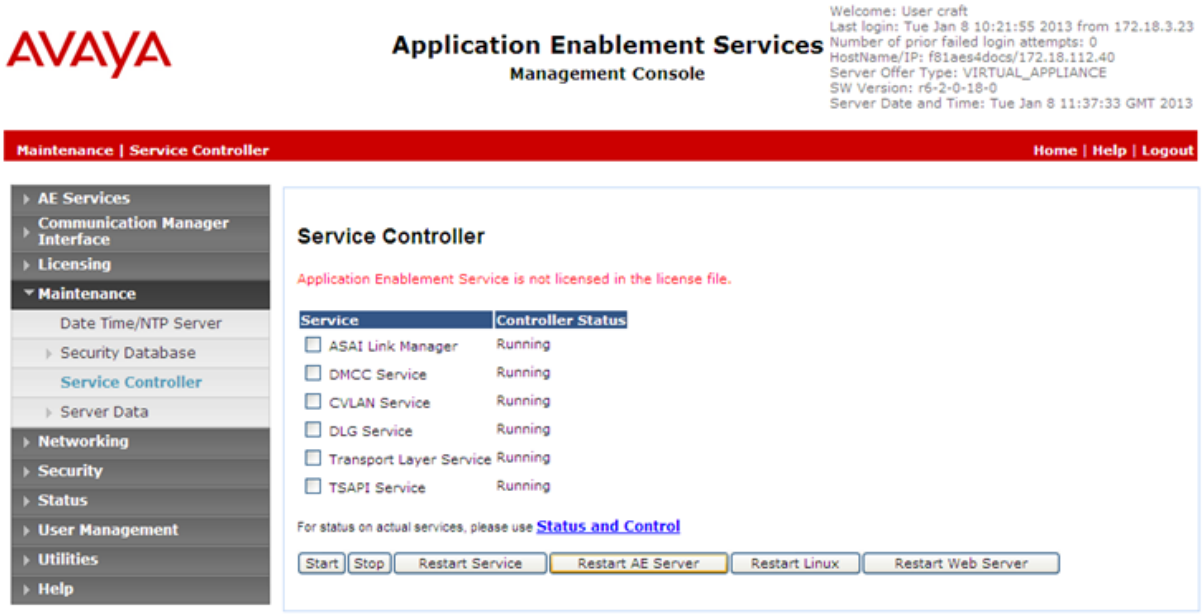
Procedure steps

Step	Action
1	In the left pane of the AES management console, click **Maintenance**.
2	Click **Service Controller**.
3	Click **Restart Linux**, to restart the AES Linux server.
4	Click **Restart**.

--End--

Procedure job aid

The Avaya Aura® Application Enablement Services server maintenance service controller menu.



Verifying the AES services are running

The configuration changes made to the AES server take effect only when the AES server starts. Check that the changes are applied correctly after the restart.

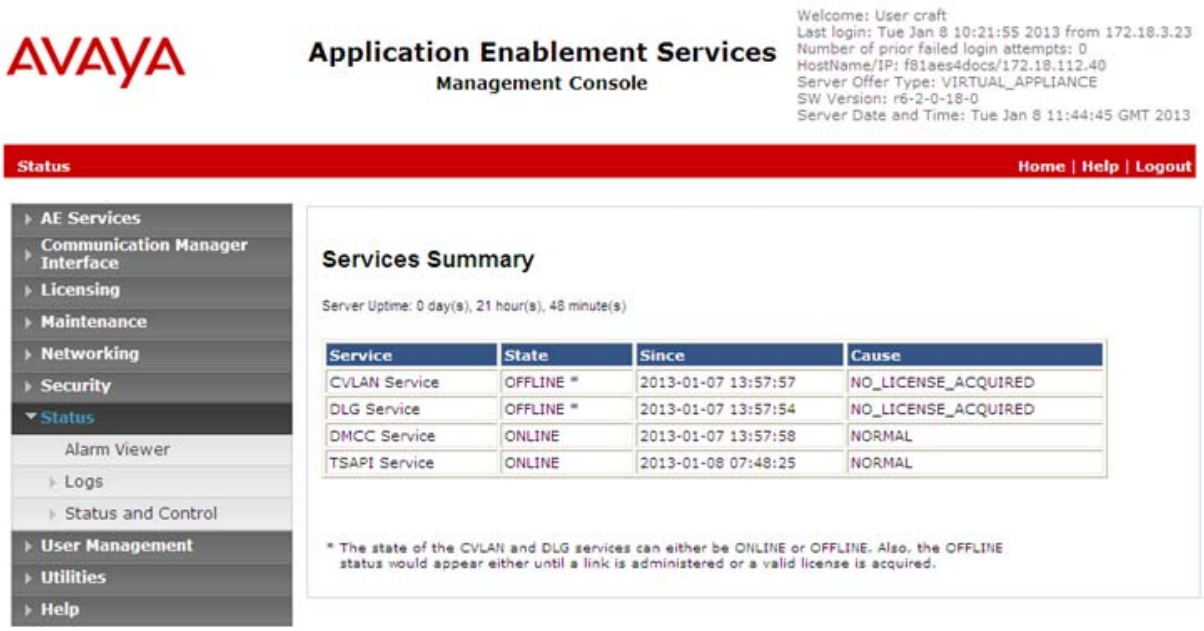
Procedure steps

Step	Action
1	In the left pane of the AES management console, click **Status**.
2	Ensure the **DMCC Service** has an **ONLINE** state and a **Normal** cause.
3	Ensure the **TSAPI Service** has an **ONLINE** state and a **Normal** cause.

--End--

Procedure job aid

The Avaya Aura® Application Enablement Services server - Services Summary showing the DMCC Service and the TSAPI Service.



Verifying the AES connection to the Communication Manager switch

After restarting the Application Enablement Services (AES) server, confirm that it is still communicating with the Communication Manager.

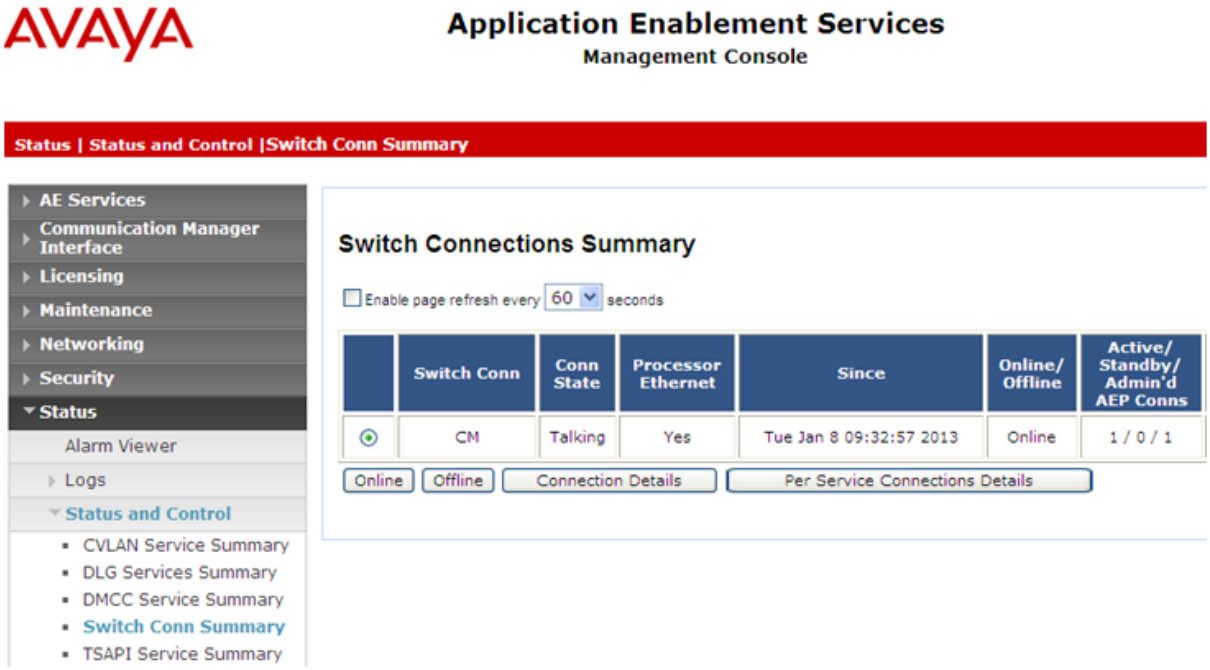
Procedure steps

Step	Action
1	In the left pane of the AES management console, click **Status**.
2	Click **Status and Control**.
3	Click **Switch Conn Summary**.
4	Ensure that the **Switch Connections Summary** has a **Conn State** of **Talking**.

--End--

Procedure job aid

The Avaya Aura® Application Enablement Services server - Switch Connections Summary.



Verifying the AES TSAPI connection

After restarting the AES server, confirm that it is still communicating with the Telephony Service API (TSAPI).

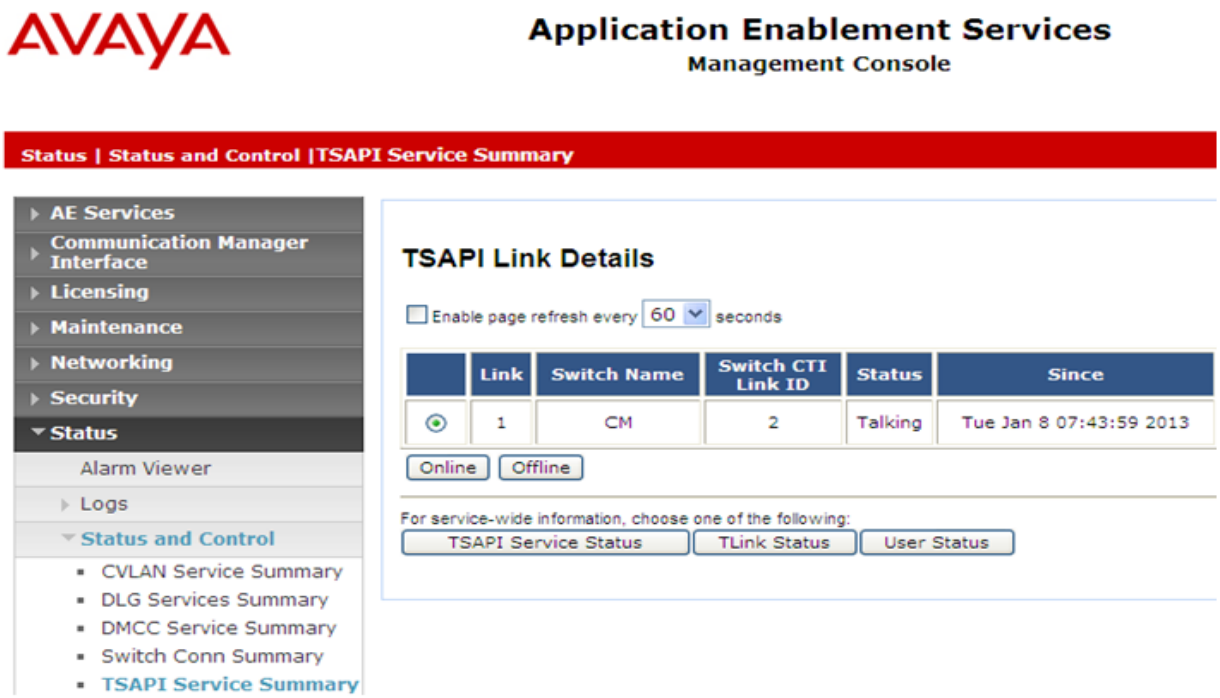
Procedure steps

Step	Action
1	In the left pane of the AES management console, click **Status**.
2	Click **Status and Control**.
3	Click **TSAPI Service Summary**.
4	Ensure that the **TSAPI Link Details** has a **Status** of **Talking**.

--End--

Procedure job aid

The Avaya Aura® Application Enablement Services server - TSAPI Service Summary.



Debugging the AES server

After restarting the AES server, if there server communication issues, you can use the error log files to diagnose and resolve the issue.

Procedure steps

Step	Action
1	In the left pane of the AES management console, click **Status**.
2	Click **Logs**, **Error Logs**. *The list of error logs appears on the right pane.*
3	Select the file to view, scroll down, and click **view**. Copy all text and paste it into a text editor to view.

--End--

Procedure job aid

The Avaya Aura® Application Enablement Services server - Error Logs.


AVAYA
Application Enablement Services
Management Console
Welcome: User craft
Last login: Tue Jan 8 10:21:55 2013 from 172.18.3.23
Number of prior failed login attempts: 0
HostName/IP: f81aes4docs/172.18.112.40
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-2-0-18-0
Server Date and Time: Tue Jan 8 11:56:19 GMT 2013
Status | Logs | Error Logs
Home | Help | Logout
AE Services
Communication Manager Interface
Licensing
Maintenance
Networking
Security
Status
Alarm Viewer
Logs
Audit Logs
Error Logs
Install Logs
Security Logs
Syslog
Tripwire Logs
User Management Service
Status and Control
Error Logs
Log File
Timestamp
dmcc-api.log.0
Jan 7, 2013
dmcc-api.log.1
May 29, 2012
dmcc-error.log.0
Jan 7, 2013
dmcc-error.log.1
May 29, 2012
dmcc-jtapi-error.log
May 29, 2012
dmcc-nist.log.0
Jan 7, 2013
dmcc-nist.log.1
May 29, 2012
dmcc-trace.log.0
Jan 8, 2013
dmcc-trace.log.1
May 29, 2012
dmcc-wrapper.log
Jan 7, 2013
lcm-api.log.0
Jan 7, 2013

Contact Center server software installation section

- Voice and Multimedia Contact Server with Avaya Media Server software installation (page 115)

Voice and Multimedia Contact Server with Avaya Media Server software installation

This chapter describes the steps to install the Voice and Multimedia Contact Server with Avaya Media Server software. This includes the following server software:

- Contact Center Manager Server (CCMS)
- Contact Center License Manager (LM)
- Contact Center Manager Administration (CCMA)
- Communication Control Toolkit (CCT)
- Contact Center Multimedia (CCMM)
- Orchestration Designer (OD)
- Avaya Media Server

You can change the name of a Voice and Multimedia Contact Server with Avaya Media Server after installation is complete, but because this is time consuming, Avaya recommends that you configure the server final production name before installing Contact Center software.

Example server details	Active Voice and Multimedia Contact Server
Name	AACCHOST1
IP Address	172.18.71.110

You can create an administration account on the server and then install Avaya Aura® Contact Center using the account. This Avaya Aura® Contact Center administration account must have full administrative privileges. You must upgrade and patch Avaya Aura® Contact Center using this administration account. You can rename this account after installing Avaya Aura® Contact Center, but you must not delete the account. If you delete the account used to install Avaya Aura® Contact Center, Avaya Aura® Contact Center stops working.

Prerequisites to Voice and Multimedia Contact Server software installation

- Ensure that your new Contact Center license file is available. This sample solution uses a WebLM license file obtained from the Avaya Product Licensing and Delivery System (PLDS).
- Ensure that the Voice and Multimedia Contact Server with Avaya Media Server meets or exceeds the minimum hardware and platform requirements as specified in *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
- Download and review the Avaya Aura® Contact Center Release Notes. The Release Notes contain the known issues, patches, and workarounds specific to a release and

patch line-up of Avaya Aura® Contact Center. For more information about the Avaya Aura® Contact Center Release Notes, see www.avaya.com/support.

Installing Windows Server 2008 Release 2

Install the Windows operating system, which is required for the Contact Center server software. During the installation, configure the Windows settings as listed.

Prerequisites

- Ensure that you have a newly formatted server that meets the specifications in *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210) on which to install Microsoft Windows Server 2008 Release 2.
- Ensure that you have a DVD for Windows Server 2008 Release 2.
- Install the network interface card in the server.
- Know the IP addresses for the contact center subnet.

Procedure steps

Step	Action
1	Insert the Windows Server 2008 64-bit Release 2 Standard Edition or Windows Server 2008 64-bit Release 2 Enterprise Edition DVD into the DVD drive.
2	Install Windows Server 2008 Release 2 according to the instructions supplied by the DVD.
3	On the first install page, select your language for installation.
4	Click **Next**.
5	On the **Installation** window, select a **Language to install** from the list.
6	Select a **Time and currency** format from the list.
7	Select **Keyboard or input** method from the list.
8	Click **Next**.
9	Click **Install Now**.
10	Select an operating system from the list.
11	Click **Next**.
12	On the first Install Windows screen, read the terms of the license agreement and select **I accept the license terms**.
13	Click **Next**.
14	Select **Custom**.
15	Select the disk partition on which you want to install Windows Server 2008.

Attention: You can use the partition management options to configure the partitions on your server. The Operating System partition must be 60GB or greater. The minimum recommended Operating System disk partition size is 80GB.

16 Click **Next**.

The install proceeds and automatically restarts the server several times.

17 After completing the installation, log on to the server as Administrator. Enter and confirm the local Administrator password.

18 In the **Initial Configuration Tasks** window, select **Activate Windows** and follow the instructions or the Microsoft documentation to activate your server.

19 Select **Set time zone** and complete the information as required for your system.

This setting must match on Contact Center Manager Server and Avaya Media Server.

20 Select **Configure Networking** and complete the information for your Network Interface Card (NIC) with the server IP address.

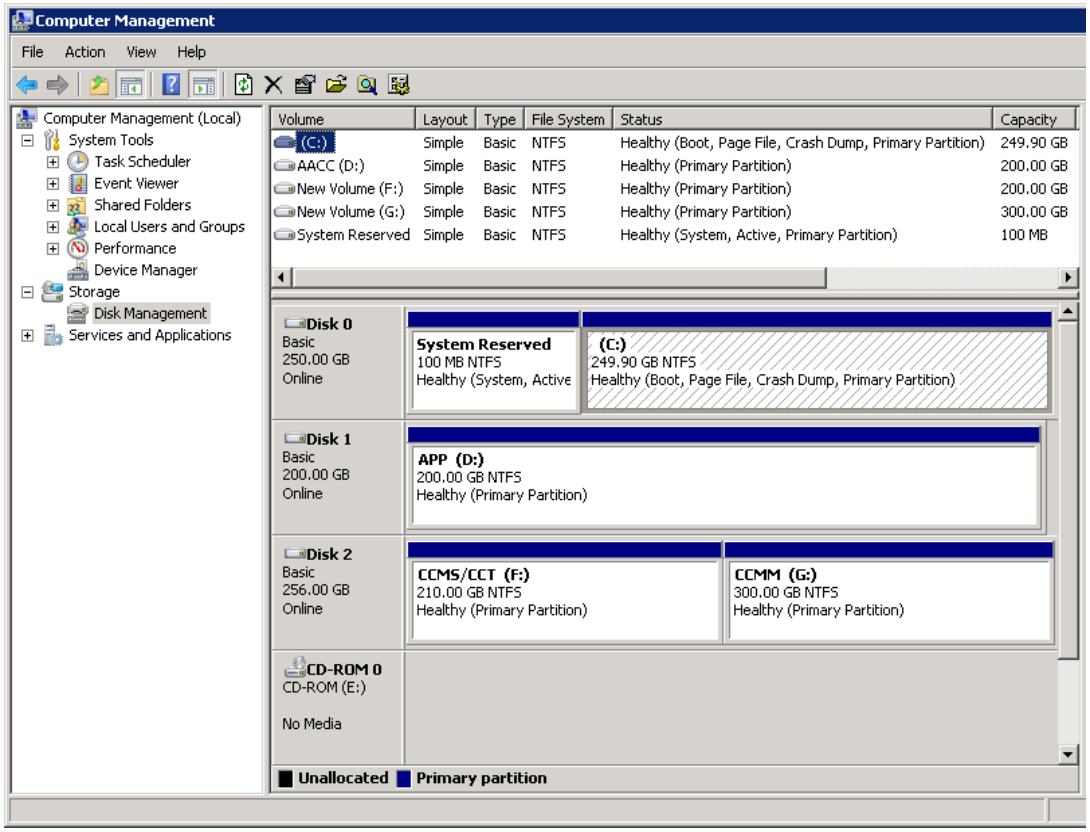
21 Select **Provide computer name and domain** and complete the information for your server name and domain settings.

22 Configure disk drive C: to be the only primary partition on your hard drive.

23 Change the DVD drive letter to E: to ensure the correct drive letters are free for the drives needed for the Avaya Aura® Contact Center application components.

24 Configure the remaining drives for this server as follows:

— D: 80Gb Application drive, minimum.
— F: 210Gb CCMS/CCT Database drive, minimum.
— G: 300Gb CCMM Database drive, minimum.



25 Install any drivers required for your hardware configuration.

--End--

Installing the most recent operating system service packs

Install the most recent supported operating system service packs. You must download the supported operating system service pack included in the Avaya Contact Center Service Packs Compatibility and Hotfix Availability list to ensure your Contact Center server software functions correctly with the supported operating system patches.

Prerequisites

- Access the Avaya Contact Center Service Packs Compatibility and Hotfix Availability list on the support Web site www.avaya.com/support.
- Review the recommendations on operating system service updates in *Avaya Aura*® *Contact Center Planning and Engineering* (NN44400-210).

Procedure steps

Step	Action
1	Log on to the server and disable the Windows Update feature. There are a number of methods for disabling the Windows Update feature, refer to the Windows Server 2008 documentation for a method suitable to your solution. Disabling the Windows Update feature prevents Windows Server 2008 from automatically applying operating system patches and potentially rebooting the server.
2	Review the Contact Center Service Packs Compatibility and Security Hotfixes Applicability list to determine the most recent Avaya Aura® Contact Center supported patches or service packs.
3	Download the appropriate Microsoft Windows Server 2008 patches for the Avaya Aura® Contact Center software installed on this server.
4	Install the most recent Microsoft Windows Server 2008 service pack that is validated with Avaya Aura® Contact Center by following the Microsoft Installation instructions.

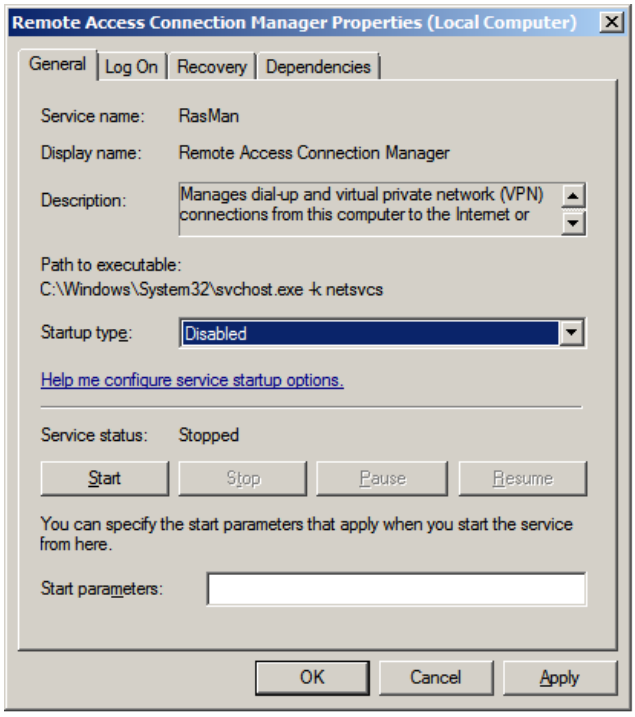
--End--

Disabling the Remote Access services

Disable the Remote Access services on the core contact center server, to support Communication Control Toolkit. Microsoft Remote Desktop continues to run after you disable Remote Access services. After you disable the services, restart the server.

Procedure steps

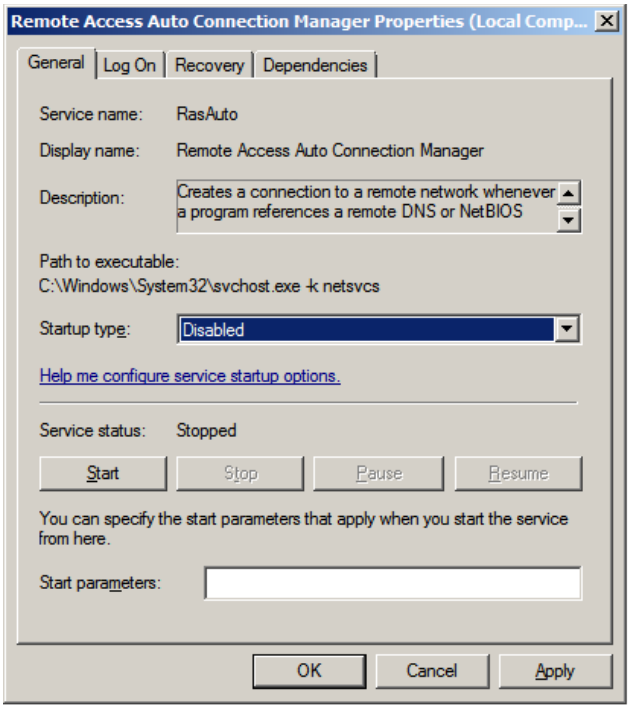
Step	Action
1	Choose **Start**, **Administrative Tools**, **Services**.
2	In the **Services** window, right-click the **Remote Access Connection Manager** icon.
3	Click **Properties**.
4	In the **General** tab, from the **Startup type** list, select **Disabled**.



5 Click **OK**.

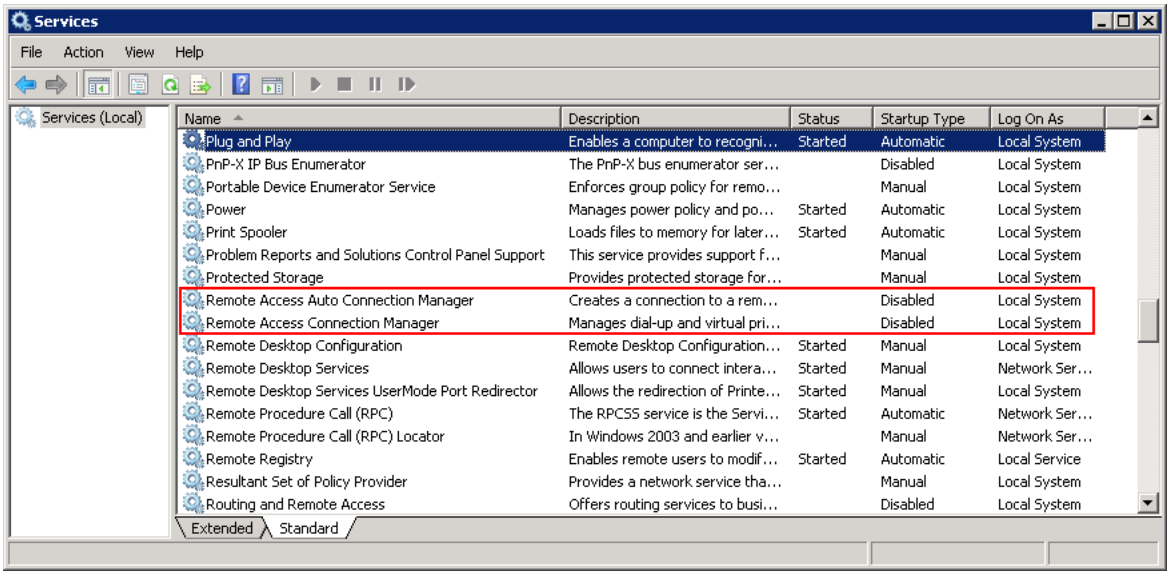
6 In the **Services** window, right-click the **Remote Access Auto Connection Manager** icon.

7 Click **Properties**.



8 In the **General** tab, from the **Startup type** list, select **Disabled**.

9 Click **OK**.



10 In the **Services** window, click **File**, **Exit**.

11 Restart the server.

--End--

Adding the server to a domain

Add the server to an existing domain. Perform this procedure before installing any Contact Center software.

Ask your Domain Administrator to add a Domain Name System (DNS) static entry for this server. Each Contact Center server in a domain requires a DNS static entry.

Attention: Avaya Aura® Contact Center High Availability solutions do not support Windows Server 2008 Dynamic DNS.

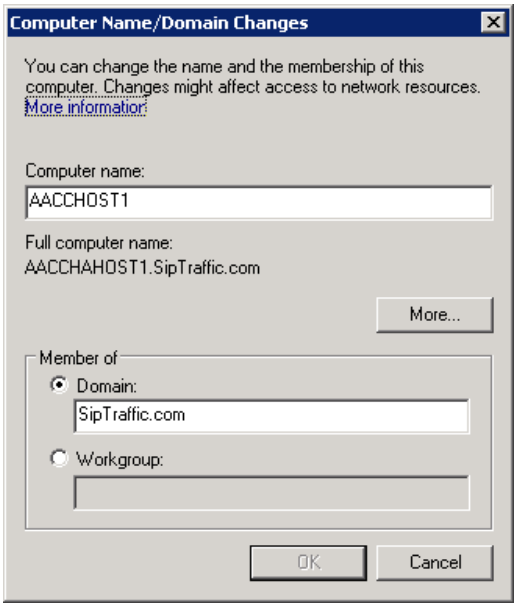
In High Availability solutions, ask your Domain Administrator to add one DNS static entry for each managed name and associated managed IP address. A typical High Availability campus solution with a pair of servers requires three DNS static entries; one DNS static entry for the active server, one DNS static entry for the standby server, and one DNS static entry for the managed name and associated IP address.

Prerequisites

- On this server, configure a preferred Domain Name System (DNS) server on the Network Interface Card (NIC).

Procedure steps

Step	Action
1	Log on to the server using an administrator account.
2	Click **Start**, **Administrative Tools**, **Server Manager**.
3	Beside **Computer Information**, click **Change System Properties**.
4	In the **System Properties** dialog box, click the **Computer Name** tab.
5	Click **Change**.
6	In the **Computer Name/Domain Changes** dialog box, select the **Domain** option.
7	Type the domain name (you must provide the fully qualified domain name, which includes the prefix and suffix), for example siptraffic.com.
8	Click **OK**.
9	Type the domain administrator **User name** and **Password**.



10 Click **OK**.

11 Restart the server when the system prompts you to do so.

--End--

Downloading the most recent Contact Center patches to the server

To ensure that you have the most current software, download the most recent Contact Center patches from www.avaya.com/support to each server.

Procedure steps

Step	Action
1	Log on to the server using an administrator account.
2	Create a folder **ProductUpdates** on the **D:** drive.
3	Download the most recent Contact Center service pack file and save it on the Contact Center server in the **ProductUpdates** folder.
4	Right-click the service pack zip file and select **Extract All** from the context menu.

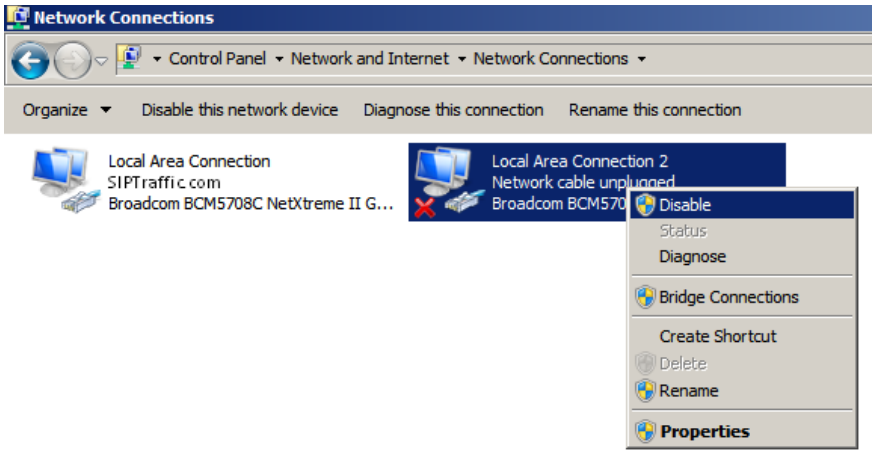
--End--

Disabling unused Network Adapters

Disable all unused Network Adapters or Network Interface Cards (NICs) to improve network communications and to prevent the incorrect configuration of unused NICs during Contact Center server commissioning.

Procedure steps

Step	Action
1	Log on to the server using an Administrator account.
2	Click **Start**, **Control Panel**, **Network and Internet**, **Network and Sharing Center**, **Change Adapter Settings**.



Step	Action
3	Right-click the unused Network Adapter, and select **Disable**.
4	Repeat this procedure for any unused Network Adapters.

--End--

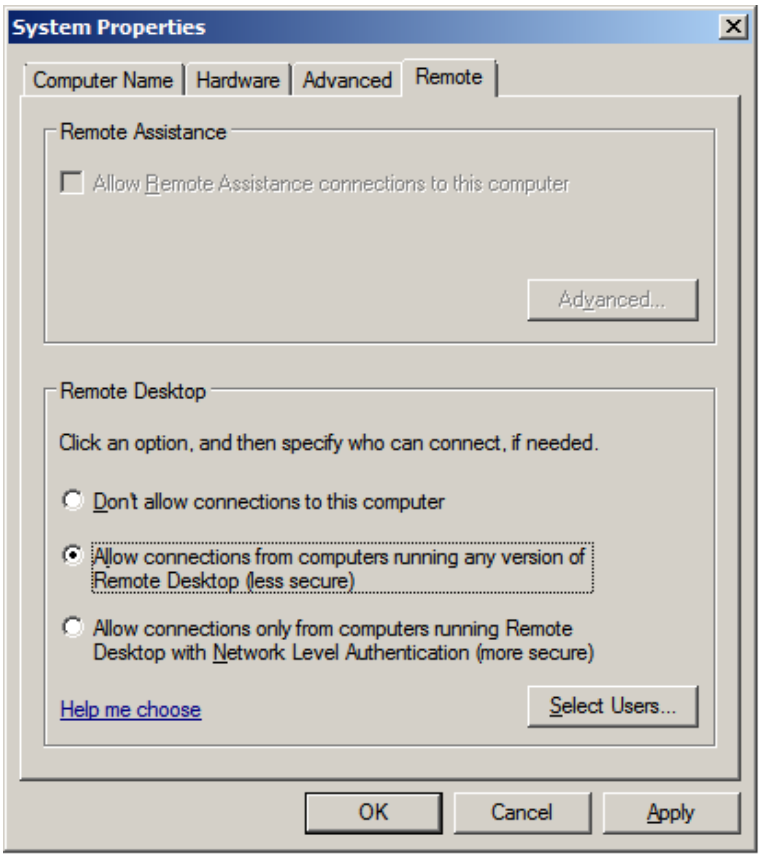
Enabling Microsoft Remote Desktop connection

Enable Microsoft Remote Desktop connection as your remote access tool. Microsoft Remote Desktop provides remote access for personnel supporting the server.

Procedure steps

Step	Action
1	Log on to the server using an administrator account.
2	Choose **Start**, **Control Panel**, **System and Security**.
3	In the **System** section, select **Allow remote access**.
4	Click the **Remote** tab.

5 Select **Allow connections from computers running any version of Remote Desktop (less secure)**.



6 Click **OK**.

--End--

Configuring Data Execution Prevention

Configure the Data Execution Prevention (DEP) hardware and software to perform additional checks on memory that protect the Contact Center server against malicious code exploitation.

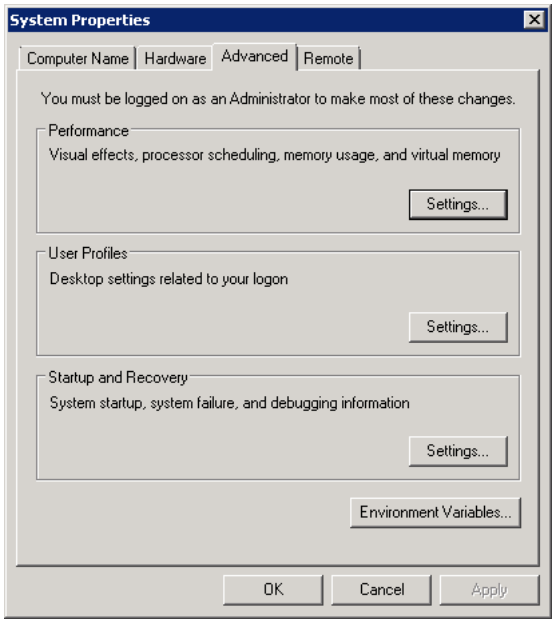
Procedure steps

Step	Action
1	Log on to the server using an Administrator account.
2	Choose **Start, Control Panel, System and Security**.

3 Click **System**.

4 In the **System** window, click **Advanced system settings**.

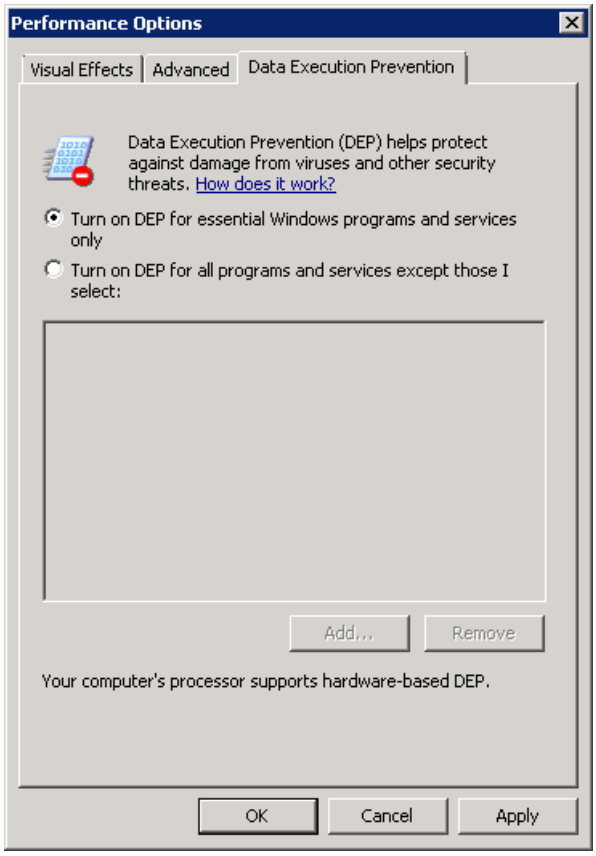
5 In the **System Properties** dialog box, click the **Advanced** tab.



6 Under **Performance**, click **Settings**.

7 In the **Performance Options** dialog box, click the **Data Execution Prevention** tab.

8 On the **Data Execution Prevention** tab, select **Turn on DEP for essential Windows programs and services only**.



9 Click **OK**.

10 On the **System Properties** dialog box, click **OK**.

11 Click **OK** to restart the computer.

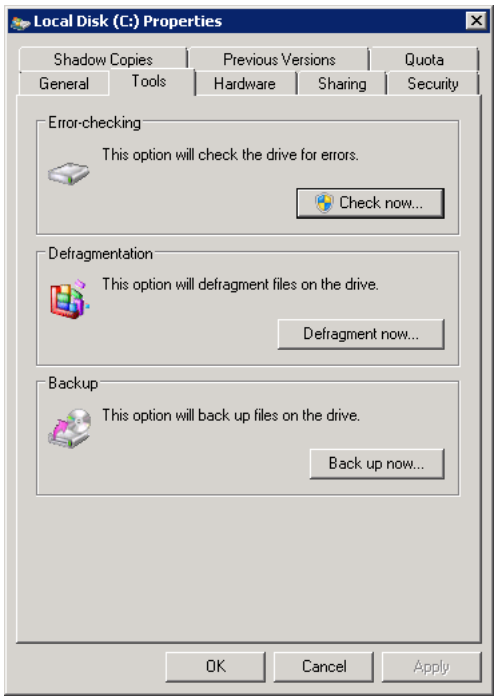
--End--

Scheduling Weekly Disk Defragmentation

Schedule weekly Disk Defragmentation for drive C: and drive D: to optimize performance and avoid potential outages.

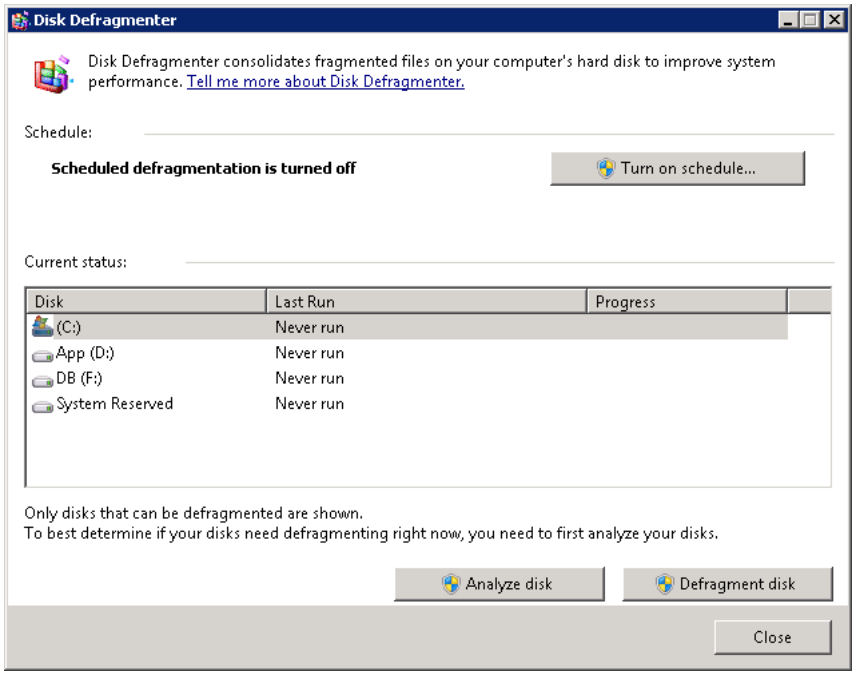
Procedure steps

Step	Action
1	Click **Start**, **Computer**.
2	Right-click drive C: and select **Properties**.
3	Click the **Tools** tab.



4 Select **Defragment Now**.

5 Click **Turn on Schedule**.



6 Select **Run on a schedule (recommended)**.

7 Under **Frequency**, select **Weekly**.

8 Under **Day**, select the day you want to schedule the defragmentation process.

9 Under **Time**, select an off-peak time at which you want to schedule the defragmentation process.

10 Click **Select Disks**.

11 In the **Disk Defragmenter: Select Disks for Schedule** window, select drive C: and drive D:.

12 Click **OK**.

13 Click **OK**.

14 Click **Close**.

15 On the **Properties** dialog box, click **OK**.

--End--

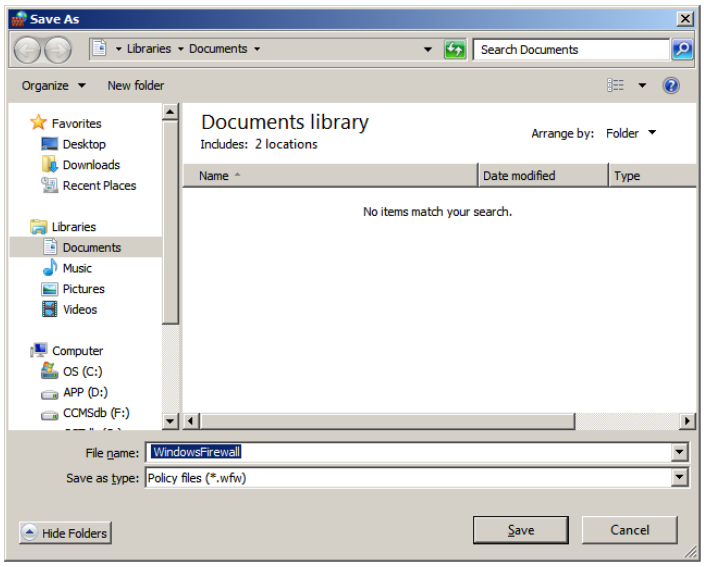
Importing the Contact Center Firewall Security policy

Import the Avaya Aura® Contact Center Firewall Security policy to ensure all contact center servers in the solution can communicate.

Export and backup your existing firewall security policy before importing the Avaya Aura® Contact Center Firewall Security policy. You can use this backup policy to rollback the Avaya Aura® Contact Center Firewall Security policy.

Procedure steps

Step	Action
1	Download the most recent Avaya Aura® Contact Center Firewall Security policy from www.avaya.com/support.
2	Log on to the server using an Administrator account.
3	Choose **Start**, **Administrative Tools**, **Windows Firewall with Advanced Security**.
4	Choose **Actions**, **Export Policy**.
5	In the **File name** box, type the name for the backup policy.



6 Click **Save**.

Windows exports the existing policy. You can use this backup policy to rollback the Avaya Aura® Contact Center Firewall Security policy, if you ever need to.

7 On the **Policy successfully exported** message box, click **OK**.

8 Choose **Actions**, **Import Policy**.

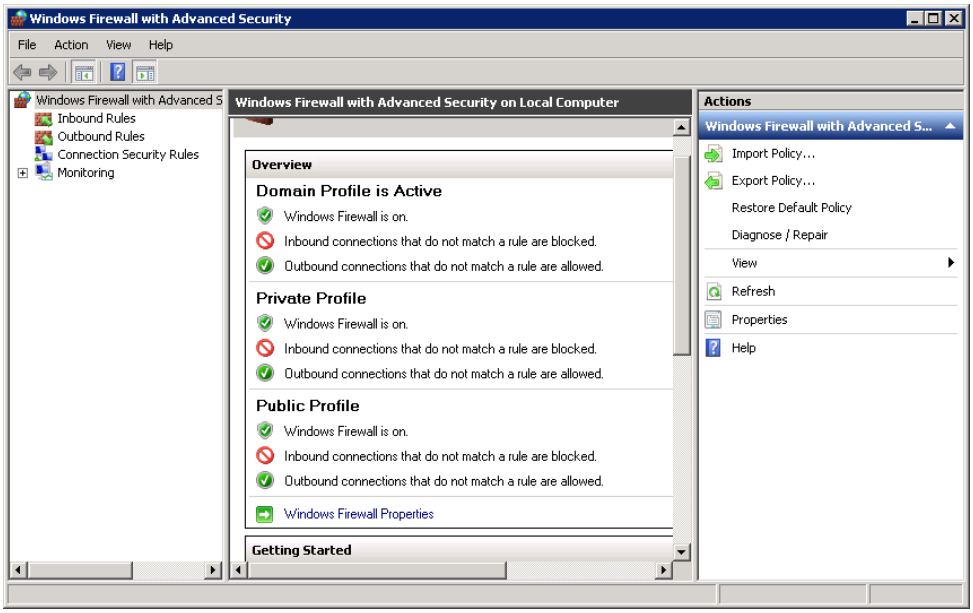
9 On the policy overwrite message box, click **Yes**.

10 Navigate to the folder containing the Avaya Aura® Contact Center Firewall Security policy and select the policy.

11 Click **Open**.

Windows imports the Avaya Aura® Contact Center Firewall Security policy.

12 On the **Policy successfully imported** message box, click **OK**.



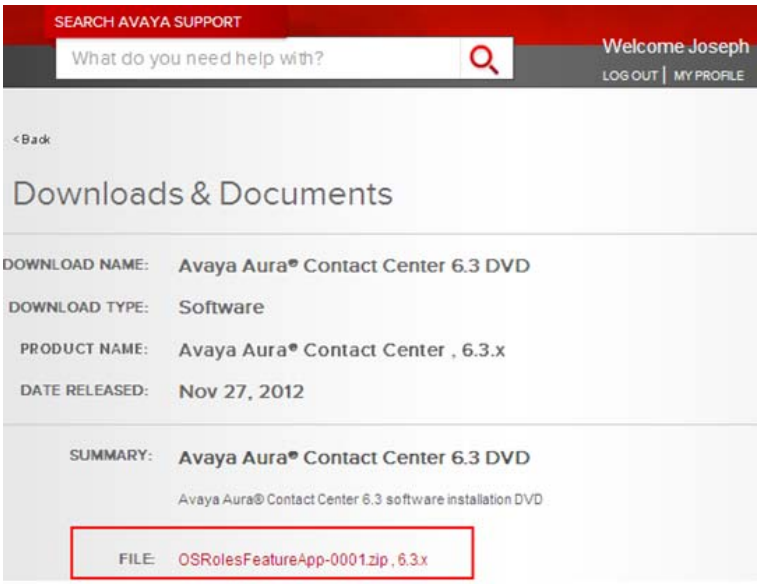
--End--

Downloading the Roles and Features Installer

The Avaya Aura® Contact Center Roles and Features Installer utility configures your Windows Server 2008 operating system. You must download the Roles and Features Installer from the support Web site http://support.avaya.com.

Procedure steps

Step	Action
1	Log on to http://support.avaya.com.
2	Navigate to the Avaya Aura® Contact Center Release 6.3.x section of the Avaya Support Web site.
3	Under Downloads and Documents, click on the file to download the Avaya Aura® Contact Center Roles and Features Installer.



4 Save the OSRolesFeatureApp-0001 folder to a location on your server.

--End--

Installing the required Windows roles and features

The Avaya Aura® Contact Center Roles and Features Installer is a new utility that configures your Windows Server 2008 operating system. The Roles and Features Installer installs the following required Windows Server 2008 roles and features:

- Active Directory Lightweight Directory Services
- Application Server
- Web Server (IIS)
- SNMP Services
- Windows Server Backup Features

Prerequisites

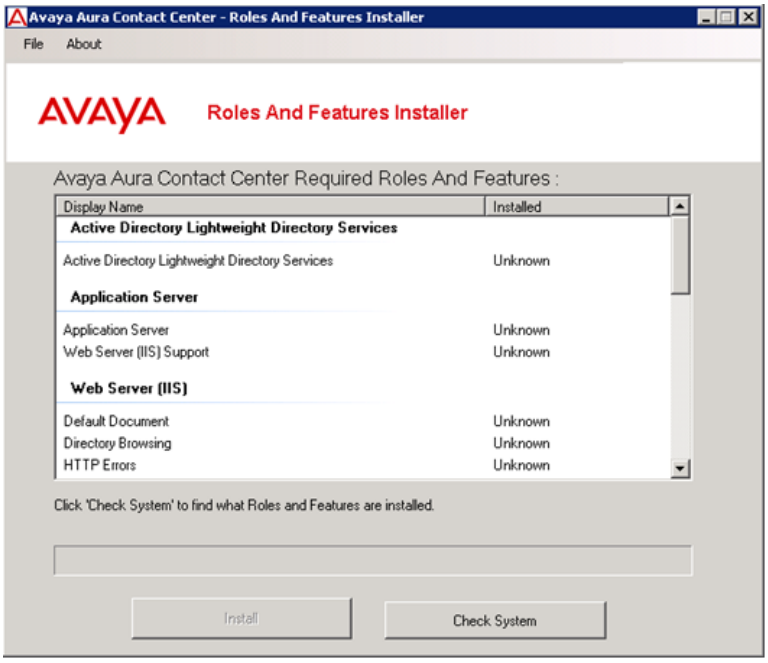
- Download the Avaya Aura® Contact Center Roles and Features Installer from the Avaya support website and save the application to a location on your server.

Procedure steps

Step	Action
1	Log on to the server.
2	Open the OSFeatureRolesApp-0001 folder.

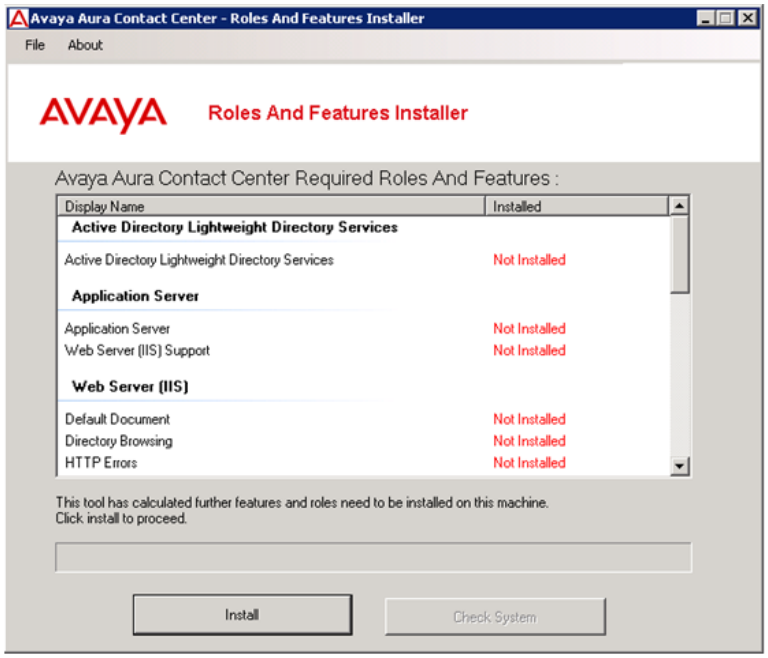
3 Open the APP folder and double-click **InstallWindowsFeatures**.

The Avaya Aura® Contact Center Roles and Features Installer appears.



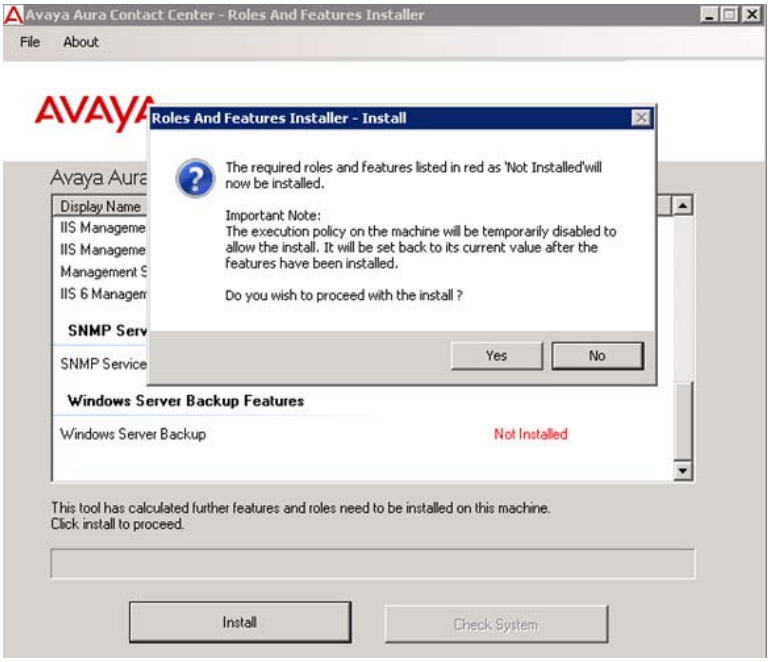
4 Click **Check System**.

The Avaya Aura® Contact Center Roles and Features Installer checks if the required roles and features are installed.



5 If all of the required roles and features are not installed, click **Install**.

6 Click **Yes**.



7 After the installation is complete, click **OK**.

--End--

Configuring Windows Server 2008

Before you install Contact Center software on your server, create a repair disk and back up the operating system configuration.

Prerequisites

- Install Microsoft Windows Server 2008 64-bit Release 2 on your server.

Procedure steps

Step	Action
1	Log on to the Windows Server 2008 server using an administrator account.
2	Select the **Don't display this screen on startup** check box.
3	Choose **Start**, **All Programs**, **Accessories**, **System Tools**, **Windows Server Backup**.
4	Follow the on-screen instructions to select what files you want to back up.

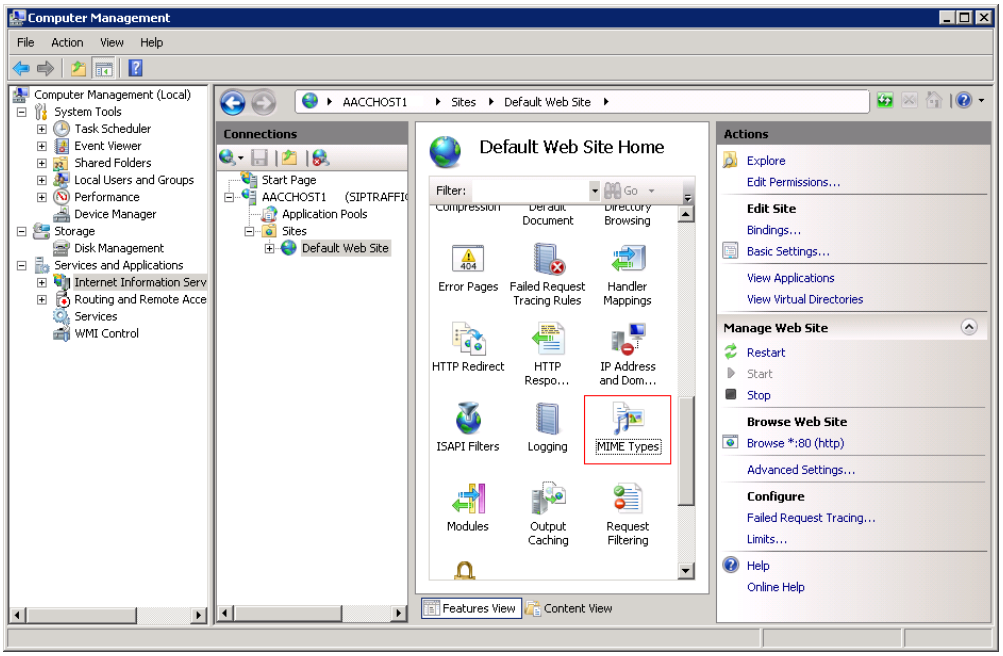
--End--

Configuring MIME types to support Microsoft updates

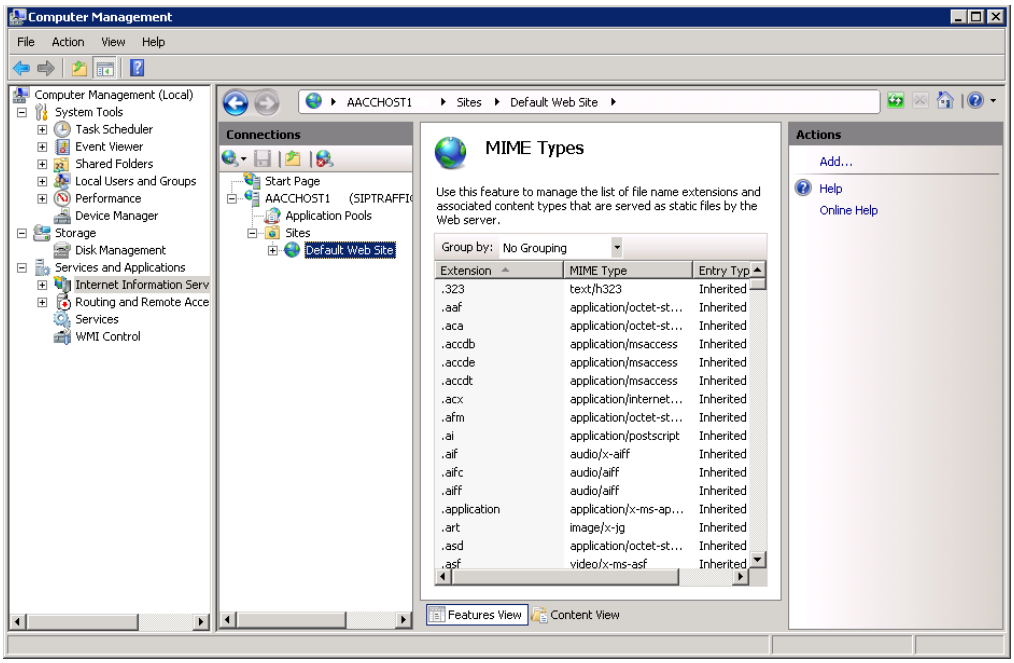
Configure the Multipurpose Internet Mail Extension (MIME) types to support Microsoft updates and patches.

Procedure steps

Step	Action
1	Log on to the server using an Administrator account.
2	Click **Start**, **Administrative Tools**, **Computer Management**.
3	In the **Computer Management** dialog box, expand **Services and Applications**, **Internet Information Services (IIS Manager)**.
4	Under **Connections**, expand **AACCHOST1**, **Sites**, **Default Web Site**.
5	Select **Default Web Site**.



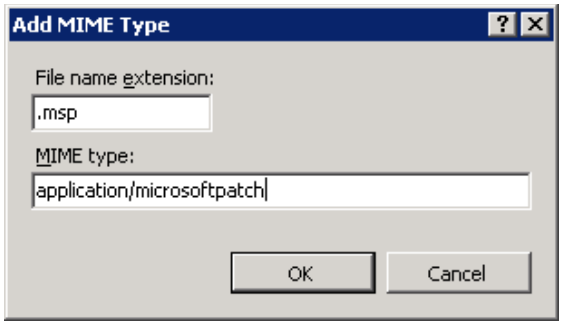
6 In the **Default Web Site Home** pane, under **IIS**, double-click **MIME Types**.



7 On the **Actions** list in the right pane, click **Add**.

8 In the **File name extension** box, type **.msp**.

9 In the **MIME Type** box, type **application/microsoftpatch**.

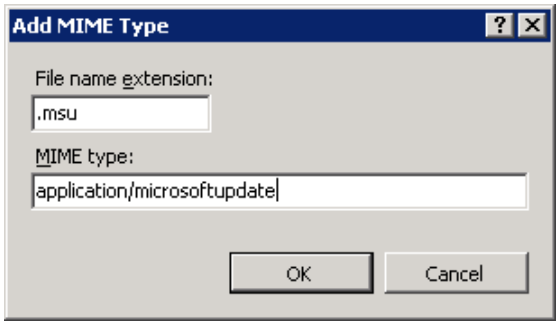


10 Click **OK**.

11 On the **Actions** list in the right pane, click **Add**.

12 In the **File name extension** box, type **.msu**.

13 In the **MIME Type** box, type **application/microsoftupdate**.

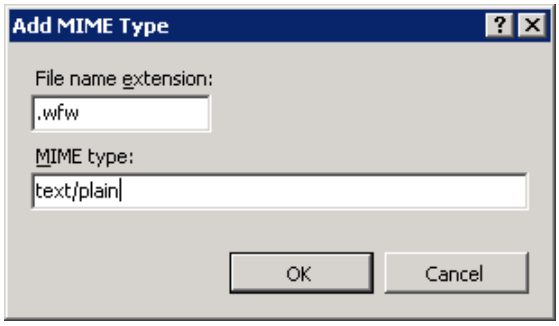


14 Click **OK**.

15 On the **Actions** list in the right pane, click **Add**.

16 In the **File name extension** box, type **.wfw**.

17 In the **MIME Type** box, type **text/plain**.



18 Click **OK**.

19 Close the **Computer Management** window.

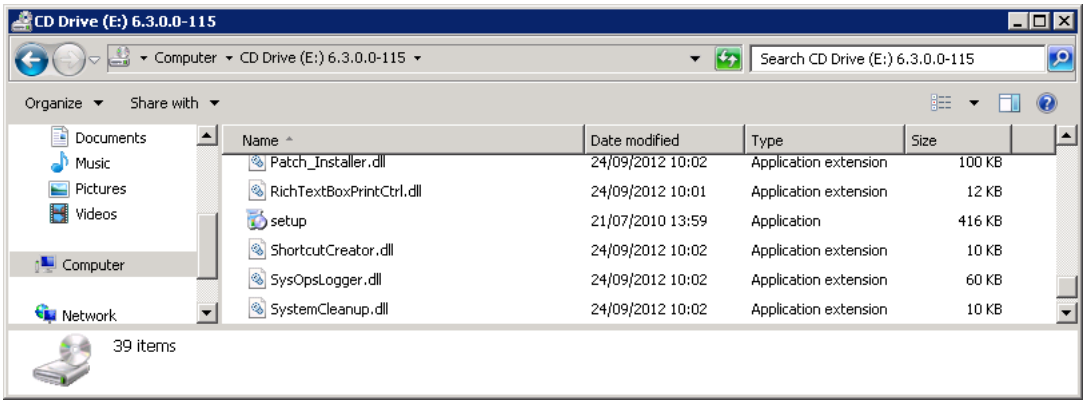
--End--

Installing the Voice and Multimedia Contact Server with Avaya Media Server software

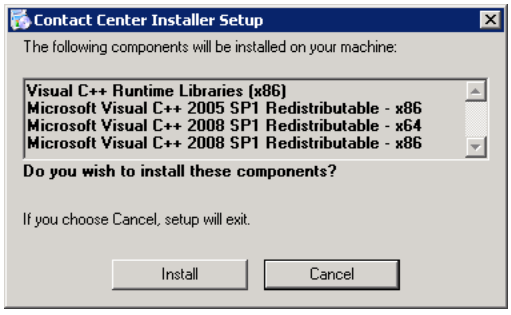
Install the Contact Center Voice and Multimedia Contact Server software and enable your contact center to route contacts to the agents that can answer the call with the correct skills.

Procedure steps

Step	Action
1	Log on to the server, using an Administrator account.
2	Insert the Contact Center DVD into the DVD drive of your server.

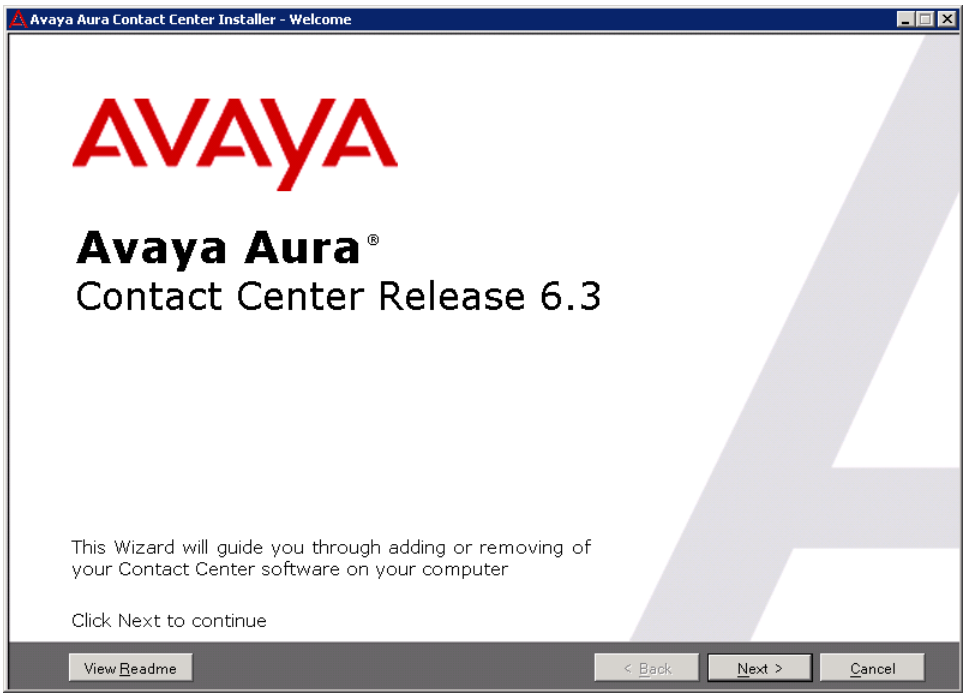


3	If the installation does not automatically start, double-click **Setup.exe**.
4	Click **Install** to install the Visual C++ runtime libraries on the server.



If you are prompted to restart the server, click **Yes** and repeat step 3.

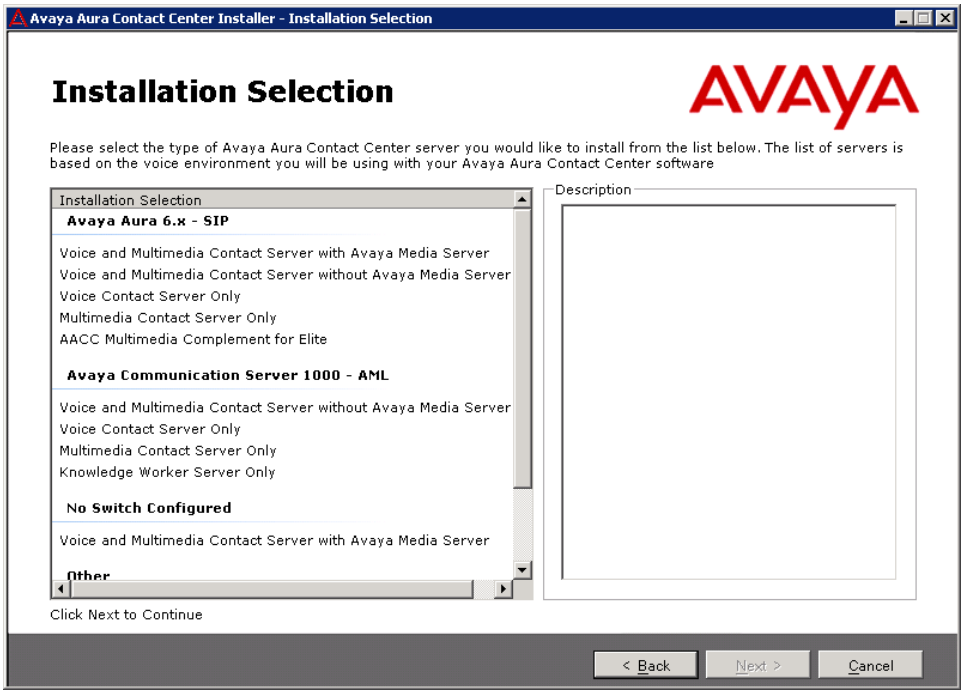
5	On the **Welcome** window, click **Next**.



6 On the **License Agreement** window, read the terms of the agreement.

7 Click **I Accept the Terms of the End-User License Agreement**.

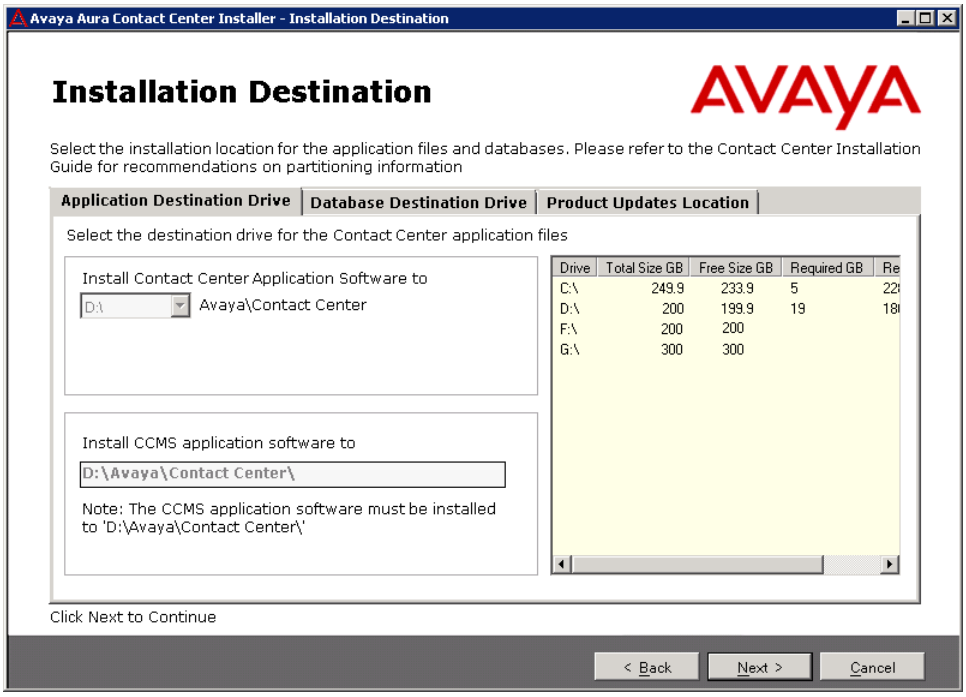
8 Click **Next**.


Avaya Aura Contact Center Installer - Installation Selection
Installation Selection
AVAYA
Please select the type of Avaya Aura Contact Center server you would like to install from the list below. The list of servers is based on the voice environment you will be using with your Avaya Aura Contact Center software
Installation Selection
Avaya Aura 6.x - SIP
Voice and Multimedia Contact Server with Avaya Media Server
Voice and Multimedia Contact Server without Avaya Media Server
Voice Contact Server Only
Multimedia Contact Server Only
AACC Multimedia Complement for Elite
Avaya Communication Server 1000 - AML
Voice and Multimedia Contact Server without Avaya Media Server
Voice Contact Server Only
Multimedia Contact Server Only
Knowledge Worker Server Only
No Switch Configured
Voice and Multimedia Contact Server with Avaya Media Server
Other
Description
Click Next to Continue
< Back
Next >
Cancel

9 On the **Installation Selection** window, under **Avaya Aura 6.x - SIP**, select **Voice and Multimedia Contact Server with Avaya Media Server**.

10 Click **Next**.

11 On the **Installation Destination** window, on the **Application Destination Drive** tab, from the **Install Contact Center Application Software to** list, select **D:**.

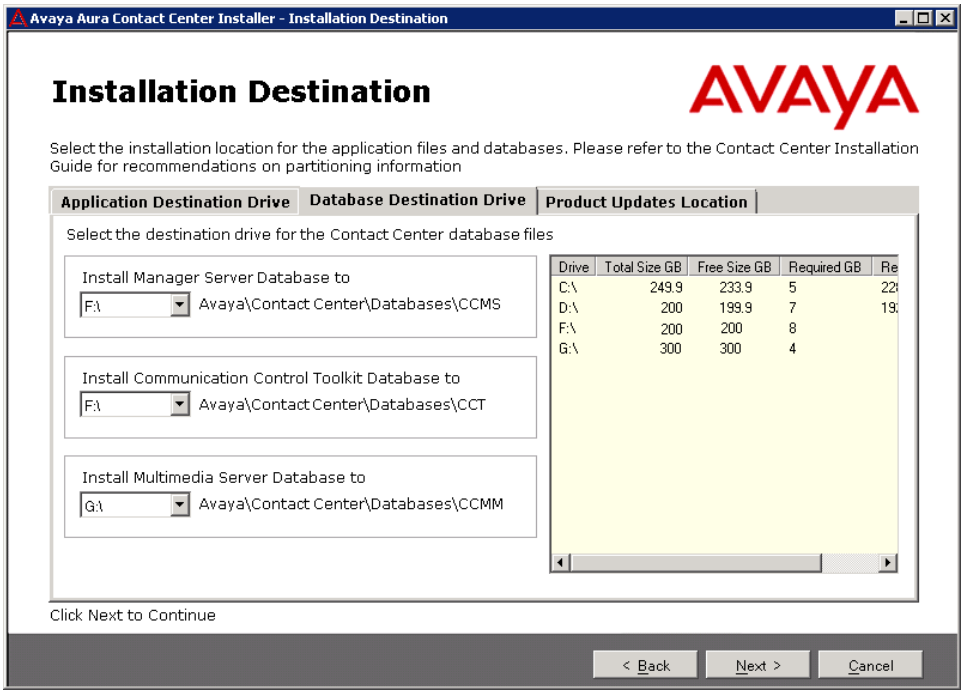


12 Click the **Database Destination Drive** tab.

13 From the **Install Manager Server Database to list**, select the drive for the Contact Center Manager Server database. select **F:**.

14 From the **Install Communication Control Toolkit Database to** list, select **F:**.

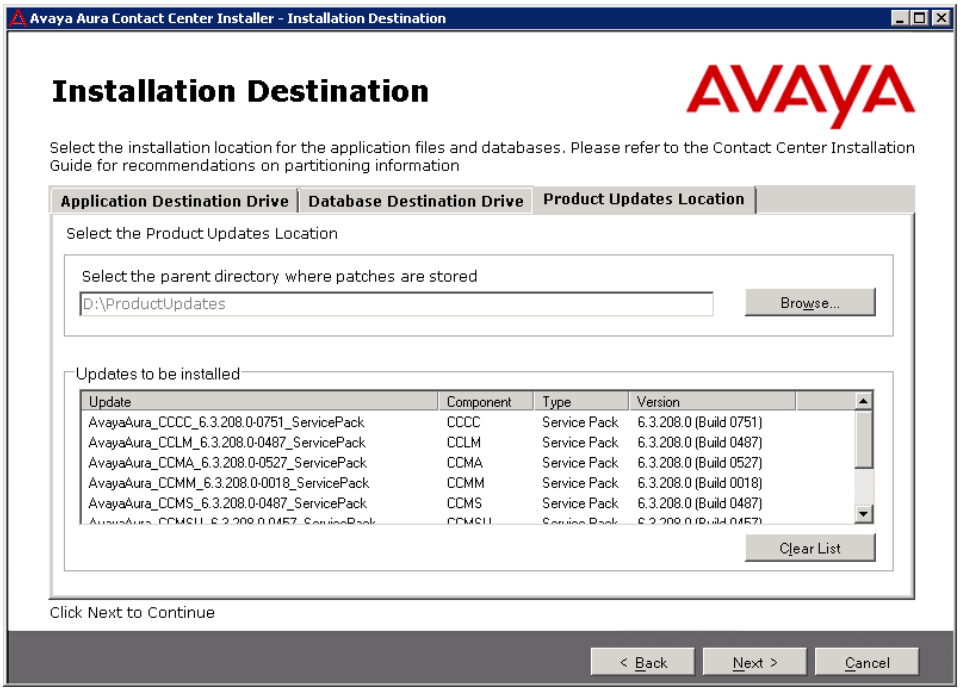
15 From the **Install Multimedia Server Database to** list, select **G:**.



16 Click the **Product Updates Location** tab.

17 Under **Select the parent directory where patches are stored**, click **Browse**.

18 Select the **D:\ProductUpdates** folder.

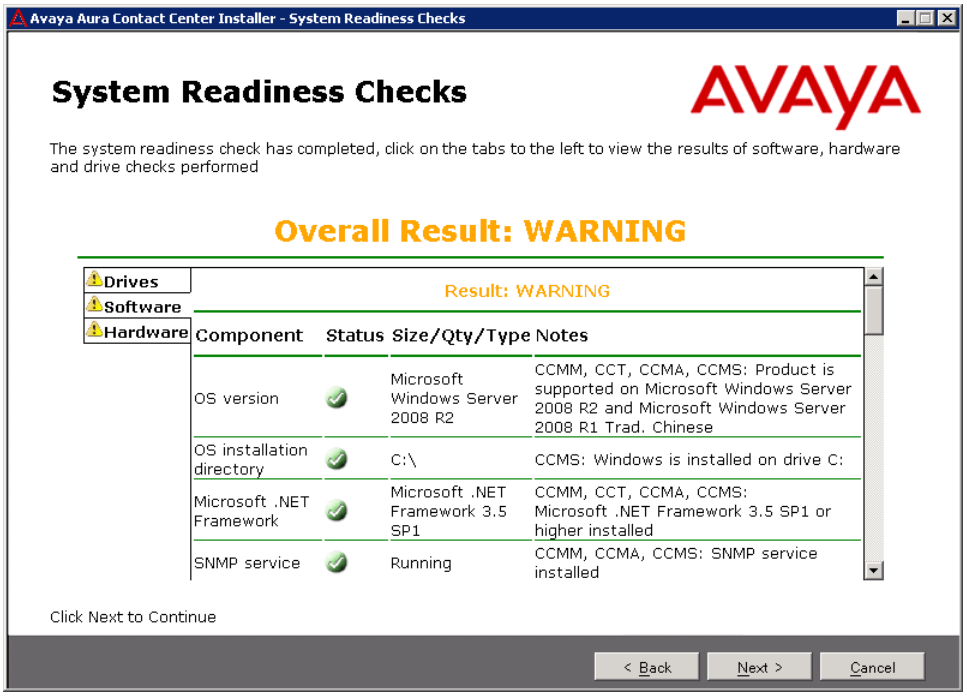


19 Click **Next**.

The System Readiness Check runs on the server.

20 If you have followed the previous instructions in this guide, the **System Readiness Checks** returns a **Pass**.

You can ignore warnings if you understand the potential impact to the operation of the contact center and decide it is not applicable.



21 Click **Next**.

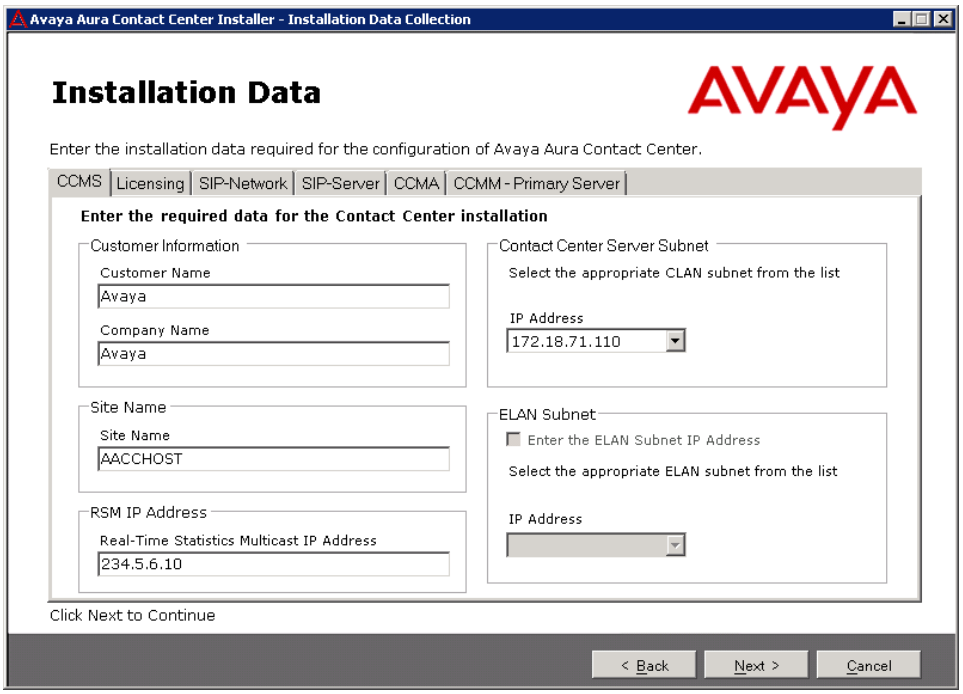
22 On the **Installation Data** window, select the **CCMS** tab. Complete the fields as follows:

Customer Name — Type the name of the contact center company, for example Avaya.

Company Name — Type the name of the contact center company, for example Avaya.

Site Name — Type the name of the site, for example AACCHOST. Do not enter the server name here, use a unique site name. The site name must not contain spaces or nonalphabetical characters except hyphen (-) and underscore (_). The first character must be a letter. The site name can consist of 6 to 15 characters.

Contact Center Server Subnet IP Address — Select the Voice and Multimedia Contact Server with Avaya Media Server IP address. For example, select 172.18.71.110.



23 Select the **Licensing** tab.

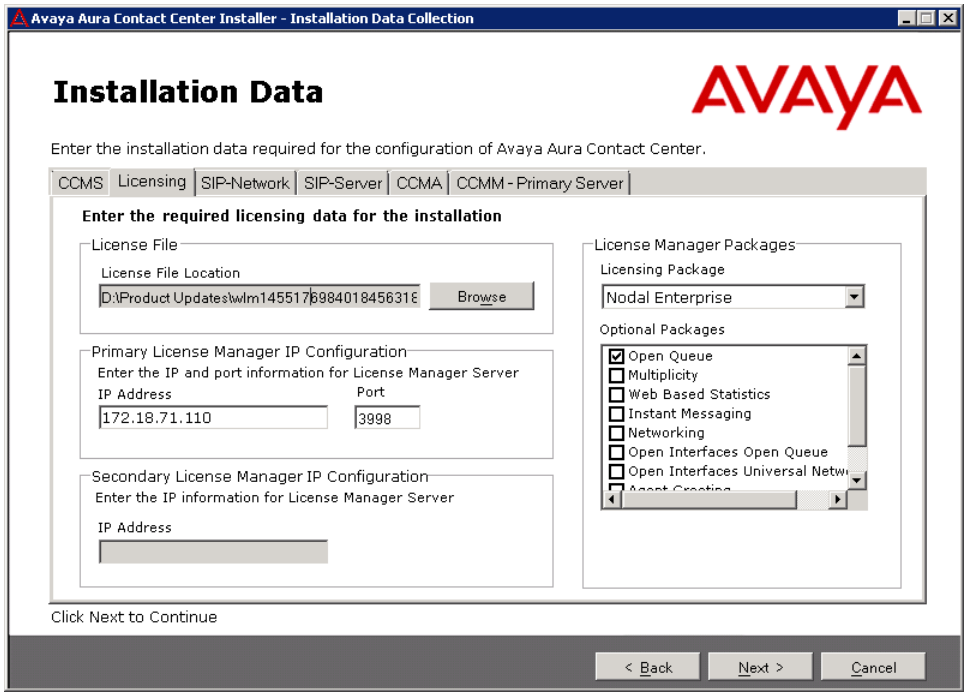
24 Complete the **Licensing** tab fields as follows:

License File Location — Use the **Browse** button to find and select the license file that you downloaded to the server. This sample solution uses a WebLM license file obtained from the Avaya Product Licensing and Delivery System (PLDS).

IP Address — Type the IP address of the license server. For example, type 172.18.71.110.

CCMS Package list — Select **Nodal Enterprise**.

Optional Packages — Select **Open Queue** as required.

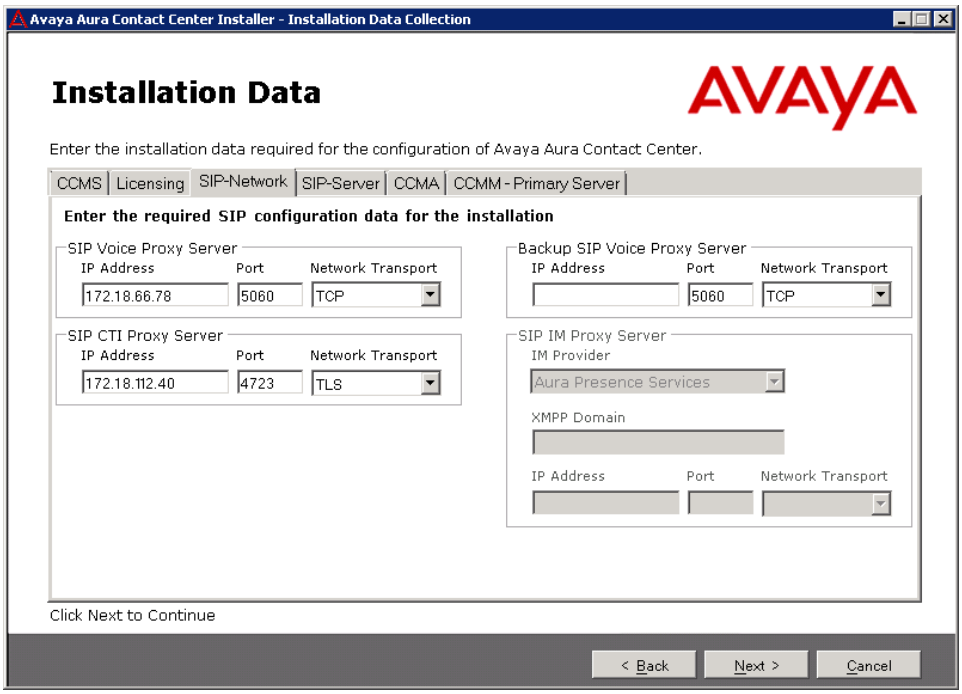


25 Select the **SIP-Network** tab.

26 Complete the **SIP-Network** tab fields as follows:

SIP Voice Proxy Server - IP Address — Type the IP address of the Session Manager SIP entity. For example, type 172.18.66.78.

SIP CTI Proxy Server - IP Address — Type the IP address of the Application Enablement Server. For example, type 172.18.112.40.



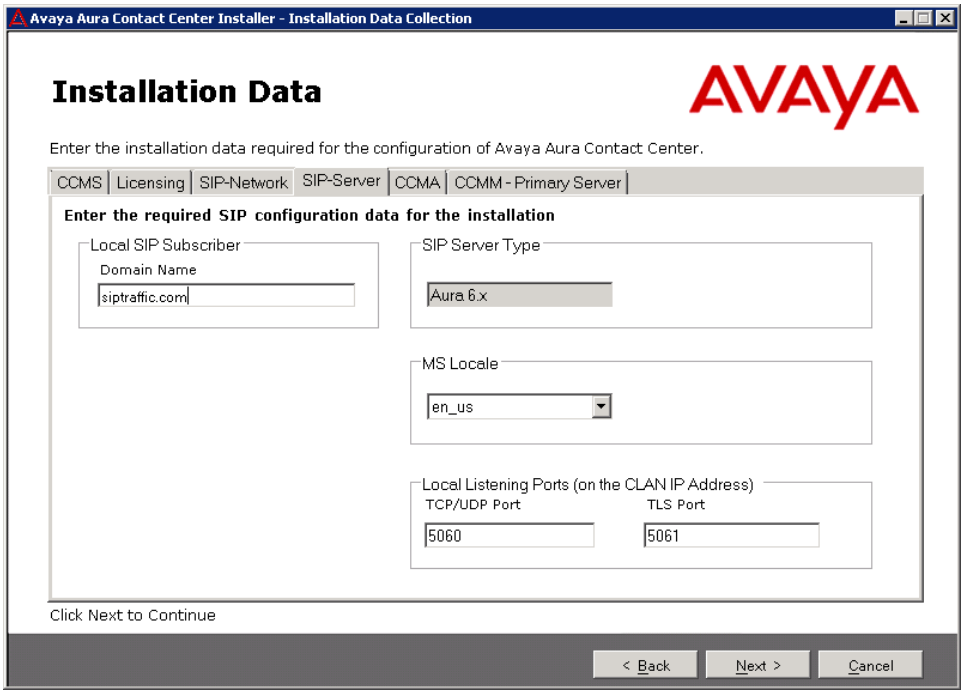
27 Select the **SIP-Server** tab.

28 Complete the **SIP-Server** tab fields as follows:

Local SIP Subscriber - Domain Name — Type the SIP domain name. For example, type siptraffic.com.

MS Locale — Select **en_us**.

For the remaining boxes and lists, accept the defaults.



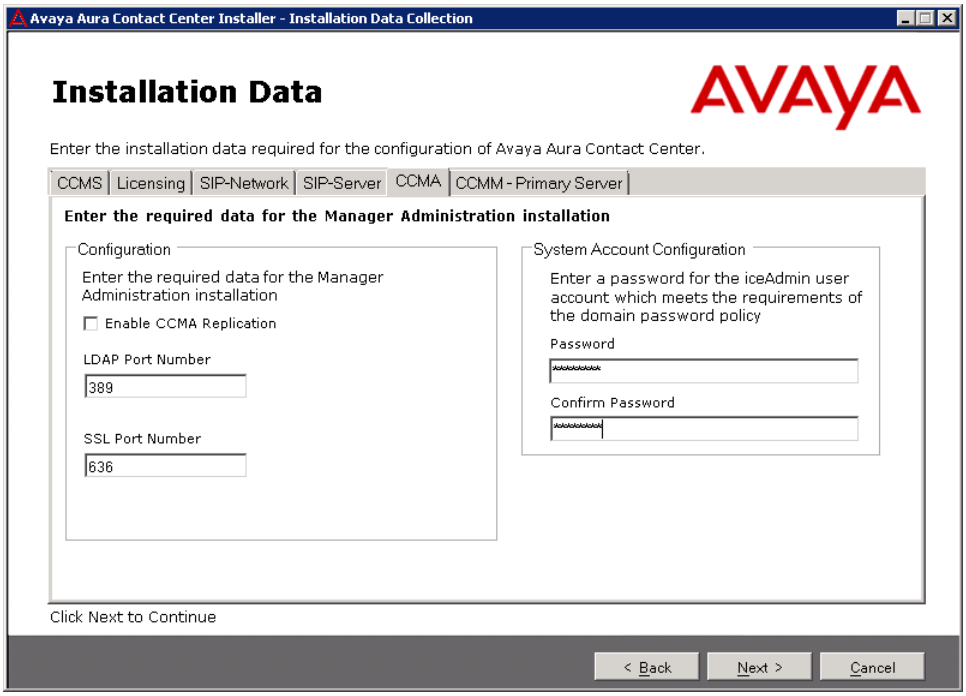
29 Select the **CCMA** tab.

30 Complete the **CCMA** tab fields as follows:

Configuration - Enable CCMA Replication — **Attention!**: leave this check box clear. You select this option only on the standby server.

System Account Configuration - Password — Type the password for the CCMA System Account (iceAdmin). Enter a complex password which meets the requirements of your domain policy.

System Account Configuration - Confirm Password — Re-type the password for the CCMA System Account (iceAdmin). Enter a complex password which meets the requirements of your domain policy.



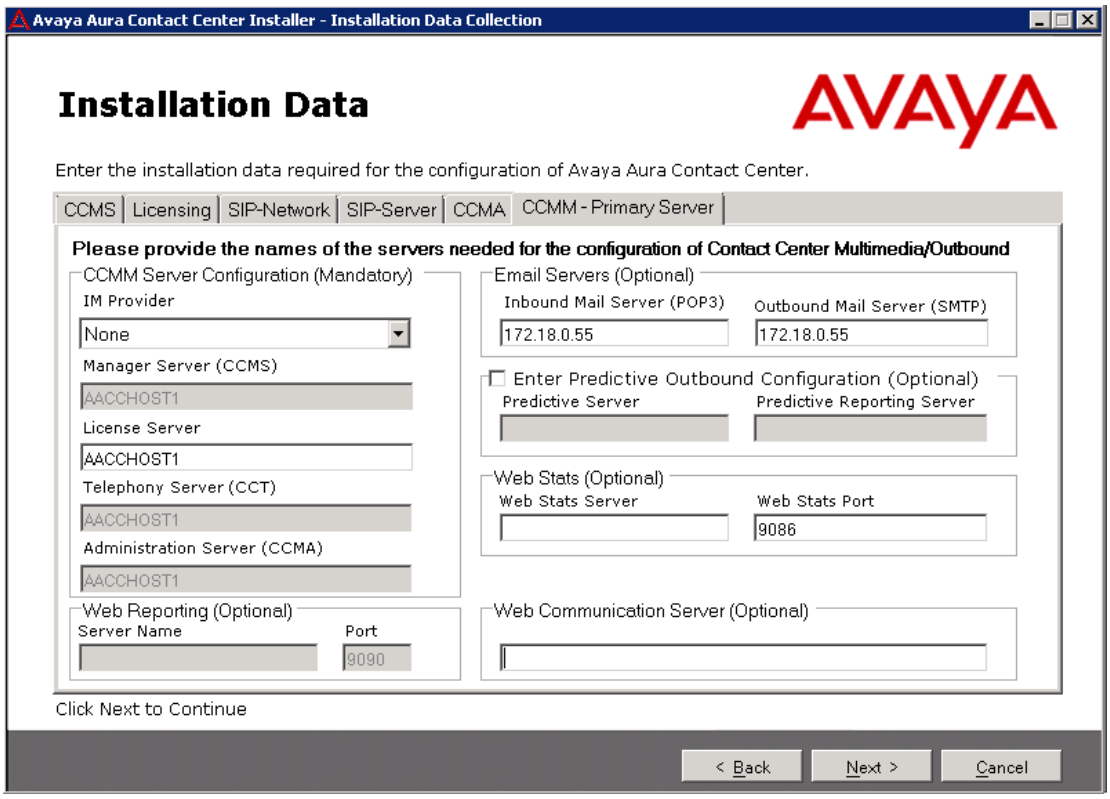
31 Select the **CCMM** tab, and configure the Contact Center Multimedia details.

32 From the **IM Provider** list, select either None, Microsoft OCS or Aura Presence Services. IM and presence features are supported for Avaya Aura® Presence Services server and Microsoft Office Communications Server. Instant Messaging is supported only in SIP-enabled contact center solutions.

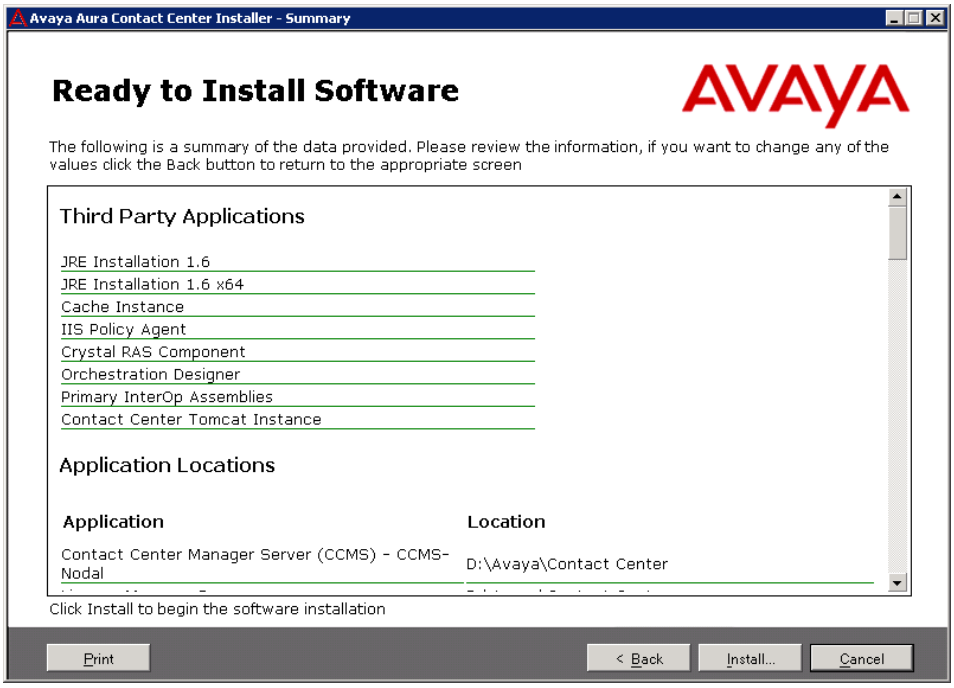
33 In the **License Server** box, type the name of the server on which the Contact Center License Manager software is installed. For example, type AACCHOST1.

34 In the **Inbound Mail Server (POP3)** box, type the name or IP address of the server on which email messages are received in your network. For example, type 172.18.0.55.

35 In the **Outbound Mail Server (SMTP)** box, type the name or IP address of the server from on which email messages are sent. Your inbound and outbound mail servers can have the same name. For example, type 172.18.0.55.



36 Click **Next**.



37 On the **Summary** window, review and verify the information.

38 Click **Install**.

39 After the installation is complete, click **Finish**.

40 Click **Yes** to restart the server.

--End--

Installing Voice and Multimedia Contact Server software patches

Install the most recent Voice and Multimedia Contact Server software service patches to ensure that you have the most current development updates.

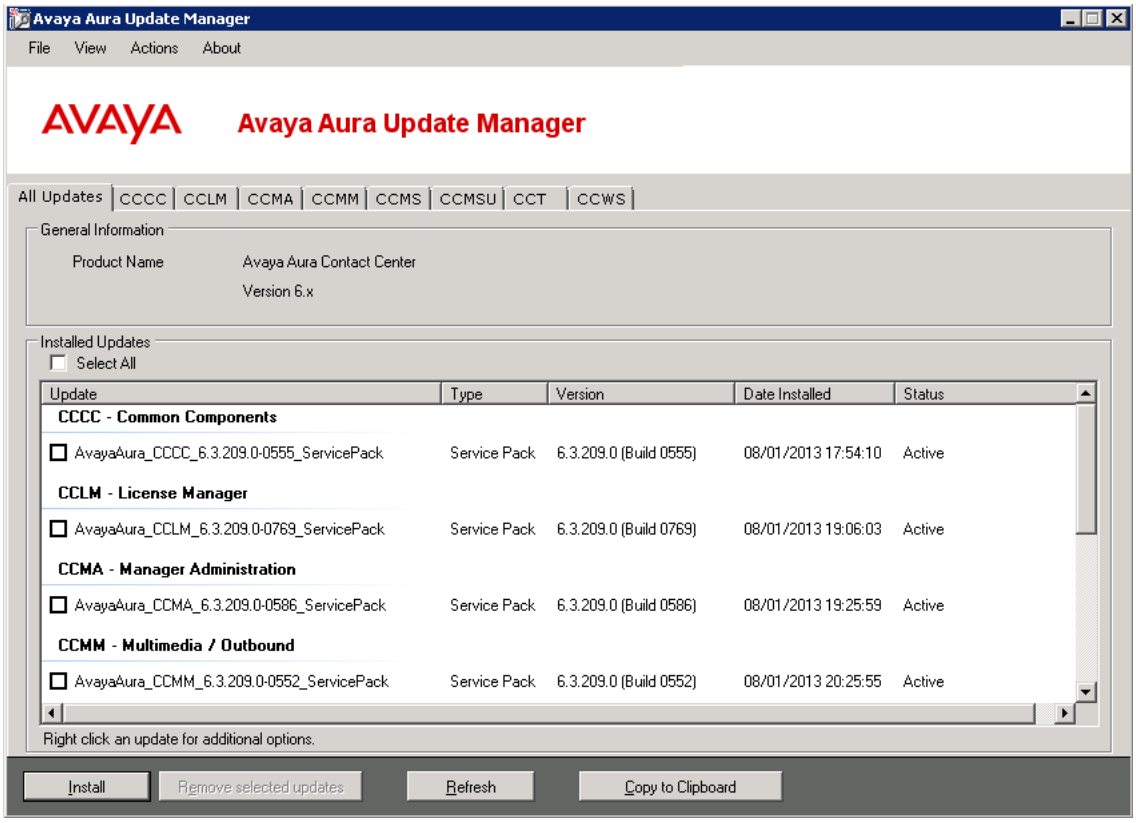
During a patch installation, all System Management and Monitoring Component (SMMC) services and the SMMC System Tray application stop to allow Contact Center files to be patched. After patching the server, if the patch does not require a server reboot, you must start the SMMC applications manually.

Prerequisites

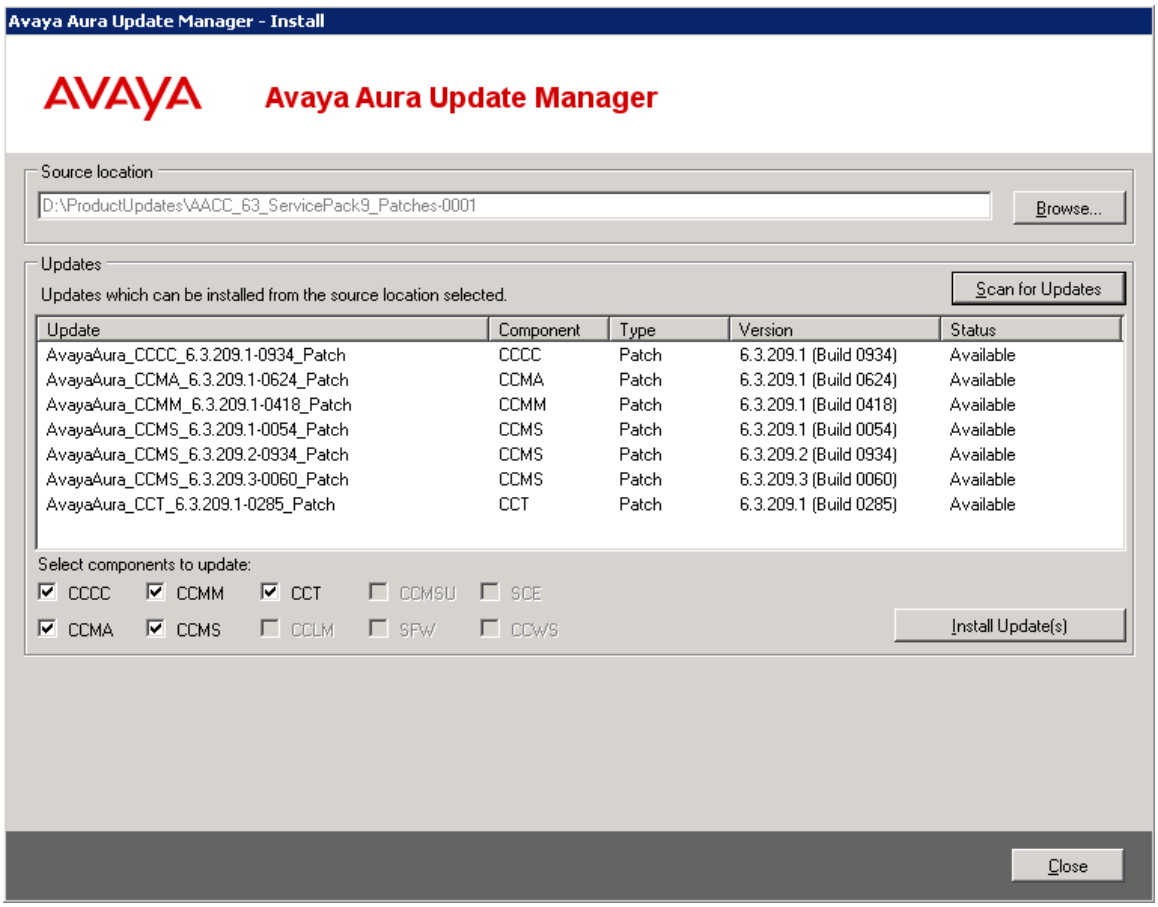
- Download the most recent Avaya Aura® Contact Center patches.

Procedure steps

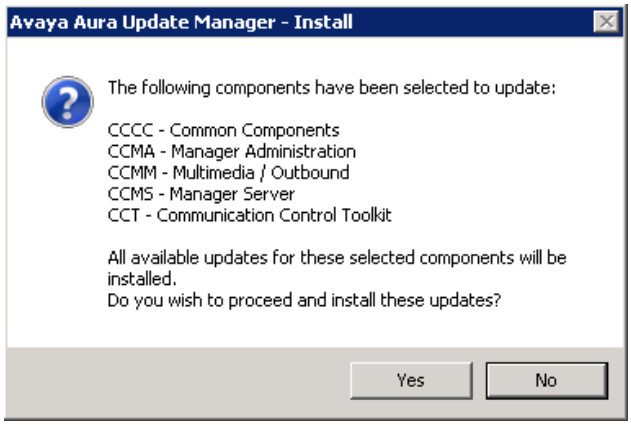
Step	Action
1	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Common Utilities**, **Contact Center Patch Manager**.



2	Click **Install**.
3	Click **Browse** and navigate to the folder where you have downloaded the server packs.
4	Click **Scan for Updates**. *The Contact Center Updates section displays the available patches.*
5	Select the appropriate patch.



6 Click **Install Update(s)**.



7 Click **Yes**.

The Patch Manager installs the patch and displays a confirmation message.

8 If prompted to reboot your server, click **Close** and restart your server.

9 If the Voice and Multimedia Contact Server is not restarted, click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Common Utilities**, **SMMC SystemTray**.

10 On the Windows system tray, right-click the SMMC system tray icon, and select **Start SMMC**.

--End--

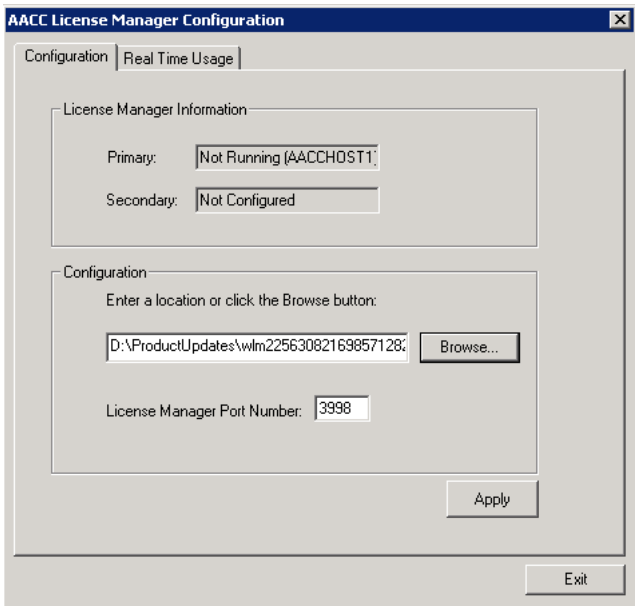
Configuring the WebLM license file

Configure Contact Center License Manager to use a WebLM file. Then restart the Contact Center Tomcat Instance on the Contact Center License Manager server to commission the WebLM license file for the first time.

When you install Contact Center License Manager, an instance of Apache Tomcat Server is also installed on the same server. The default port number for Apache Tomcat is 8081. If you need to change the port number to avoid conflicts with third-party software, see your Apache Tomcat documentation.

Procedure steps

Step	Action
1	Log on to the Voice and Multimedia Contact Server.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **License Manager**, **Configuration**.
3	On the **LM Config** dialog box, click **OK**.
4	On the Configuration tab, click **Browse**.
5	Navigate the file system and locate the WebLM license file.
6	Click **Open**.



7 Click **Apply**.

An LM dialog box appears, which you must ignore for now.

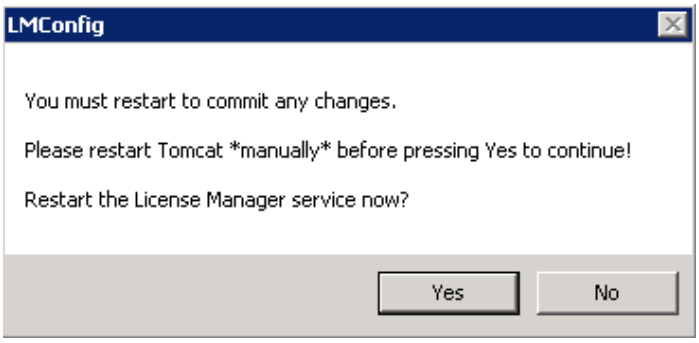
8 On the Start menu, choose **All Programs** > **Administrative Tools** > **Services**.

9 Right-click the **Contact Center Tomcat Instance** service, and click **Stop**.

10 Right-click the **Contact Center Tomcat Instance** service, and click **Start**.

11 Close the services window.

12 On the LM dialog box, click **Yes** to restart the Contact Center License Manager services.



13 Click **OK** to close the window.

14 Click **Exit**.

--End--

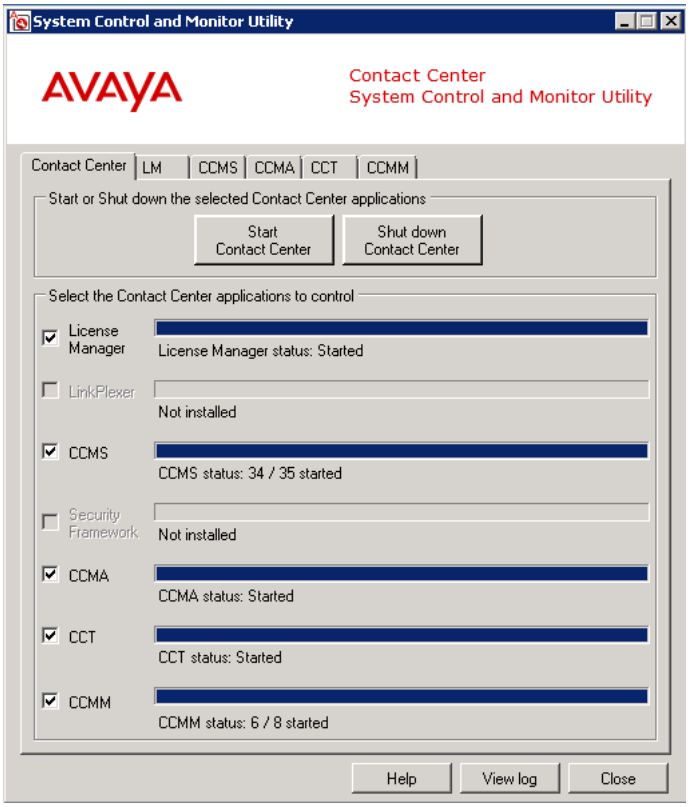
Confirming that the Contact Center services start

Confirm that all appropriate Contact Center services start on the Contact Center server.

Use the System Control and Monitor Utility to start and stop all Contact Center applications including the license manager. The System Control and Monitor Utility can also start, stop, or monitor the services.

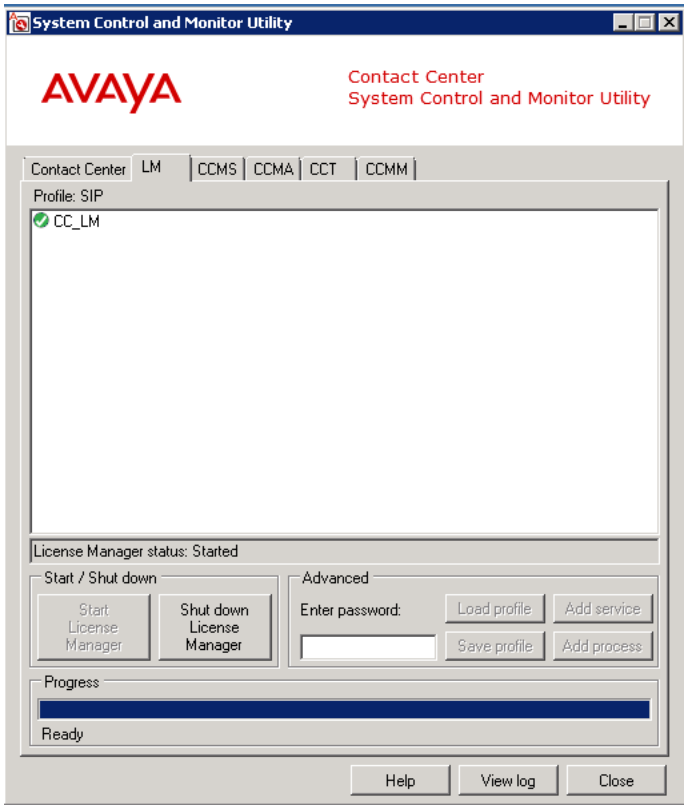
Procedure steps

Step	Action
1	Log on to the Voice and Multimedia Contact Server.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Common Utilities**, **System Control and Monitor Utility**.
3	Click the **Contact Center** tab.
4	Select the applications to start on the current server by selecting the application name check boxes.



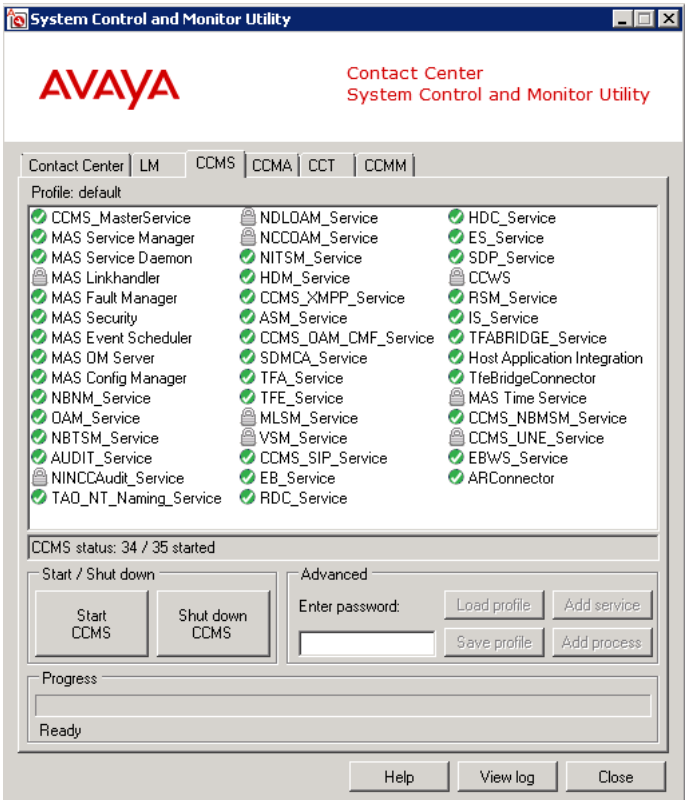
5	Click **Start Contact Center**.
6	Click **OK**.
7	Click the **LM** tab.

8 Ensure that all services in the **Profile** box have a green circle next to them.



9 Click the **CCMS** tab.

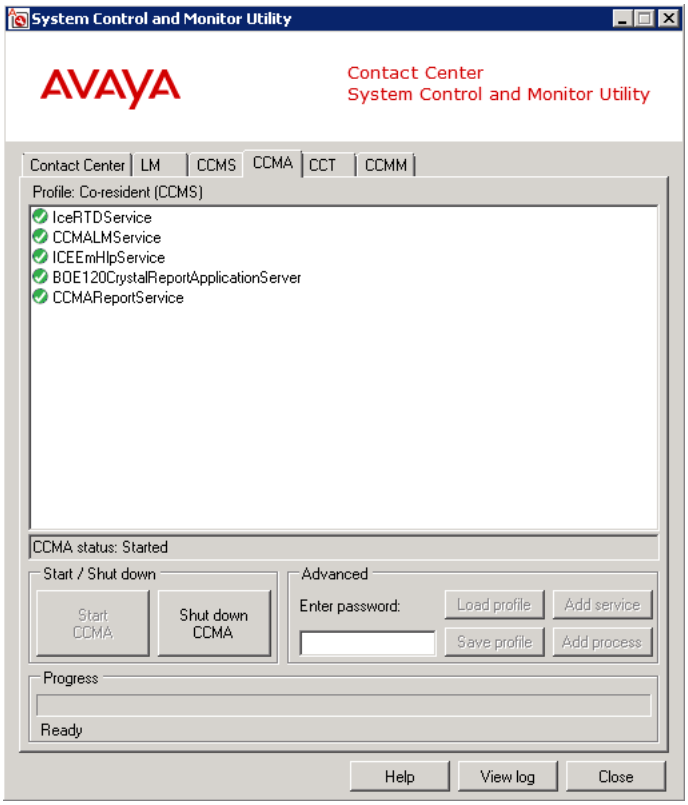
10 Ensure that the main CCMS services in the **Profile** box have a green circle next to them. CCMS services with a padlock icon are not licensed and therefore do not start.



11 If some of the services are not started, click **Start CCMS**.

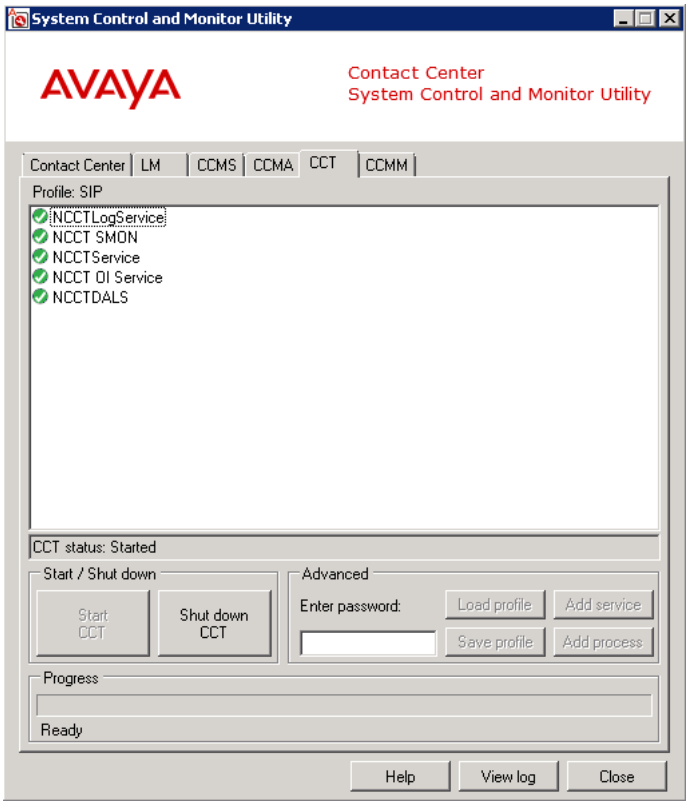
12 Click the **CCMA** tab.

13 Ensure that all services in the **Profile** box have a green circle next to them.



14 Select the **CCT** tab.

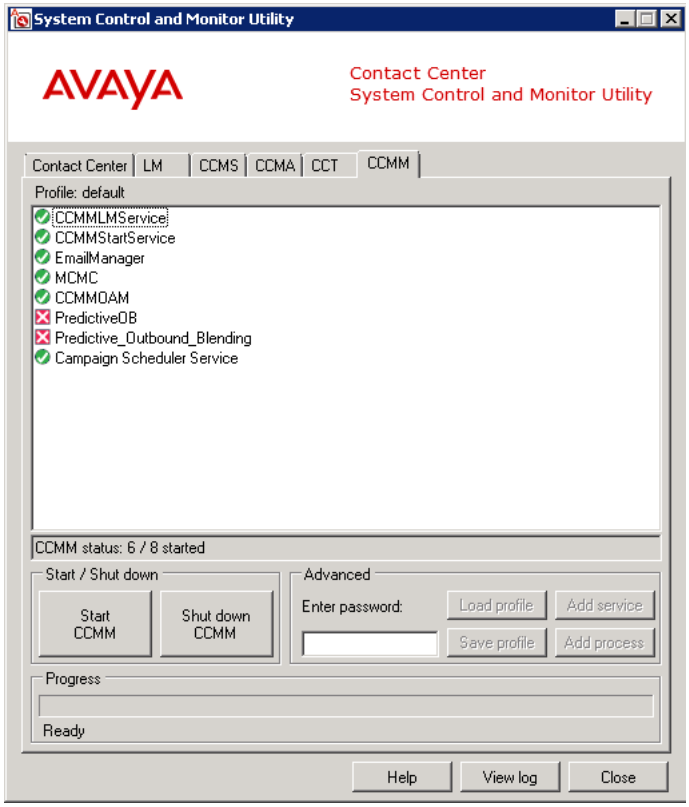
15 Confirm that the Communication Control Toolkit services are running.



16 If a Communication Control Toolkit service is not running, click **Start CCT**.

17 Select the **CCMM** tab.

18 Confirm that the Contact Center Multimedia services are running. Predictive Outbound Blending is not licensed or enabled on this server.



19 If a Contact Center Multimedia service is not running, click **Start CCMM**.

20 Click **Close**.

--End--

Updating the CCMA Administration user password

Update the CCMA Administration account password on your Contact Center Manager Administration server using the iceAdmin Password Change utility.

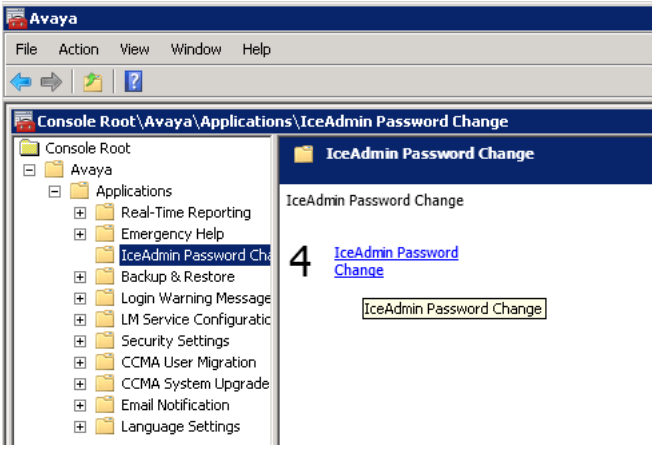
The CCMA Administration account is an administrator account for the Contact Center Manager Administration server.

Procedure steps

Step	Action
1	Log on to the Voice and Multimedia Contact Server.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Manager Administration**, **Configuration**.

3 In the **Avaya Applications Configuration** window, in the left pane, expand **Avaya**, **Applications**, **iceAdmin Password Change**.

4 In the right pane, click the **iceAdmin Password Change** icon.



5 In the **Old Password** box, type the password for the CCMA Admin user account that you configured at install time.

6 In the **New Password** box, type a password for the CCMA Admin user account. Enter a complex password which meets the requirements of your domain policy.

7 In the **Confirm Password** box, type the password again.

8 Click **OK**.

--End--

Configuring Internet Explorer on the Voice and Multimedia Contact Server

Configure Internet Explorer on the Voice and Multimedia Contact Server to access Contact Center Manager Administration for the first time.

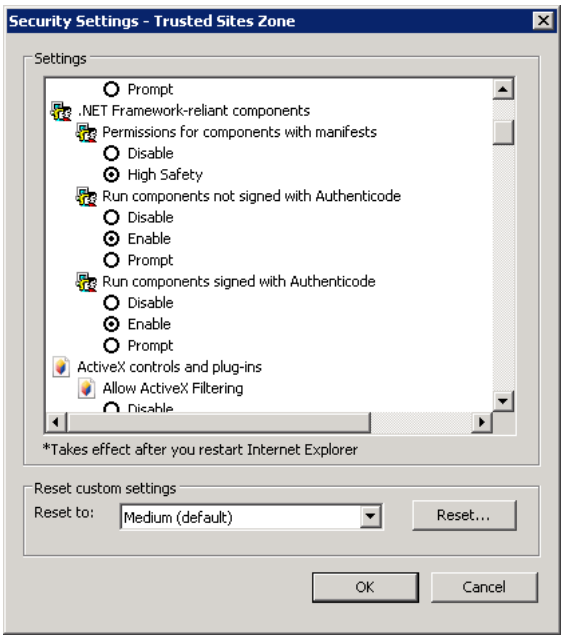
Install Microsoft Internet Explorer 7.0, 8.0 or 9.0 (32 bit version only). Contact Center Manager Administration supports only the 32 bit version of Microsoft Internet Explorer.

Procedure steps

Step	Action
1	On the Voice and Multimedia Contact Server, start Internet Explorer.
2	From the menu, select **Tools, Internet Options**.
3	In the **Internet Options** dialog box, click the **Security** tab.
4	Click the **Trusted Sites** icon.
5	Click **Custom Level**.

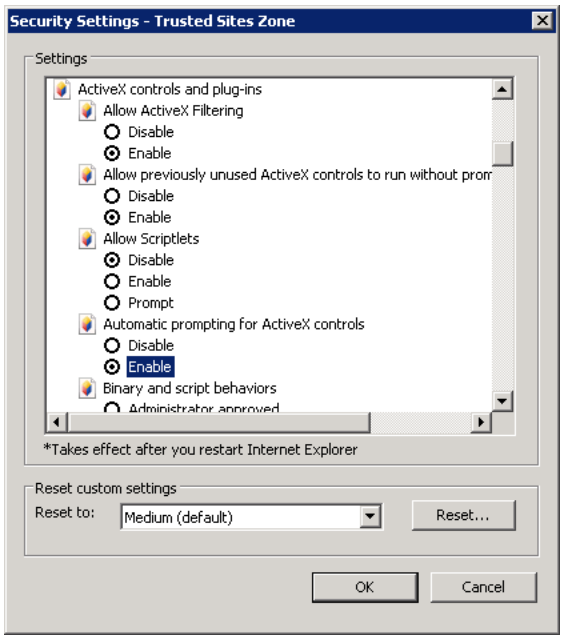
6 In the **Security Settings** dialog box for trusted sites, under the **.NET Framework-reliant components** heading, select **Enable** for the following:

- **Run components not signed with Authenticode**
- **Run components signed with Authenticode**



7 Under the **ActiveX controls and plug-ins** heading, select **Enable** for the following:

- **Automatic prompting for ActiveX controls**
- **Run ActiveX Controls and plug-ins**
- **Script ActiveX Controls marked safe for scripting**

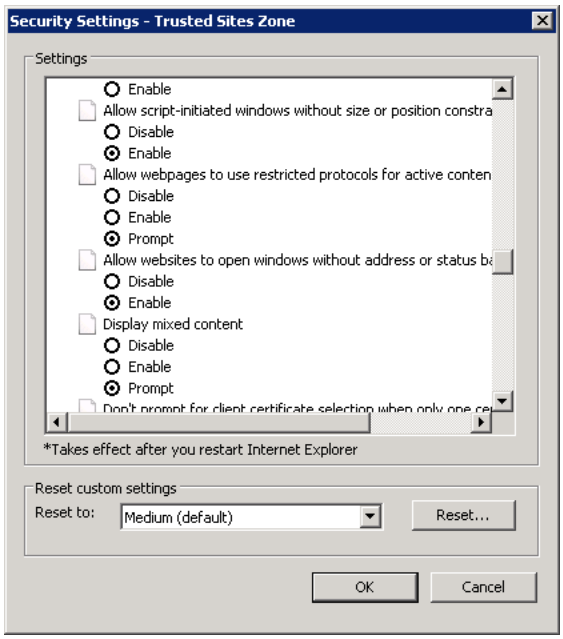


8 Under the **Downloads** heading, select **Enable** for the following:

- **Automatic prompting for file downloads**
- **File download**

9 Under the **Miscellaneous** heading, for **Allow script-initiated windows without size or position constraints**, select **Enable**.

10 Under the **Miscellaneous** heading, for **Allow websites to open windows without address or status bars**, select **Enable**.



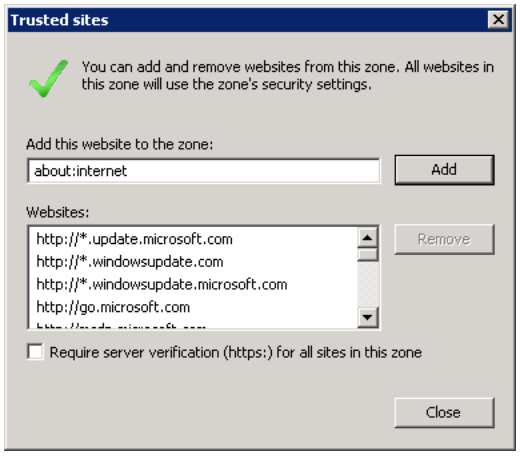
11 Click **OK**.

12 If you have enabled ActiveX options, when a message appears asking you to confirm your choice, click **Yes**.

13 Click the **Trusted Sites** icon.

14 Click **Sites**.

15 In the **Trusted sites** dialog box, clear the **Require server verification (https:) for all sites in this zone** check box.

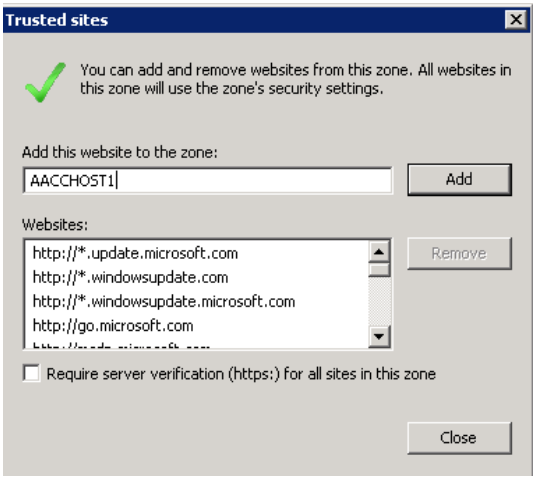


16 In the **Add this Web site to the zone** box, type the server name (not the IP address) for your Voice and Multimedia Contact Server.

OR

If you have used the fully qualified domain name when you installed the Voice and Multimedia Contact Server, in the **Add this Web site to the zone** box, type the fully qualified domain name.

17 Click **Add**.



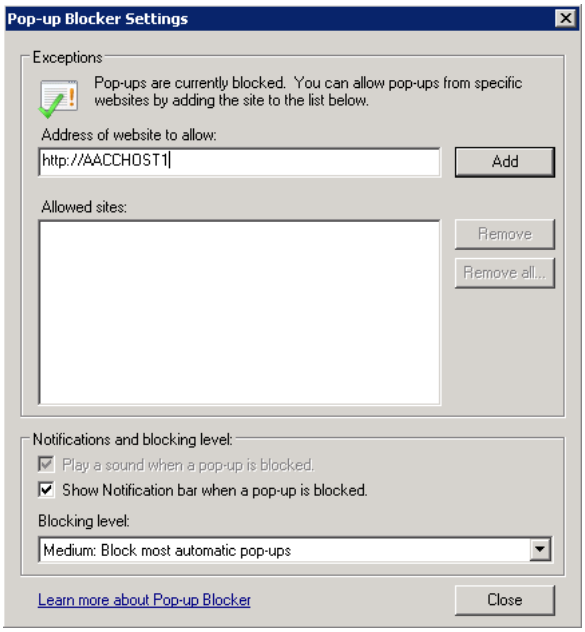
18 Click **Close** to return to the **Internet Options** dialog box.

19 Click the **Privacy** tab.

20 In the **Pop-up Blocker** section, select the **Turn on Pop-up Blocker** check box.

21 Click **Settings**.

22 In the **Pop-up Blocker Settings** dialog box, in the **Address of website to allow** box, type the Voice and Multimedia Contact Server URL, http://<AACCHOST1>/.

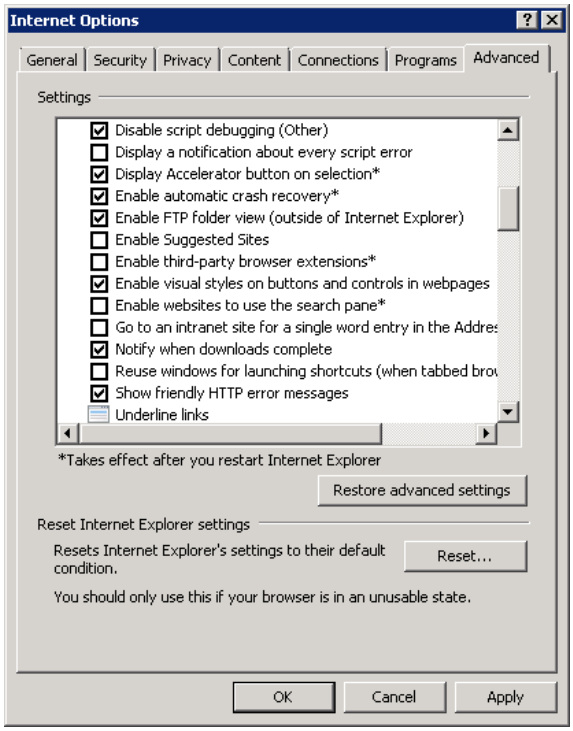


23 Click **Add**.

24 Click **Close**.

25 In the **Internet Options** dialog box, click the **Advanced** tab.

26 Under **Browsing**, clear the **Reuse windows for launching shortcuts** check box.



27 Click **Apply**.

28 Click **OK** to exit the **Internet Options** dialog box.

29 Restart Internet Explorer to activate your changes.

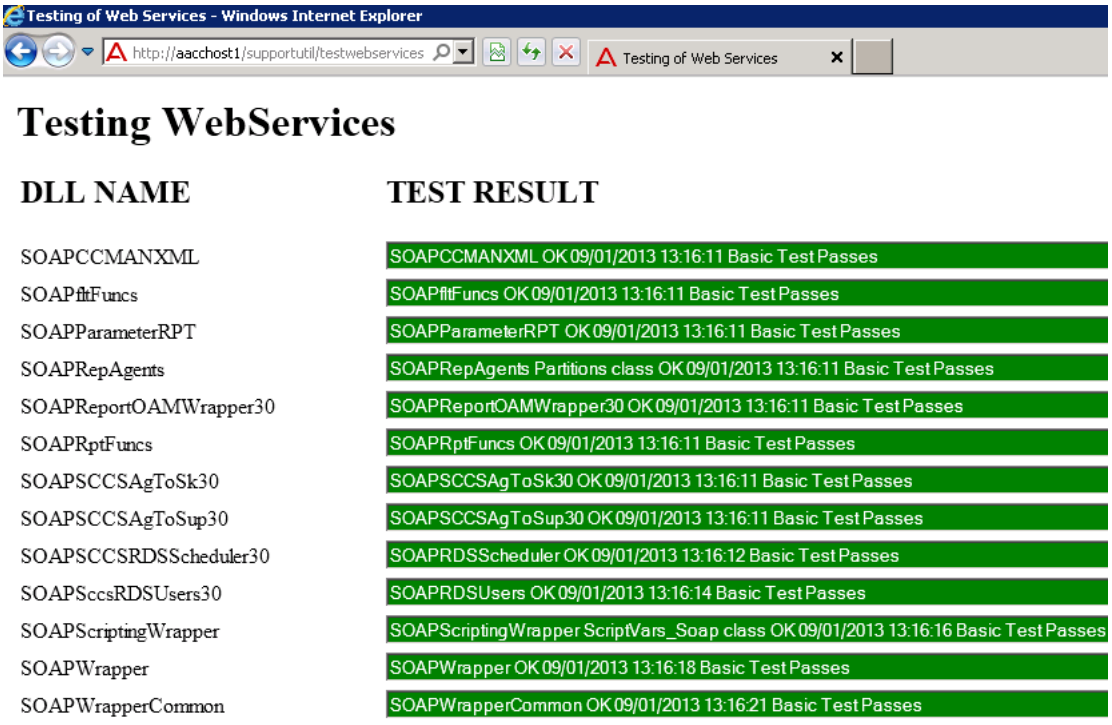
--End--

Verifying the Web Services

Verify the Web Services to ensure CCMA web services are running correctly.

Procedure steps

Step	Action
1	Start Internet Explorer.
2	Enter the following: http://<SERVER NAME>/supportutil/testwebservices.asp Where SERVER NAME is the name of the Voice and Multimedia Contact Server. For example, enter the following: http://AACCHOST1/supportutil/testwebservices.asp The web services that appear in green are running correctly.



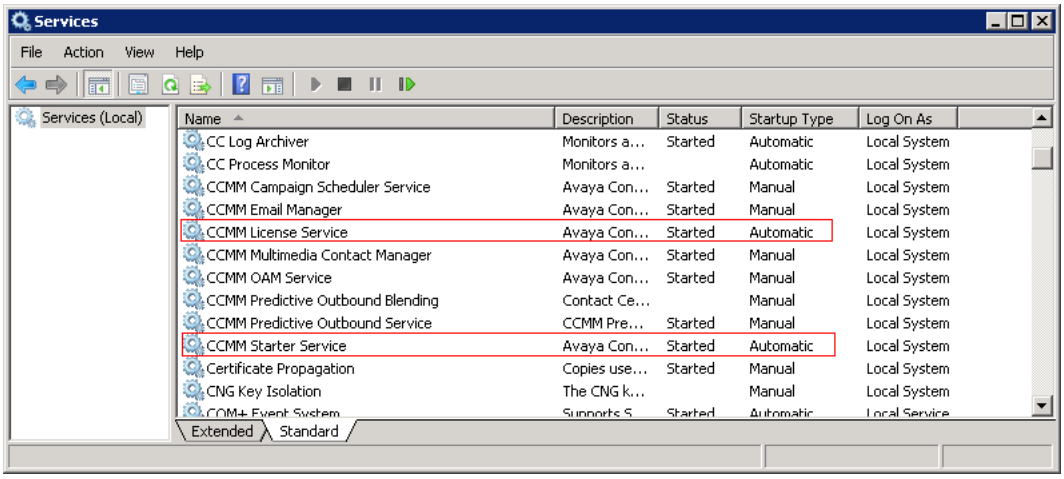
--End--

Verifying that Contact Center Multimedia services start

Verify that Contact Center Multimedia services start to ensure that contacts are routed immediately after the server restarts for any reason.

Procedure steps

Step	Action
1	On the Voice and Multimedia Contact Server, click **Start**, **Administrative Tools**, **Services**.
2	In the **Services** window, verify that the **CCMM License Service** status is **Started** and the startup type is **Automatic**.
3	In the Services window, verify that the **CCMM Starter Service** status is **Started** and the startup type is **Automatic**.



4	Verify that the following services started: • CCMM Multimedia Contact Manager • CCMM OAM service • CCMM Campaign Scheduler service • CCMM Email Manager
5	If any service did not start, in the **Services** window, right-click the service name, and click **Start**.

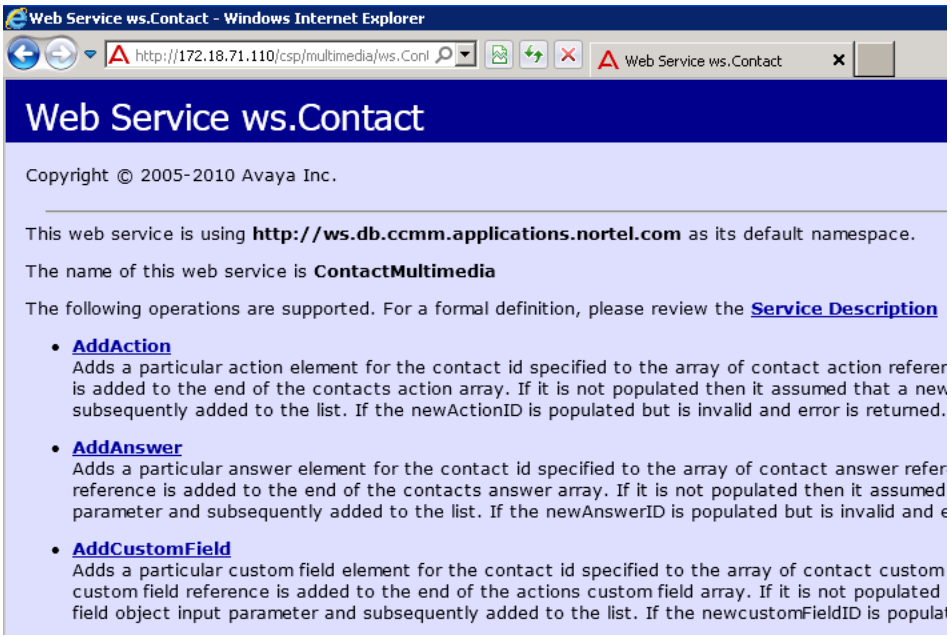
--End--

Verifying the Multimedia database installation

Verify that the Multimedia database is installed and configured correctly.

Procedure steps

Step	Action
1	On the Voice and Multimedia Contact Server, open Internet Explorer.
2	Enter the following: **http://172.18.71.110/csp/multimedia/ws.Contact.cls**



3	If a Web page does not appear, contact your Avaya technical support prime.

--End--

Scheduling Contact Center Manager Administration backups

Schedule Contact Center Manager Administration backups to a folder to create a snapshot of the preselected CCMA data files. You can create the folder on the same server or on another domain server.

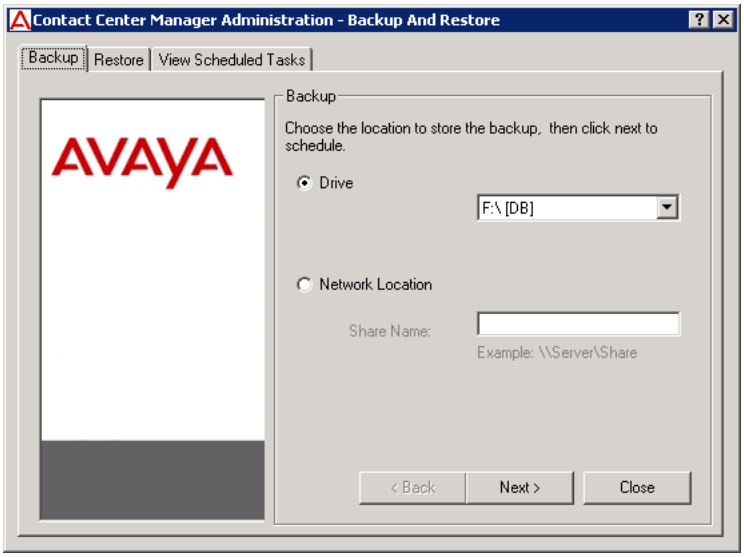
The Backup and Restore utility is automatically installed on the Voice and Multimedia Contact Server.

Prerequisites

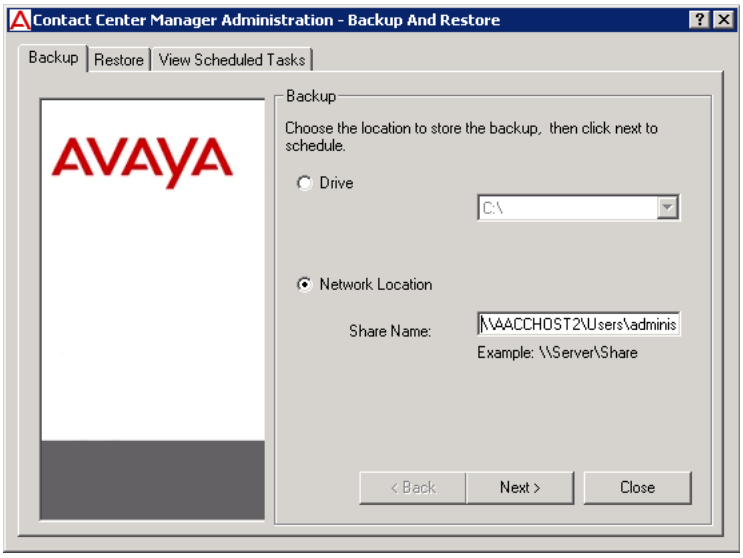
- On a backup server, create a shared folder to store the CCMA backup data.
- Ensure that you have write privileges on the server where you want to store the CCMA data you are backing up.
- Log on to the CCMA server with administrative privileges.

Procedure steps

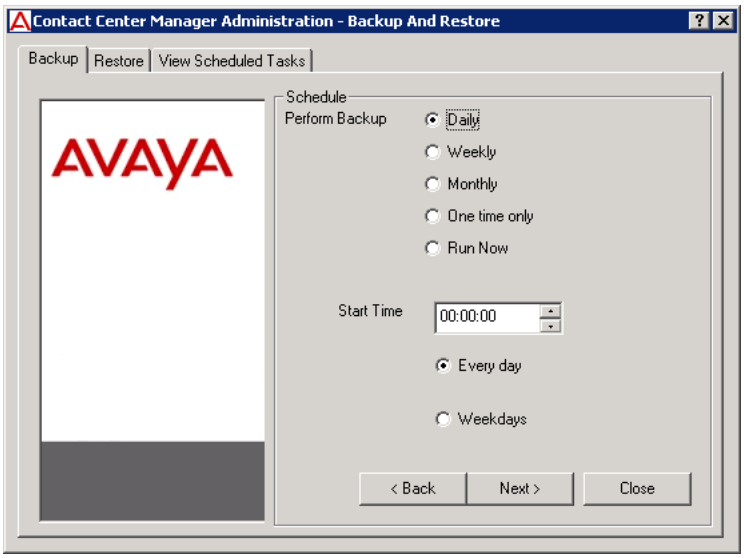
Step	Action
1	Log on to the Voice and Multimedia Contact Server.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Manager Administration**, **Configuration**.
3	In the left pane of the Configuration window, expand **Avaya**, **Applications**.
4	In the **Avaya Applications Configuration** window, select **Backup & Restore**.
5	In the right-hand pane, click **Backup & Restore**.
6	In the **Contact Center Manager Administration - Backup and Restore** utility, select the **Backup** tab.



7	In the **Backup** window, select **Network Location**.
8	In the **Share Name** box, specify the Network Location where you want to store the backup. For example, specify **\\AACCHOST2\Users\administrator\Desktop\DB_store**. This is a shared folder on the standby server.



9 Click **Next**.



10 On the **Schedule** page, select **Daily**.

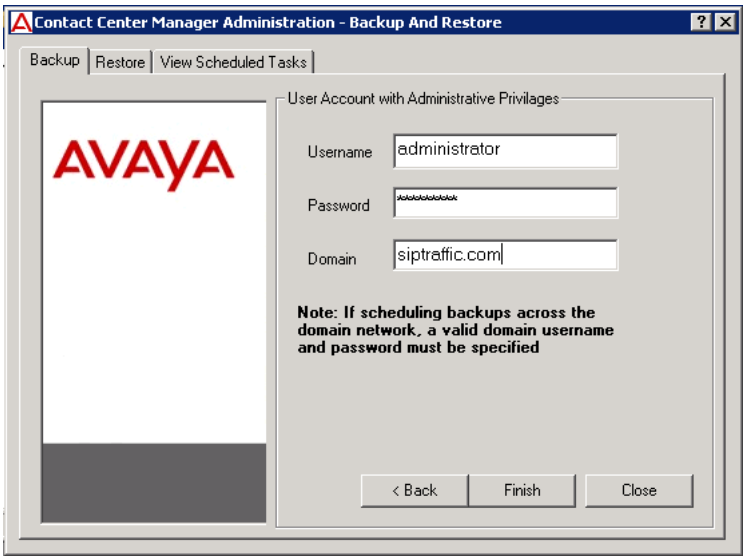
11 In the **Start Time** box, select a start time suitable for your solution.

12 Click **Next**.

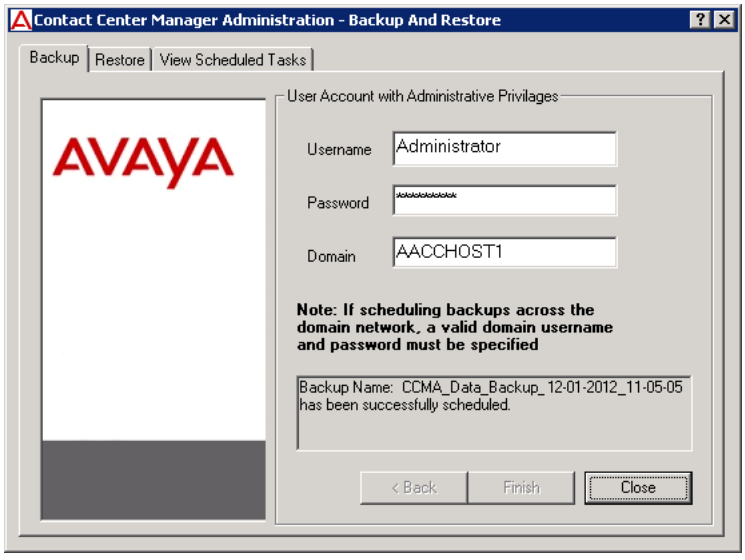
13 In the **Username** box on the **User Account with Administrative Privileges** page, type a valid Windows administrator name for the server on which you want to store the backup.

14 In the **Password** box, type the password for the specified Windows administrator.

15 If you selected a backup location on another server in a domain, type the domain in the **Domain** field. The default option is **this computer**.



16 Click **Finish**.



17 Click **Close**.

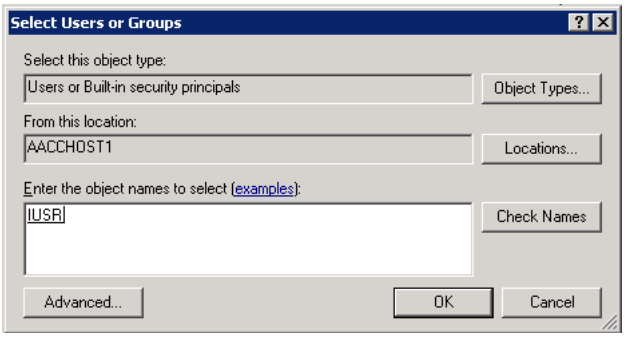
--End--

Providing local users with Log on as a service right

Provide local users with log on as a service right to ensure that administrators and the agents in your Contact Center have access to the Contact Center Agent Desktop application.

Procedure steps

Step	Action
1	Click **Start**, **Administrative Tools**, **Local Security Policy**.
2	Under **Security Settings**, in the left pane, double-click **Local Policies**.
3	In the left pane, click **User Rights Assignment**.
4	In the right pane, double-click **Log on as a service**.
5	Click **Add User or Group**.
6	Click **Locations**.
7	In the **Locations** dialog box, select the Voice and Multimedia Contact Server name from the list.
8	Click **OK**.
9	In the **Enter the object name to select** box, type **IUSR**.
10	Click **Check Names** to verify that the user name exists on the local computer.



11	Click **OK**.
12	Click **Apply** to save the changes.
13	Click **OK**.
14	Close the **Local Security Settings** window.

--End--

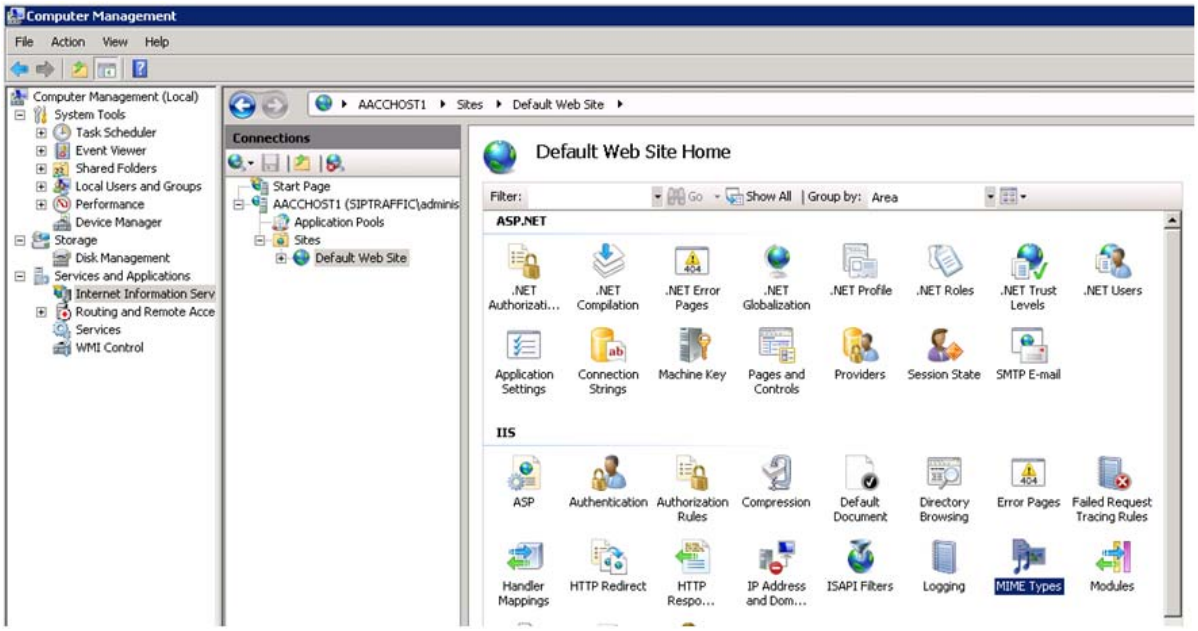
Configuring the MIME types

Configure the Multipurpose Internet Mail Extension (MIME) types to ensure that agents can access email message attachments.

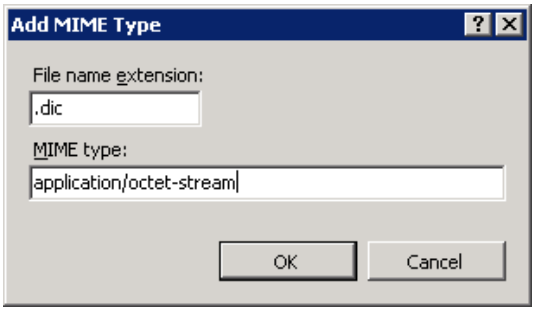
If any of these MIME types are already configured, skip the configuration steps for that MIME type.

Procedure steps

Step	Action
1	On the Voice and Multimedia Contact Server, click **Start**, **Administrative Tools**, **Computer Management**.
2	In the **Computer Management** dialog box, expand **Services and Applications**, **Internet Information Services (IIS) Manager**.
3	In the **Connections** pane, under the Host Server (AACCHOST1) name, select **Sites**.
4	Select **Default Web Site**.



5	In the **Default Web Site Home** pane, under **IIS**, select **MIME Types**.
6	Double-click **MIME Types**.
7	On the **Actions** list on the right pane, click **Add**.
8	In the **File name extension** box, type **.dic**.
9	In the **MIME Type** box, type **application/octet-stream**.

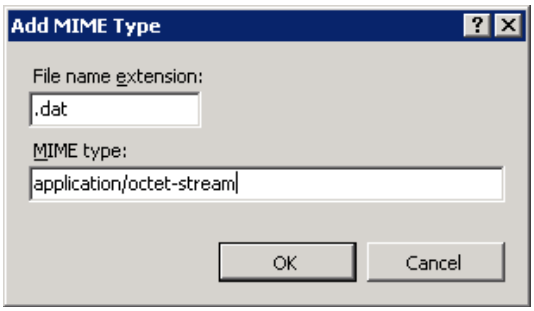


10 Click **OK**.

11 On the **Actions** list on the right, click **Add**.

12 In the **File name extension** box, type **.dat**.

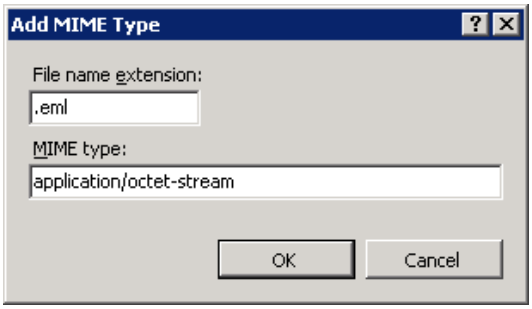
13 In the **MIME Type** box, type **application/octet-stream**.



14 Click **OK**.

15 From the **MIME Types** list, locate .eml and select **Edit** from the **Actions** list on the right.

16 In the **MIME Type** box, type **application/octet-stream**.



17 Click **OK**.

18 Close the **Computer Management** window.

--End--

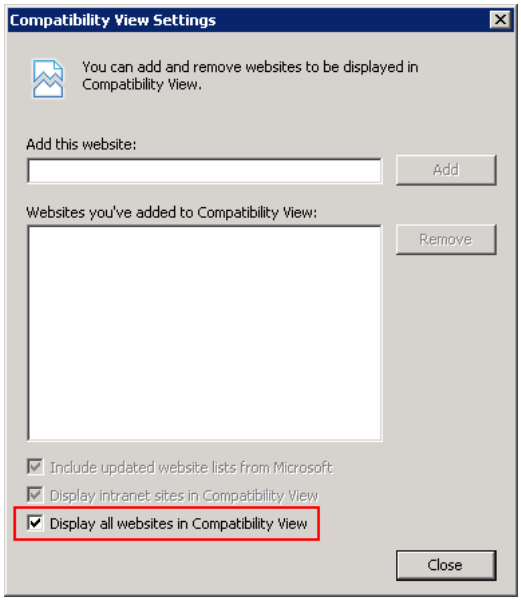
Configuring Internet Explorer 9.0 for Avaya Media Server Element Manager

If you plan to use Microsoft Internet Explorer 9.0 to access the Avaya Media Server - Element Manager, you must first configure Internet Explorer 9.0.

If you are using other versions of Microsoft Internet Explorer, skip this procedure.

Procedure steps

Step	Action
1	Start Microsoft Internet Explorer 9.0.
2	From the **Tools** menu, choose **Compatibility View Settings**.
3	Select **Display all websites in Compatibility View**.



4	Click **Close**.

--End--

Logging onto Avaya Media Server Element Manager

Element Manager (EM) is a web-based administration tool that facilitates the Operation, Administration, and Maintenance (OAM) of Avaya Media Server.

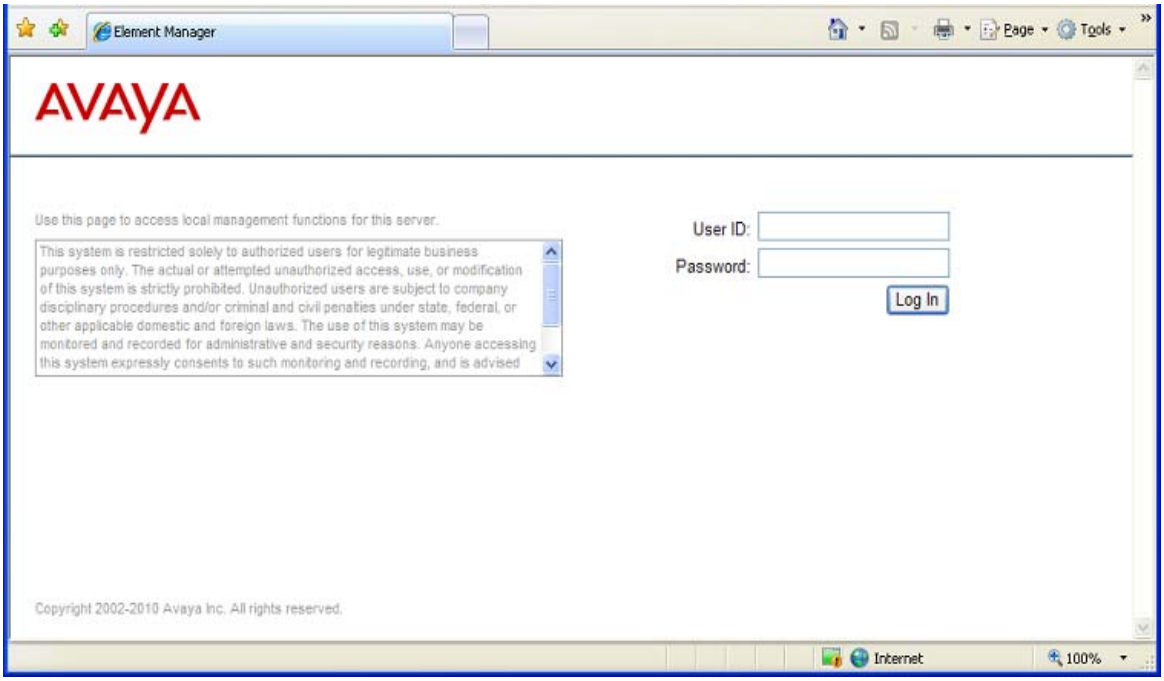
Procedure steps

Step	Action
1	On the Voice and Multimedia Contact Server, start a Web browser.

2 In the address box, enter https://<SERVER_IP_ADDRESS>:8443/em.
To access the Avaya Media Server Element Manager (EM) on the Voice and Multimedia Contact Server with Avaya Media Server, enter

https://localhost:8443/em

3 In the **User ID** box, type Administrator.



4 In the **Password** box, type the server Administrator password.

5 Click **Log In**.

--End--

Patching Avaya Media Server software

You can patch Avaya Media Server using Avaya Media Server Quick Fix Engineering (QFE) patches. Avaya Media Server QFE patches are not installed or maintained by the Avaya Aura® Contact Center Patch Manager, they are independent of Avaya Aura® Contact Center. You must always install QFE patches sequentially, as QFE patches are dependent on previous patches.

You must lock Avaya Media Server before applying patches and unlock it after you install the patches. In a multiple node configuration, apply a patch one node at a time, allowing the calls to be handled by other nodes in the Contact Center. Follow the procedure for each node.

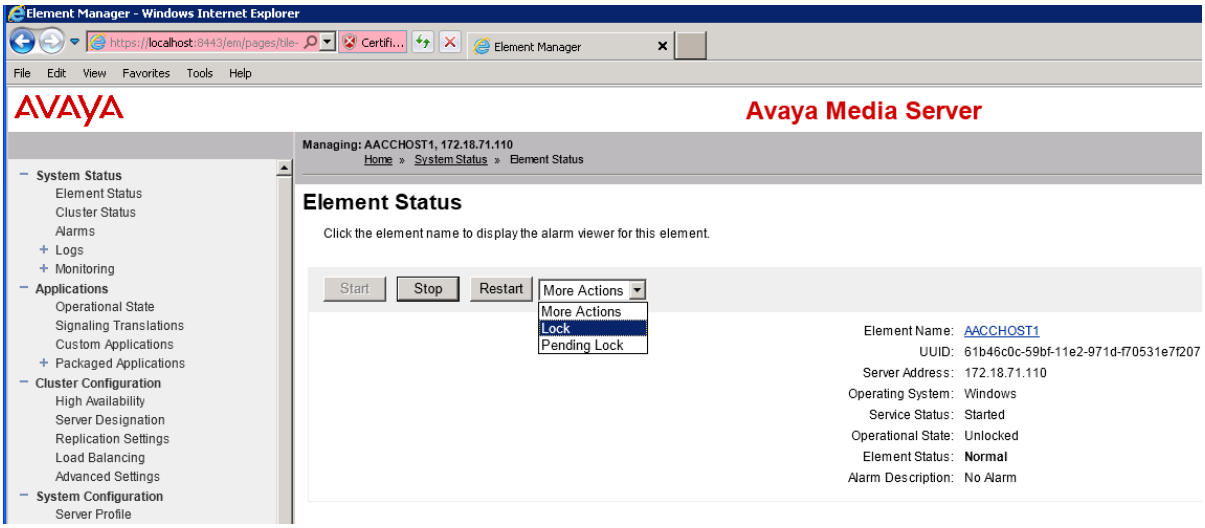
Attention: Follow the instructions in the Avaya Aura® Contact Center Release Notes and in each Avaya Media Server patch Readme file.

Prerequisites

- Download and review the Avaya Aura® Contact Center Release Notes. The Release Notes contain the known issues, patches, procedures, and workarounds specific to a release and patch line-up of Avaya Aura® Contact Center. For more information about the Avaya Aura® Contact Center Release Notes, see www.avaya.com/support.
- Read the QFE Readme files for the most recent information and instructions.
- Download the most recent Avaya Media Server Quick Fix Engineering patches and store them in the QFE subdirectory on the Avaya Media Server. QFE patches are ZIP files, do not un-zip QFE patches. The Avaya Media Server patching utility uses the QFE ZIP files. For a Windows server, the default QFE folder location is D:\Avaya\MAS\Multimedia_Applications\MAS\QFE.

Procedure steps

Step	Action
1	Navigate to the Element Manager of the Avaya Media Server node installed on the Voice and Multimedia Contact Server.
2	Select **System Status**, **Monitoring**, **Active Sessions** to check for active sessions on the server.
3	If there are no active sessions, click **System Status**, **Element Status** and skip to step 7.
4	In the navigation pane, click **System Status**, **Element Status**.
5	From the **More Actions** list, select **Pending Lock** to lock the Avaya Media Server after all processes finish.
6	Wait for existing active sessions to end.
7	In the **More Actions** menu, select **Lock**.



8 Click **Confirm**.

9 Close Element Manager.

10 Open a command prompt window.

11 Obtain the correct name of the new QFE patch by entering the following command:

```
maspatch list all
```

The name of the file is not necessarily the same as the name of the patch name.

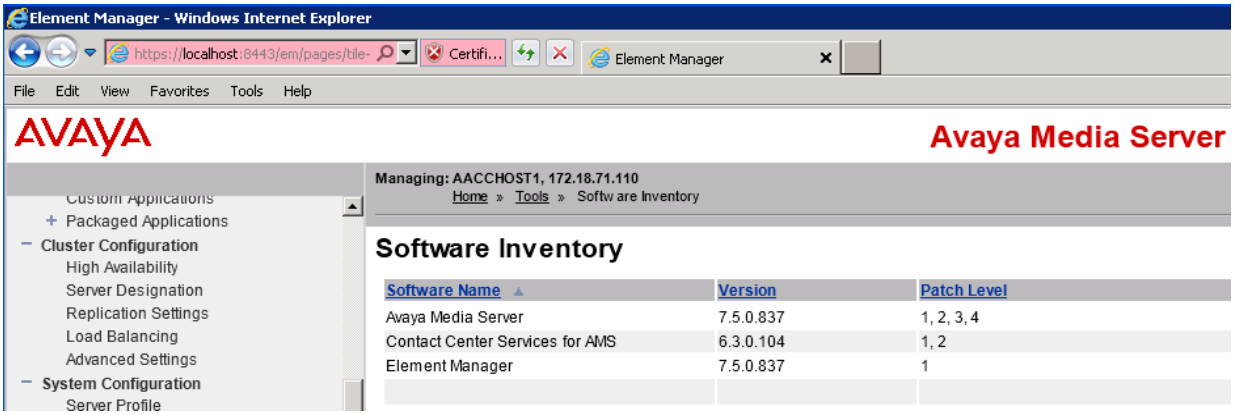
12 Under the **QFE Name** column, note the name of the patch (patchname).

13 To install all downloaded QFE patches on the system, enter the following command:

```
maspatch apply all
```

14 When the patch application is complete, open the Element Manager navigation pane, and click **Tools**, **Software Inventory**.

15 Verify the patch version listed in the **Patch Level** column is correct.



16 Select **System Status**, **Element Status**, and click **Start** if applicable. Confirm the operation.

17 From the **More Actions** list, select **Unlock** to unlock the Avaya Media Server. Confirm the operation.

--End--

Contact Center commissioning section

- Avaya Media Server commissioning (page 185)
- Voice and Multimedia Contact Server with Avaya Media Server commissioning (page 199)
- Multimedia commissioning (page 241)
- Orchestration Designer commissioning (page 279)

Avaya Media Server commissioning

This chapter describes the commissioning procedures for configuring trust relationships and media on the Avaya Media Server.

Configuring media on the Avaya Media Server

Avaya MS provides default media for standard ringback and busy tones.

Administrators provision additional media such as recorded announcements (RAN) and music for Avaya MS to provide meaningful treatments to the customer.

Media file formats

Avaya MS provides optimum playback performance with .WAV files transcoded as Linear 16-bit PCM, 8KHz Mono with a sampling rate of 128kbits/sec. Create your announcement and music media files with this transcoding before copying them onto the Avaya MS server.

Media organization

In Avaya MS Element Manager (EM), you organize media within a content namespace. The content namespace name must match the contact center SIP domain name; that is, the Local SIP Subscriber Domain Name in Contact Center Manager Server–Server Configuration.

Within the content namespace, you use content groups to subdivide the media into logical groups. You must create one locale-specific content group. The locale-specific content group must match the Local SIP Subscriber MS Locale in Contact Center Manager Server (CCMS) Server Configuration utility.

You can create one or more additional content groups for music. Typically you store different types of music media in different content groups.

To use treatments in Orchestration Designer (OD) flow applications or scripts, you create routes in Contact Center Manager Administration (CCMA) that link to the media files in the Avaya MS locale-specific content group. To use scripted music in OD flow applications or scripts, you create routes in Contact Center Manager Administration (CCMA) that link to the Avaya MS content groups containing the music files. The OD flow applications or scripts reference these routes to access the treatment files and scripted music on the Avaya MS server.

The SIP domain for the example contact center is siptraffic.com. The locale configured on the CCMS server is en_us.

The media content namespace structure is as follows:

```
siptraffic.com      <= media content namespace, matches SIP domain
      | en_us       <= locale-specific media content group (announcements)
      | folk        <= media content group (folk music)
      | jazz        <= media content group (jazz music)
      | rock        <= media content group (rock music)
```

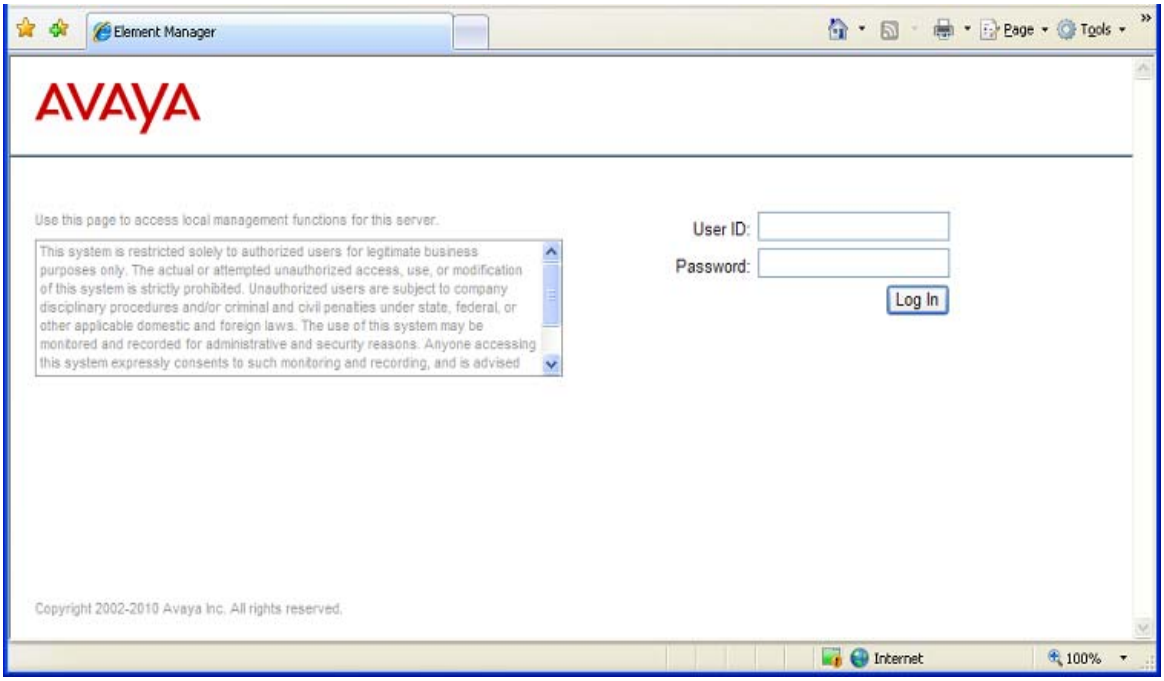
The locale-specific content group matches the locale configured on the Avaya Aura® Contact Center Manager Server server.

Logging onto Avaya Media Server Element Manager

Element Manager (EM) is a web-based administration tool that facilitates the Operation, Administration, and Maintenance (OAM) of Avaya Media Server.

Procedure steps

Step	Action
1	On the Voice and Multimedia Contact Server, start a Web browser.
2	In the address box, enter https://<SERVER_IP_ADDRESS>:8443/em. To access the Avaya Media Server Element Manager (EM) on the Voice and Multimedia Contact Server with Avaya Media Server, enter **https://localhost:8443/em**
3	In the **User ID** box, type the user ID of the server Administrator.



4 In the **Password** box, type the server Administrator password.

5 Click **Log In**.

--End--

Confirming the Contact Center packaged application locale

Confirm the locale configuration of the core Contact Center Services Packaged Applications to ensure the contact center receives the correct tones and announcements.

Procedure steps

Step	Action
1	Log on to the Avaya Media Server Element Manager.
2	In the navigation pane, click **Applications**, **Packaged Applications**, **Contact Center**.
3	On the **General Settings** page, confirm that the **Default Locale** is **en_us**.

--End--

Configuring the SIP port on a co-resident Avaya Media Server

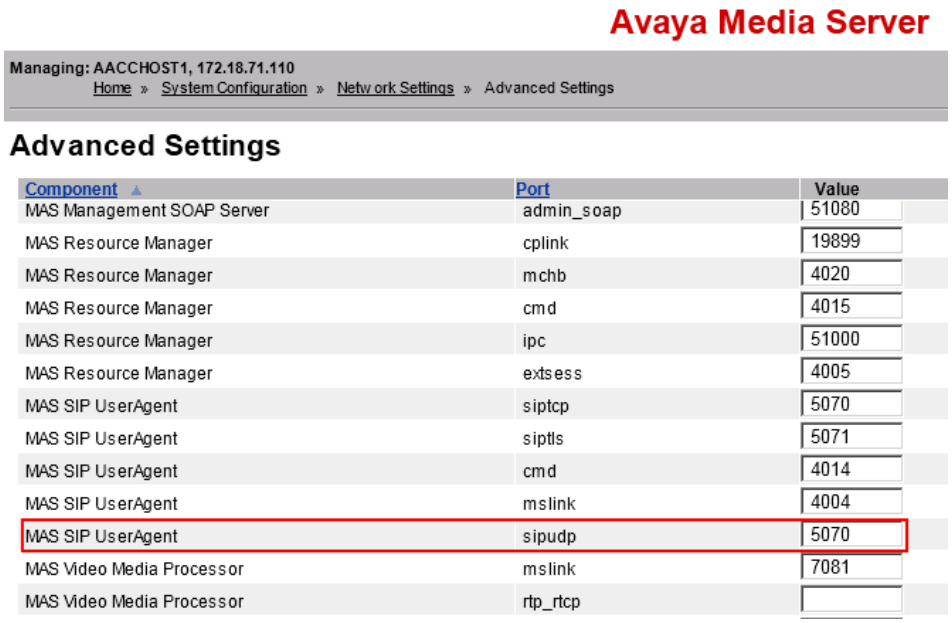
Configure the SIP port on the co-resident Avaya Media Server so that it does not have a port clash with the Contact Center Manager Server SIP port. The default standalone Avaya Media Server SIP port is 5060.

Prerequisites

- Access the Element Manager for the Avaya Media Server.

Procedure steps

Step	Action
1	In the navigation pane, click **System Configuration**.
2	Click **Network Settings**.
3	Click **Advanced Settings**.
4	Under **Advanced Settings**, in the **sipudp** box in the **MAS SIP UserAgent** component, type **5070**.



5	Click **Save**.

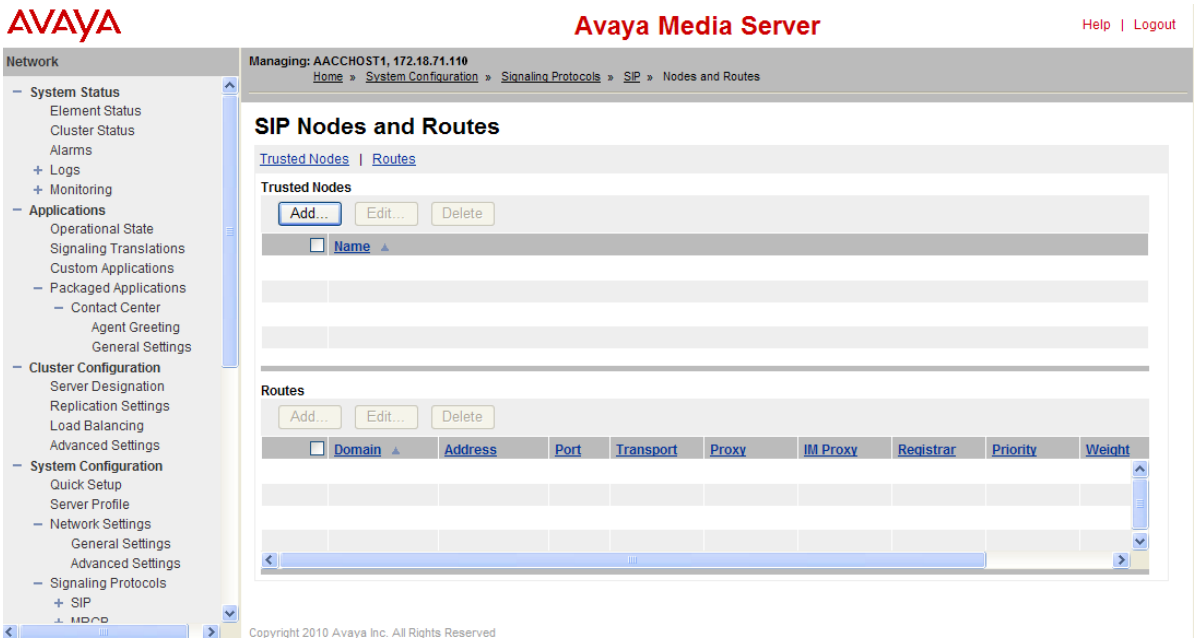
--End--

Adding Contact Center Manager Server as a trusted node

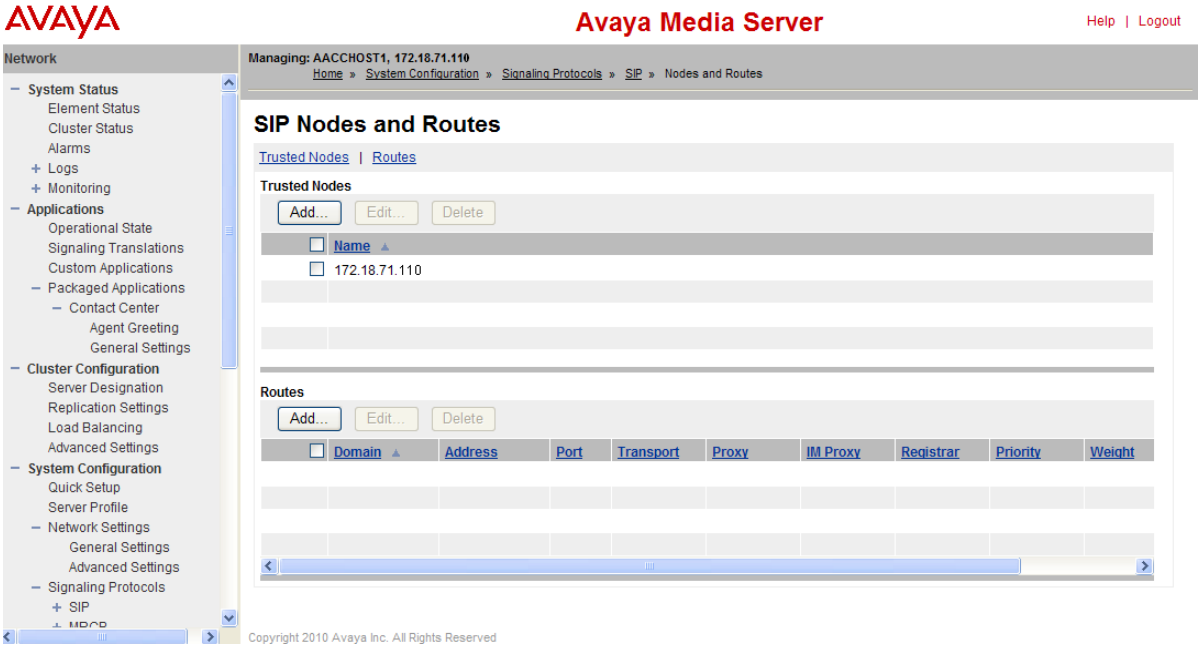
Add Contact Center Manager Server server as a trusted node to allow Avaya Aura® Contact Center to use the Avaya Media Server services.

Procedure steps

Step	Action
1	In the navigation pane, click **System Configuration**, **Signaling Protocols**, **SIP**.
2	Click **Nodes and Routes**.
3	Click the **Trusted Nodes** link.



4	Click **Add**.
5	On the **Add SIP Trusted Node** page, in the **Host or Server Address** box, type the name or IP address of the Voice and Multimedia Contact Server. For example, type 172.18.71.110.
6	Click **Save**.



--End--

Adding the media content namespace

Create the content namespace to organize the media treatments for the contact center.

Administrators provision additional media such as recorded announcements (RAN) and music for Avaya Media Server to provide meaningful treatments to the customer.

The locale-specific content group matches the locale configured on the Avaya Aura® Contact Center Manager Server server.

Procedure steps

Step	Action
1	In the navigation pane, click **Tools**, **Media Management**.
2	On the **Media Management** page, under **Content Namespaces**, click **Add**.
3	In the **Name** box, type **siptraffic.com**.
4	Click **Save**.



--End--

Adding the locale-specific media content group

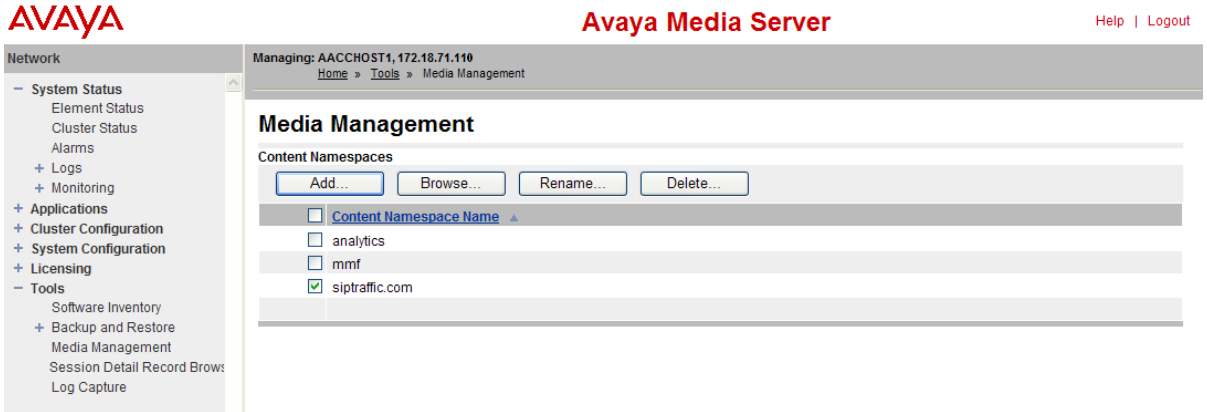
Create the locale specific content group required to store media for announcements.

Prerequisites

- Create the media content namespace. For more information about adding content namespaces, see Adding the media content namespace (page 190).

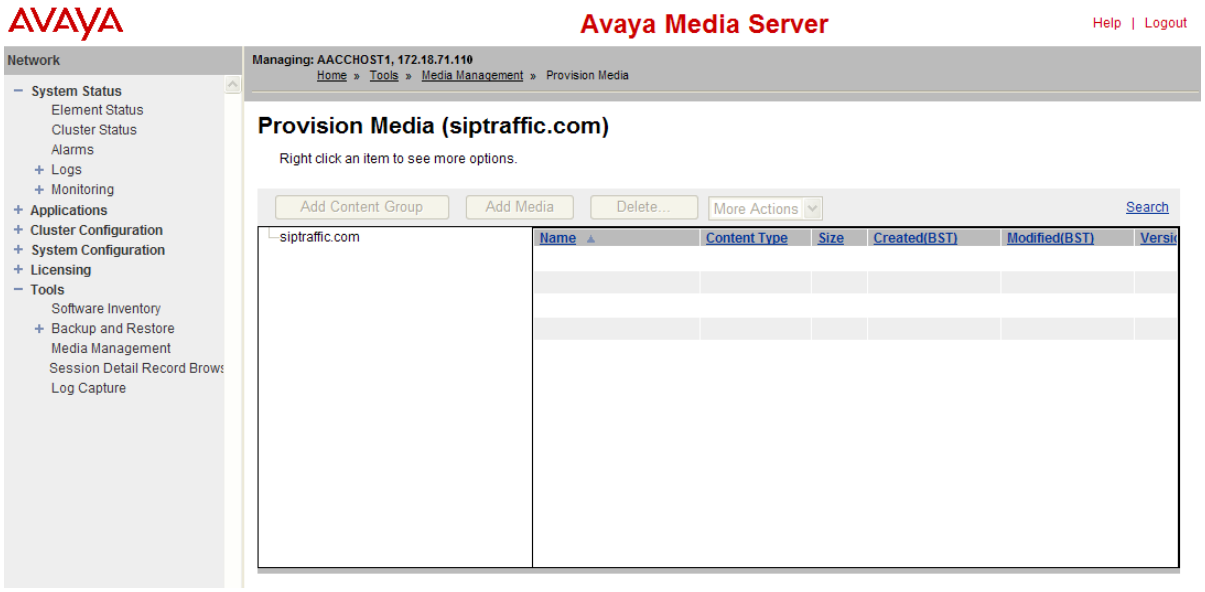
Procedure steps

Step	Action
1	In the navigation pane, click **Tools**, **Media Management**.
2	On the **Media Management** page, under **Content Namespaces**, select the content namespace, for example select **siptraffic.com**.



3 Click **Browse**.

Avaya MS displays the Provision Media page.

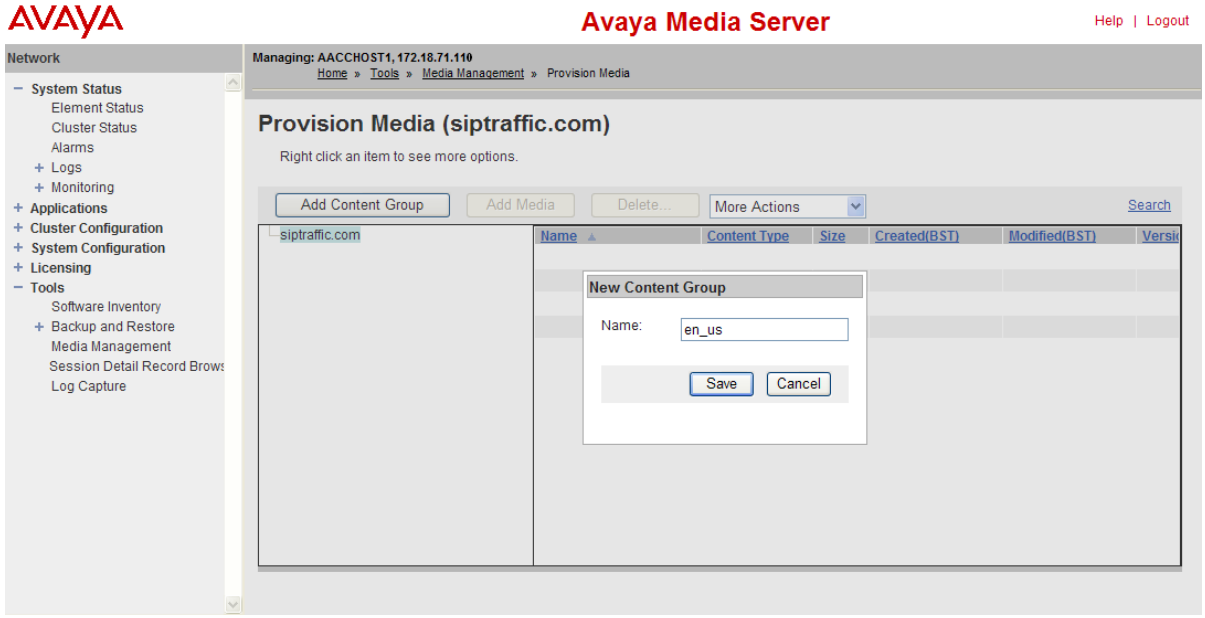


4 On the **Provision Media** page, in the left pane, select the content namespace. For example, select siptraffic.com.

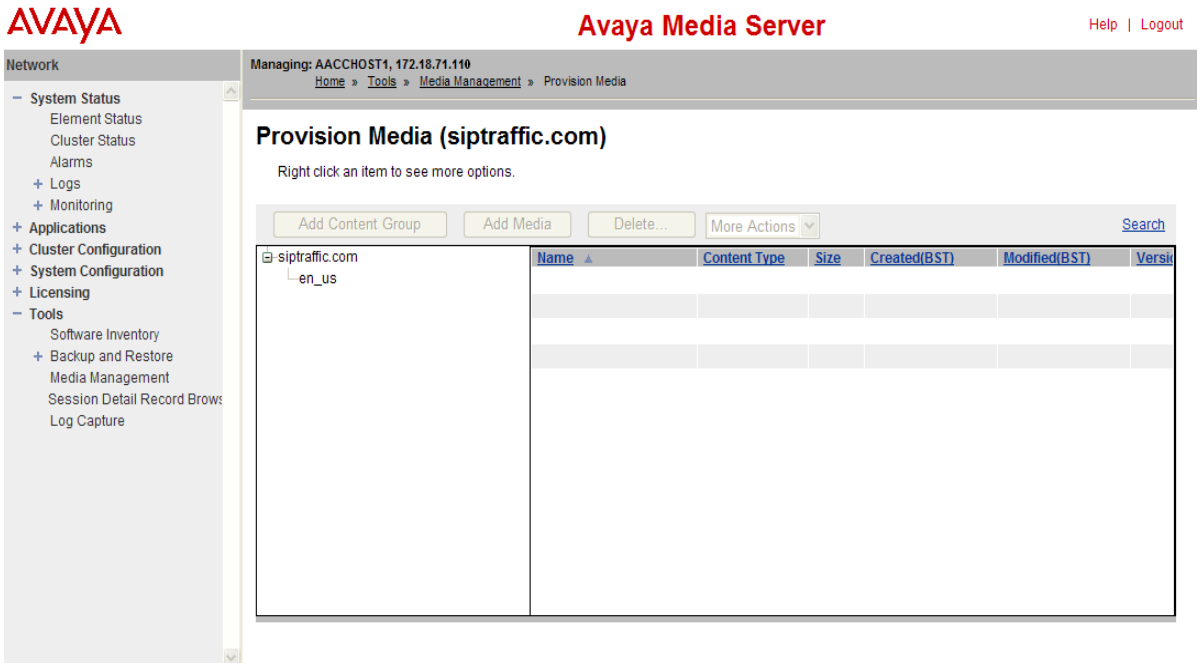
5 Click **Add Content Group**.

Avaya MS displays the New Content Group page.

6 In the **New Content Group** dialog box, in the **Name** box, type **en_us**.



7 Click **Save**.



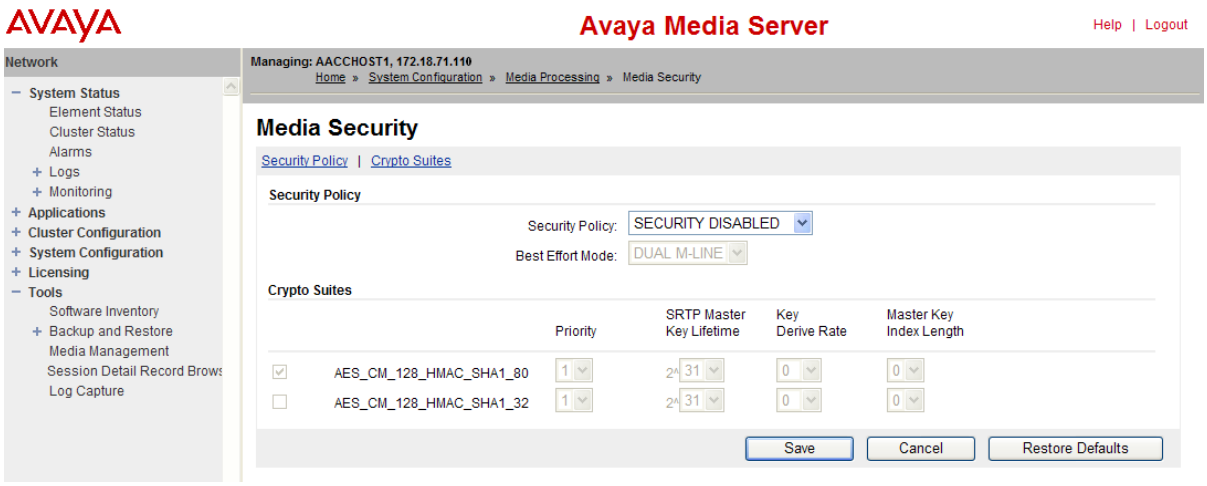
--End--

Configuring Avaya Media Server settings for SIP-enabled contact center

Configure the Avaya Media Server settings to ensure Avaya Media Server provides the optimal service for the Contact Center application.

Procedure steps

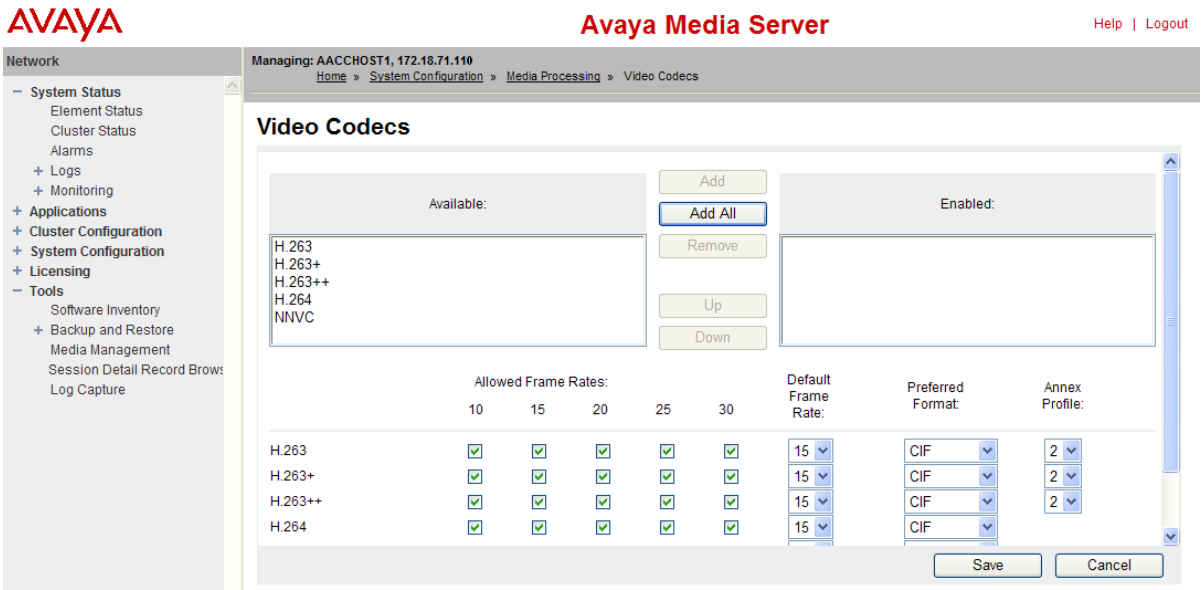
Step	Action
1	Log on to Element Manager.
2	In the navigation pane, click **System Configuration**, **Media Processing**, **Media Security**.
3	On the **Media Security** page, from the **Security Policy** list, select **Security Disabled**.



4 Click **Save**.

5 In the navigation pane, click **System Configuration**, **Media Processing**, **Video Codecs**.

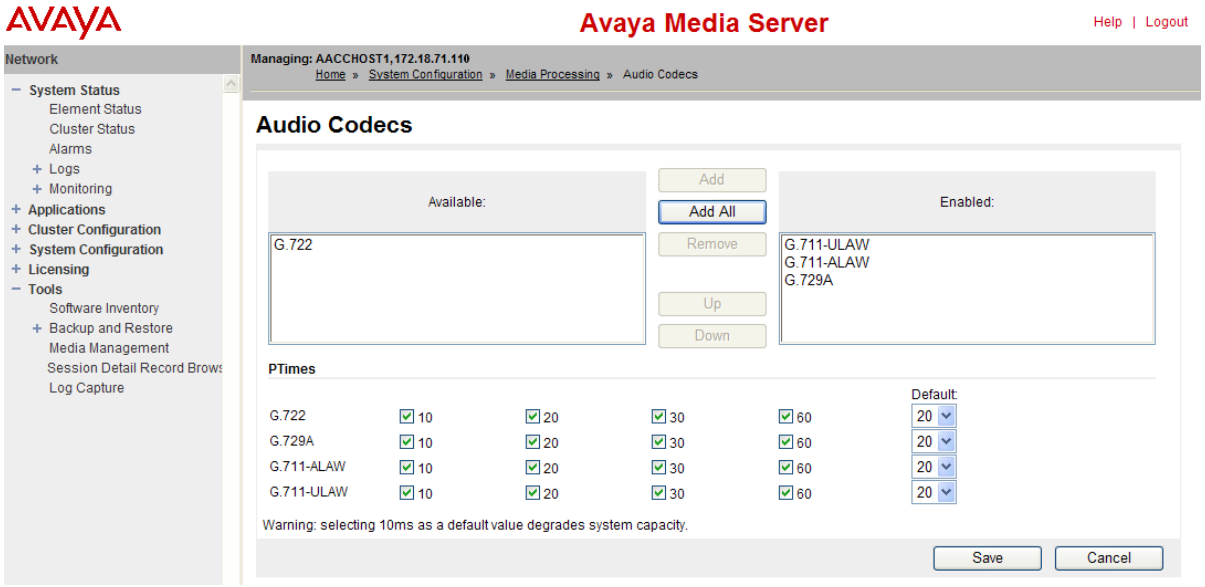
6 On the **Video Codecs** page, remove all codecs.



7 Click **Save**.

8 In the navigation pane, click **System Configuration**, **Media Processing**, **Audio Codecs**.

9 On the **Audio Codecs** page, ensure that the codecs you want to support appear in the **Enabled** list.

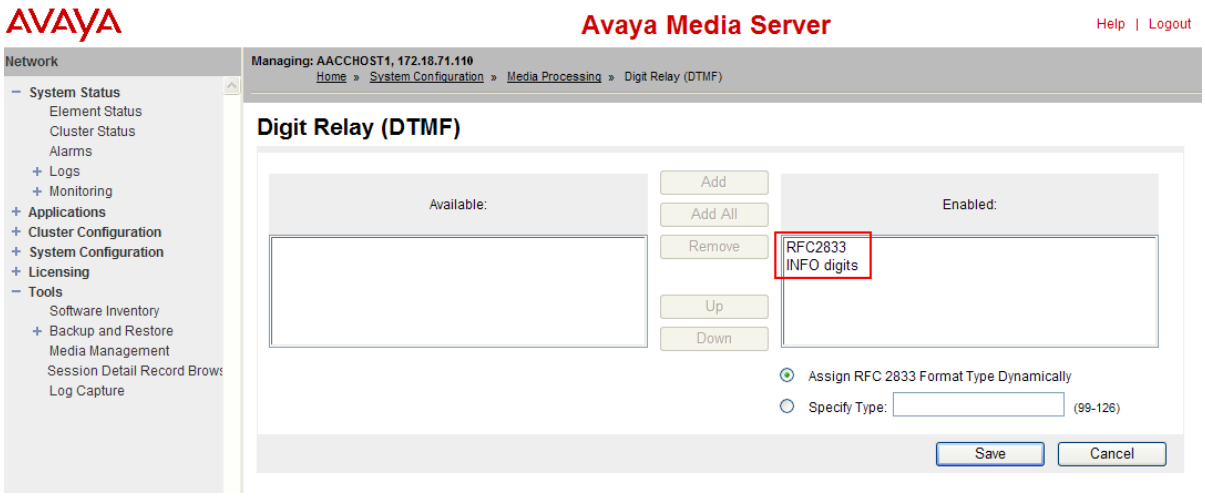


10 Click **Save**.

11 In the navigation pane, click **System Configuration**, **Media Processing**, **Digit Relay (DTMF)**.

12 On the **Digit Relay (DTMF)** page, enable **RFC2833**.

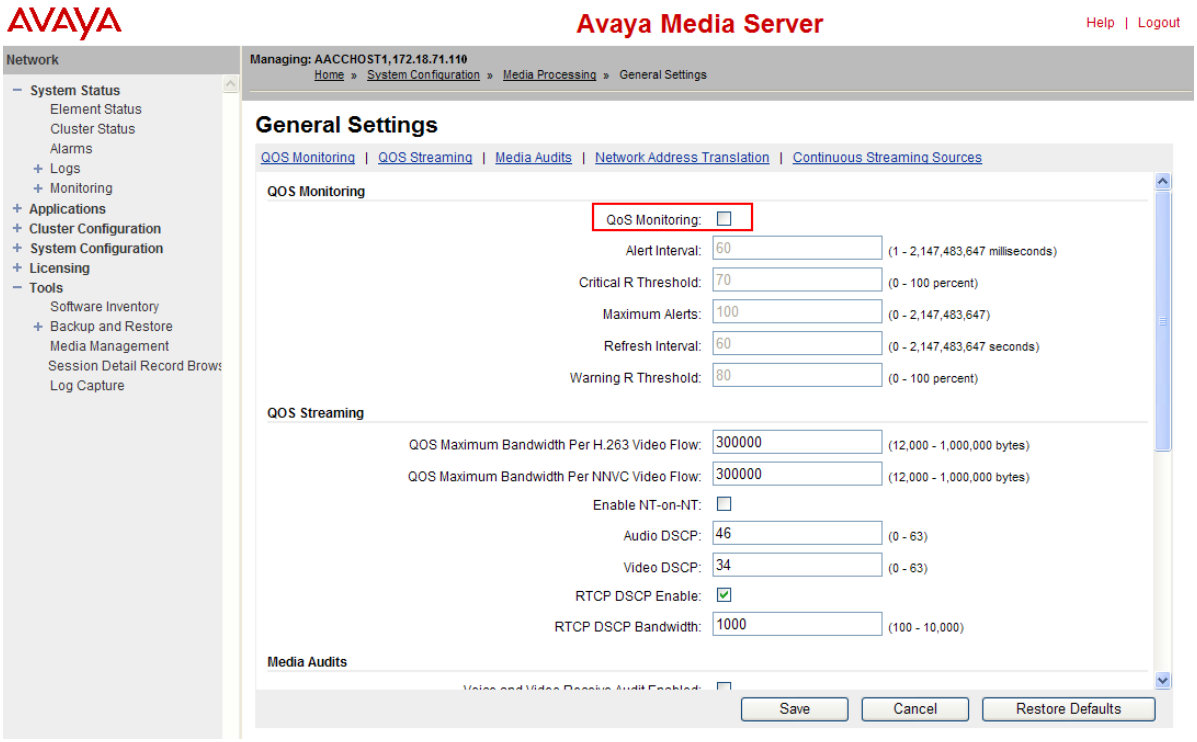
13 On the **Digit Relay (DTMF)** page, enable **INFO digits**. You must enable INFO digits after enabling RFC2833; RFC2833 must appear first on the list.



14 Click **Save**.

15 In the navigation pane, click **System Configuration**, **Media Processing**, **General Settings**.

16 On the **General Settings** page, clear the **QoS Monitoring** check box.



17 Click **Save**.

--End--

Uploading a batch zip file

You can upload a batch file to provision multiple media files on the Avaya Media Server in a single step. This can include all the media to provide call treatments such as announcements or music.

You can provision the media in a content namespace by using one ZIP file for the whole content namespace or by creating one content group at a time. After you upload the media file, Element Manager (EM) displays it in a tree view. The root of the tree is the content namespace and individual content groups appear below it. EM displays the content namespace and the content groups in the left pane, and the media files contained in the selected content group in the right pane.

Prerequisites

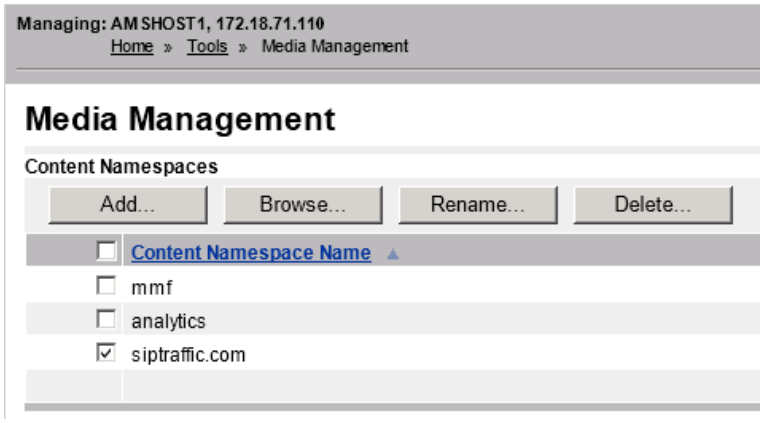
- Add the content namespace.

- Create the media files for a Content Namespace on your local system. You must organize the media files in the required file structure. Then zip the media files.

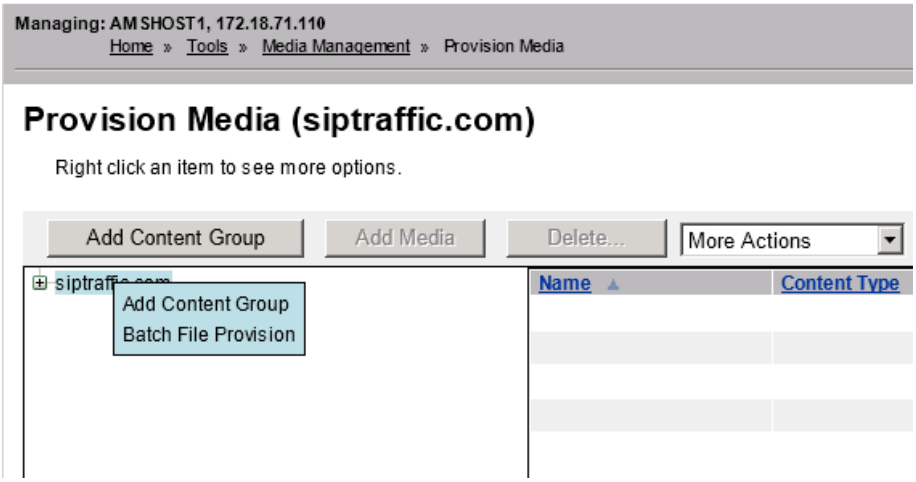
Attention: You must give the root directory the same name as the content namespace name.

Procedure steps

Step	Action
1	Log on to Element Manager from the system on which you have created the batch zip file.
2	In the navigation pane, click **Tools**, **Media Management**.
3	On the **Media Management** page, select the check box next to the content namespace to which you want to add the media. For example, select siptraffic.com.



4	Click **Browse**. *Avaya MS displays the **Provision Media** page.*
5	On the **Provision Media** page, right-click the content namespace and select **Batch File Provision** on the shortcut menu.



6 On the **Batch File Provision** dialog box, click **Browse**, and then navigate to the zip file to upload.

7 Click **Always overwrite file with the same name**.

OR

Click **Do not overwrite files with the same name**.

8 Click **Upload**.

--End--

Voice and Multimedia Contact Server with Avaya Media Server commissioning

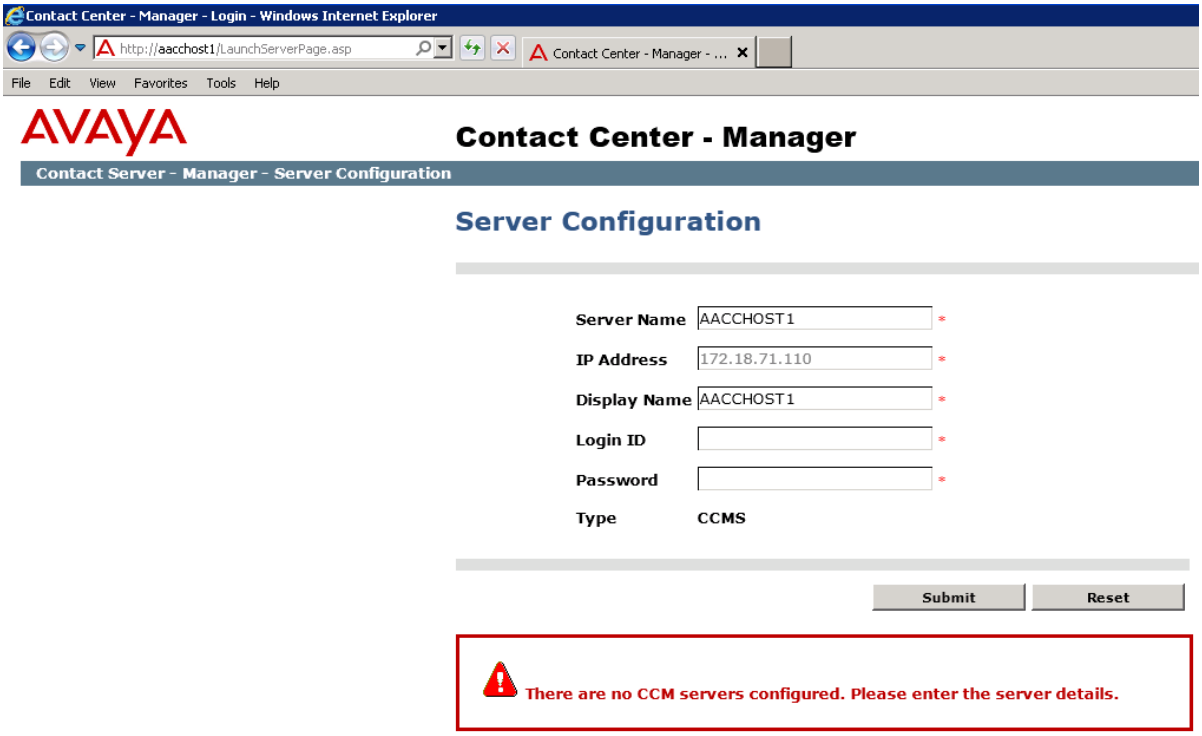
This section describes how to configure a Voice and Multimedia Contact Server with Avaya Media Server in a SIP-enabled contact center.

Logging on to Contact Center Manager Administration for the first time

When you log on to Contact Center Manager Administration for the first time, you must log on as the default administrator, webadmin. For security reasons, change the default password when you first log on to the application.

Procedure steps

Step	Action
1	Start Internet Explorer.
2	In the **Address** box, type the following: http://AACCHOST1 where AACCHOST1 is the server name of the *Voice and Multimedia Contact Server*.
3	In main logon window, in the **User ID** box, type the default user account - webadmin.
4	In the Password box, type the default password - webadmin.
5	Press **Login**. You can modify the default password only. You cannot change the default user name. **Attention:** If you are prompted to install Avaya published plug-ins for Contact Center Manager Administration, on the plug-in message box, click Install.
6	The **Server Configuration** page appears.



7 In the **Login ID** box, type the Login ID for Contact Center Manager Server. The Login ID corresponds to a user account created using the Contact Center Manager Server Utility. The default Login ID is sysadmin. For example, type sysadmin.

8 In the **Password** box, type the password for the Contact Center Manager Server. The default password is avaya1. For example, type avaya1.

You can modify the default password only. You cannot change the default user name.

9 Click **Submit**.

The Contact Center Manager Administration launchpad appears.



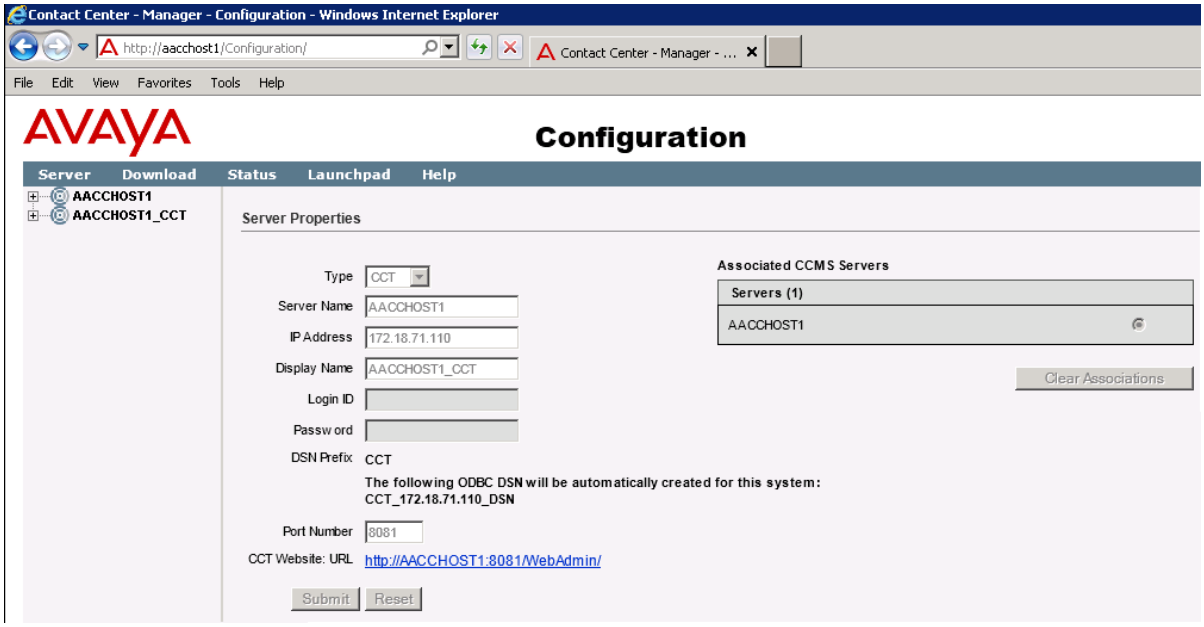
--End--

Adding Communication Control Toolkit to Contact Center Manager Administration

Add Communication Control Toolkit (CCT) to Contact Center Manager Administration (CCMA) and associate it to a Contact Center Manager Server (CCMS) server. The CCT server Display Name must be unique.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration.
2	On the Launchpad, click **Configuration**.
3	From the **Server** menu, click **Add Server**.
4	From the **Type** list, select **CCT**.
5	In the **Server Name** box, type the CCT server name, for example AACCHOST1.
6	In the **Display Name** box, type the unique display name for the CCT server, for example type AACCHOST1_CCT.
7	In the **Associated CCMS Servers** list, select the CCMS with which you want to associate this CCT server.
8	Click **Submit**.



--End--

Adding the Multimedia server to Contact Center Manager Administration

Add the Contact Center Multimedia (CCMM) server to Contact Center Manager Administration (CCMA) to provide reporting and connectivity support.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration.
2	On the **Launchpad**, click **Configuration**.
3	On the configuration menu, select **Server**, **Add Server**.
4	From the **Type** list, select CCMM.
5	In the **Server Name** box, type the computer name of the Multimedia server, for example AACCHOST1.
6	Press the **Tab** key. If the DNS static entry for the CCMM server exists the server IP address automatically appears in the IP Address box. Otherwise, type the IP address for the CCMM server.
7	In the **Display Name** box, type the name of the Multimedia server as you want it to appear in the system tree in Contact Center Manager Administration.

The system automatically assigns a display name that is the same as the server name. To enter a different display name, you must enter a unique name. For example, type AACCHOST1_CCMM.

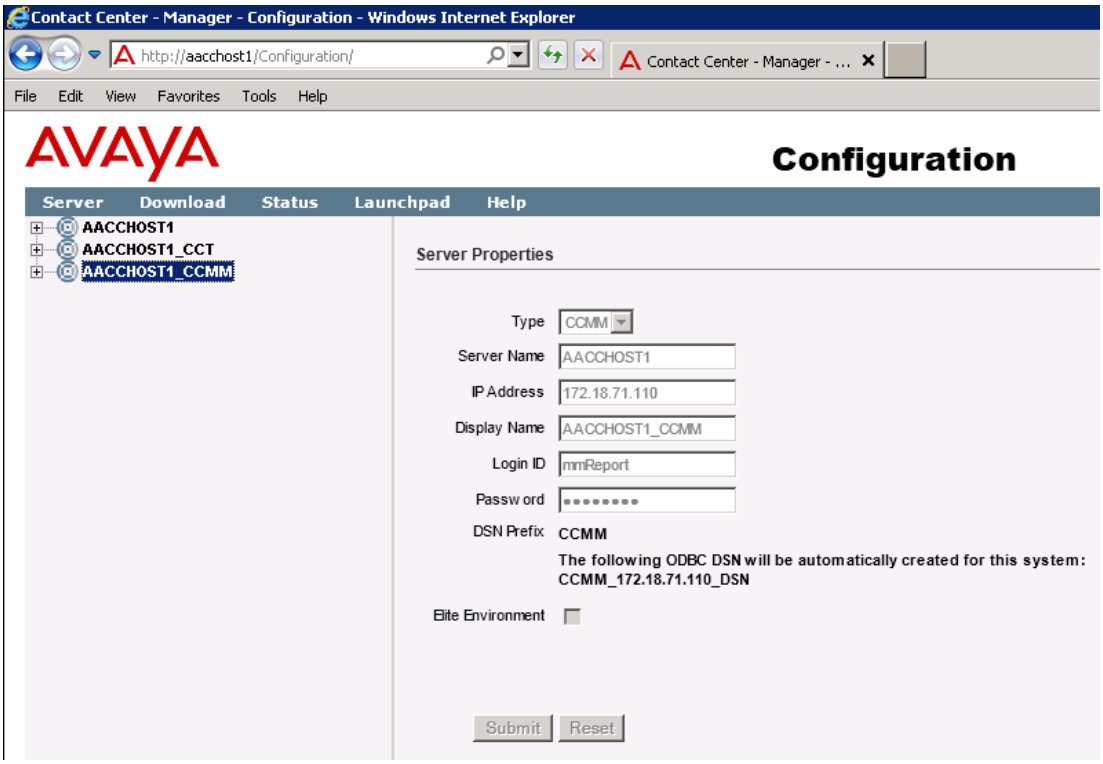
8 To add a Contact Center Multimedia server, in the **Login ID** box, type **mmReport**.

9 In the **Password** box, type the default password, **mmRep**.

Attention: You must change this password if the system sends a message that contains a log on request for validation.

10 If an **Elite Environment** check box is visible, clear the **Elite Environment** check box. Do not select the Elite Environment option.

11 Click **Submit**.



12 Click the plus symbol (+) beside the server name to access the server.

13 Select the Contact Center Manager Server with which you want to associate Contact Center Multimedia, for example select AACCHOST1.

14 In the left pane, right-click the Contact Center Manager Server with which you want to associate Contact Center Multimedia and then click **Edit Properties**.

15 Under **Associated Reporting Server**, select the check box next to the Contact Center Multimedia server name.



16 Click **Submit**.

--End--

Configuring global settings

In the Global Settings window, you can set the global values on the Contact Center Manager Server, which include Agent Order preference, default RAN route, default IVR DN, Expected Wait Time (EWT) algorithm, Broadcast Ports and default timer, and the server designated for historical statistical data.

Procedure steps

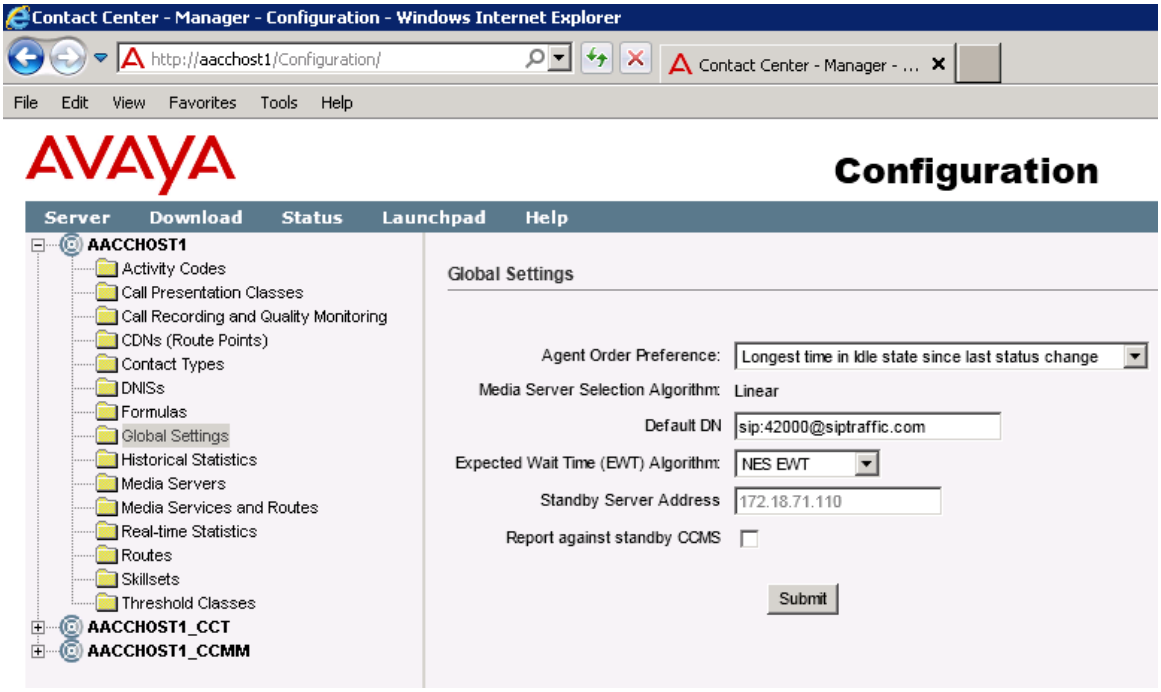
Step	Action
1	Log on to the Contact Center Manager Administration.
2	On the **Launchpad**, click **Configuration**.
3	In the left pane, expand the server on which you want to configure global settings. For example, expand AACCHOST1.
4	Select the **Global Settings** folder.
5	From the **Agent Order Preference** list, choose how to present contacts to agents based on their idle time.
6	In the **Default DN** box, type the default DN to use when a script defaults or a treated call is not answered. Avaya recommends that you configure an attendant as the Default DN.
7	In the **Expected Wait Time Algorithm** field, select either **NES EWT** or **Enhanced EWT** algorithm. For example, select **NES EWT**.
8	Click **Submit**.

--End--

Variable	Value
Agent Order Preference	Choose how to present contacts to agents based on their idle time. Valid values: • **Longest total time in idle state since login**—Choose this option to present contacts to the agent who accumulated the most idle time since logging on. • **Longest time in idle state since last status change**—Choose this option to present contacts to the agent who have accumulated the most idle time since the last status change for that agent (this is the system default setting). • **Longest total time since last CDN/ACD call**—Choose this option to present contacts to the agent with the longest elapsed time since handling a CDN/ACD call. **Attention:** The system does not reset the timer when the agent switches to the Not Ready state.
Default DN	In the Default DN box, type the default DN to use when a script defaults or a treated call is not answered. Avaya recommends that you configure an attendant as the Default DN.
Expected Wait time (EWT) Algorithm	Select either NES EWT or Enhanced EWT as required. Valid values: • **NES EWT**—This is a legacy algorithm for calculating the expected wait time using real data available in the system. (Actual wait time of previously serviced contacts.) • **Enhanced EWT**—This is a new algorithm, which is more accurate than the NES EWT. This also uses actual wait time data available in the system.
Reporting against standby CCMS	Select to enable historical report statistics to be gathered from the standby CCMS server specified in the Address box. If the standby server goes down, then historical reporting statistics are taken from the primary server automatically.
Submit	Save your changes.

Procedure job aid

The Contact Center Manager Server — Global Settings window.



Adding route points for voice contacts

Add route points for voice and contacts.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration with administrative privileges.
2	On the **Launchpad**, click **Configuration**.
3	In the left pane, expand the CCMS server. For example, expand AACCHOST1.
4	Select the **CDNs (Route Points)** folder.
5	On the **CDNs (Route Points)** window, in the **Name** box, type the name of the first voice route point. For example, type 52000.
6	In the **Number** box, type the number for the route point. For example, type 52000.
7	In the **URI** box, type the value for the Uniform Resource Indicator (URI) of the route point on the SIP server. For example, type sip:52000@siptraffic.com.
8	From the **Call Type** list, select **Local**.

9 Select the **Acquired?** check box to indicate to the system to acquire and process calls using this URI.

10 Select the next row of the grid to add and acquire another Route Point.

11 Select the **Open Queue** tab.

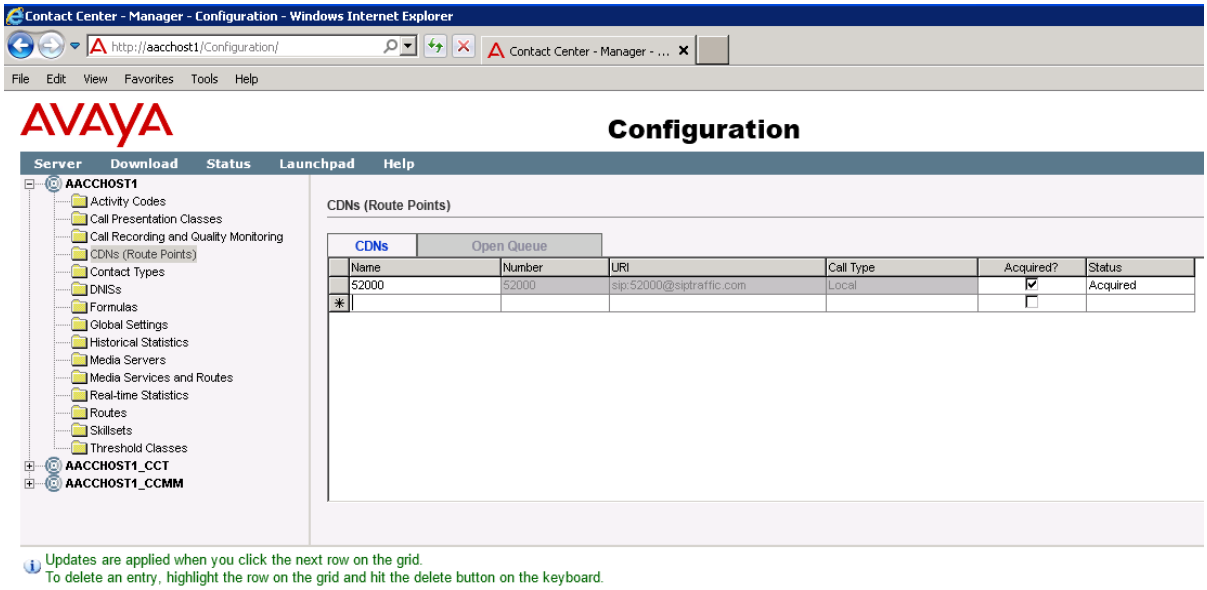
12 On the **OpenQRoutePointAddress** row, select **Acquired?** and select the next row of the grid.

--End--

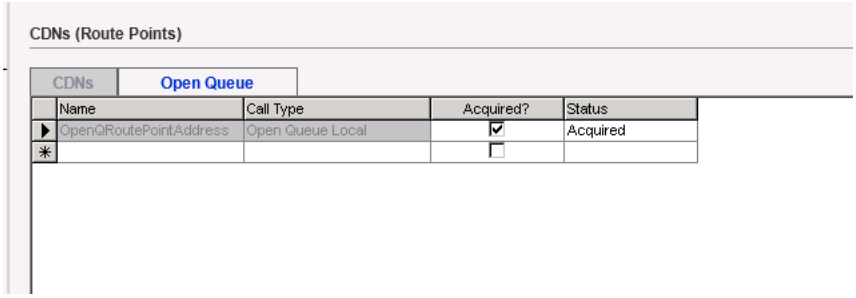
Procedure job aid

Example of the SIP Route Point. SIP calls to the number 52000 are handled by this "Acquired" route point.

Example of configuring and acquiring a route point



Example of configuring and acquiring a route point

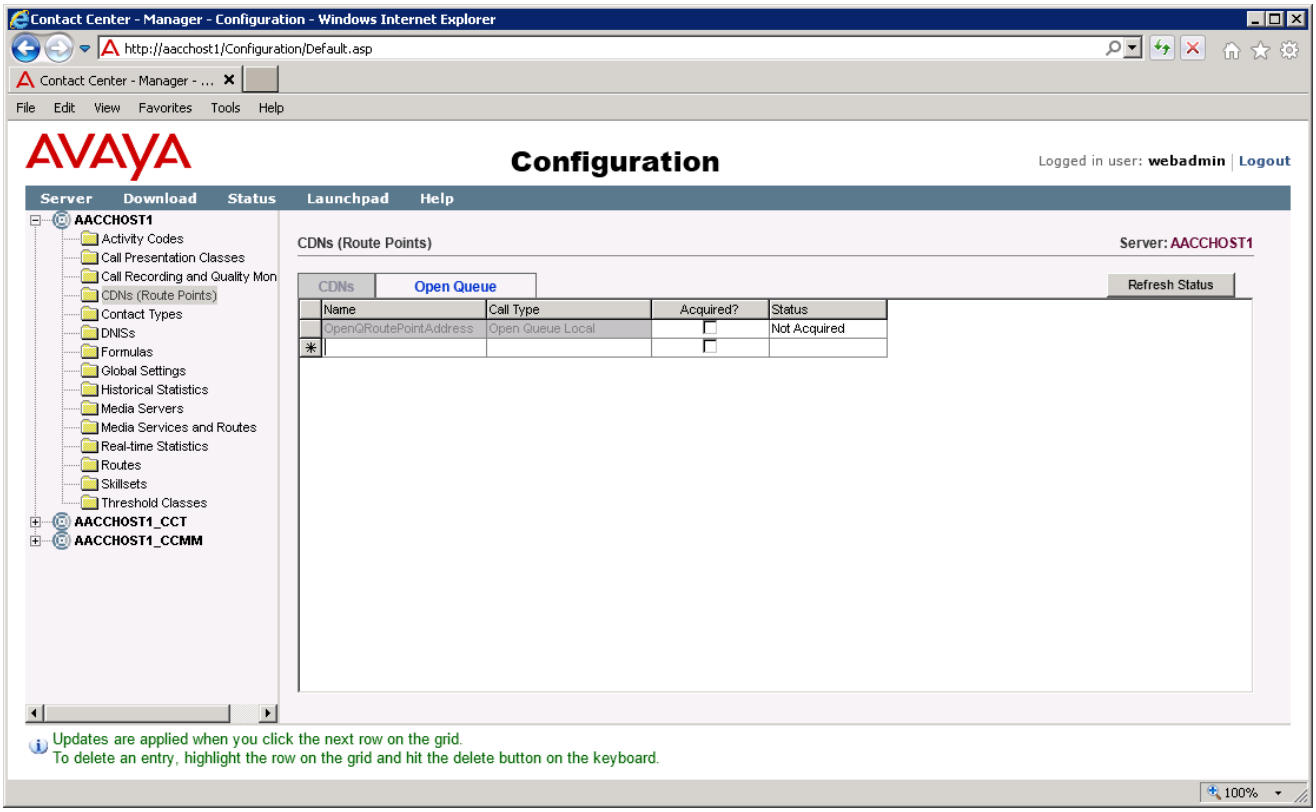


Adding a route point for email contacts

Add an email route point for email contacts. A route point is a logical address used by Contact Center to accept incoming contacts or as a point to which contacts are routed. An email route point is an address that enables incoming email contacts to be treated by Contact Center.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration with administrative privileges.
2	On the **Launchpad**, click **Configuration**.
3	In the left pane, expand the CCMS server. For example, expand AACCHOST1.
4	Select the **CDNs (Route Points)** folder.
5	Select **Open Queue**.



6 In the name box, type the name for the email Route Point. For example, type EmailContactsRP.

7 From the **Open Queue Local** list, select **Open Queue Local**.

8 Select the **Acquired?** check box.

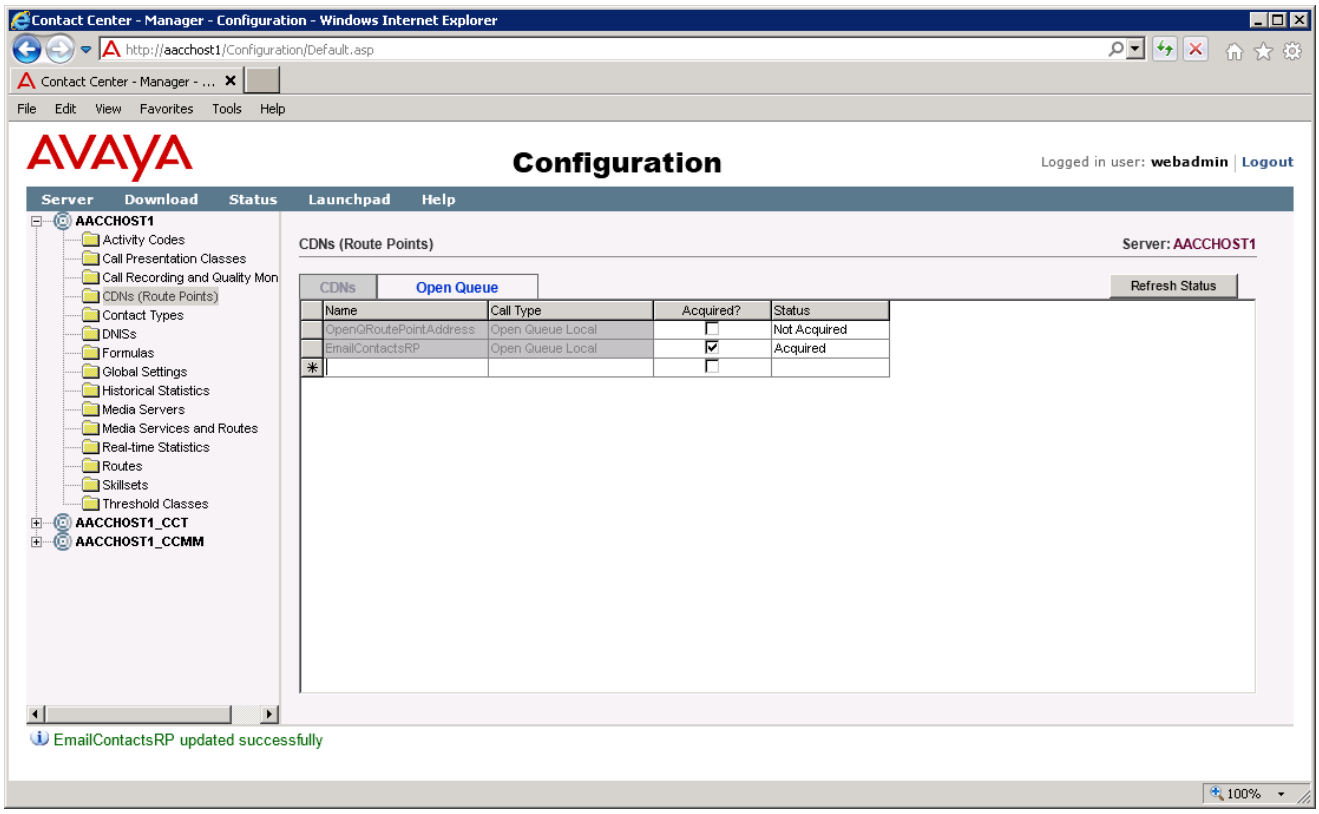
9 Click on the next row in the Open Queue table to store the Route Point details.

--End--

Procedure job aid

Example of the email Route Point.

Example of configuring and acquiring a route point



Adding the media server

Add the Avaya Media Server to Contact Center Manager Server using Contact Center Manager Administration.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration with administrator privileges.
2	On the **Launchpad**, click **Configuration**.
3	In the left pane, expand the CCMS server. For example, expand AACCHOST1.
4	From the list of configuration items for the Contact Center Manager Server, select **Media Servers**.

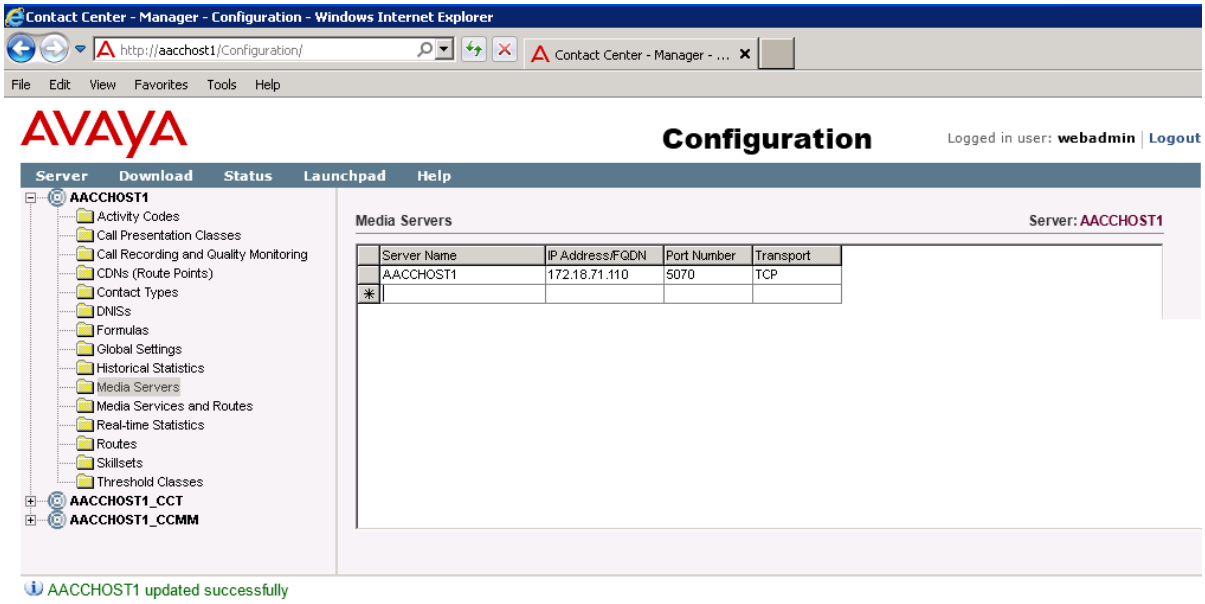
5 On the **Media Servers** window, in the **Server Name** box, type the name of the Avaya Media Server. For example, type AACCHOST1.

6 In the **IP Address** box, type the IP address for the Avaya Media Server. For example, type 172.18.71.110.

7 In the **Port Number** box, type the port number. For example, type 5070. This Avaya Media Server SIP port number must match the SIP port number configured on your Avaya Media Server. For more information, see Configuring the SIP port on a co-resident Avaya Media Server (page 203).

8 Ensure that the value for **Transport** is **TCP**.

9 Select the next row of the grid to add the Media Server.



--End--

Adding media servers to the required media services

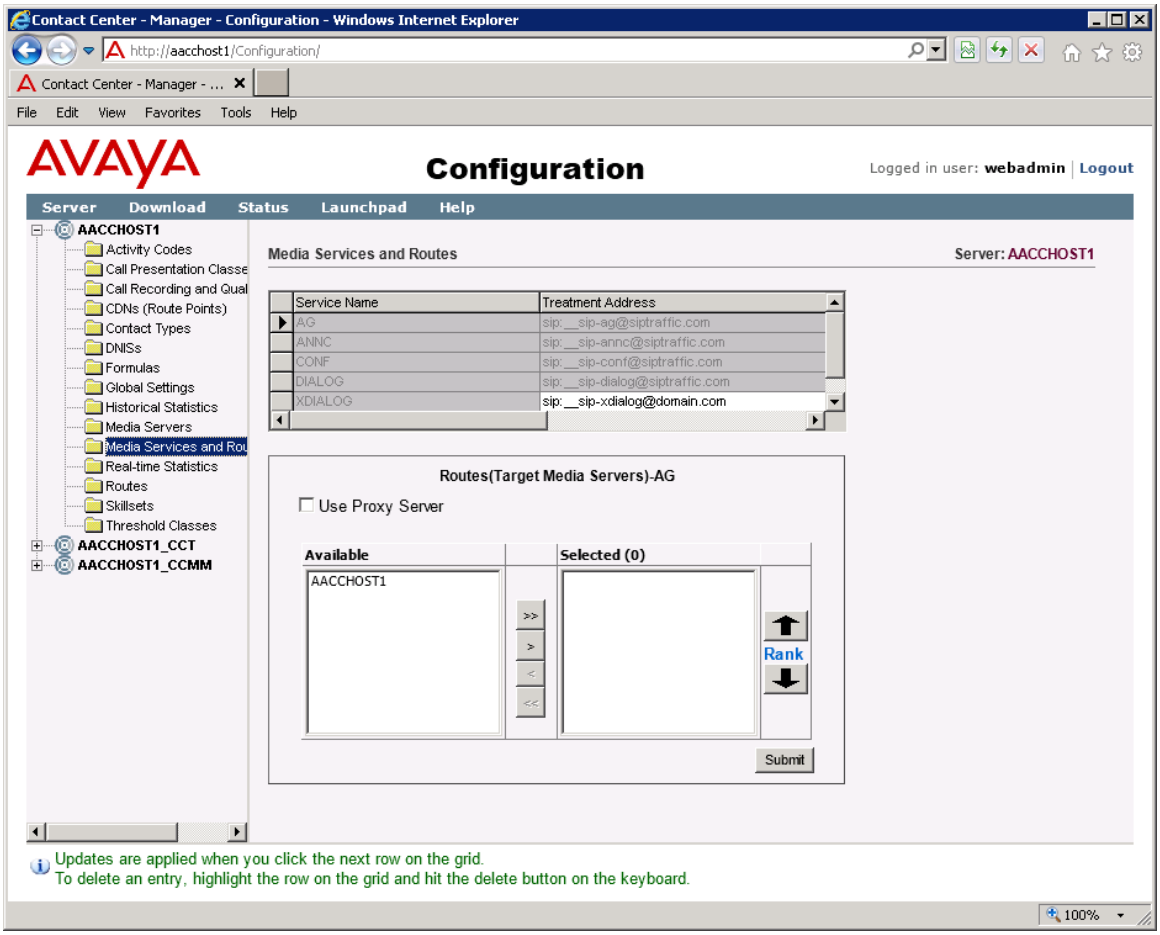
Each SIP-enabled contact center requires at least one Avaya Media Server to supply the following services:

- Announcements (ANNC)
- Conferences (CONF)
- Interactive Voice Response (IVR) dialog (DIALOG)

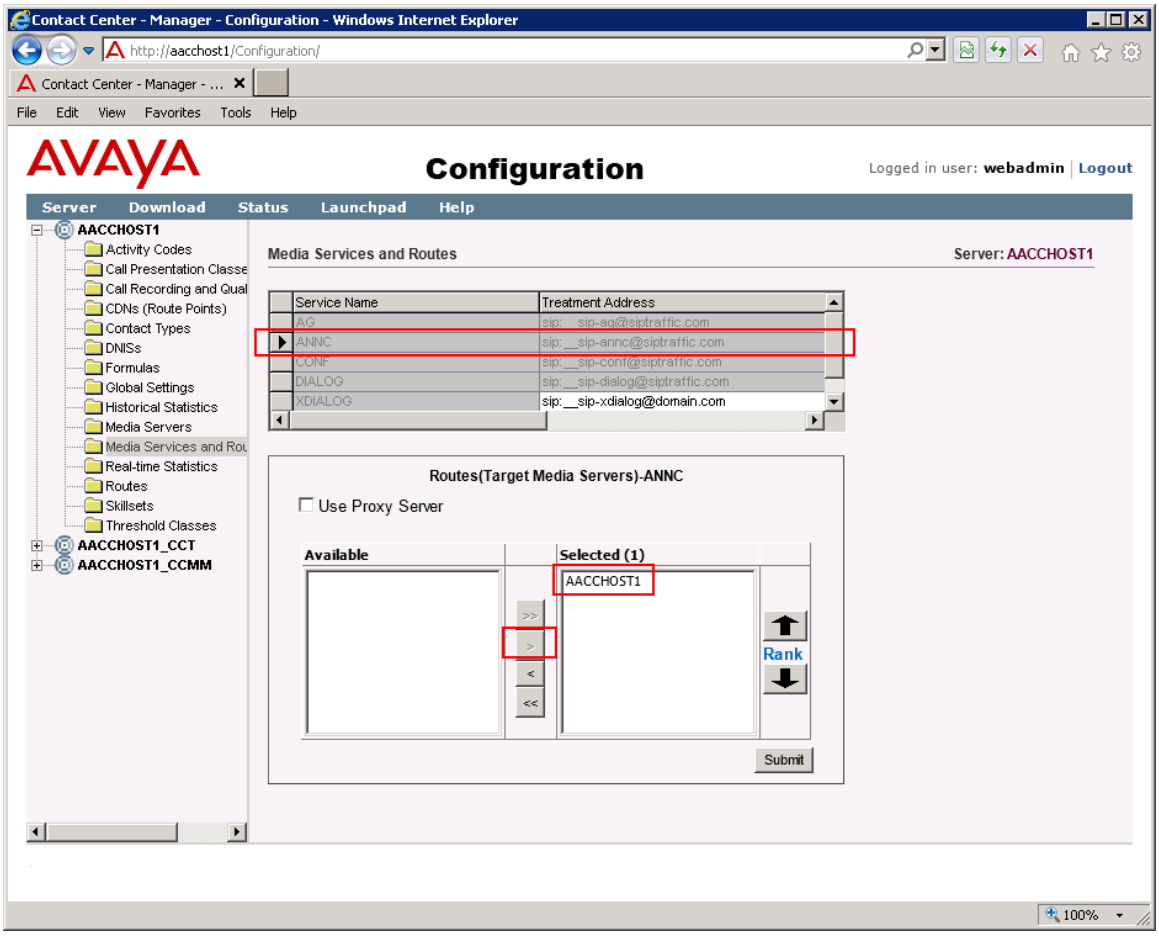
You must assign the Avaya Media Server for each announcement, conferencing, and dialog service.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration.
2	On the **Launchpad**, click **Configuration**.
3	In the left pane, expand the CCMS server. For example, expand AACCHOST1.
4	From the list of configuration items for the Contact Center Manager Server, select **Media Services and Routes**.



5	From the **Service Name** list, select **ANNC**.
6	In the **Routes (Target Media Servers)** section, from the **Available** list, select the Avaya Media Server server name. For example, select AACCHOST1.
7	Click the **>** arrow key. *AACCHOST1 is added to the list of Selected Announcement media servers.*



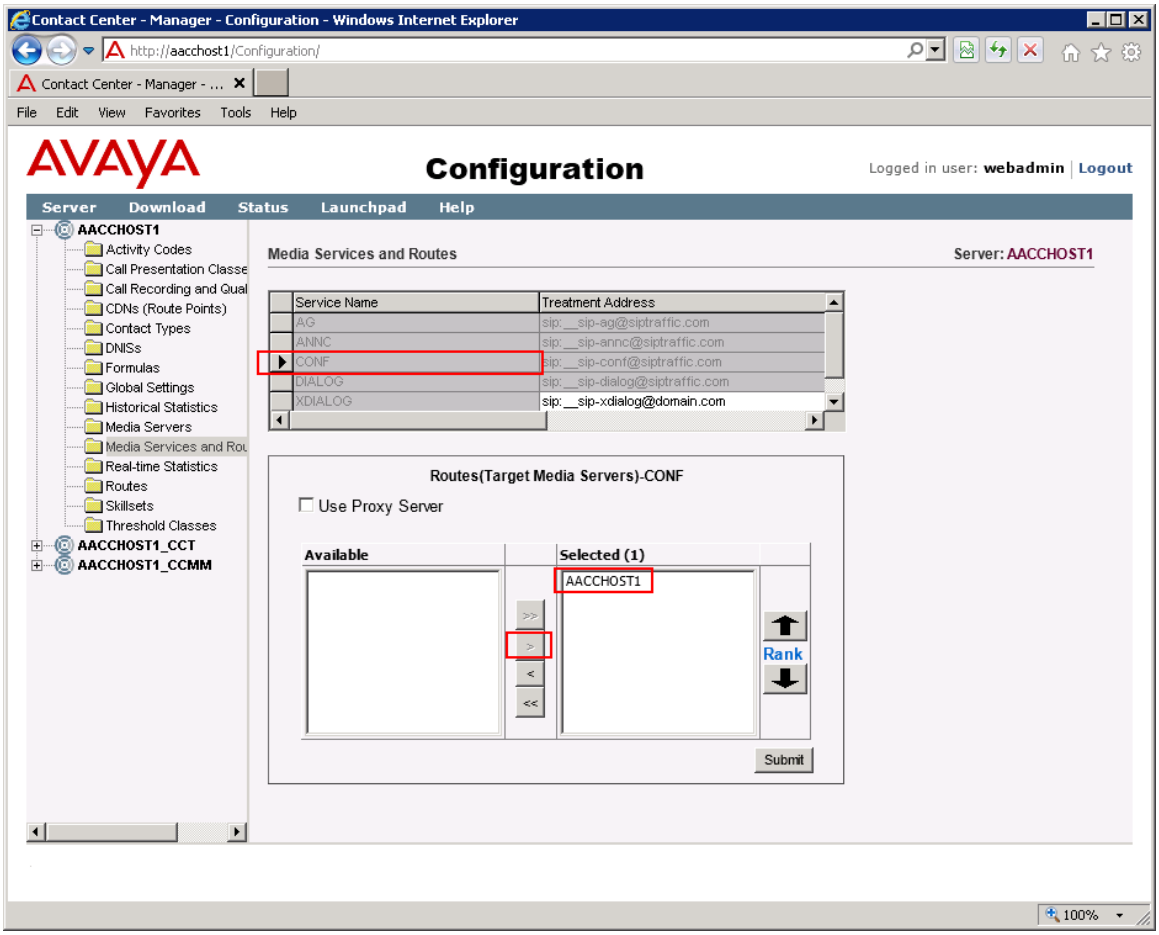
8 Click **Submit**.

9 From the **Service Name** list, select **CONF**.

10 In the **Routes (Target Media Servers)** section, from the **Available** list, select the Avaya Media Server server name. For example, select AACCHOST1.

11 Click the **>** arrow key.

AACCHOST is added to the list of Selected Conference media servers.



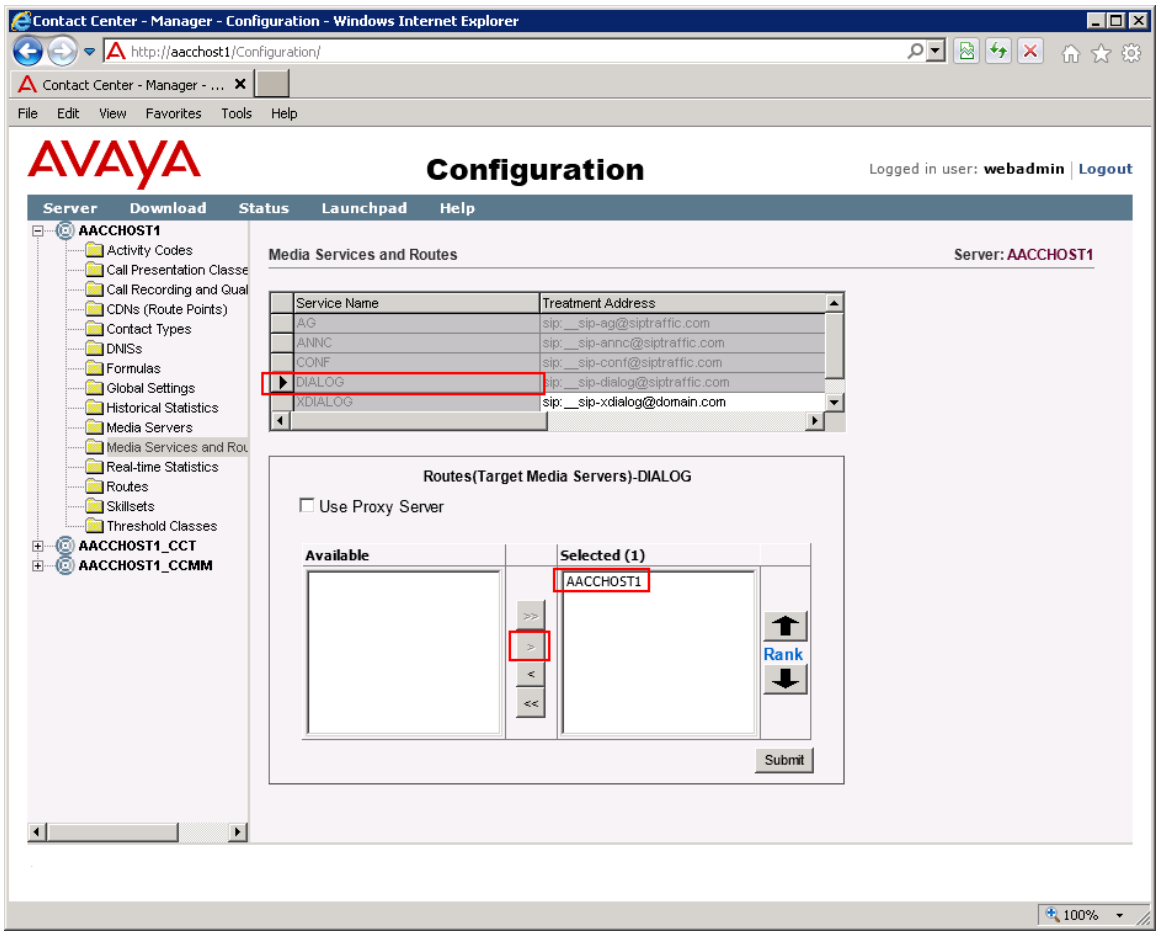
12 Click **Submit**.

13 From the **Service Name** list, select **DIALOG**.

14 In the **Routes (Target Media Servers)** section, from the **Available** list, select the Avaya Media Server server name. For example, select AACCHOST1.

15 Click the **>** arrow key.

AACCHOST1 is added to the list of Selected Conference Dialog media servers.



16 Click **Submit**.

--End--

Editing an activity code

Edit an activity code to change the name or display name of an activity code. You cannot change the activity code number. To change an activity code number, you must delete the activity code, and then create a new activity code with a new number.

An activity code is a number that an agent can enter on a phone to track the time spent on specific activities or service areas, or to track Not Ready reasons. Agents can enter up to three activity codes during a single contact. If the agent enters no activity code, the activity code for the contact is the system default activity code.

- System default activity code—If an agent does not enter an activity code while working on the contact, the system uses the system default activity code.
- Skillset default activity code—If an agent presses the activity code key twice during a contact without entering an activity code, the system uses the skillset default activity code.

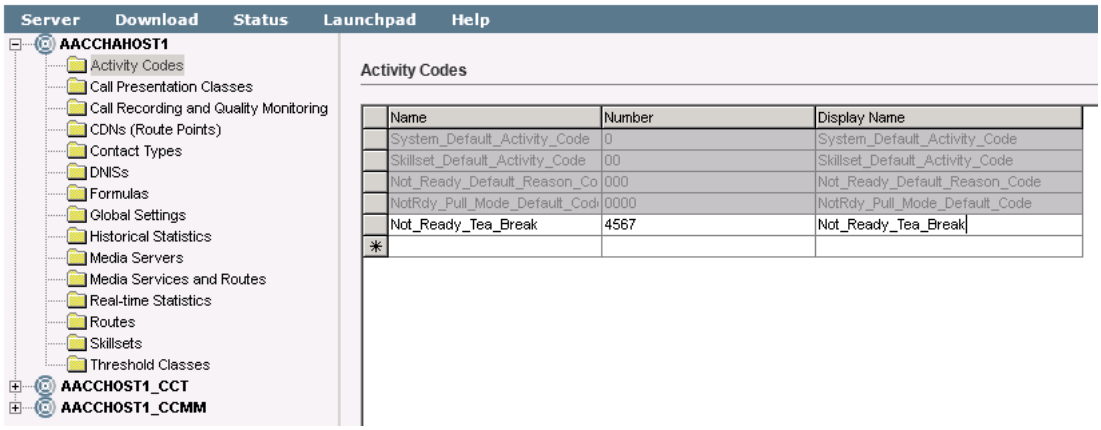
A default activity code is assigned to a contact, if the contact is not queued to a skillset and if no other activity code is assigned.

Prerequisites

- Configure at least one activity code.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration with administrator privileges.
2	On the **Launchpad**, click **Configuration**.
3	In the left pane, expand the server containing the activity code to change. For example, select AACCHOST1. *The server shows its resources.*
4	Select the **Activity Codes** folder.
5	In the right pane, highlight the activity code name to change.
6	In the **Name** box, type the new name. For example, type Not_Ready_Tea_Break.
7	In the **Number** box, type a number of the code. For example, type 4567.
8	In the **Display Name** box, type a display name for the activity code. For example, type Not_Ready_Tea_Break.



9 Click any other row in the table to save your changes.

--End--

Creating a threshold class

Create a threshold class to specify how statistics are treated in reports and real-time displays. You can create threshold classes to distinguish between types of information that the system collects.

For example, you can create different agent threshold classes for customer service trainees and for senior customer service representatives. You can also create different skillset threshold classes for weekday performance and weekend performance.

Prerequisites

Attention: Display thresholds apply to both nodal and network-consolidated real-time displays. Therefore, when you define threshold classes on multiple servers in a networked environment, consider making the values the same on each server. This way, when users launch network-consolidated real-time displays, the threshold conditions shown reflect uniform settings across all servers.

- You must define two values for display thresholds—the low end and the high end of the normal range.

Procedure steps

Step **Action**

1. Log on to Contact Center Manager Administration with administrator privileges.
2. On the **Launchpad**, click **Configuration**.
3. In the left pane, expand the server on which to create the threshold class. For example, select AACCHOST1.

   The server shows its resources.
4. Select the **Threshold Classes** folder.
5. In the right pane, in the **Name** box, type the name of the new threshold class. For example, type Agent_Voice_Template.
6. From the **Type** list, select the threshold class type. For example, type **Agent**.
7. Click any other row in the grid to update the table and submit the threshold class name.

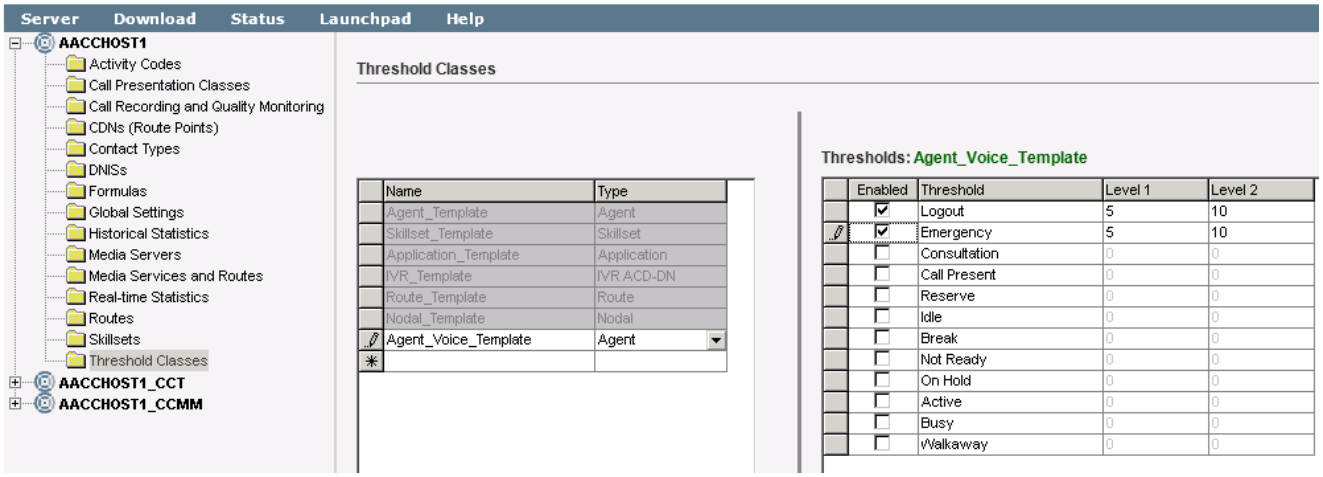
   The Thresholds table appears in the right pane.
8. In the **Enabled** box of the **Thresholds** table, select the check box for each statistic for which to define thresholds.
9. In the **Level 1** box, type the value for the low end of the normal range for display thresholds.
10. For display thresholds only, in the **Level 2** box, type the value for the high end of the normal range.
11. Click any other row in the grid to submit your changes.

--End--

Variable	Value
Level 1 box	The low end of the normal range for display thresholds. For pegging thresholds, enter the cut-off value for this statistic. You must define the service level threshold for both Application and Skillset statistics. However, the values for each type of statistic can be different. The Calls Answered After Threshold value for Skillset statistics is the number of local and incoming network skillset calls answered after a delay greater than or equal to the service-level threshold for this skillset. Delays are calculated from the time the call is queued at the skillset to the time the call is answered.
Type list	The type of threshold class that you can create depends on the type of PABX or server on which you create the threshold classes. You can choose from Agent, Application, Skillset, and Route threshold classes.

Procedure job aid

Threshold Classes define how statistics are treated in reports and real-time displays.



Creating a call presentation class

Create a call presentation class to determine how contacts are presented to an agent's phone.

A call presentation class is a collection of preferences that determines how contacts are presented to an agent. A call presentation class specifies whether a break time between contacts is permitted, whether an agent can place DN calls on hold for incoming ACD calls, and whether an agent phone displays that the agent is reserved for a network call.

- Automatically answer the contact at the agent's phone.
- Return the contact to the queue if the contact is not answered within a specified period.
- Allow the contact to ring at the agent's phone until it is answered or abandoned.

In addition, you can choose whether to present contacts to agents when they are busy on a DN call, and whether to allow the agent time to wrap up a contact after it ends.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration with administrator privileges.
2	On the **Launchpad**, click **Configuration**.

3 In the system tree, expand the server on which to add the call presentation class. For example, expand AACCHOST1.

The server shows its resources.

4 Select the **Call Presentation Classes** folder.

5 In the right pane, in the **Name** box, type the name of the call presentation class as it appears in reports, for example CPC_demo.

6 From the **Presentation Option** list, select the one of the following call presentation options:

- **Return to Queue**
- **Call Force Delay**
- **Let Call Ring**

7 If you selected the **Call Force Delay** presentation option, in the **Call Force Delay Timer** box, type the number of seconds after which the contact is automatically answered at the agent's phone and proceed to step 10.

8 In the **Return to Queue After N Seconds** box, type the time after which the contact returns to the queue if not answered.

9 From the **After Return to Queue, Make Phoneset** list, select the mode in which the phone is placed after the contact returns to the queue.

10 In the **After Call, Break for N Seconds** box, type the amount of time that the agent is in the break state after a call ends.

11 Select the **Answer by Placing DN Call on Hold** check box so that agents can place DN calls on hold to answer Contact Center Manager Server calls. This check box is disabled when on a SIP-enabled server.

12 Select the **Agent Reserved for Network Call** check box to display the message *Reserved* on the agent's phone when the server reserves the agent for a network call.

13 Click any other row in the grid to submit your changes and to save the call presentation class.

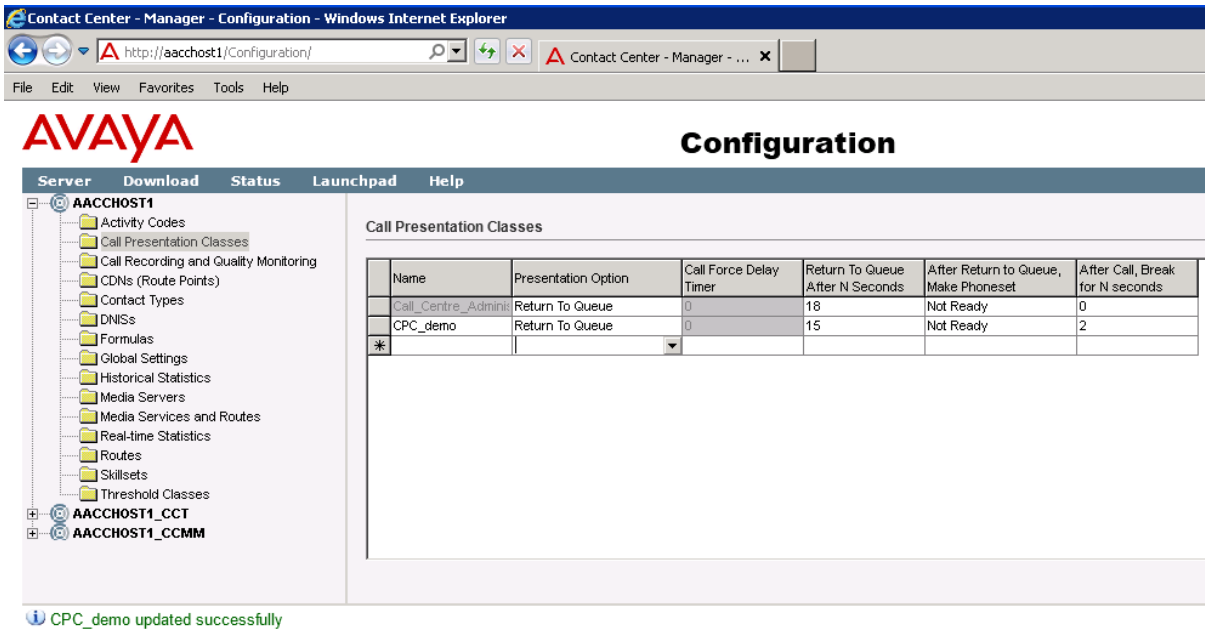
--End--

Variable definitions

Variable	Value
Name box	The name assigned to the call presentation class. Valid values: 30-character maximum (no special characters, no spaces).
Presentation Option list	Select one of the following call presentation options for the call presentation class: • Call Force Delay—Choose this option to force a call on an agent if the agent does not answer the call within the specified amount of time. If you select this option, you must specify the time delay in seconds in the Call Force Delay Timer box. Call Force Delay is not supported for Instant Message contacts in a SIP-enabled contact center. • Return to Queue—Choose this option to return a call to the queue if the agent does not answer the call within the specified amount of time. • Let Call Ring—Choose this option to let the call ring at the phone until the agent answers the call. Let Call Ring is not supported for voice or Instant Message contacts in a SIP-enabled contact center.
Call Force Delay Timer box	If you select Call Force Delay from the Presentation Option list, in the Call Force Delay Timer box, type the time delay in seconds.
Return to Queue After N Seconds box	If you select Return To Queue from the Presentation Option list, in the Return To Queue After N Seconds box, type the wait interval in seconds. If you do not select Return to Queue as the presentation option, the value is N/A.
After Return to Queue, Make Phoneset list	If you select Return To Queue from the Presentation Option list, from the After Return To Queue, Make Phoneset list, select one of the following values: • Logout • Not Ready • N/A
After Call, Break for N Seconds box	The amount of time, in seconds, that an agent is in break state at the end of a call and before the next call. The agent can use this time to complete processing related to the finished call. Valid values: 0–300 (seconds)
Agent Reserved for Network Call check box	Select this check box to display the message *Reserved* on the agent's phone when the server reserves the agent for a network call.

Procedure job aid

Call presentation classes determine how contacts are presented to an agent's phone.



Enabling Multiplicity

Enable Multiplicity to allow agents manage multiple concurrent contacts. Configure multiplicity presentation classes (MPC) in CCMA. Each agent is assigned either the default MPC or a customized MPC. Enable multiplicity in the licensing tab of the Server Configuration utility.

If your contact center is not licensed for Multiplicity, skip this procedure.

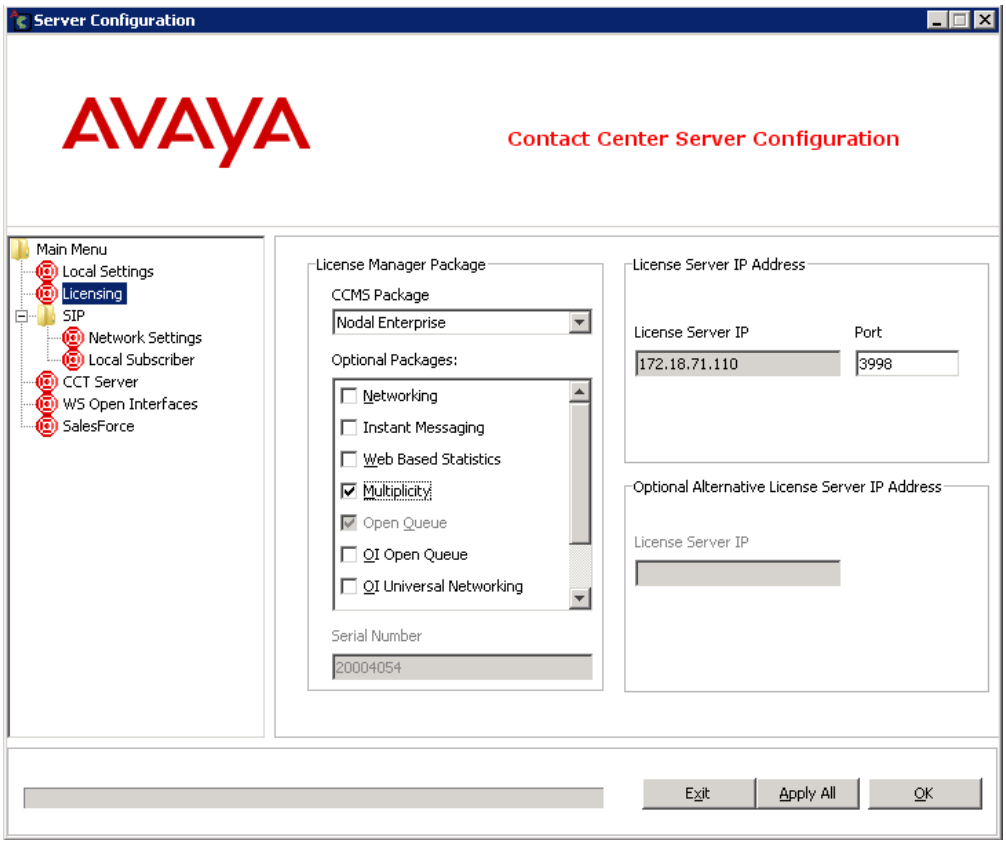
Prerequisites

- Ensure that the Contact Center License Manager is licensed to provide Multiplicity.
- Ensure that the Contact Center License Manager is licensed to provide agent licenses for the required contact types.

Attention: You must restart your server at the end of this procedure.

Procedure steps

Step	Action
1	Log on to the Voice and Multimedia Contact Server.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Manager Server**, **Server Configuration**.
3	Click the **Licensing** tab.
4	From the **Optional Packages** list, select **Multiplicity**.



5	Click **OK**.
6	Click **Yes** to restart the server.

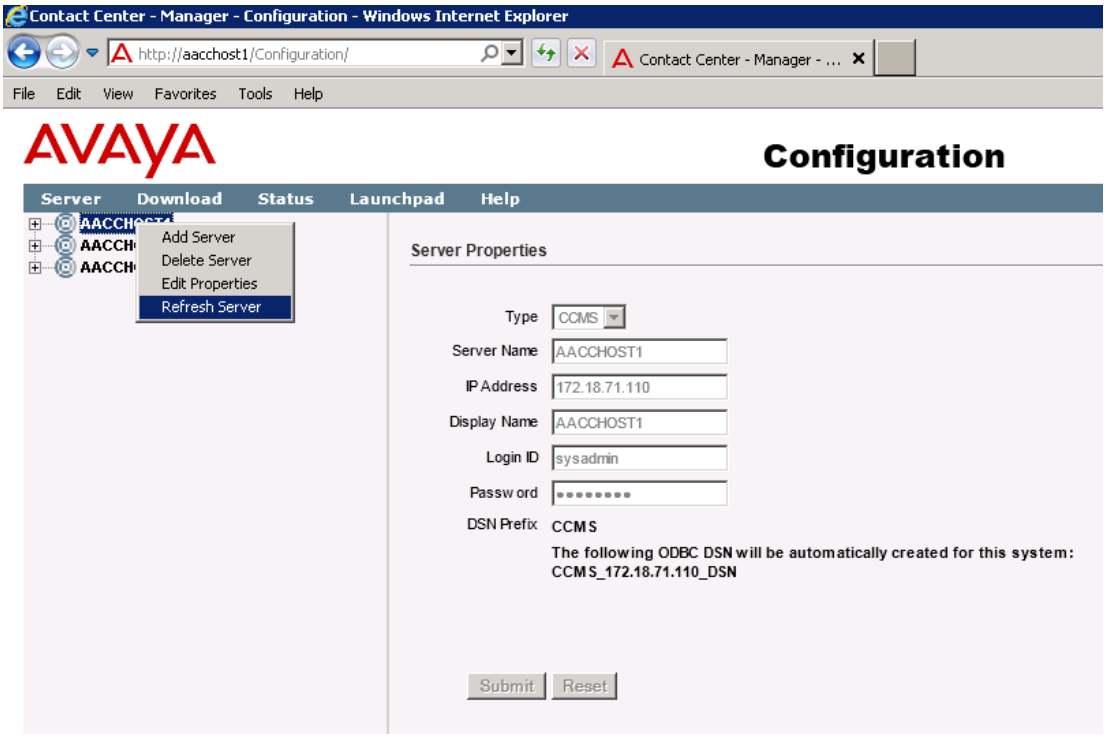
--End--

Refreshing your servers

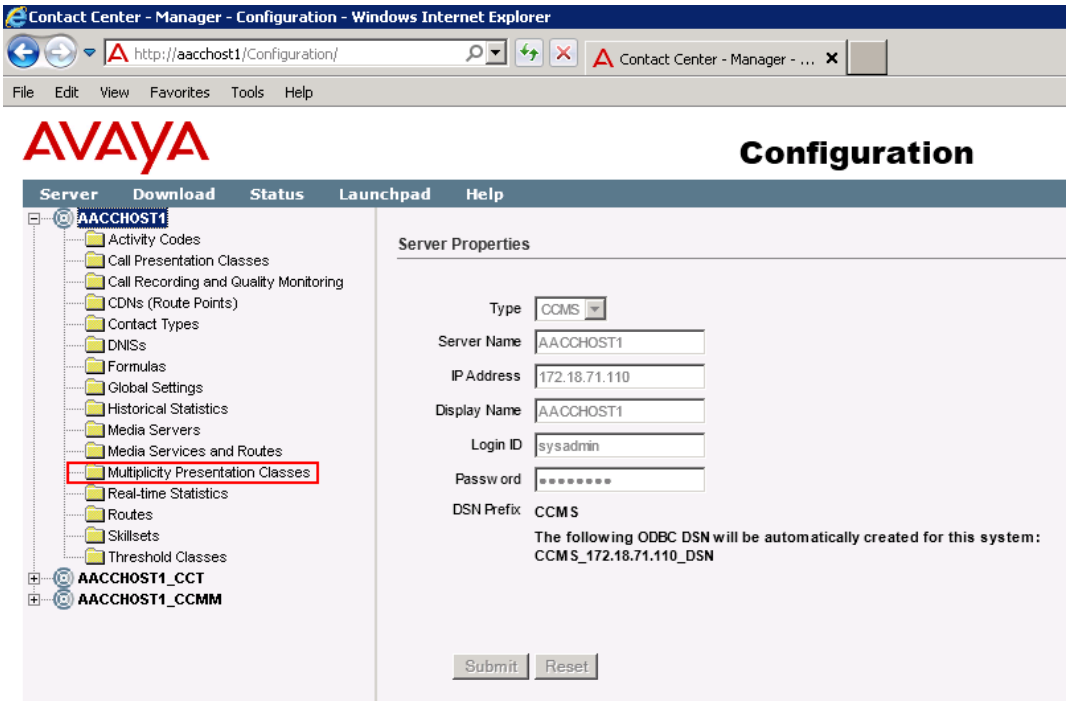
Refresh your servers after you enable a Contact Center Manager Server feature such as Multiplicity.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration with administrator privileges.
2	On the Launchpad, click **Configuration**.
3	In the left pane, select the server to refresh. For example, select AACCHOST1.
4	From the **Server** menu, choose **Refresh Server,** or right-click on the server, and choose **Refresh Server**.



5	In the confirmation window, click **Yes**. *A message box appears stating that you must refresh all browsers attached to Contact Center Manager Administration. If a Contact Center Manager Server feature changes, that change is reflected in the browsers only when you refresh them.*
6	Click **Yes** to refresh the server. *After the Refresh complete, Contact Center Manager Administration displays a message informing you whether the operation was successful.* *The Multiplicity Presentation Class feature is now visible in Contact Center Manager Administration.*


Contact Center - Manager - Configuration - Windows Internet Explorer
http://aacchost1/Configuration/
Contact Center - Manager - ...
File Edit View Favorites Tools Help
AVAYA
Configuration
Server Download Status Launchpad Help
AACCHOST1
Activity Codes
Call Presentation Classes
Call Recording and Quality Monitoring
CDNs (Route Points)
Contact Types
DNISs
Formulas
Global Settings
Historical Statistics
Media Servers
Media Services and Routes
Multiplicity Presentation Classes
Real-time Statistics
Routes
Skillsets
Threshold Classes
AACCHOST1_CCT
AACCHOST1_CCMM
Server Properties
Type CCMS
Server Name AACCHOST1
IP Address 172.18.71.110
Display Name AACCHOST1
Login ID sysadmin
Password
DSN Prefix CCMS
The following ODBC DSN will be automatically created for this system:
CCMS_172.18.71.110_DSN
Submit Reset

--End--

Creating a Multiplicity Presentation Class

Create a Multiplicity Presentation Class (MPC) to determine how an agent using Avaya Aura® Agent Desktop can work with multiple contacts at one time. Use a multiplicity presentation class to specify the following:

- which contact types to present to the agents
- the maximum number of active contacts an agent has at one time by contact type or skillsets
- whether voice contacts can interrupt Multimedia contacts
- whether Multimedia contacts are presented while agent is on a voice call

If your contact center is not licensed for Multiplicity, skip this procedure.

Multiplicity allows an agent can handle multiple concurrent contacts. At any one time an agent can be active on a voice and multimedia contact; only one of these can be active, the others automatically are on hold.

Multiplicity is configured and assigned to agents using Multiplicity Presentation Class (MPC). A MPC is a collection of multiplicity configuration options. Every agent must be assigned an MPC. A default MPC is not modifiable and allows an agent handle a single contact.

Multiplicity is a licensed feature.

Procedure steps

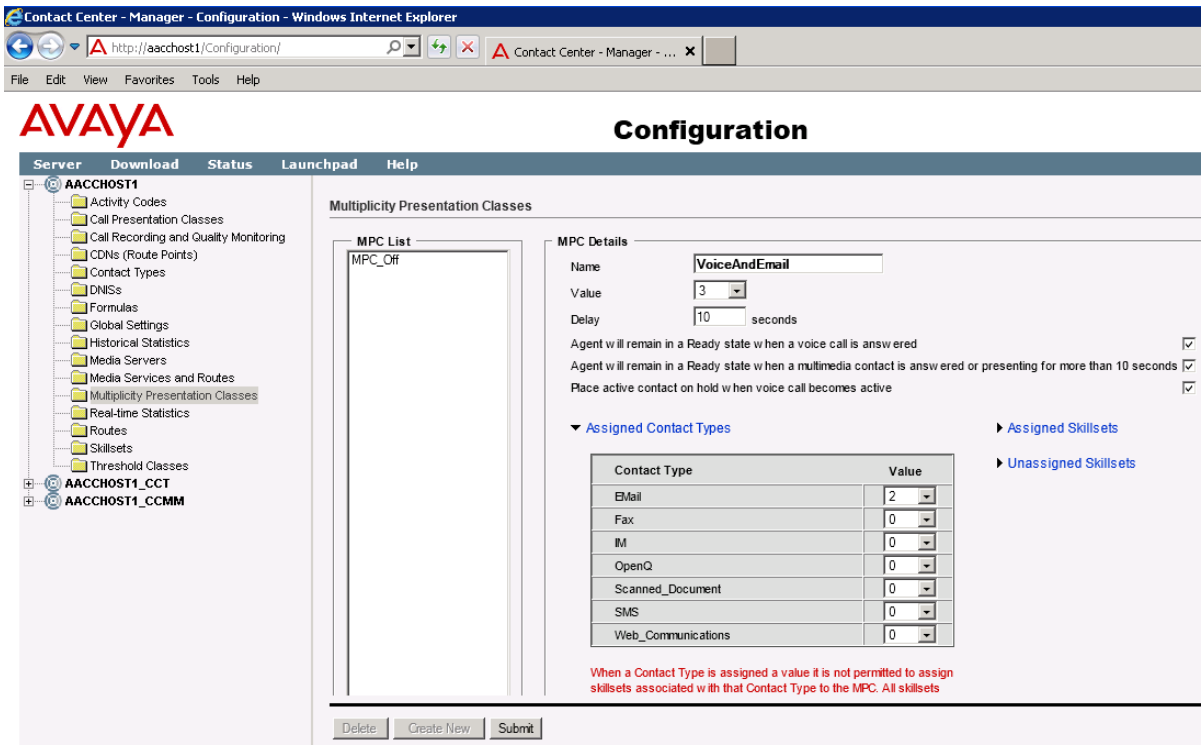
Step	Action
1	In the system tree, expand the server on which to add the Multiplicity presentation class. *The server resources appear.*
2	Select the **Multiplicity Presentation Classes** folder.
3	In the right pane, click **Create New**.
4	In the **Name** box, type the name of the new Multiplicity Presentation Class. For example, type VoiceAndEmail.
5	From the **Value** list, select the maximum number of contacts that an agent using this MPC is allowed to have active at one time. For example, select 3.
6	In the **Delay** box, type a delay in seconds that occurs between each contact presented to the agent.
7	To allow agents using this MPC to receive multimedia contacts while they are active on voice contacts, select **Agent will remain in a Ready state when a voice call is answered**.
8	To allow agents using this MPC to receive voice contacts while they have active multimedia contacts, select **Agent will remain in a Ready state when**

a multimedia contact is answered or presenting for more than 10 seconds.

9 Select **Place active contact on hold when voice call becomes active** to set the active multimedia contact on hold when the agent accepts a presenting voice contact.

10 In the **Assigned Contact Types** list, use the **Value** list for each contact type to specify the maximum number of contacts from each contact type that the agent can have active at one time.

11 For example, from the **EMail** list select 2.



12 Click **Submit** to submit your changes and to save the multiplicity call presentation class.

--End--

Variable definitions

Variable	Value
Name	The name assigned to the multiplicity presentation class. Valid value: 30-character maximum (no special characters, no spaces).
Value	Select the maximum number of contacts that an agent can keep active at one time on Agent Desktop. When the agent reaches this limit, the contact center does not present any more contacts to them until the agent closes a contact.
Delay	The time that the contact center waits between sending contacts to the agent. This prevents the agent from receiving multiple simultaneous contacts. If an agent configured with this MPC also has a call presentation class with a value for After Call Break for N Seconds, Contact Center Manager Server uses the greater of the two values between contacts. Valid values: 10-300.
Agent will remain in a Ready state when a voice call is answered	Select to allow the agent to receive multimedia contacts while they are on a voice call.
Agent will remain in a Ready state when a multimedia contact is answered or presenting for more than 10 seconds	Select to allow the agent to receive a voice call while they are working on a Multimedia contact.
Place active contact on hold when voice call becomes active	Select to set the active multimedia contact on hold when the agent accepts a presenting voice call, allowing the agent to focus on the voice contact.
Assigned Contact Types	Lists the contact types that you can include in the multiplicity presentation class.
Assigned Contact Types–Value	Select the maximum number of contacts of this contact type that the agent can have active on Agent Desktop. These lists automatically have a maximum value equal to the number set in the Value field. The cumulative total of the values you select for all contact types does not impact the overall maximum number of contacts as set in the Value field.
Assigned Skillsets	Displays skillsets selected for this multiplicity presentation class.

(1 of 2)

Variable	Value
Assigned Skillsets –Value	Select the maximum number of contacts from this skillset that the agent can have active on Agent Desktop. These lists automatically have a maximum value equal to the number set in the Value field. The cumulative total of the values you select for all contact types does not impact the overall maximum number of contacts as set in the Value field.
Unassigned Skillsets	Allows you to search for and select skillsets to assign to this multiplicity presentation class. You can only select skillsets if there is a zero value for their corresponding contact type in the Assigned Contact Types list. The skillsets you select appear in the Assigned Skillset list when you click Submit.
Skillset name	The drop down list allows you to specify a search option. The text box allows you to specify the text for which to search the CCMS skillsets.
Search	Initiate a search of the CCMS skillset list using the criteria in the Skillset Name fields. Matching skillsets display in a list below. You can only select skillsets if there is a zero value for their corresponding contact type in the Assigned Contact Types list.
List All	Display the complete CCMS skillset list. You can only select skillsets if there is a zero value for their corresponding contact type in the Assigned Contact Types list.
Delete	Delete the selected multiplicity presentation class. You can delete only an updated or completed multiplicity presentation class.
Create New	Create a new multiplicity presentation class.
Submit	Save changes to the selected multiplicity presentation class.

(2 of 2)

Adding a skillset for voice contacts

A skillset is the ability or group of abilities necessary to answer a specific type of contact. Skillsets are the basic building blocks of skill-based routing. Skillsets are used to match callers with the agents who can best meet the callers' needs.

Prerequisites

- Define the activity code to be assigned as the default activity code for the skillset if you do not want to use system-defined default.
- Define the threshold class to assign to this skillset, if you do not want to use the default threshold class.
- Define the Contact Type to assign to this skillset, if you do not want to use the default Contact Types. This is applicable only if Open Queue is enabled on the Contact Center Manager Server.

Procedure steps

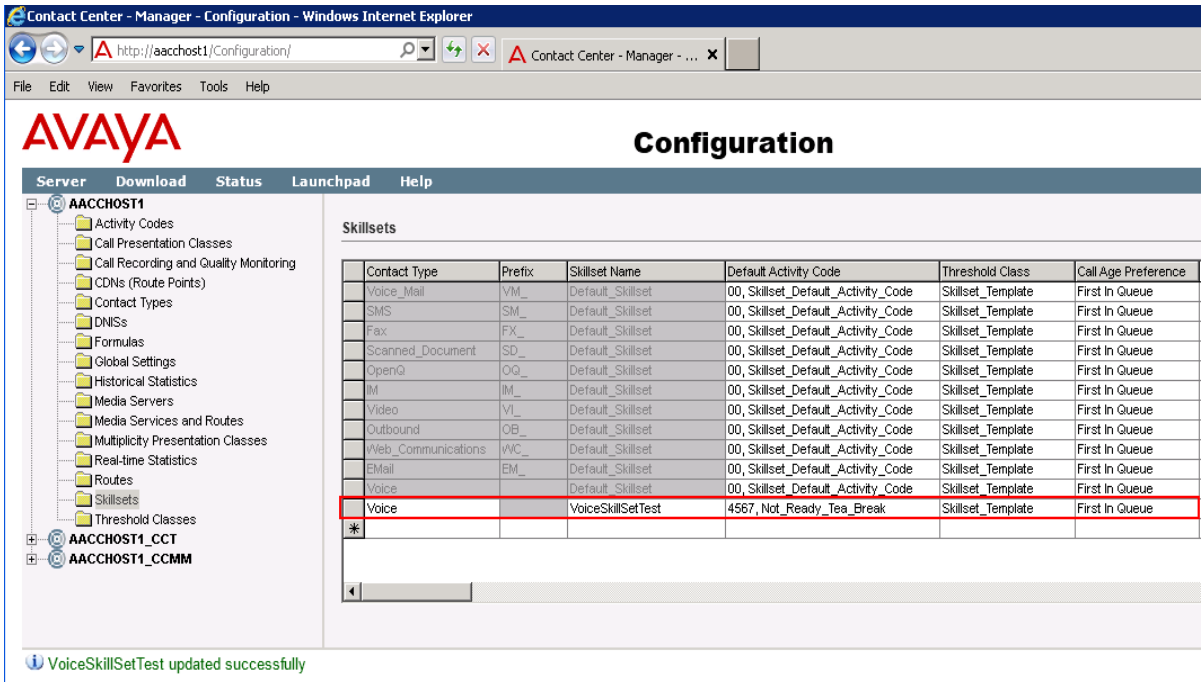
Step	Action
1	Log on to Contact Center Manager Administration with administrator privileges.
2	On the **Launchpad**, click **Configuration**.
3	In the left pane, expand the server to which to add the skillset. For example, expand AACCHOST1.
4	Select the **Skillsets** folder.
5	Select a value from the **Contact Type** drop-down list. CCMA automatically populates the **Prefix** field with the appropriate skillset name prefix. Select the **Voice** type.
6	In the **Skillset Name** box, type a name for the skillset, for example enter **VoiceSkillSetTest**.
7	From the **Default Activity Code** list, select the activity code that is registered whenever this skillset is used, for example Not_Ready_Tea_Break.
8	From the **Threshold Class** list, select the threshold class associated with this skillset, for example Skillset_Template.
9	From the **Call Age Preference** list, select the method to configure the order of contacts in the queue. If you want priority given to the oldest contact in the system, select **Oldest**. If you want to give priority to the first contact in the queue, select **First In Queue**.
10	In the **Target Service level** field, enter target service level threshold value.
11	Select the **Service Level Routing** check box. You can enable Service Level Routing enhancement by selecting the Service Level Routing check box and setting a valid Target Service Level value.

Attention: At least one agent within the range of normal priorities to the skillset and one agent within the range of standby skillset must be assigned in order to enable Service Level Management enhancement.

12	Optionally, in the **Comment** box, type any comments you have about the skillset.
13	Click any other row in the grid to save your changes.

--End--

Procedure job aid



Adding a skillset for email contacts

A skillset is the ability or group of abilities necessary to answer a specific type of contact. Skillsets are the basic building blocks of skill-based routing. Skillsets are used to match callers with the agents who can best meet the callers' needs.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration with administrator privileges.
2	On the **Launchpad**, click **Configuration**.
3	In the left pane, expand the server to which to add the skillset. For example, expand AACCHOST1.
4	Select the **Skillsets** folder.
5	Select a value from the **Contact Type** drop-down list. CCMA automatically populates the **Prefix** field with the appropriate skillset name prefix. Select the **Email** type.

6 In the **Skillset Name** box, type a name for the skillset, for example enter **EmailSkillSetTest**.

7 From the **Default Activity Code** list, select the activity code that is registered whenever this skillset is used, for example Not_Ready_Tea_Break.

8 From the **Threshold Class** list, select the threshold class associated with this skillset.

9 From the **Call Age Preference** list, select the method to configure the order of contacts in the queue. If you want priority given to the oldest contact in the system, select **Oldest**. If you want to give priority to the first contact in the queue, select **First In Queue**.

10 In the **Target Service level** field, enter target service level threshold value.

11 Select the **Service Level Routing** check box.

You can enable Service Level Routing enhancement by selecting the Service Level Routing check box and setting a valid Target Service Level value.

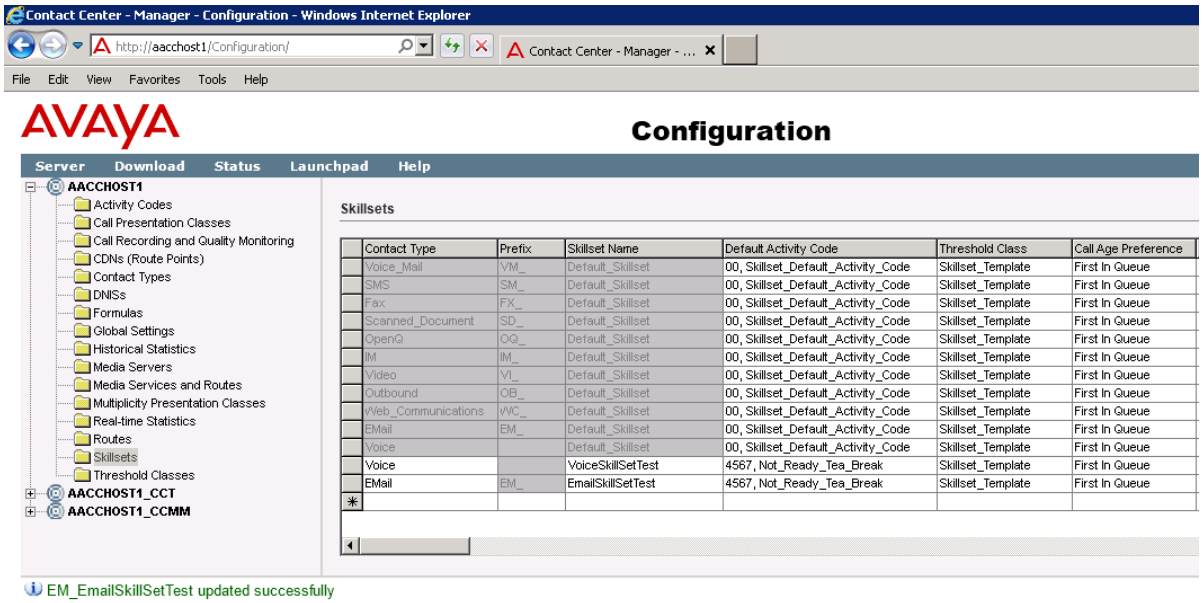
Attention: At least one agent within the range of normal priorities to the skillset and one agent within the range of standby skillset must be assigned in order to enable Service Level Management enhancement.

12 Optionally, in the **Comment** box, type any comments you have about the skillset.

13 Click any other row in the grid to save your changes.

--End--

Procedure job aid



Editing a contact type

Edit a contact type to change the description of the contact type or to change the default skillset assigned to that contact type.

Contact types are the media types by which (inbound) contacts arrive into a contact center and by which a contact center sends (outbound) contacts.

A contact type determines how a contact center handles contacts. An example is email message: when a contact center customer sends an email message, the contact center receives the message, and routes the message according to various email-specific rules. If required, an agent with email ability processes the email message.

Note the following:

- You cannot delete a default contact type.
- You cannot edit the contact type name or the skillset prefix.
- You cannot edit a contact type if a skillset or an agent is associated with it.

The following table lists the default contact types.

Contact types

Default Contact Type	Skillset Prefix	Description	Supported on
Voice	—	Default Voice Contact Type	Open Queue-enabled Contact Center Manager Server SIP-enabled Contact Center Manager Server
E-mail	EM_	Default CCMM email Contact Type	Open Queue-enabled Contact Center Manager Server

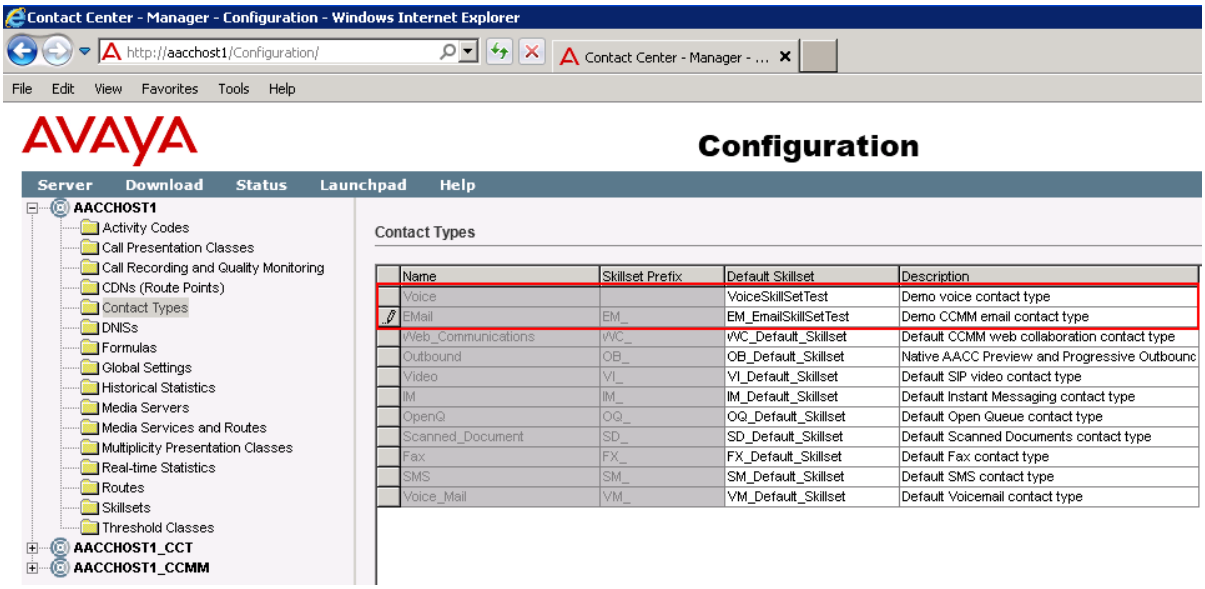
Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration with administrator privileges.
2	On the **Launchpad**, click **Configuration**.
3	In the left pane, expand the server on which to edit the contact type. For example, expand AACCHOST1.
4	Select the **Contact Types** folder.
5	In the right pane, select the **Contact Type** to edit. For example, select the Voice or EMail contact types.
6	To sort the contact types, click a column header.

For example, if you click the **Name** column header, the contact types are sorted alphabetically, according to Contact Type name.

7 From the **Default Skillset** list, select a new default skillset, and then press **Tab**. For example, edit the default skillset for the Voice or EMail contact type. You can select the **VoiceSkillSetTest** skillset or the **EmailSkillSetTest** skillset.

8 In the **Description** box, type a new description for the contact type.



9 Click any other row in the grid to save your changes.

--End--

Variable definitions

Variable	Value
Name	The name used to identify the Contact Type. **Attention:** You cannot modify Contact Type names.
Skillset Prefix	The prefix that identifies the default skillset that handles contacts of this Contact Type. There is no Skillset Prefix for the default Contact Type, Voice. Skillsets without a Skillset Prefix default to Contact Type, Voice. Valid value: 3-character maximum, the last of which must be an underscore (_) (no special characters, must be unique) **Attention:** You cannot modify a Skillset Prefix for a default Contact Type.

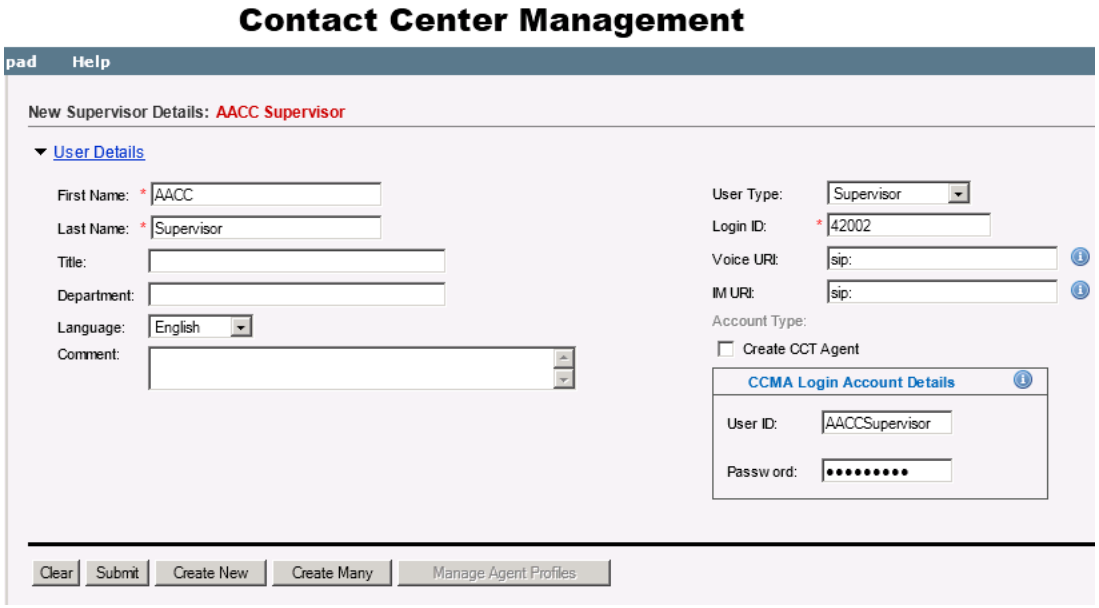
Variable	Value
Default Skillset	Select the skillset to which Contacts route for processing, when they are not handled in a script. Valid values: 30-character maximum, no special characters allowed. **Attention:** This field is optional and must be unique. You must first configure the Default Skillset in Contact Center Manager Administration. The Default Skillset must have the same Skillset Prefix as the Contact Type.
Description	The description for the Contact Type. Valid value: Maximum 60 characters (optional, can be updated, special characters are allowed).

Adding a supervisor

Complete this procedure in Contact Center Management to add a supervisor to a contact center. You must add a supervisor before you add an agent.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration with administrator privileges.
2	On the **Launchpad**, click **Contact Center Management**.
3	In the left pane, click the Contact Center Manager Server under which to add the agent. For example, expand AACCHOST1.
4	From the **Add** menu, select **Supervisor**.
5	In the **New Supervisor Details** window, in the **Login ID** box, type the supervisor login identity number. For example, type 42002.
6	In the **First Name** box, type the first name for the supervisor.
7	In the **Last Name** box, type the last name for the supervisor.
8	In the **CCMA Login Account Details** section, in the **User Name** box, type the supervisor logon name for CCMA.
9	In the **CCMA Login Account Details** section, in the **Password** box, type the supervisor logon password for CCMA.
10	Click **Submit** to save your changes.



--End--

Adding an agent

Complete this procedure to add an agent in Contact Center Management.

In the Agents view, you can search for particular agents or list all agents on a server. You can also use the agents view to:

- view and edit the agents' properties, including the skillsets and partitions to which the agents are assigned
- delete the agents from the server one at a time or in bulk
- quickly create a new agent by copying a current agent's properties
- quickly create many new agents by importing a CSV file
- associate an agent with a Communication Control Toolkit user

To open the agents view, select View/Edit, Agents. Select a server in the system tree to log onto the server and work with the configured agents.

Partly configured agents appear in the Contact Center Management Agents list with a grey agent icon. You can delete only these agents.

Two types of agents are available in Contact Center Management:

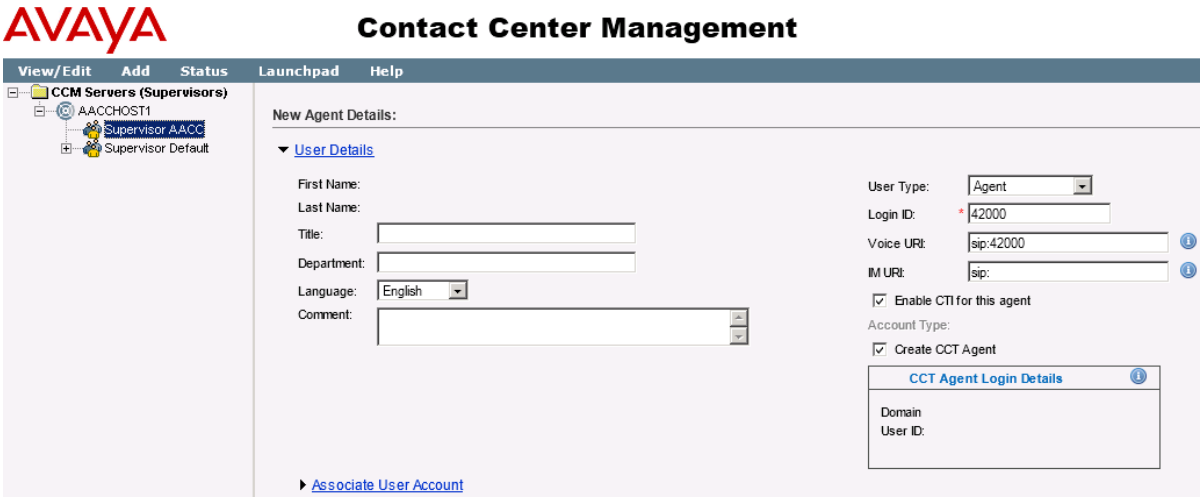
- Agents
- Supervisor/agents

Prerequisites

- Ensure that you have a domain user account on your contact center domain with privileges to list the domain users.
- Ensure that you have created the Windows domain account for the agent, for example siptraffic\AACC_Agent1. For more information about creating domain user accounts for agents, see Domain Administrator requirements (page 45).

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration with administrator privileges.
2	On the **Launchpad**, click **Contact Center Management**.
3	In the left pane, click the Contact Center Manager Server under which to add the agent. For example, expand AACCHOST1.
4	From the **Add** menu, select **Agent**.
5	In the **New Agent Details** window, from the **User Type** list, select Agent.
6	In the **Login ID** box, type the agent login identity number. For example, type 42000.
7	In the **Voice URI** box, type the SIP address of the TR87-controlled terminal dedicated to this agent. For example, type sip:42000@siptraffic.com.
8	Select **Enable CTI for this agent**.
9	Select **Create CCT Agent**.



10 Expand **Associate User Account**.

11 Select **Search domain users**.

12 In the **Server IP (or DNS)** box, type the Domain Controller server IP address. For example, type 172.18.71.252.

13 Select **Specify Domain Account**.

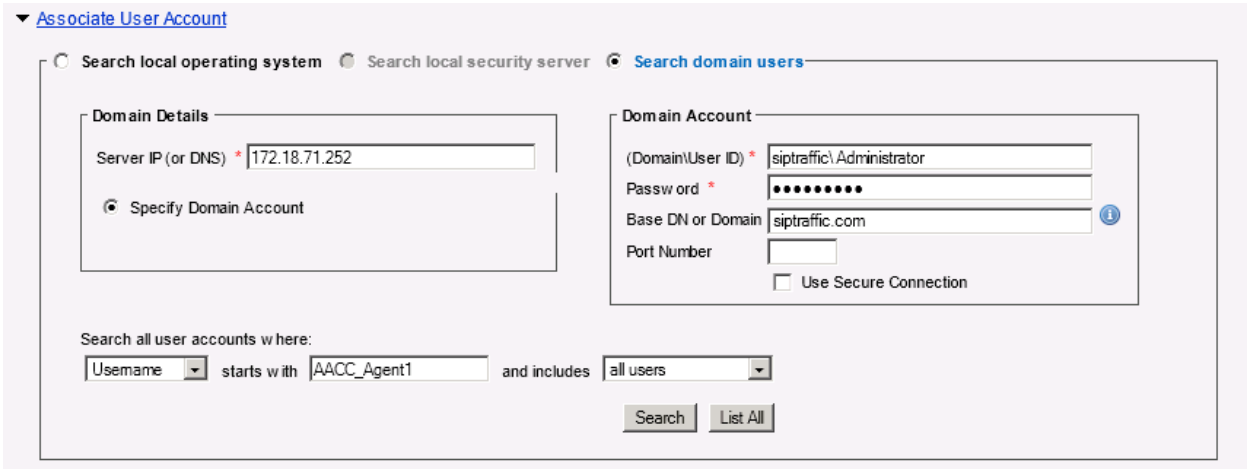
14 In the **Domain Account** section, in the **(Domain\User ID)** box, type a network login identity with administrative rights. For example, type siptraffic\Administrator.

15 In the **Domain Account** section, in the **Password** box, type the password for the administrator account.

16 In the **Domain Account** section, in the **Base DN or Domain** box, type the domain name. For example, type siptraffic.com

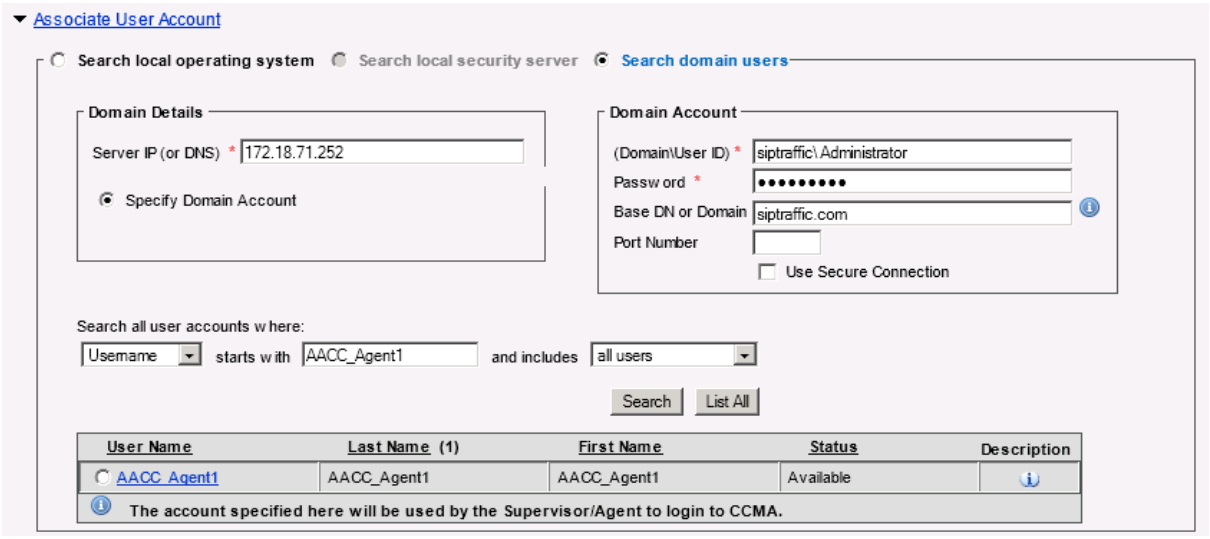
17 From the **Search all user accounts where** list, select **Username**.

18 In the **starts with** box, type the agent user account name. For example, type AACC_Agent1.



19 Click **Search**.

20 From the list of **Users**, select the agent account, by selecting the corresponding check box in the **User Name** column.



21 In the **Agent Information** section, from the **Primary Supervisor** list select a supervisor, for Supervisor AACC.

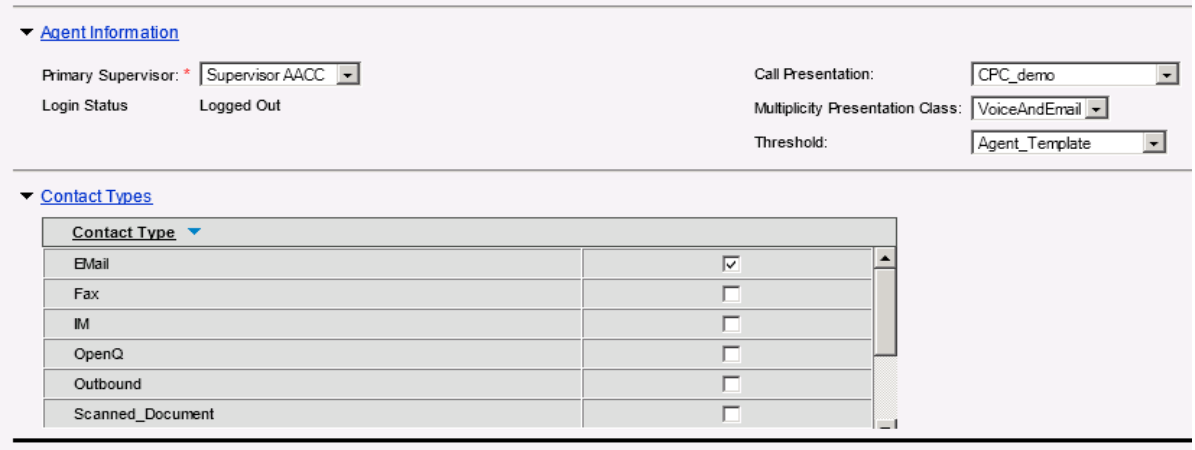
22 From the **Call Presentation** list, select a Call Presentation Class, for example CPC_demo.

23 From the **Multiplicity Presentation Class** list, select a Multiplicity Presentation Class, for example VoiceAndEmail.

24 From the **Threshold** list, select a Threshold Class, for example Agent_Template.

25 Expand **Contact Types**.

26 From the **Contact Type** list, select **EMail** and **Voice**.



27 Expand **Skillsets**.

28 Expand **Assign Skillsets**.

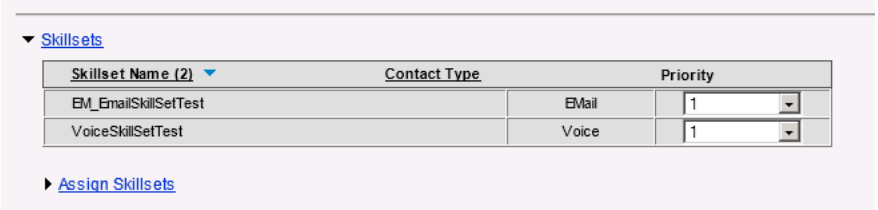
29 In the **Skillsets** area, click **List All** to list all skillsets configured on the server.

30 For each skillset, select the appropriate priority level, from the **Priority List** to assign to the agent, or select **Standby** to put the agent in the standby mode for this skillset.

Priority levels range from 1 to 48, with 1 being the highest priority for the skillset.

31 For the **VoiceSkillSetTest** skillset, select a **Priority** of **1**.

32 For the **EM_EmailSkillSetTest** skillset, select a **Priority** of **1**.



33 Click **Submit** to save your changes.

--End--

Multimedia commissioning

The Contact Center Multimedia server supports multimedia contacts. To manage the multimedia contacts, you must configure general administrator settings and global routing options.

The Contact Center Multimedia Administrator application has settings that you can use to configure properties in the Avaya Aura® Agent Desktop to help the agents access database information and work with contacts.

Use this chapter to set up your contact center with the optional configurations for routing email contacts, to fulfill your customer requirements.

When you commission your contact center, you configure the email server, a default email skillset, and a default recipient with at least one rule group. The default settings ensure email messages go only to agents with the ability to handle email messages. You can customize your contact center with additional skillsets, rule groups, and email servers.

To further enhance your customer service, you can configure routing tools to use in rule groups. Use keyword groups and sender groups to decide how to route contacts. Configure which skillset and priority the email contact is assigned to based on the input for routing contacts. Use automatic suggestions for the agent to reply quickly to an email or automatic responses to send a reply to the customer without agent interaction. You can close the contact immediately after sending the automatic response. This chapter describes how to configure all optional routing tools.

You can configure outbound email settings, such as which skillset to use as a reply address and a list of email addresses that must not receive automatic responses. For each skillset you use to route contacts, you can have a signature with your corporate branding or special information based on the skillset.

Other types of contacts generate email messages that are routed using the inbound and outbound email options.

You can configure general email settings to minimize space and format special characters for other languages.

Perform the procedures in this chapter to configure the Agent Desktop settings.

Prerequisites for general configuration

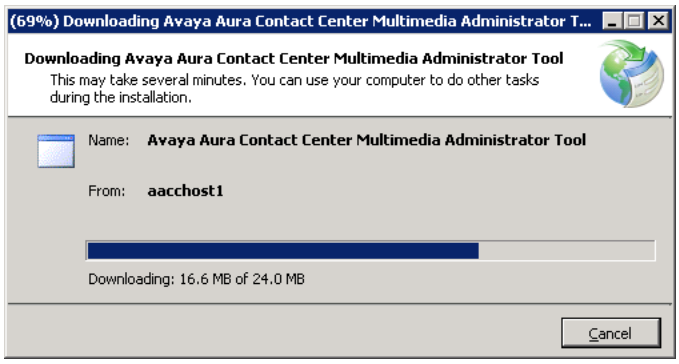
- Log on to the Contact Center Manager Administration application.

Logging on to the Multimedia Administration tool for the first time

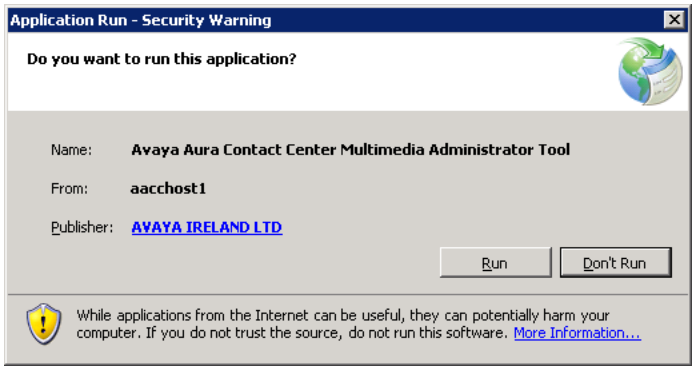
Log on to the Contact Center Multimedia Administration tool to configure the Contact Center Multimedia administration tool. The Contact Center Multimedia Administration application is launched from the Contact Center Manager Administration Web client.

Procedure steps

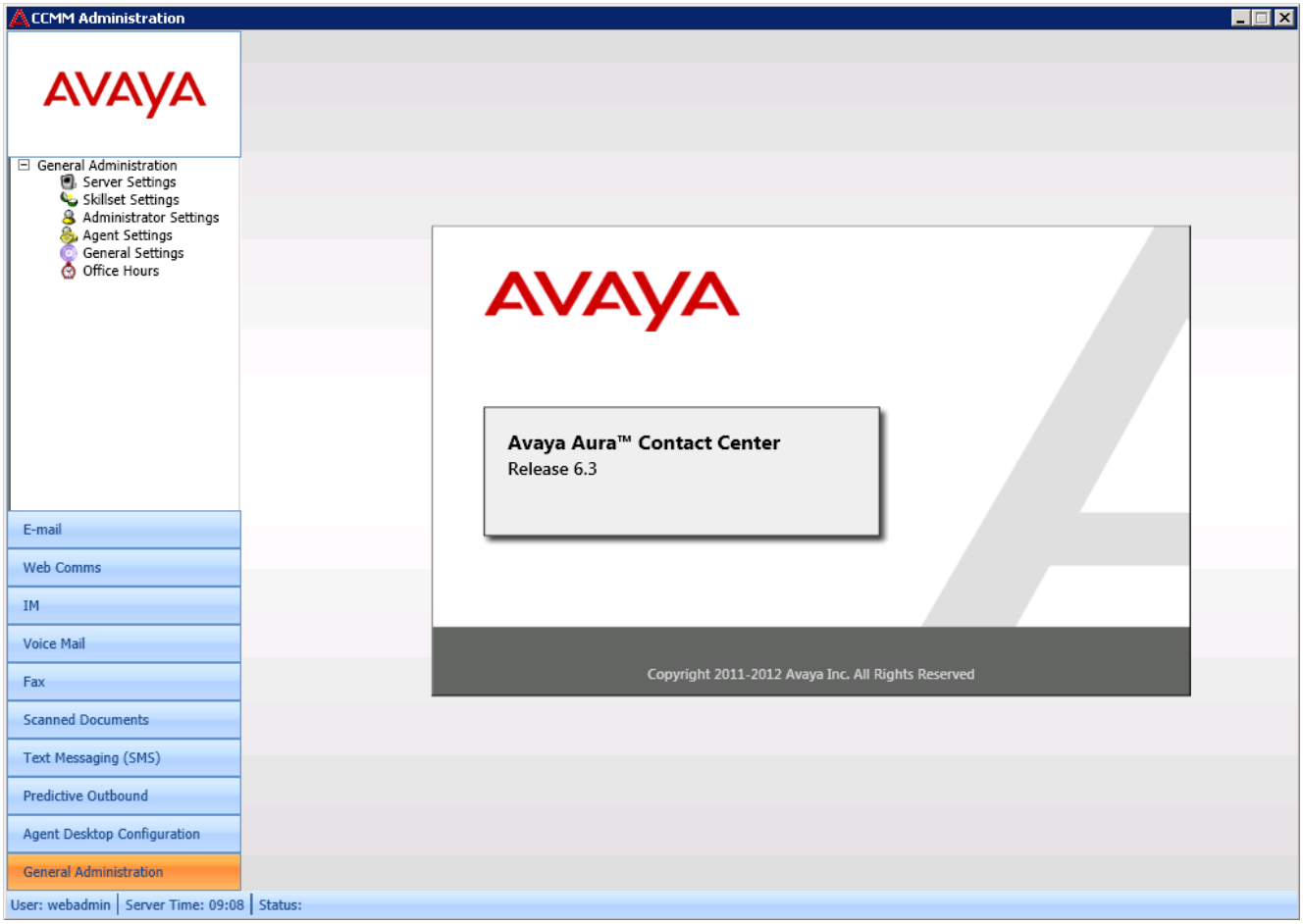
Step	Action
1	Log on to the Voice and Multimedia Contact Server.
2	Start Internet Explorer.
3	Log on to Contact Center Manager Administration with administrative privileges.
4	On the **Launchpad**, click **Multimedia**.
5	In the left pane, select AACCHOST1_CCMM.
6	Select **Install Prerequisite Software**, and click **Launch Multimedia Client**. *It takes some time for the prerequisites to install.*
7	On the Internet Explorer window, click **Run**. *The Contact Center Multimedia Administration tool appears.*



Step	Action
8	As the CCMM **Administrator Tool** downloads, you may see the following message box. If this message box appears, click **Run**.



9 The CCMM Administration tool downloads to your CCMA client computer and opens.



--End--

Verifying the server settings

Configure the Contact Center application servers. The default server settings are configured when installing Contact Center Multimedia.

The following server types appear by default, since the install required the details for these servers:

- Contact Center Manager Server
- Communication Control Toolkit

- Contact Center Manager Administration
- Inbound POP3 Sever
- Outbound SMTP Server

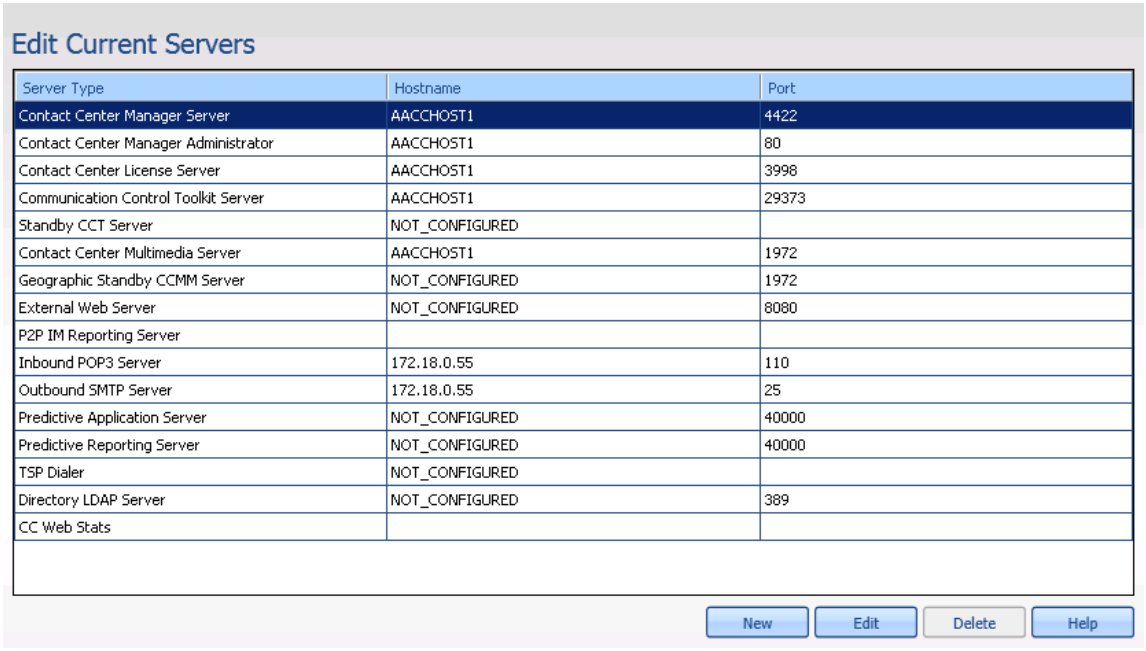
Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration with administrator privileges.
2	On the **Launchpad**, click **Multimedia**.
3	In the left column, select the Multimedia server on which you want to configure server settings. Select AACCHOST1_CCMM.
4	In the right pane, click **Launch Multimedia Client**. *The CCMM Administration Tool opens.*
5	In the left column of the CCMM Administration Tool, select **General Administration**.
6	Click **Server Settings**.
7	Verify the server settings matched your selection during Contact Center Multimedia installation.
8	If any of the server settings do not match, click **Edit** to change the settings.

--End--

Procedure job aid

The Server Settings window lists the servers with which the Contact Center Multimedia communicates.



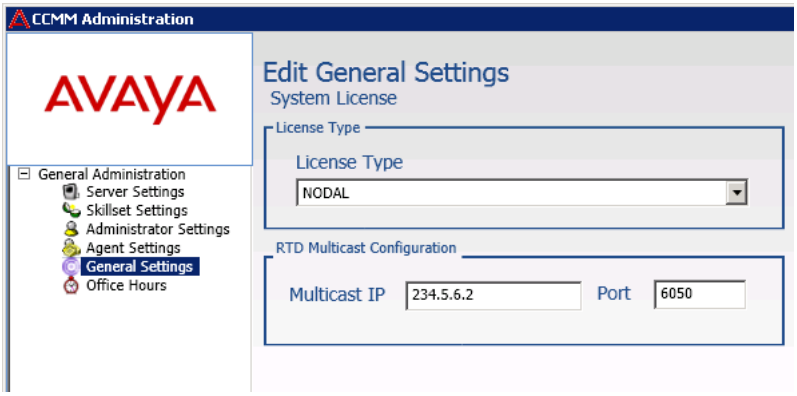
Configuring the multimedia license type

Configure the license type for the Contact Center Multimedia server. The license you choose must match the system license purchased for your contact center.

Nodal licensing is for single sites of Contact Center; corporate licensing enables multiple sites.

Procedure steps

Step	Action
1	Log on to the Voice and Multimedia Contact Server.
2	Start Internet Explorer.
3	Log on to Contact Center Manager Administration with administrative privileges.
4	On the **Launchpad**, click **Multimedia**.
5	In the left column, select the Multimedia server on which you want to configure server settings. Select AACCHOST1_CCMM.
6	In the right pane, click **Launch Multimedia Client**. *The CCMM Administration Tool opens.*
7	In the left column, click **General Administration**.
8	Click **General Settings**.
9	Under **License Type**, select the type of license used in your contact center. Select **NODAL**.



10	Click **Save**.

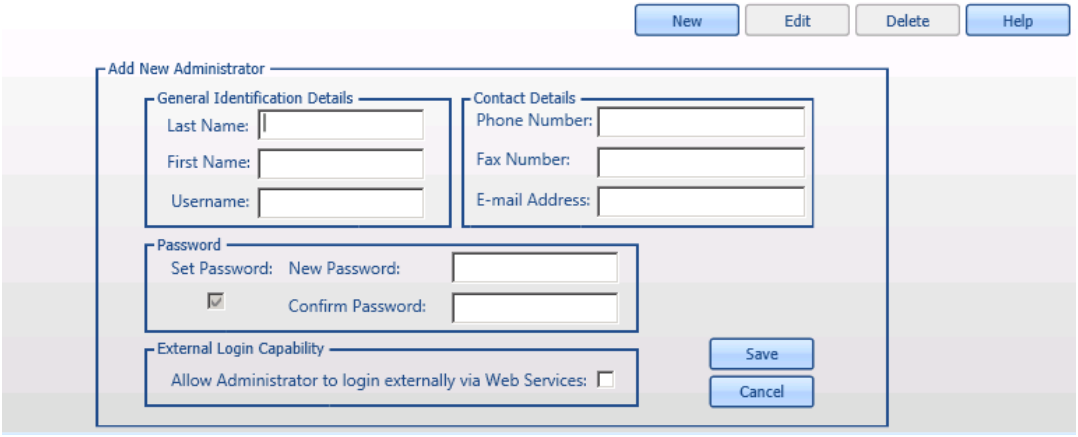
--End--

Configuring CCMM administrators

Configure an additional Contact Center Multimedia administrator.

Procedure steps

Step	Action
1	Log on to the Voice and Multimedia Contact Server.
2	Start Internet Explorer.
3	Log on to Contact Center Manager Administration with administrative privileges.
4	On the **Launchpad**, click **Multimedia**.
5	In the left column, select the Multimedia server on which you want to configure server settings. Select AACCHOST1_CCMM.
6	In the right pane, click **Launch Multimedia Client**. *The CCMM Administration Tool starts.*
7	In the left column, click **General Administration**.
8	Click **Administrator Settings**.
9	Click **New**.



10	In the **General identification** section, type the **Last Name**, the **First Name**, and the **Username** of the Administrator.
11	In the **Contact Details** section, add information about how to contact the Administrator, such as the **Phone Number**, **Fax Number**, and **E-mail Address**.
12	In the **Password** section type a password and confirm it in the confirm password field.
13	Click **Save**.

--End--

Configuring holidays

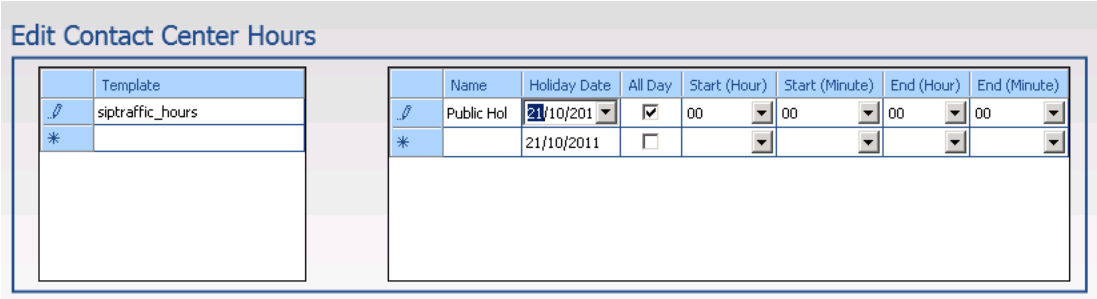
Configure the days and hours that your contact center is closed for holidays.

Configuring the office hours is important to determine accurate service levels for contacts that may have a delayed response such as email, voice mail, SMS, scanned documents, and faxes. For example, if a contact is received on a holiday, the queue time for the contact includes only the time the contact center is open.

You can use the office hour calendar in email rules to determine the skillset to which to route the contact.

Procedure steps

Step	Action
1	Log on to the Voice and Multimedia Contact Server.
2	Start Internet Explorer.
3	Log on to Contact Center Manager Administration with administrative privileges.
4	On the **Launchpad**, click **Multimedia**.
5	In the left column of the CCMM Administration tool, click **General Administration**.
6	Click **Office hours**.
7	Under **Template**, type the name of a calendar to configure. For example, type siptraffic_hours.
8	In the holiday box, under **Name**, type the name of a public holiday.
9	Select the **Holiday Date** for the holiday, and specify the time for the holiday. You can choose from **All Day** or specify a **Start time** and **End time**.



10	Click **Save**.

--End--

Configuring office hours

Configure the days and hours that your contact center is open each week.

Configuring the office hours is important to determine accurate service levels for contacts that may have a delayed response such as email, voice mail, SMS, scanned documents, and faxes. For example, if a contact is received on Friday and processed on Monday and you configure the office hours to show the contact center is closed over the weekend, the queue time for the contact only includes the time the contact center is open.

You can use the office hour calendar in email rules to determine the skillset to which to route the contact. The email rules can send a specific response if the office is closed.

The office hour calendar uses sliders to indicate closed times for your contact

center. The Start Closed Period slider is a blue triangle (). The End Closed

Period slider is a red triangle (). Each closed period is shown in red with a Start Closed Period and End Closed Period, at the beginning and at the end of the closed office hours.

Prerequisites

- Know the office hours of the contact center.

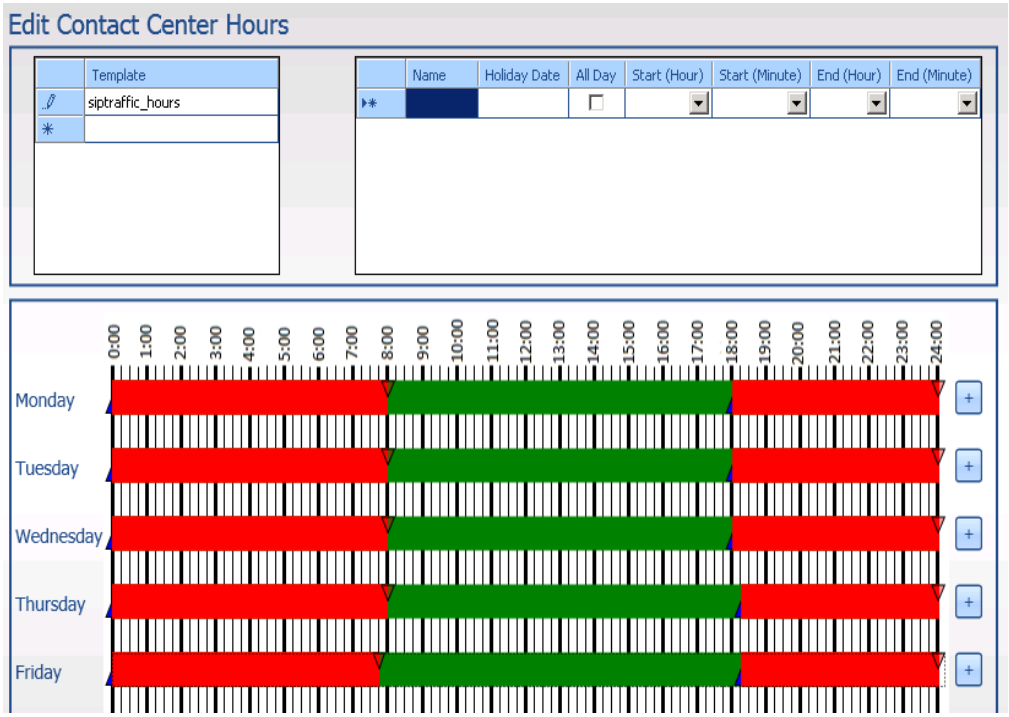
Procedure steps

Step	Action
1	Log on to the Voice and Multimedia Contact Server.
2	Start Internet Explorer.
3	Log on to Contact Center Manager Administration with administrative privileges.
4	On the **Launchpad**, click **Multimedia**.
5	In the left column of the CCMM Administration tool, click **General Administration**.
6	Click **Office hours**.
7	Under **Template**, type or select the name of a calendar to configure.
8	Configure holidays for the office hours template.
9	Beside a day of the week, click the **+** button.
10	For the day you select, move the Start Closed Period and End Closed Period sliders to define a period when the contact center is closed. *Open hours for the contact center are shown by the green bars. Closed hours are in red.*
11	Repeat step 9 and step 10 for every day of the week.
12	Click **Save**.

--End--

Procedure job aid

Example of configuring the Office Hours in Contact Center Multimedia.



Applying office hours

Apply a designated calendar showing open and closed hours of the contact center controlled by the Contact Center Multimedia server.

The designated calendar is used in email settings for the contact center.

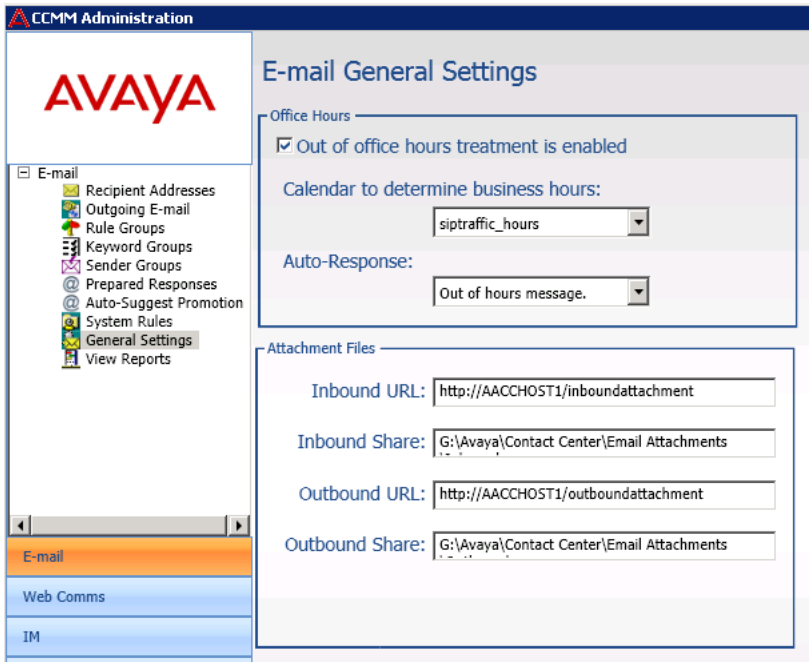
You can respond to email messages by selecting the office hours calendar to send automatic messages to incoming email contacts. You can select which rule group to apply the global office hours to. You can also configure a calendar for each skillset in your contact center.

Prerequisites

- Create a calendar template with office hours or holidays.

Procedure steps

Step	Action
1	Log on to the Voice and Multimedia Contact Server.
2	Start Internet Explorer.
3	Log on to Contact Center Manager Administration with administrative privileges.
4	On the **Launchpad**, click **Multimedia**.
5	In the Contact Center Multimedia Administration application, click **E-mail**.
6	In the left column of the CCMM Administration tool, click **General Settings**.
7	Under **Office Hours**, select the **Out of hours treatment is enabled** check box to automatically send an out-of-office type message to the customer when the contact center is closed.
8	Select the calendar you want to use to determine the business hours for your contact center. For example, select siptraffic_hours.
9	Select the automatic response for the out of office hours notice.



10	Click **Save**.

--End--

Configuring the email settings

Configure the following email settings for email messages entering and leaving your designated contact center mailboxes:

- how frequently you scan the email server for new messages
- the location in which attachments are stored
- automatic numbering of email messages
- which text is searched when you use keywords for rules

Default values are provided for required fields. You can change or accept the default values for the optional settings.

Procedure steps

Step	Action
1	Log on to the Voice and Multimedia Contact Server.
2	Start Internet Explorer.
3	Log on to Contact Center Manager Administration with administrative privileges.
4	On the **Launchpad**, click **Multimedia**.
5	In the left column of the CCMM Administration tool, click **E-mail**.
6	Click **General Settings**.
7	Clear **Out of office hours treatment is enabled**.
8	To configure a mailbox scan interval, under **Mailbox Scan Interval**, in the **Open Duration** box, type the time in minutes. For example, select 1 minute.
9	To change the attachment file locations, under **Attachment Files**, type the new paths for the inbound and outbound URL and shared folders into the fields provided.
10	To include the customer ID or contact ID in a number for the outgoing email message numbering, select the **Customer** check box, the **Contact ID** check box, or both.
11	To include the email message body in the keyword search, select the **Include email body in keyword search** check box.
12	Click **Save**.

--End--

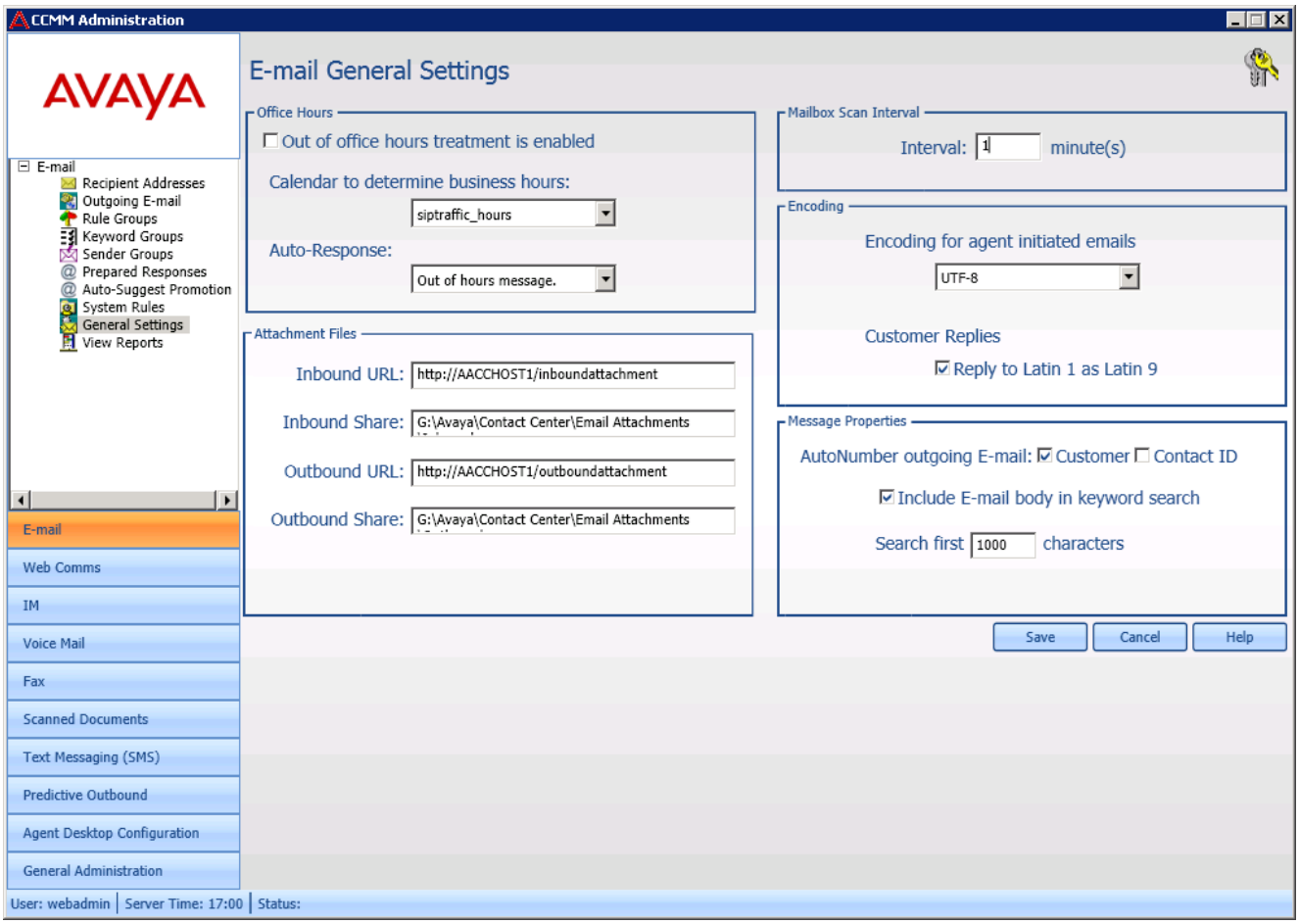
Variable definitions

Variable	Value
Open Duration	The interval between mailbox scans to check for new incoming email messages. You can specify minutes and seconds between each scan.
Inbound Url	The uniform resource locator (URL) that contains the location of the inbound email attachments.
Inbound Share	The path of the shared folder on the Contact Center Multimedia server in which the inbound email attachments are stored.
Outbound Url	The uniform resource locator (URL) that contains the location of the outbound email attachments.
Outbound Share	The path of the shared folder on the Contact Center Multimedia server in which the outbound email attachments are stored.
Autonumber outgoing email	Select the check box to number the email message automatically with either the customer ID, the contact ID, or both. The number appears in the subject of the message for identification.
Include email body in keyword search	Select the check box to enable a keyword search in both the subject and the body of the email message.
Search for first characters	Specify the number of characters in the content of the body of the email message that you search for keywords if you enabled the keyword search in the body of the email message.

Procedure job aid

Configure the email settings for email messages entering and leaving your designated contact center mailboxes.

Example of configuring email general settings



Configuring skillsets for email

Configure a route point for each skillset, and to use the skillsets in rules. A route point is a location on the open queue that enables incoming calls to be queued and run through a script on the Contact Center Manager Server.

An automatic signature is text automatically added at the bottom of an outgoing message. For example, you can encourage customers to visit your customer support Web site by adding the URL and other promotional information or disclaimer text to every message.

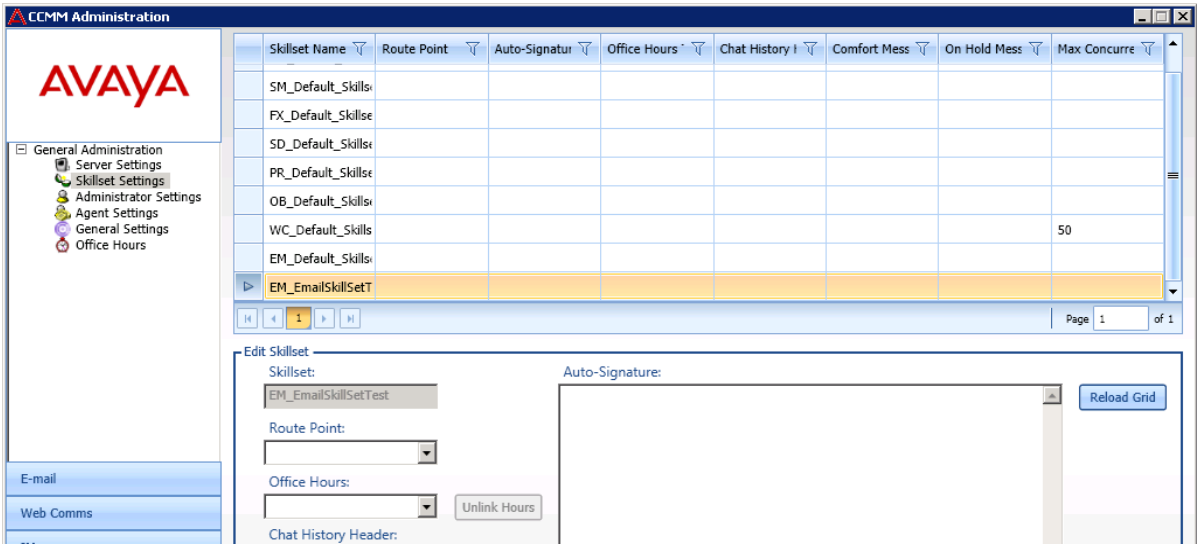
You can also apply an office hours template for your skillset. If agents in a different time zone or different department have a different set of office hours, you can apply an office hour template that is different from the global office hours schedule configured in general email settings to this skillset.

Prerequisites

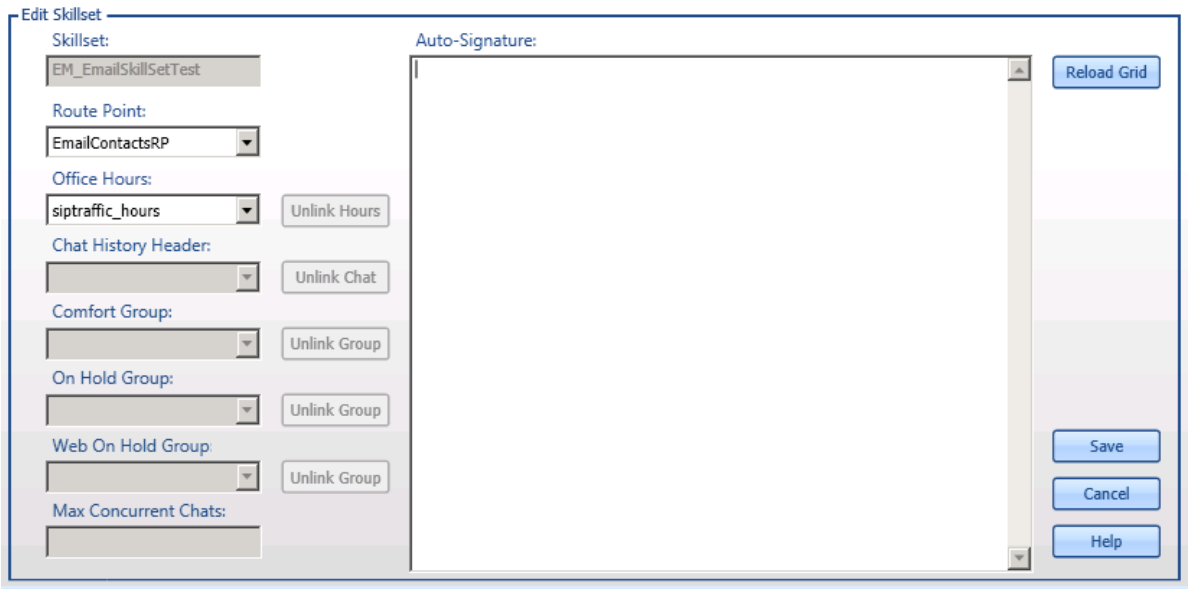
- Configure an office hour template.

Procedure steps

Step	Action
1	Log on to the Voice and Multimedia Contact Server.
2	Start Internet Explorer.
3	Log on to Contact Center Manager Administration with administrative privileges.
4	On the **Launchpad**, click **Multimedia**.
5	In the left column of the CCMM Administration tool, click **General Administration**.
6	Click **Skillset Settings**.
7	Select a skillset for which to assign a route point. For example, select **EM_EmailSkillSetTest**.



8	From the **Route Point** list, select the route point to assign to the skillset. For example, select **EmailContactsRP**.
9	Under **Office Hours**, choose an office hour template that gives the office hours particular to the selected skillset. For example, select **siptraffic_hours**.
10	If applicable, in the **Auto Signature** box, type the signature to assign to the skillset.



11 Click **Save**.

--End--

Creating a keyword group

Create a keyword group that you can use to create a rule to route email messages to skillsets. You must assign at least one keyword to a keyword group before you can save the keyword group.

The keyword search in an email message is not case-sensitive. For example, if you add the word John, the Email Manager also matches JOHN and john. You can specify a spelling accuracy in the keyword group.

The Keyword box supports the Unicode UTF-8 character set.

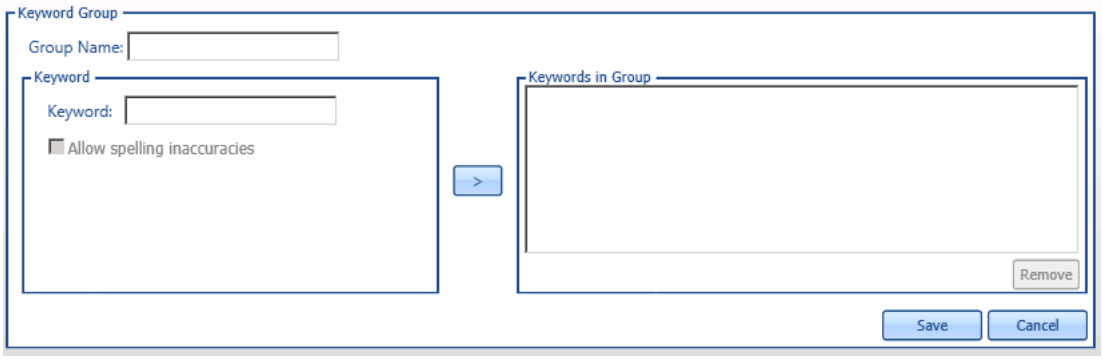
Procedure steps

Step	Action
1	Log on to the Voice and Multimedia Contact Server.
2	Start Internet Explorer.
3	Log on to Contact Center Manager Administration with administrative privileges.
4	On the **Launchpad**, click **Multimedia**.

5 In the left column of the CCMM Administration tool, click **E-mail**.

6 Click **Keyword Groups**.

7 Click **New**.

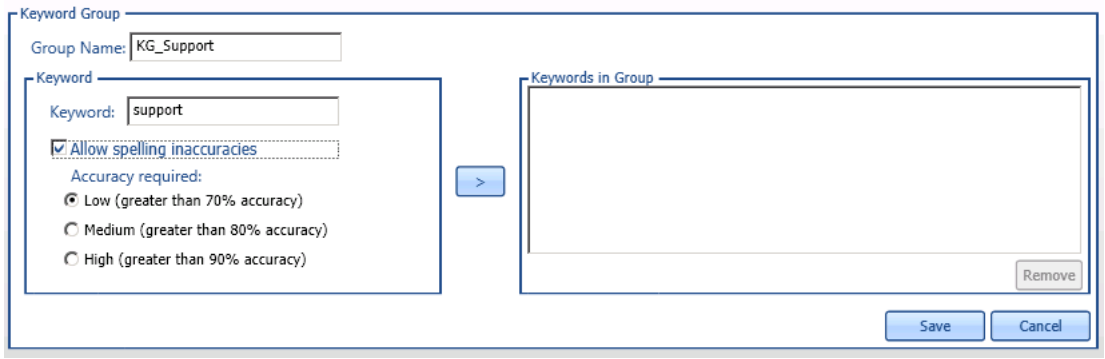


8 In the **Keyword Group** section, in the **Group Name** box, type the name of this Keyword Group. For example, type KG_Support.

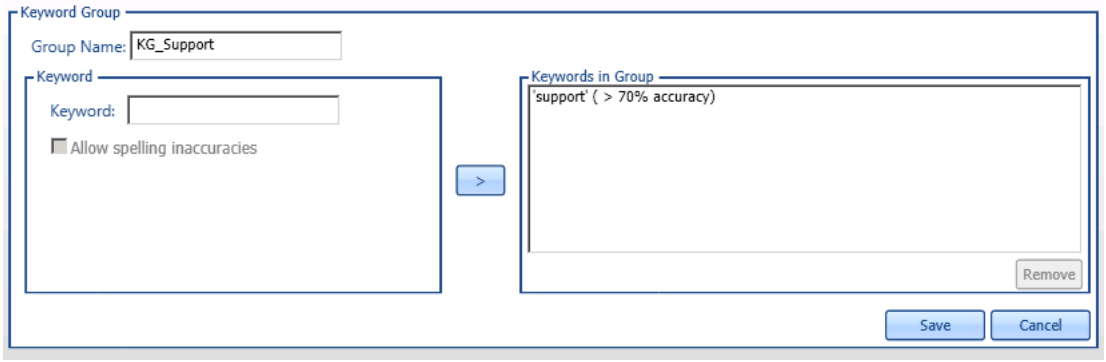
9 In the **Keyword** box, type the keyword. For example type support.

10 To allow misspellings of the word, select the **Allow spelling inaccuracies** check box.

11 Under **Accuracy required**, select **Low (greater than 70% accuracy)**.



12 Click the right-arrow button (>).

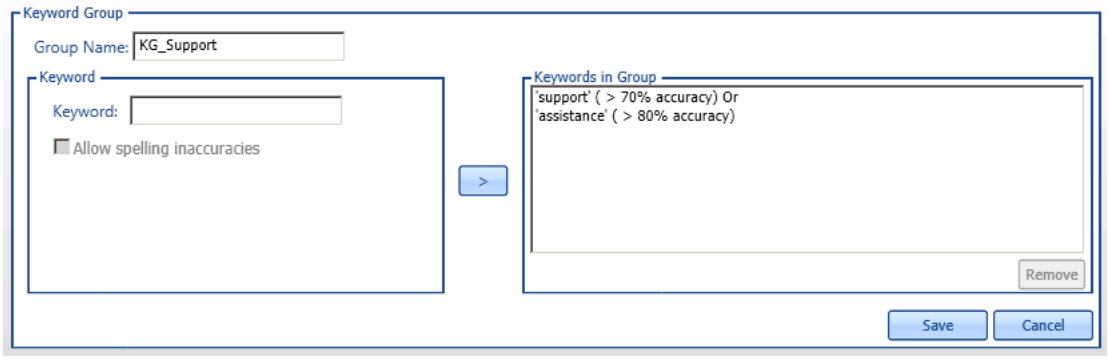


13 In the **Keyword** box, type the keyword. For example type assistance.

14 To allow misspellings of the word, select the **Allow spelling inaccuracies** check box.

15 Under **Accuracy required**, select **Medium (greater than 80% accuracy)**.

16 Click the right-arrow button.



17 Click **Save**.

--End--

Creating a rule group and a rule

Create a rule group containing one rule to route email contacts to a skillset. In this example, the rule specifies a specific word which, when found in the email message, Contact Center uses to route the email contact.

Procedure steps

Step	Action
1	Log on to the Voice and Multimedia Contact Server.
2	Start Internet Explorer.

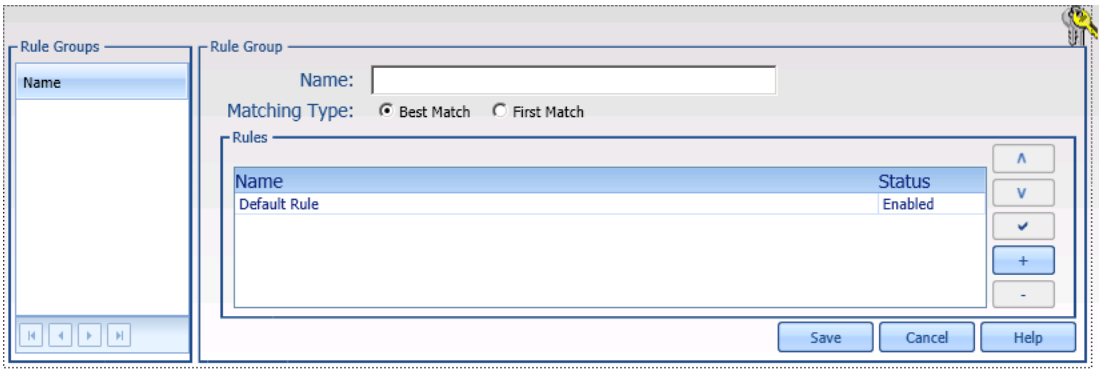
3 Log on to Contact Center Manager Administration with administrative privileges.

4 On the **Launchpad**, click **Multimedia**.

5 In the left column of the CCMM Administration tool, click **E-mail**.

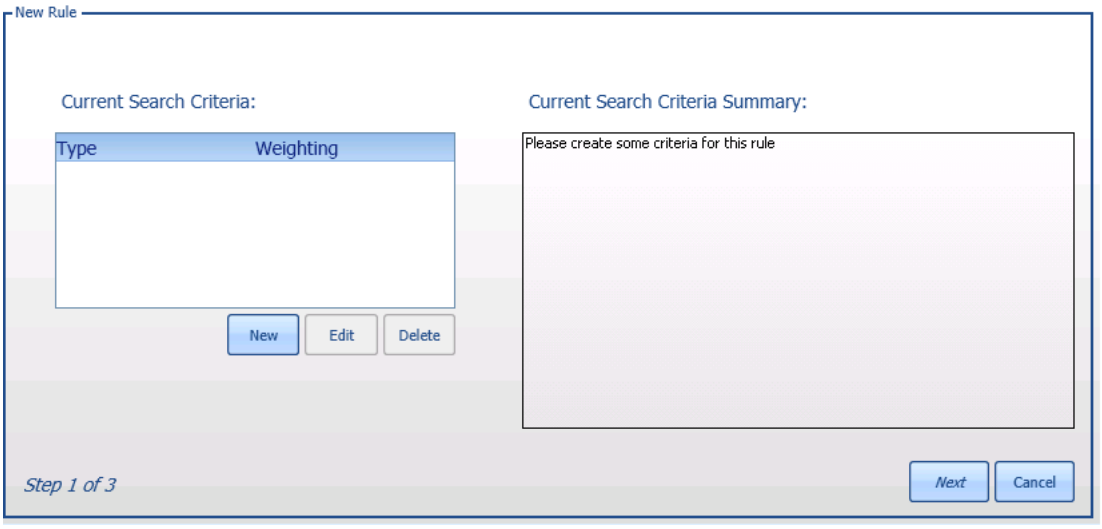
6 Select **Rule Groups**.

7 Under **Rule Groups**, click **New**.



8 In the **Name** box, type the name for the rule group. For example, type RG_Support.

9 Under **Rules**, select the plus button (+).

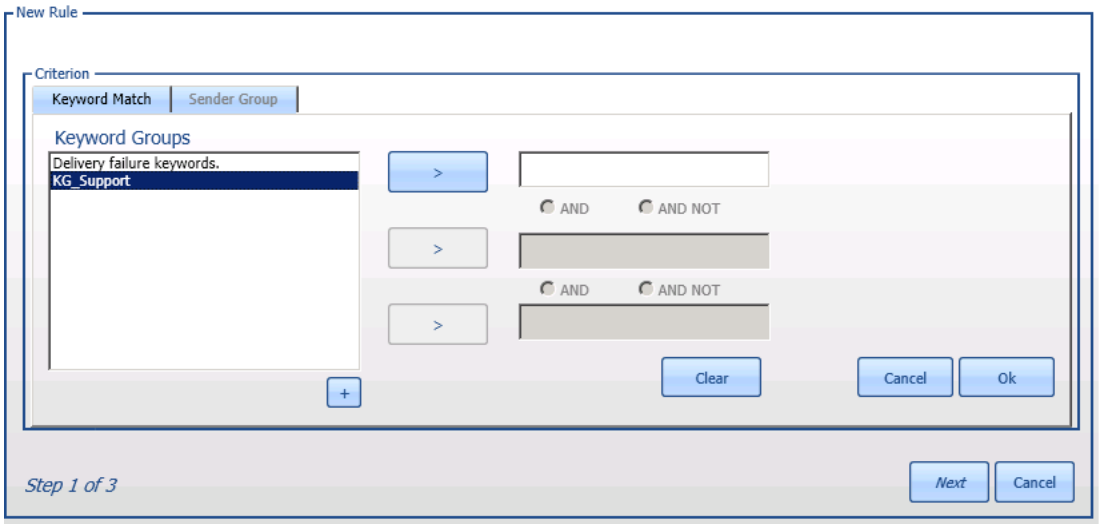


10 Under **New Rule**, in the **Current Search Criteria** section, click **New**.

11 From the **Add new Criterion** list, select **Keyword Match**.

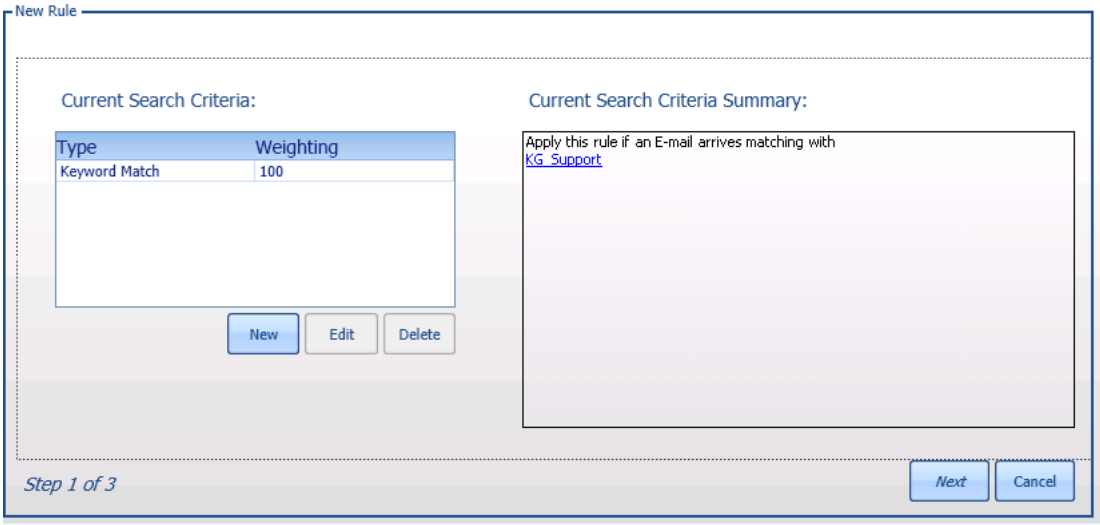
12 Click **Go**.

13 On the **Keyword Match** tab, from the **Keyword Groups** list, select the keyword group you just created, for example KG_Support.



14 Click the right arrow button (>).

15 Click **OK**.



16 Click **Next**.

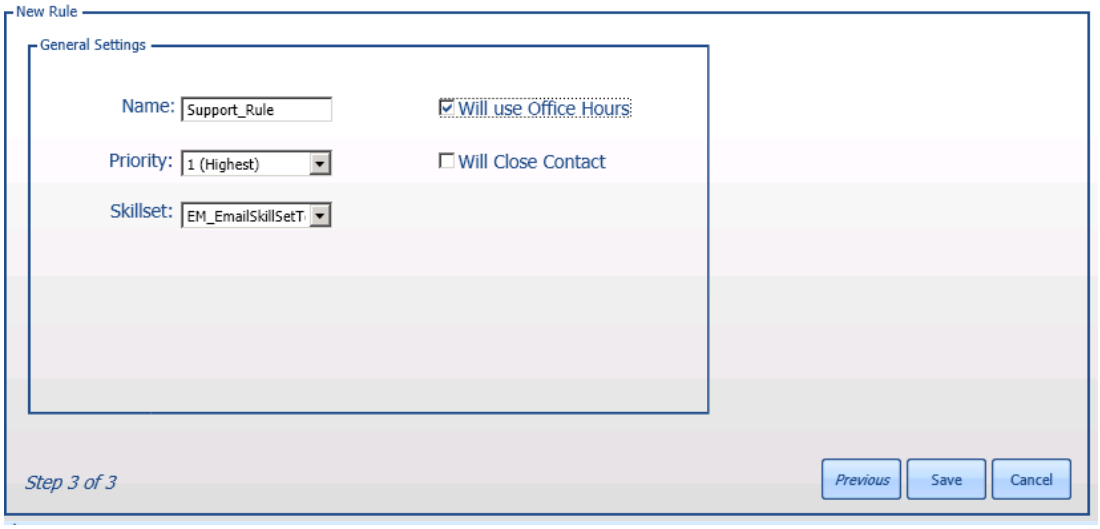
17 Click **Next**.

18 Under **General Settings**, in the **Name** box, type a name for the rule, for example Support_Rule.

19 From the **Priority** list, select **1 (Highest)**.

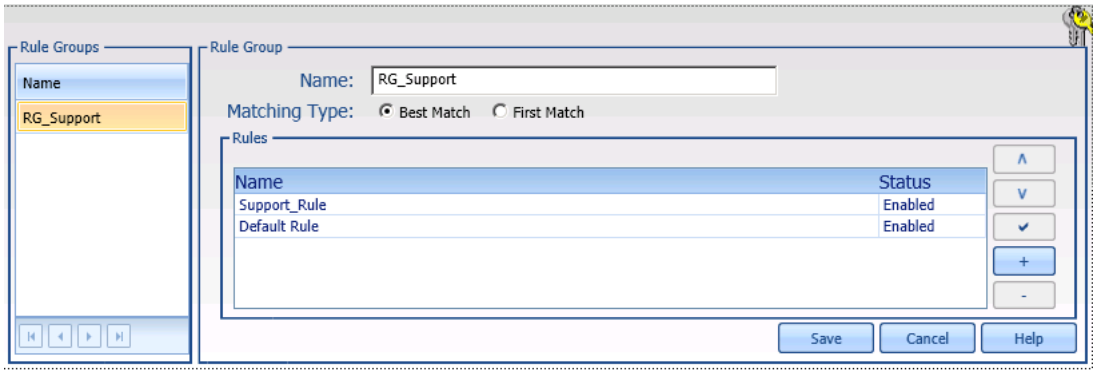
20 From the **Skillset** list, select the skillset to which you want Contact Center to route email messages matching this rule, for example EM_EmailSkillSetTest.

21 Select the **Will use Office Hours** check box.



22 Under **New Rule**, click **Save**.

23 Under **Rule Group**, click **Save**.



--End--

Creating an email recipient mailbox

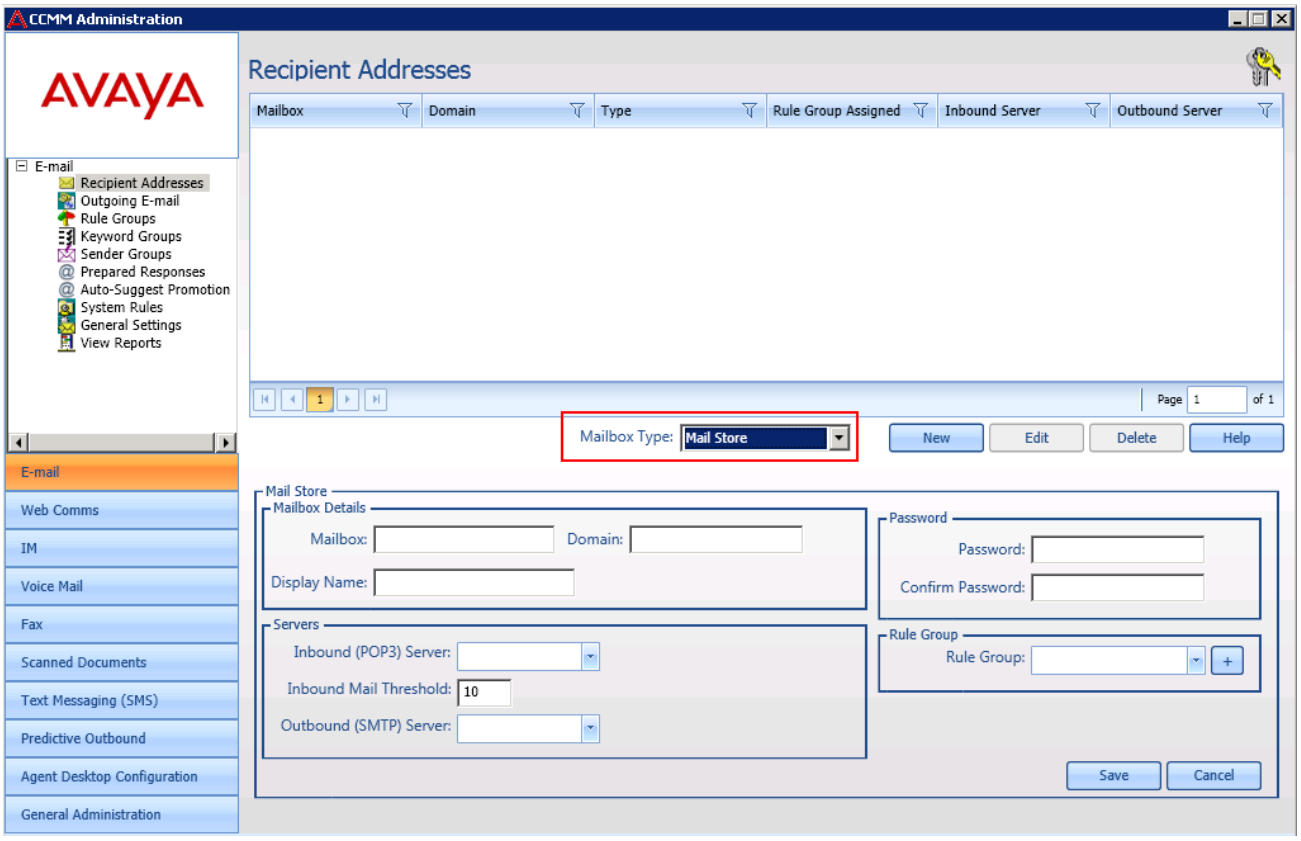
Create a recipient email box to ensure that at least one email box is configured for your contact center. You must configure one recipient to commission the server. You can create additional mailboxes to have the Contact Center Manager Server poll a mailbox on the email server and handle contacts based on the recipient address.

Prerequisites

- Ensure that any enabled email address you want to configure in the Email Manager is already configured on your corporate email server.

Procedure steps

Step	Action
1	Log on to the Voice and Multimedia Contact Server.
2	Start Internet Explorer.
3	Log on to Contact Center Manager Administration with administrative privileges.
4	On the **Launchpad**, click **Multimedia**.
5	In the left column of the CCMM Administration tool, click **E-mail**.
6	Click **Recipient Addresses**.
7	Click **New**.
8	In the list box, select **Mail Store**.



9	Under **Mailbox Details**, in the **Mailbox** box, type the SMTP mailbox name. For example, type mailbox99.
10	In the **Domain** box, type the domain for your email server. For example, type labmail.com.

11 In the **Display Name** box, type the name to appear in the email From address. For example, type mailbox99.

12 In the **Password** box, type the password for the mailbox.

Attention: When you change a password on the email server, you must update this password in the Multimedia Administrator.

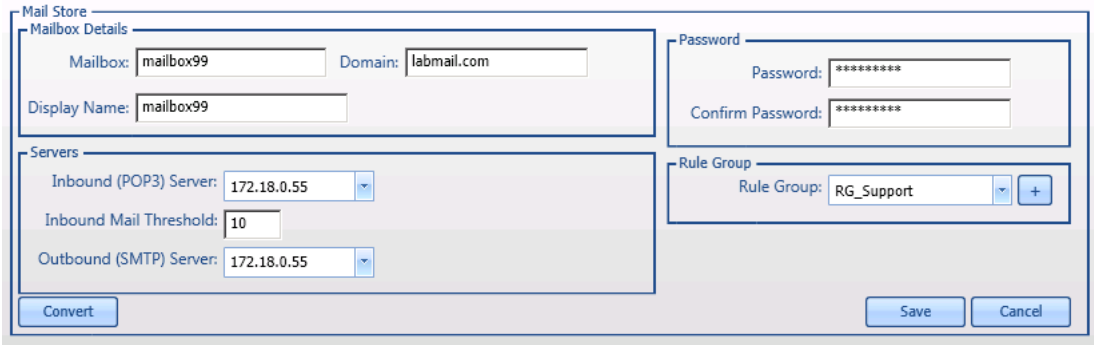
13 In the **Confirm Password** box, type the same password you typed in the **Password** box.

14 In the **Inbound POP3 Server** box, ensure that the host name of your POP3 server appears. For example, select 172.18.0.55.

15 In the **Inbound Mail Threshold** box, type the maximum number of email messages to be retrieved from the mailbox every scan interval. You can enter a different value for this variable for each mailbox. For example, type 10.

16 In the **Outbound SMTP Server** box, ensure that the host name of your SMTP server appears. For example, select 172.18.0.55.

17 In the **Rule Group** box, select the name of the Rule Group to assign to the recipient mailbox. For example, select **RG_Support**.



18 Click **Save**.

--End--

Variable definitions

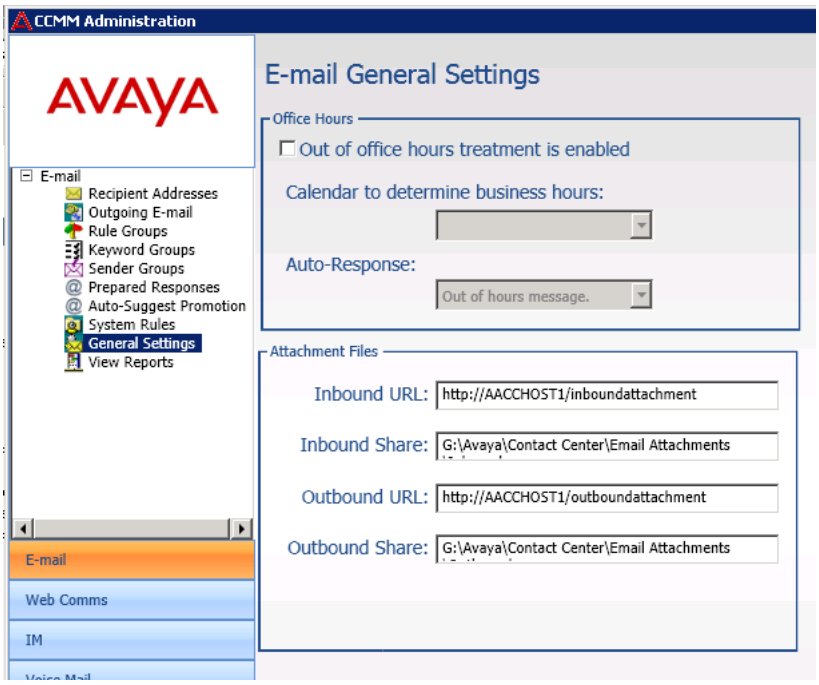
Variable	Value
Display Name	The name to appear in the email From address. For example, Sales Department.
Domain	The domain name for the email server.
Mailbox	The name of a mailbox on the email server. If the Contact Center Multimedia server is in the same domain as the email server, in the Mailbox Name box, type the address, and in the E-mail Domain box, type the domain name. If the Contact Center Multimedia server is not in the same domain as the email server, and you are using Windows 2000, in the Mailbox Name box, type the address in the format domain\user. If the Contact Center Multimedia server is not in the same domain as the email server, and you use a version of Windows later than Windows 2000, in the Mailbox Name box, type the address in the format user@domain. **Attention:** Mailbox names are case-sensitive. You must type the mailbox name exactly as it appears on your server.
Password and Confirm	The password used to access the mailbox on the email server. Retype the password in the Confirm box to ensure accuracy.
Inbound Mail Threshold	The maximum number of email messages to be retrieved from the mailbox every scan interval. You can enter a different value for this variable for each mailbox. The default value is 10.
Rule Group	The name of the rule group that applies to this recipient mailbox. Configure rule group properties in the Contact Center Multimedia Administrator.
Inbound (POP3) Server	The name of the email server that handles email messages coming into the contact center.
Outbound (SMTP) Server	The name of the email server that delivers email messages that leave the contact center.

Configuring email attachment file locations

Configure the locations for inbound and outbound email attachments.

Procedure steps

Step	Action
1	Log on to the Voice and Multimedia Contact Server.
2	Start Internet Explorer.
3	Log on to Contact Center Manager Administration with administrative privileges.
4	On the **Launchpad**, click **Multimedia**.
5	In the left column, select the Multimedia server on which you want to configure server settings. Select AACCHOST1_CCMM.
6	In the right pane, click **Launch Multimedia Client**. *The CCMM Administration Tool opens.*
7	In the left column, select **E-mail**, **General Settings**.
8	Under **Attachment Files**, in the **Inbound URL** box, type the URL for files attached to inbound email messages. For example, type http://AACCHOST1/inboundattachment.
9	Under **Attachment Files**, in the **Inbound Share** box, type the share location for files attached to inbound email messages. For example, type G:\Avaya\Contact Center\Email Attachments\Inbound.
10	Under **Attachment Files**, in the **Outbound URL** box, type the URL for files attached to outbound email messages. For example, type http://AACCHOST1/outboundattachment.
11	Under **Attachment Files**, in the **Outbound Share** box, type the share location for files attached to outbound email messages. For example, type G:\Avaya\Contact Center\Email Attachments\Outbound.



12 Click **Save**.

--End--

Selecting the outgoing email address

You can send email messages from the email address to which the original message was sent or from a general email address in the contact center.

You can choose the response email address based on a skillset.

Prerequisites

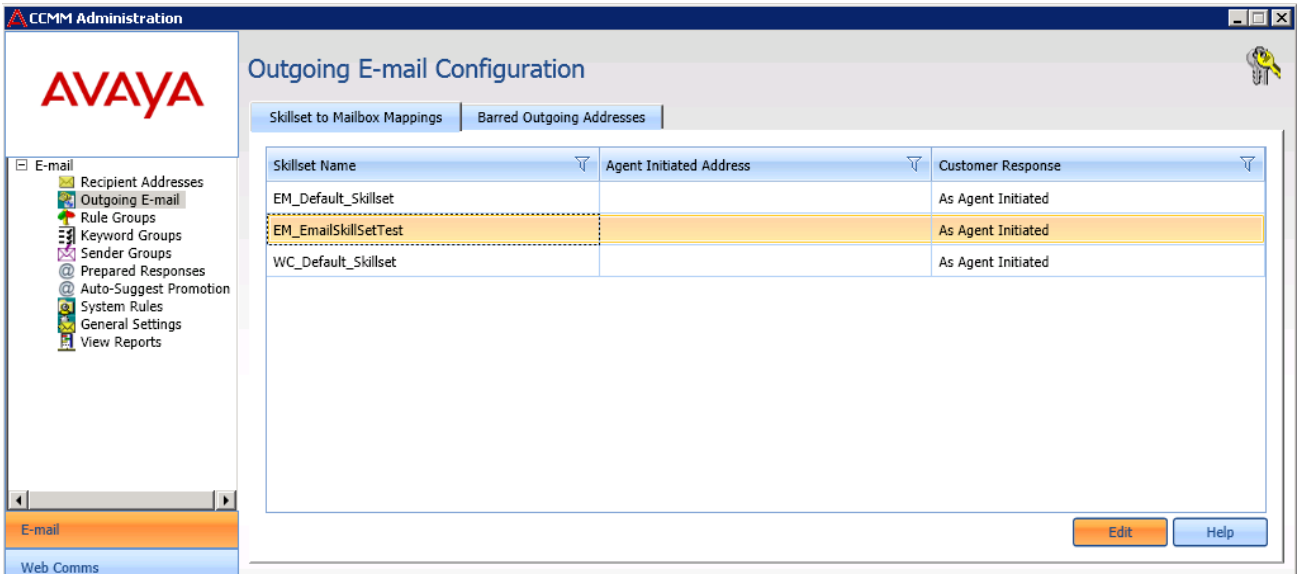
- Configure the email mailbox from which to send outbound email messages.

Procedure steps

Step	Action
1	Log on to the Voice and Multimedia Contact Server.
2	Start Internet Explorer.
3	Log on to Contact Center Manager Administration with administrative privileges.
4	On the **Launchpad**, click **Multimedia**.
5	In the left column of the CCMM Administration tool, click **E-mail.**

6 Click **Outgoing E-mail**.

7 On the **Skillset to Mailbox Mappings** tab, select a skillset. For example, select EM_EmailSkillSetTest.

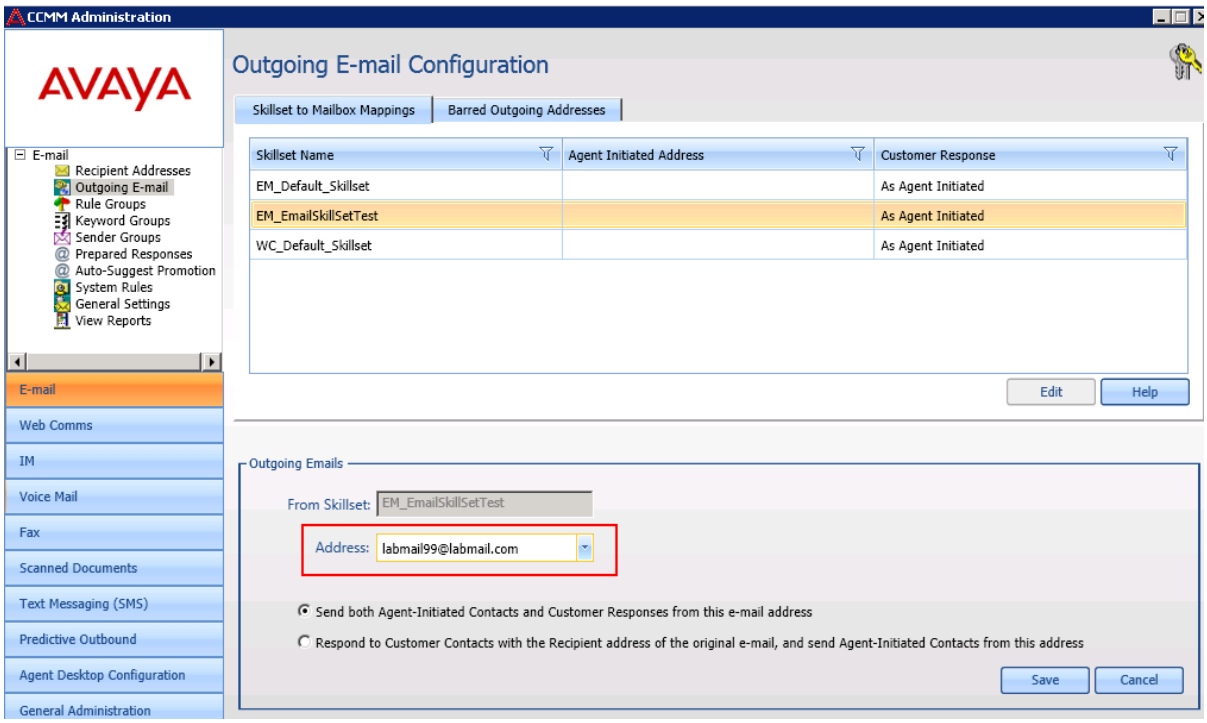


8 Click **Edit**.

9 In the **Address** box, select the address from which you want email messages sent from this skillset. For example, select mailbox99@labmail.com.

10 To send customer responses from an address specified for the skillset, click **Send both Agent-initiated Contacts and Customer Responses from this email address**, and then select the email address for the outgoing email.

11 To send customer responses from the address that the customer used, click **Respond to Customer Contacts with the Recipient address of the original email, and send Agent-Initiated Contacts from this address**.



12 Click **Save**.

--End--

Configuring Agent Desktop Configuration General Settings

Agents, by default, see all contacts in the contact center. You can restrict the access to show agents only the contacts assigned to the agent's skillsets.

Active Contact Timer

Configure the hours and minutes that you want a contact to remain open on a desktop without activity. When this time expires, the contact is automatically placed into pending state. The default time in the Contact Center Multimedia configuration is 1 hour (60 minutes). The actual time that the contact can be open on the desktop without activity is 1 hour less than the maximum open duration for contacts as defined on Contact Center Manager Server. The default maximum open duration on the Contact Center Manager Server is 1 hour.

Callback Timer

Configure the callback timer as a range of minutes to days for the system to wait before re-offering a pending contact to agents. An agent can delay the contact or place the contact into the pending state, because they are waiting for additional information to complete the contact.

The callback timer can be 2 minutes to 200 days (about 6 months). The default range provides the limits to which the you configure the callback time. The actual time value appears by default in the Agent Desktop application when the agent reschedules the contact.

Callback Trunk Access

Configure the callback trunk access to ensure that you can create a callback to the customer you work with using the same contact type. The customer can request a callback, and you can schedule callbacks.

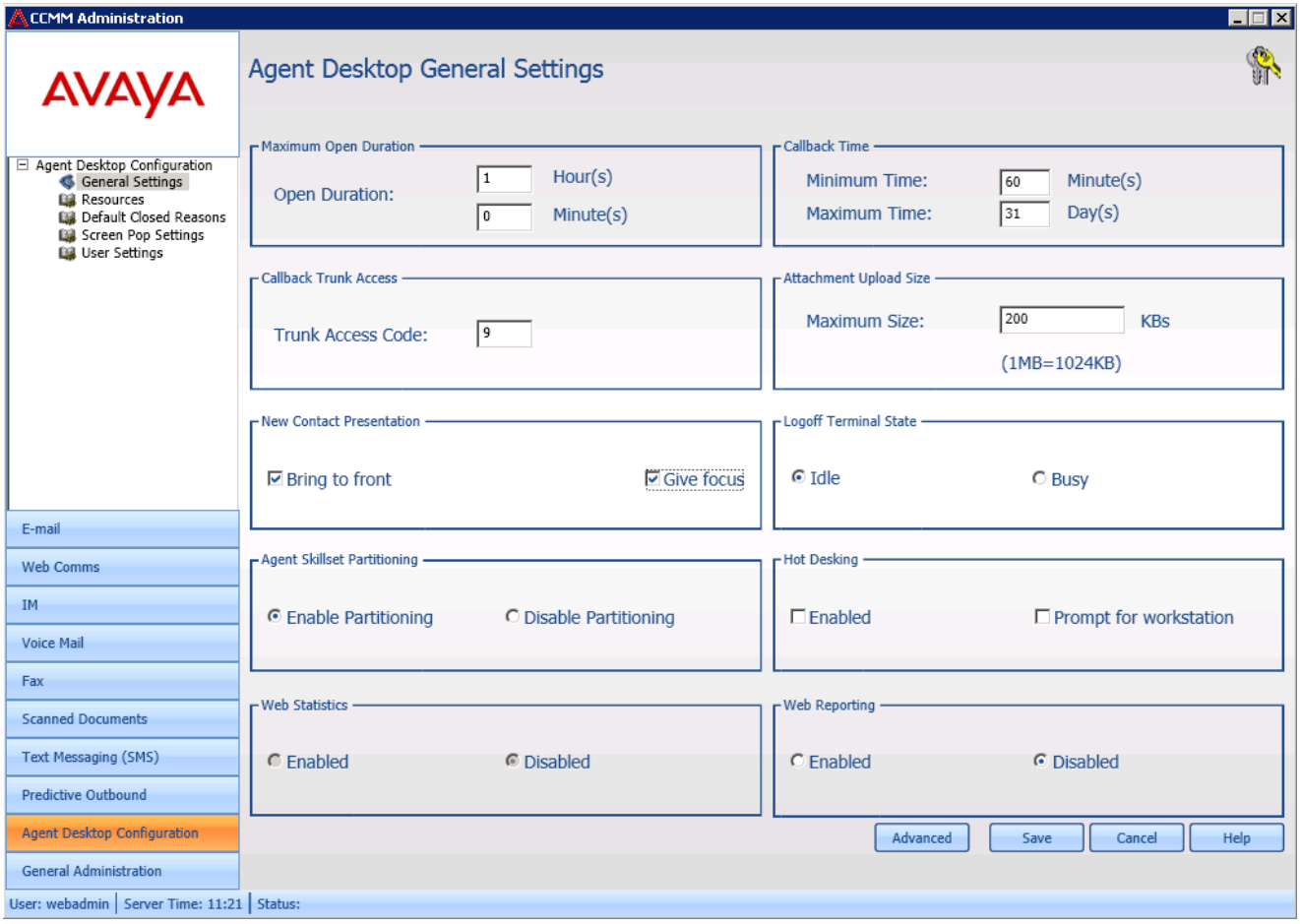
Procedure steps

Step	Action
1	Log on to the Voice and Multimedia Contact Server.
2	Start Internet Explorer.
3	Log on to Contact Center Manager Administration with administrative privileges.
4	On the **Launchpad**, click **Multimedia**.
5	In the left column of the CCMM Administration tool, click **Agent Desktop Configuration**.
6	Click **General Settings**.
7	In the **Maximum Open Duration** box, type the maximum number of hours and minutes that you want contacts to be active before they move to pending state. For example type 1 hour.
8	Under **Callback Time**, type a number of minutes in the **Minimum Time** box. For example, type 60 minutes.
9	Under **Callback Time**, type a maximum number of days in the **Maximum Time** box. For example type 31 days.
10	Under **Callback Trunk Access**, type the trunk access number in the **Trunk Access Code** box. For example, type 9.
11	Under **New Contact Presentation**, select **Bring to front** and **Give Focus**.
12	Under **Agent Skillset Partitioning**, select **Enable Partitioning**.
13	Under **Logoff Terminal State**, select **Idle**.
14	Click **Save**.

--End--

Procedure job aid

Example of configuring Agent Desktop Configuration General Settings



Controlling access to email message text

Agents, by default, cannot edit text in an email message. You can either enable particular agents or enable all agents to delete text from email messages that enter the contact center.

For example, select this feature so agents can delete credit card information from an email message to protect confidential customer information.

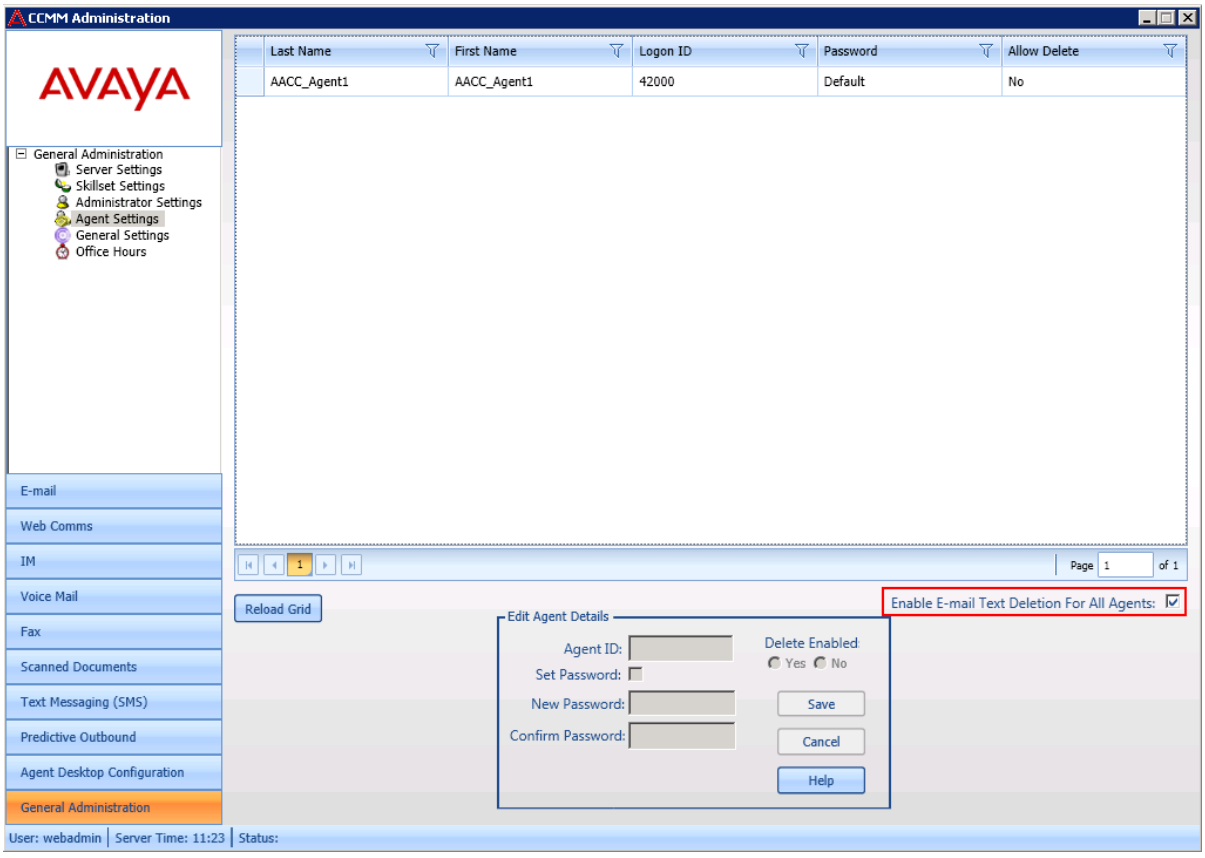
Procedure steps

Step	Action
1	Log on to the Voice and Multimedia Contact Server.
2	Start Internet Explorer.
3	Log on to Contact Center Manager Administration with administrative privileges.
4	On the **Launchpad**, click **Multimedia**.
5	In the left column of the CCMM Administration tool, click **General Administration**.
6	Click **Agent Settings**.
7	Select the **Enable Email Text Deletion For All Agents** check box, to enable all agents to delete text from email messages.
8	Click **Save**.

--End--

Procedure job aid

Example of controlling access to email message text



Viewing real-time traffic reports by contact type

For email, voice mail, fax, SMS, and scanned documents, you can view traffic reports for each contact type.

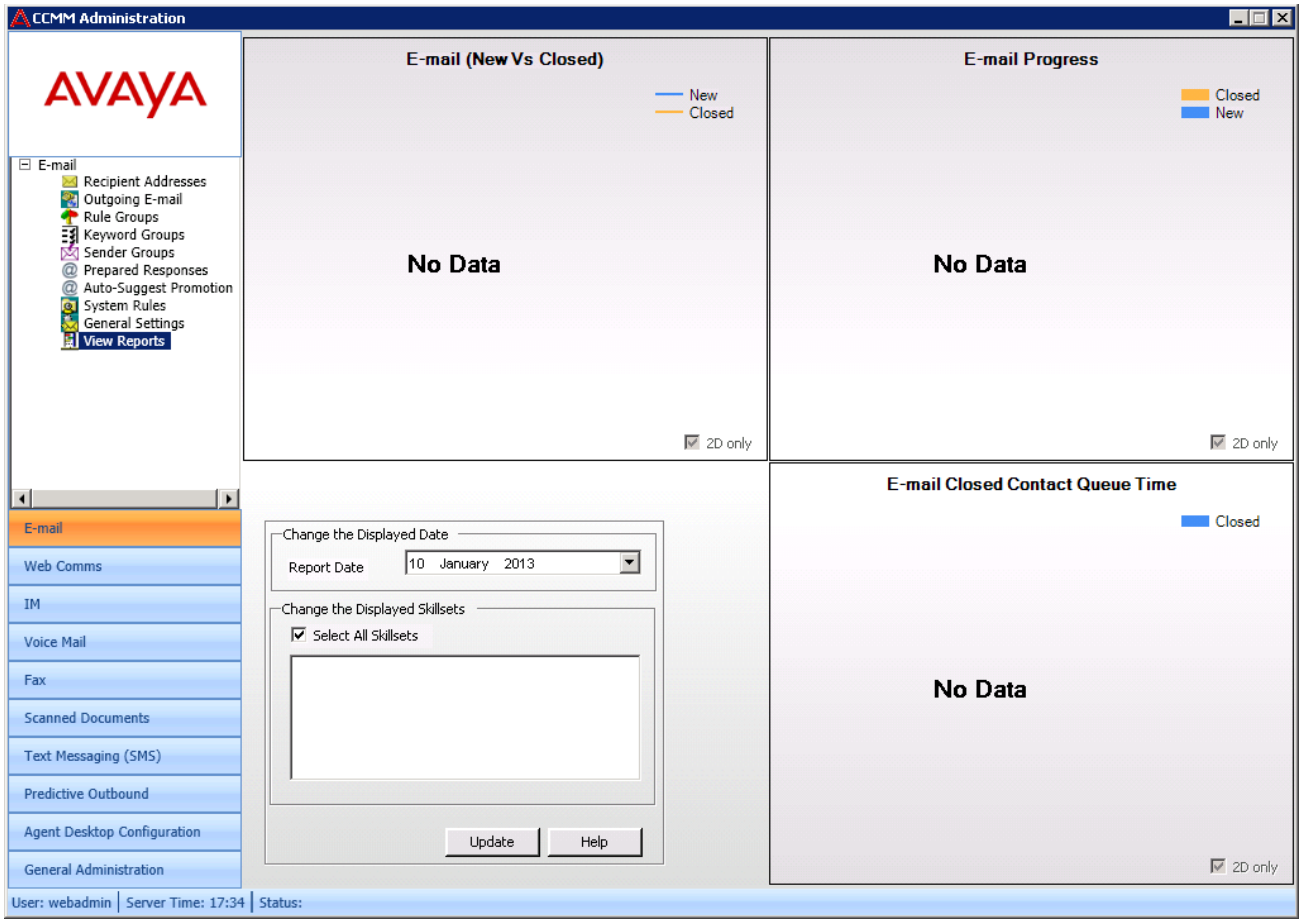
The reports appear in the Contact Center Multimedia Administration utility to show the current traffic status. The following reports appear when you select View Reports in the left column of the Contact Center Multimedia application. You can choose the report date and the skillsets represented in all displayed real-time reports.

- The New Vs. Closed report shows the number of contacts in a new and closed state in a given span of time for the selected date and skillsets.
- The Progress report shows the number of contacts in a new or closed state on a defined date to determine the traffic levels for that date.
- The Closed Contacts Queue Time report shows the average time a contact spends in queue, while the contact center is open.

You can change the time for the displayed traffic reports.

Procedure steps

Step	Action
1	Log on to the Voice and Multimedia Contact Server.
2	Start Internet Explorer.
3	Log on to Contact Center Manager Administration with administrative privileges.
4	On the **Launchpad**, click **Multimedia**.
5	Select a media type that supports the traffic report views. For example, select **E-mail**.
6	Click **View Reports**.



--End--

Configuring the reporting credentials

Configure the password for the mmReport user. The mmReport user is configured in the Multimedia database to pass data and reporting information to Contact Center Manager Administration to generate real-time and historical reports, and integrated reporting.

If you change the password in the Contact Center Multimedia Administrator application, you must update the Contact Center Multimedia password in Contact Center Manager Administration.

Procedure steps

Step	Action

1 Log on to the Voice and Multimedia Contact Server.

2 Start Internet Explorer.

3 Log on to Contact Center Manager Administration with administrative privileges.

4 On the **Launchpad**, click **Multimedia**.

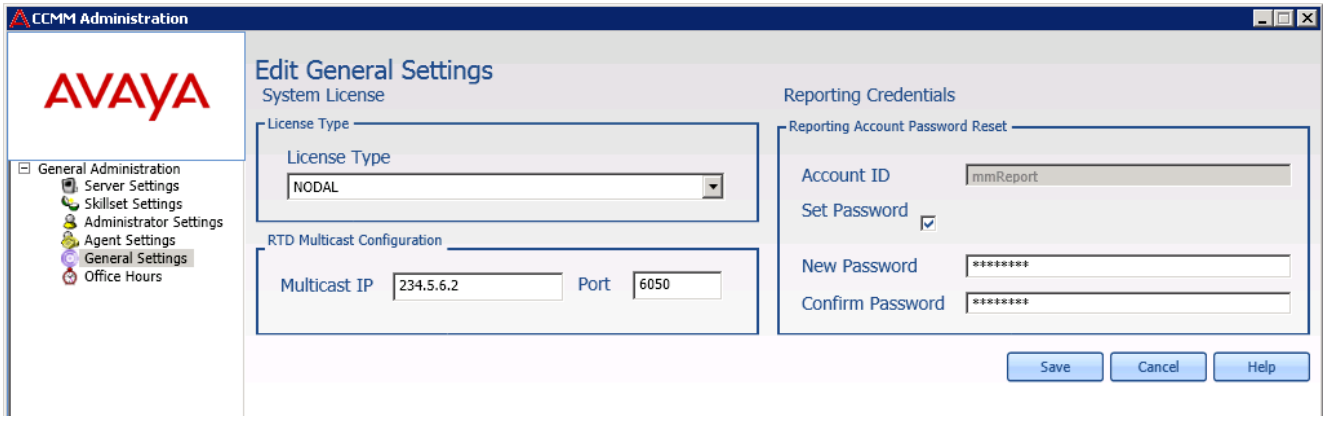
5 In the left column, of the CCMM Administration tool, click **General Administration**.

6 Click **General Settings**.

7 Under **Reporting Account Password Reset**, select the account ID for reporting. The default account is mmReport.

8 Click **Set Password** to change the default password.

Type the password in the **New Password** and **Confirm Password** boxes, for example type mmReport as the password.



9 Click **Save**.

--End--

Updating the System Default Rule

Update the System Default Rule to ensure that an email message arriving at each configured recipient mailbox is assigned a skillset and can be routed.

When you create a recipient mailbox, the System Default Rule is copied as the last regular rule into the list of rules for the recipient mailbox.

The automatic signature is text appended to each email message sent from the contact center in addition to the agent message. The text in the automatic signature contains corporate disclaimer information and must be in a fixed-width font. The automatic signature appears in an email message after any personal signature, which is configured in the Agent Desktop application.

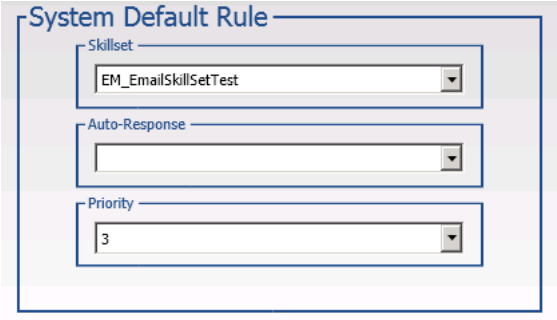
The System Default rule is used in every rule group configured in Contact Center Multimedia.

Prerequisites

- Ensure that you know the default settings for the System Delivery Failure Rule:
  - use the email default skillset, EM_Default_Skillset
  - use no automatic response
  - assign priority 3 (medium high)
- Use caution when you change the properties of the System Default Rule:
  - If you change the properties of the rule, you affect the behavior of the system default rule, which affects all recipient mailboxes.
  - If you delete the skillset associated with the default rule, EM_Default_Skillset is used.
  - If you delete EM_Default_Skillset, the system stops processing email messages.
- Configure the route points for the skillset you assign to the System Default Rule.

Procedure steps

Step	Action
1	Log on to the Voice and Multimedia Contact Server.
2	Start Internet Explorer.
3	Log on to Contact Center Manager Administration with administrative privileges.
4	On the **Launchpad**, click **Multimedia**.
5	In the left column of the CCMM Administration tool, click **E-mail**.
6	Under **System Rules**, in the **System Default Rule** section, from the **Skillset** list, select a skillset name. For example, select **EM_EmailSkillSetTest**.
7	To change the automatic response settings, under **Auto-Responses**, select another automatic response from the list.
8	To change the priority, under **Priority**, select a different priority for the contact. For example, select **3**.



9 Click **Save**.

--End--

Variable definitions

Variable	Value
Skillset	A label applied to a set of skills, capabilities, or knowledge that an agent requires to respond to a request. The skillsets are retrieved from the Contact Center Manager Server database. You must select a route point for a skillset used to route contacts.
Auto Response	A message sent to a customer with no agent interaction. An automatic response can be an intelligent response, such as a sales promotion flyer, or an acknowledgement, such as, “Thank you for your email. We will respond to you within three days.”
Priority	The priority given to a request for a skillset agent. The lower the priority number, the greater the priority. The values of the priorities range from 1 to 6. For example, a call with priority 1 is handled before a call with priority 6.

Updating the System Delivery Failure Rule

Update the System Delivery Failure Rule to ensure that any email message that contains particular phrases such as undeliverable, returned mail, unknown recipient, delivery failure, or delivery report is deleted and not assigned to an agent.

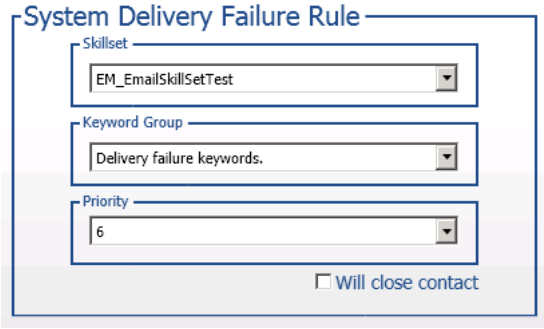
When you create a recipient mailbox, the System Delivery Failure Rule is copied as the first regular rule into the list of rules for the recipient mailbox.

Prerequisites

- Ensure that you are licensed to handle email messages.
- Ensure that you know the default settings for the System Delivery Failure Rule:
  - use the email default skillset, EM_Default _Skillset
  - use keyword group delivery failure keywords
  - assign priority 6 (lowest)
- Use caution when you change the properties of the System Default Rule:
  - If you change the properties of the rule, you affect the behavior of the system default rule, which affects all recipient mailboxes.
  - If you delete the skillset associated with the default rule, EM_Default_Skillset is used.
  - If you delete EM_Default_Skillset, the system stops processing email messages.
- Configure the route point for the skillset you plan to assign to the System Delivery Failure Rule.

Procedure steps

Step	Action
1	Log on to the Voice and Multimedia Contact Server.
2	Start Internet Explorer.
3	Log on to Contact Center Manager Administration with administrative privileges.
4	On the **Launchpad**, click **Multimedia**.
5	In the left column of the CCMM Administration tool, click **E-mail**.
6	Under **System Rule**, in the **System Delivery Failure Rule** section, from the **Skillset** list, select a skillset name. For example, select **EM_EmailSkillSetTest**.
7	To change the keyword group, under **Keyword Group**, select an existing keyword group from the list.
8	To change the priority, under **Priority**, select a different priority for the contact. For example, select **6**.
9	Select the **Will close contact** check box to have the rule to close the contact.



10 Click **Save**.

--End--

Variable definitions

Variable	Value
Skillset	A label applied to a set of skills, capabilities, or knowledge that an agent requires to respond to a request. The skillsets are retrieved from the Contact Center Manager Server database. You must select a route point for a skillset used to route outbound contacts.
Keyword group	A list of words that you can search in an email message. Keyword groups associate keywords and expressions considered important by the contact center to be handled in a particular way.
Priority	The priority given to a request for a skillset agent. The lower the priority number, the greater the priority. The values of the priorities range from 1 to 6. For example, a call with priority 1 is handled before a call with priority 6.
Will close contact	Select the check box to close the email contact after the system delivery failure rule determines that the contact is not appropriate for the contact center. Clear the check box to leave the email contact open for review.

Configuring Microsoft Exchange for sending outgoing email

If Microsoft Exchange is installed on your email server, configure it to send outgoing email from the Contact Center Multimedia Agent Desktop.

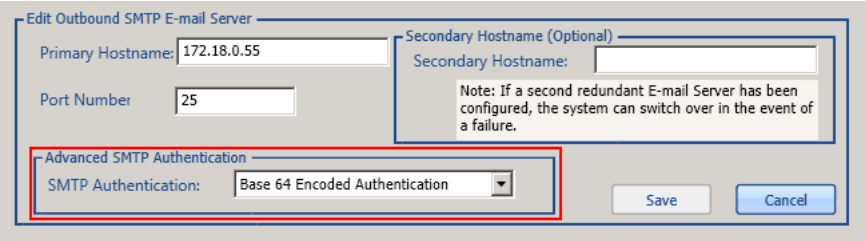
If you use Microsoft Exchange 2003, additional configuration is not required.

Prerequisites

- Ensure that you use Microsoft Exchange 2007 or later on your email server.

Procedure steps

Step	Action
1	Log on to the Voice and Multimedia Contact Server.
2	Start Internet Explorer.
3	Log on to Contact Center Manager Administration with administrative privileges.
4	On the **Launchpad**, click **Multimedia**.
5	In the left column of the CCMM Administration tool, click **General Administration**.
6	Click **Server Settings**.
7	Select the **Outbound Server (SMTP)**.
8	Click **Edit**.
9	Under **Advanced SMTP Authentication**, select **Base 64 Encoded Authentication**.



10	Click **Save**.
11	Close the Contact Center Manager Administration window.
12	Log on to the Exchange server.
13	Open the **Exchange Management** Console.
14	Click **Server Configuration**, **Hub Transport**, **Receive Connectors Tab**.
15	Right-click **Default <Servername>** and click **Properties**.
16	Click the **Authentication** tab.
17	Disable all authentication except the following: • Basic Authentication • Exchange Server Authentication • Integrated Windows Authentication
18	Close the **Exchange Management** Console.

--End--

Orchestration Designer commissioning

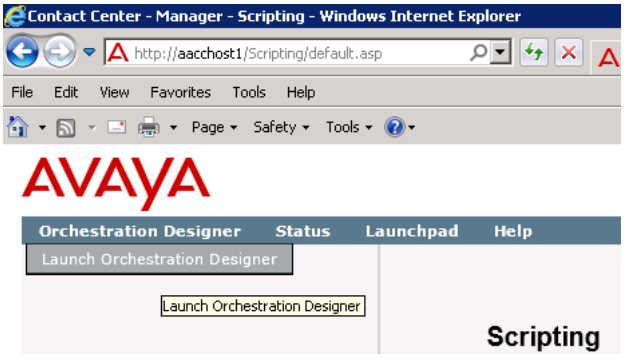
This chapter describes how to commission Orchestration Designer and create an application flow to route contacts to an appropriate queue in the contact center.

Installing the Orchestration Designer client

Install the Orchestration Designer client to manage Contact Center applications. Applications route contacts based on contact criteria, such as skillset or customer name.

Procedure steps

Step	Action
1	Start Internet Explorer.
2	In the **Address** box, type http://<Voice and Multimedia Contact Server name>. For example, type **http://AACCHOST1**
3	Press **Enter**.
4	Log on to the Contact Center Manager Administration browser as webadmin using the configured password.
5	On the **Launchpad**, click **Scripting**.
6	In the **Scripting** window, click **Orchestration Designer**, and then click **Launch Orchestration Designer**.



7	In the message box requesting you to download a .msi file, click **OK**.
8	In the dialog box, click **Run**.
9	In the **Orchestration Designer- InstallShield Wizard**, click **Next**.

10 In the **User Name** box, type a name.

11 In the **Organization** box, type your company name.

12 Select **Anyone who uses this computer (all users)**.

13 Click **Next**.

14 Accept the default **Destination Folder**.

15 Click **Next**.

16 Click **Install**.

17 Click **Finish**.

--End--

Opening Orchestration Designer

Open Orchestration Designer to configure the routing in your contact center environment.

Procedure steps

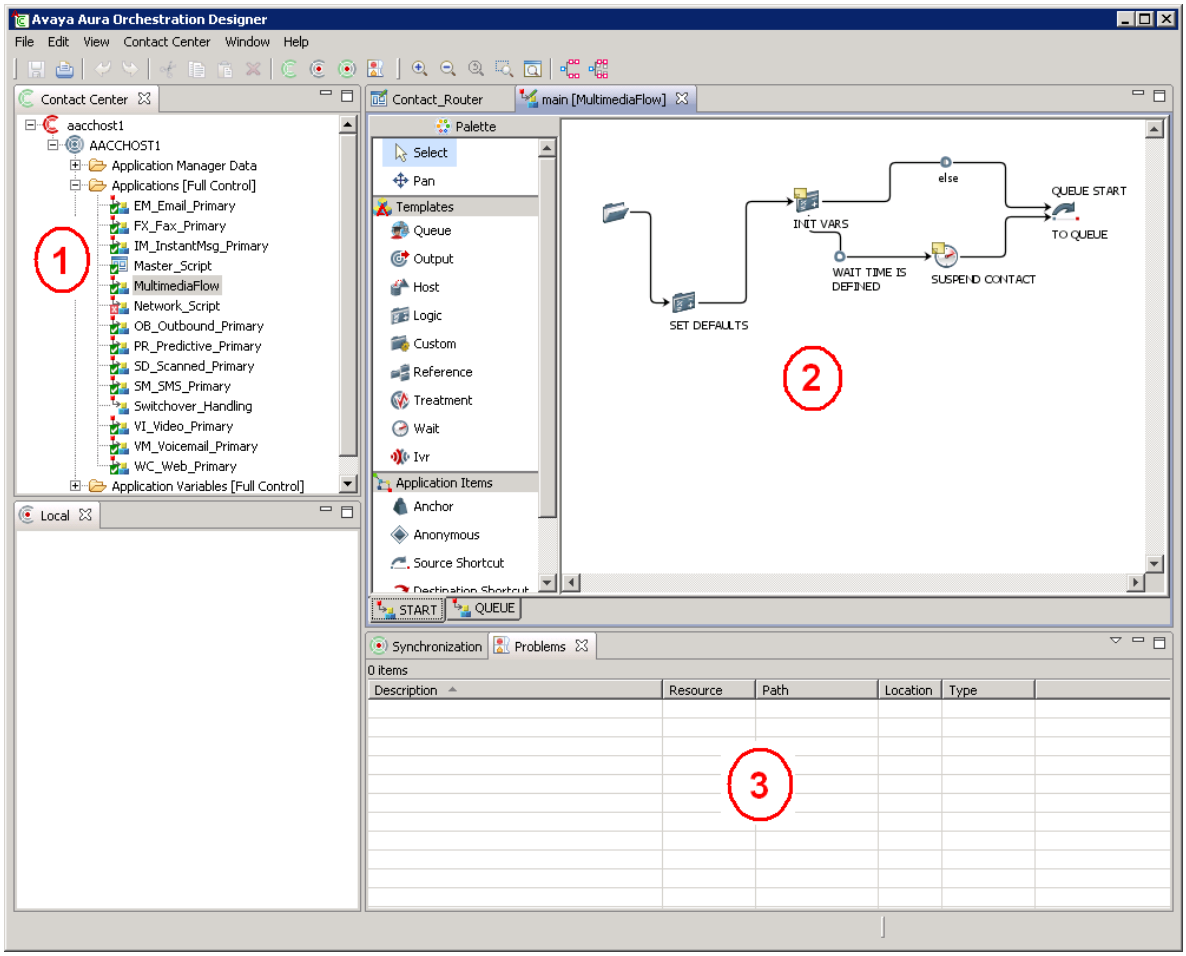
Step	Action
1	Open the Contact Center Manager Administration browser.
2	Log on to the Contact Center Manager Administration application as a user with scripting access.
3	Click **Scripting**.
4	Click Orchestration Designer menu, and then click **Launch** Orchestration Designer.

--End--

Procedure job aid

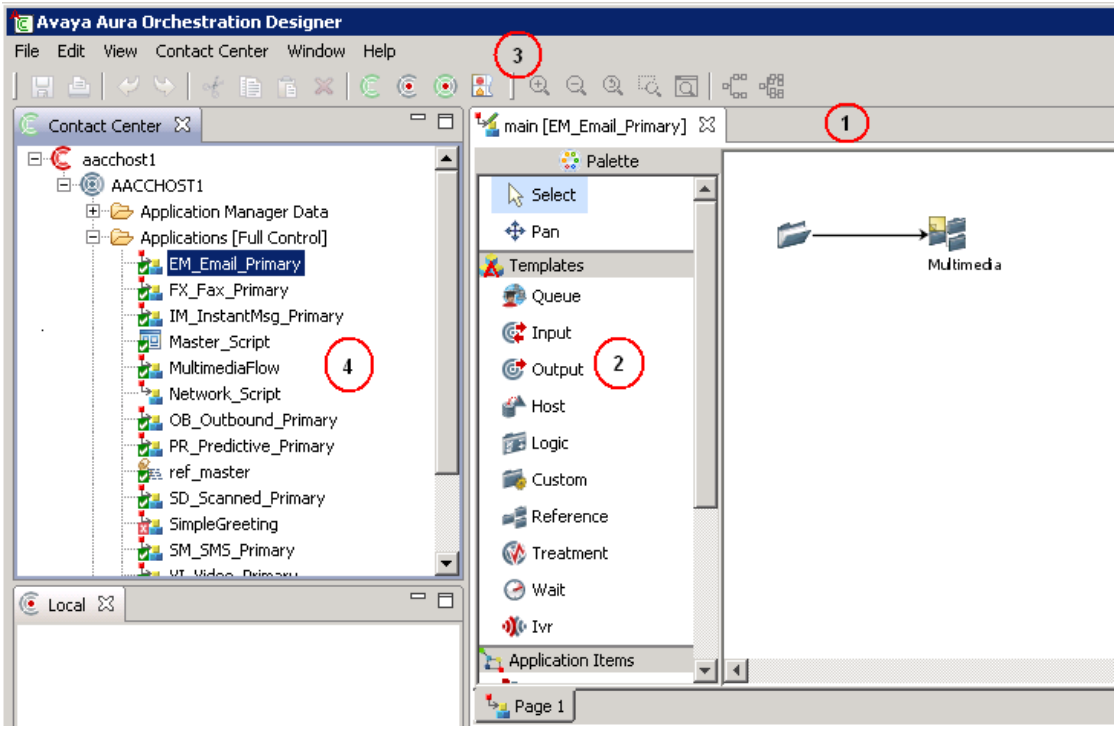
The following images displays Orchestration Designer for Contact Center. Each part of the window contains a label that describes what appears in the panel.

Orchestration Designer for Contact Center



1	Contact Center view: The Contact Center view of Orchestration Designer shows all applications, application variables, and application management data currently configured in your Contact Center.
2	Application editor view: The Application editor is the main tool to create or modify the applications. It provides the canvas on which to place the blocks to build your Contact Center applications.
3	Problems view: The Problems view shows the errors in the current script or flow application. You can use the Problems view to determine the location and cause of the problem.

Orchestration Designer tabs



1	View tabs: The tabs located across the top of the Application editor represent main pages and block editors for the flow applications on which you work.
2	Palette bar: The icons represent blocks that you can use to build your Contact Center applications. The blocks you see depend on the switch you use in your Contact Center.
3	Edit bar: Located horizontally above the Application editor, provides quick access to cut, copy, paste, delete. It also contains formatting buttons for your application.
4	Application Manager Data folder contains a list of all the agents, skillsets, CDNs, and DNISs. Applications folder contains a list of all the applications in the system. Applications are used to control how contacts are routed through the Contact Center and the treatment each contact receives. Applications Variables contains a list of all the variables in the system. Variables are used to change the nature of a flow at run time without changing the application.

You can also start Orchestration Designer from the Start menu. Click Start, All Programs, Avaya, Contact Center, Orchestration Designer.

If you start Orchestration Designer using the Start menu, you can create and work with applications and variable data in a local version of Orchestration Designer without affecting the working contact center.

The local version of Orchestration Designer allows you to perform the following tasks:

- Access all information without restrictions by access classes.
- Perform updates without affecting your Contact Center applications.
- Create applications using Orchestration Designer before the rest of the Contact Center software is installed.

By default, the Local and Problems views appear in your Orchestration Designer window. The top right corner is reserved for the script or flow application editor.

Only one instance of Orchestration Designer can run at a time.

View name	Description
Contact Center view	The Contact Center view shows all of the applications, variables, and application management data that are currently inactive or active in your Contact Center. You can make minor changes to applications in the Contact Center view. However, Avaya recommends that you work on a copy of the application in the Local view to make significant changes.
Local view	The Local view shows all of the applications, variables, application management data, and intrinsics saved on the local machine. You need not be connected to a Contact Center Manager Administration or to the network to work with this data. You can upload applications to the Contact Center view after you finish your modifications.
Synchronization view	The Synchronization view shows the differences between all objects stored on the Contact Center Manager Server (Contact Center view) and the objects stored on the Local client (Local view) after you use the Synchronization command.
Problems view	The Problems view shows the errors in the current application. You can use the problems view to determine where the problem is, and determine the reason for the problem.

Creating a new graphical flow using Orchestration Designer

Open Orchestration Designer and create a new graphical flow application.

Procedure steps

Step	Action
1	In the **Address** box, type http://<Contact Center Manager Administration Server name>. For example, type http://AACCHOST1.
2	Press **Enter**.

3 Log on to the Contact Center Manager Administration browser as webadmin using the configured password.

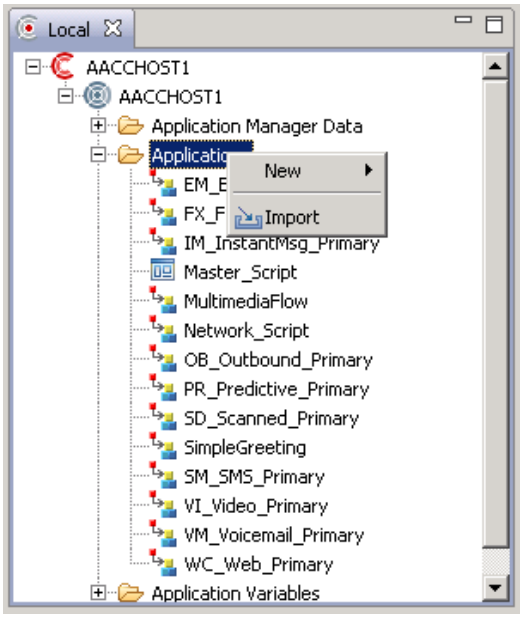
4 On the **Launchpad**, click **Scripting**.

5 Click Orchestration Designer menu, and then click **Launch** Orchestration Designer.

6 Select the **Contact Center** view, if it is not already open in the current view.

7 In the **Contact Center** pane, expand **AACCHOST1**, **AACCHOST1**.

8 Right-click **Applications [Full Control]**, and select **New**, **Application**.



9 In the **New Contact Center Application** dialog box, select **Create in Contact Center**.

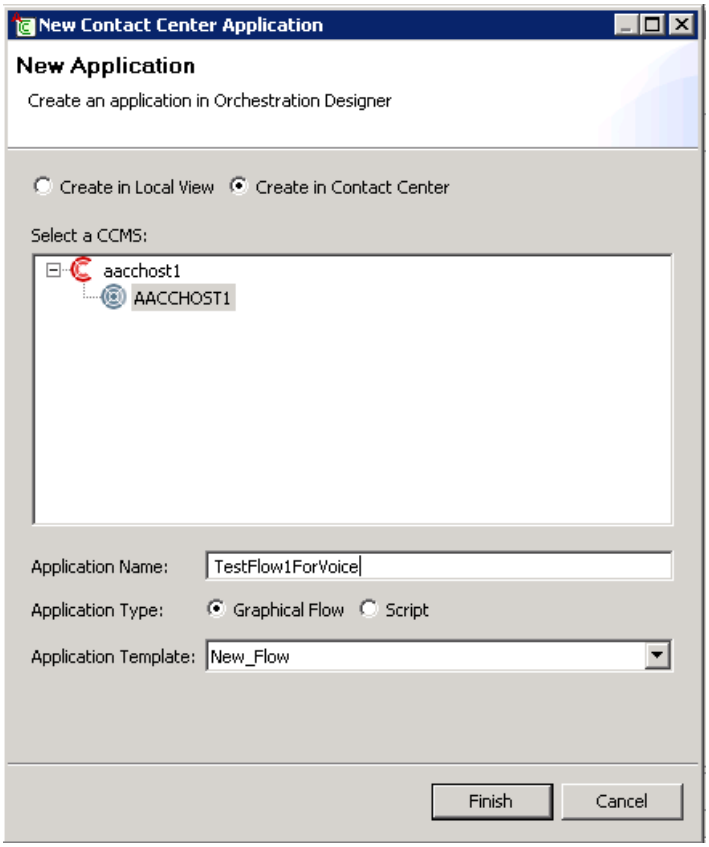
10 In the **Application Name** box, type the name of your new flow application. For this example, the name is TestFlow1ForVoice.

11 In **Application Type**, select **Graphical Flow**.

Graphical Flow is the default selection.

12 In **Application Template**, select **New_Flow**.

New_Flow is the default selection. You can choose from a variety of existing templates. For this example, start with a blank flow.



13 Click **Finish**.

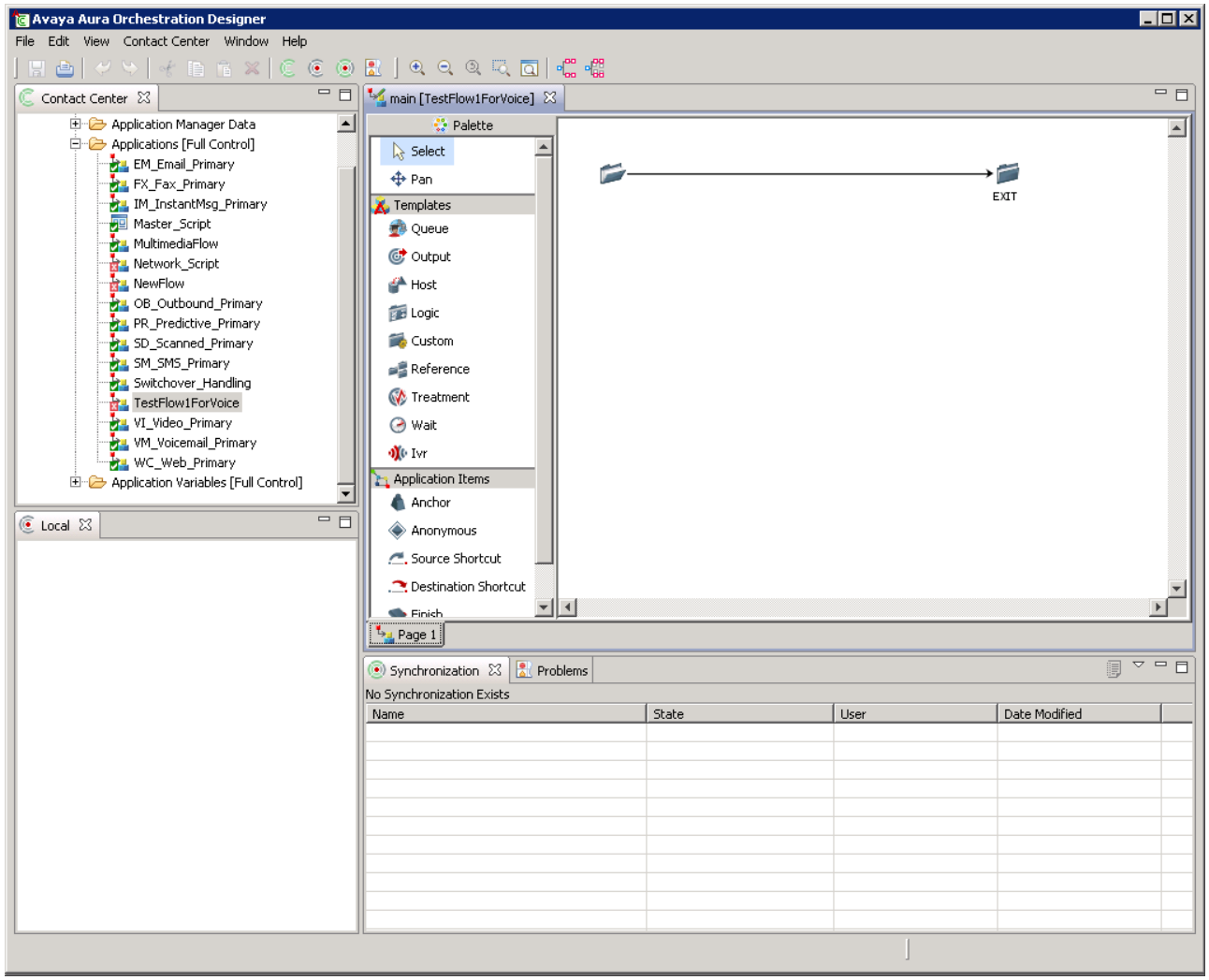
The Flow Editor opens with a Start node and an Exit node in the application flow.

--End--

Procedure job aid

Create a new Graphical Flow to route Route Point calls to the new agent skillset.

Example of a new graphical flow



Configuring a graphical flow using Orchestration Designer

Configure a graphical flow application to route contacts to an appropriate queue in the contact center.

Procedure steps

Step	Action
1	In the **Address** box, type http://<Contact Center Manager Administration Server name>. For example, type http://AACCHOST1.

2 Press **Enter**.

3 Log on to the Contact Center Manager Administration browser as webadmin using the configured password.

4 On the **Launchpad**, click **Scripting**.

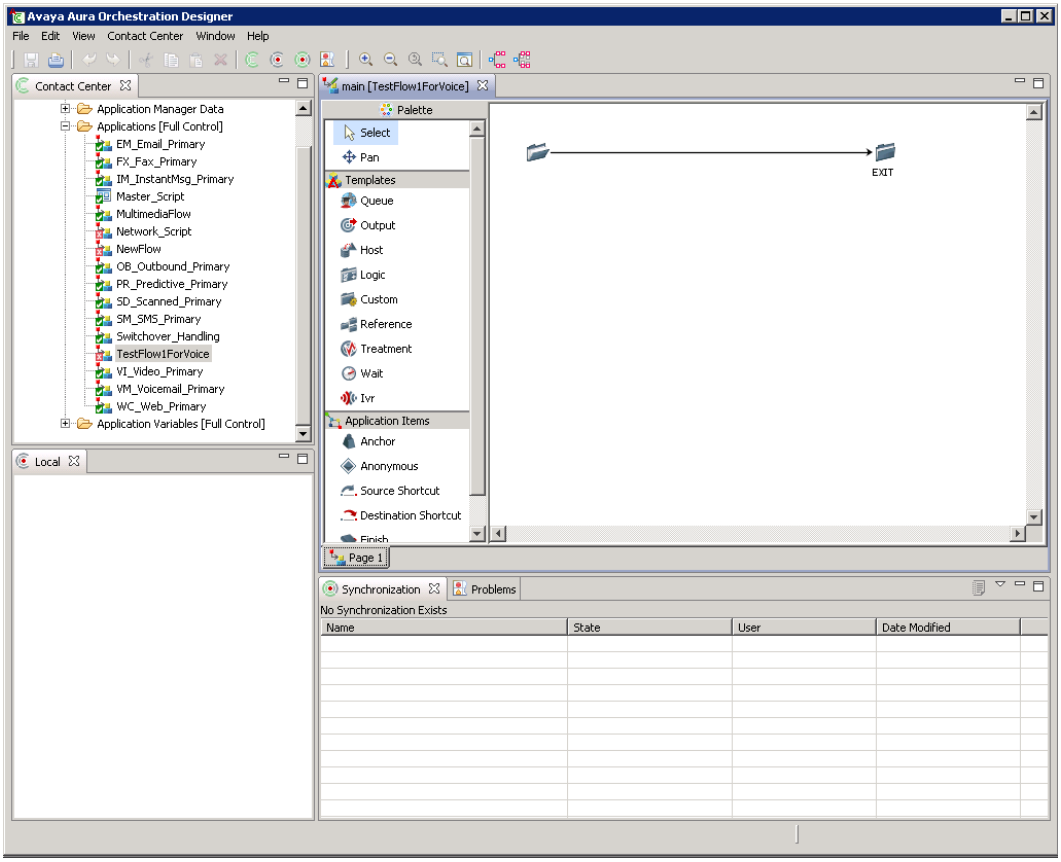
5 Click Orchestration Designer menu, and then click **Launch** Orchestration Designer.

6 Select the **Contact Center** view, if it is not already open in the current view.

7 In the **Contact Center** pane, expand **AACCHOST1**, **AACCHOST1**, **Applications [Full Control]**.

8 On the **Contact Center** pane, double-click the **TestFlow1ForVoice** application.

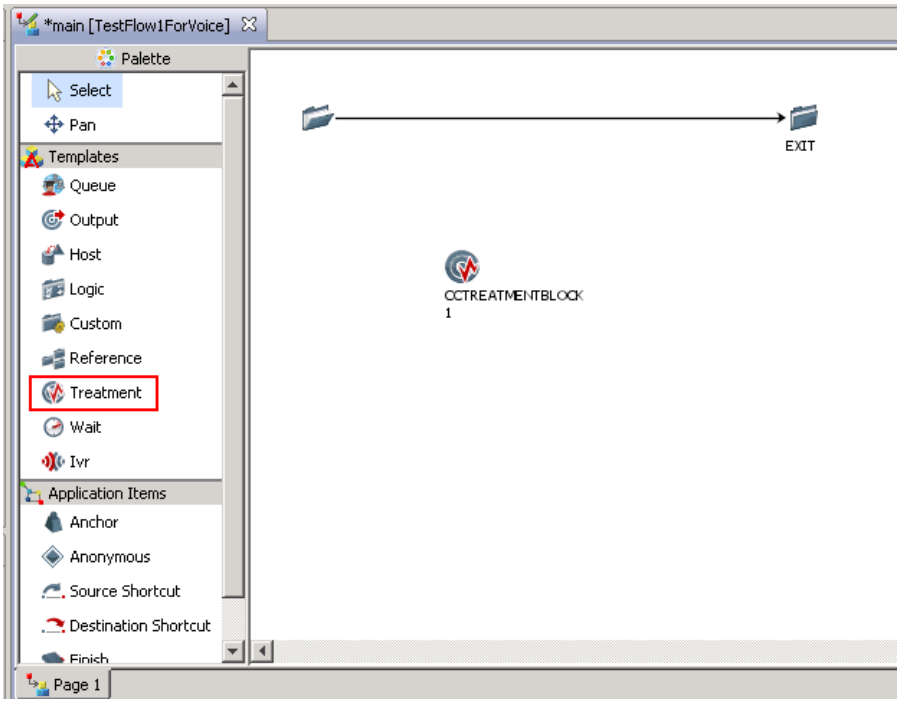
The TestFlow1ForVoice application opens in the Application view.



9 From the palette bar, select the **Treatment** block icon.

10 Click the **Main [TestFlow1ForVoice]** panel.

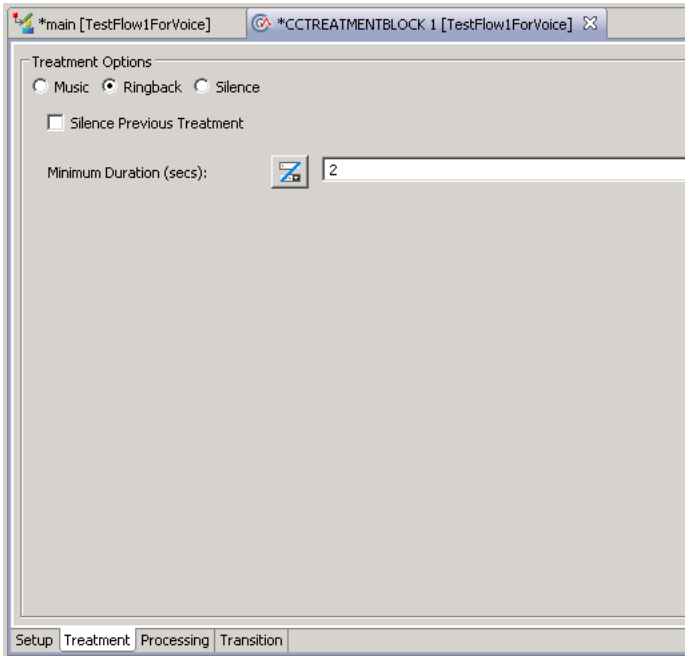
The CCTREATMENTBLOCK icon appears in the Main Flow Editor.



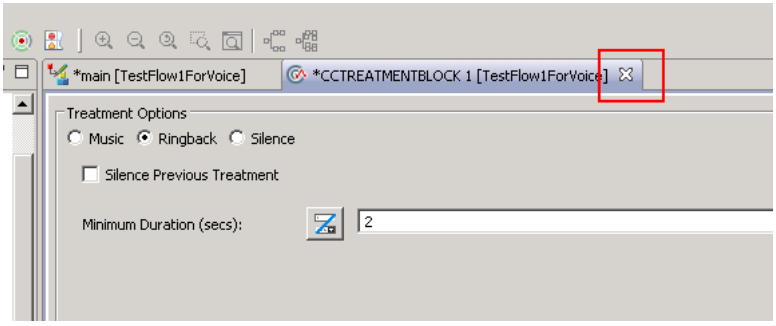
11 Double-click the **CCTREATMENTBLOCK** icon to open the details for the block.

12 Select the **Ringback** option.

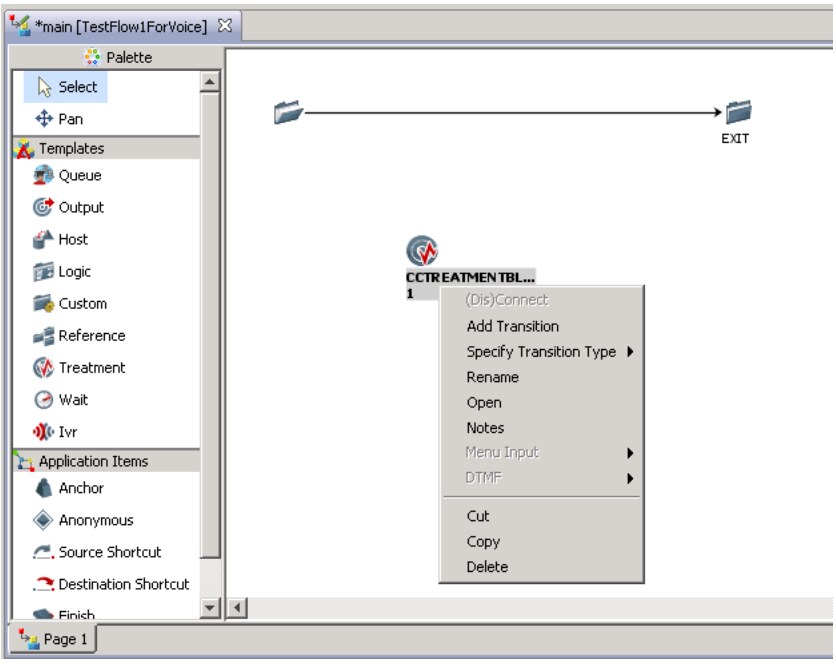
13 In the **Minimum Duration (secs)** box, type 2.



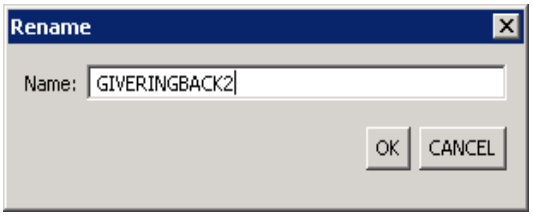
14 Click the **X** on the **Treatment** tab to save and close the treatment block.



15 Right-click on the **CCTREATMENTBLOCK** treatment block and select **Rename**.



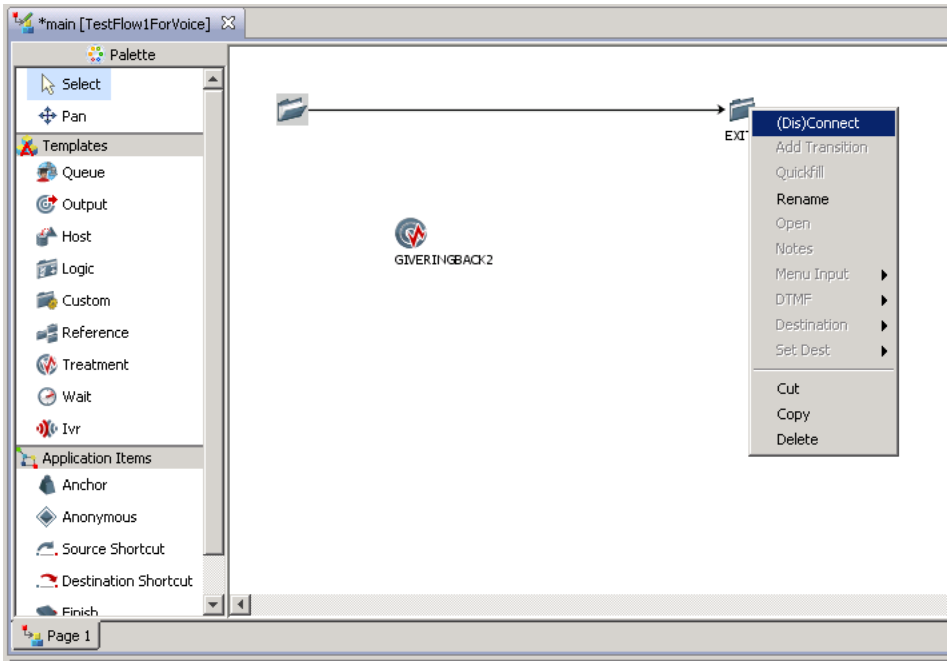
16 On the **Rename** dialog, in the **Name** box, type the new name for the block, for example, type GIVERINGBACK2.



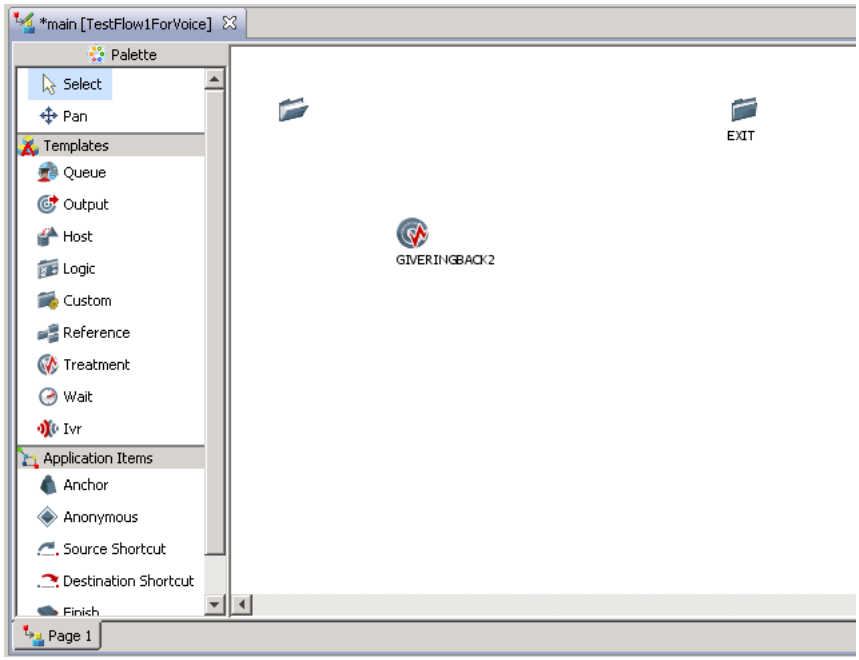
17 Click **OK**.

18 In the **Main [TestFlow1ForVoice]** panel, left-click the **Start** node.

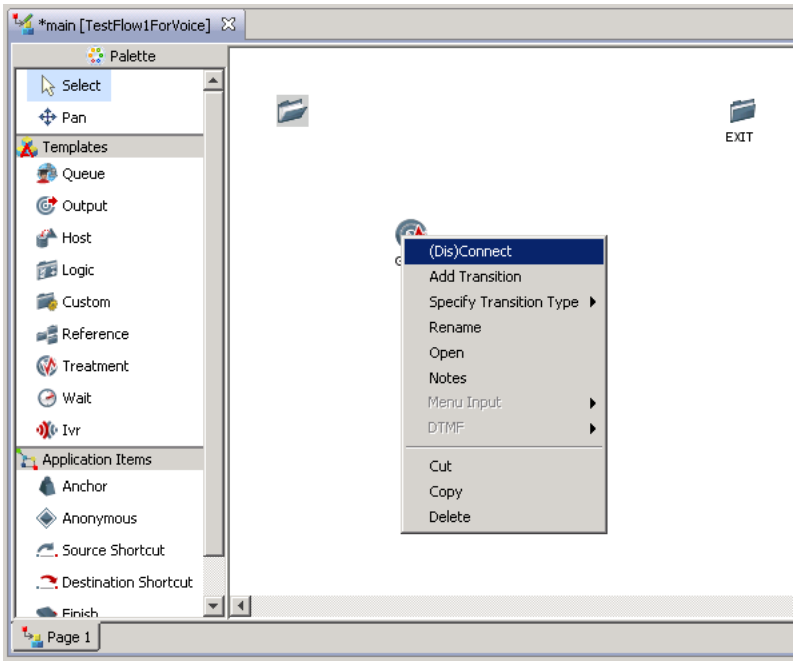
19 Right-click the **Exit** block and select **(Dis)Connect**.



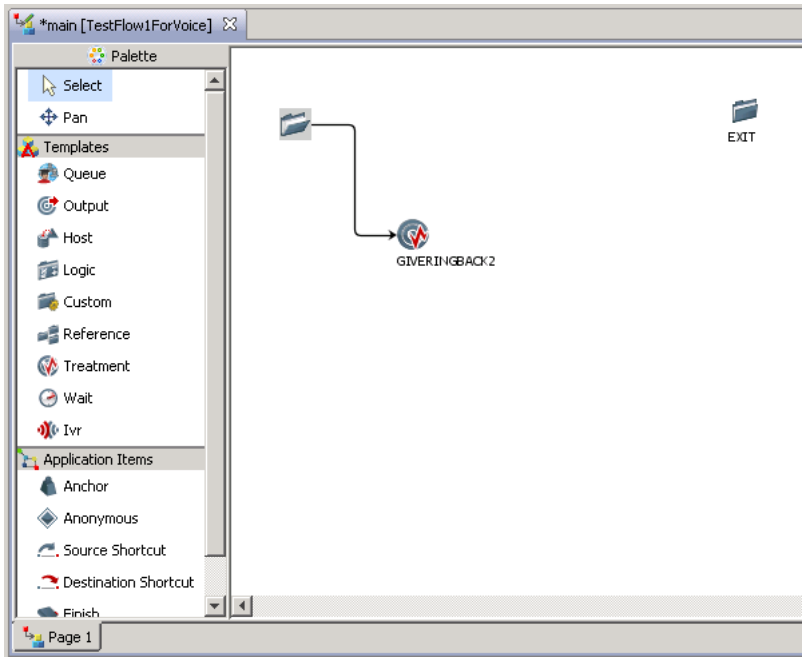
20 The link from the **Start** node to the **Exit** block disappears.



21 Left-click the **Start** node and then right-click on the **GIVERINGBACK2** treatment block, and select **(Dis)Connect**.



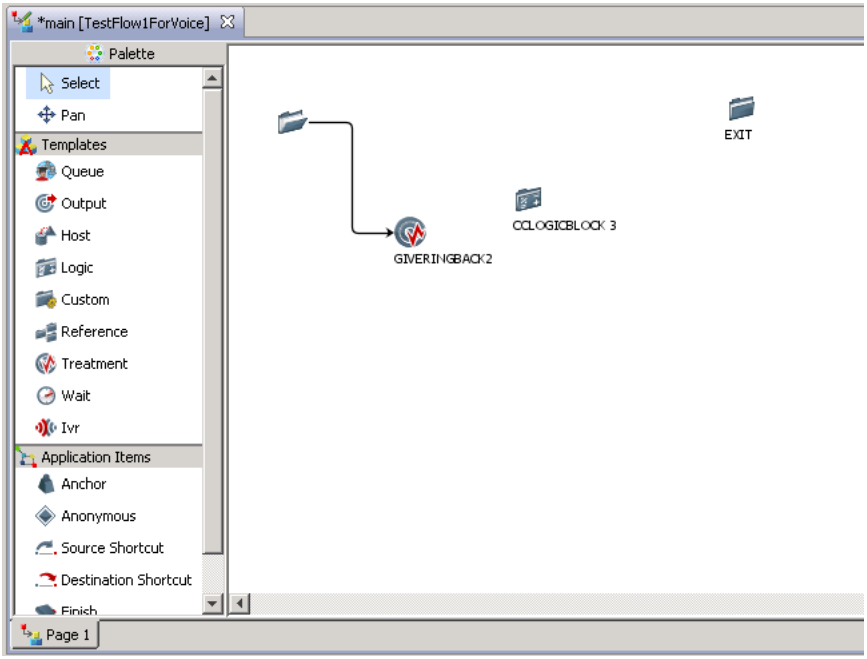
22 This creates a link from the **Start** node to the **GIVERINGBACK2** block.



23 From the palette bar, select the **Logic** block icon.

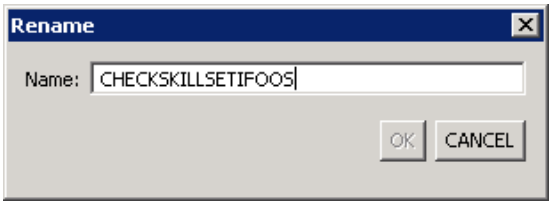
24 Click the **Main [TestFlow1ForVoice]** panel.

The CCLOGICBLOCK icon appears in the Main Flow Editor.



25 Right-click on the **CCLOGICBLOCK** logic block and select **Rename**.

26 On the **Rename** dialog, in the **Name** box, type CHECKSKILLSETIFOOS.



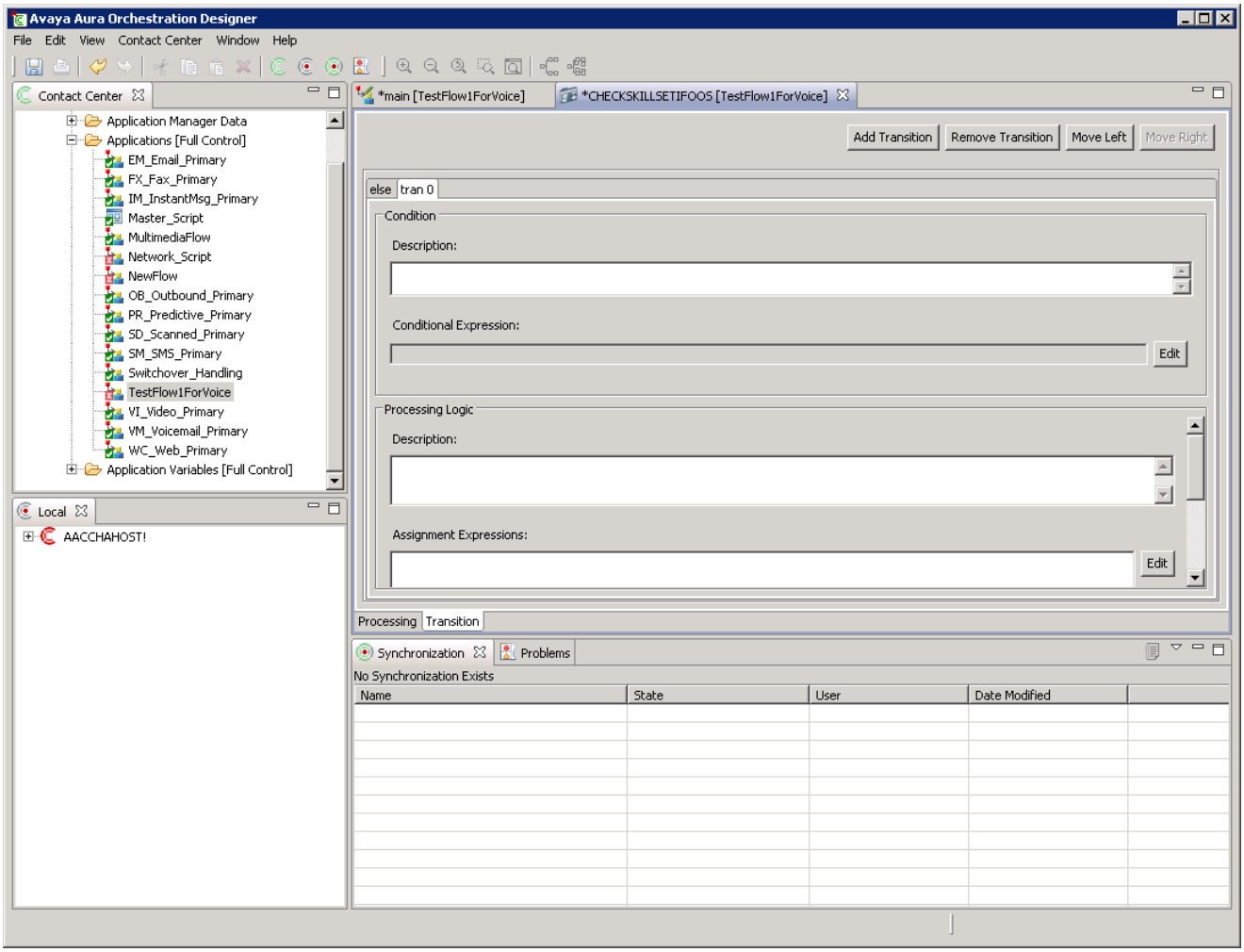
27 Click **OK**.

28 Double-click the **CHECKSKILLSETIFOOS** icon to open the details for the block.

29 Select the **Transition** pane.

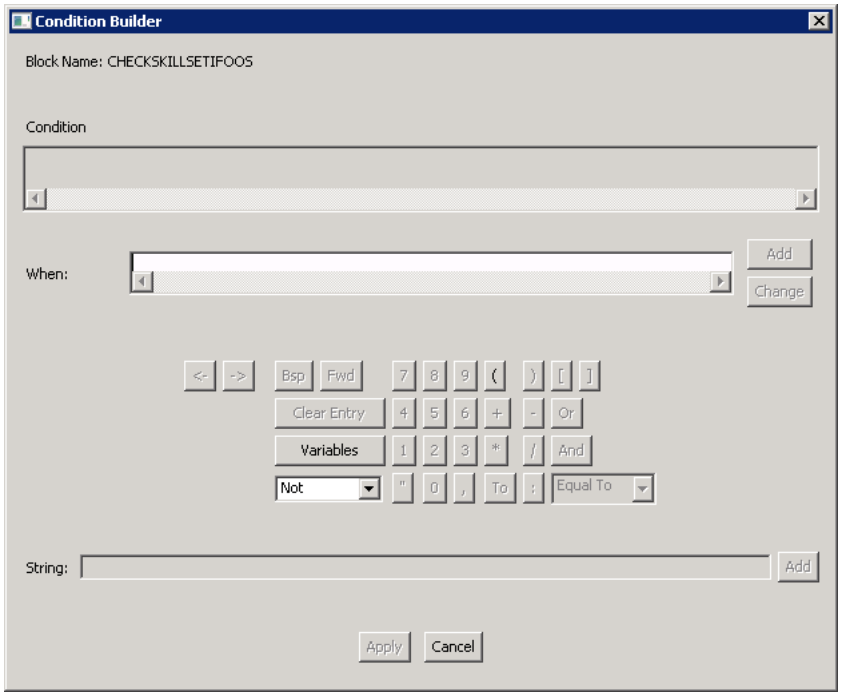
30 Click **Add Transition**.

31 Select the **tran 0** tab.



32 In the **Condition** section, click **Edit**.

The Condition Builder dialog appears.

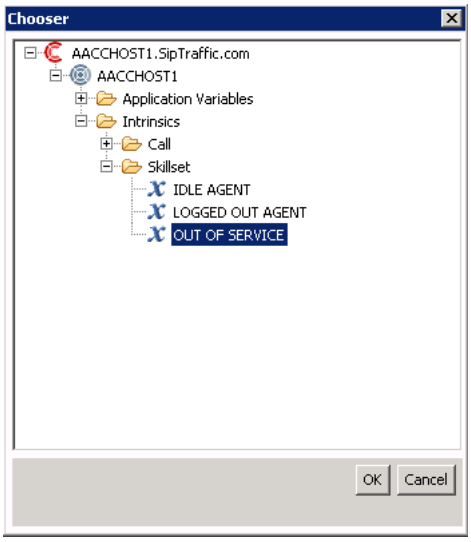


33 On the logic block **Condition Builder**, from the list, select **Not**. You must select **Not**, even if it is the default.

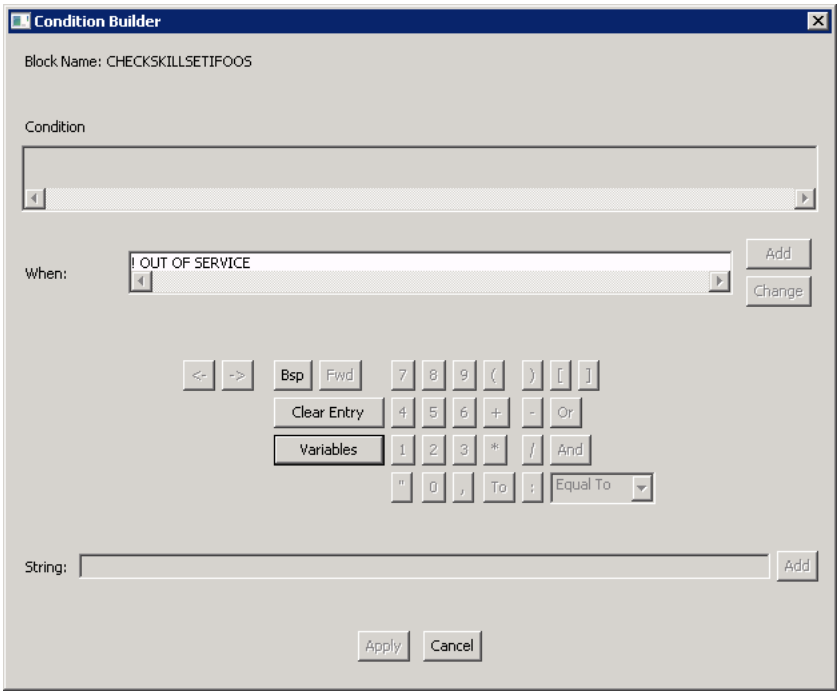
34 Click **Variables**.

A Chooser dialog appears.

35 From the **Chooser** menu, navigate to the **Skillset** options and select **OUT OF SERVICE**.

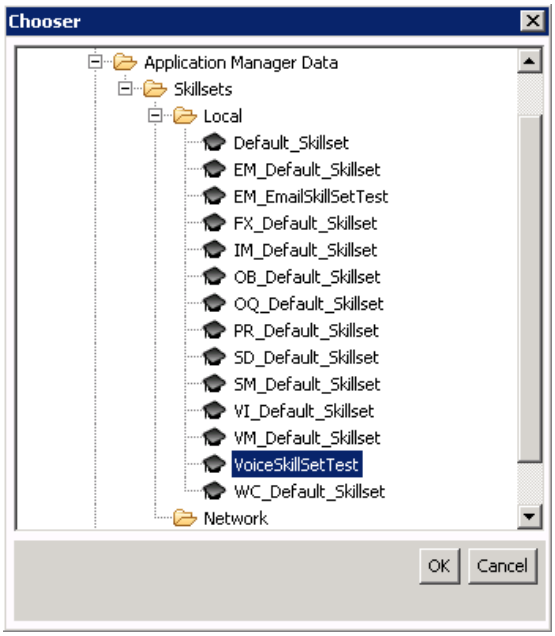


36 Click **OK**.



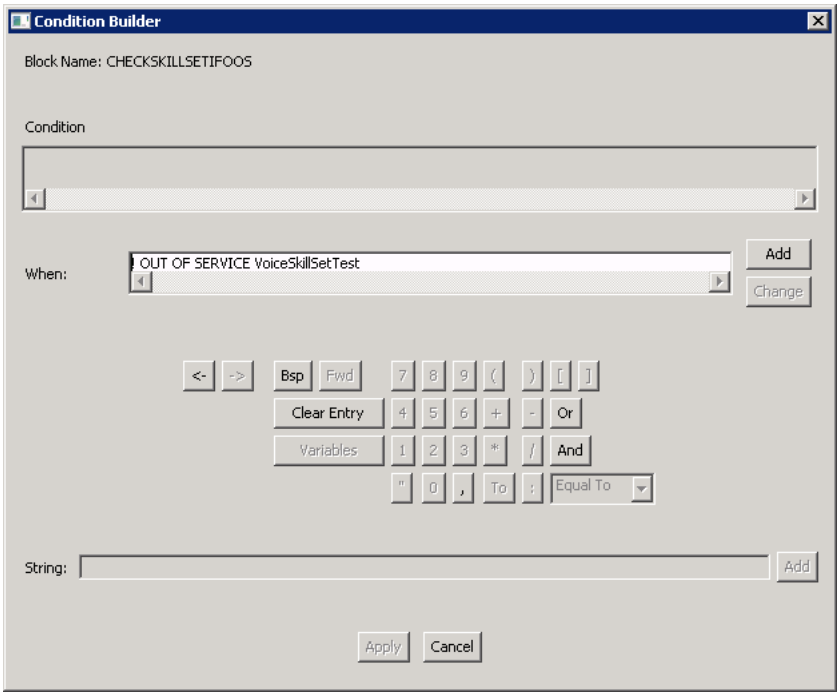
37 Click **Variables**.

38 From the **Chooser** menu, navigate to the local **Skillset** options and select the voice skillset **VoiceSkillSetTest**.

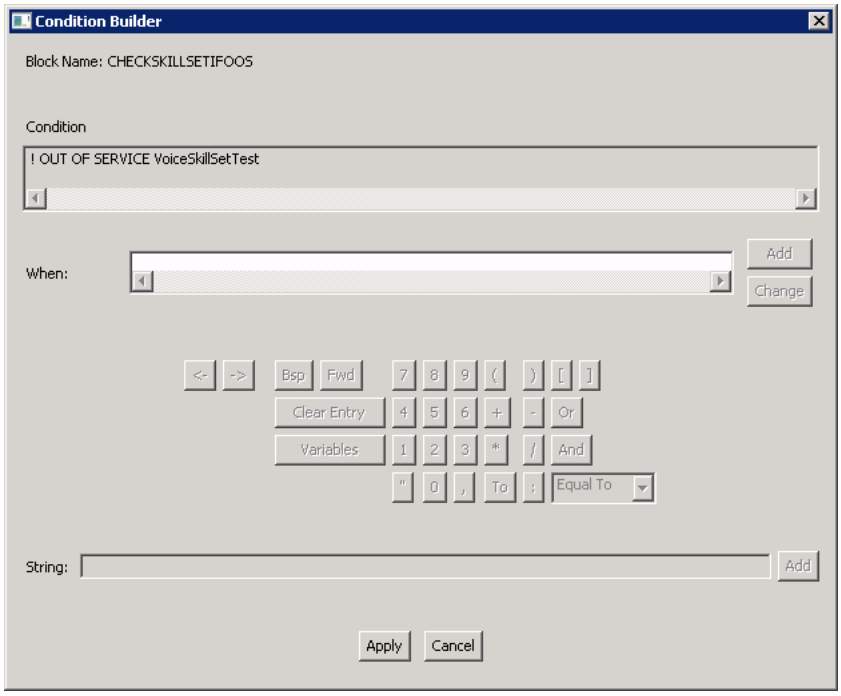


39 Click **OK**.

40 The **CHECKSKILLSETIFOOS** logic block is now configured to check if the voice skillset is in service before routing contacts to it.



41 Click **Add**, to add the expression to the condition.



42 Click **Apply**.

43 Close the **CHECKSKILLSETIFOOS** logic block.

The logic block is now configured to check that the skillset VoiceSkillSetTest is in service before routing contacts to it.

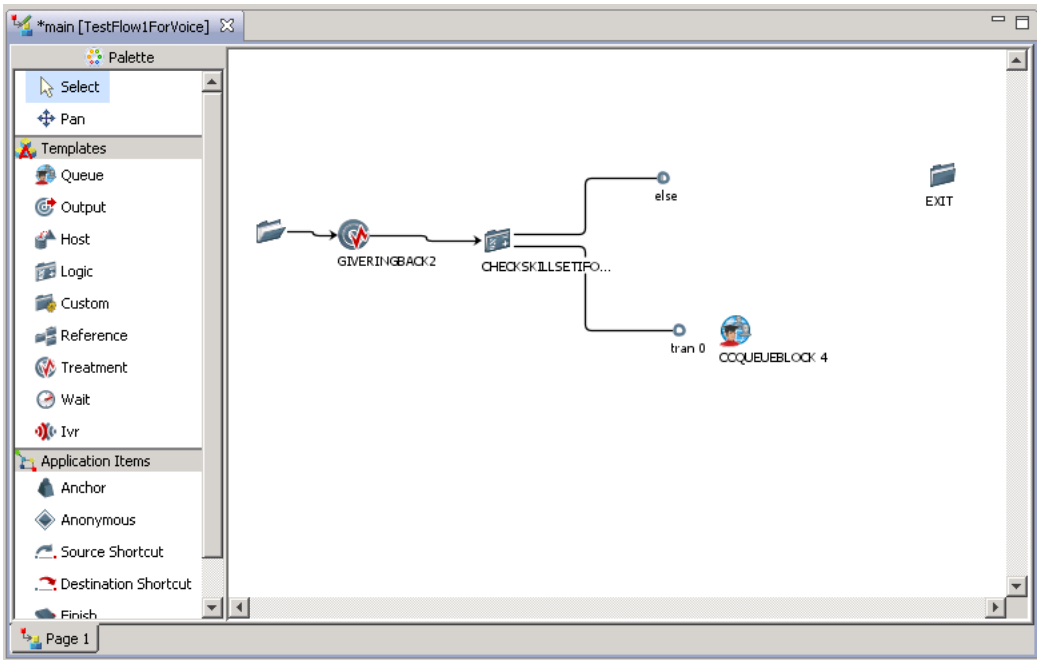
44 Left-click the **GIVERINGBACK2** treatment block and then right-click on the **CHECKSKILLSETIFOOS** logic block, and select **(Dis)Connect**.

This creates a link from the GIVERINGBACK2 treatment block to the CHECKSKILLSETIFOOS logic block.

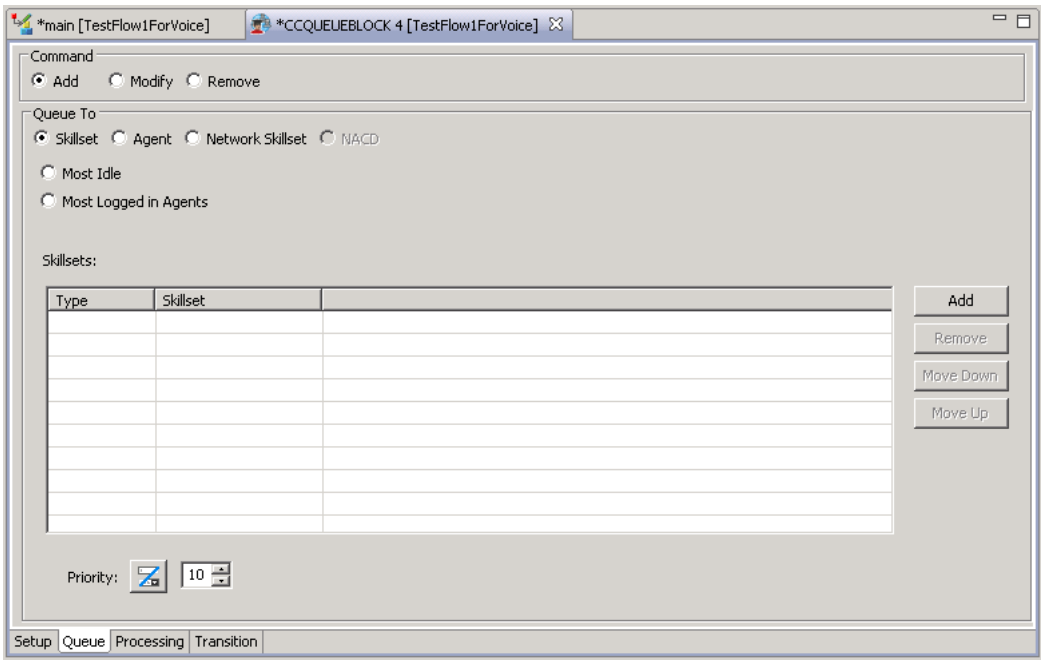
45 From the palette bar, select the Queue block icon.

46 Click the **Main [TestFlow1ForVoice]** panel.

The CCQUEUEBLOCK icon appears in the Main Flow Editor.



47 Double-click the **CCQUEUEBLOCK** icon to open the details for the queue block.



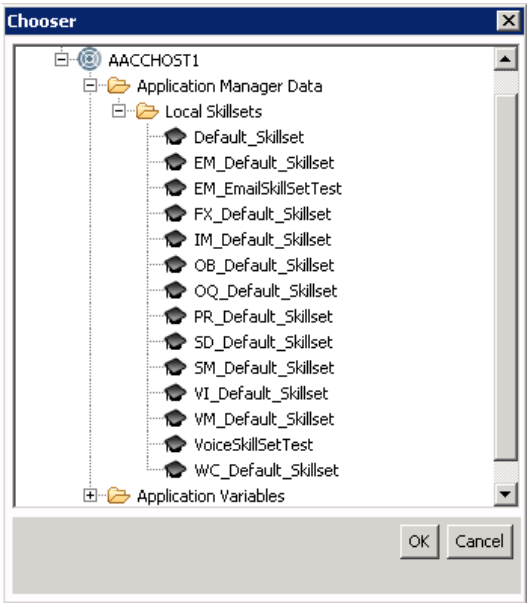
48 In the **Command** section, select **Add**.

49 In the **Queue To** section, select **Skillset**.

50 Click **Add**.

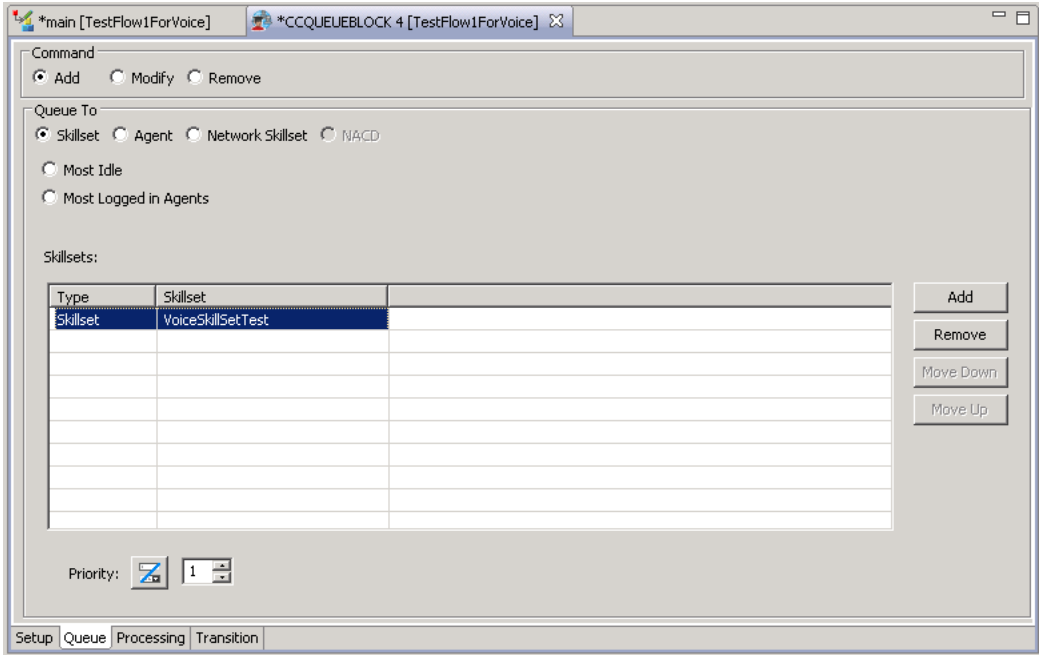
A Chooser dialog appears.

51 On the **Chooser** dialog, navigate to the **Local Skillsets**.



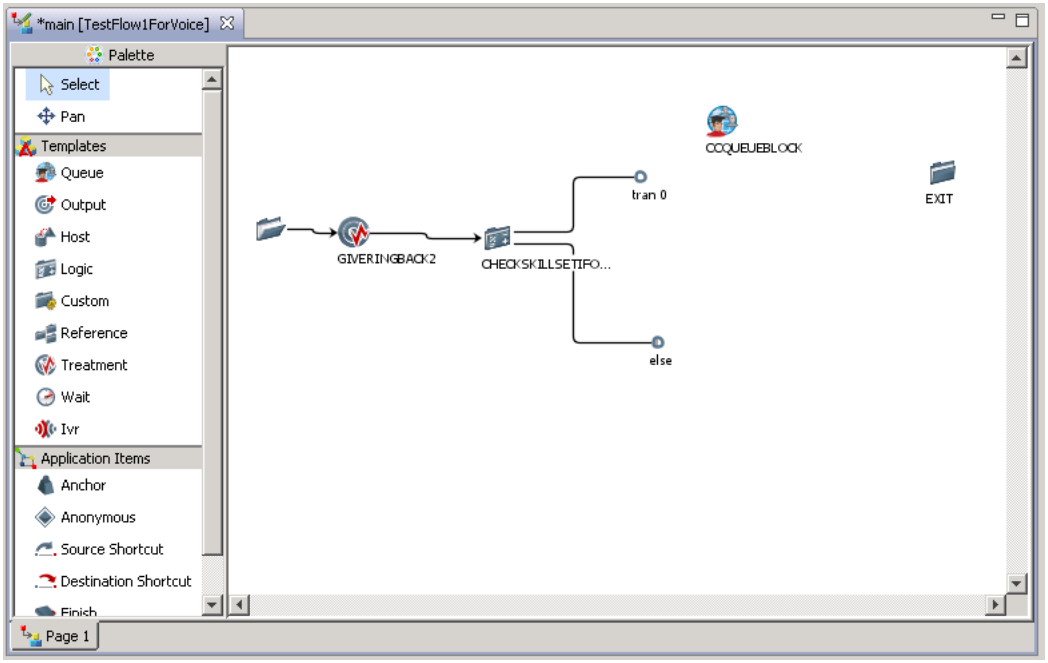
52 Select the **VoiceSkillSetTest** voice skillset.

53 Click **OK**.



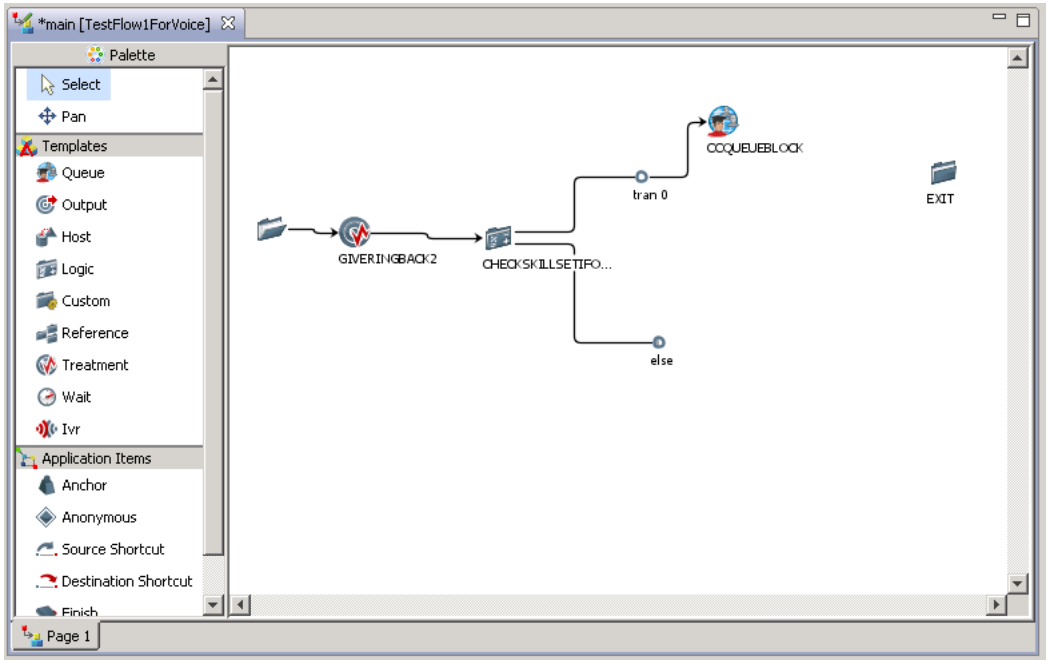
54 Change the **Priority** to **1**.

55 Close the **CCQUEUEBLOCK** queue block.



56 Left-click on the **CHECKSKILLSETIFOOS** logic block - **tran 0** condition and then right-click on the **CCQUEUEBLOCK** queue block, and select **(Dis)Connect**.

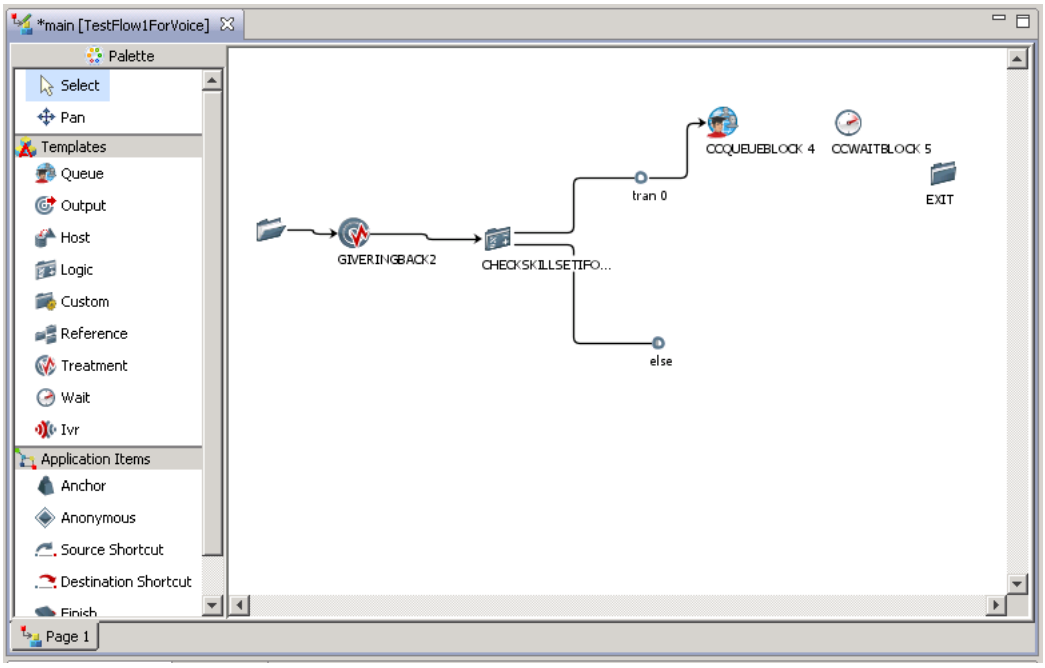
This creates a link from the CHECKSKILLSETIFOOS logic block - tran 0 condition, to the CCQUEUEBLOCK queue block.



57 From the palette bar, select the **Wait** block icon.

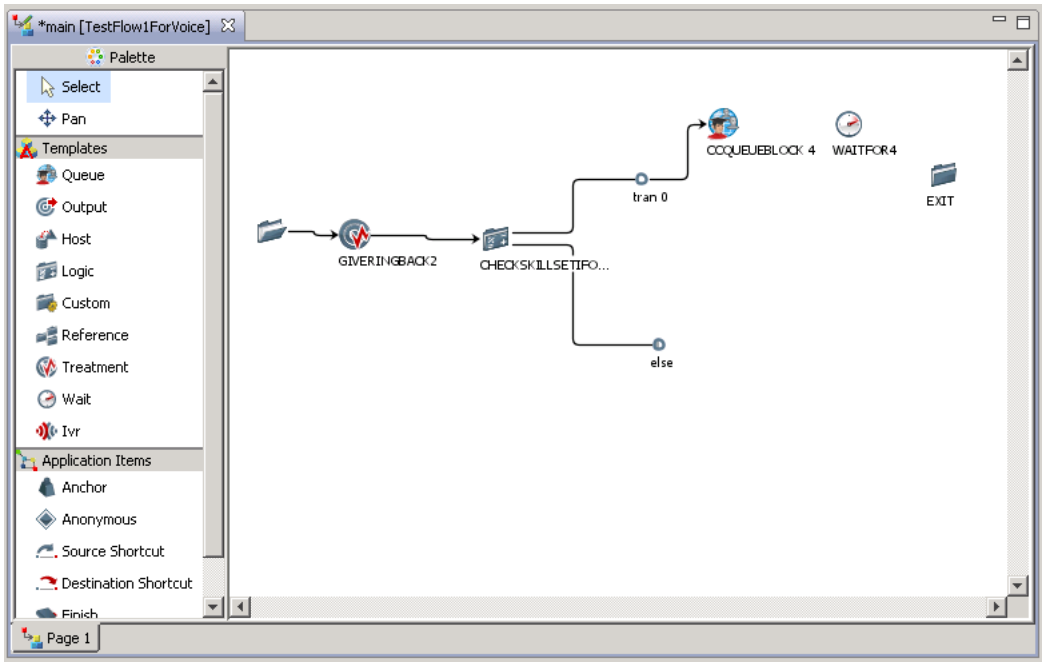
58 Click the **Main [TestFlow1ForVoice]** panel.

The CCWAITBLOCK icon appears in the Main Flow Editor.

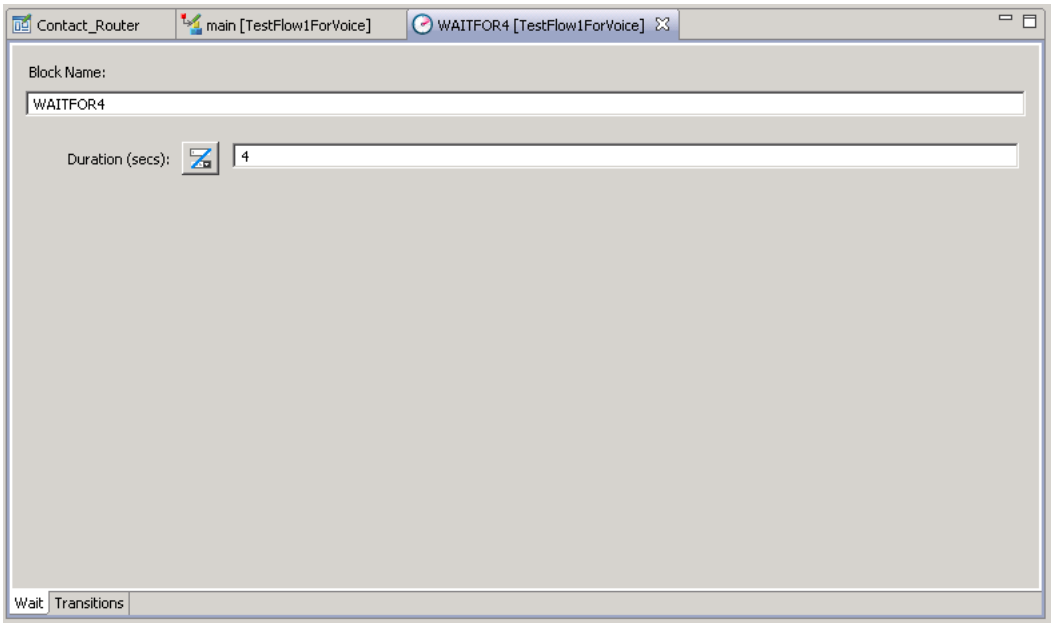


59 Right-click on the **CCWAITBLOCK** wait block and select **Rename**.

60 On the **Rename** dialog, in the **Name** box, type WAITFOR4.



61 Double-click the **WAITFOR4** wait block icon to open the details for the block.



62 In the **Duration (secs)** box, type 4.

63 Close the **WAITFOR4** wait block.

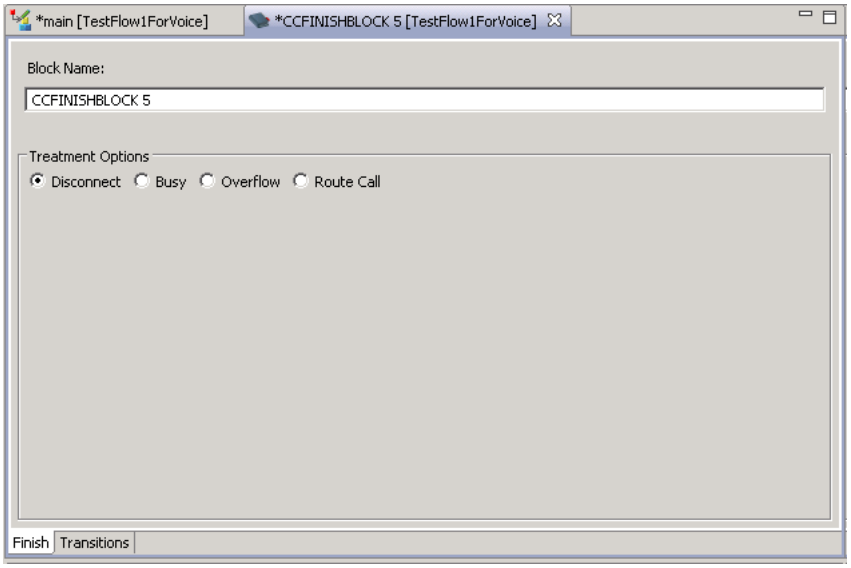
64 Left-click on the **CCQUEUEBLOCK** block and then right-click on the **WAITFOR4** block, and select **(Dis)Connect**.

65 From the **Application Items** menu, select the **Finish** block icon.

66 Click the **Main [TestFlow1ForVoice]** panel.

The CCFINISHBLOCK finish icon appears in the Main Flow Editor.

67 Double-click the **CCFINISHBLOCK** finish block icon to open the details for the block.



68 Select the **Disconnect** option.

69 Close the **CCFINISHBLOCK** finish block.

70 Left-click on the **WAITFOR4** wait block and then right-click on the **CCFINISHBLOCK** finish block, and select **(Dis)Connect**.

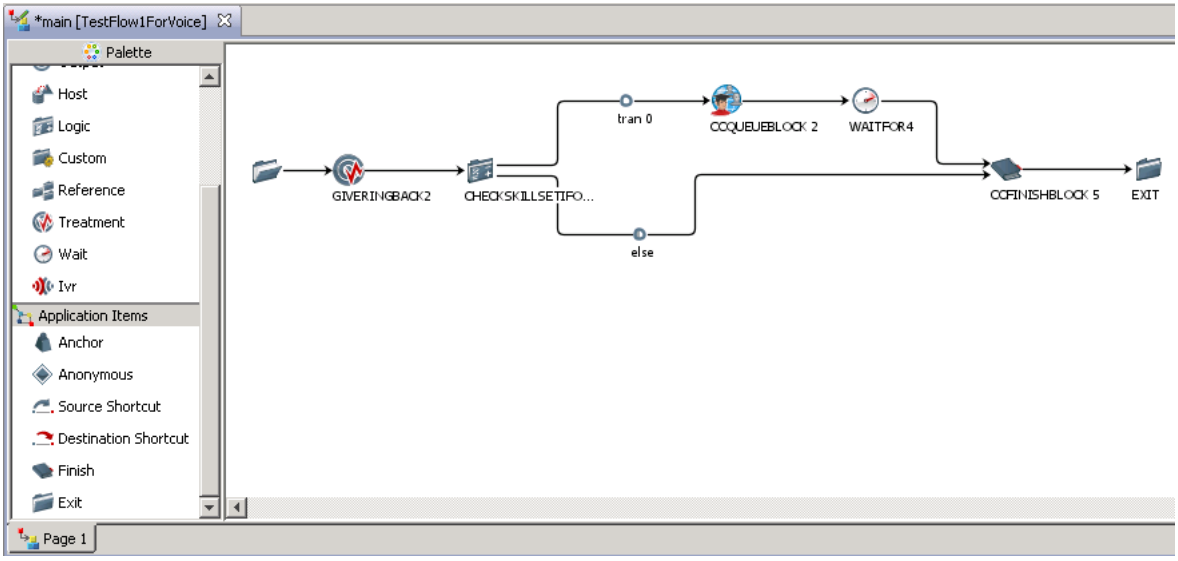
This creates a link from the WAITFOR4 wait block to the CCFINISHBLOCK finish block.

71 Left-click on the **CHECKSKILLSETIFOOS** logic block - **else** condition and then right-click on the **CCFINISHBLOCK** finish block, and select **(Dis)Connect**.

This creates a link from the CHECKSKILLSETIFOOS logic block to the CCFINISHBLOCK finish block.

72 Left-click on the **CCFINISHBLOCK** finish block and then right-click on the **EXIT** block, and select **(Dis)Connect**.

This create a link from the CCFINISHBLOCK finish block to the EXIT block.

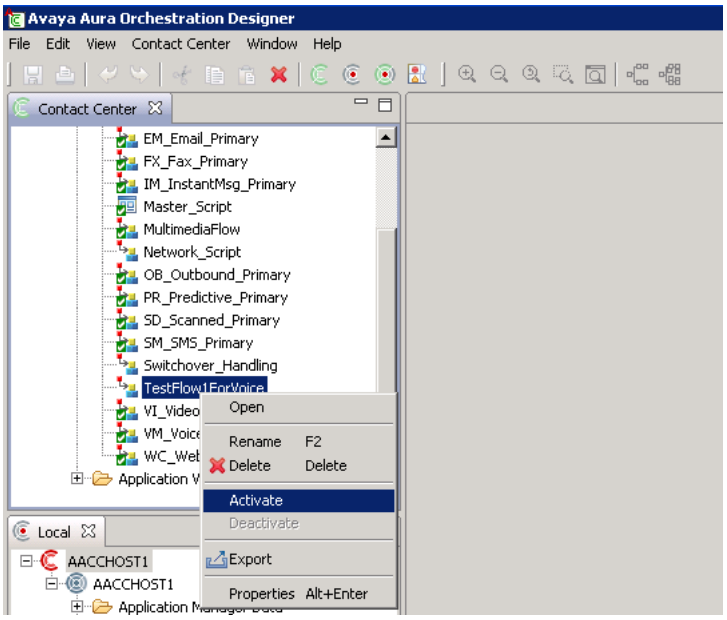


73 Select the **Main [TestFlow1ForVoice]** panel.

74 Click the **X** on the **Main [TestFlow1ForVoice]** panel to save and close the flow application.

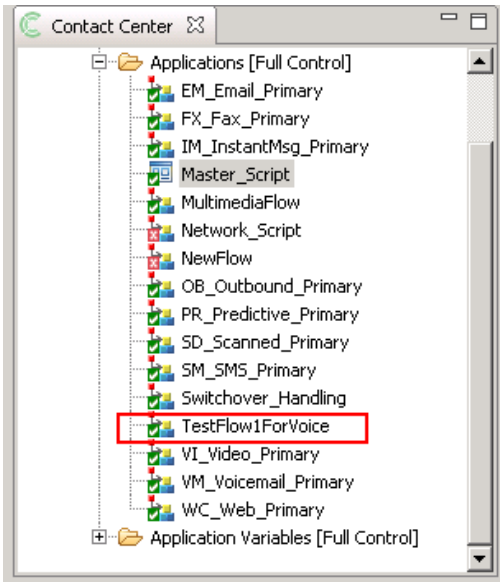
75 On the Save Resource dialog box, click **Yes** to save your changes.

76 To activate the flow, right-click on the flow in Contact Center view, and select **Activate**.



77 On the **Activate Application** message box, click **OK**.

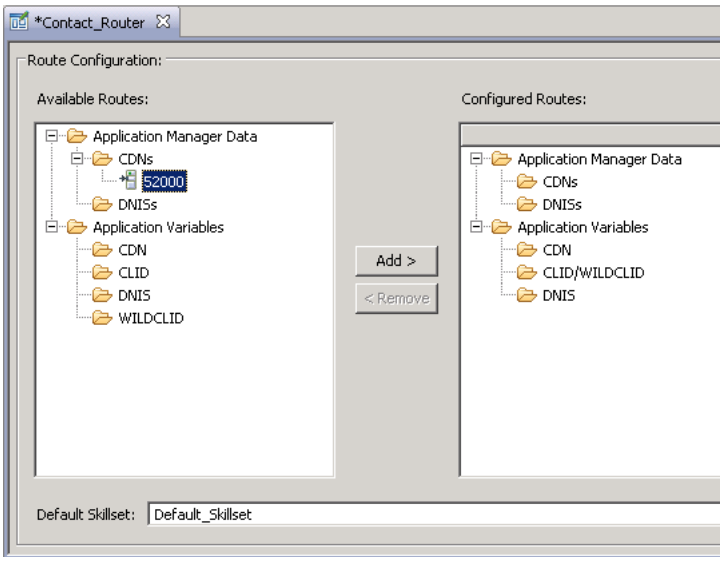
The TestFlow1ForVoice flow activates.



78 In the **Contact Center** view, double-click on **Master_Script**.

79 In the **Application** view, select **Contact_Router**.

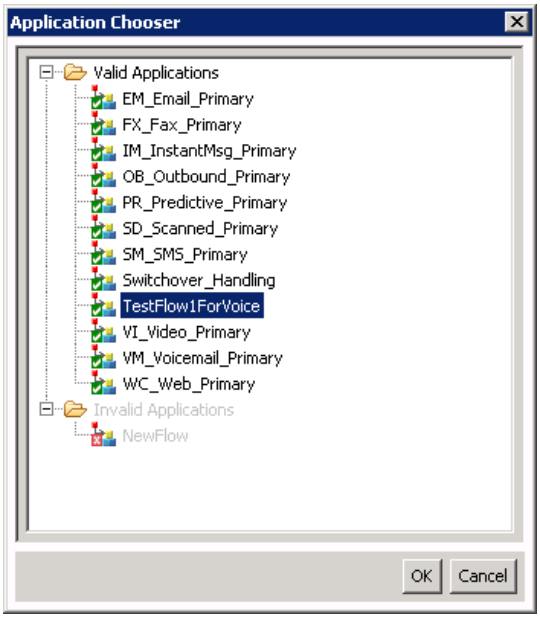
80 In the **Route Configuration** section, under **Available Routes**, **Application Manager Data**, expand **CDNs** and select your CDN or Route Point. For example, select **52000**.



81 Click **Add**.

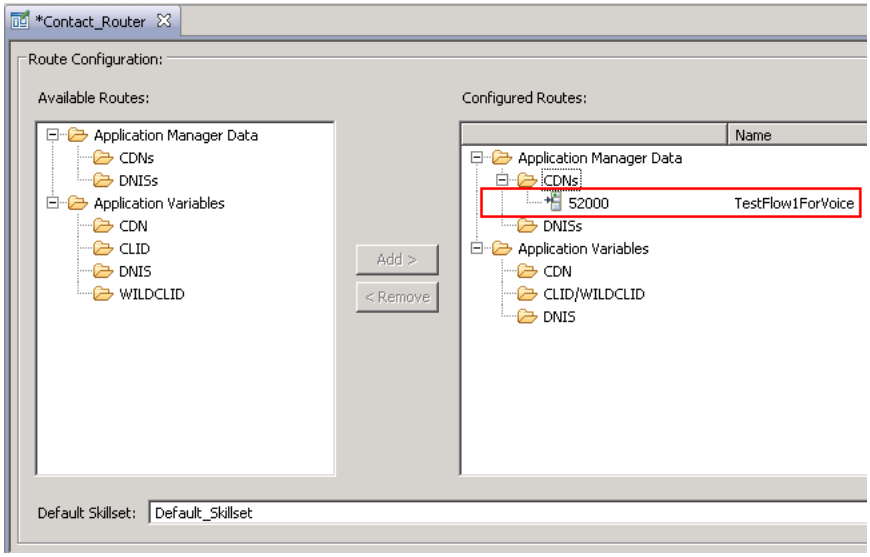
An Application Chooser dialog appears.

82 On the **Application Chooser**, select **TestFlow1ForVoice**.



83 Click **OK**.

Calls to the 52000 CDN (Route Point) are routed to the TestFlow1ForVoice graphical flow application for treatment and queueing to an appropriate agent skillset queue.



84 Close **Contact_Router**.

A Save Resource message box appears.

85 Click **Yes**.

86 On the **Confirm** message box, click **OK**.

--End--

Configuring the Switchover Handling script

In Contact Centers using the Mission Critical High Availability feature, the Switchover Handling Script handles calls in treatment during a switchover.

During normal operation, contacts to the Contact Center are routed to the Master script for processing, treatments and queuing to an appropriate skillset. The active CCMS server uses the media processing capabilities of Avaya Media Server to provide ringback, conferencing, and other treatments to these calls.

If the active CCMS server is shutdown or fails, a switchover occurs, and the standby CCMS server starts processing calls. The standby CCMS server is now the active CCMS server. New calls that arrive after the switchover are presented to the Master script on the currently active CCMS server and call processing continues as normal.

Calls that were in treatment on the Avaya Media Server during the switchover cannot be returned to their original active CCMS because it is no longer available, so these calls are routed to the Switchover Handling Script on the currently active CCMS.

The Switchover Handling Script expedites the calls that were in treatment at the time of the active server failure. This means that calls are queued as quickly as possible to an appropriate skillset for that contact type. This can be a default skillset, or a skillset defined by the Contact Center administrator.

Calls in treatment during a switchover may contain data, depending on their position in the script on the active server before the switchover occurred. Avaya recommends that you modify the default Switchover Handling Script to check each call for useful data. If the call has useful data or intrinsics, queue it to the most appropriate skillset as normal. If the call does not have useful data, queue the call to the appropriate default skillset.

Attention: After a High Availability switchover, multimedia contacts may be redirected to a different skillset queue. After a switchover, multimedia contacts are requeued to a skillset appropriate to their contact intrinsics. If the multimedia contacts have insufficient intrinsic data or if the appropriate skillset is Out Of Service, the multimedia contacts are queued to the default contact type skillset. Email contacts transferred to agents or Pulled Closed email contacts that are in-queue at switchover time are queued to a skillset after switchover. They are not queued to the agent.

You use Contact Center Orchestration Designer to edit the default Switchover Handling Script. The Switchover Handling script does not support commands that delay the handling of calls.

The Switchover Handling Script does not support the following HDX commands:

- SEND INFO
- SEND REQUEST
- GET RESPONSE

The Switchover Handling Script does not support the following commands:

- EXECUTE SCRIPT
- GIVE BUSY
- GIVE MUSIC
- GIVE OVERFLOW
- GIVE RAN
- GIVE RINGBACK
- GIVE SILENCE

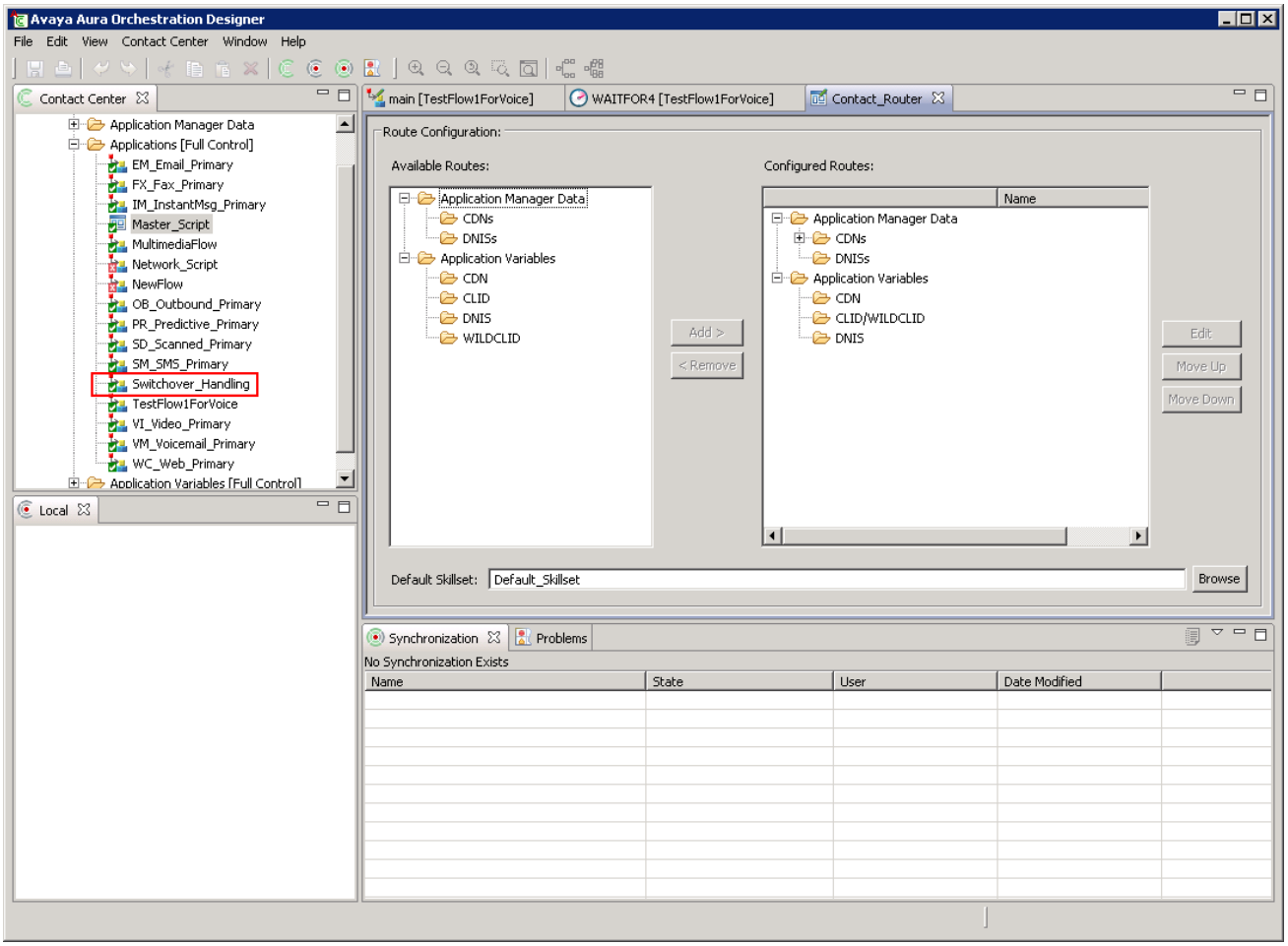
A Switchover Handling Script containing these commands does not validate in Contact Center Orchestration Designer.

The Switchover Handling Script is used only in Mission Critical High Availability solutions.

Other applications cannot start the Switchover Handling Script, and the Switchover Handling Script cannot start other applications.

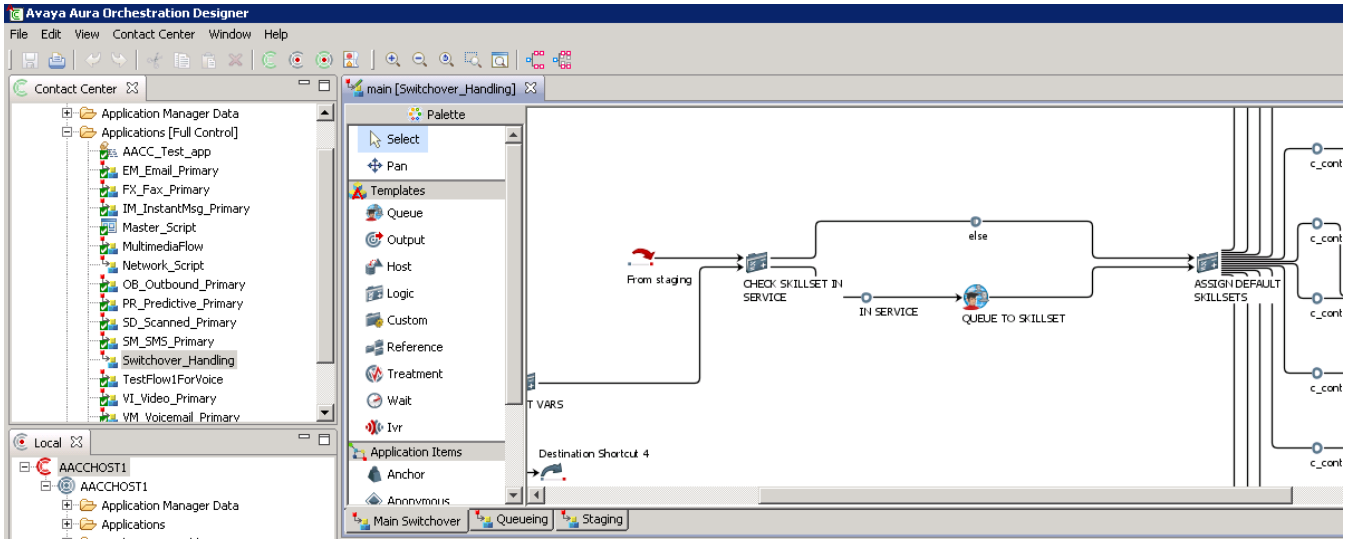
Procedure steps

Step	Action
1	In the **Address** box, type http://<Contact Center Manager Administration Server name>. For example, type http://AACCHOST1.
2	Press **Enter**.
3	Log on to the Contact Center Manager Administration browser as webadmin using the configured password.
4	On the **Launchpad**, click **Scripting**.
5	Click Orchestration Designer menu, and then click **Launch** Orchestration Designer.
6	Select the **Contact Center** view, if it is not already open in the current view.
7	In the **Contact Center** pane, expand **AACCHOST1**, **AACCHOST1**.

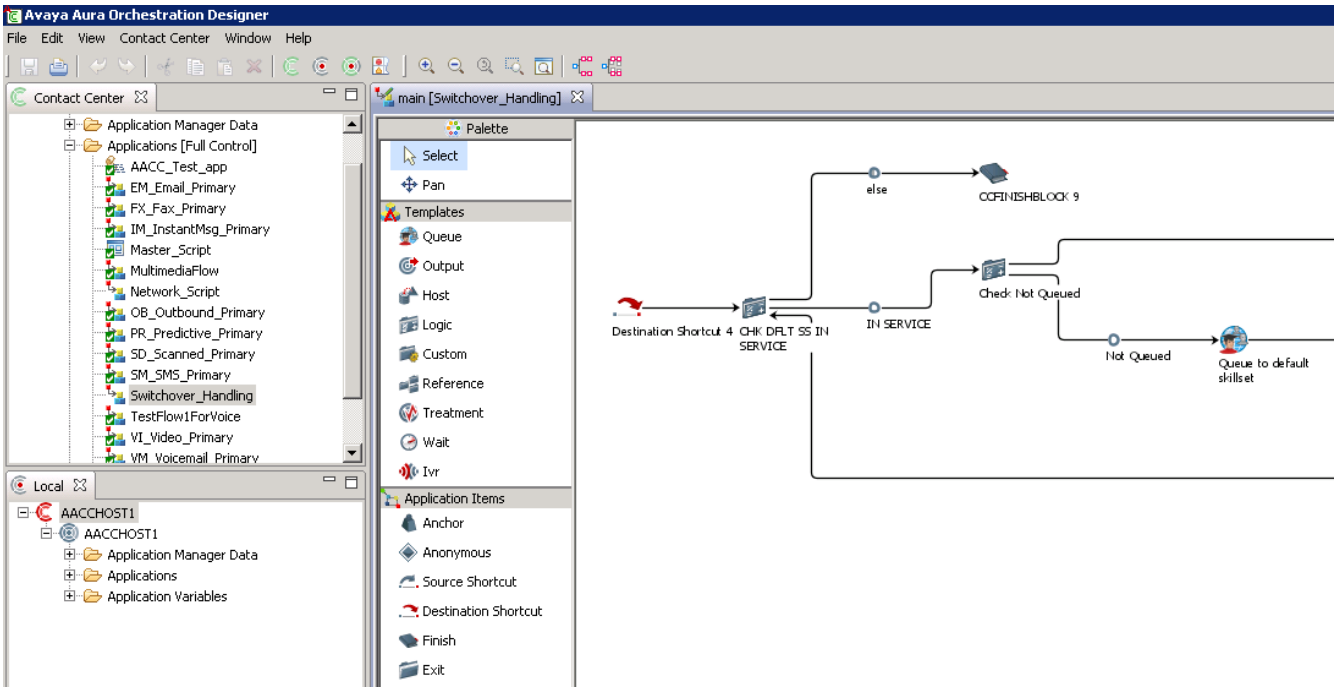


8 On the **Contact Server** pane, double-click the **Switchover_Handling** application.

The Switchover_Handling application opens in the Application view.

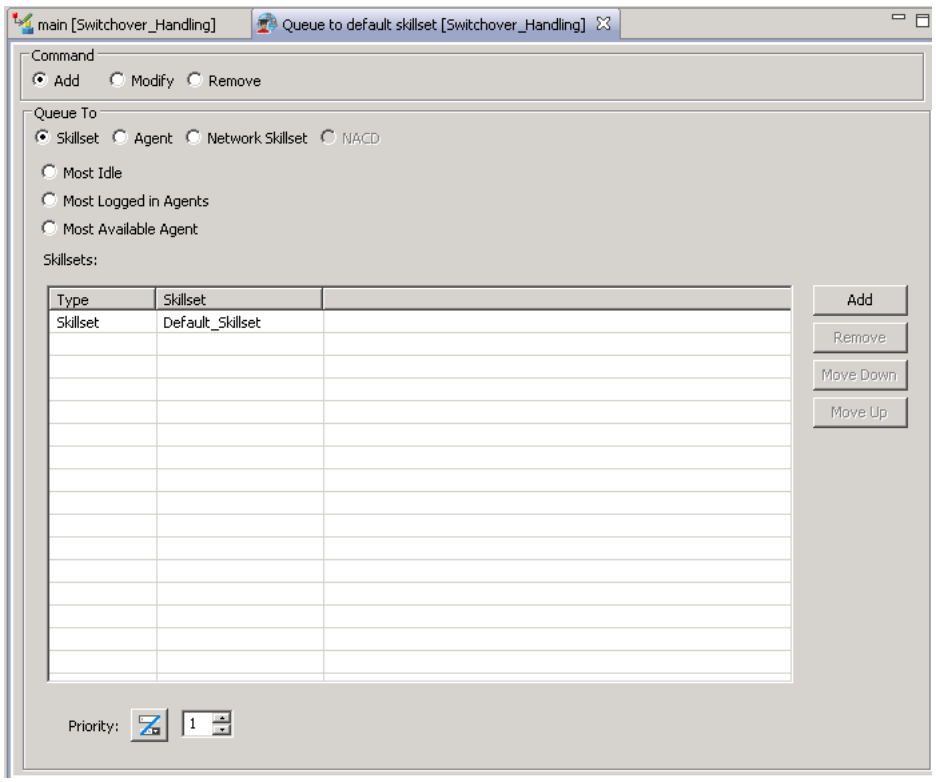


9 On the **Switchover_Handling** Application view, select the **Queueing** tab.



10 Double-click on the **Queue to default skillset** queue block.

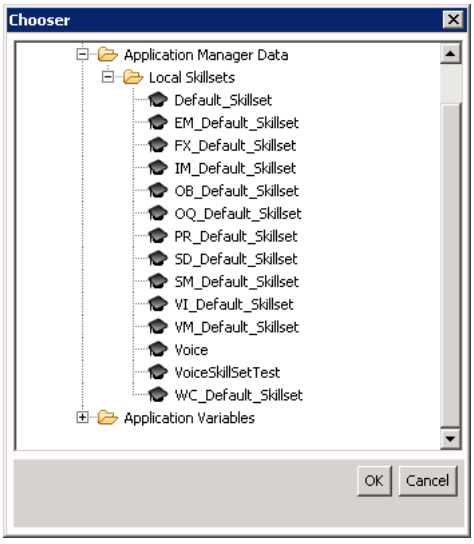
The Queue to default skillset queue block appears.



11 In the **Queue To** section, click **Add**.

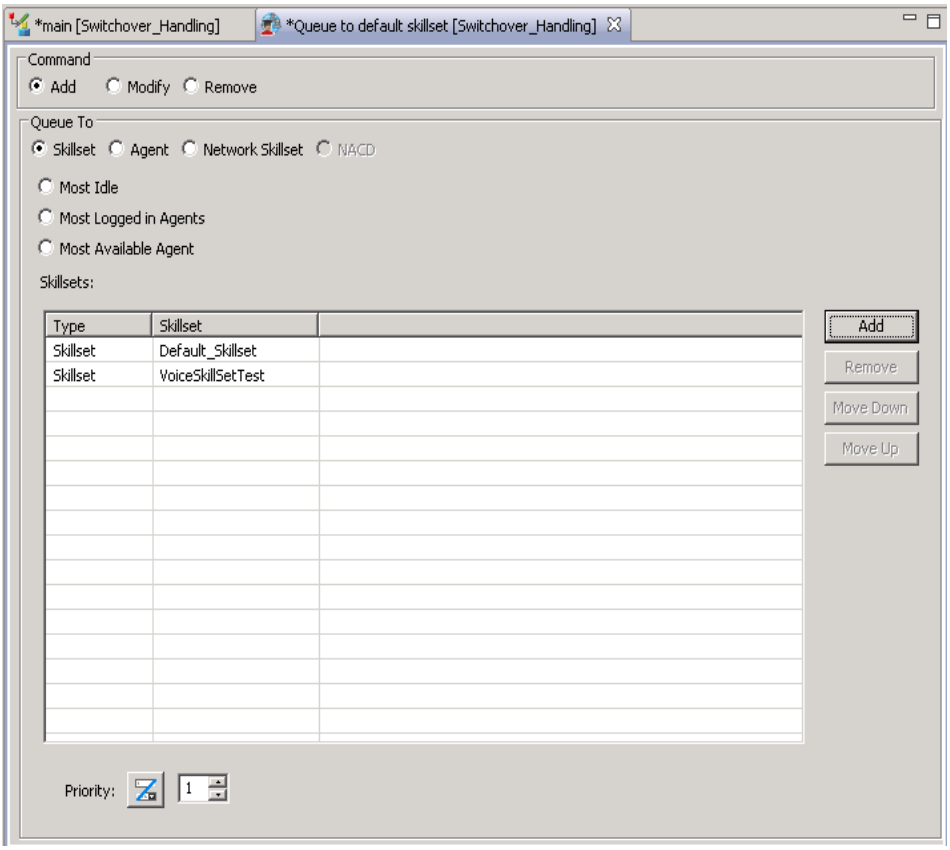
A Chooser dialog box appears.

12 On the **Chooser** dialog, navigate to the **Local Skillsets**, and select **VoiceSkillSetTest**.

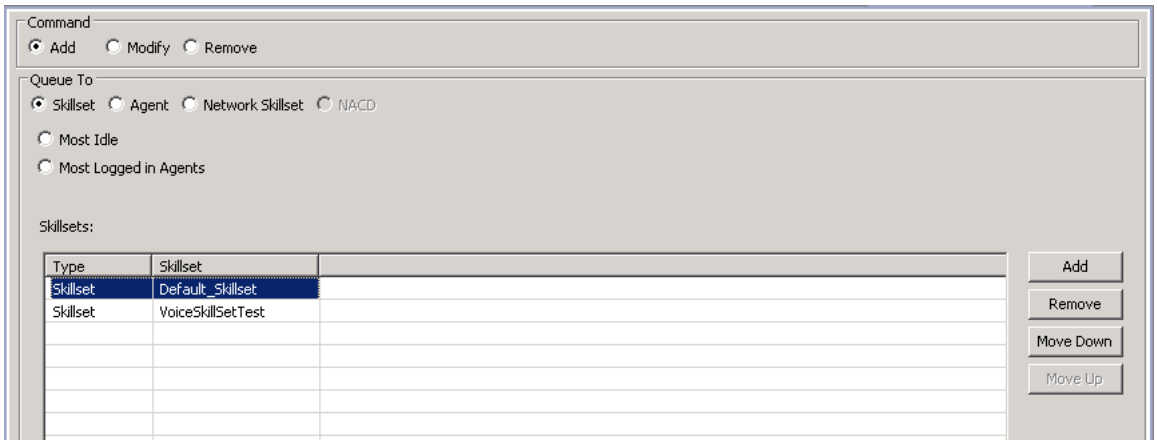


13 Click **OK**.

The VoiceSkillSetTest skillset is added to the Skillsets list.

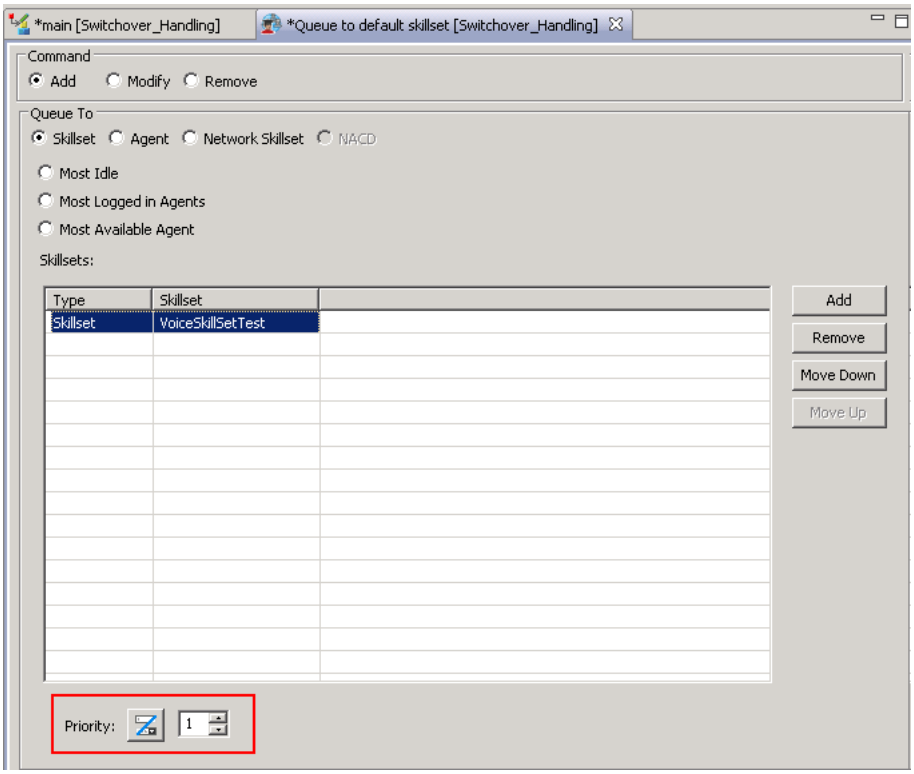


14 On the **Skillsets** list, select **Default_Skillset**.



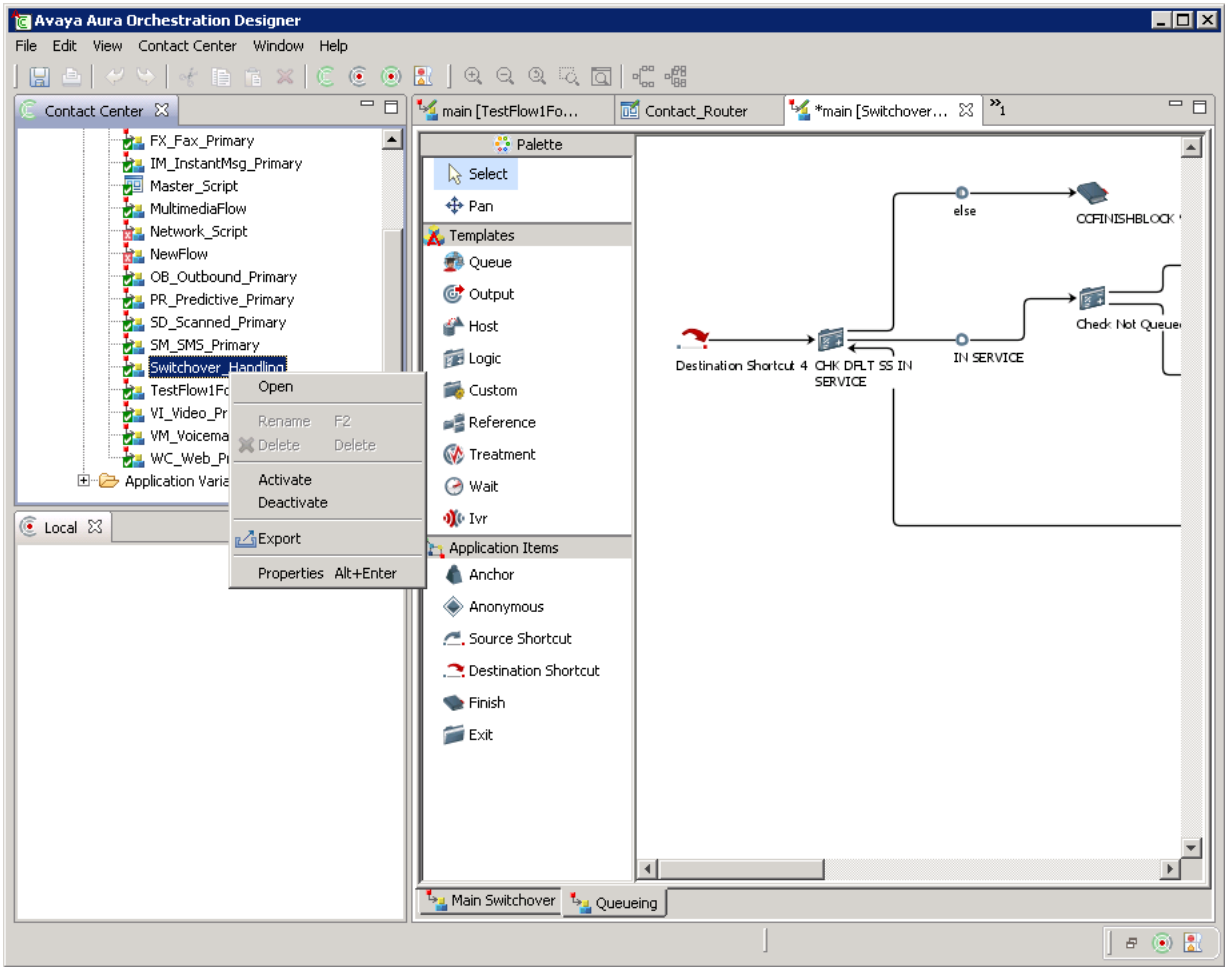
15 Click **Remove**.

16 Verify that the **Priority** for the **VoiceSkillSetTest** skillset is **1**.



17 Close the **Queue to default skillset** queue block

18 To activate the **Switchover_Handling** application, right-click on the flow in the list of application, and select **Activate**.



19 On the **Activate Application** message box, click **OK**.

--End--

Agent Desktop section

- Agent Desktop – Client software installation (page 317)
- Agent Desktop – Handling voice calls (page 325)
- Agent Desktop – Handling email messages (page 335)
- Agent Desktop – Multiplicity (page 341)

Agent Desktop – Client software installation

This chapter describes how to install the Agent Desktop client software on each client computer in your contact center. The Agent Desktop enables agents to handle contacts of all media types enabled in your contact center. The Agent Desktop is part of the Avaya Aura® Contact Center solution.

You install the Agent Desktop client application on the client computers from the server by accessing a Web location on the Contact Center Multimedia server.

You can change the name of an Agent Desktop computer, but because this is time consuming, Avaya recommends that you configure the computer final production name before installing Contact Center software.

Example computer details	Agent desktop computer
Name	XPClientDoc1
IP Address	172.18.71.118
Agent user account	AACC_Agent1
Domain	siptraffic.com

Prerequisites for Agent Desktop client software installation

- Install Contact Center Multimedia software.
- Install an Agent Desktop supported operating systems on the client computer.
- Install Internet Explorer Release 7.0, 8.0 or 9.0 on the client computer.
- Download and review the Avaya Aura® Contact Center Release Notes. The Release Notes contain the known issues, patches and workarounds specific to a release and patch line-up of Avaya Aura® Contact Center. For more information about the Avaya Aura® Contact Center Release Notes, see www.avaya.com/support.

Creating Domain users and groups for agents

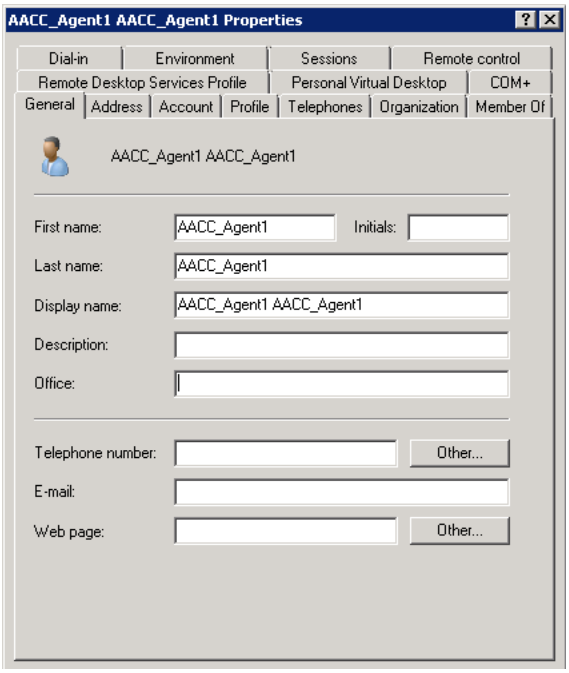
Agents need a domain account to log on to the a desktop computer and use Agent Desktop. Create a domain user account for each Contact Center agent. Add the agent desktop computers to the domain, then add the desktop computers to a Windows domain organizational unit (OU).

Attention: You must have domain administration rights to perform this procedure. If you do not have domain administration rights, ask your Domain Administrator to create or modify the user accounts, desktop accounts, and organizational unit required by Avaya Aura® Contact Center.

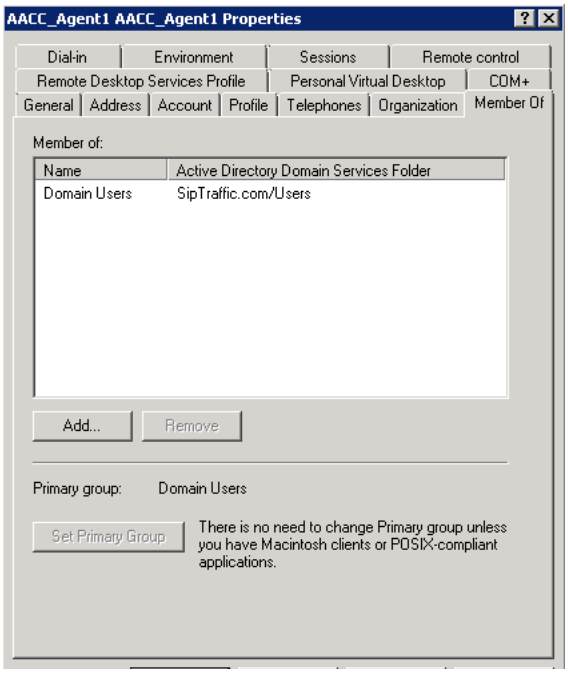
Attention: This is an administrative procedure. Therefore, ask the Domain Administrator to perform this task.

Procedure steps

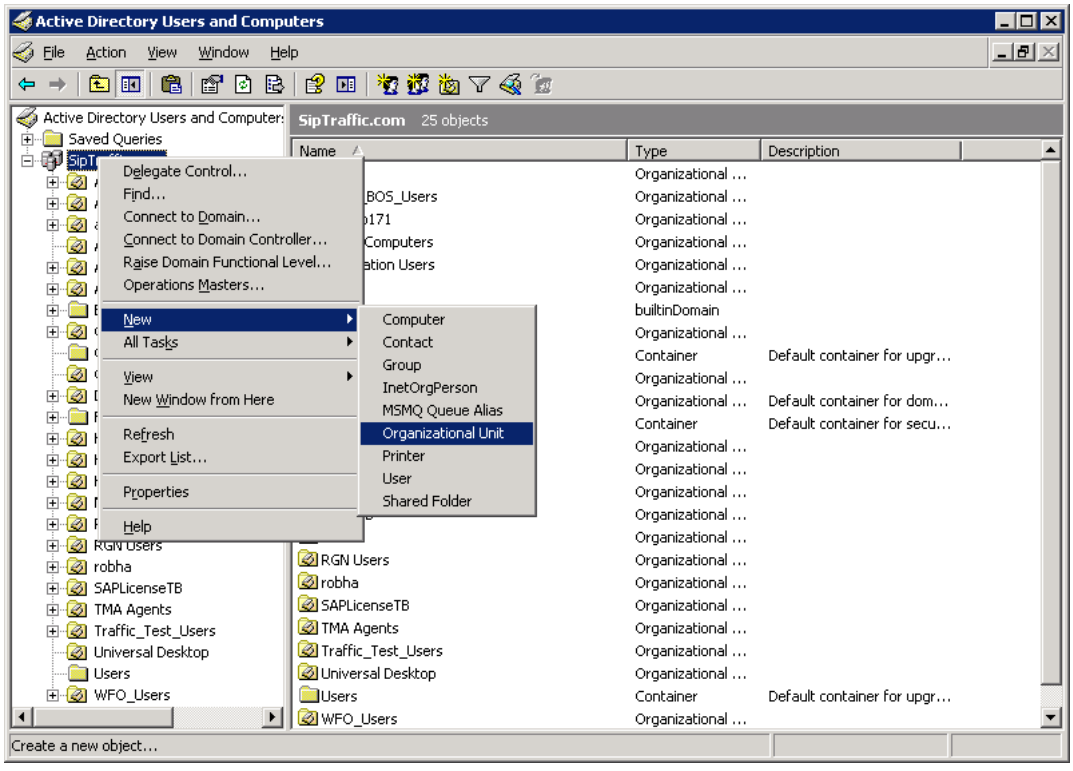
Step	Action
1	Create a domain account for each Contact Center agent.



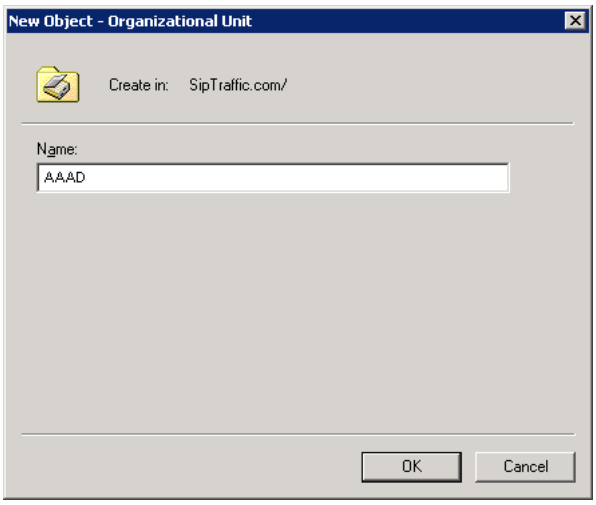
2	Add the agent desktop computers to a domain. For example, add the agent desktop computers to the **siptraffic.com** domain.



3 On the Domain Controller, create a Windows organization unit (OU) to contain all the desktop computers for the agents using Agent Desktop.



4 For example, in the siptraffic.com domain, create an organization unit (OU) called AAAD.



5 Add the all the agent desktop computers to this OU. For example, add all the agent desktop computers to the AAAD OU.

--End--

Assigning a group policy for embedded softphone settings

Assign the Group Policy administrative template with specific settings for Agent Desktop to your Windows domain controller. You need to copy the administrative template file from the Voice and Multimedia Contact Server to the Windows domain controller. You also need to add all the desktop computers for the agents using Agent Desktop to an organization unit (OU) on the contact center domain.

Prerequisites for assigning the group policy

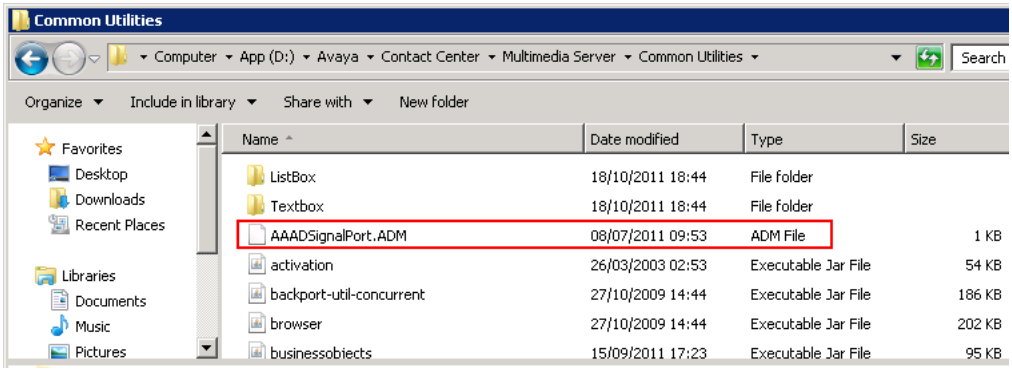
- You understand Windows group policy management.
- On the contact center domain, you have created a Windows OU that contains all the desktop computers for the agents using Agent Desktop.

Attention: This procedure describes the steps to follow on Windows 2008 Server. If you are using an earlier version of Windows for your domain controller, refer to the appropriate Windows documentation.

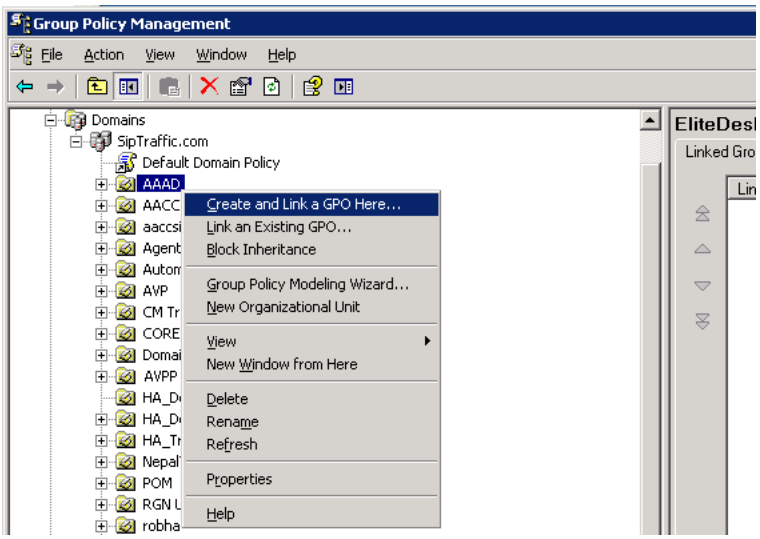
Attention: This procedure requires a reboot of all the desktop computers for the agents using Agent Desktop.

Procedure steps

Step	Action
1	On the Voice and Multimedia Contact Server, navigate to the `D:\Avaya\Contact Center\Multimedia Server\Common Utilities` folder and locate the AAADSignalPort.ADM file.



2	Copy the administrative template file to your Domain Controller.
3	On the Windows domain controller, choose **Start**, **Administrative Tools**, **Group Policy Management**.
4	Right-click the OU to which you want to link the Group Policy administrative template. This is the OU that contains the agents' desktop computers.



5	Select **Create and Link a GPO Here**. *Windows displays the **New GPO** dialog.*
6	In the **Name** box, type a name for the new GPO.
7	Click **OK**.

8 Right-click the GPO you created.

9 Select **Edit**.

*Windows displays the **Group Policy Object Editor** dialog.*

10 Expand **Computer Configuration**.

11 Under **Computer Configuration**, right-click **Administrative Templates**.

12 Select **Add/Remove Templates**.

*Windows displays the **Add/Remove Templates** dialog.*

13 Click **Add**.

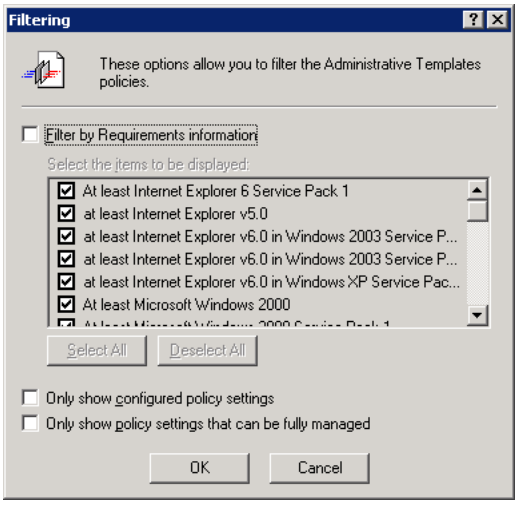
*Windows displays the **Policy Templates** dialog.*

14 Browse to the location where you copied the AAADSignalPort.ADM file, select this file, and click **OK**.

15 Click **Close**.

16 From the **View** menu, select **Filtering**.

17 Select **Only show policy settings that can be fully managed**.



18 Click **OK**.

19 Under **Administrative Templates** select the policy template you added.

20 In the right-hand pane, right-click the **SignalProtocol** setting.

Windows displays the SignalProtocol Properties dialog.

21 On the **Setting** tab, select **Enabled**.

22 Type "1" in the **Signal Protocol** box.

23 Click **OK**.

24 Exit the **Group Policy Object Editor**.

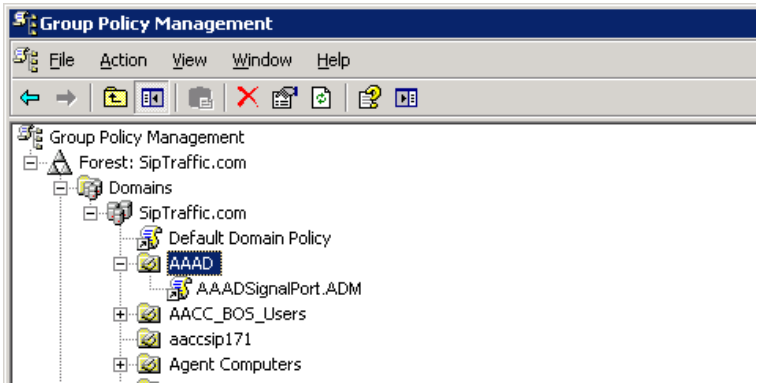
Step	Action
25	Ensure all agents restart their desktop computers before accessing the Agent Desktop application for the first time.

--End--

Procedure job aid

The following image shows the Administrative Templates applied to the AAAD organization unit (OU) on the contact center domain, siptraffic.com.

Agent Desktop Group Policy administrative template



Installing the Agent Desktop client software

Install the Agent Desktop client software on each client computer. Install the Agent Desktop client software from the Voice and Multimedia Contact Server.

Install one of the supported operating systems for Agent Desktop on the client computer. The supported operating systems are as follows:

- Windows XP with Service Pack 2 (SP2) or later
- Windows 7
- Windows Vista

Install Internet Explorer Release 7.0, 8.0 or 9.0.

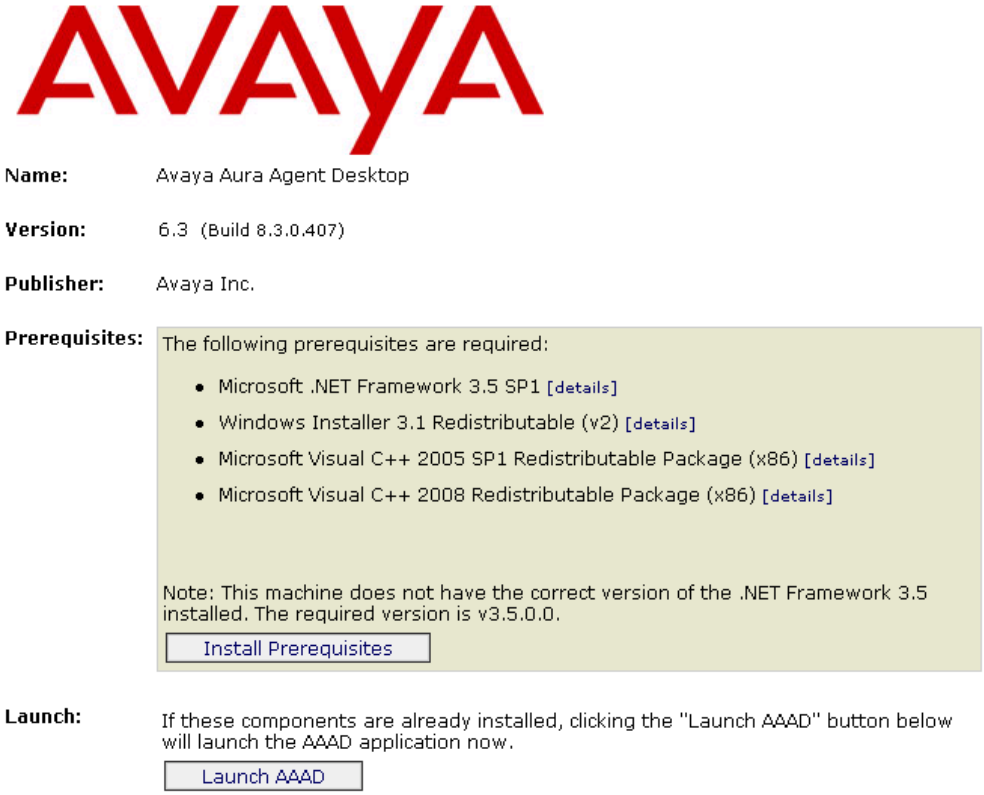
Procedure steps

Step	Action
1	On the client computer, start Internet Explorer.
2	On the Agent Desktop client computer, in Internet Explorer, type the URL in this format: < Voice and Multimedia Contact Server name>/agentdesktop. For example, type:

http://AACCHOST1/agentdesktop

3 On the **Agent Desktop** page, click **Install Prerequisites**.

The client downloads the .NET Framework and C++ software from the server and installs the application on the client. Follow the on-screen instructions to download and install the required software.



4 Click **Launch AAAD**.

5 On the **Application Install - Security Warning** message box, click **Install**.

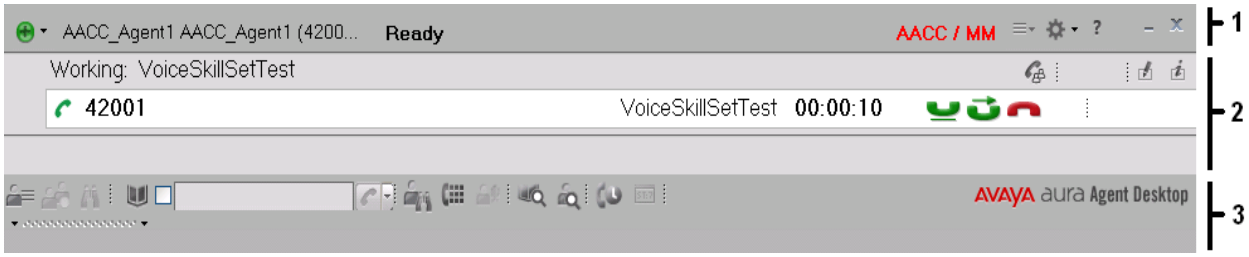
--End--

Agent Desktop – Handling voice calls

Avaya Aura® Agent Desktop is a single-interface client application used to interact with customers. You can respond to customer contacts through a variety of media, including phone, outbound contacts, email, Web communication, instant messaging, fax, scanned documents and SMS text messages. Agent Desktop provides automation for customer responses to eliminate repetitive actions, such as typing a common response in an email message.

This chapter describes the main user interface of the Agent Desktop application. There are three main sections to the Agent Desktop user interface:

Example of Agent Desktop layout



1	Top bar (page 325)
2	Work list window (page 326)
3	Action bar (page 328)

The Agent Desktop also provides other controls and menus that are explained in the following chapters.

Work item paradigm

The main Agent Desktop user interface is based on a work item paradigm. Each agent-to-customer interaction is a work item. Work items appear on the Agent Desktop work list. If you perform an interaction associated with that work item (for example, an IM consultation with an expert), then that interaction is displayed as part of the original work item.

The work list consists of work items and control buttons corresponding to the work item. The controls and functions change depending on the work list window behavior. When a new contact arrives, Agent Desktop adds the new contact as a work item to the work list.

Top bar

The Top bar appears at the top of the Agent Desktop window. The Top bar provides the system status and main controls to operate Agent Desktop.

Example of Top bar layout



The agent status icon appears on the top left corner of the Agent Desktop Top bar. It shows the agent status, agent name, agent login ID, and agent dialable number.

The Top bar has the following icons:

Top bar icons

Icon	Name	Description
	Mute / Unmute	Place the call on mute while using the computer (softphone) to place and receive calls. Use the same button to unmute.
	Audio Monitor	View the current audio levels used for your microphone and speakers.
	Terminal action	Access Emergency, Observe and Intrinsics controls.
	User preferences	Access user preferences and change audio settings for the softphone.
	Agent status	Select agent status.
	Help	Access help information.

Use the Terminal Action menu to perform the following tasks:

Terminal Action Menu

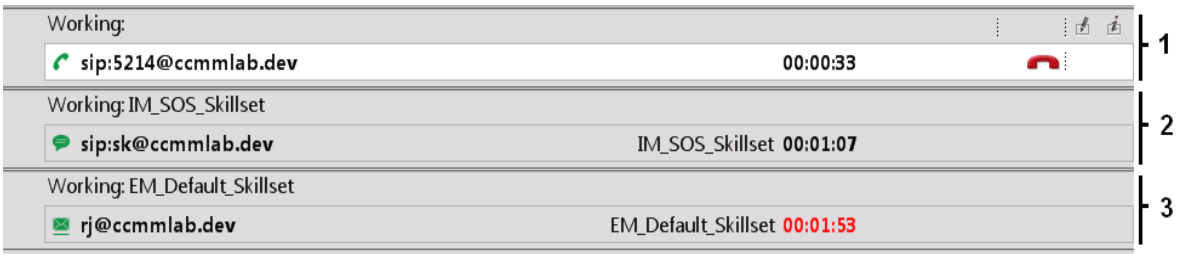
Command	Description
Observe	Used by supervisors or agent-supervisors to listen in on a contact.

Work list window

The work list window contains work items and control buttons corresponding to the work item. The controls and functions change depending on the information in the work list window. The top right corner of the work list window has work item controls. These controls are common to all work items on the work list. When a new contact arrives, Agent Desktop adds the new contact as a work item to the work list.

The following image displays the work list windows and controls.

Example of work list layout



The illustrated work list shows three work items:

1	A voice call work item, at the top of the work list.
2	An Instant Message (IM) work item, in the middle of the work list.
3	An email work item, at the bottom of the work list. The email work item is on hold.

- A work item is a collection of interactions with a customer, another agent, a supervisor, or an expert.
- A work list is a collection of work items. When you receive a new contact, it is added to the work list so that you can monitor your current contacts. When you finish with the contact, or reject the contact, the work item is removed from the list.

Work item controls

Each work item has a number of contact-related controls. These controls change depending on the work list window behavior and contact type.

Examples of work item controls

Voice	IM	E-mail	Name	Description
			Accept	Accept the work item.
			Release	Release or reject the work item.
			Hold	Place the work item on hold.
			Transfer	Transfer the work item contact.
			Conference	Conference the work item.
			Activity code	Set the work item activity code.
			Work item details	Read the work items details.

Only appropriate controls are displayed on work items. For example, voice-related controls are displayed on a voice work item. IM related controls are displayed on IM work item.

Action bar

The Action bar contains global controls to create a new work item, to search contacts, and to open secondary windows. The Action bar stays at the bottom of the Agent Desktop window and remains at the bottom as the window expands.

Example of Action bar layout



Use the Action bar at the bottom of the main interface to create new contacts. New voice, IM, or email contacts are collectively called new work items in the Work Item Paradigm.

Action bar commands

Icon	Name	Description
	Customer Details	View customer details.
	Contact Presence	Contact presence.
	Observe	Listen in or participate in agent-customer calls or chat sessions. (Used by Supervisors only)
	Phone book	Contact agents through the LDAP agent contact directory.
	Initiate Contact	Start a new work item.
	Call Supervisor	Call your supervisor.
	DTMF	Generate DTMF tones.
	Agent Greeting	Used to record an agent greeting.
	Contact Search	Search for contacts.
	Customer Search	Search for customers.
	Schedule Callback	Schedule a callback.
	Agent Statistics	Display agent statistics scroll bar.

Starting Agent Desktop

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

Procedure steps

Step	Action
1	Log on to an Agent Desktop client computer in the siptraffic.com domain using the siptraffic\AACC_Agent1 Windows (and Contact Center Agent) account.
2	On the Agent Desktop client computer, in Internet Explorer, type the URL in this format: <Voice and Multimedia Contact Server name>/agentdesktop. For example, type: http://AACCHOST1/agentdesktop
3	Click **Launch AAAD**.

--End--

Procedure job aid

The system automatically configures your status to Logged Out, when you launch Agent Desktop.

The Agent Desktop

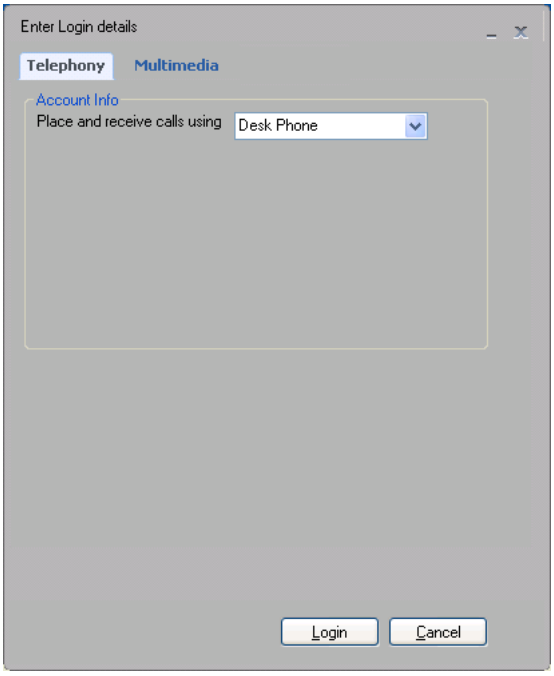


Logging on to Agent Desktop when using a desktop phone

Log on to Agent Desktop after you start the Agent Desktop application. While you log on, you can choose between a desktop phone and a softphone based on your usage mode. The system automatically configures your status to Not Ready. Change your status to Ready to indicate that you are available to handle all media types for which you are licensed and configured. If you are assigned to a skillset for a particular contact type, you can receive and create contacts in that contact type.

Procedure steps

Step	Action
1	Start Agent Desktop.
2	On the Agent Desktop Top bar, from the **Status** list, select **Login**.
3	Click the **Telephony** tab.



4 Select **Desk Phone** from the **Place and receive calls using** drop-down list.

5 On the **Multimedia** tab, type your **ID** and **Password**. For example type 42000 as the ID and 42000 as the password.

6 Click **Login**.

The system verifies your password and logs you on to the Agent Desktop application and into Avaya Aura® Contact Center. The Logged out icon changes to Logged In. The status icon changes to Not Ready.

--End--

Variable definitions

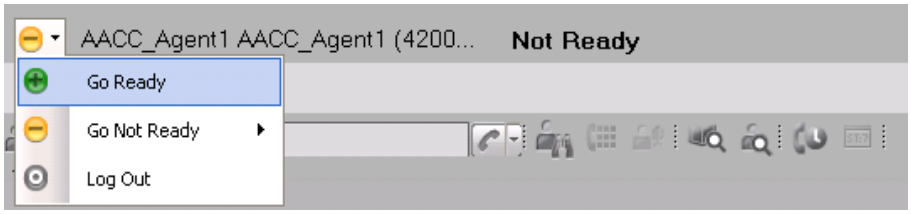
Description	Value
ID (Multimedia)	Your log on ID appears in the ID box, based on your Communication Control Toolkit configuration.
Password (Multimedia)	Initially, for multimedia agents, your password is the same as your Agent Logon ID. The system verifies your password and logs you on to the Agent Desktop application and into Avaya Aura® Contact Center. The Logged out icon changes to Logged In.

Changing your status to Ready

Change your status to Ready when you are available to create or receive contacts.

Procedure steps

Step	Action
1	On the Agent Desktop Top bar menu, click the Status icon.
2	Select **Go Ready**.



Agent Desktop places you in Ready status. The status icon changes to green and the Top bar displays the Ready status.

--End--

Accepting a test call

Accept and work with telephone calls. The relevant work item controls become active and the call timer appears in the work item.

Prerequisites

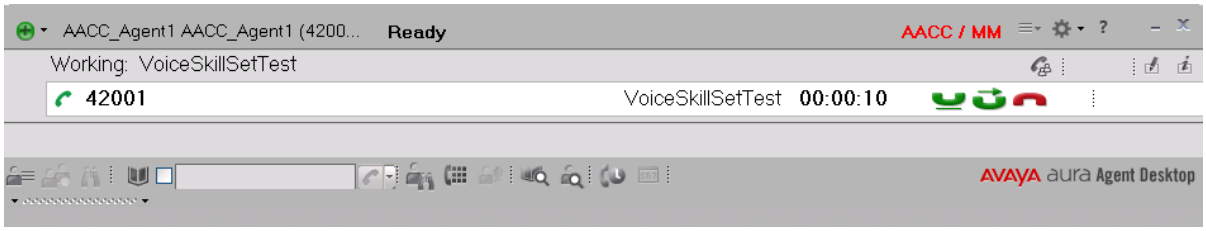
- Ensure that you are in Ready state.
- Ensure that you have a skillset designated to handle telephone calls.

Procedure steps

Step	Action
1	Generate a test call to the contact center. For example, from another phone on the same Communication Manager, dial the contact center route point of 52000.
2	On the Agent Desktop, select the new alerting work item and click the Accept work item control. *The top pane of the Agent Desktop shows the customer details and history of all past calls with the contact.*

--End--

Procedure job aid



Ending the test call

End a call when a call is completed. If you were in the Ready status before the call, you automatically return to the Ready when you terminate the call. If you require time to perform call wrap-up tasks before you accept another call, change your status to Not Ready and enter a Not Ready Reason Code in the Code field of the Top bar. Not Ready Reason codes are defined by the Administrator.

Procedure steps

Step	Action
1	On the work item, click **Release**.

--End--

Logging off from Agent Desktop

Log off from Agent Desktop when you are ready to exit the application.

A warning message appears asking you to confirm that you want to close the Agent Desktop and log off.

Prerequisites

Ensure that you do not have any contact open. If a contact is open, you must close the contacts before you log off of the application.

Procedure steps

Step	Action
1	On the Agent Desktop Top bar menu, click the Status icon.
2	Click **Log Out**.

Agent Desktop logs you off. The status icon changes to red and the Top bar displays the Logged Out status.

--End--

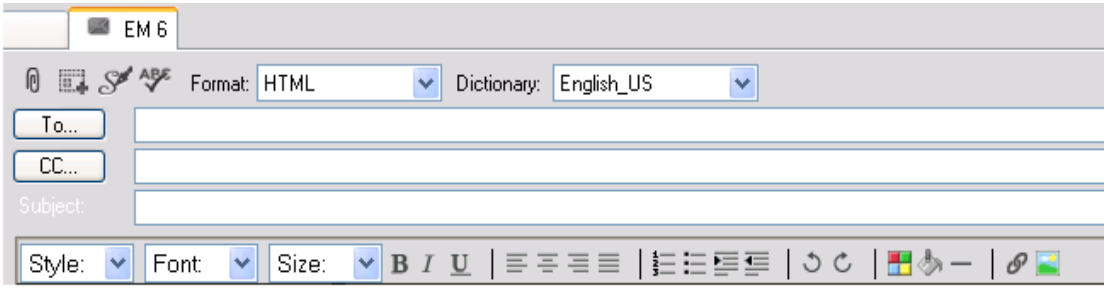
Agent Desktop – Handling email messages

This chapter describes how to perform email tasks using Avaya Aura® Agent Desktop:

- Accept the incoming email contact.
- Send a reply.

You can also use Agent Desktop to create a new email message.

Example of email toolbar



The Agent Desktop email editor offers improved email editing, formatting feature buttons, and management in HTML-format email messages. The feature buttons are added to the bottom of the email toolbar.

- Undo (Ctrl+z)
- Text font
- Text style
- Color text
- Bold text
- Italic text
- Text indent
- Underlined text
- Highlighted text
- Horizontal line-rule support
- Insert image links
- Insert hyperlink
- Text justification
- Numbered lists

- Bulleted lists

These formatting and additional insertion buttons are only displayed on the email editor toolbar when HTML format email is selected. Plain text format email messages do not support text formatting.

The following table shows the email feature buttons.

E-mail editing and formatting controls

Control	Function
	Bold selected text
	Italicize selected text
	Underline selected text
	Align text with left margin
	Center text
	Align text with right margin
	Numbered list items
	Bulleted list items
	Indent selected text
	Outdent selected text
	Undo last change
	Redo the last change
	Change color of selected text
	Insert a hyperlink
	Insert a graphic
	E-mail attachment
	Spell check

Accepting an incoming contact

Accept an incoming contact to display customer details and begin contact with a customer. Agent Desktop expands to show the customer details and a call timer appears in the work item. The new incoming email is presented as a new work item in the work list window.

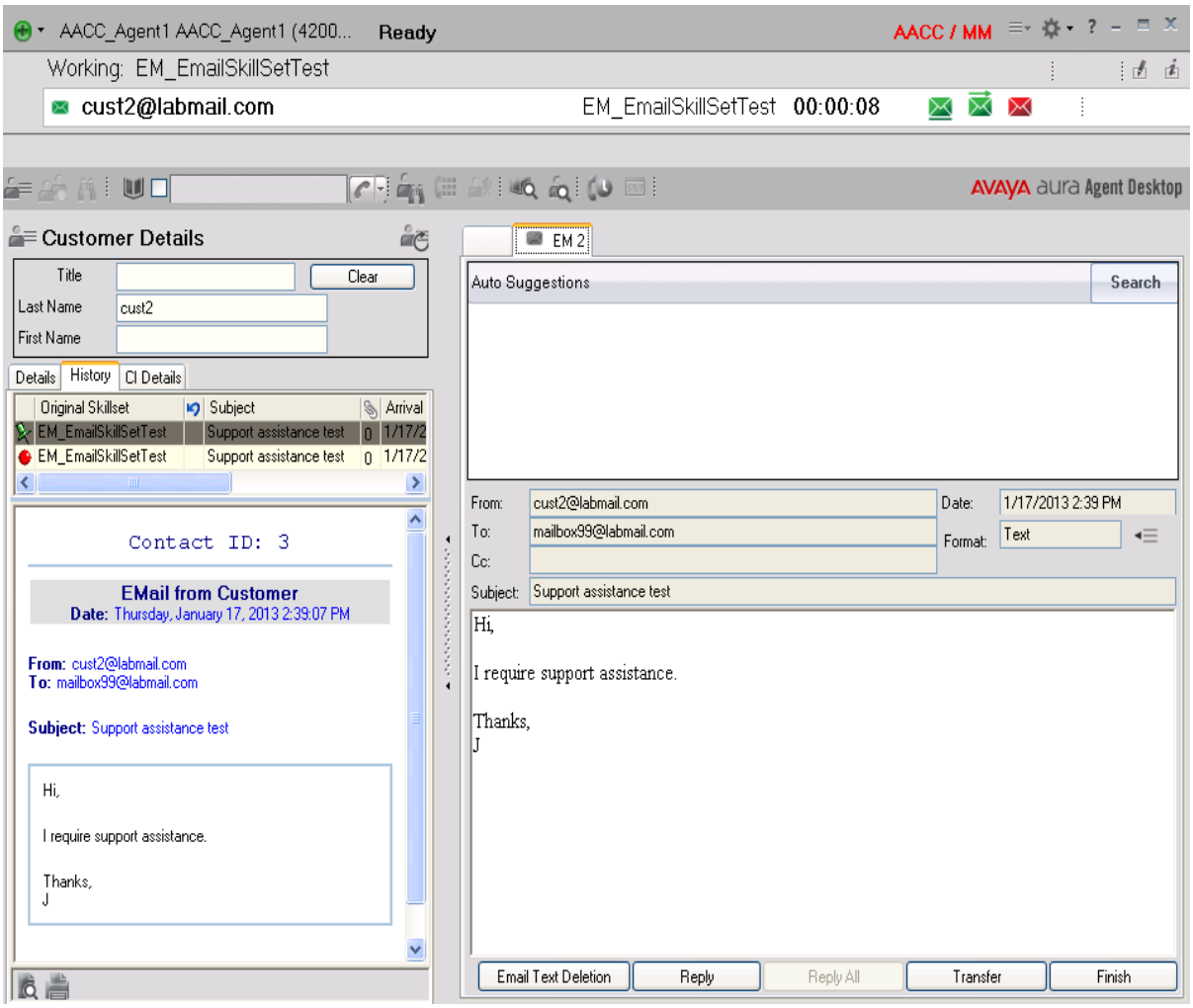
Procedure steps

Step	Action
1	Generate a test email. For example, create an email requesting support or assistance and send this email to mailbox99@labmail.com. The email must contain the keyword Assistance or Support. *The test email is presented to the logged on agent.*
2	On the Agent Desktop, click **Accept**. *The email opens in the E-mail Display panel.* *The customer details for the email opens in the bottom left hand Customer Details panel.*

--End--

Procedure job aid

Example of using Avaya Aura® Agent Desktop to accept an email message from a Customer.



Replying to an email message

Reply to an email message when a customer sends an email to the Contact Center requesting a response. Create a response to a customer in the same format as the original request.

You can use several features in the Agent Desktop interface to create your email response in HTML or plain text:

- Auto suggestions
- the address book

- one or more response templates
- an automatic signature
- an attached file
- the spelling checker

You can also add a comment to an email message in the Agent Note box for reference for later communications with the customer. The customer does not see the content of the Agent Note box.

Procedure steps

Step	Action
1	After you review the customer contact, click **Reply**.
2	In the E-mail Response window, accept the default To email address, with the same email address from which the message was sent.
3	In the **Subject** box, accept the subject currently displayed or edit the subject.
4	Add text to the reply using one or both of the following methods: • Type the message text. • Add a template response.
5	If you use HTML text and you want to bold, underline, or italicize any text, select the text and click the appropriate button to apply formatting. You cannot format plain text.
6	To change the text size, select the text and click the up arrow to increase the font size, or click the down arrow to decrease the font size.
7	To perform a spell check, click the Check Spelling icon.
8	To add an attachment to the email response, click Insert a file.
9	In the **Agent Note** box, type additional information about the contact or the customer. Only agents and supervisors can view the information in the **Agent Note** box.
10	Click **Send**.
11	Close the contact. If required, select a reason for closing the contact.

--End--

Closing the email contact

Close the email contact when the contact is complete. When you close a contact, select a Closed Reason code. The Closed Reason codes that appear are applicable to the contact type being closed.

Procedure steps

Step	Action
1	Click **Close** to complete the contact.
2	Select one of the configured **Closed Reason** codes that best describes the reason you closed your email message.

--End--

Agent Desktop – Multiplicity

Avaya Aura® Contact Center and Avaya Aura® Agent Desktop support multiplicity. Multiplicity allows an agent to handle multiple concurrent contacts. At any one time an agent can be active on a voice and multimedia contact; only one of these can be active, the others automatically are on hold.

Agents use the Avaya Aura® Agent Desktop application to process email, Web communications, instant message, outbound, SMS text, scanned document, faxed document, voice mail, depending on the applications your Contact Center is licensed to handle. For voice contacts, the agent can handle the incoming contacts, such as accepting the incoming contact, transferring the contact to another agent, and performing required duties to complete a contact.

For multimedia contacts, the agent can handle the incoming and outgoing contacts including accepting the incoming contact, dealing with the contact, such as talking to the customer, or sending them information in a text format, and performing other duties required to complete the contact.

Using the Multiplicity feature, an agent can work on any of the following contacts simultaneously:

- Voice call
- Email
- Fax
- Instant Message
- OpenQ, contact center multimedia generic contact
- Scanned Document
- SMS
- Web Communications

Multiplicity is configured and assigned to agents using Multiplicity Presentation Class (MPC) in Contact Center Manager Administration (CCMA). A MPC is a collection of multiplicity configuration options. Every agent must be assigned an MPC. A default MPC is not modifiable and allows an agent handle a single contact.

Multiplicity Presentation Class (MPC) configuration options include the following:

- maximum number of concurrent contacts the agent can handle
- time to wait before presenting the next contact to the agent

- check box to allow presentation of a voice call while working on multimedia contacts
- check box to allow presentation of multimedia contact while active on a voice call
- maximum number of contacts that can be presented for each contact type
- maximum number of contacts that can be presented for individual skillsets

The maximum number of concurrent contacts that an agent can be assigned is five. The consumption of agent licenses in not affected by multiplicity. An agent continues to consume agent licenses at log on for each contact type assigned to the agent.

Multiplicity is a licensed feature.

Accepting a route point call

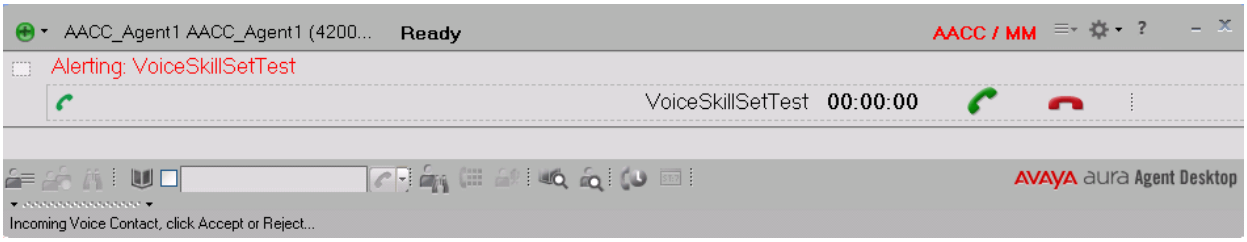
Accept and work with calls. The relevant work item controls become active and the call timer appears in the work item.

Prerequisites

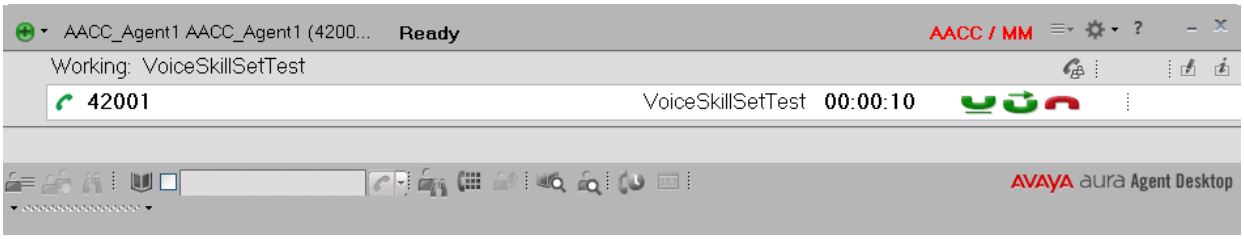
- Log on and ensure that you are in Ready state.
- Ensure that you have a skillset designated to handle telephone calls.
- Generate a test call to the contact center. For example, generate a call to the 52000 route point.

Procedure steps

Step	Action
1	On the Agent Desktop, the new call appears as a flashing Work Item.



2	Select the new alerting work item and click the **Accept** work item control.



--End--

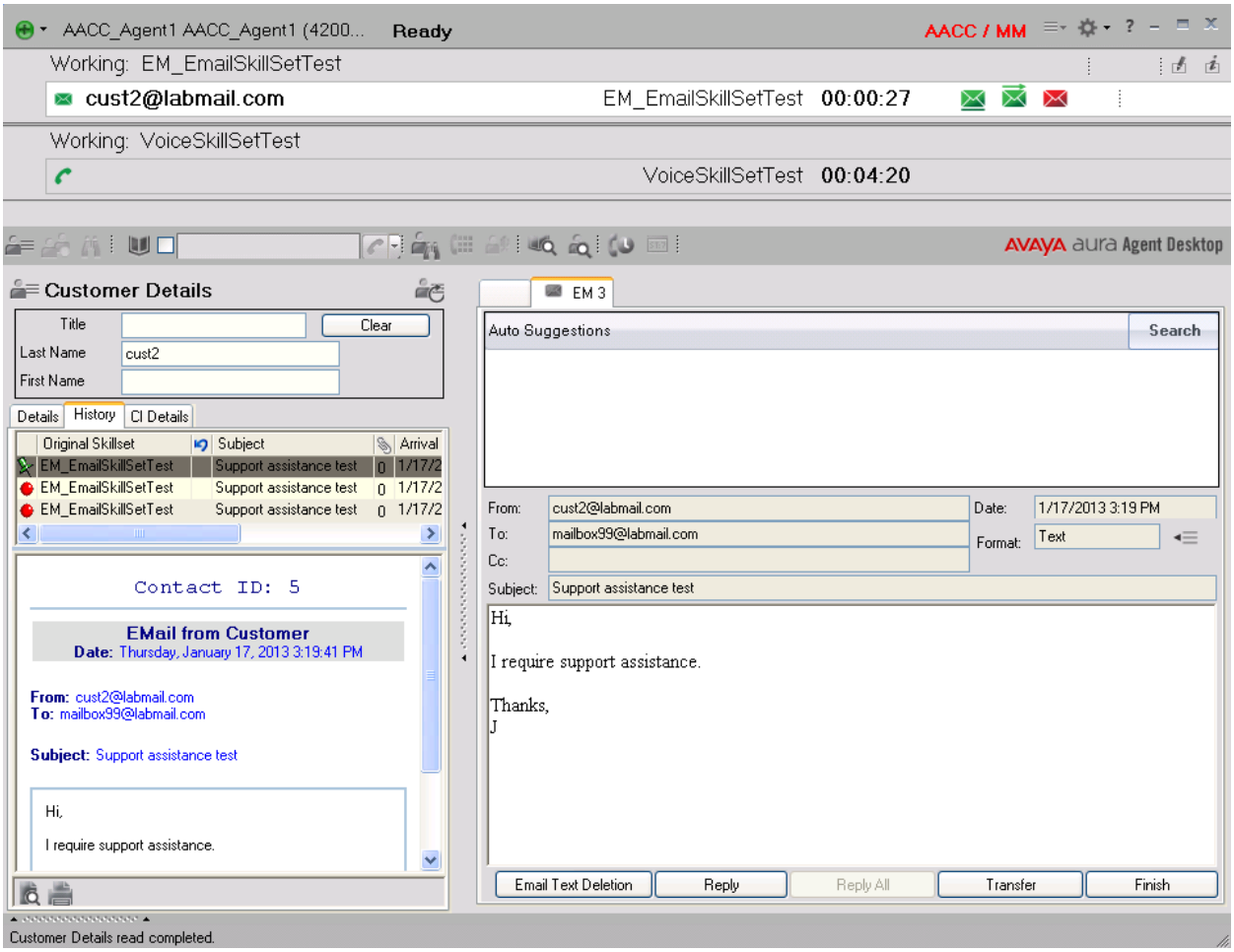
Accepting an incoming email contact while handling a voice contact

While handling a voice contact, accept an incoming contact to display customer details and begin contact with a customer.

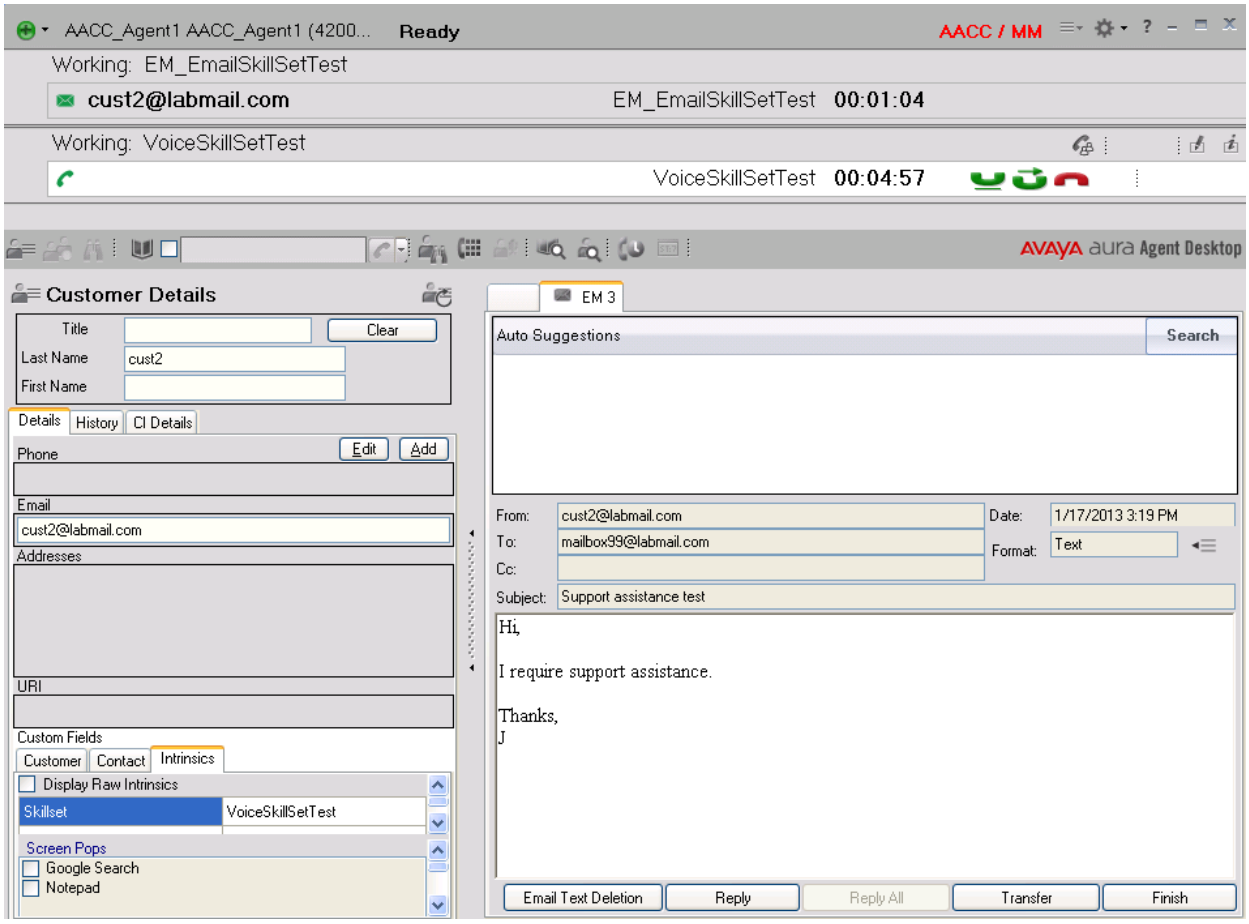
Agent Desktop expands to show the customer details and a call timer appears in the work item. The new incoming email is presented as a new work item in the work list window.

Procedure steps

Step	Action
1	Generate a test email. For example, create an email requesting support or assistance and send this email to mailbox99@labmail.com. The email must contain the keyword Assistance or Support. *The test email is presented to the logged on agent.*
2	On the Agent Desktop, click **Accept**. *The email opens in the Email Display panel.* *The customer details for the email appear in the bottom left-hand Customer Details panel.*



3 After accepting the email contact, you can return to the voice contact by selecting the voice contact from the Agent Desktop Work Item list.



--End--

Closing a customer contact

Close the email or voice contact when the contact is complete. When you close a contact, select a Closed Reason code. The Closed Reason codes that appear are applicable to the contact type being closed.

Procedure steps

Step	Action
1	Select the voice or email content from the Work Item list.
2	Click **Close** to complete the contact.

--End--

Avaya Media Server section

- Avaya Media Server – Removing Avaya Media Server software (page 349)
- Avaya Media Server – Primary server software installation (page 357)
- Avaya Media Server – Backup server software installation (page 377)
- Avaya Media Server – High Availability commissioning (page 397)
- Avaya Media Server – Commissioning (page 413)

Avaya Media Server – Removing Avaya Media Server software

This chapter describes how to uninstall Avaya Media Server software (Windows version) from the Voice and Multimedia Contact Server. The procedures in this section must be performed during a scheduled maintenance window.

Backing up the Locale Specific Media Files on Windows

Back up the Avaya Media Server locale-specific media files so you can restore them to the new Linux server. Locale-specific media files are used by your contact center Orchestration Designer (OD) flow applications.

Attention: If you use more than one language in your Contact Center prompts and media files, you must back up each language separately. For example, Play Prompt IVR blocks allow you to choose the locale from which OD plays prompts to callers. In a Canadian contact center, the flow applications can play either Canadian English or Canadian French prompts depending on the caller's preference.

Procedure steps

Step	Action
1	Log on to the Voice and Multimedia Contact Server with Avaya Media Server.
2	Navigate to the default location for the default locale-specific media files for your system. For example, navigate to D:\Avaya\MAS\Multimedia_Applications\MAS\platdata\Announcements\contactcenter\default\us\en\l16.
3	Create a .ZIP file of the contents of the folder, and save it to a network location from which you can download it to the Linux server.
4	Repeat these steps for each locale and language from which your contact center uses media files.

--End--

Backing up the batch zip file

You can upload a batch file to provision multiple media files on the Avaya Media Server in a single step. Back up the Avaya Media Server batch zip file you created at Uploading a batch zip file (page 196). You can then restore it to the new Linux server.

Procedure steps

Step	Action
1	Ensure that the media batch file is stored in an accessible and secure location.

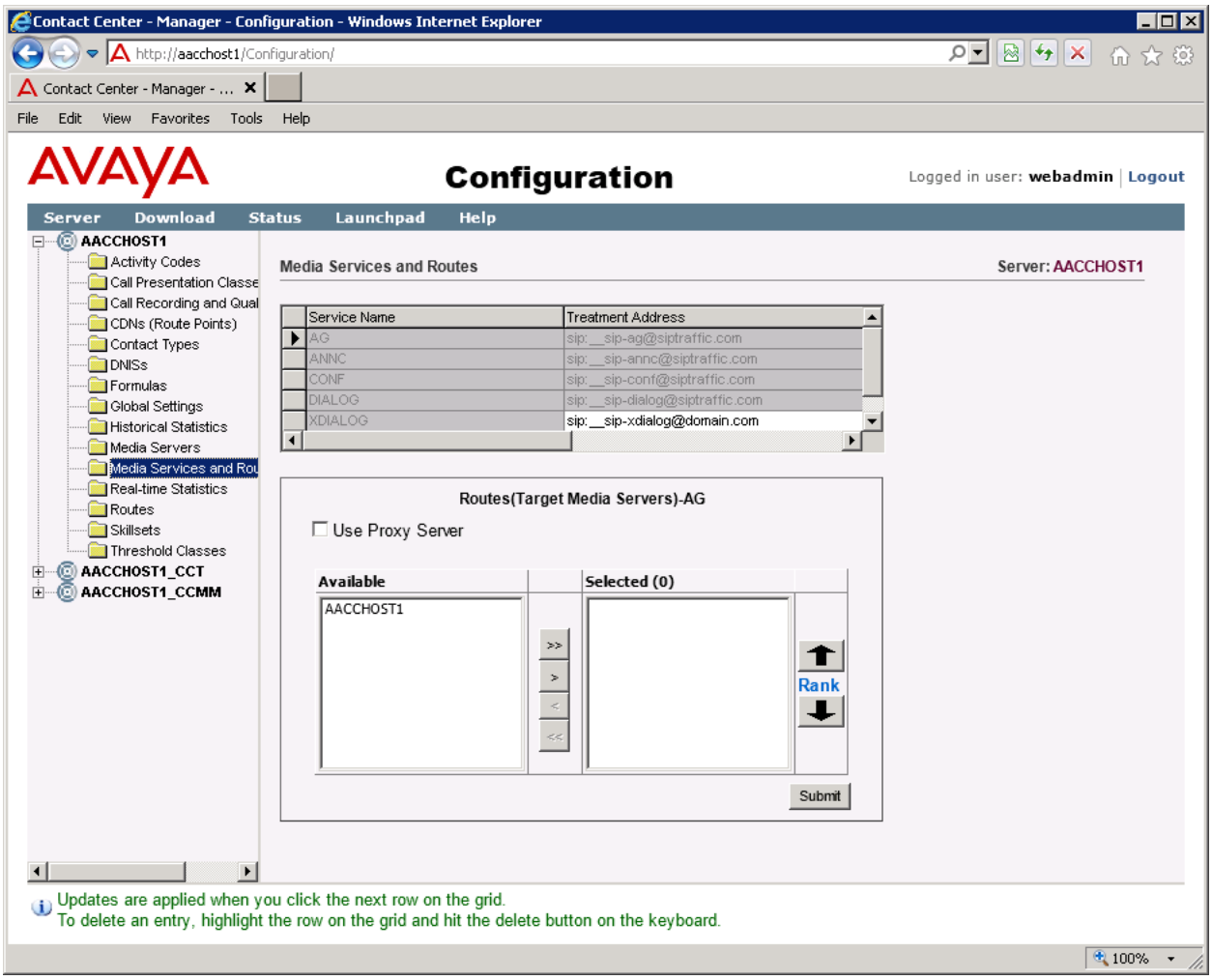
--End--

Removing Avaya Media Server from CCMA

Remove Avaya Media Server from CCMA so that Contact Center stops using the old Avaya Media Server (Windows version) resources.

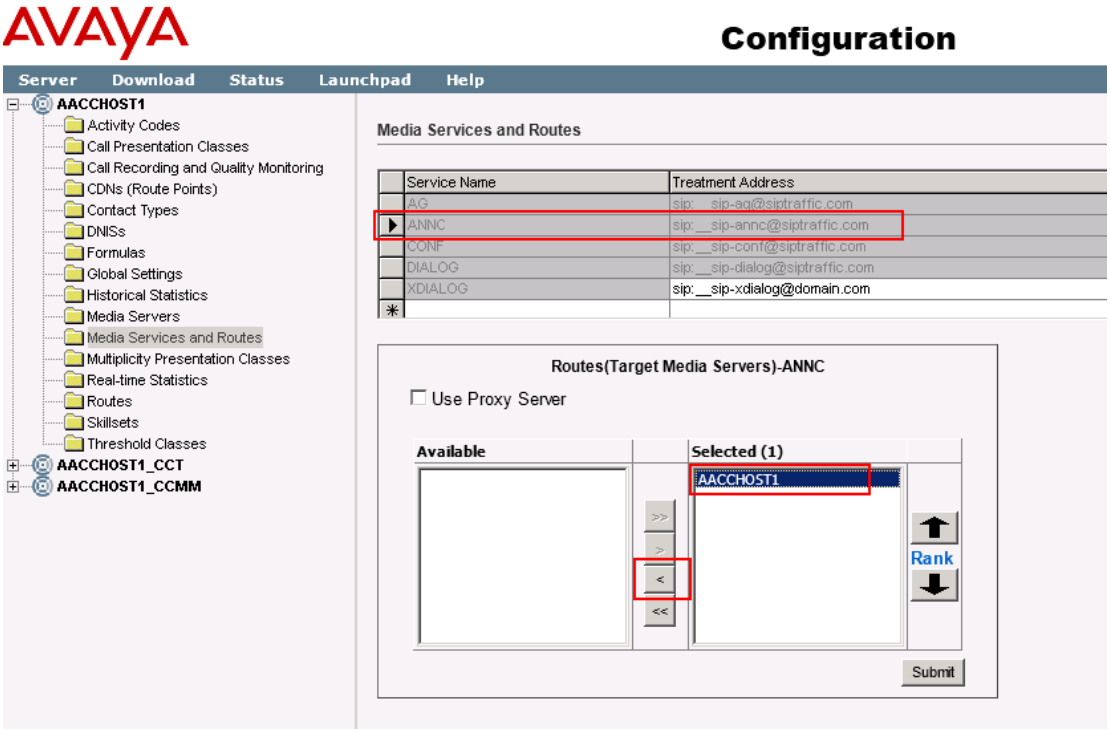
Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration.
2	From the Launchpad, click **Configuration**.
3	In the left pane, expand the CCMS server that uses the existing Avaya Media Server. *The server expands to show its resources.*
4	Select the **Media Services and Routes** folder.



5 From the **Service Name** list, select **ANNC**.

6 In the **Routes (Target Media Servers)** section, from the **Selected** list, select the Avaya Media Server server name. For example, select AACCHOST1.



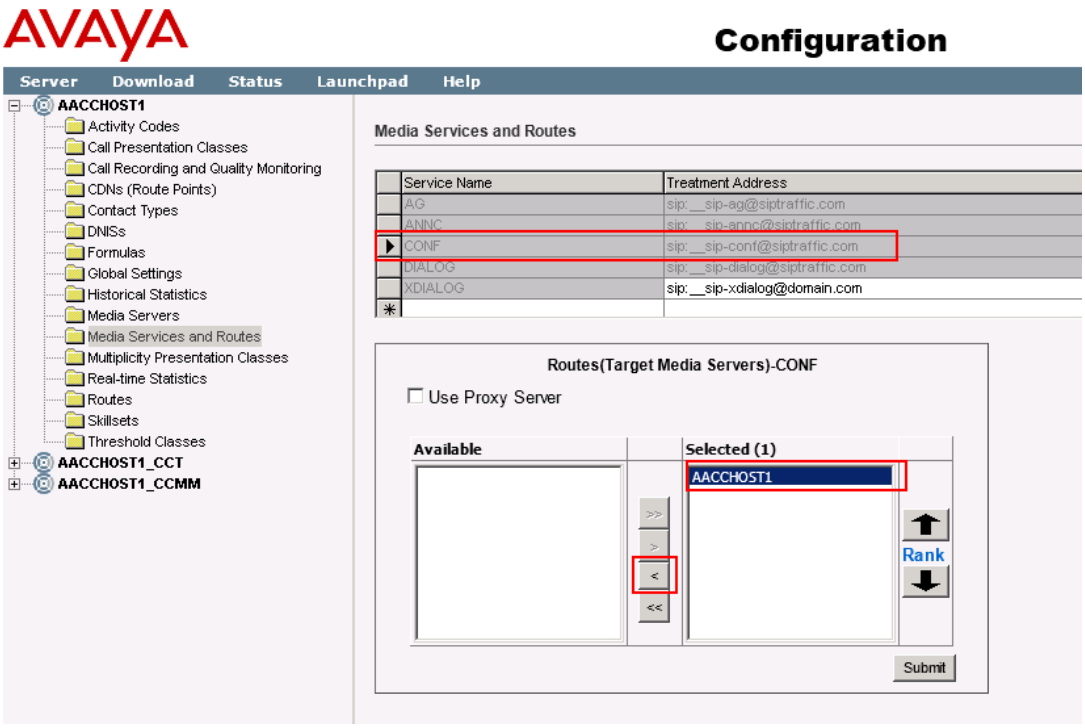
7 Click the **<** arrow key.

AACCHOST1 is removed from the list of Selected Announcement media servers.

8 Click **Submit**.

9 From the **Service Name** list, select **CONF**.

10 In the **Routes (Target Media Servers)** section, from the **Selected** list, select the Avaya Media Server server name. For example, select AACCHOST1.



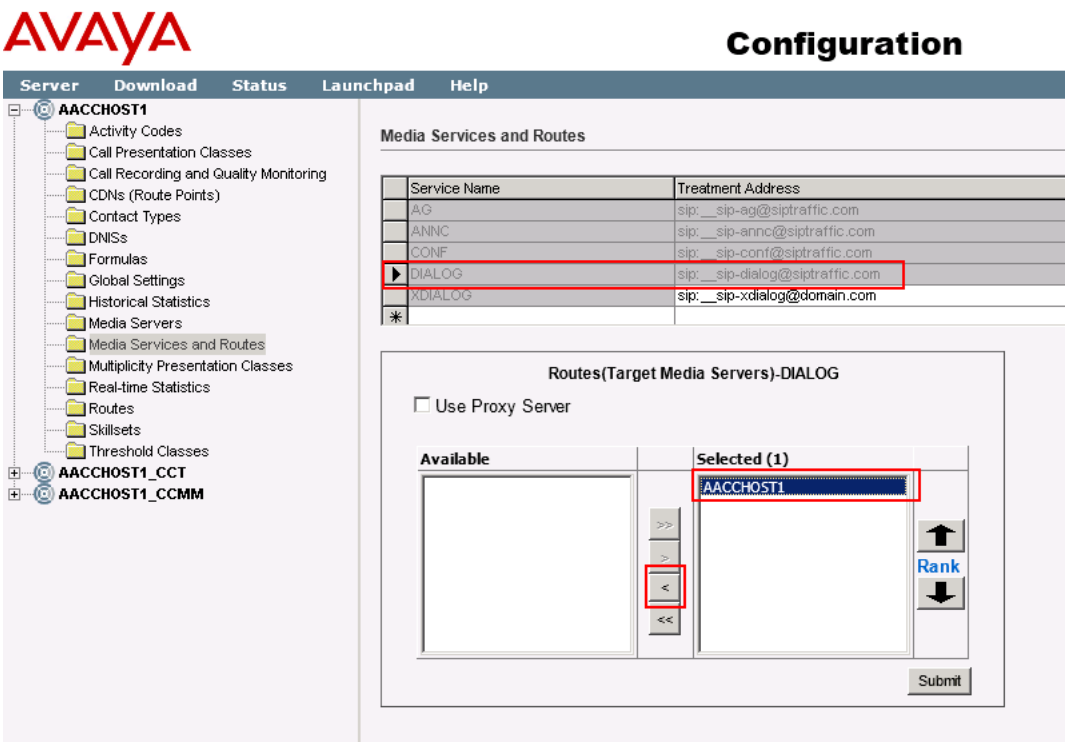
11 Click the **<** arrow key.

AACCHOST1 is removed from the list of Selected Conference media servers.

12 Click **Submit**.

13 From the **Service Name** list, select **DIALOG**.

14 In the **Routes (Target Media Servers)** section, from the **Selected** list, select the Avaya Media Server server name. For example, select AACCHOST1.

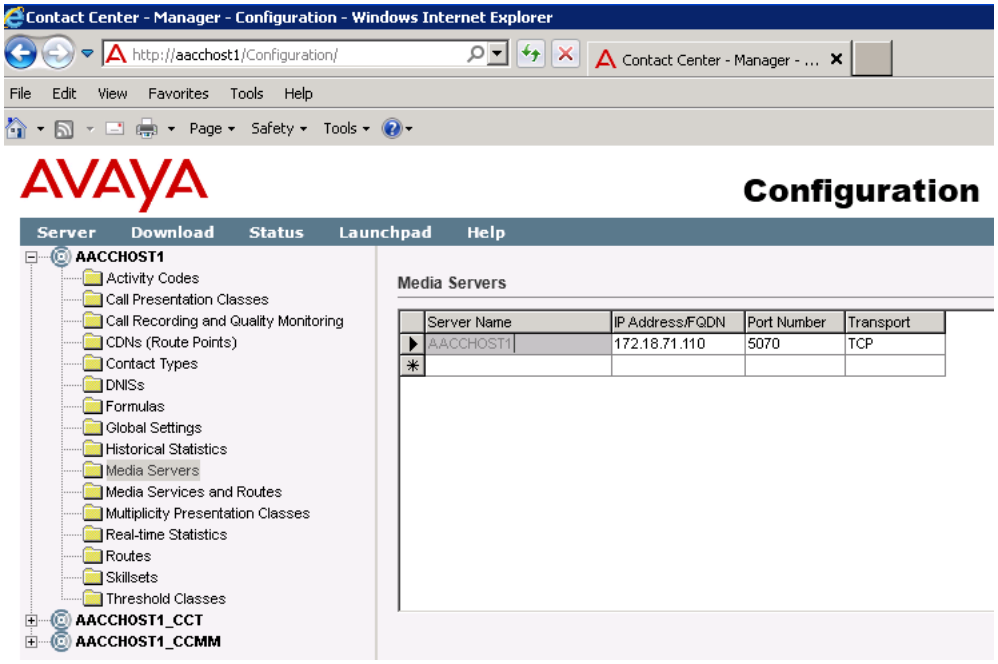


15 Click the **<** arrow key.

AACCHOST1 is removed from the list of Selected Dialog media servers.

16 Click **Submit**.

17 Select the **Media Servers** folder.



18 In the right pane, select the Avaya Media Server (Windows version), and press **Delete**.

19 On the confirmation dialog box, click **Yes**.

--End--

Uninstalling Avaya Media Server

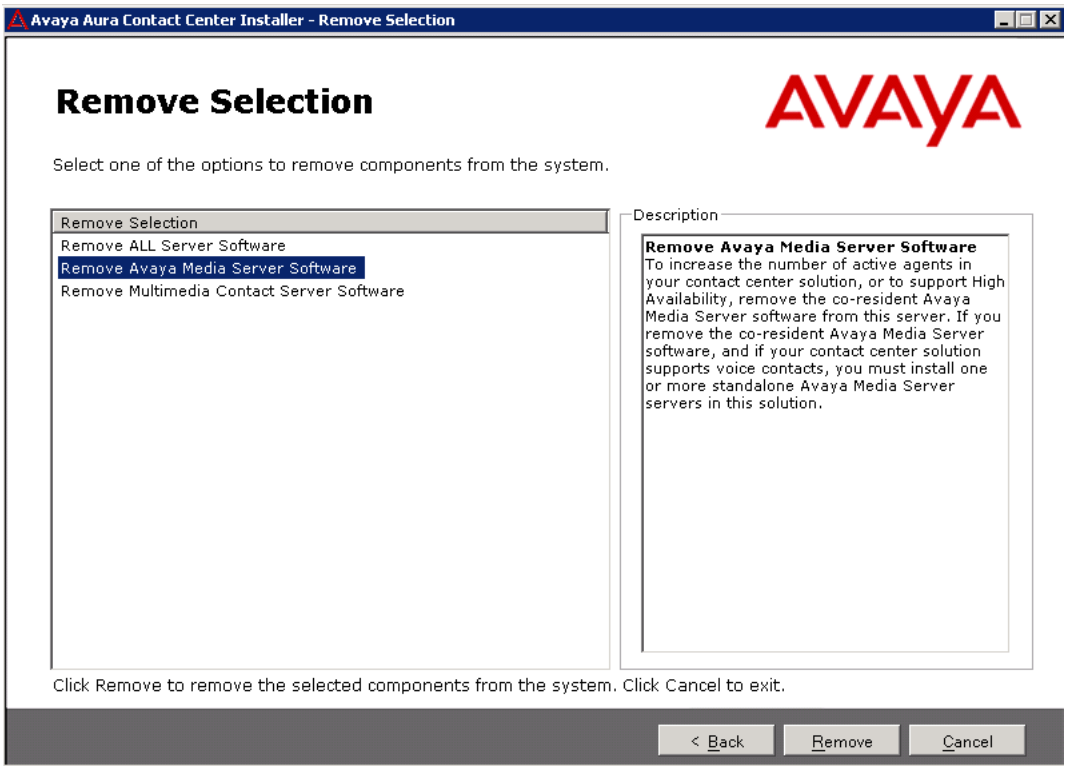
You must remove the Avaya Media Server software from the Voice and Multimedia Contact Server to support High Availability. Because this is a High Availability deployment, you must install Avaya Media Server on the Linux operating system.

Prerequisites

- To maintain the Avaya Media Server database, ensure that you back up the database to another network location.
- Ensure that all Contact Center services are stopped and all agents are logged out.

Procedure steps

Step	Action
1	Log on to the Voice and Multimedia Contact Server with Avaya Media Server.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Uninstall Contact Center**.
3	On the **Welcome** window, click **Next**.
4	On the **Remove Selection** window, select **Remove Avaya Media Server Software**.



5 Click **Remove**.

6 Confirm the software applications to remove.

7 Click **Remove**.

8 After the installation is complete, click **Finish**.

9 If you are prompted, restart the server.

--End--

Avaya Media Server – Primary server software installation

This chapter describes how to install Avaya Media Server software on the primary server in your SIP-enabled Avaya Aura® Contact Center solution. Because this is a High Availability deployment, you must install Avaya Media Server on the Linux operating system.

Avaya Media Server is a software based media processing platform. The Avaya Aura® Contact Center DVD contains an enhanced version of Avaya Media Server, which contains an additional component—Contact Center Services for Avaya Media Server. The Contact Center Services package application provides the conference, announcement, and dialog services required by a SIP-enabled Contact Center.

You can change the name of an Avaya Media Server server after installation is complete, but because this is time consuming, Avaya recommends that you configure the server final production name before installing Contact Center software.

Example server details	Primary Avaya Media Server
Name	AMSHOST1
IP Address	172.18.71.113

You can create an administration account on the server and then install Avaya Media Server using the account. This Avaya Media Server administration account must have full administrative privileges. You must upgrade and patch Avaya Media Server using this administration account. You must not delete the account. If you delete the account used to install Avaya Media Server, Avaya Media Server stops working.

Prerequisites to Avaya Media Server installation

- Ensure that the Avaya Media Server server meets or exceeds the minimum hardware and platform requirements as specified in *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
- Download and review the Avaya Aura® Contact Center Release Notes. The Release Notes contain the known issues, patches, and workarounds specific to a release and patch line-up of Avaya Aura® Contact Center. For more information about the Avaya Aura® Contact Center Release Notes, see www.avaya.com/support.

Installing the Linux server for Avaya Media Server

Install the Linux server operating system so you can install the Avaya Media Server software.

Avaya Aura® Contact Center supports only Red Hat Enterprise Linux R6.3 (32–bit version) for Avaya Media Server. Avaya Media Server supports only Red Hat Enterprise Linux R6.3 (32–bit version) with English as the selected language.

These instructions are general: depending on your site you can have specific configuration requirements for your Linux servers. If you do not have specific requirements, select the installation defaults except where this procedure specifies otherwise.

Prerequisites

- Ensure your new server hardware meets all the requirements described in *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).

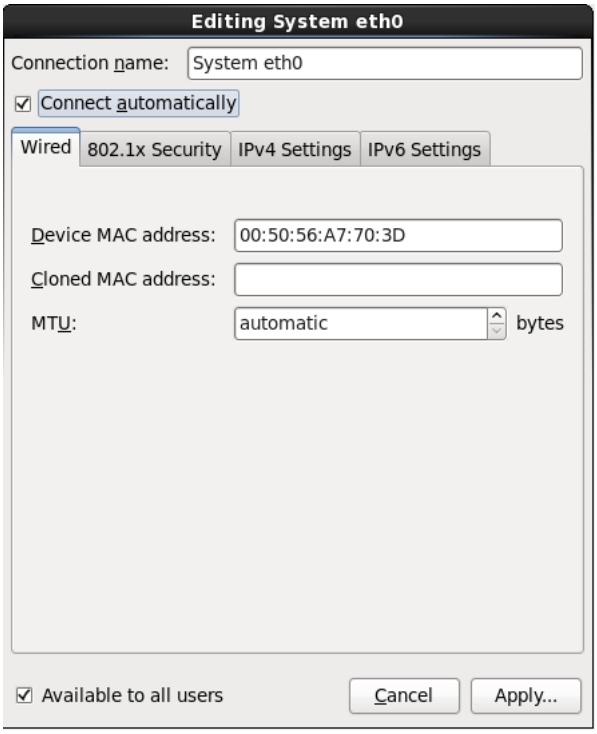
Procedure steps

Step	Action
1	Place the Linux installation disk in the DVD drive of the primary server and turn the server on.
2	Restart the server by powering it off, then powering it on again.
3	On the **Welcome to Red Hat Enterprise Linux 6.3!** screen, select **Install or upgrade an existing system**.
4	On the **Disc Found** screen, select **OK** if you want to test your installation media (DVD), or select **Skip** to continue. Testing the media can take a long time, but it helps prevent installation problems that can occur due to bad media.
5	On the **Red Hat Enterprise Linux 6** splash screen, select **Next**.
6	On the **What language would you like to use for the installation** screen, select **English (English)**. Avaya Media Server supports only the English operating system.
7	On the **Select an appropriate keyboard for the system** screen, select the keyboard type for your server, and click **Next**.
8	On the **What type of devices will your installation involve** screen, select **Basic Storage Devices**, and click **Next**.
9	If the installer displays the **Storage Device Warning** screen, click **Yes, discard any data**, and click **Next**.
10	If the installer displays the **At least one existing installation has been detected on your system** screen, select **Fresh Installation**, and click **Next**.
11	On the **Please name this computer** screen, in the **Hostname** box, enter the host name for this server. For example, enter AMSHOST1.
12	Click **Configure Network**.

13 Select the Ethernet interface that you are going to connect to your physical network, and click **Edit**.

14 On the **Network Connections** screen, select **Connect automatically**.

15 On the **Network Connections** screen, select the **Wired** tab.

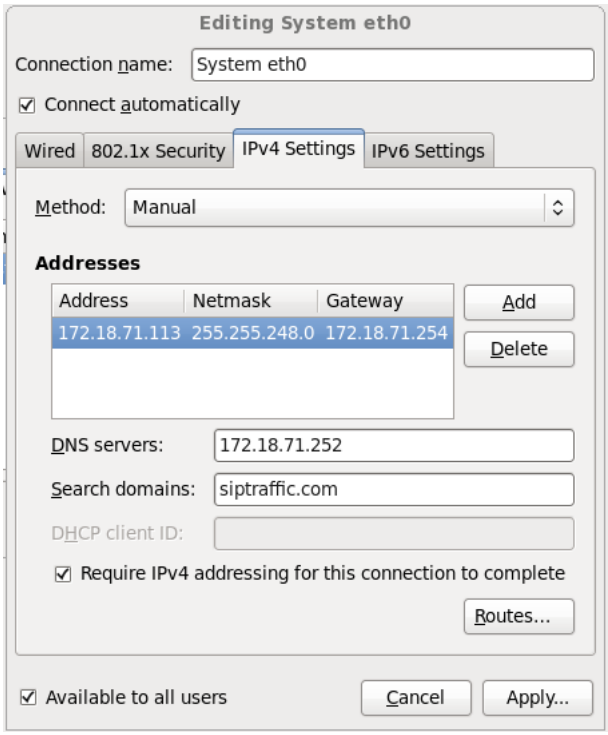


16 On the **Editing** screen for the interface you selected, select the **IPv4 Settings** tab.

17 From the **Method** list, select **Manual**.

18 Click **Add**.

19 Enter the IP address, network mask, and gateway for this server. For example, enter an IP address of 172.18.71.113.



20 In the **DNS servers** box, enter the IP address of the DNS server for your network.

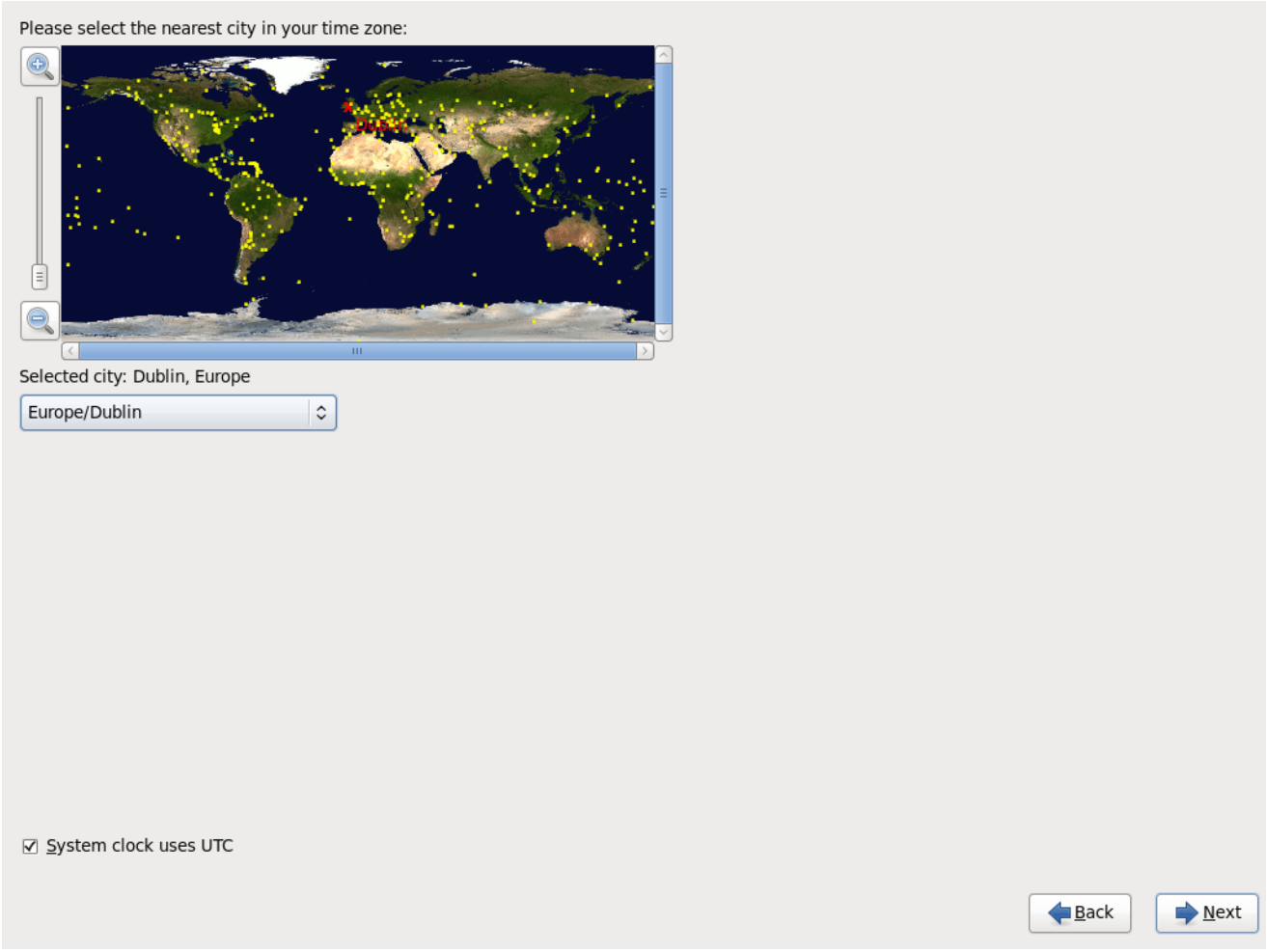
21 In the **Search domains** box, enter the domain for this server.

22 Click **Apply**.

23 On the **Network Connections** screen, click **Close**.

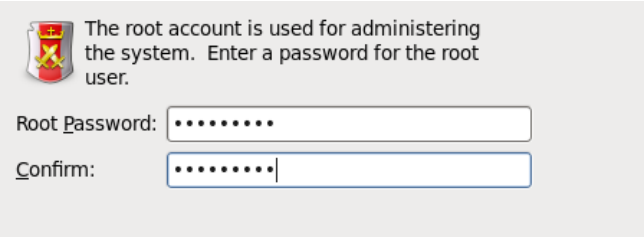
24 Click **Next**.

25 On the **Please select the nearest city in your time zone** screen, select the nearest city to your server's location. For example, select Europe/Dublin.

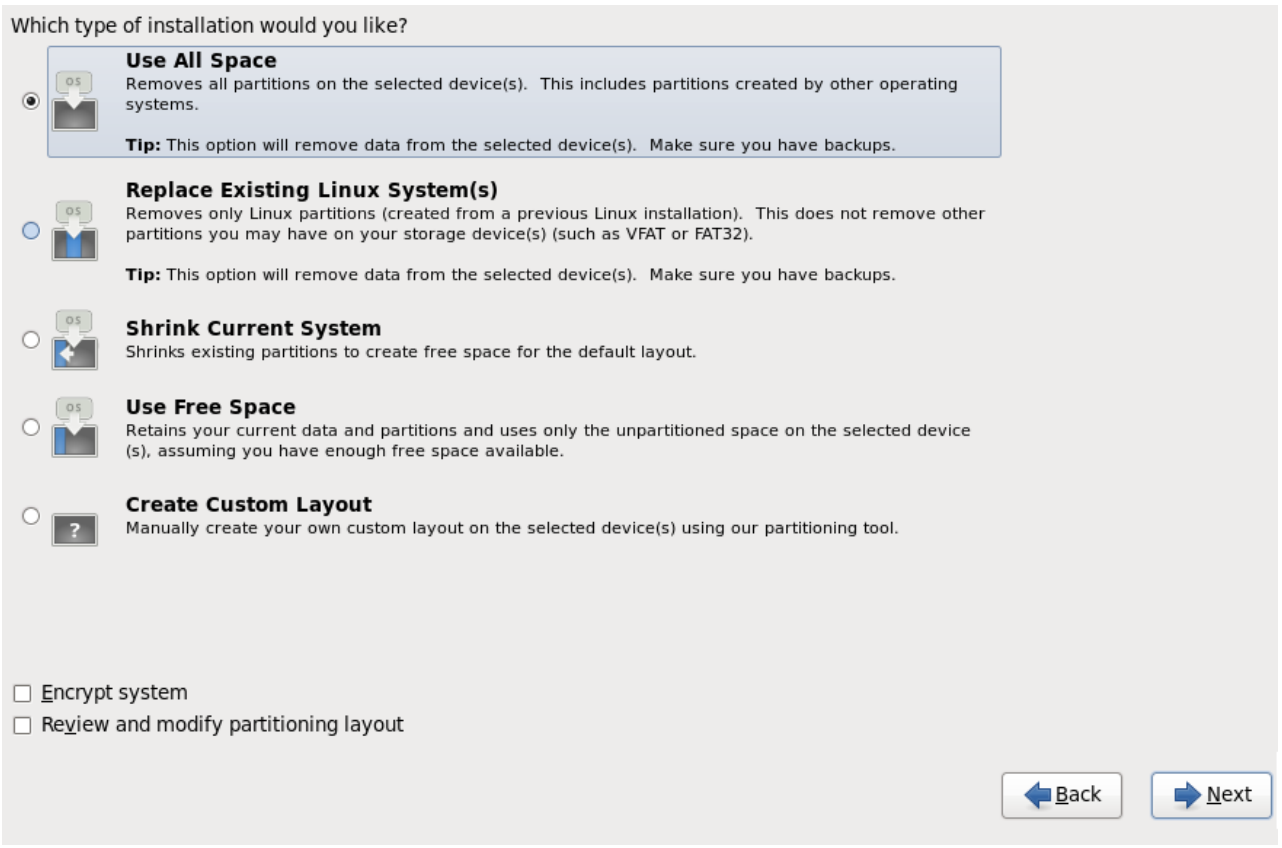


26 Select **System clock uses UTC**, and click **Next**.

27 In the **Root Password** box, type and confirm the root password for this server, and click **Next**.

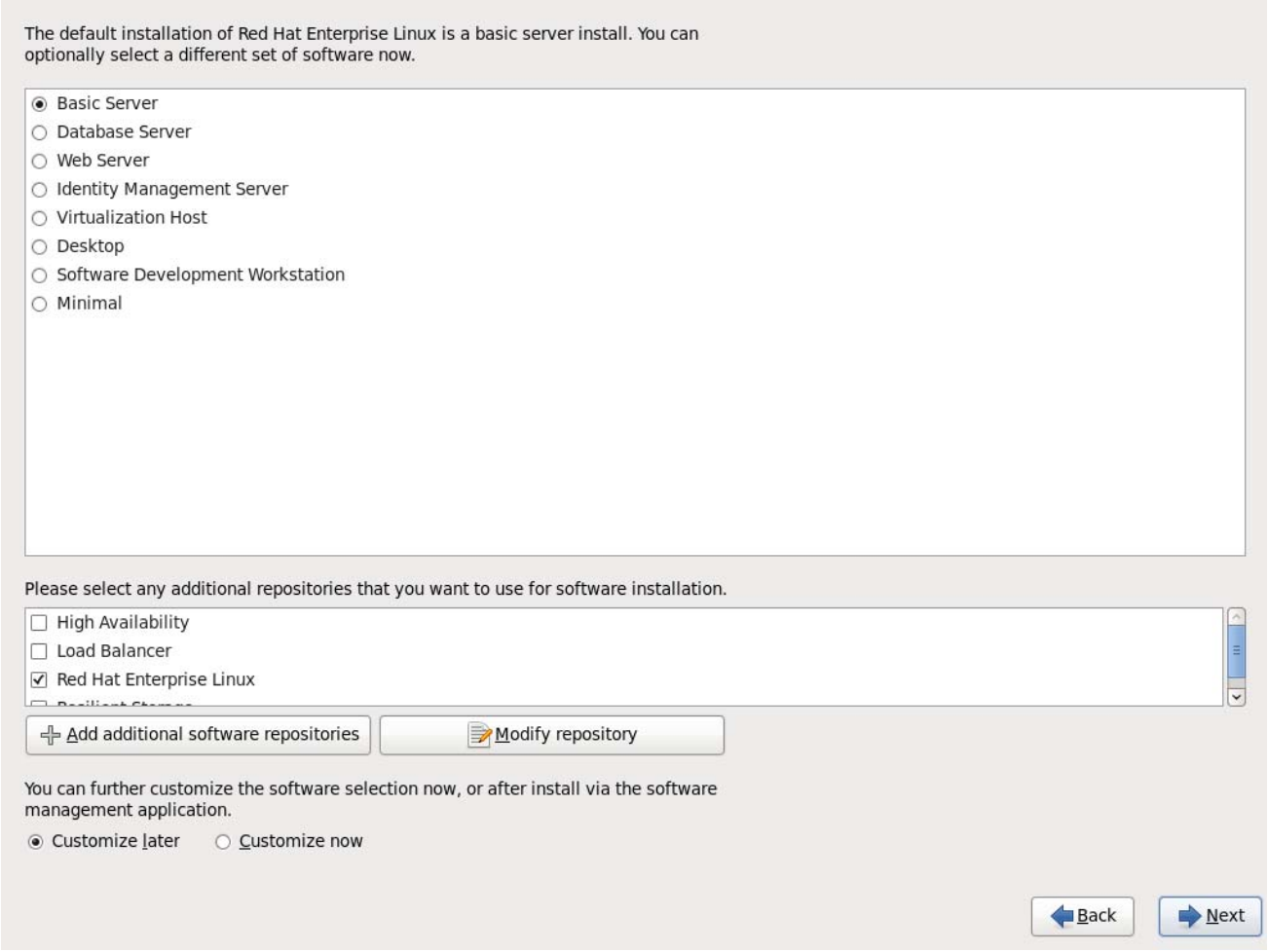


28 On the **Which type of installation would you like** screen, select **Use All Space**, and click **Next**.



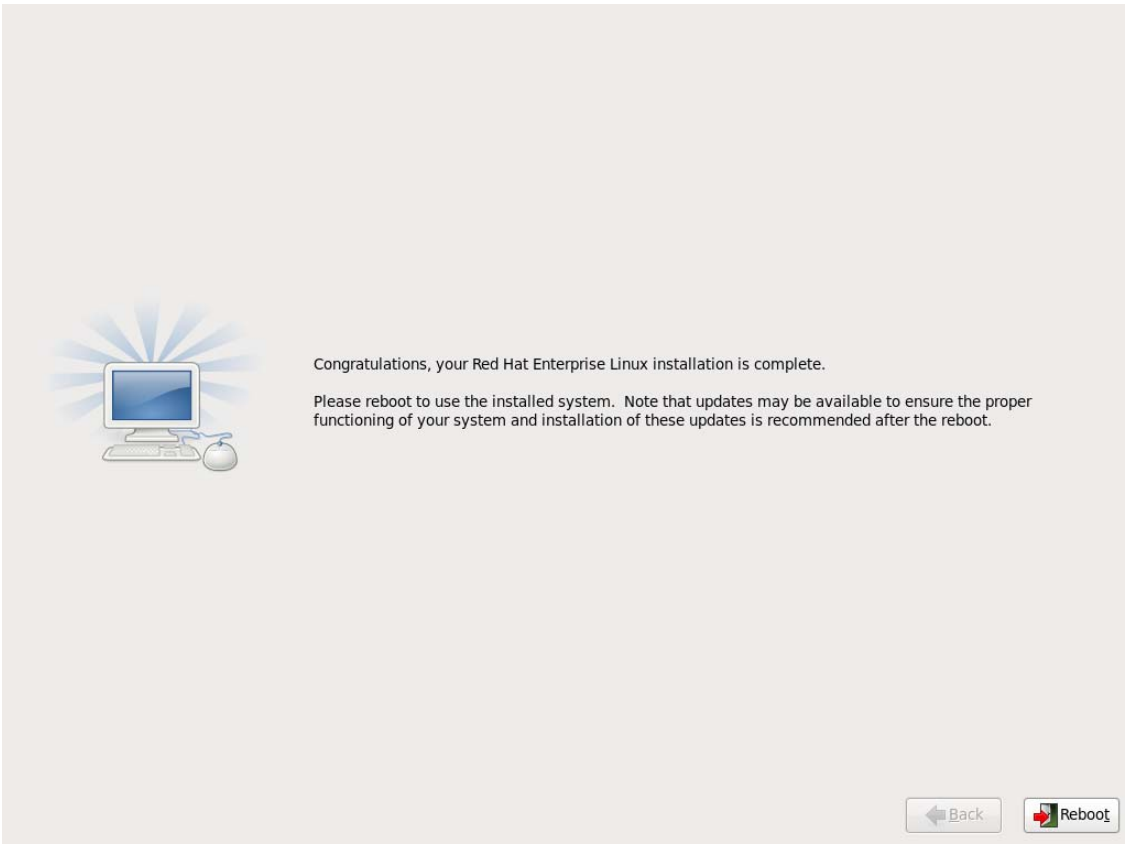
29 On the **Writing storage configuration to disk** screen, select **Write changes to disk**.

30 On the default installation of Red Hat Enterprise Linux screen, select **Basic Server**.

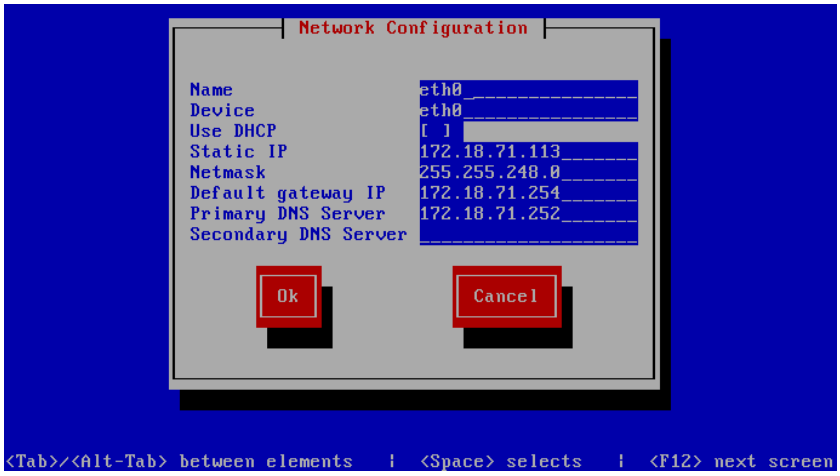


31 Click **Next**.

32 Complete the installation and reboot the server.



33 Log on to the server and verify that the Ethernet connection is operating correctly. You can use the ifconfig, ping, and ifup commands to check and start the connection. You can use the system-config-network-tui command to verify your network configuration details. If the connection does not work, refer to your Red Hat documentation for troubleshooting guidance. The following is an example of using the **system-config-network-tui** command:



--End--

Installing the required packages on the Linux server

Avaya Media Server (Avaya MS) requires specific 32–bit Linux packages to operate correctly. Check whether these packages are installed and install any that are missing. This procedure explains how to use the YUM package manager to check, install, and remove packages.

You must remove the mysql-libs package from the Avaya MS server.

Prerequisites

- Log on to the Linux server using the root account.

Procedure steps

Step	Action
1	Put the Red Hat Enterprise Linux DVD in the server DVD drive.
2	Change to the root user by running the following command: **`su –`**
3	Mount the Red Hat Enterprise Linux DVD by running the following commands: **`mkdir /mnt/cdrom`** **`mount /dev/cdrom /mnt/cdrom`**
4	Set up the YUM repository by copying the yum .repo file from the RHEL DVD, using the following commands: **`cp /mnt/cdrom/media.repo /etc/yum.repos.d/`**
5	Set up the YUM repository .repo file permissions. For example:

chmod +rw /etc/yum.repos.d/media.repo

6 Use the vi editor to open the YUM repository .repo file. For example, enter:

vi /etc/yum.repos.d/media.repo

7 Use the vi editor to add the following lines to the end of the YUM repository .repo file. This configures YUM to point to the mounted DVD image.

```
baseurl=file:///mnt/cdrom
enabled=1
```

8 For each Linux package required for Avaya MS, use the yum info command to check whether it is installed on the server. For example, the following command checks whether the libX11.i686 package is installed:

yum info libX11

For the list of required packages, see Procedure job aid (page 366).

9 If you find a required 32–bit Linux package is not present on the server, run the yum install command to install it. For example, the following command installs the libX11.i686 package:

yum install libX11.i686

10 If the libXdmcp Linux package is not present on the server, run the yum install command to install it. For example, the following command installs the libXdmcp.i686 package:

yum install libXdmcp.i686

11 Use the yum remove command to remove the mysql-libs package from the server:

yum remove mysql-libs

--End--

Procedure job aid

The following example shows the complete set of commands to mount the RHEL DVD, set up the YUM repository, check and install the libX11 and libXdmcp packages, and remove the mysql-libs package. Linux packages required for Avaya Media Server. Avaya Media Server requires 32–bit versions of the following RHEL 6.x packages:

```
su -
Password: *******
mkdir /mnt/cdrom
mount /dev/cdrom /mnt/cdrom
cp /mnt/cdrom/media.repo /etc/yum.repos.d/
chmod +rw /etc/yum.repos.d/media.repo
vi /etc/yum.repos.d/media.repo
      /* --- Add the following lines to the end of the file, save and
quit
      baseurl=file:///mnt/cdrom
      enabled=1 --- */
yum info libX11
yum install libX11.i686
```

```
yum info libXdmcp
yum install libXdmcp.i686
yum remove mysql-libs
```

When you run the yum info command, the Arch: heading of the output contains i686 if the installed package is the 32-bit version. The Repo: heading shows Installed if the package is already installed.

- **cyrus-sasl-lib**
- **e2fsprogs-libs**
- **glibc**
- **iproute**
- **keyutils-libs**
- **krb5-libs**
- **libICE**
- **libSM**
- **libX11**
- **libXau**
- **libXdmcp**
- **libXext**
- **libXt**
- **libgcc**
- **libidn**
- **libselinux**
- **libsepol**
- **libstdc++**
- **net-snmp-utils**
- **openldap**
- **zlib**

Adding a Linux user group and user

Create a Linux user group, create a Linux user and make the user a member of the user group.

For example, create a user group named amsgroup, and then create a user amsuser as a member of that group. You then use this account to access Avaya Media Server - Element Manager.

Procedure steps

Step	Action
1	Open a Linux terminal on the Linux server.
2	Change to root user by running the following command: **su –**
3	Use the Linux groupadd command to create a new group. For example, enter **groupadd amsgroup**.
4	Use the Linux useradd command to create a new user in the group you created. For example, enter **useradd amsuser -G amsgroup**.
5	Use the Linux passwd command to configure the password for the user. For example, enter **passwd amsuser**.

--End--

Preparing the Linux server for Avaya Media Server

Prepare the Linux server so you can install the Avaya Media Server software. Security Enhanced Linux (SELinux) enforces the access rules, which apply to the processes and files on a Linux server. To support Avaya Aura® Contact Center and Avaya Media Server, you must disable SELinux.

When a network address is added to a Linux server, the corresponding entries in the Linux /etc/hosts configuration file are not compatible with the Avaya Media Server PVI checker. You must edit the Linux hosts file to enable Avaya Media Server network communication.

Procedure steps

Step	Action
1	Open a Linux terminal on the Linux server.
2	Change to the root user account by running the following command: **su –**
3	Enter **sestatus**, to check the SELinux status. If the status is disabled then skip to step 8.

```
[root@AMSHOST1   ~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /selinux
Current mode:                   enforcing
Mode from config file:          enforcing
Policy version:                 24
Policy from config file:        targeted
[root@AMSHOST1   ~]# _
```

4 To disable SELInux, using the vi text editor, edit the /etc/selinux/config configuration file. For example, enter:

vi /etc/selinux/config

5 Change the SELINUX line to read **SELINUX=disabled**

```
[root@AMSHOST1   ~]# more /etc/selinux/config

# This file controls the state of SELinux on the system.
# SELINUX=disabled
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these two values:
#     targeted - Targeted processes are protected,
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted


[root@AMSHOST1   ~]# _
```

6 Reboot the server to apply the SELinux updates.

7 Open a Linux terminal on the Linux server.

8 Change to the root user account.

9 Using the vi text editor, edit the /etc/hosts configuration file. For example, enter:

vi /etc/hosts

10 Edit the hosts file to include the IP address and name of the primary and backup Avaya Media Servers.

```
[root@AMSHOST1 ~]# more /etc/hosts
127.0.0.1 localhost.localdomain localhost
172.18.71.113 AMSHOST1.siptraffic.com AMSHOST1
172.18.71.114 AMSHOST2.siptraffic.com AMSHOST2
[root@AMSHOST1 ~]# _
```

11 Save the hosts file and exit the editor.

--End--

Configuring Network Time Protocol

The High Availability primary and backup Avaya Media Servers must be synchronized in time. You use Network Time Protocol (NTP) to synchronize both servers with each other and with the contact center solution.

Procedure steps

Step	Action
1	Log on to the primary Avaya Media Server.
2	Edit the /etc/ntp.conf file to specify the NTP Server for both Avaya Media Servers. Edit the /etc/ntp.conf file to specify the NTP server. For example, add this line to the ntp.conf file: server <NTP IP Address> Where <NTP IP Address> is the IP address of your NTP server.
3	Open a Linux terminal on the Avaya Media Server.
4	Start the Network Time Protocol ntpd client service. This is done using the command: **service ntpd start**
5	Configure the Network Time Protocol ntpd client service to automatically start after a Linux server reboot. This is done using the command: **chkconfig ntpd on**
6	Verify that the Network Time Protocol client is working. This is done using the command: **ntpq -p**

--End--

Installing the Avaya Media Server software

Install the Avaya Media Server (Avaya MS) software to provide media processing for contacts in a SIP-enabled contact center environment.

Prerequisites

- Read the Contact Center Release Notes and the Avaya Media Server Release Notes for the most recent instructions.
- Log on to the Linux server.
- Obtain the Avaya Aura® Contact Center Release 6.3 DVD. The latest Avaya Aura® Contact Center 6.3 DVD may not contain the most recent version of the Avaya

Media Server software. Read the Avaya Aura® Contact Center Release Notes to ensure that you are using the most recent version of Avaya Media Server software.

Procedure steps

Step	Action
1	Log on to the Linux server and change to the root user by running the following command: **`su -`**
2	Stop the Linux firewall using the following command: **`service iptables stop`**
3	Create a folder on the Avaya MS server by running the following command: **`mkdir /tmp/AvayaMS`**
4	Mount the Avaya Aura® Contact Center Release 6.3 DVD, for example type the following: **`mount /dev/cdrom /mnt/cdrom/`**
5	Copy the Avaya Media Server installation file to the temporary directory you created. For example: **`cp "/mnt/cdrom/Install Software/AMS/linux/ MediaServer_7.5.0.837_2012.09.12.bin" /tmp/AvayaMS`**
6	Copy the most recent version of the Contact Center Services for Avaya Media Server software to the temporary folder on the Linux server. For example, copy **`ContactCenterServicesForAMS_6.3.0.104`** to **`/tmp/AvayaMS`**.
7	Navigate to the directory where the files have been copied too. **`cd /tmp/AvayaMS`**
8	Grant executable permissions to the Avaya MS installation file. For example: **`chmod +x MediaServer_7.5.0.837_2012.09.12.bin`**
9	Start the Avaya MS installer by running the following command: **`./MediaServer_7.5.0.837_2012.09.12.bin`**
10	The installer displays the License Agreement. Press **Enter** to page through the license agreement.
11	To accept the license agreement and continue with the install, enter Y.
12	When prompted `Install Element Manager?`, enter `Y` to install the Element Manager.
13	When prompted for the `Linux group name`, press **Enter** to accept the default or specify the target **amsgroup** group. For example, select **amsgroup** so all members of this group can log on and use Avaya Media Server - Element Manager. • Press Enter to accept the default.

- Specify an existing user group. Select an existing user group so members of that group can log on and use Avaya Media Server Element Manager. For example, select the **amsgroup** user group.

14 When prompted `Where would you like to install?`, press **Enter** to accept the default of `/opt/avaya`.

The installer displays the progress of the Avaya Media Server installation.

```
Some platform compatibility warnings have been detected.
The installation will be allowed to continue.

See /root/maspviresult.xml for detailed results.

Overall:  WARNING

Drives:   PASS
Hardware: PASS
Software: WARNING

PRESS <ENTER> TO ACCEPT THE FOLLOWING (Continue):



================================================================================
Installing...
-------------

 [==================|==================|==================|==================]
 [------------------|------------------|------------------|------------------]
```

15 Once the Avaya Media Server software installs, press **Enter** to exit the install.

16 Assign executable permissions to the Contact Center Services For Avaya Media Server installation file. For example,

`chmod +x ContactCenterServicesForAMS_6.3.0.104`

17 Start the Contact Center Services for Avaya Media Server installer by running the installation file. For example,

`./ContactCenterServicesForAMS_6.3.0.104`

The installer displays the progress of the Contact Center Services For Avaya Media Server installation.

18 When the Contact Center Services for Avaya Media Server installation completes, copy the Avaya MS firewall configuration file to the system using the following command:

`cp /opt/avaya/iptables.AMS75 /etc/sysconfig/iptables`

Overwrite the existing firewall, if prompted to do so.

19 Run the shell script to set up the Avaya MS environment using the following command:

`. /etc/profile.d/masenv.sh`

Note: the extra space before /etc is intentional.

20 Restart the Linux firewall using the following command:

```
service iptables start
```

21 Reboot the Linux server.

--End--

Installing the Avaya Media Server patches

Install a new Quick Fix Engineering (QFE) patch to apply a change to the Avaya Media Server system. You must lock Avaya Media Server before applying patches and unlock it after the patches are installed.

Quick Fix Engineering (QFE) patches are available for Avaya Media Server and Avaya Aura® Contact Center Service for Media (CCSM).

Prerequisites

- Download the most recent Avaya Media Server and Element Manager Quick Fix Engineering patches and store them in the QFE subdirectory on the Avaya Media Server server. QFE patches are ZIP files, do not un-zip QFE patches. The Avaya Media Server patching utility uses the QFE ZIP files. For a Linux server the default QFE folder location is /opt/avaya/ma/MAS/qfe.

Procedure steps

Step	Action
1	On a computer that can access the primary Avaya Media Server, start a Web browser.
2	In the address box, enter https://<AMS_SERVER_IP_ADDRESS>:8443/em. To access the primary Avaya Media Server Element Manager (EM), enter https://172.18.71.113:8443/em
3	In the **User ID** box, type amsuser.
4	In the **Password** box, type the amsuser password.
5	Click **Log In**.
6	In the navigation pane, click **System Status**, **Element Status**.
7	From the **More Actions** list, select **Pending Lock** to lock the Avaya Media Server after all processes finish.
8	Click **Confirm** to change the Element Status.
9	Close Avaya Media Server Element Manager.
10	Open a Linux terminal on the Linux server.

11 Change to the root user by running the following command:

```
su -
```

12 Copy the Linux QFE files to the /opt/avaya/ma/MAS/qfe folder.
For example use:

```
cp QFE-* /opt/avaya/ma/MAS/qfe
```

13 Obtain the correct name of the new QFE patch by entering the following command:

```
maspatch list all
```

The name of the file is not necessarily the same as the name of the patch name.

14 Install all of the patches in numerical order. To install all new patches on the system, enter the following command:

```
maspatch apply all
```

15 When the patch application is complete, open the Element Manager navigation pane, and select **Tools**, **Software Inventory**.

16 Verify the patch version listed in the **Patch Level** column is correct.

17 In the Element Manager navigation pane, click **System Status**, **Element Status**.

18 From the **More Actions** list, select **Unlock** to unlock the Avaya Media Server.

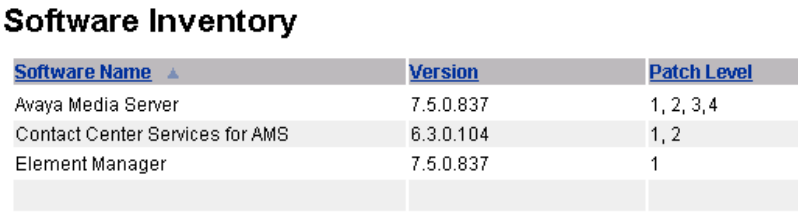
19 Click **Confirm** to change the Element Status.

--End--

Procedure job aid

Avaya Media Server - Element Manager Software Inventory showing the patches.

Example of Avaya Media Server Software Inventory



Securing your Avaya Media Server

Apply optional security measures to your operating system to further secure your server.

Scanning software can degrade the performance and decrease the reliability of the system. Install virus scanning software only if the system connects to an exposed network or to the Internet.

To maintain server performance, you must schedule virus scans during maintenance periods or low usage hours only.

Procedure steps

Step	Action
1	Harden the operating system using defined site procedures.
2	Install antivirus software. If you install antivirus software, ensure that you exclude the following directories from the scans. The following are the default install locations. If you installed Avaya Media Server in a different location, navigate to the necessary directories and exclude them from antivirus scans. • /opt/avaya/ma/MAS/platdata • /opt/avaya/ma/MAS/common/log

--End--

Avaya Media Server – Backup server software installation

This chapter describes how to install Avaya Media Server software on the backup server in your SIP-enabled Avaya Aura® Contact Center solution. Since this is a High Availability deployment, you must install Avaya Media Server on the Linux operating system.

Avaya Media Server is a software based media processing platform. The Avaya Aura® Contact Center DVD contains an enhanced version of Avaya Media Server which contains an additional component—Contact Center Services for Avaya Media Server. The Contact Center Services package application provides the conference, announcement, and dialog services required by a SIP-enabled Contact Center.

You can change the name of an Avaya Media Server server after installation is complete, but because this is time consuming, Avaya recommends that you configure the server final production name before installing Contact Center software.

Example server details	Backup Avaya Media Server
Name	AMSHOST2
IP Address	172.18.71.114

You can create an administration account on the server and then install Avaya Media Server using the account. This Avaya Media Server administration account must have full administrative privileges. You must upgrade and patch Avaya Media Server using this administration account. You must not delete this account. If you delete the account used to install Avaya Media Server, Avaya Media Server stops working.

Prerequisites to Avaya Media Server installation

- Ensure that the Avaya Media Server server meets or exceeds the minimum hardware and platform requirements as specified in *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
- Download and review the Avaya Aura® Contact Center Release Notes. The Release Notes contain the known issues, patches, and workarounds specific to a release and patch line-up of Avaya Aura® Contact Center. For more information about the Avaya Aura® Contact Center Release Notes, see www.avaya.com/support.

Installing the Linux server for Avaya Media Server

Install the Linux server operating system so you can install the Avaya Media Server software.

Avaya Aura® Contact Center supports only Red Hat Enterprise Linux R6.3 (32–bit version) for Avaya Media Server. Avaya Media Server supports only Red Hat Enterprise Linux R6.3 (32–bit version) with English as the selected language.

These instructions are general: depending on your site you can have specific configuration requirements for your Linux servers. If you do not have specific requirements, select the installation defaults except where this procedure specifies otherwise.

Prerequisites

- Ensure your new server hardware meets all the requirements described in *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).

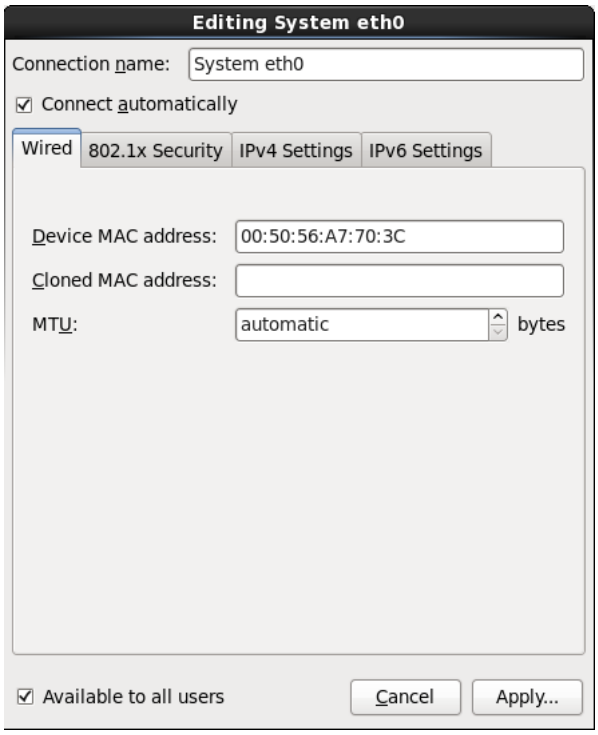
Procedure steps

Step	Action
1	Place the Linux installation disk in the DVD drive of the primary server and turn the server on.
2	Restart the server by powering it off, then powering it on again.
3	On the **Welcome to Red Hat Enterprise Linux 6.3!** screen, select **Install or upgrade an existing system**.
4	On the **Disc Found** screen, select **OK** if you want to test your installation media (DVD), or select **Skip** to continue. Testing the media can take a long time, but it helps prevent installation problems that can occur due to bad media.
5	On the **Red Hat Enterprise Linux 6** splash screen, select **Next**.
6	On the **What language would you like to use for the installation** screen, select **English (English)**. Avaya Media Server supports only the English operating system.
7	On the **Select an appropriate keyboard for the system** screen, select the keyboard type for your server, and click **Next**.
8	On the **What type of devices will your installation involve** screen, select **Basic Storage Devices**, and click **Next**.
9	If the installer displays the **Storage Device Warning** screen, click **Yes, discard any data**, and click **Next**.
10	If the installer displays the **At least one existing installation has been detected on your system** screen, select **Fresh Installation**, and click **Next**.
11	On the **Please name this computer** screen, in the **Hostname** box, enter the host name for this server. For example, enter AMSHOST2.
12	Click **Configure Network**.

13 Select the Ethernet interface that you are going to connect to your physical network, and click **Edit**.

14 On the **Network Connections** screen, select **Connect automatically**.

15 On the **Network Connections** screen, select the **Wired** tab.

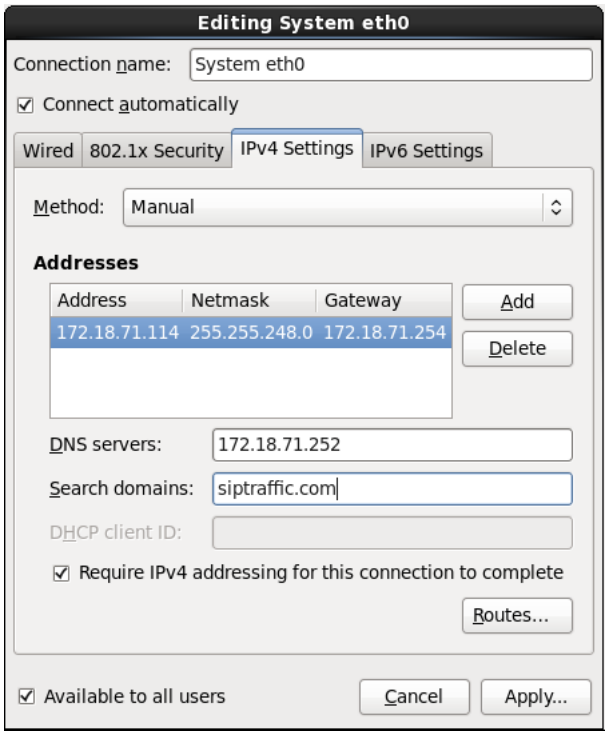


16 On the **Editing** screen for the interface you selected, select the **IPv4 Settings** tab.

17 From the **Method** list, select **Manual**.

18 Click **Add**.

19 Enter the IP address, network mask, and gateway for the standby Avaya Media Server. For example, enter an IP address of 172.18.71.114.



20 In the **DNS servers** box, enter the IP address of the DNS server for your network.

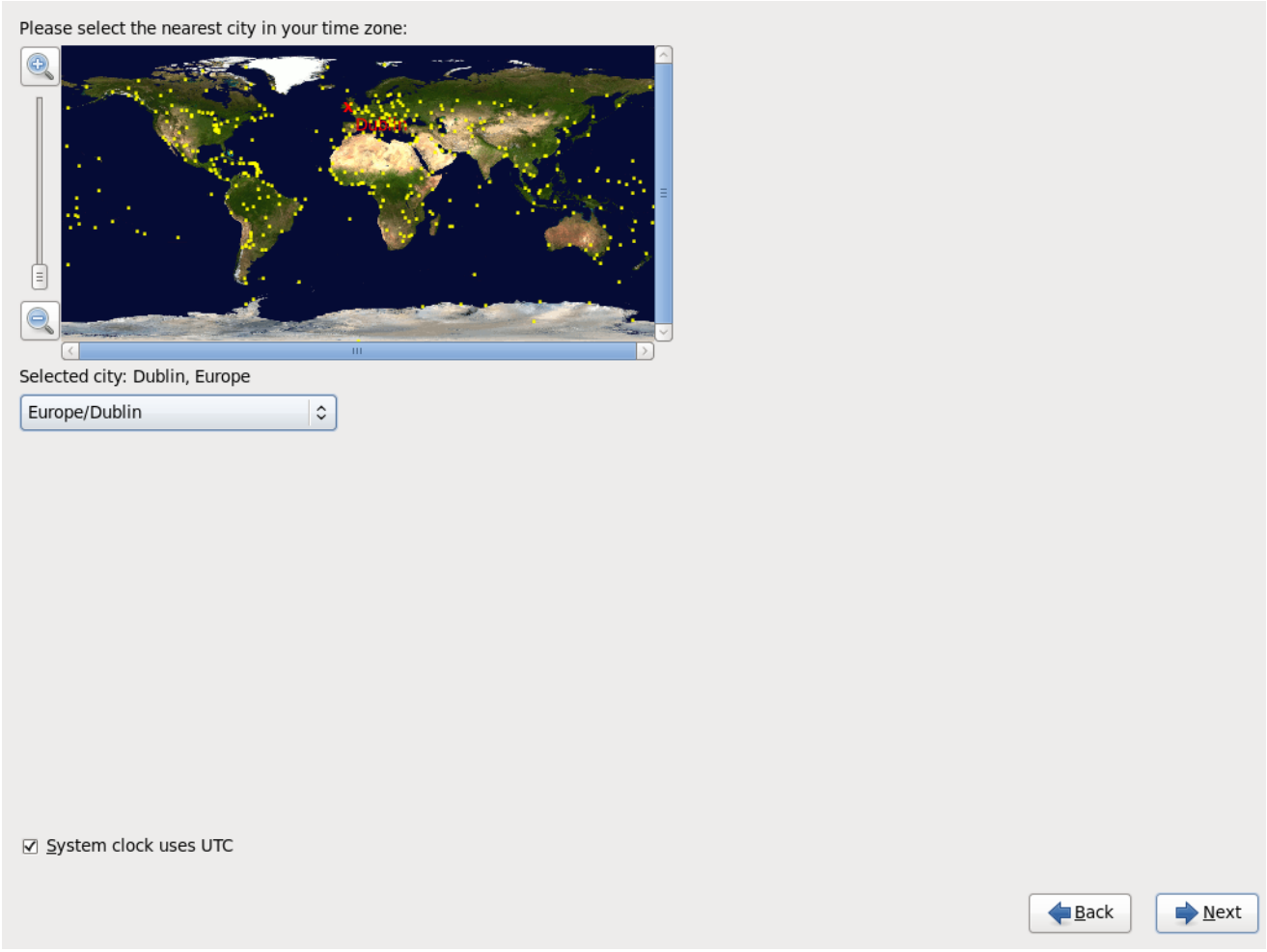
21 In the **Search domains** box, enter the domain for this server.

22 Click **Apply**.

23 On the **Network Connections** screen, click **Close**.

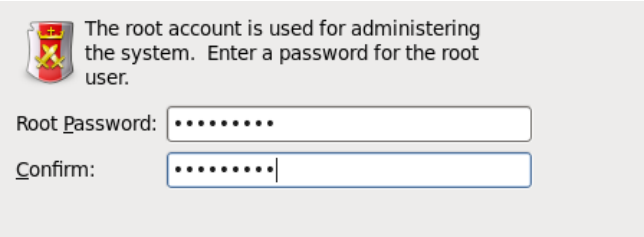
24 Click **Next**.

25 On the **Please select the nearest city in your time zone** screen, select the nearest city to your server's location. For example, select Europe/Dublin.

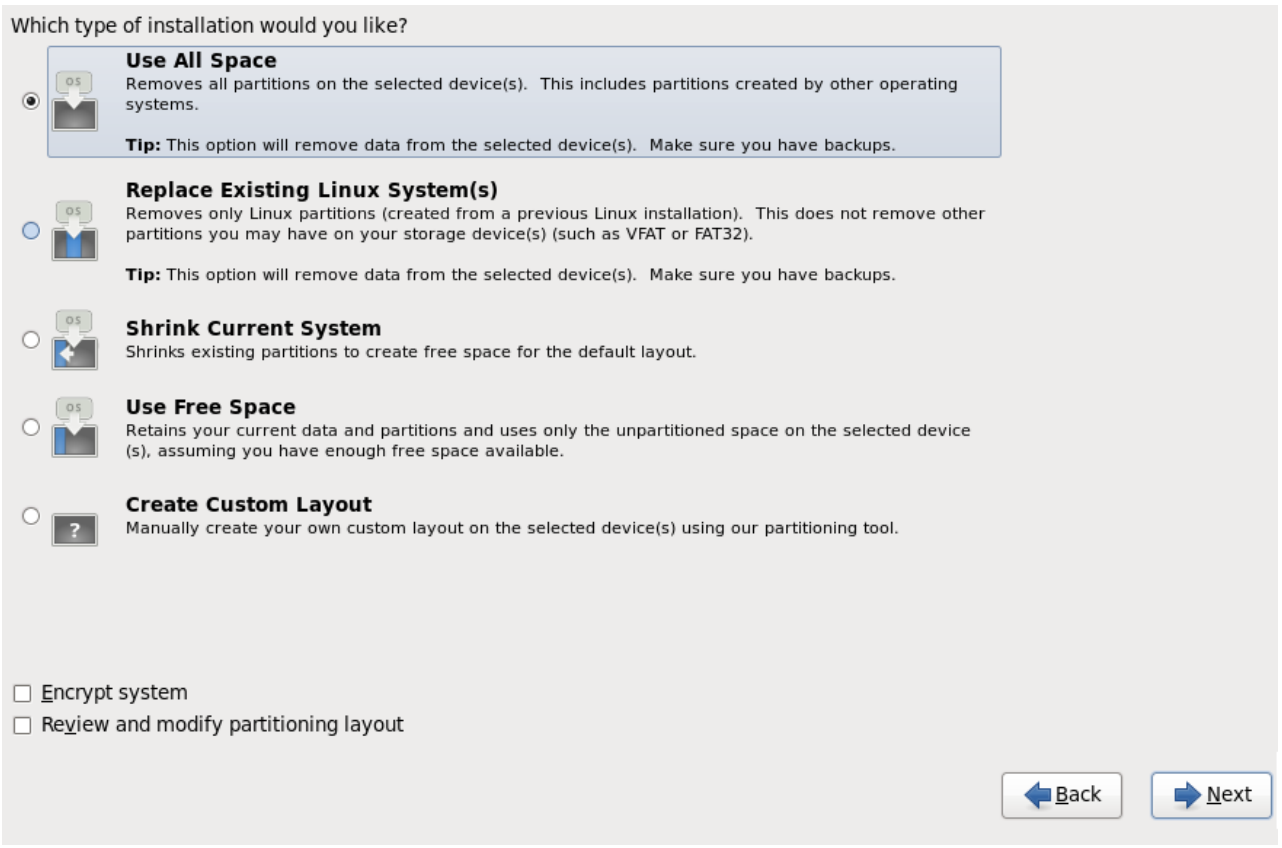


26 Select **System clock uses UTC**, and click **Next**.

27 In the Root Password box, type and confirm the root password for this server, and click **Next**.

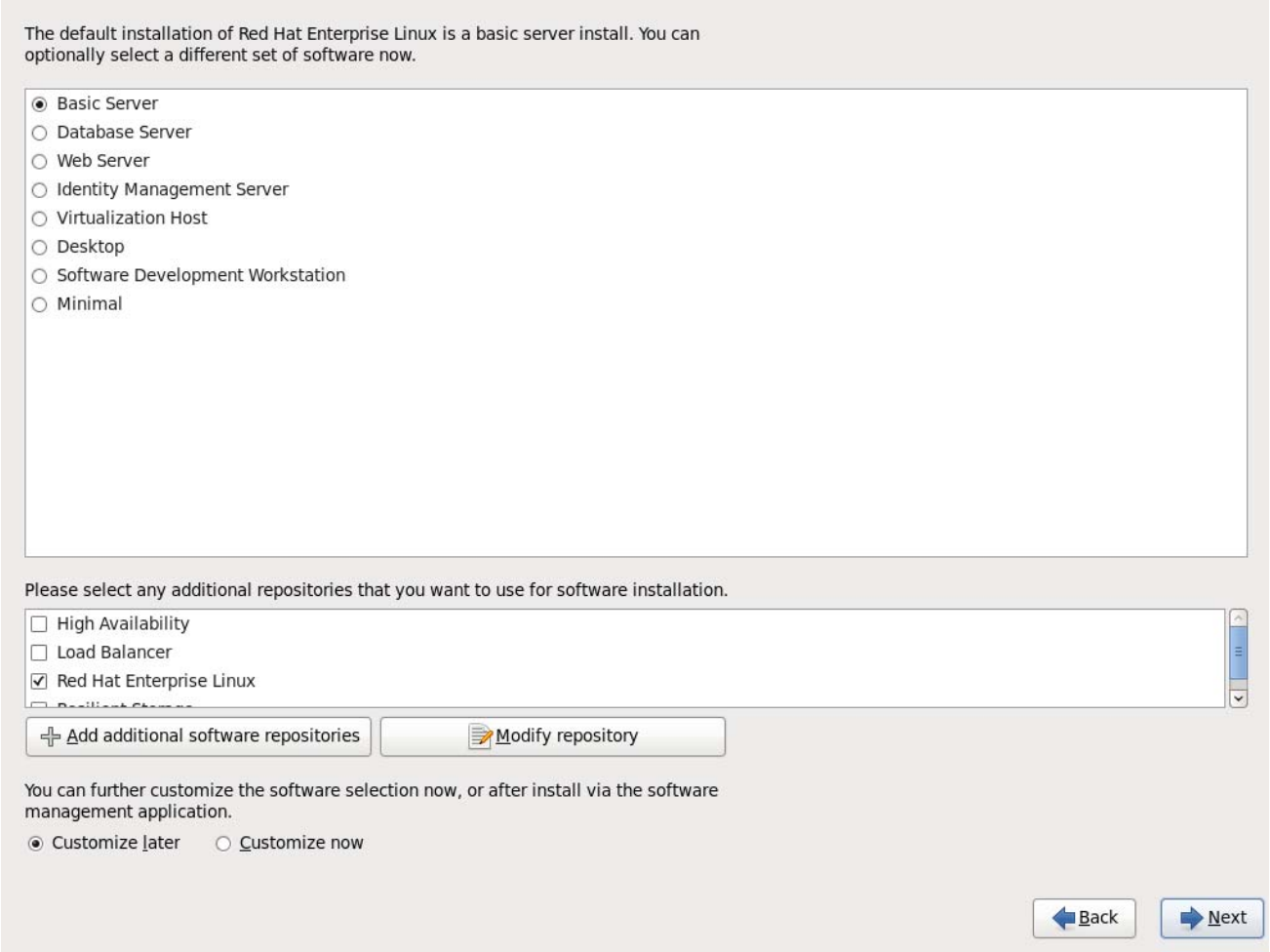


28 On the **Which type of installation would you like** screen, select **Use All Space**, and click **Next**.



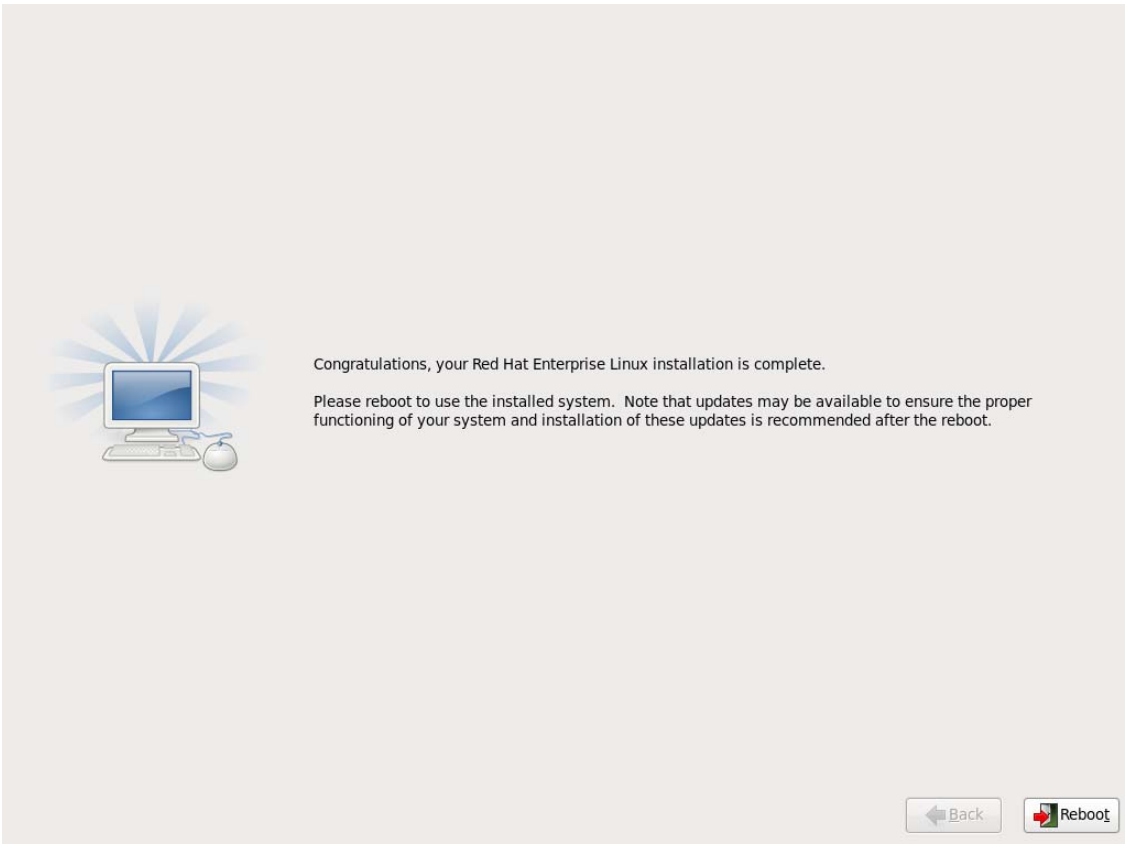
29 On the **Writing storage configuration to disk** screen, select **Write changes to disk**.

30 On the default installation of Red Hat Enterprise Linux screen, select **Basic Server**.

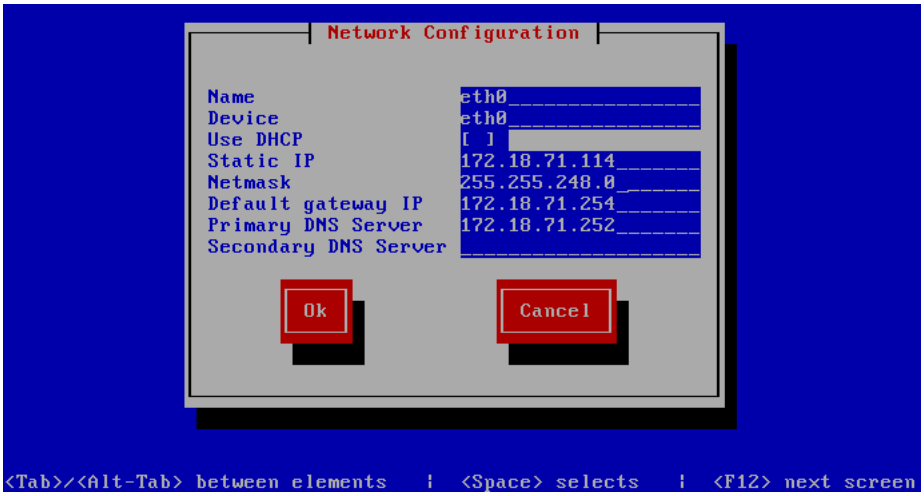


31 Click **Next**.

32 Complete the installation and reboot the server.



33 Log on to the server and verify that the Ethernet connection is operating correctly. You can use the ifconfig, ping, and ifup commands to check and start the connection. You can use the system-config-network-tui command to verify your network configuration details. If the connection does not work, refer to your Red Hat documentation for troubleshooting guidance. The following is an example of using the **system-config-network-tui** command:



--End--

Installing the required packages on the Linux server

Avaya Media Server (Avaya MS) requires specific 32–bit Linux packages to operate correctly. Check whether these packages are installed and install any that are missing. This procedure explains how to use the YUM package manager to check, install, and remove packages.

You must remove the mysql-libs package from the Avaya MS server.

Prerequisites

- Log on to the backup Linux server using the root account.

Procedure steps

Step	Action
1	Put the Red Hat Enterprise Linux DVD in the server DVD drive.
2	Change to the root user by running the following command: **`su –`**
3	Mount the Red Hat Enterprise Linux DVD by running the following commands: **`mkdir /mnt/cdrom`** **`mount /dev/cdrom /mnt/cdrom`**
4	Set up the YUM repository by copying the yum .repo file from the RHEL DVD, using the following commands: **`cp /mnt/cdrom/media.repo /etc/yum.repos.d/`**

5 Set up the YUM repository .repo file permissions. For example:

chmod +rw /etc/yum.repos.d/media.repo

6 Use the vi editor to open the YUM repository .repo file. For example, enter:

vi /etc/yum.repos.d/media.repo

7 Use the vi editor to add the following lines to the end of the YUM repository .repo file. This configures YUM to point to the mounted DVD image.

```
baseurl=file:///mnt/cdrom
enabled=1
```

8 For each Linux package required for Avaya MS, use the yum info command to check whether it is installed on the server. For example, the following command checks whether the libX11.i686 package is installed:

yum info libX11

For the list of required packages, see Procedure job aid (page 386).

9 If you find a required 32–bit Linux package is not present on the server, run the yum install command to install it. For example, the following command installs the libX11.i686 package:

yum install libX11.i686

10 If the libXdmcp Linux package is not present on the server, run the yum install command to install it. For example, the following command installs the libXdmcp.i686 package:

yum install libXdmcp.i686

11 Use the yum remove command to remove the mysql-libs package from the server:

yum remove mysql-libs

--End--

Procedure job aid

The following example shows the complete set of commands to mount the RHEL DVD, set up the YUM repository, check and install the libX11 and libXdmcp packages, and remove the mysql-libs package. Linux packages required for Avaya Media Server. Avaya Media Server requires 32–bit versions of the following RHEL 6.x packages:

```
su -
Password: *******
mkdir /mnt/cdrom
mount /dev/cdrom /mnt/cdrom
cp /mnt/cdrom/media.repo /etc/yum.repos.d/
chmod +rw /etc/yum.repos.d/media.repo
vi /etc/yum.repos.d/media.repo
      /* --- Add the following lines to the end of the file, save and
quit
      baseurl=file:///mnt/cdrom
      enabled=1 --- */
```

```
yum info libX11
yum install libX11.i686
yum info libXdmcp
yum install libXdmcp.i686
yum remove mysql-libs
```

When you run the yum info command, the Arch: heading of the output contains i686 if the installed package is the 32-bit version. The Repo: heading shows Installed if the package is already installed.

- **cyrus-sasl-lib**
- **e2fsprogs-libs**
- **glibc**
- **iproute**
- **keyutils-libs**
- **krb5-libs**
- **libICE**
- **libSM**
- **libX11**
- **libXau**
- **libXdmcp**
- **libXext**
- **libXt**
- **libgcc**
- **libidn**
- **libselinux**
- **libsepol**
- **libstdc++**
- **net-snmp-utils**
- **openldap**
- **zlib**

Adding a Linux user group and user

Create a Linux user group, create a Linux user and make the user a member of the user group.

For example, create a user group named amsgroup, and then create a user amsuser as a member of that group. You then use this account to access Avaya Media Server - Element Manager.

Procedure steps

Step	Action
1	Open a Linux terminal on the Linux server.
2	Change to root user by running the following command: **su -**
3	Use the Linux groupadd command to create a new group. For example, enter **groupadd amsgroup**.
4	Use the Linux useradd command to create a new user in the group you created. For example, enter **useradd amsuser -G amsgroup**.
5	Use the Linux passwd command to configure the password for the user. For example, enter **passwd amsuser**.

--End--

Preparing the Linux server for Avaya Media Server

Prepare the Linux server so you can install the Avaya Media Server software. Security Enhanced Linux (SELinux) enforces the access rules, which apply to the processes and files on a Linux server. To support Avaya Aura® Contact Center and Avaya Media Server, you must disable SELinux.

When a network address is added to a Linux server, the corresponding entries in the Linux /etc/hosts configuration file are not compatible with the Avaya Media Server PVI checker. You must edit the Linux hosts file to enable Avaya Media Server network communication. Remove hostname and Fully Qualified Domain Name (FQDN) references from the 127.0.0.1 localhost line in the hosts file.

Procedure steps

Step	Action
1	Open a Linux terminal on the Linux server.
2	Change to the root user account by running the following command: **su –**

3 Enter **sestatus**, to check the SELinux status. If the status is disabled then skip to step 8.

```
[root@AMSHOST2   ~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /selinux
Current mode:                   enforcing
Mode from config file:          enforcing
Policy version:                 24
Policy from config file:        targeted
[root@AMSHOST2   ~]# _
```

4 To disable SELInux, using the vi text editor, edit the /etc/selinux/config configuration file. For example, enter:

vi /etc/selinux/config

5 Change the SELINUX line to read **SELINUX=disabled**

```
[root@AMSHOST2   ~]# more /etc/selinux/config

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these two values:
#     targeted - Targeted processes are protected,
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted


[root@AMSHOST2   ~]# _
```

6 Reboot the server to apply the SELinux updates.

7 Open a Linux terminal on the Linux server.

8 Change to the root user account.

9 Using the vi text editor, edit the /etc/hosts configuration file. For example, enter:

vi /etc/hosts

10 Edit the hosts file to include the IP address and name of the primary and backup Avaya Media Servers.

```
[root@AMSHOST2 ~]# more /etc/hosts
127.0.0.1   localhost.localdomain localhost
172.18.71.113 AMSHOST1.siptraffic.com AMSHOST1
172.18.71.114 AMSHOST2.siptraffic.com AMSHOST2
[root@AMSHOST2 ~]# _
```

11 Save the hosts file and exit the editor.

--End--

Configuring Network Time Protocol

The High Availability primary and backup Avaya Media Servers must be synchronized in time. You use Network Time Protocol (NTP) to synchronize both servers with each other and with the contact center solution.

Procedure steps

Step	Action
1	Log on to the backup Avaya Media Server.
2	Edit the /etc/ntp.conf file to specify the NTP Server for both Avaya Media Servers. Edit the /etc/ntp.conf file to specify the NTP server. For example, add this line to the ntp.conf file: server <NTP IP Address> Where <NTP IP Address> is the IP address of your NTP server.
3	Open a Linux terminal on the Avaya Media Server.
4	Start the Network Time Protocol ntpd client service. This is done using the command: **service ntpd start**
5	Configure the Network Time Protocol ntpd client service to automatically start after a Linux server reboot. This is done using the command: **chkconfig ntpd on**
6	Verify that the Network Time Protocol client is working. This is done using the command: **ntpq -p**

--End--

Installing the Avaya Media Server software

Install the Avaya Media Server (Avaya MS) software to provide media processing for contacts in a SIP-enabled contact center environment.

Prerequisites

- Read the Contact Center Release Notes and the Avaya Media Server Release Notes for the most recent instructions.
- Log on to the Linux server.
- Obtain the Avaya Aura® Contact Center Release 6.3 DVD. The latest Avaya Aura® Contact Center 6.3 DVD may not contain the most recent version of the Avaya Media Server software. Read the Avaya Aura® Contact Center Release Notes to ensure that you are using the most recent version of Avaya Media Server software.

Procedure steps

Step	Action
1	Log on to the Linux server and change to the root user by running the following command: **`su -`**
2	Stop the Linux firewall using the following command: **`service iptables stop`**
3	Create a folder on the Avaya MS server by running the following command: **`mkdir /tmp/AvayaMS`**
4	Mount the Avaya Aura® Contact Center Release 6.3 DVD, for example type the following: **`mount /dev/cdrom /mnt/cdrom/`**
5	Copy the Avaya Media Server installation file to the temporary directory you created. For example: **`cp "/mnt/cdrom/Install Software/AMS/linux/ MediaServer_7.5.0.837_2012.09.12.bin" /tmp/AvayaMS`**
6	Copy the most recent version of the Contact Center Services for Avaya Media Server software to the temporary folder on the Linux server. For example, copy **`ContactCenterServicesForAMS_6.3.0.104`** to **`/tmp/AvayaMS`**.
7	Navigate to the directory where the files have been copied too. **`cd /tmp/AvayaMS`**
8	Grant executable permissions to the Avaya MS installation file. For example: **`chmod +x MediaServer_7.5.0.837_2012.09.12.bin`**
9	Start the Avaya MS installer by running the following command: **`./MediaServer_7.5.0.837_2012.09.12.bin`**
10	The installer displays the License Agreement. Press **Enter** to page through the license agreement.
11	To accept the license agreement and continue with the install, enter Y.

12 When prompted `Install Element Manager?`, enter `Y` to install the Element Manager.

13 When prompted for the `Linux group name`, press **Enter** to accept the default or specify the target **amsgroup** group. For example, select **amsgroup** so all members of this group can log on and use Avaya Media Server - Element Manager.

- Press Enter to accept the default.
- Specify an existing user group. Select an existing user group so members of that group can log on and use Avaya Media Server Element Manager. For example, select the **amsgroup** user group.

14 When prompted `Where would you like to install?`, press **Enter** to accept the default of `/opt/avaya`.

The installer displays the progress of the Avaya Media Server installation.

```
Some platform compatibility warnings have been detected.
The installation will be allowed to continue.

See /root/maspviresult.xml for detailed results.

Overall:  WARNING

Drives:   PASS
Hardware: PASS
Software: WARNING

PRESS <ENTER> TO ACCEPT THE FOLLOWING (Continue):



================================================================================
Installing...
-------------

 [==================|==================|==================|==================]
 [------------------|------------------|------------------|------------------]
```

15 Once the Avaya Media Server software installs, press **Enter** to exit the install.

16 Assign executable permissions to the Contact Center Services For Avaya Media Server installation file. For example,

`chmod +x ContactCenterServicesForAMS_6.3.0.104`

17 Start the Contact Center Services for Avaya Media Server installer by running the installation file. For example,

`./ContactCenterServicesForAMS_6.3.0.104`

The installer displays the progress of the Contact Center Services For Avaya Media Server installation.

18 When the Contact Center Services for Avaya Media Server installation completes, copy the Avaya MS firewall configuration file to the system using the following command:

```
cp /opt/avaya/iptables.AMS75 /etc/sysconfig/iptables
```

Overwrite the existing firewall, if prompted to do so.

19 Run the shell script to set up the Avaya MS environment using the following command:

```
. /etc/profile.d/masenv.sh
```

Note: the extra space before /etc is intentional.

20 Restart the Linux firewall using the following command:

```
service iptables start
```

21 Reboot the Linux server.

--End--

Installing the Avaya Media Server patches

Install a new Quick Fix Engineering (QFE) patch to apply a change to the Avaya Media Server system. You must lock Avaya Media Server before applying patches and unlock it after the patches are installed.

Quick Fix Engineering (QFE) patches are available for Avaya Media Server and Avaya Aura® Contact Center Service for Media (CCSM).

Prerequisites

- Download the most recent Avaya Media Server and Element Manager Quick Fix Engineering patches and store them in the QFE subdirectory on the Avaya Media Server server. QFE patches are ZIP files, do not un-zip QFE patches. The Avaya Media Server patching utility uses the QFE ZIP files. For a Linux server the default QFE folder location is /opt/avaya/ma/MAS/qfe.

Procedure steps

Step	Action
1	On a computer that can access the backup Avaya Media Server, start a Web browser.
2	In the address box, enter https://<AMS_SERVER_IP_ADDRESS>:8443/em. To access the backup Avaya Media Server Element Manager (EM), enter https://172.18.71.114:8443/em
3	In the **User ID** box, type amsuser.
4	In the **Password** box, type the amsuser password.
5	Click **Log In**.
6	In the navigation pane, click **System Status**, **Element Status**.

7 From the **More Actions** list, select **Pending Lock** to lock the Avaya Media Server after all processes finish.

8 Click **Confirm** to change the Element Status.

9 Close Avaya Media Server Element Manager.

10 Open a Linux terminal on the Linux server.

11 Change to the root user by running the following command:

```
su -
```

12 Copy the Linux QFE files to the /opt/avaya/ma/MAS/qfe folder.
For example use:

```
cp QFE-* /opt/avaya/ma/MAS/qfe
```

13 Obtain the correct name of the new QFE patch by entering the following command:

```
maspatch list all
```

The name of the file is not necessarily the same as the name of the patch name.

14 Install all of the patches in numerical order. To install all new patches on the system, enter the following command:

```
maspatch apply all
```

15 When the patch application is complete, open the Element Manager navigation pane, and select **Tools**, **Software Inventory**.

16 Verify the patch version listed in the **Patch Level** column is correct.

17 In the Element Manager navigation pane, click **System Status**, **Element Status**.

18 From the **More Actions** list, select **Unlock** to unlock the Avaya Media Server.

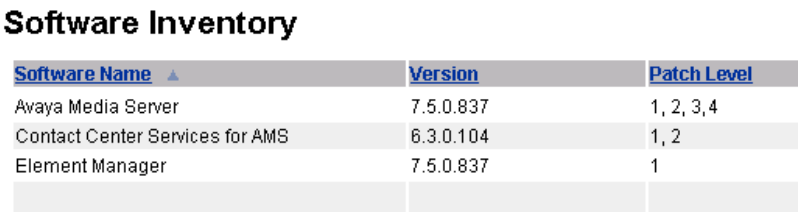
19 Click **Confirm** to change the Element Status.

--End--

Procedure job aid

Avaya Media Server - Element Manager Software Inventory showing the patches.

Example of Avaya Media Server Software Inventory



Software Inventory

Software Name	Version	Patch Level
Avaya Media Server	7.5.0.837	1, 2, 3, 4
Contact Center Services for AMS	6.3.0.104	1, 2
Element Manager	7.5.0.837	1

Securing your Avaya Media Server

Apply optional security measures to your operating system to further secure your server.

Scanning software can degrade the performance and decrease the reliability of the system. Install virus scanning software only if the system connects to an exposed network or to the Internet.

To maintain server performance, you must schedule virus scans during maintenance periods or low usage hours only.

Procedure steps

Step	Action
1	Harden the operating system using defined site procedures.
2	Install antivirus software. If you install antivirus software, ensure that you exclude the following directories from the scans. The following are the default install locations. If you installed Avaya Media Server in a different location, navigate to the necessary directories and exclude them from antivirus scans. • /opt/avaya/ma/MAS/platdata • /opt/avaya/ma/MAS/common/log

--End--

Avaya Media Server – High Availability commissioning

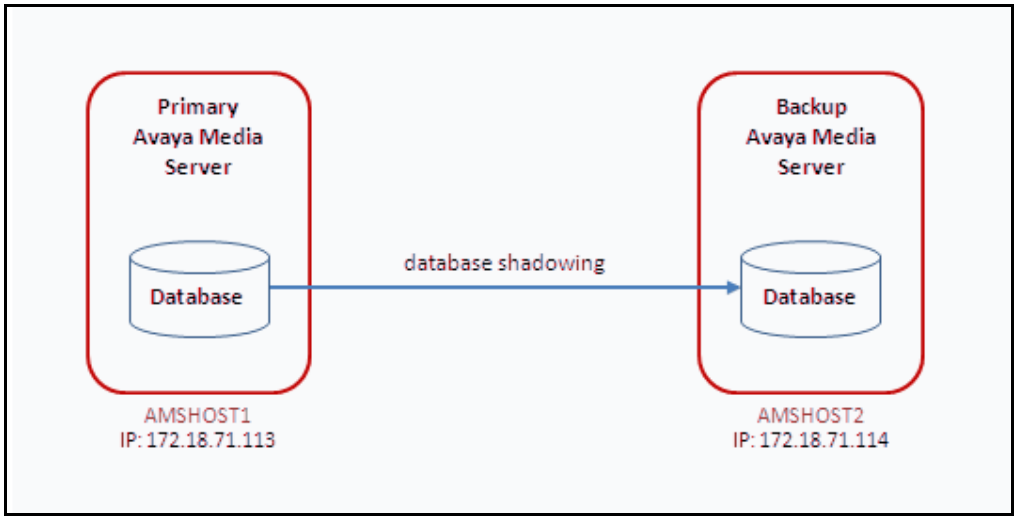
The Avaya Media Server High Availability feature uses two media servers operating in a stand-by deployment. Both the servers have identical configuration and provide full media processing capabilities.

Example server details	Value
Primary server name	AMSHOST1
Primary server IP Address	172.18.71.113
Backup server name	AMSHOST2
Backup server IP Address	172.18.71.114
Managed name	AMSMANHOST
Managed (Service) IP Address	172.18.71.115

You configure the High Availability feature by designating one Avaya Media Server as the primary server and the other Avaya Media Server as the backup server. Both servers communicate with each other using a heartbeat mechanism. The Backup Avaya Media Server shadows the Primary Avaya Media Server.

The High Availability primary and backup Avaya Media Servers must be synchronized in time. You use Network Time Protocol (NTP) to synchronize both servers with each other and with the contact center solution.

Example of Avaya Media Server database shadowing



Resolving the Managed name to the Service IP Address

Complete the following procedure for the Primary and Backup Avaya Media Server servers to resolve the Managed server name to the Service IP address.

Attention: Avaya Aura® Contact Center High Availability solutions do not support Windows Server 2008 Dynamic DNS.

Ask your Domain Administrator to add a Domain Name System (DNS) static entry for the Primary and Backup servers and one additional DNS static entry for each Managed name and associated Service (Managed) IP address.

A typical High Availability campus solution with a pair of Avaya Media Servers requires three DNS static entries; one DNS static entry for the primary server, one DNS static entry for the backup server, and one DNS static entry for the Managed name and associated service IP address.

Perform this procedure for both the Primary and Backup servers.

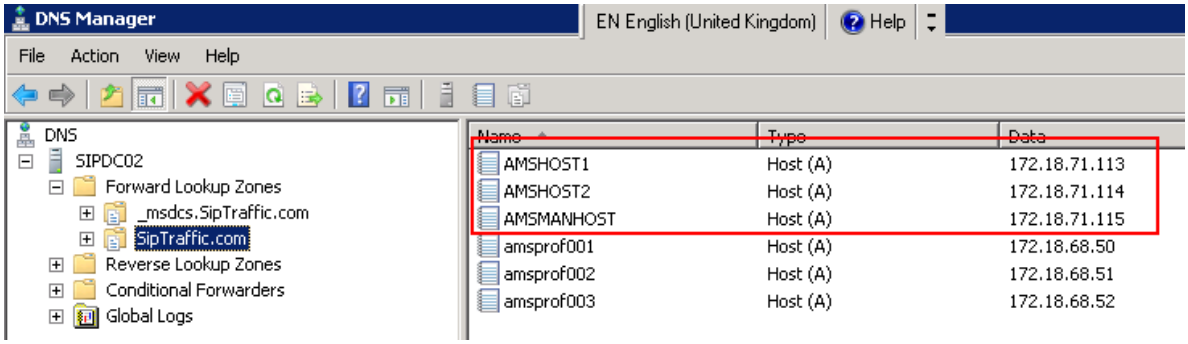
Procedure steps

Step	Action
1	Ask your Domain Administrator to add a Domain Name System (DNS) static entry for the Primary and Backup Avaya Media Servers and one additional DNS static entry for each Managed name and associated Managed IP address.

--End--

Procedure job aid

The following DNS window shows the three static entries in the siptraffic.com domain. The primary server - hostname AMSHOST1 with an IP address 172.18.71.113. The backup (secondary) server - hostname AMSHOST2 with an IP address 172.18.71.114. And the Managed name and Managed IP - AMSMANHOST and 172.18.71.115.



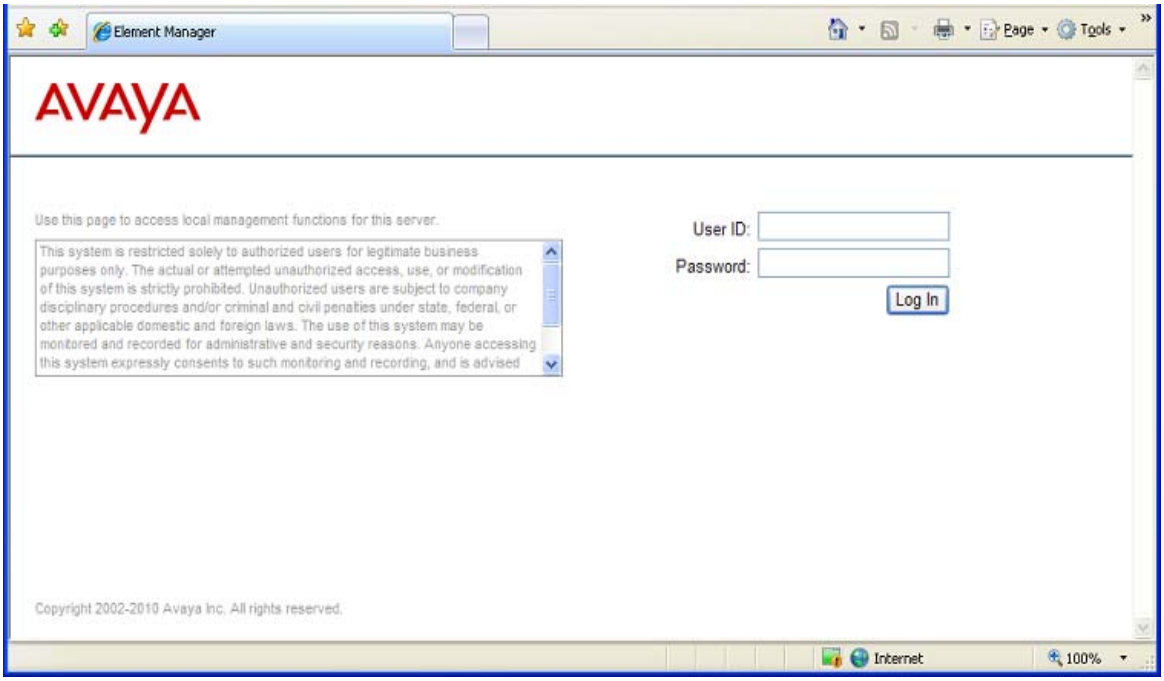
Logging on to Avaya Media Server Element Manager

Element Manager (EM) is a Web-based administration tool that facilitates the Operation, Administration, and Maintenance (OAM) of Avaya Media Server.

In Avaya Media Server – High Availability solutions, you must use the primary Avaya Media Server – Element Manager to perform normal configuration operations. Use the backup Avaya Media Server (AMS) – Element Manager only to perform High Availability configuration.

Procedure steps

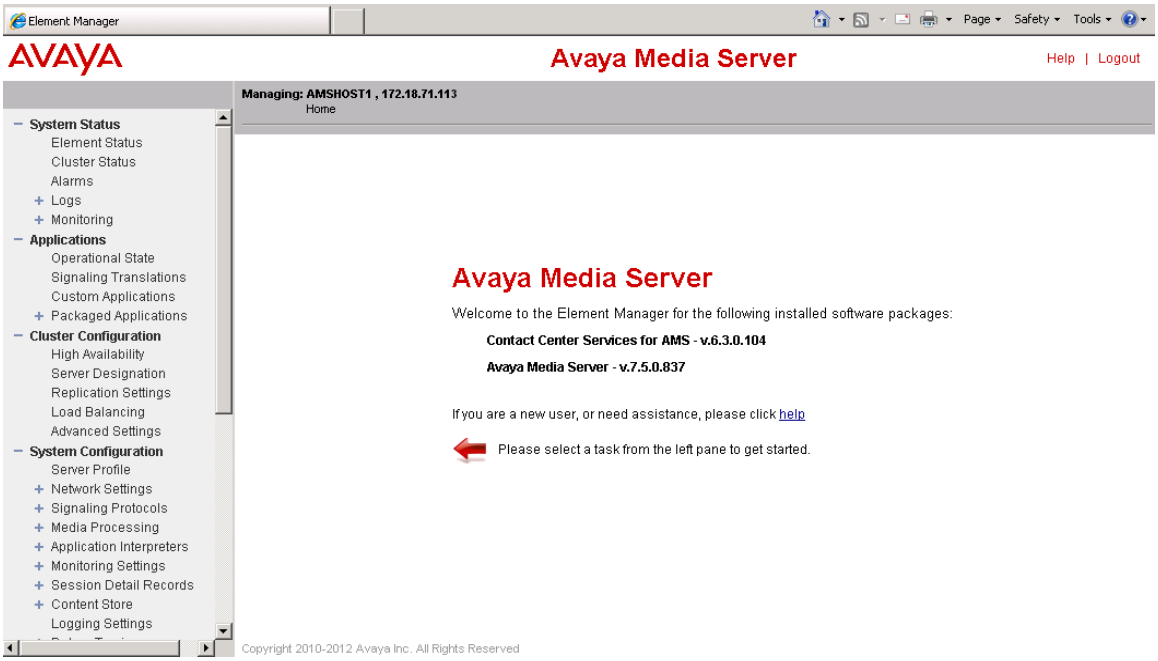
Step	Action
1	Start a Web browser.
2	In the address box, enter https://<AMS_SERVER_IP_ADDRESS>:8443/em. To access the primary Avaya Media Server EM enter https://172.18.71.113:8443/em To access the backup Avaya Media Server EM enter https://172.18.71.114:8443/em



3 In the **User ID** box, type amsuser.

4 In the **Password** box, type the amsuser password.

5 Click **Log In**.



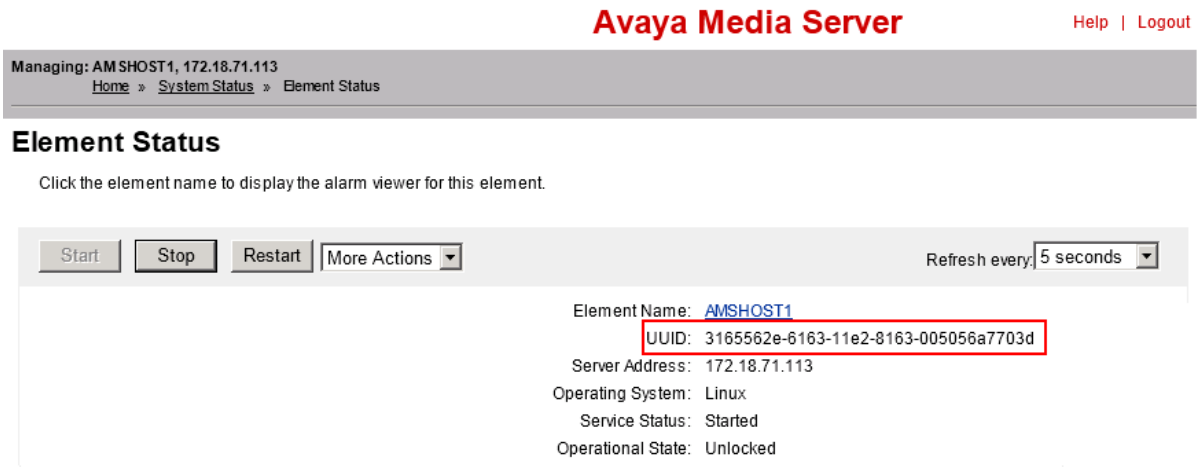
--End--

Obtaining the Universally Unique Identifier

Perform this procedure to obtain the Universally Unique Identifier (UUID) of the primary Avaya Media Server. You need to enter the primary server UUID when you configure the backup server in the high availability pair.

Procedure steps

Step	Action
1	Log on to the Element Manager for the primary Avaya Media Server. For example log on to: https://172.18.71.113:8443/em
2	In the navigation pane, click **System Status**.
3	Click **Element Status**.



4	Record the UUID from the Element Status page. Copy the UUID into your Windows clipboard.

--End--

Configuring the High Availability primary Avaya Media Server

Designate the primary Avaya Media Server as a primary, and create a replication username and password for the high availability pair.

Procedure steps

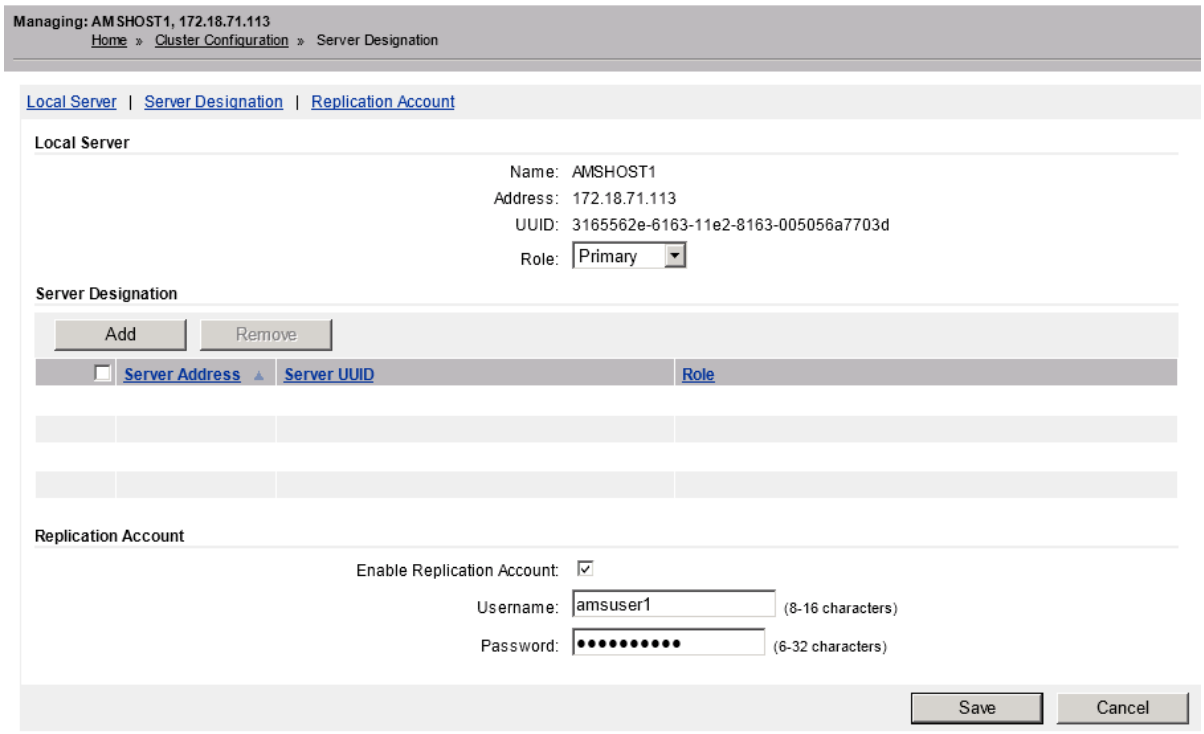
Step	Action
1	Log on to the Element Manager for the primary Avaya Media Server. For example log on to: https://172.18.71.113:8443/em
2	In the navigation pane, click **Cluster Configuration**.
3	Click **Server Designation**.
4	Under **Local Servers**, from the **Role** list, select **Primary**.
5	Under **Replication Account**, select the **Enable Replication Account** check box.
6	In the **Username** box, type a username for the replication account. This value is arbitrary, but you must use the same value on the backup server. For example type amsuser1.
7	In the **Password** box, type a password for the replication account. This value is arbitrary, but you must use the same value on the backup server. For example amsuser1.
8	Click **Save**.
9	Click **Confirm**.

--End--

Procedure job aid

Configure the primary Avaya Media Server to create a replication account for the High Availability pair.

Example of designating an Avaya Media Server as a primary server



Configuring the High Availability backup Avaya Media Server

Designate the backup server of the High Availability pair, configure it with the primary server UUID and IP address, and enter the replication account details.

Procedure steps

Step	Action
1	Log on to the Element Manager for the backup Avaya Media Server. For example log on to: https://172.18.71.114:8443/em
2	Access the Element Manager for the backup Avaya Media Server.
3	In the navigation pane, click **Cluster Configuration**.
4	Select **Server Designation**.
5	Under **Local Servers**, from the **Role** list, select **Backup**.
6	Under **Server Designation**, type the UUID of the Primary server in the **Primary Server UUID** box or paste the UUID data stored in your Windows clipboard earlier.

7 In the **Primary Server Address** box, type the primary server IP address. For example type 172.18.71.113.

8 Under **Replication Account**, select the **Enable Replication Account** check box.

9 In the **Username** box, type the username for the replication account that you specified on the primary server. For example type amsuser1, to match the account name entered when configuring High Availability on the primary server.

10 In the **Password** box, type the password for the replication account that you specified on the primary server. For example type amsuser1.

11 Click **Save**.

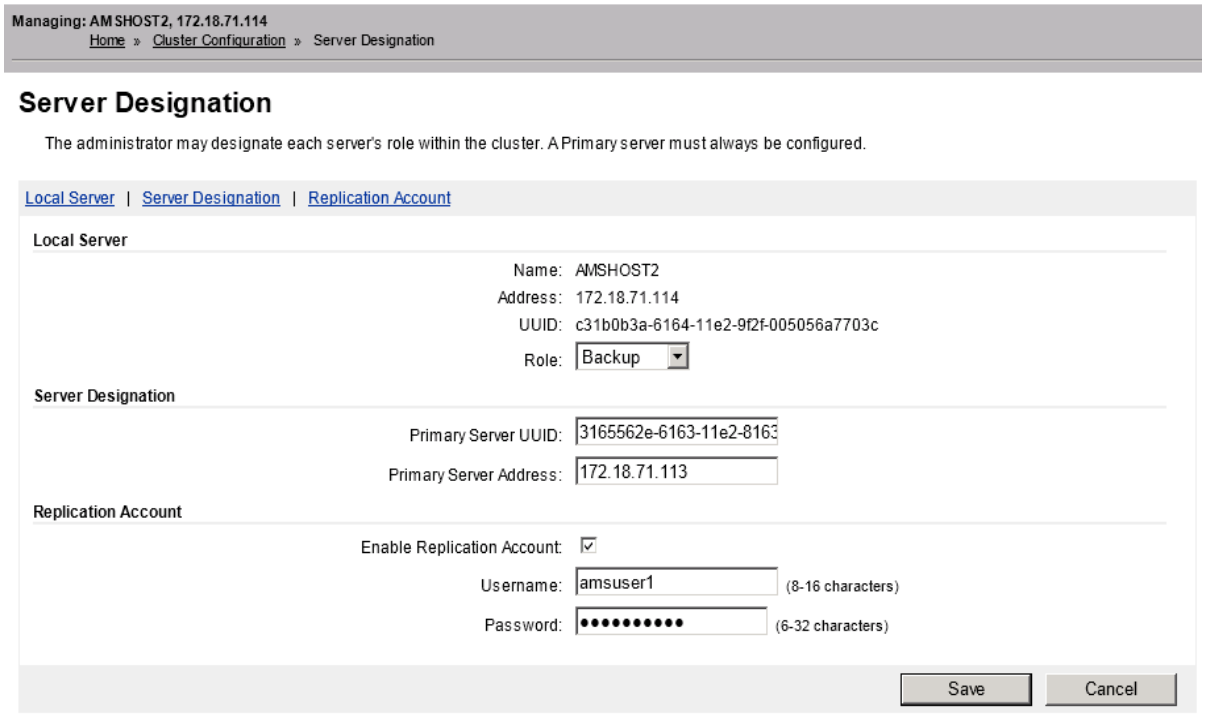
12 Click **Confirm**.

--End--

Procedure job aid

Configure the backup Avaya Media Server to enter the primary server UUID and IP address, and the replication account for the High Availability pair.

Example of designating an Avaya Media Server as a backup server



Enabling High Availability on the backup server

Configure the backup server to start replicating from the primary server for High Availability.

Procedure steps

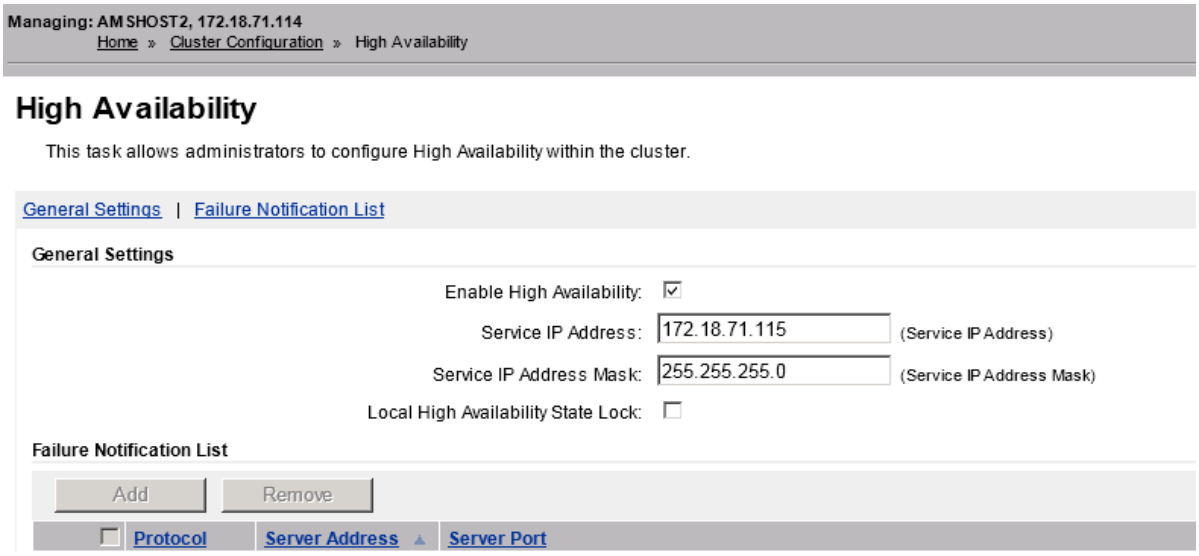
Step	Action
1	Log on to the Element Manager for the backup Avaya Media Server. For example log on to: https://172.18.71.114:8443/em
2	In the navigation pane, click **Cluster Configuration**.
3	Click **High Availability**.
4	Under **General Settings**, select the **Enable High Availability** check box.
5	In the **Service IP Address** box, type the managed IP address for this High Availability pair. For example type 172.18.71.115.
6	In the **Service IP Address Mask** box, type the Subnet mask for the managed IP address. For example type 255.255.255.0.
7	Ensure **Local High Availability State Lock** is not selected.
8	Click **Save**.
9	Click **Confirm**.

--End--

Procedure job aid

Enable High Availability on an Avaya Media Server backup server to complete creating a High Availability pair.

Example of Avaya Media Server High Availability backup server



Completing High Availability pair configuration

Perform the following procedure on the primary server to complete the High Availability server pairing.

Procedure steps

Step	Action
1	Access the Element Manager for the primary Avaya Media Server. In the Web browser address box, enter https://172.18.71.113:8443/em
2	Log on to Element Manager.
3	In the navigation pane, click **Cluster Configuration**.
4	Click **Server Designation**.
5	Ensure the **Local Server Role** is set to **Primary**.
6	Ensure one server is shown under **Server Designation** and the server has **the** Role of **Backup**.
7	Ensure **Enable Replication Account** is selected.
8	If the backup server is not listed in the **Server Designation** section, then click **Add**.
9	In the **Server Address** box, type the IP address of the backup server. For example, type 172.18.71.114.

10 In the **Server UUID** box, type the UUID of the backup server.

11 Under **Role**, select **Backup**.

12 Click **Save**.

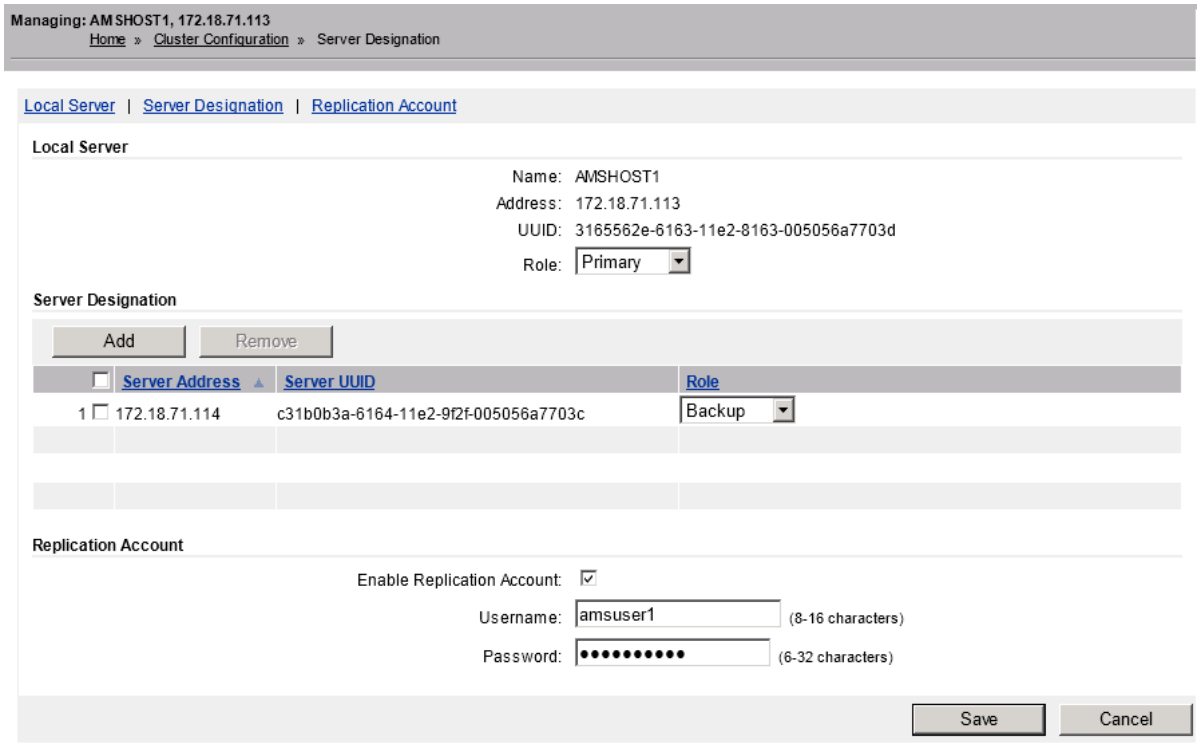
13 Click **Confirm**.

--End--

Procedure job aid

Configure an Avaya Media Server primary server to start creating a High Availability pair.

Example of configuring Avaya Media Server High Availability on the primary server



Enabling High Availability on the primary Avaya Media Server

Enable High Availability on the primary Avaya Media Server.

Procedure steps

Step	Action
1	Select one Avaya Media Server as the primary server. For example, choose 172.18.71.113 as the primary Avaya Media Server.

2 Access the Element Manager for the primary Avaya Media Server. In the Web browser address box, enter

https://172.18.71.113:8443/em

3 Log on to Element Manager.

4 In the navigation pane, click **Cluster Configuration**.

5 Click **High Availability**.

6 Under **General Settings**, select the **Enable High Availability** check box.

7 In the **Service IP Address** box, type the managed IP address for this High Availability pair, for example type 172.18.71.115.

8 In the **Service IP Address Mask** box, type the subnet mask for the managed IP address. For example type 255.255.255.0.

9 Under the **Failure Notification List**, click **Add** to add the Contact Center Manager Server managed IP address.

Avaya MS sends a notification to Contact Center Manager Server if a failover occurs.

10 In the **Server Address** box, type the managed IP address of the Voice and Multimedia Contact Server. For example, type 172.18.71.112.

11 In the **Server Port** box, type 57012. This Avaya Media Server - Failure Notification List - Server Port number must match the Contact Center Manager Server High Availability utility - Local SMMC Port number.

12 Click **Save**.

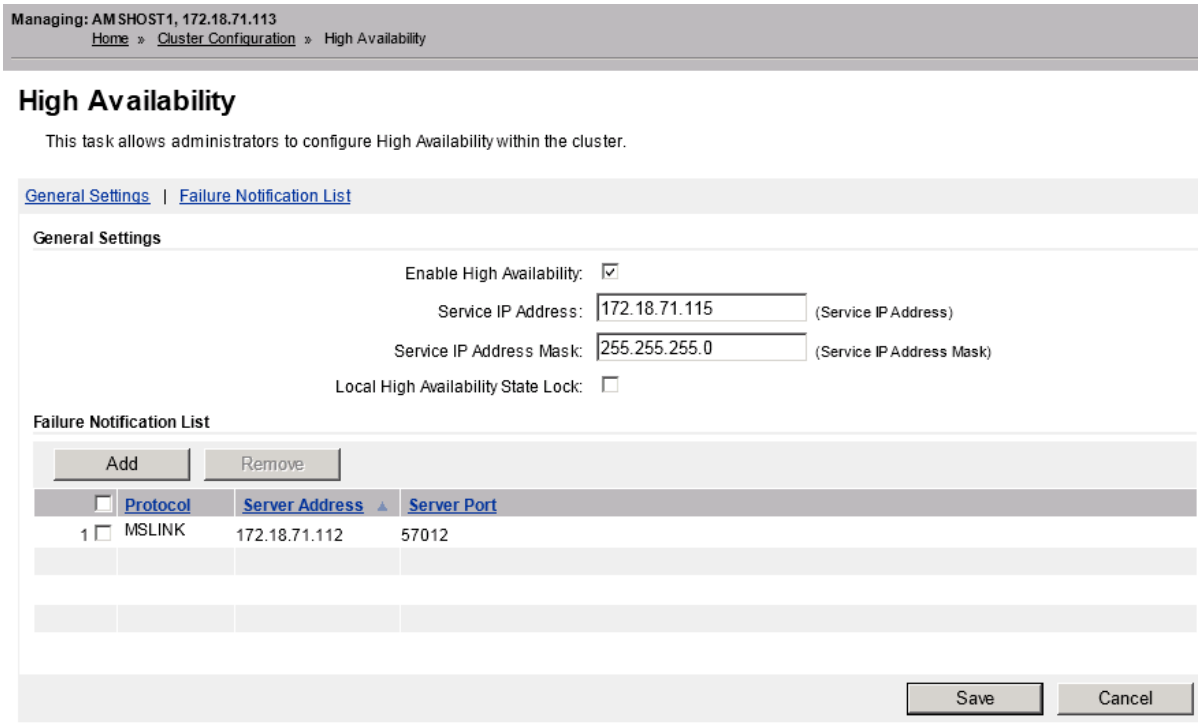
13 Click **Confirm**.

--End--

Procedure job aid

Configure an Avaya Media Server primary server to start creating a High Availability pair.

Example of configuring Avaya Media Server High Availability on the primary server



Restarting the primary and backup servers

Restart both servers so that the backup server can begin replicating from the primary server. Ensure that the primary server is fully operational before starting the backup server.

Procedure steps

Step	Action
1	Shut down the backup server.
2	Perform an operating system restart on the primary server. For example, open a Linux terminal and enter **Reboot**.
3	When the primary server is fully operational, start the backup server.

--End--

Reviewing High Availability configuration and status

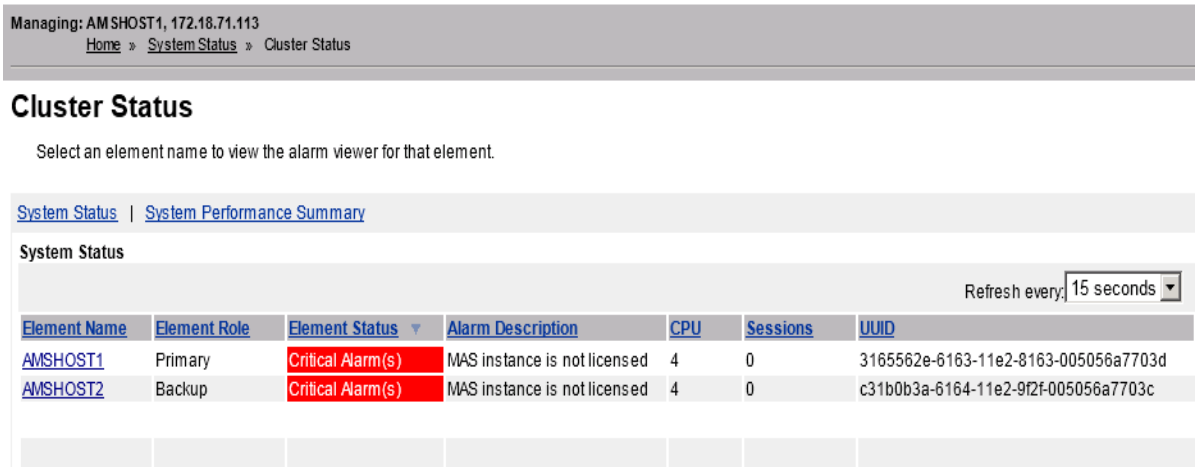
Perform the following steps to ensure High Availability is fully configured.

At this stage in the configuration, the primary and backup Avaya Media Server servers are not yet licensed. If there are license related issues in the alarms list, you can ignore these at this stage of the configuration.

You can configure an un-licensed Avaya Media Server, but it cannot process contacts until a valid license is applied. Avaya Media Server license details are configured later in Contact Center Manager Administration during Media Server configuration.

Procedure steps

Step	Action
1	In the primary Avaya Media Server Element Manager navigation pane, click **System Status**.
2	Click **Cluster Status**.
3	Ensure only two nodes are listed.
4	Ensure one **Element Role** is listed for both the primary and backup server.
5	Ensure no alarms are listed, with the exception of those related to licensing, in the **Alarm Description** column.



6	In the backup Avaya Media Server Element Manager navigation pane, click **System Status**.
7	Click **Cluster Status**.
8	Ensure only two nodes are listed.
9	Ensure one **Element Role** is listed for both the primary and backup server.
10	Ensure no alarms are listed, with the exception of those related to licensing, in the **Alarm Description** column.

--End--

Avaya Media Server – Commissioning

This chapter describes the commissioning procedures for setting up trust relationships and media on the primary Avaya Media Server (Avaya MS).

Configuring media on the Avaya Media Server

Avaya MS provides default media for standard ringback and busy tones.

Administrators provision additional media such as recorded announcements (RAN) and music for Avaya MS to provide meaningful treatments to the customer.

Media file formats

Avaya MS provides optimum playback performance with .WAV files transcoded as Linear 16-bit PCM, 8KHz Mono with a sampling rate of 128kbits/sec. Create your announcement and music media files with this transcoding before copying them onto the Avaya MS server.

Media organization

In Avaya MS Element Manager (EM), you organize media within a content namespace. The content namespace name must match the contact center SIP domain name; that is, the Local SIP Subscriber Domain Name in Contact Center Manager Server–Server Configuration.

Within the content namespace, you use content groups to subdivide the media into logical groups. You must create one locale-specific content group. The locale-specific content group must match the Local SIP Subscriber MS Locale in Contact Center Manager Server (CCMS) Server Configuration utility.

You can create one or more additional content groups for music. Typically you store different types of music media in different content groups.

To use treatments in Orchestration Designer (OD) flow applications or scripts, you create routes in Contact Center Manager Administration (CCMA) that link to the media files in the Avaya MS locale-specific content group. To use scripted music in OD flow applications or scripts, you create routes in Contact Center Manager Administration (CCMA) that link to the Avaya MS content groups containing the music files. The OD flow applications or scripts reference these routes to access the treatment files and scripted music on the Avaya MS server.

The SIP domain for the example contact center is siptraffic.com. The locale configured on the CCMS server is en_us.

The media content namespace structure is as follows:

```
siptraffic.com      <= media content namespace, matches SIP domain
      | en_us       <= locale-specific media content group (announcements)
      | folk        <= media content group (folk music)
      | jazz        <= media content group (jazz music)
      | rock        <= media content group (rock music)
```

The locale-specific content group matches the locale configured on the Avaya Aura® Contact Center Manager Server server.

Confirming the Contact Center packaged application locale

Confirm the locale configuration of the core Contact Center Services Packaged Applications to ensure the contact center receives the correct tones and announcements.

Procedure steps

Step	Action
1	Log on to Element Manager of the primary Avaya Media Server. For example, to access the Element Manager of the primary Avaya Media Server, enter https://172.18.71.113:8443/em in a Web browser.
2	In the navigation pane, click **Applications**, **Packaged Applications**, **Contact Center**.
3	On the **General Settings** page, confirm that the **Default Locale** is **en_us**.

--End--

Adding the Contact Center Manager Server as a trusted node

Add the active and standby Contact Center Manager Server servers as trusted nodes to allow Avaya Aura® Contact Center to use the Avaya Media Server services.

You must also add the Managed IP address of the Contact Center Manager Server (CCMS) HA pair to the list of trusted nodes.

Procedure steps

Step	Action
1	In the navigation pane, click **System Configuration**, **Signaling Protocols**, **SIP**.

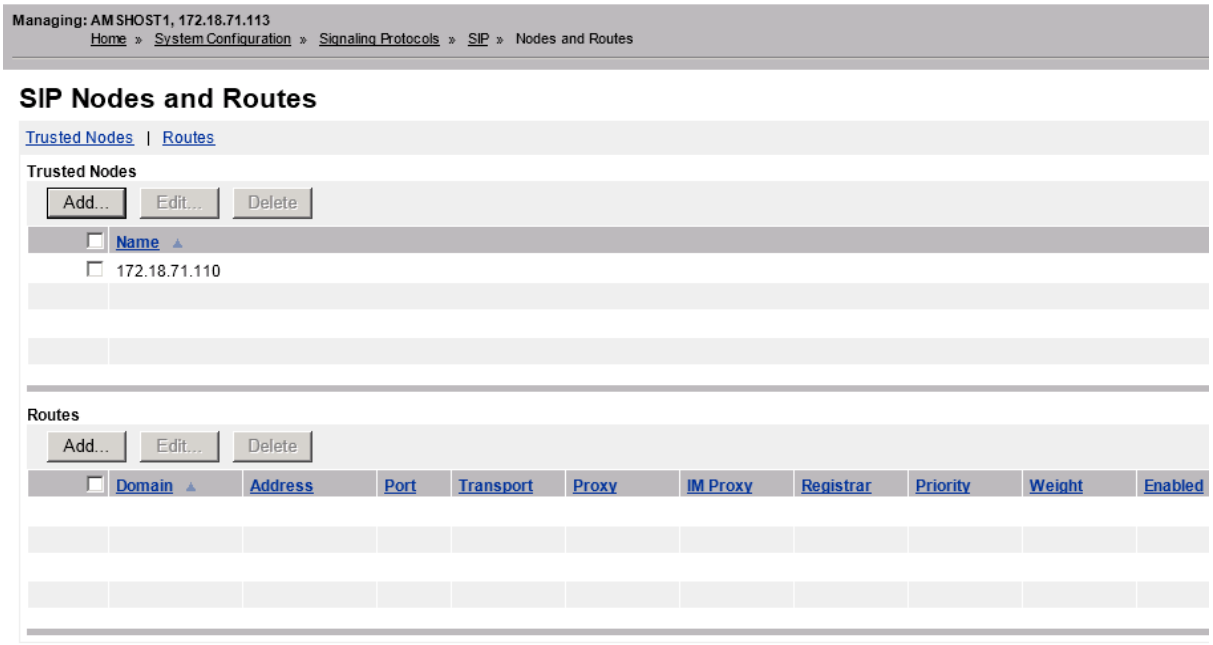
2 Click **Nodes and Routes**.

3 Click the **Trusted Nodes** link.

4 Click **Add**.

5 On the **Add SIP Trusted Node** page, in the **Host or Server Address** box, type the name or IP address of the active Voice and Multimedia Contact Server. For example, type 172.18.71.110.

6 Click **Save**.



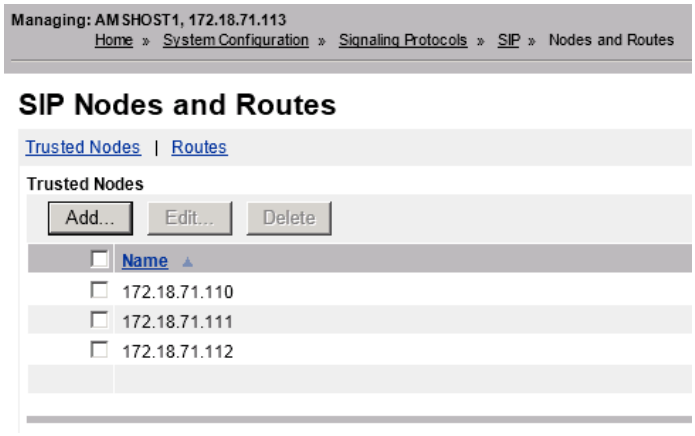
7 Click **Add**.

8 On the **Add SIP Trusted Node** page, in the **Host or Server Address** box, type the name or IP address of the standby Voice and Multimedia Contact Server. For example, type 172.18.71.111.

9 Click **Save**.

10 Click **Add**.

11 On the **Add SIP Trusted Node** page, in the **Host or Server Address** box, type the Managed IP address of the Voice and Multimedia Contact Server High Availability server pair. For example, type 172.18.71.112.



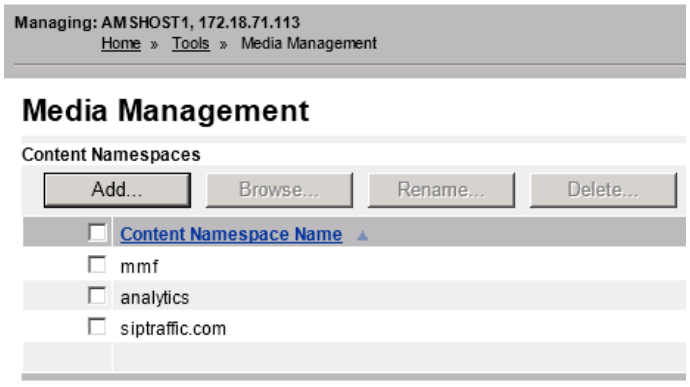
--End--

Adding the media content namespace

Create the content namespace to organize the media treatments for the contact center.

Procedure steps

Step	Action
1	In the navigation pane, click **Tools**, **Media Management**.
2	On the **Media Management** page, under **Content Namespaces**, click **Add**.
3	In the **Name** box, type **siptraffic.com**.
4	Click **Save**.



--End--

Adding the locale-specific media content group

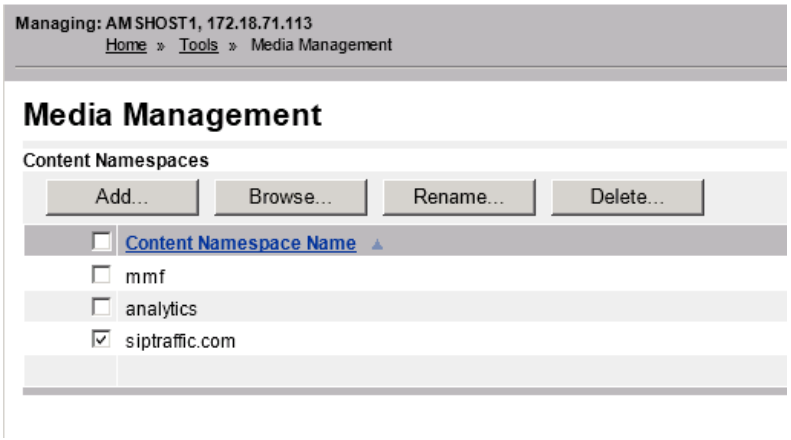
Create the locale specific content group required to store media for announcements.

Prerequisites

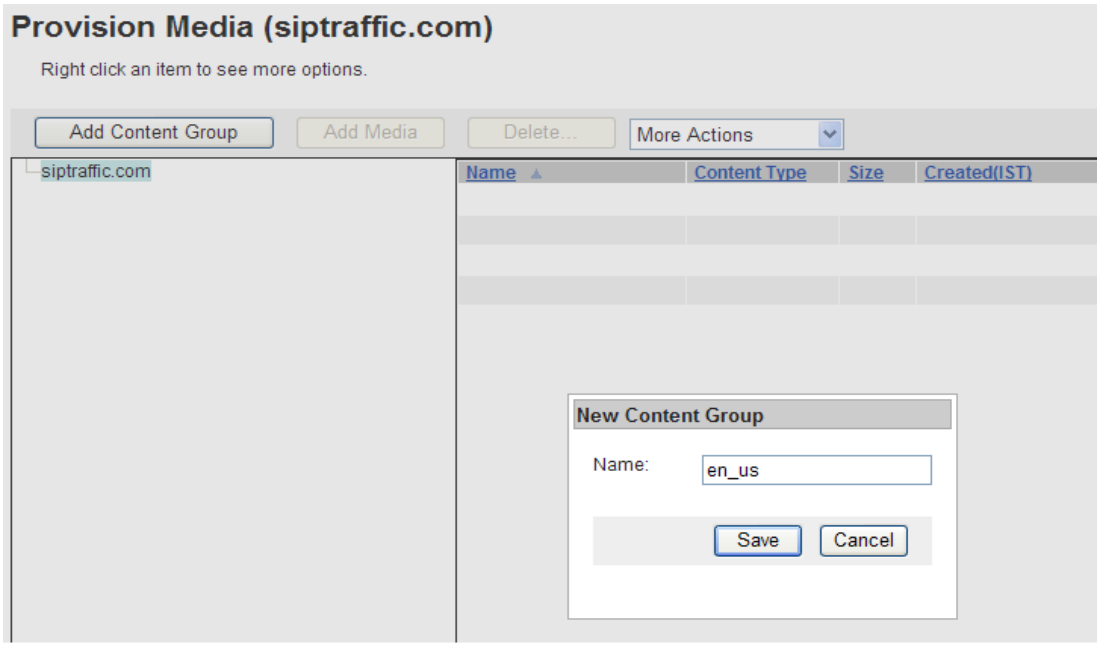
- Create the media content namespace. For more information about adding content namespaces, see Adding the media content namespace (page 416).

Procedure steps

Step	Action
1	In the navigation pane, click **Tools**, **Media Management**.
2	On the **Media Management** page, under **Content Namespaces**, select the content namespace, for example select **siptraffic.com**.



3	Click **Browse**. *Avaya MS displays the Provision Media page.*
4	On the **Provision Media** page, in the left pane, select the content namespace, siptraffic.com.
5	Click **Add Content Group**. *Avaya MS displays the New Content Group page.*
6	In the **New Content Group** dialog box, in the **Name** box, type **en_us**.



7 Click **Save**.

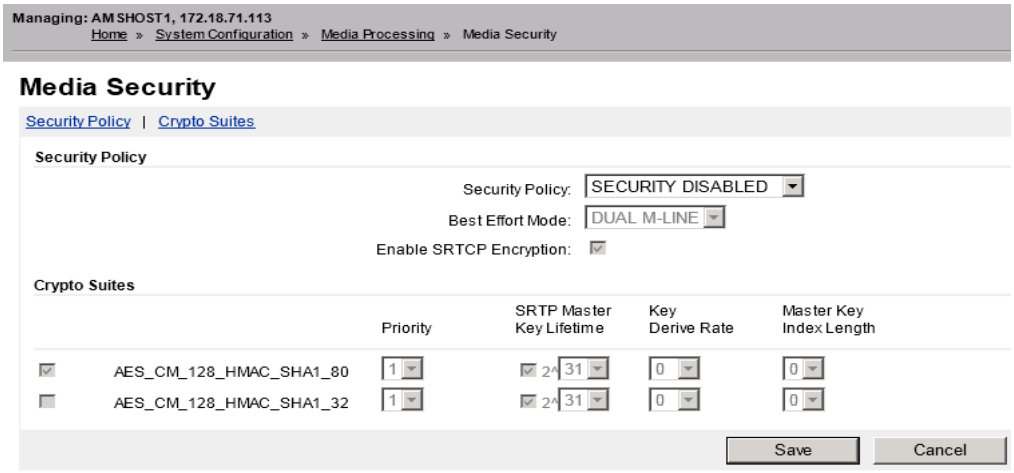
--End--

Configuring Avaya Media Server settings for SIP-enabled contact center

Configure the Avaya Media Server settings to ensure Avaya Media Server can provide the optimal service for the Contact Center application.

Procedure steps

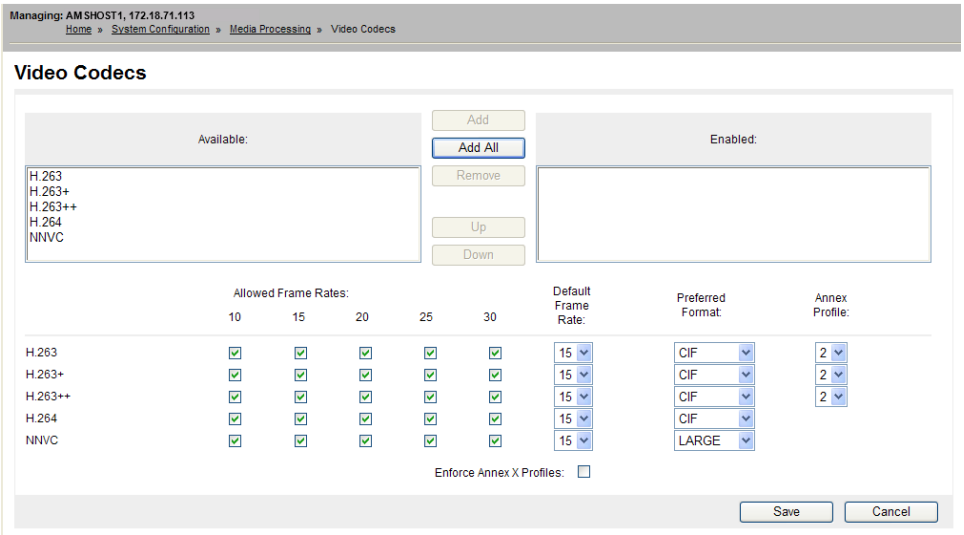
Step	Action
1	Log on to Element Manager.
2	In the navigation pane, click **System Configuration**, **Media Processing**, **Media Security**.
3	On the **Media Security** page, from the **Security Policy** list, select **Security Disabled**.



4 Click **Save**.

5 In the navigation pane, click **System Configuration**, **Media Processing**, **Video Codecs**.

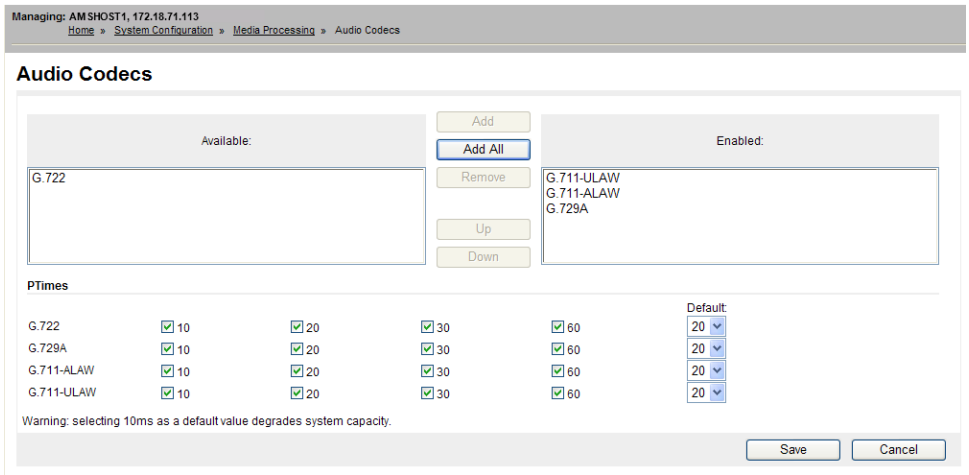
6 On the **Video Codecs** page, remove all codecs. From the **Enabled** list, select each video codec and click **Remove**.



7 Click **Save**.

8 In the navigation pane, click **System Configuration**, **Media Processing**, **Audio Codecs**.

9 On the **Audio Codecs** page, ensure that the codecs you want to support appear in the **Enabled** list.

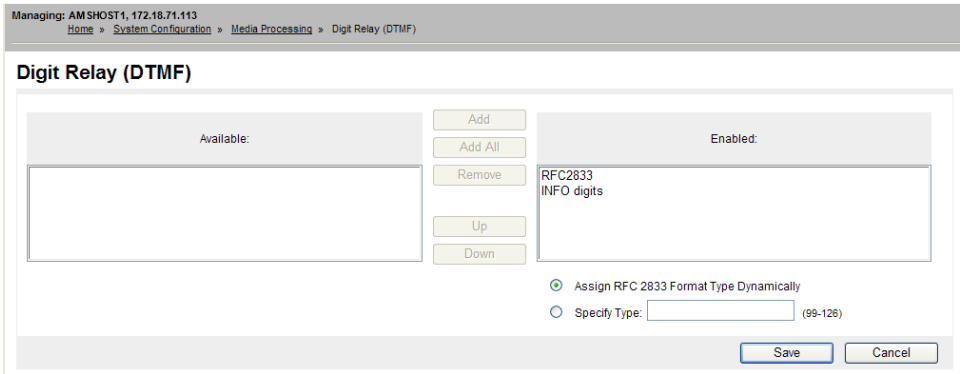


10 Click **Save**.

11 In the navigation pane, click **System Configuration**, **Media Processing**, **Digit Relay (DTMF)**.

12 On the **Digit Relay (DTMF)** page, enable **RFC2833**.

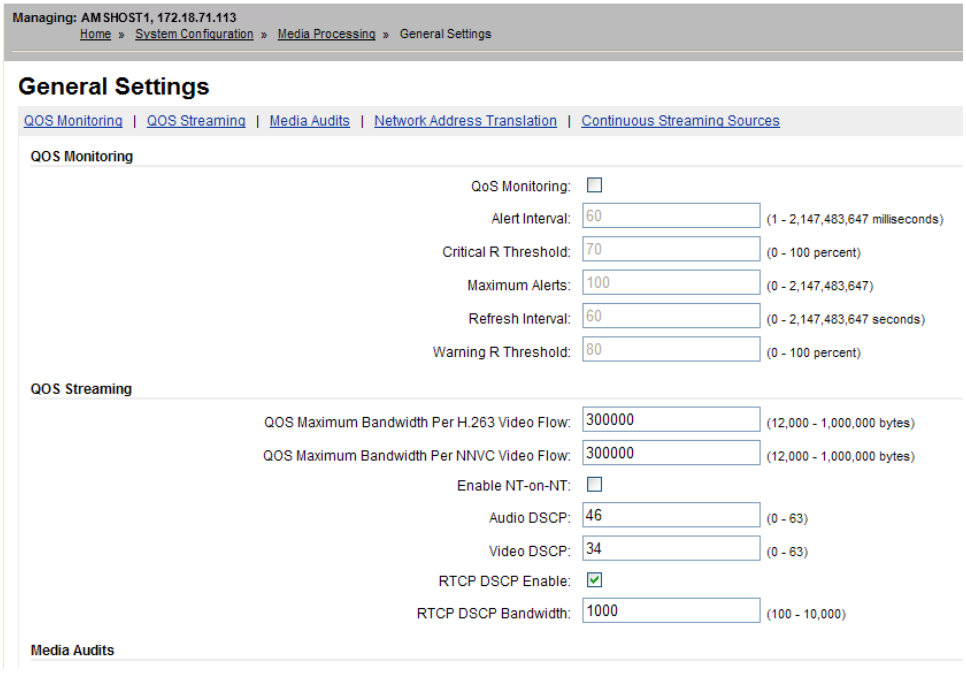
13 On the **Digit Relay (DTMF)** page, enable **INFO digits**. You must enable INFO digits after enabling RFC2833; RFC2833 must appear first on the list. To move RFC2833 to the top of the list, select **RFC2833**, and click **Up**.



14 Click **Save**.

15 In the navigation pane, click **System Configuration**, **Media Processing**, **General Settings**.

16 On the **General Settings** page, clear the **QoS Monitoring** check box.



17 Click **Save**.

--End--

Restoring the Locale Specific Media Files on Linux

Restore the Avaya Media Server locale-specific media files that you backed up earlier. You must restore the media files to both Avaya MS servers.

If you did not choose the default Avaya MS installation path, you can use a Linux environment variable to locate the correct directory for the locale specific directories. For example on a Linux Avaya MS, the location of the US English files is `$MASHOME/platdata/Announcements/contactcenter/default/us/en/l16`.

Attention: If you use more than one language in your Contact Center prompts and recorded announcements, you must restore each language separately.

Procedure steps

Step	Action
1	Open a Linux terminal on the primary Linux server.
2	Use the su command to change to the root user account. For example,

```
su -
```

3. Create a temporary directory to which you can download the media files you backed up from the Windows server. For example,

   ```
   mkdir /tmp/localemedia
   ```

4. Navigate to the location for the default locale-specific media files for your system. For example,

   ```
   cd /opt/avaya/ma/MAS/platdata/Announcements/
   contactcenter/default/xx/yy/l16
   ```

   where xx is the country portion of the locale and yy is the language portion of the locale.

5. Copy the .ZIP file of the locale-specific media you backed up from the Windows server. For example

   ```
   cp /tmp/localemedia/l16_backup.zip
   ```

   to /opt/avaya/ma/MAS/platdata/Announcements/contactcenter/default/xx/yy/l16.

6. Unzip the file to the current locale-specific directory. Overwrite the default files with the files you are copying, if the files contained in the backed up folder are what you require.

7. Repeat these steps for each locale and language from which you backed up media files.

8. Repeat these steps on the backup Avaya MS server.

--End--

Uploading a batch zip file

You can upload a batch file to provision multiple media files on the Avaya Media Server in a single step. This can include all the media to provide call treatments such as announcements or music.

You can provision the media in a content namespace by using one ZIP file for the whole content namespace or by creating one content group at a time. After you upload the media file, Element Manager (EM) displays it in a tree view. The root of the tree is the content namespace and individual content groups appear below it. EM displays the content namespace and the content groups in the left pane, and the media files contained in the selected content group in the right pane.

Prerequisites

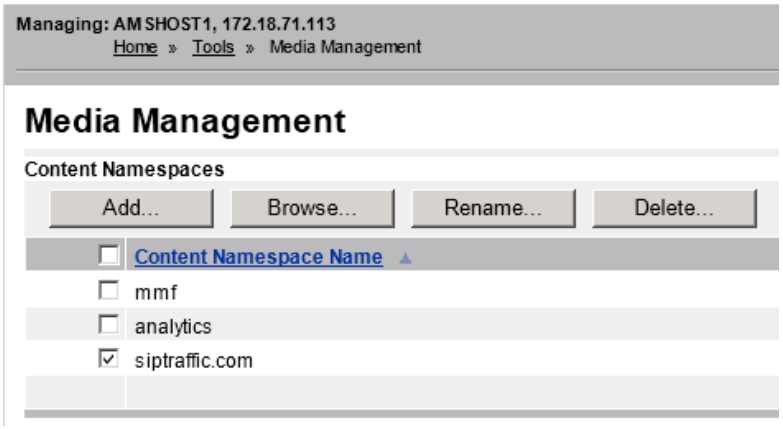
- Add the content namespace.

- Copy the media files from the stored location onto the system you are accessing Element Manager from. See Backing up the batch zip file (page 350).

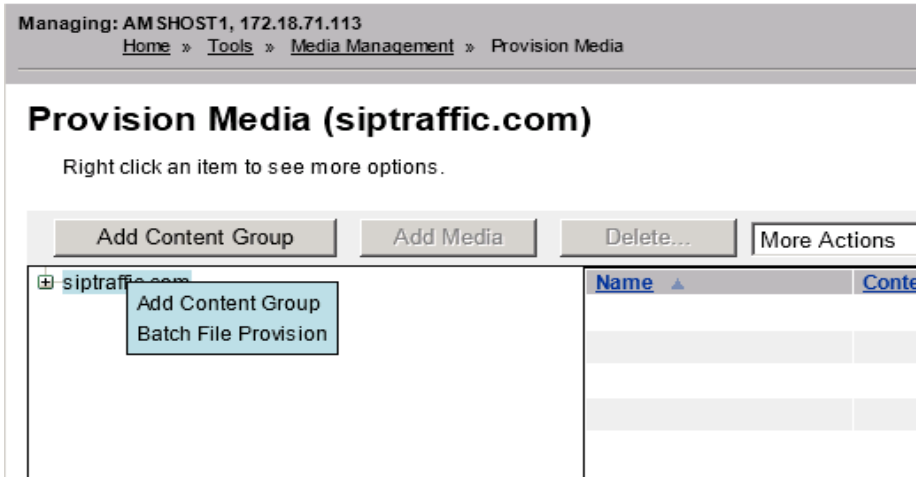
Attention: You must give the root directory the same name as the content namespace name.

Procedure steps

Step	Action
1	Log on to Element Manager from the system on which the copied batch zip file is located.
2	In the navigation pane, click **Tools**, **Media Management**.
3	On the **Media Management** page, select the check box next to the content namespace to which you want to add the media. For example, select siptraffic.com.



4	Click **Browse**. *Avaya MS displays the **Provision Media** page.*
5	On the **Provision Media** page, right-click the content namespace and select **Batch File Provision** on the shortcut menu.



6 On the **Batch File Provision** dialog box, click **Browse**, and then navigate to the zip file to upload.

7 Click **Always overwrite file with the same name**.

OR

Click **Do not overwrite files with the same name**.

8 Click **Upload**.

--End--

Adding the media server

Add the Avaya Media Server to Contact Center Manager Server using Contact Center Manager Administration.

Procedure steps

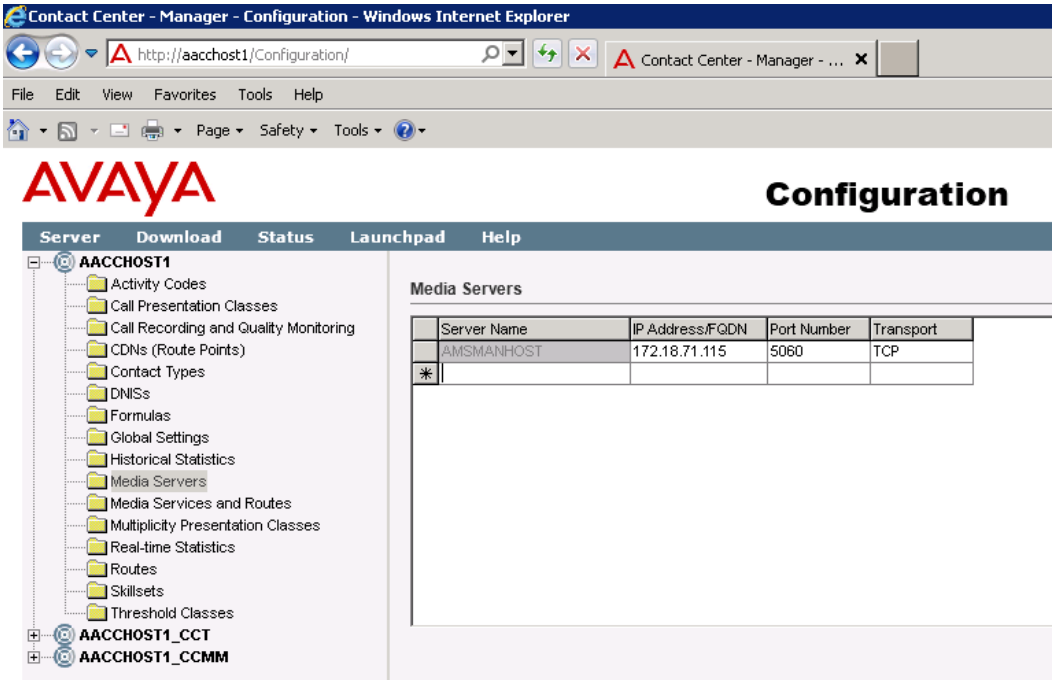
Step	Action
1	Log on to Contact Center Manager Administration with administrator privileges.
2	On the **Launchpad**, click **Configuration**.
3	In the left pane, expand the CCMS server. For example, expand AACCHOST1.
4	From the list of configuration items for the Contact Center Manager Server, select **Media Servers**.
5	On the **Media Servers** window, in the **Server Name** box, type the managed name of the Avaya Media Server HA pair. For example, type AMSMANHOST.

6 In the **IP Address** box, type the service IP address for the Avaya Media Server. For example, type 172.18.71.115.

7 In the **Port Number** box, type the port number. For example, type 5060.

8 Ensure that the value for **Transport** is **TCP**.

9 Select the next row of the grid to add the Media Server.



--End--

Adding media servers to the required media services

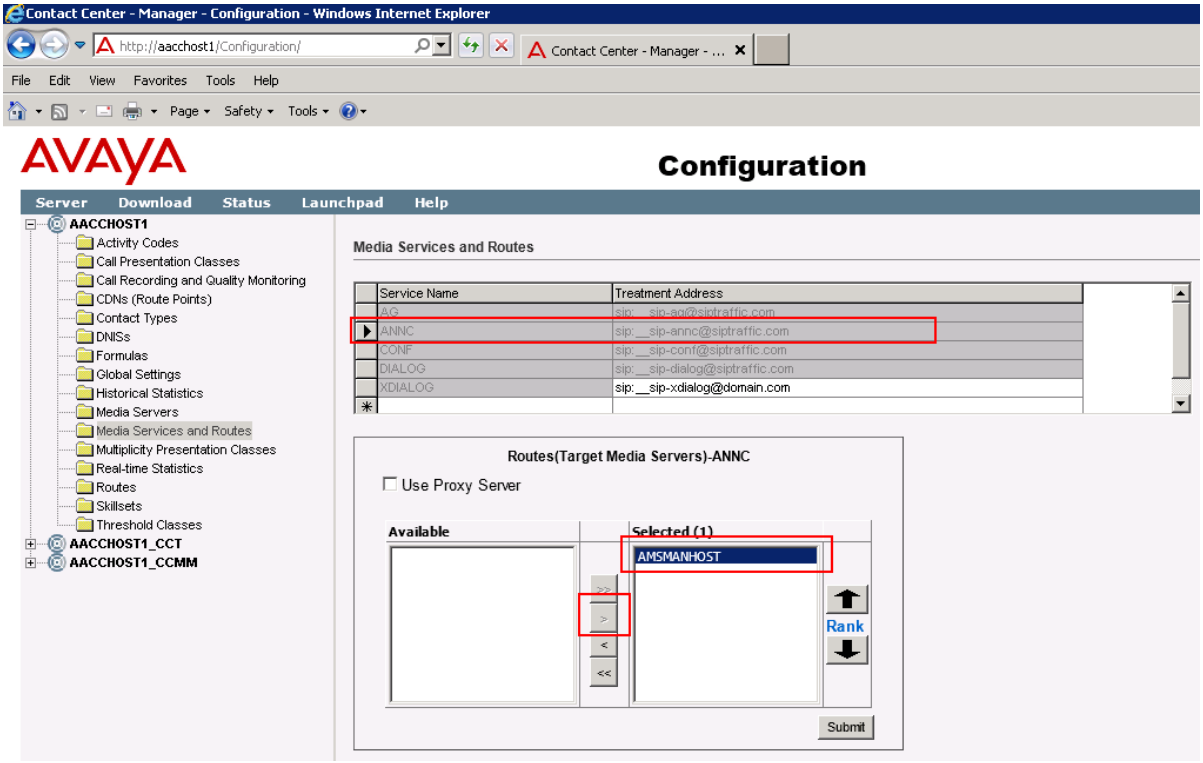
Each SIP-enabled contact center requires at least one Avaya Media Server to supply the following services:

- Announcements (ANNC)
- Conferences (CONF)
- Interactive Voice Response (IVR) dialog (DIALOG)

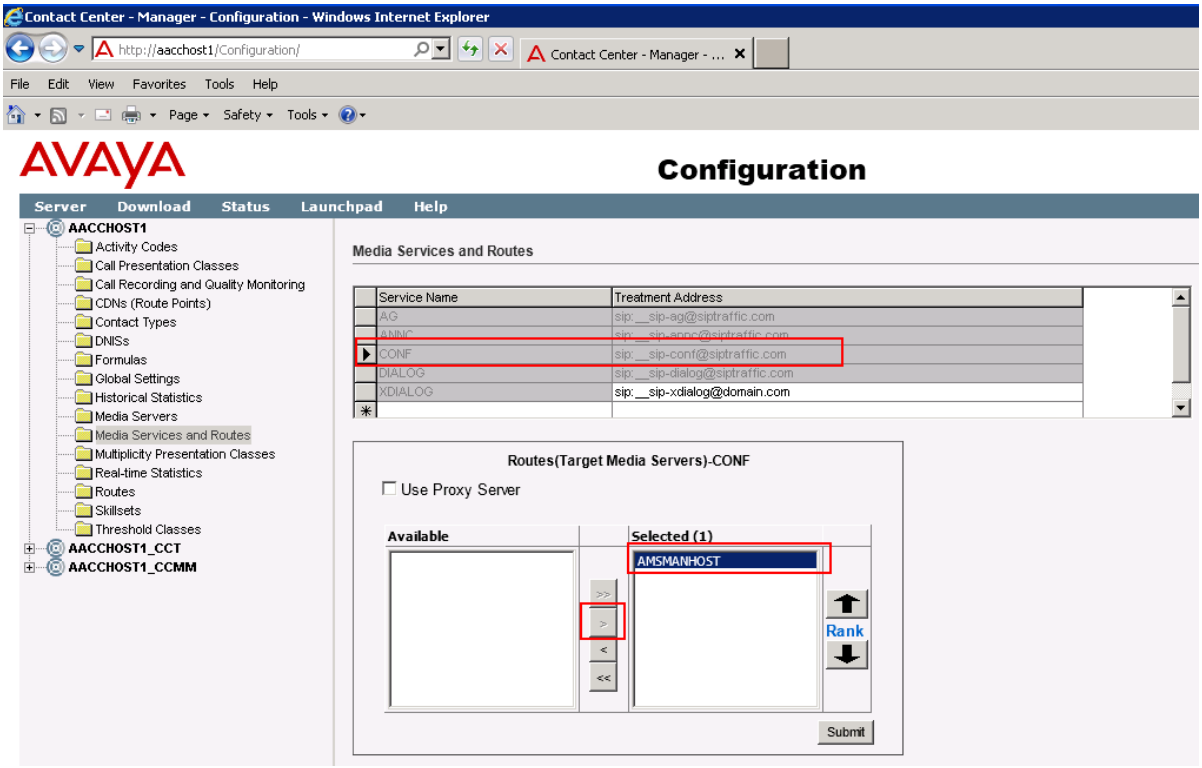
You must assign the Avaya Media Server media server for each announcement, conferencing, and dialog service.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration.
2	On the **Launchpad**, click **Configuration**.
3	In the left pane, expand the CCMS server. For example, expand AACCHOST1.
4	From the list of configuration items for the Contact Center Manager Server, select **Media Services and Routes**.
5	From the **Service Name** list, select **ANNC**.
6	In the **Routes (Target Media Servers)** section, from the **Available** list, select the Avaya Media Server server name. For example, select AMSMANHOST.
7	Click the **>** arrow key. *AMSMANHOST is added to the list of Selected Announcement media servers.*



8	Click **Submit**.
9	From the **Service Name** list, select **CONF**.
10	In the **Routes (Target Media Servers)** section, from the **Available** list, select the Avaya Media Server server name. For example, select AMSMANHOST.
11	Click the **>** arrow key. *AMSMANHOST is added to the list of Selected Conference media servers.*



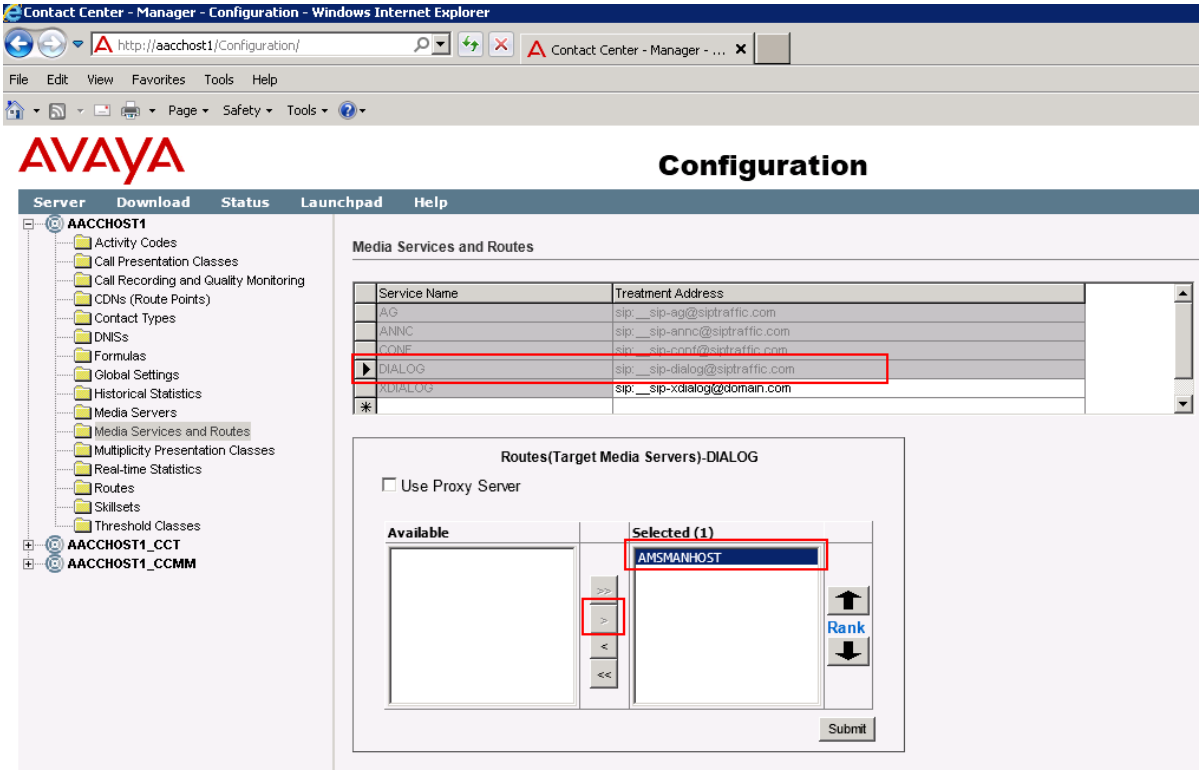
12 Click **Submit**.

13 From the **Service Name** list, select **DIALOG**.

14 In the **Routes (Target Media Servers)** section, from the **Available** list, select the Avaya Media Server server name. For example, select AMSMANHOST.

15 Click the **>** arrow key.

AMSMANHOST is added to the list of Selected Conference Dialog media servers.



16 Click **Submit**.

--End--

Restarting License Manager to push Avaya Media Server licenses

Avaya Aura® Contact Center supports WebLM. Avaya Aura® Contact Center can use WebLM to license the contact center features and to control the number of agents in your system. You can obtain a WebLM license file from the Avaya Product Licensing and Delivery System (PLDS).

When you configure an Avaya Media Server as a Media Server in Contact Center Manager Administration, Contact Center License Manager pushes the license keys to that Avaya Media Server. You must restart the License Manager service and then restart that Avaya Media Server so it can acquire these licenses. Do not configure WebLM licensing on Avaya Media Server servers.

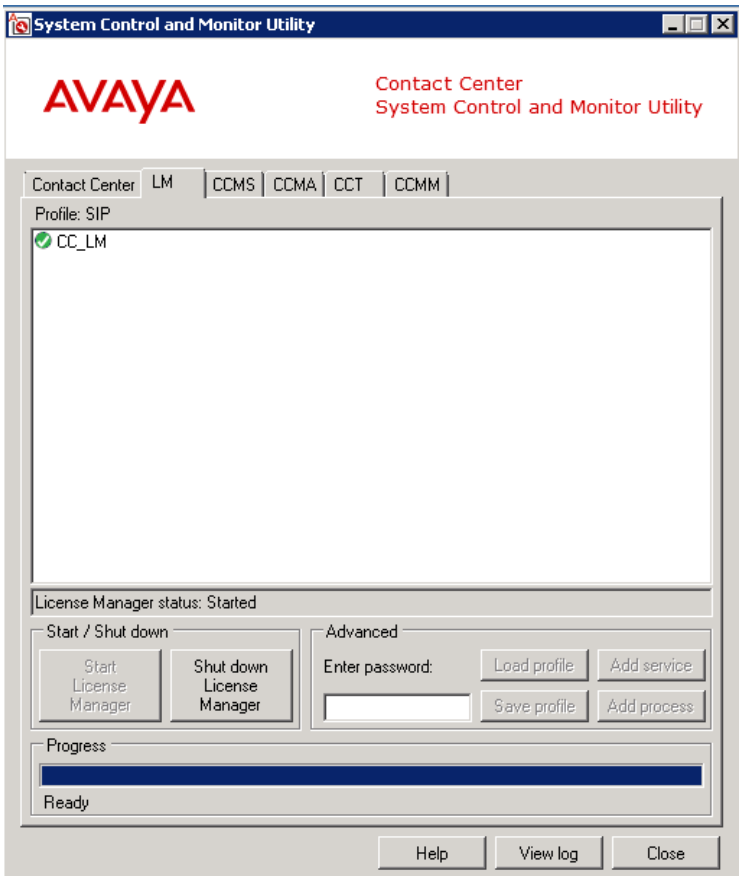
You configure an Avaya Media Server High Availability pair in Contact Center Manager Administration by entering the Managed IP address of the HA pair as the IP address of a single Media Server. Contact Center License Manager, when restarted, then provides and pushes license keys to both Avaya Media Servers of that HA pair.

Restart Contact Center License Manager to push license keys to the Avaya Media Server High Availability pair.

Attention: Ensure the Avaya Aura® Contact Center license file on the Voice and Multimedia Contact Server is enabled for High Availability.

Procedure steps

Step	Action
1	Log on to the Voice and Multimedia Contact Server.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Common Utilities**, **System Control and Monitor Utility**.
3	Click the **LM** tab.
4	Ensure that all services in the **Profile** box have a green circle next to them.



5	Click **Shut down License Manager**.
6	Click **Start License Manager**.
7	Click **Close**.

--End--

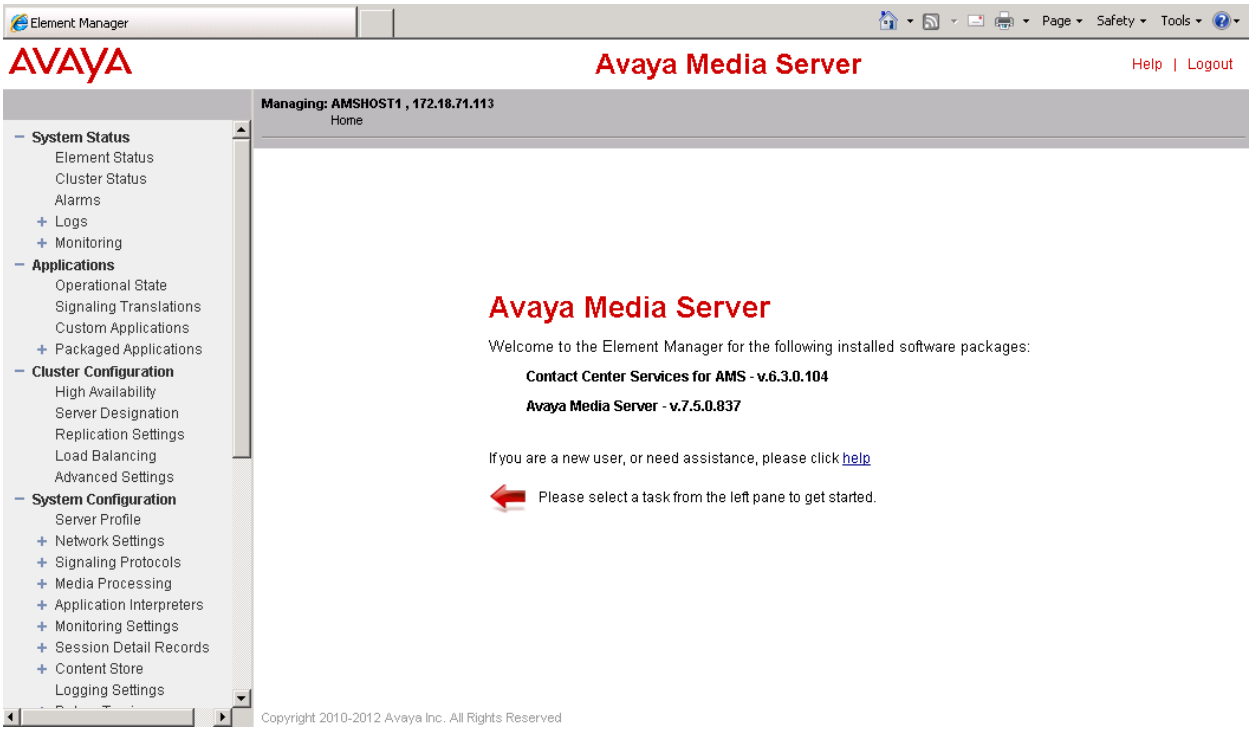
Verifying Avaya Media Server licensing

Perform the following steps to ensure Avaya Media Server is licensed.

At this stage in the configuration, the primary and backup Avaya Media Server servers are both licensed. You may need to restart both Avaya Media Servers to clear the license related alarms.

Procedure steps

Step	Action
1	Start a Web browser.
2	In the address box, enter https://<AMS_SERVER_IP_ADDRESS>:8443/em. To access the primary Avaya Media Server EM enter https://172.18.71.113:8443/em To access the backup Avaya Media Server EM enter https://172.18.71.114:8443/em
3	In the **User ID** box, type amsuser.
4	In the **Password** box, type the amsuser password.
5	Click **Log In**.



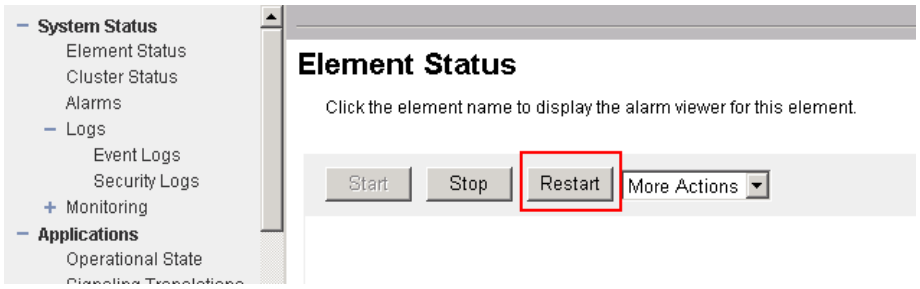
6 In the primary Avaya Media Server Element Manager navigation pane, click **System Status**.

7 Click **Element Status**.

8 If the primary or backup servers display license related alarms you must restart both servers to acquire the license keys provided by Contact Center License Manager.

9 In the primary Avaya Media Server Element Manager navigation pane, click **System Status**.

10 Click **Element Status**.



11 Click **Restart**.

12 In the backup Avaya Media Server Element Manager navigation pane, click **System Status**.

13 Click **Element Status**.

14 Click **Restart**.

--End--

Agent Desktop verification section

- Agent Desktop – Verifying voice calls (page 435)

Agent Desktop – Verifying voice calls

The Windows version of Avaya Media Server is now removed from the Voice and Multimedia Contact Server, and the Avaya Media Server High Availability pair is installed and commissioned the on Linux-based servers. You must retest voice calls on Avaya Aura® Agent Desktop and ensure that calls are routed correctly.

Starting Agent Desktop

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

Prerequisites

- Ensure that you have installed Agent Desktop.

Procedure steps

Step	Action
1	Log on to an Agent Desktop client computer in the siptraffic.com domain using the siptraffic\AACC_Agent1 Windows (and Contact Center Agent) account.
2	On the Agent Desktop client computer, in Internet Explorer, type the URL in this format: <Voice and Multimedia Contact Server name>/agentdesktop. For example, type: http://AACCHOST1/agentdesktop
3	Click **Launch AAAD**.

--End--

Procedure job aid

The system automatically configures your status to Logged Out, when you launch Agent Desktop.

Agent Desktop

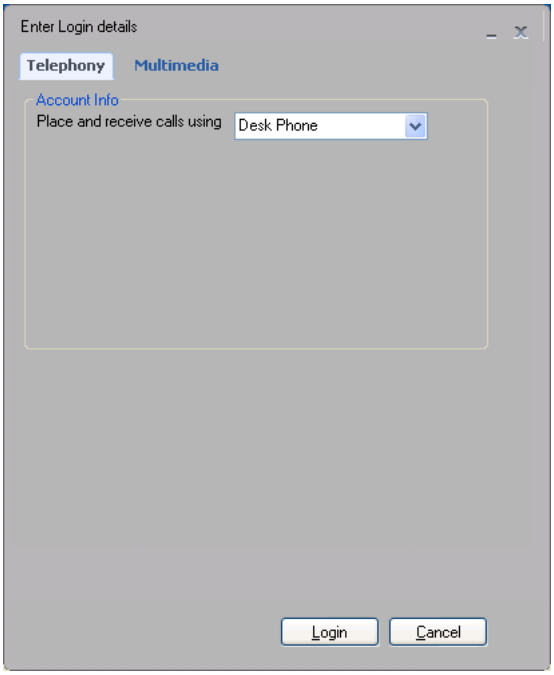


Logging on to Agent Desktop when using a desktop phone

Log on to Agent Desktop after you start the Agent Desktop application. While you log on, you can choose between a desktop phone and a softphone based on your usage mode. The system automatically configures your status to Not Ready. Change your status to Ready to indicate that you are available to handle all media types for which you are licensed and configured. If you are assigned to a skillset for a particular contact type, you can receive and create contacts in that contact type.

Procedure steps

Step	Action
1	Start Agent Desktop.
2	On the Agent Desktop Top bar, from the **Status** list, select **Login**.
3	Click the **Telephony** tab.



4	Select **Desk Phone** from the **Place and receive calls using** drop-down list.
5	On the **Multimedia** tab, type your **ID** and **Password**. For example type 42000 as the ID and 42000 as the password.
6	Click **Login**.

The system verifies your password and logs you on to the Agent Desktop application and into Avaya Aura® Contact Center. The Logged out icon changes to Logged In. The status icon changes to Not Ready.

--End--

Variable definitions

Description	Value
ID (Multimedia)	Your log on ID appears in the ID box, based on your Communication Control Toolkit configuration.
Password (Multimedia)	Initially, for multimedia agents, your password is the same as your Agent Logon ID. The system verifies your password and logs you on to the Agent Desktop application and into Avaya Aura® Contact Center. The Logged out icon changes to Logged In.

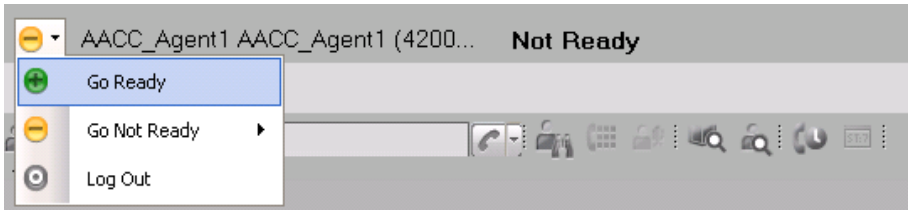
Changing your status to Ready

Change your status to Ready when you are available to create or receive contacts.

When you change your status to Ready in a SIP-enabled Contact Center, your Contacts Presence status automatically changes to Available.

Procedure steps

Step	Action
1	On the Agent Desktop Top bar menu, click the Status icon.
2	Select **Go Ready**.



Agent Desktop places you in Ready status. The status icon changes to green and the Top bar displays the Ready status.

--End--

Accepting a test call

Accept and work with telephone calls. The relevant work item controls become active and the call timer appears in the work item.

Prerequisites

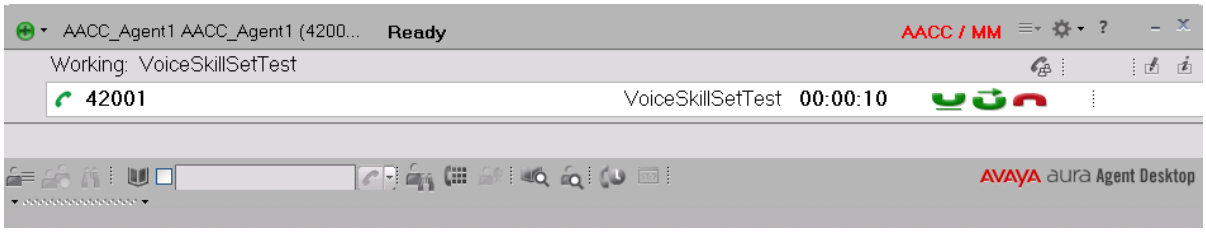
- Ensure that you are in Ready state.
- Ensure that you have a skillset designated to handle telephone calls.

Procedure steps

Step	Action
1	Generate a test call to the contact center. For example, from another phone on the same Communication Manager, dial the contact center route point of 52000.
2	On the Agent Desktop, select the new alerting work item and click the Accept work item control. *The top pane of the Agent Desktop shows the customer details and history of all past calls with the contact.*

--End--

Procedure job aid



High Availability section

- High Availability – CCMA replication pre-install configuration (page 441)
- High Availability – Voice and Multimedia Contact Server standby software installation (page 459)
- High Availability – Voice and Multimedia Contact Server commissioning (page 545)
- High Availability – Session Manager configuration (page 613)
- High Availability – Testing (page 617)

High Availability – CCMA replication pre-install configuration

This chapter describes how to configure the windows accounts used by Contact Center Manager Administration (CCMA) replication in your Avaya Aura® Contact Center solution.

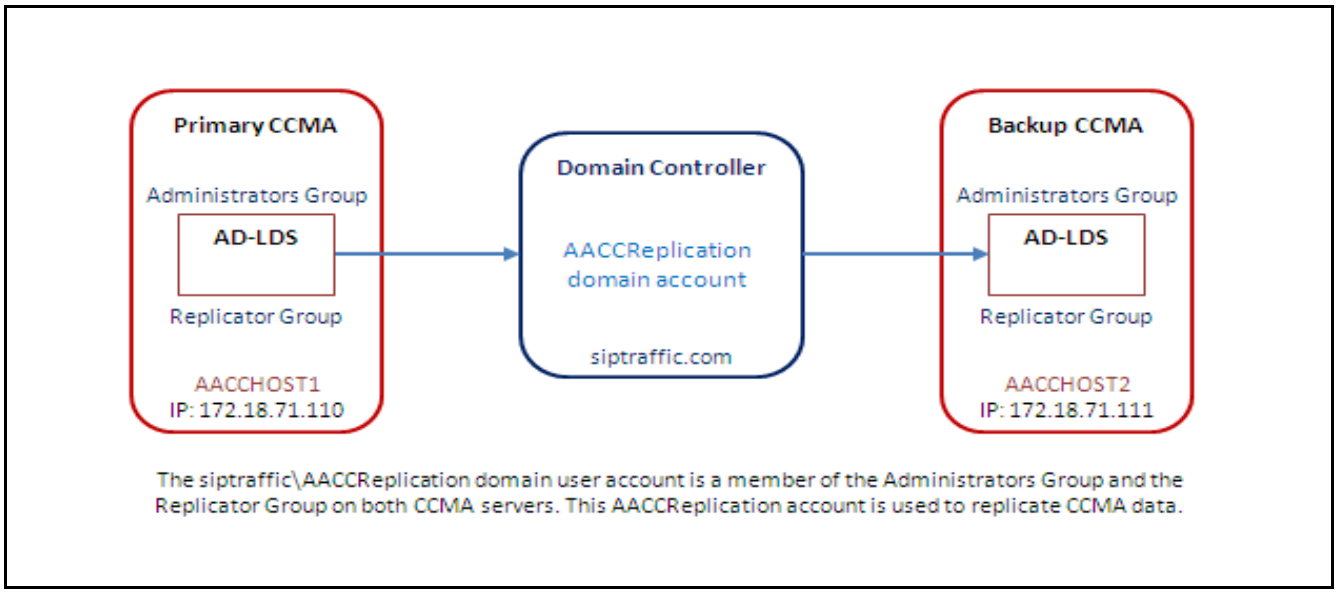
Perform these procedures on the active Avaya Aura® Contact Center server.

Example server details	Active Voice and Multimedia Contact Server
Name	AACCHOST1
IP Address	172.18.71.110

Contact Center Manager Administration (CCMA) redundancy is provided by the addition of a replication or standby CCMA server. CCMA stores configuration data in a Microsoft Active Directory - Lightweight Directory Services (AD-LDS) data store. The standby CCMA replicates the AD-LDS on the primary CCMA. The standby CCMA uses AD-LDS replication to maintain a copy of the primary CCMA configuration data. If the active CCMA fails, no loss of configuration data occurs because the standby CCMA replicates the data stored in AD-LDS.

The primary CCMA server and the standby replication CCMA server must both be in the same Windows domain for AD-LDS replication to work. AD-LDS replication uses a common windows account, used by both CCMA servers, to copy or replicate configuration data from the primary CCMA AD-LDS to the standby CCMA AD-LDS.

Using the domain user account "siptraffic\AACCReplication" for CCMA replication



Active Directory - Lightweight Directory Services data store

Contact Center Manager Administration makes use of Active Directory - Lightweight Directory Services (AD-LDS) and other data files to store application data. The following data is stored in AD-LDS:

- user information and details
- access classes
- partitions
- private and graphical real-time reports
- real-time report filters

The following data files are not stored in AD-LDS:

- scheduling data for Contact Center Management assignments
- scheduling data for historical reports
- historical report output files
- user-created historical reports imported into Contact Center Manager Administration
- real-time report exported files
- Emergency Help exported files
- Report Creation Wizard user-created formulas (stored in the file RCW.mdb)
- Report Creation Wizard user-created reports and report definitions
- Audit Trail events

Use the Contact Center Manager Administration Backup and Restore utility to manage the data not stored in AD-LDS.

A CCMA replication solution contains a primary CCMA server and a standby CCMA server. The primary CCMA server is installed with "Enable CCMA Replication" not selected. The standby CCMA server is installed with "Enable CCMA Replication" selected. The standby CCMA server is replicating the primary CCMA server AD-LDS contents.

The primary CCMA server is always the primary CCMA server. If the primary CCMA fails, the standby CCMA is still a standby CCMA, they do not switch roles. To restore CCMA solution resiliency, you must repair and reinstate the primary CCMA server, or install a new primary CCMA server using the same details as the previous primary CCMA. After a switchover, AD-LDS replication ensures that data stored in AD-LDS is available on the standby server. Data not stored in AD-LDS must be manually restored to the standby CCMA server.

Domain environments

Perform the following steps to create the AD-LDS Replication account:

- Ask your Systems Administrator to create a domain user account for use by AD-LDS Replication, for example "siptraffic\AACCReplication".
- Assign this domain user account to the local Administrators and local Replicator groups on both CCMA servers.

If the active server is a Voice and Multimedia Contact Server, you must install a Voice and Multimedia Contact Server on the standby server. All applications must be on the same patch level.

Adding the domain AD-LDS replication account to the primary administrators and replicator group

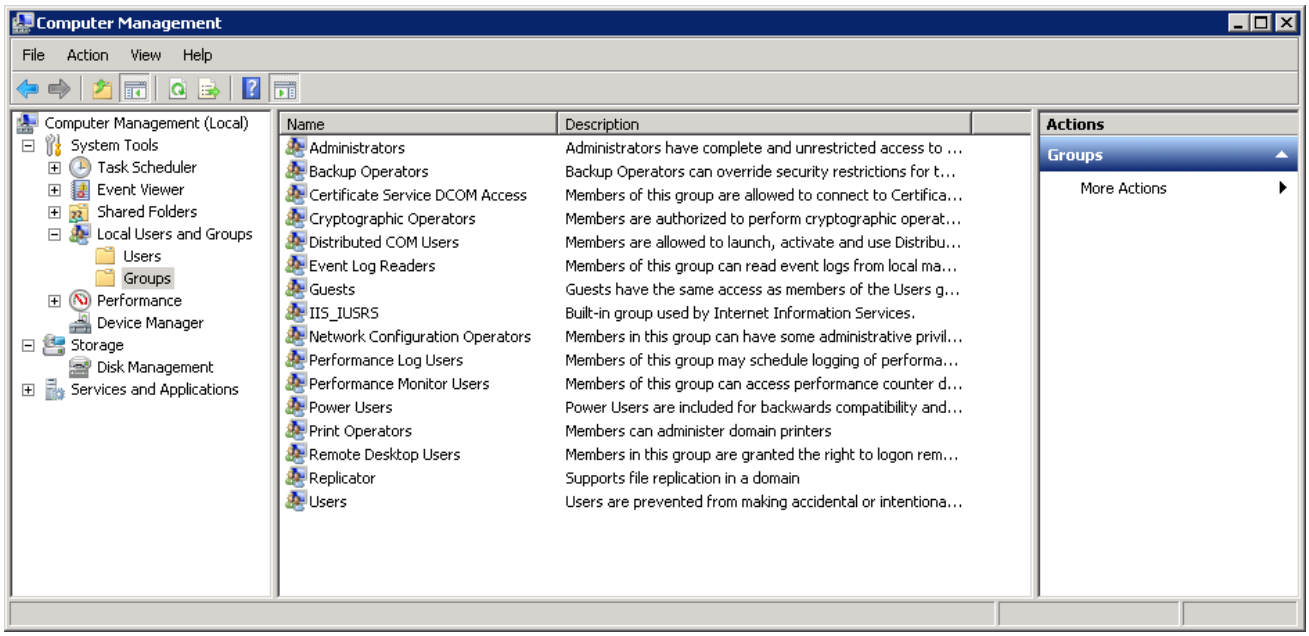
Add the AD-LDS replication account to the local Administrators and replicator group on the primary CCMA server.

Request this AD-LDS replication account from your Network or Domain Administrator. The primary and standby replicating Contact Center Manager Administration servers must both be added to the same domain.

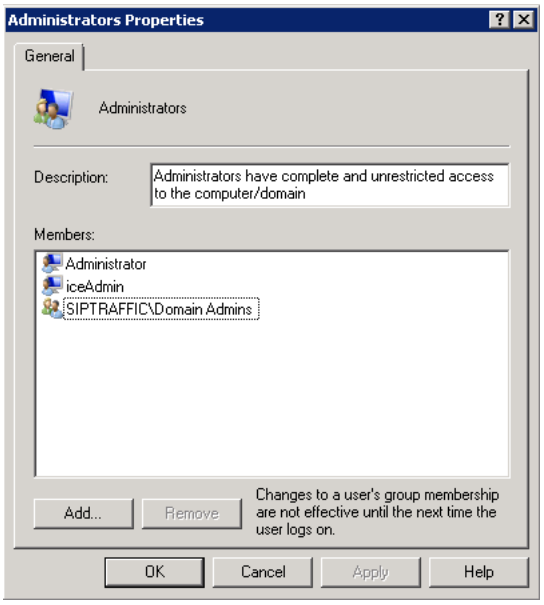
For this procedure, the name of the AD-LDS replication account is "siptraffic\AACCReplication". You can choose another name for the account.

Procedure steps

Step	Action
1	Log on to the active Contact Center Manager Administration server.
2	Click **Start**, **Administrative Tools**, **Computer Management**.
3	In the **Computer Management** window, expand **Local Users and Groups**.
4	Click the **Groups** folder.

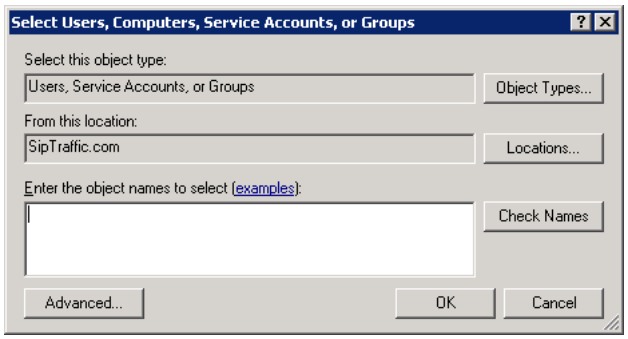


5	Double-click on the **Administrators** group.

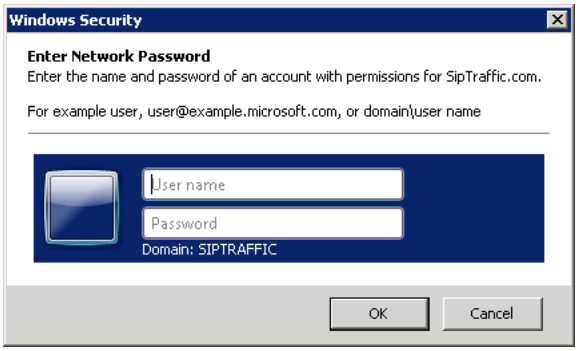


6 On the **Administrators Properties** window, click **Add**.

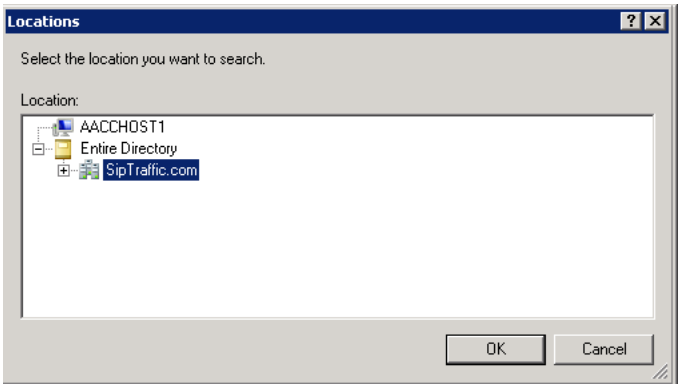
7 On the **Select Users**, **Computers**, **Service Accounts**, **or Groups** window, **click Locations**.



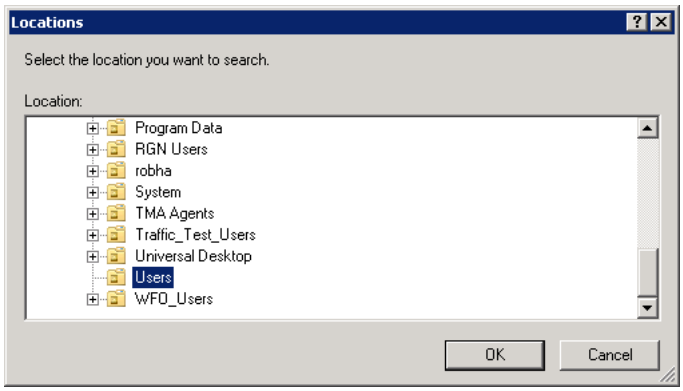
8 If a **Windows Security** dialog box appears, type a domain user account name and password for the domain.



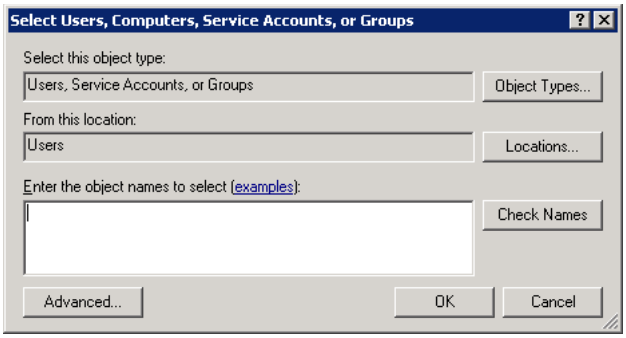
9 On the **Locations** dialog, select the domain to be used by CCMA replication, for example select siptraffic.com.



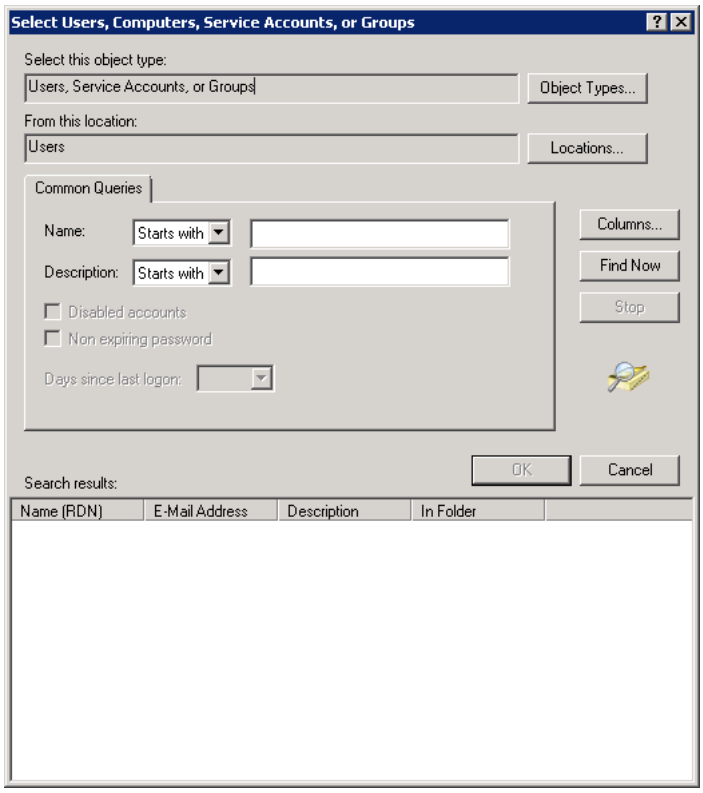
10 Expand the domain folder, scroll down and select **Users**.



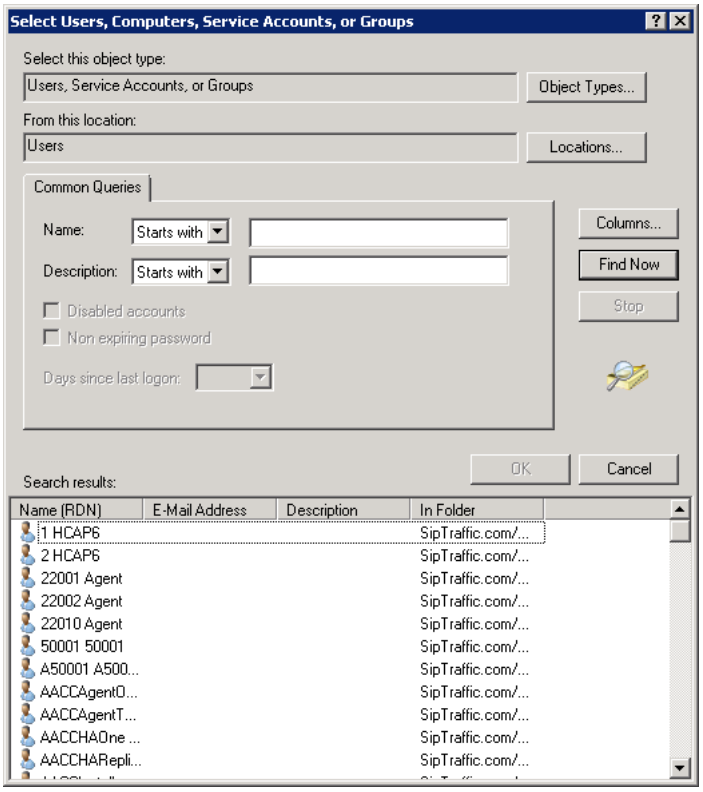
11 Click **OK**.



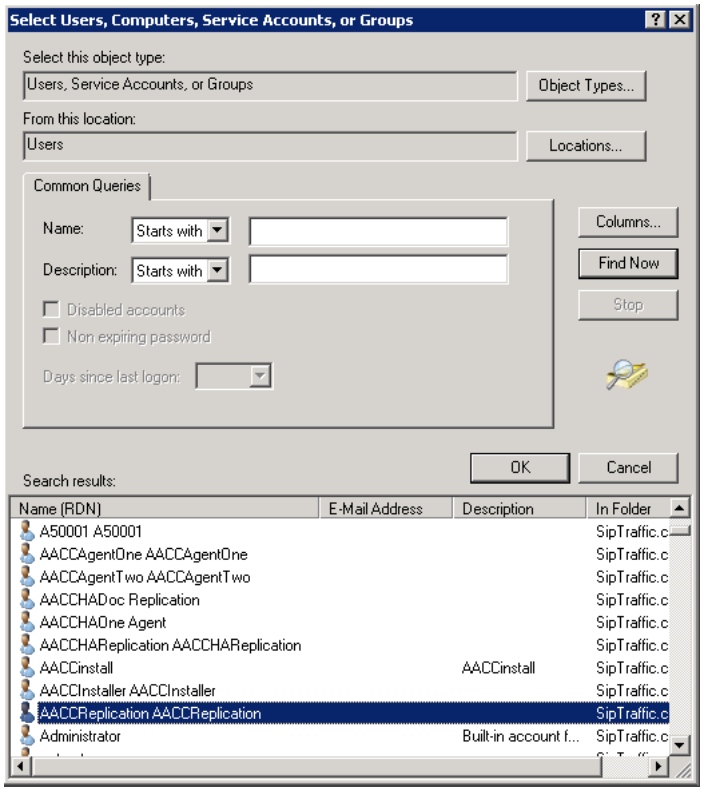
12 Click **Advanced**.



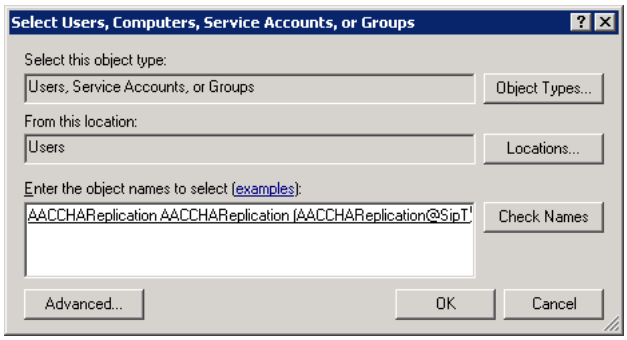
13 Click **Find Now**, to display domain users.



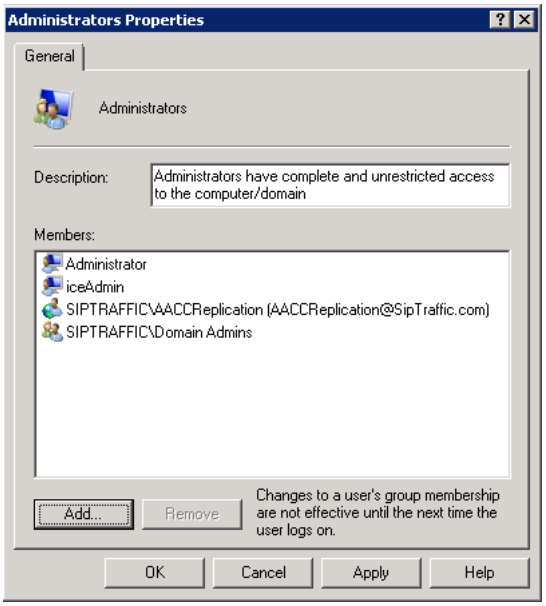
14 From the list of domain users select the CCMA replication domain user account, for example select the "siptraffic\AACCReplication" domain user account.



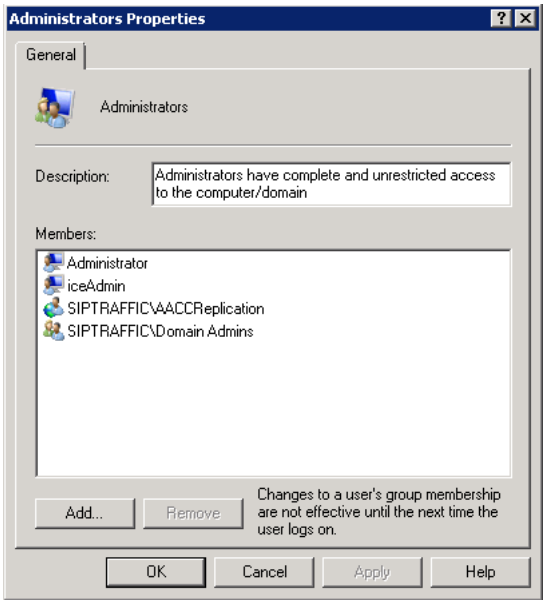
15 Click **OK**.



16 Click **OK**.

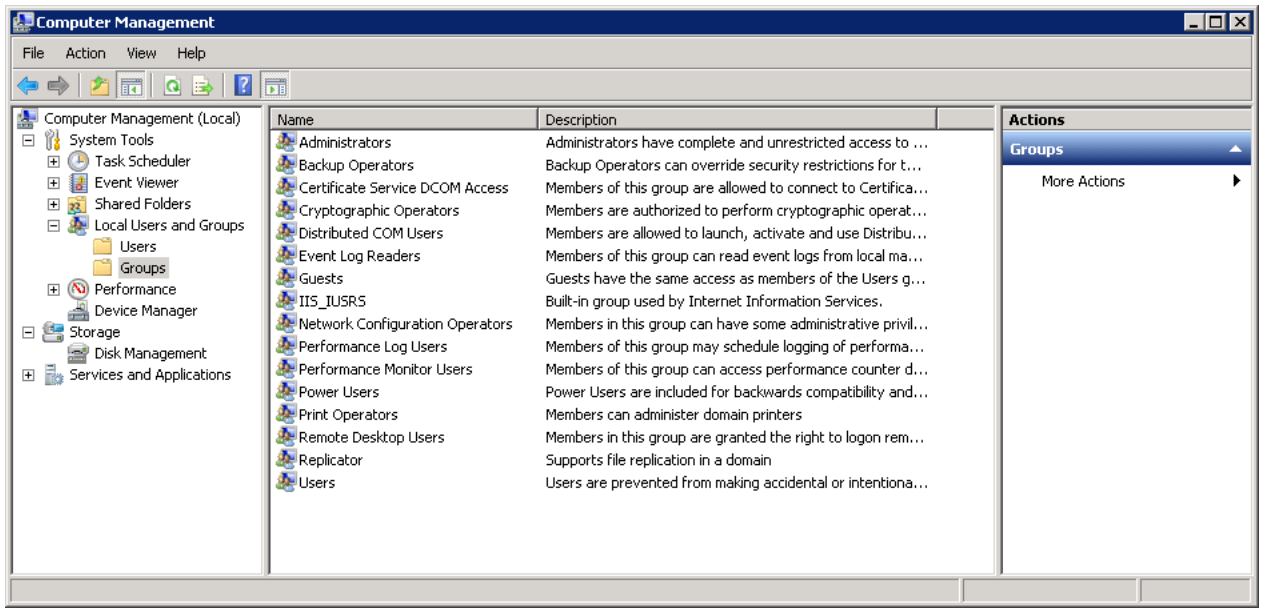


17 Click **Apply**.

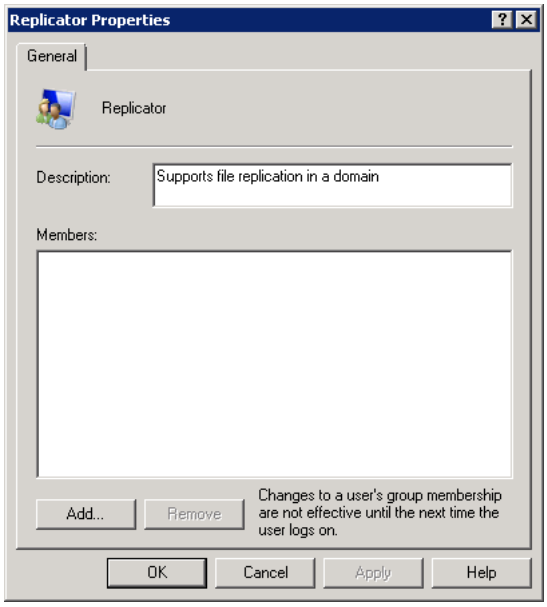


18 Click **OK**.

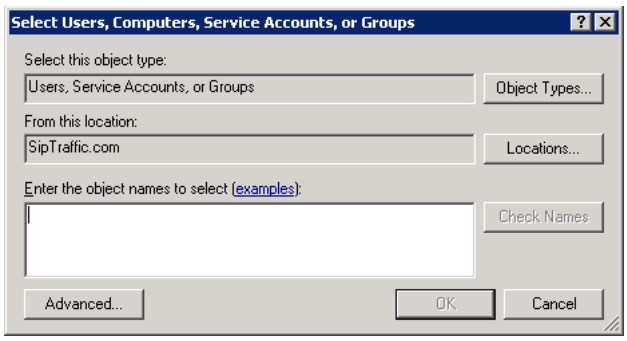
19 Click the **Groups** folder.



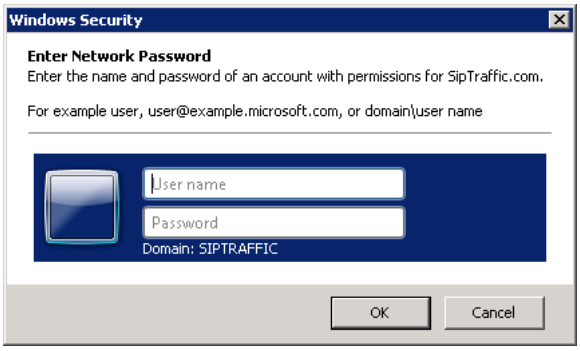
20 Double-click on the **Replicator** group.



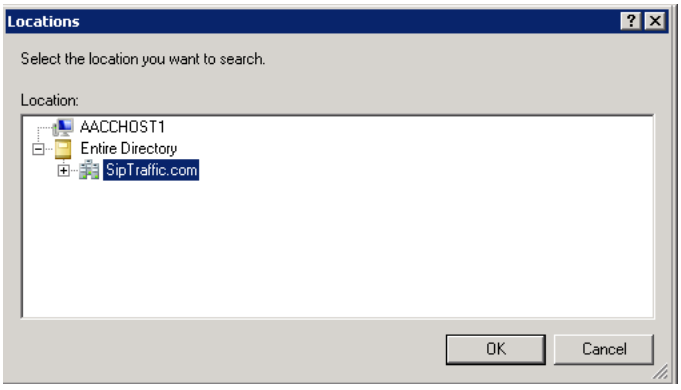
21 Click **Add**.



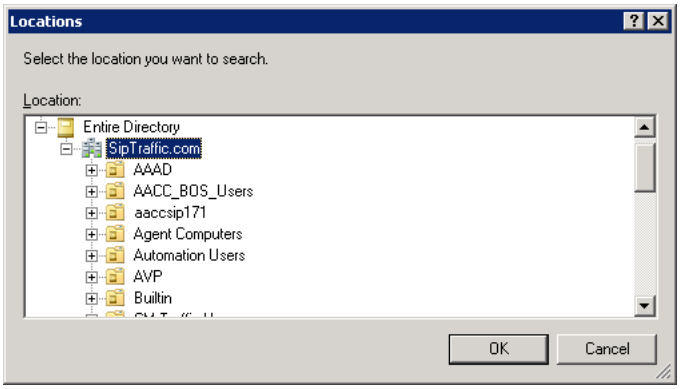
22 Click **Locations**.



23 If a **Windows Security** dialog box appears, type a domain user account name and password for the domain.

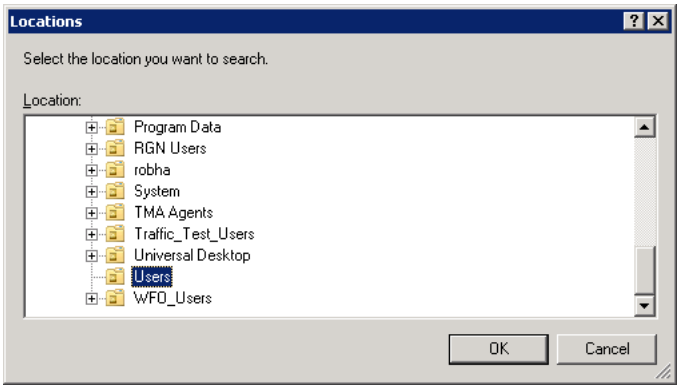


24 On the **Locations** dialog, select the domain to be used by CCMA replication. For example, select siptraffic.com.

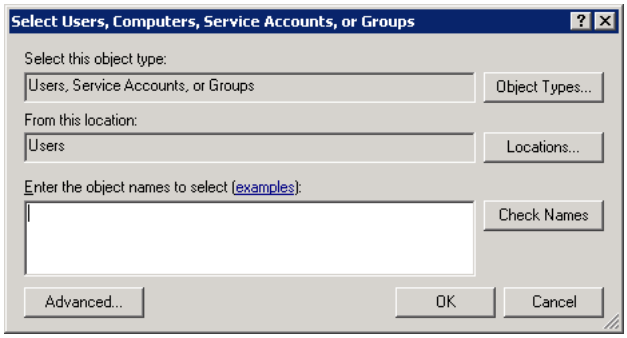


25 Expand the domain folder to display domain users.

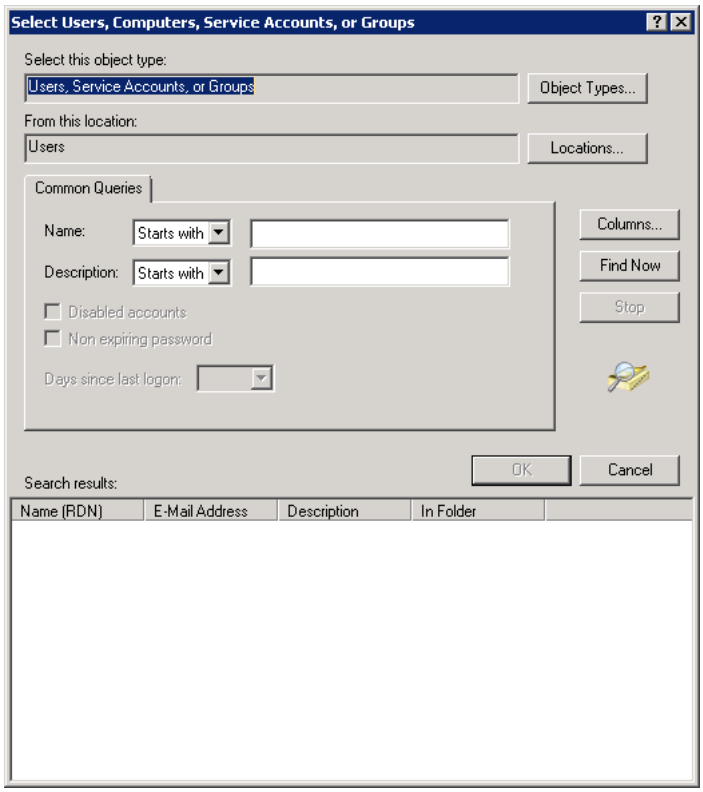
26 Click **Users**.



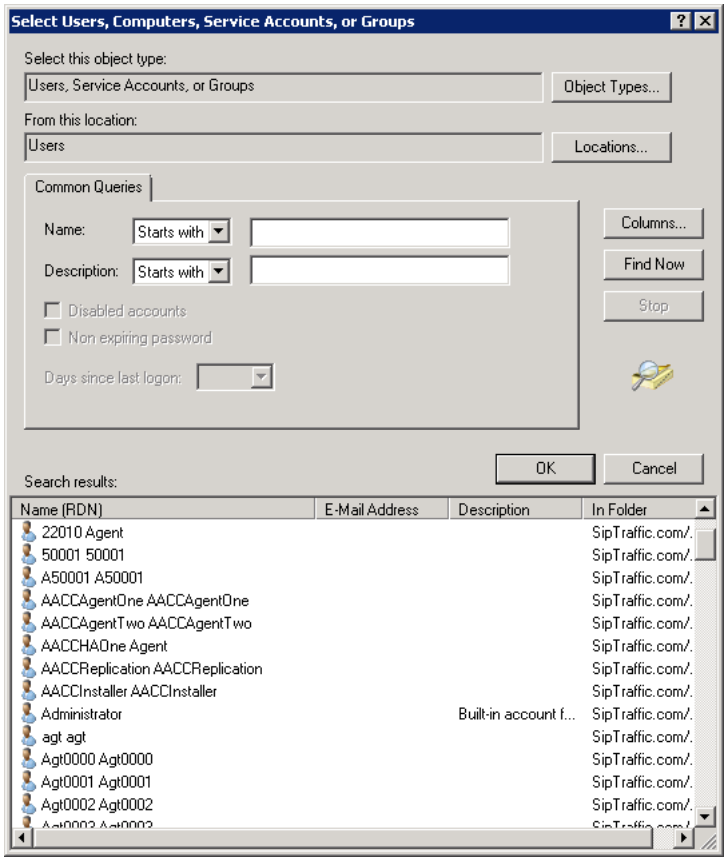
27 Click **OK**.



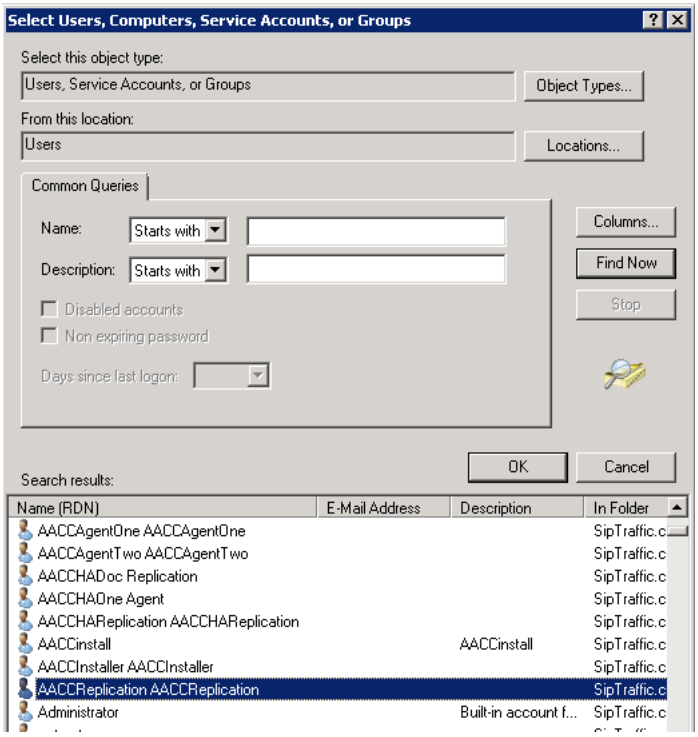
28 Click **Advanced**.



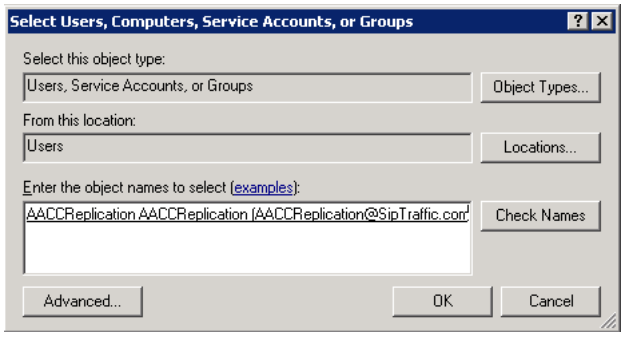
29 Click **Find Now**, to display domain users.



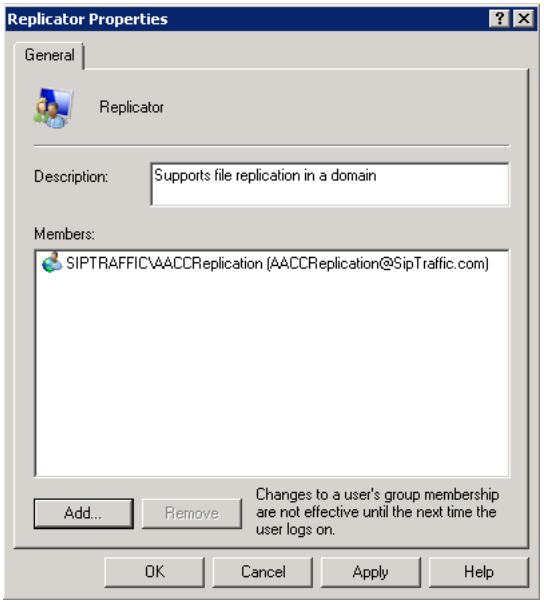
30 From the list of users select the CCMA replication domain user account, for example select the "siptraffic\AACCReplication" domain user account.



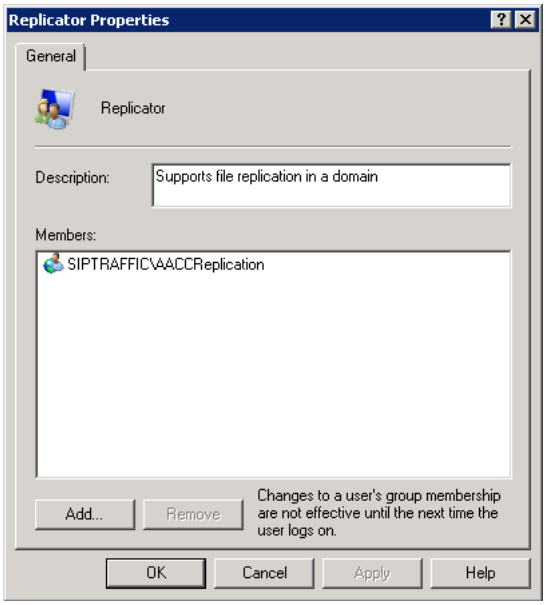
31 Click **OK**.



32 Click **OK**.



33 Click **Apply**.



34 Click **OK**.

--End--

High Availability – Voice and Multimedia Contact Server standby software installation

This chapter provides the steps to install the standby Voice and Multimedia Contact Server software on the standby server. This includes the following server software:

- Contact Center Manager Server (CCMS)
- Contact Center License Manager (LM)
- Contact Center Manager Administration (CCMA)
- Communication Control Toolkit (CCT)
- Contact Center Multimedia (CCMM)
- Orchestration Designer (OD)

You can change the name of a Voice and Multimedia Contact Server after installation is complete, but because this is time consuming, Avaya recommends that you configure the server final production name before installing Contact Center software.

Example server details	Standby Voice and Multimedia Contact Server
Name	AACCHOST2
IP Address	172.18.71.111

You can create an administration account on the server and then install Avaya Aura® Contact Center using the account. This Avaya Aura® Contact Center administration account must have full administrative privileges. You must upgrade and patch Avaya Aura® Contact Center using this administration account. You can rename this account after installing Avaya Aura® Contact Center, but you must not delete the account. If you delete the account used to install Avaya Aura® Contact Center, Avaya Aura® Contact Center stops working.

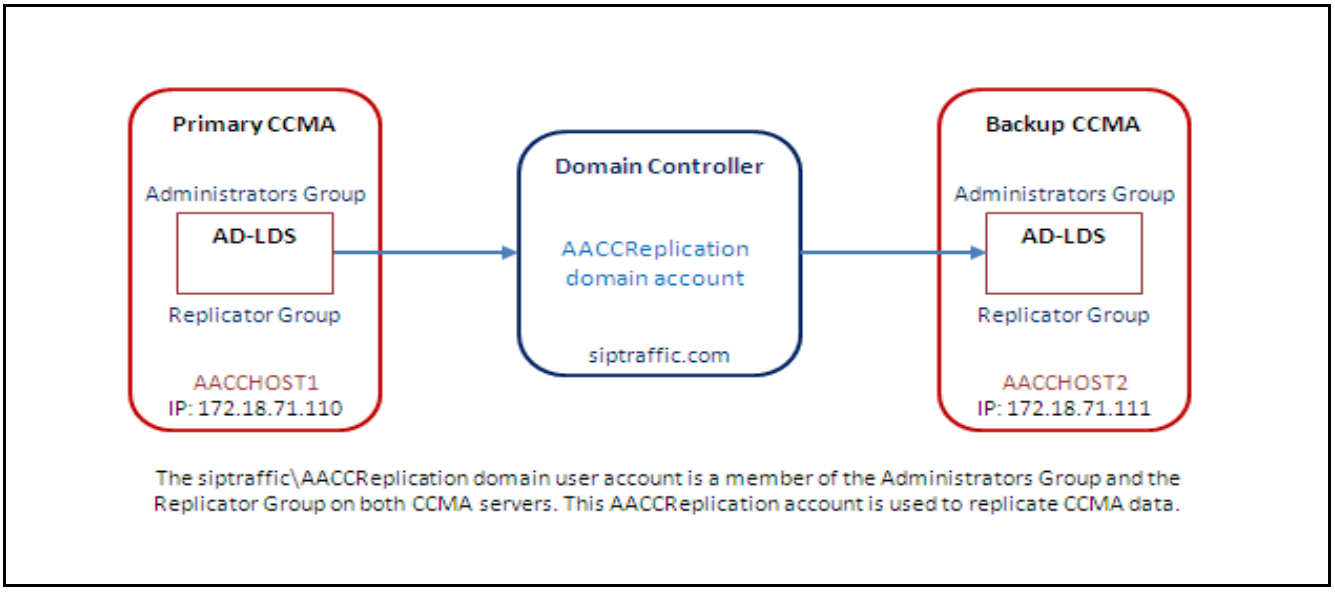
You can configure this Voice and Multimedia Contact Server as a standby server to take over contact processing and become the active server if the active server fails. This standby server provides High Availability redundancy and resiliency.

The software installation configuration on the standby server must match the configuration of your active server. If you installed Contact Center Manager Server and License Manager on your active server, then you must install these two software applications in the same location on your standby server.

CCMA stores configuration information in Microsoft Active Directory - Lightweight Directory Services (AD-LDS). Install the standby CCMA to replicate the primary CCMA AD-LDS in your Avaya Aura® Contact Center solution.

This standby CCMA provides redundancy and resiliency and can become the active CCMA if the primary CCMA fails. No automatic CCMA switchover occurs. If the active CCMA fails, the Contact Center uses the standby CCMA.

Using the domain user account "siptraffic\AACCReplication" for CCMA replication



Prerequisites to Voice and Multimedia Contact Server software installation

- Ensure that your new Contact Center license file is available. This sample solution uses a WebLM license file obtained from the Avaya Product Licensing and Delivery System (PLDS).
- Download and review the Avaya Aura® Contact Center Release Notes. The Release Notes contain the known issues, patches, and workarounds specific to a release and patch line-up of Avaya Aura® Contact Center. For more information about the Avaya Aura® Contact Center Release Notes, see www.avaya.com/support.
- Ensure the CCMA Active Directory - Lightweight Directory Services (AD-LDS) Replication account is configured on your active Avaya Aura® Contact Center server. For more information, see High Availability – CCMA replication pre-install configuration (page 441).

Installing Windows Server 2008 Release 2

Install the Windows operating system, which is required for the Contact Center server software. During the installation, configure the Windows settings as required. You must perform this procedure on each server before you install Contact Center server software on the server.

Prerequisites

- Ensure that you have a newly formatted server that meets the specifications in *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210) on which to install Microsoft Windows Server 2008 Release 2.
- Ensure that you have a DVD for Windows Server 2008 Release 2.
- Install the network interface card in the server.

Procedure steps

Step	Action
1	Insert the Windows Server 2008 64-bit Release 2 Standard Edition or Windows Server 2008 64-bit Release 2 Enterprise Edition DVD into the DVD drive of the standby server.
2	Install Windows Server 2008 Release 2 according to the instructions supplied by the DVD.
3	On the first install page, select your language for installation.
4	Click **Next**.
5	On the **Installation** window, select a **Language to install** from the list.
6	Select a **Time and currency** format from the list.
7	Select **Keyboard or input** method from the list.
8	Click **Next**.
9	Click **Install Now**.
10	Select an operating system from the list.
11	Click **Next**.
12	On the first **Install Windows** screen, read the terms of the license agreement and select **I accept the license terms**.
13	Click **Next**.
14	Select **Custom**.
15	Select the disk partition on which you want to install Windows Server 2008.

Attention: You can use the partition management options to configure the partitions on your server. The Operating System partition must be 60GB or greater. The minimum recommended Operating System disk partition is 80GB.

16	Click **Next**. The install proceeds and automatically restarts the server several times.

17 After completing the installation, log on to the server as Administrator. Enter and confirm the local Administrator password.

18 In the **Initial Configuration Tasks** window, select **Activate Windows** and follow the instructions or the Microsoft documentation to activate your server.

19 Select **Set time zone** and complete the information as required for your system.

This setting must match on Contact Center Manager Server and Avaya Media Server.

20 Select **Configure Networking** and complete the information for your Network Interface Card (NIC) with the server IP address.

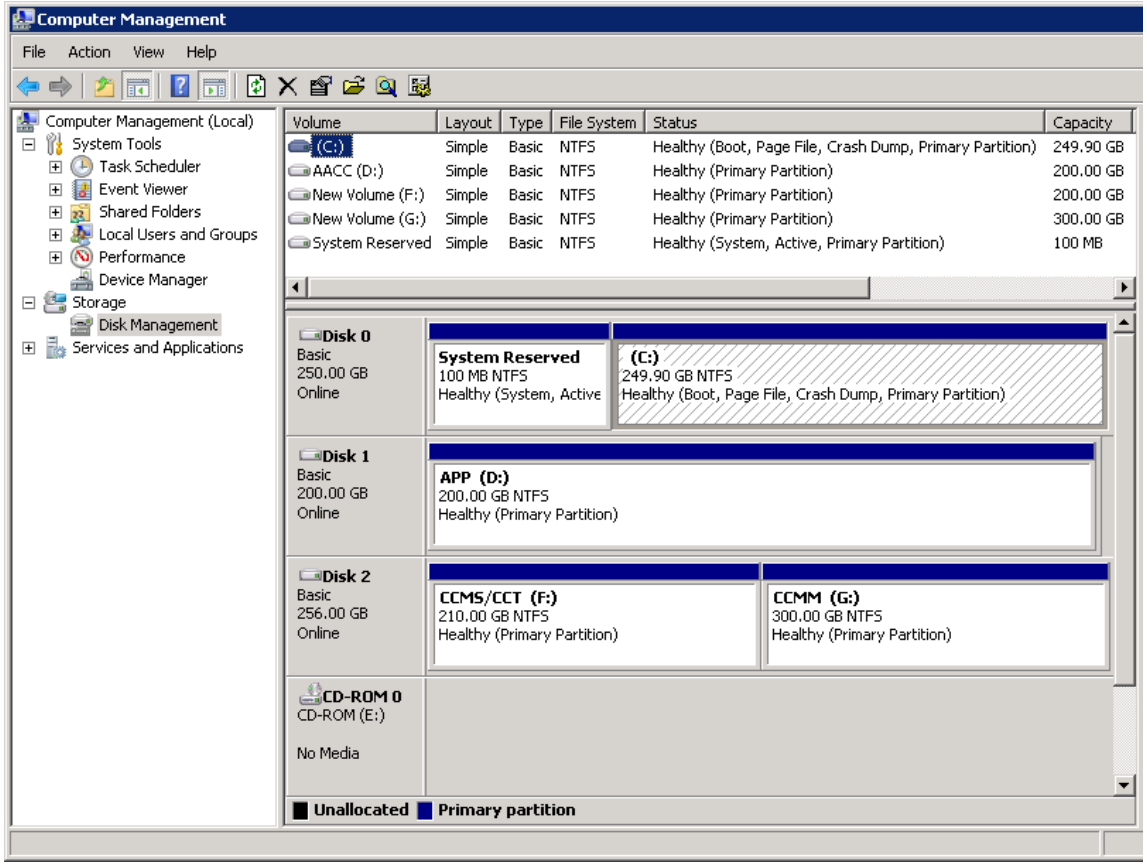
21 Select **Provide computer name and domain** and complete the information for your server name and domain settings.

22 Configure disk drive C: to be the only primary partition on your hard drive.

23 Change the DVD drive letter to E: to ensure the correct drive letters are free for the drives needed for the Avaya Aura® Contact Center application components.

24 Configure the remaining drives for this server as follows:

— D: 80Gb Application drive, minimum.
— F: 210Gb CCMS/CCT Database drive, minimum.
— G: 300Gb CCMM Database drive, minimum.



25	Install any drivers required for your hardware configuration.

--End--

Installing the most recent operating system service packs

Install the most recent supported operating system service packs. You must download the supported operating system service pack included in the Avaya Contact Center Service Packs Compatibility and Hotfix Availability list to ensure your Contact Center server software functions correctly with the supported operating system patches.

Prerequisites

- Access the Avaya Contact Center Service Packs Compatibility and Hotfix Availability list on the support Web site www.avaya.com/support.
- Review the recommendations on operating system service updates in *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).

Procedure steps

Step	Action
1	Log on to the server and disable the Windows Update feature. There are a number of methods for disabling the Windows Update feature, refer to the Windows Server 2008 documentation for a method suitable to your solution. Disabling the Windows Update feature prevents Windows Server 2008 from automatically applying operating system patches and potentially rebooting the server.
2	Review the Contact Center Service Packs Compatibility and Security Hotfixes Applicability list to determine the most recent Avaya Aura® Contact Center supported patches or service packs.
3	Download the appropriate Microsoft Windows Server 2008 patches for the Avaya Aura® Contact Center software installed on this server.
4	Install the most recent Microsoft Windows Server 2008 service pack that is validated with Avaya Aura® Contact Center by following the Microsoft Installation instructions.

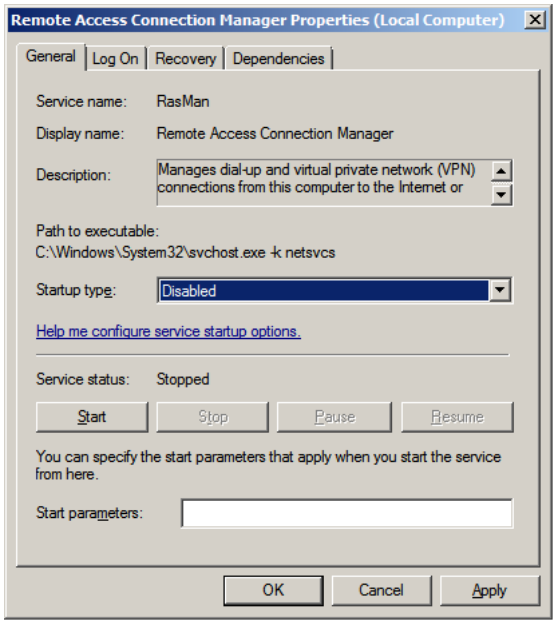
--End--

Disabling the Remote Access services

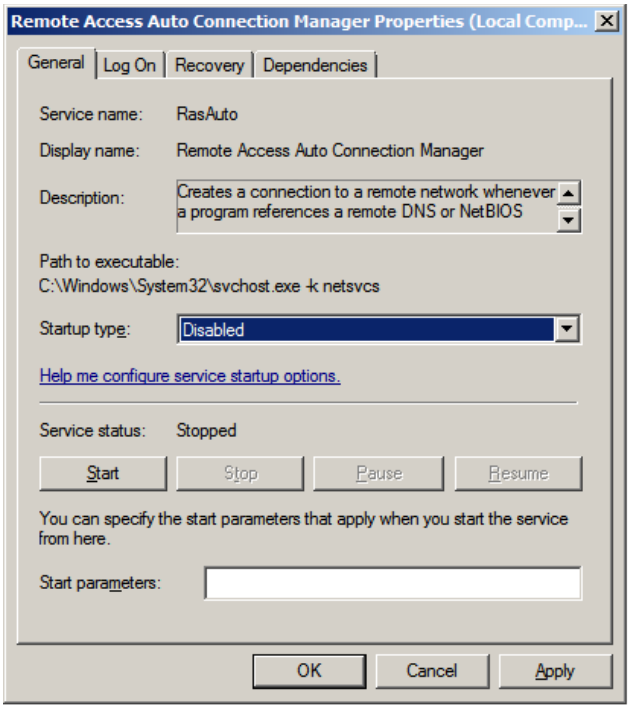
Disable the Remote Access services on the core contact center server, to support Communication Control Toolkit. Microsoft Remote Desktop continues to run after you disable Remote Access services. After you disable the services, restart the server.

Procedure steps

Step	Action
1	Choose **Start**, **Administrative Tools**, **Services**.
2	In the **Services** window, right-click the **Remote Access Connection Manager** icon.
3	Click **Properties**.
4	In the **General** tab, from the **Startup type** list, select **Disabled**.

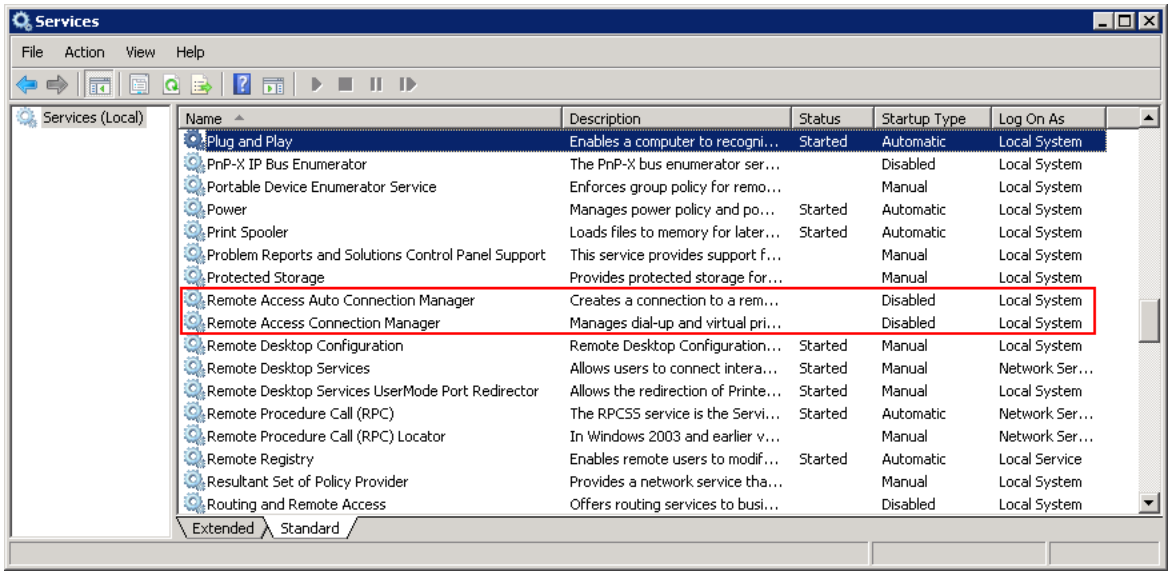


5	Click **OK**.
6	In the **Services** window, right-click the **Remote Access Auto Connection Manager** icon.
7	Click **Properties**.



8 In the **General** tab, from the **Startup type** list, select **Disabled**.

9 Click **OK**.



10 In the **Services** window, click **File**, **Exit**.

11 Restart the server.

--End--

Adding the server to a domain

Add the server to an existing domain. Do this before installing any Contact Center software.

Ask your Domain Administrator to add a Domain Name System (DNS) static entry for this server. Each Contact Center server in a domain requires a DNS static entry.

Attention: Avaya Aura® Contact Center High Availability solutions do not support Windows Server 2008 Dynamic DNS.

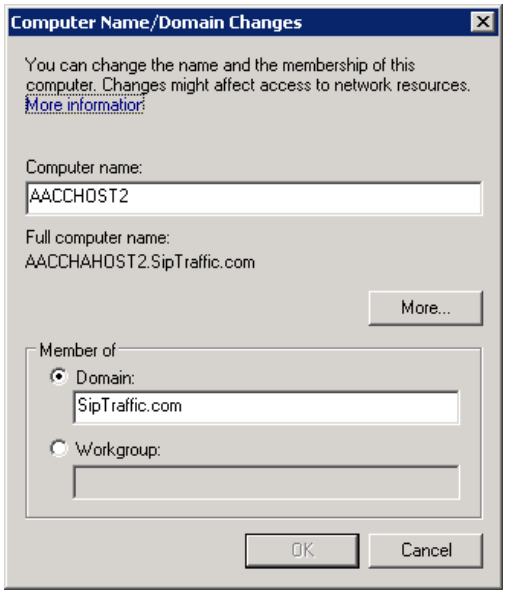
In High Availability solutions, ask your Domain Administrator to add one DNS static entry for each managed name and associated managed IP address. A typical High Availability campus solution with a pair of Voice and Multimedia Contact Server servers requires three DNS static entries; one DNS static entry for the active server, one DNS static entry for the standby server, and one DNS static entry for the managed name and associated IP address.

Prerequisites

- On this server, configure a preferred Domain Name System (DNS) server on the Network Interface Card (NIC).

Procedure steps

Step	Action
1	Log on to the server using an administrator account.
2	Click **Start**, **Administrative Tools**, **Server Manager**.
3	Beside **Computer Information**, click **Change System Properties**.
4	In the **System Properties** dialog box, click the **Computer Name** tab.
5	Click **Change**.
6	In the **Computer Name/Domain Changes** dialog box, select the **Domain** option.
7	Type the domain name (you must provide the fully qualified domain name, which includes the prefix and suffix), for example type siptraffic.com.
8	Click **OK**.
9	Type the domain administrator **User name** and **Password**.



10 Click **OK**.

11 Restart the server when the system prompts you to do so.

--End--

Downloading the most recent patches to the server

To ensure that you have the most current software, download the most recent Contact Center patches from www.avaya.com/support to each server.

Procedure steps

Step	Action
1	Log on to the server using an administrator account.
2	Create a folder **ProductUpdates** on the **D:** drive.
3	Download the most recent Contact Center service pack file and save it on the Contact Center server in the **ProductUpdates** folder.
4	Right-click the service pack zip file and select **Extract All** from the context menu.

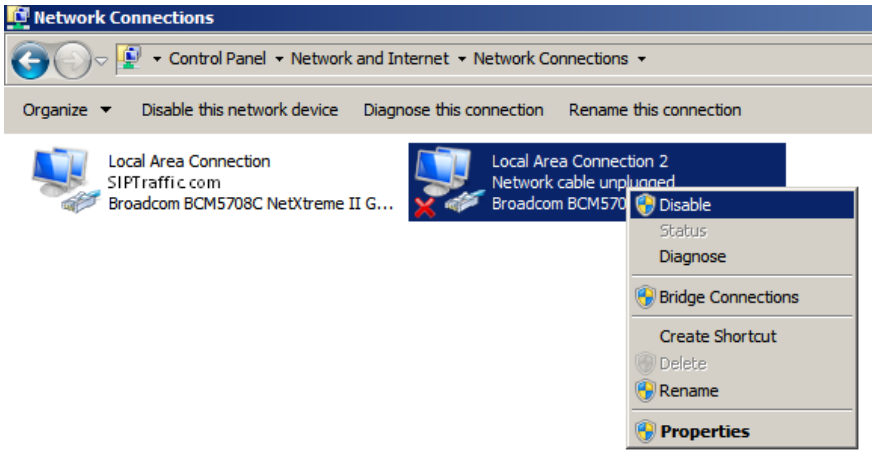
--End--

Disabling unused Network Adapters

Disable all unused Network Adapters or Network Interface Cards (NICs) to improve network communications and prevent the incorrect configuration of unused NICs during Contact Center server commissioning.

Procedure steps

Step	Action
1	Log on to the server using an administrator account.
2	Click **Start**, **Control Panel**, **Network and Internet**, **Network and Sharing Center**, **Change Adapter Settings**.



Step	Action
3	Right-click the unused Network Adapter, and select **Disable**.
4	Repeat this procedure for any unused Network Adapters.

--End--

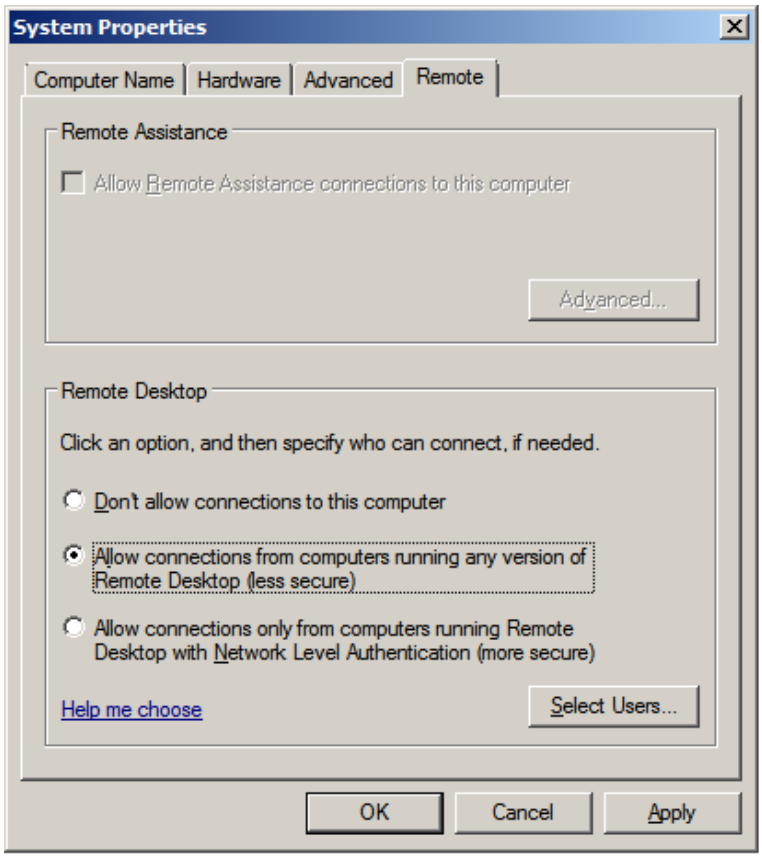
Enabling Microsoft Remote Desktop connection

Enable Microsoft Remote Desktop connection as your remote access tool. Microsoft Remote Desktop provides remote access for personnel supporting the server.

Procedure steps

Step	Action
1	Log on to the server using an administrator account.
2	Choose **Start**, **Control Panel**, **System and Security**.
3	In the **System** section, select **Allow remote access**.
4	Click the **Remote** tab.

5 Select **Allow connections from computers running any version of Remote Desktop (less secure)**.



6 Click **OK**.

--End--

Configuring Data Execution Prevention

Configure the Data Execution Prevention (DEP) hardware and software to perform additional checks on memory that protect the Contact Center server against malicious code exploitation.

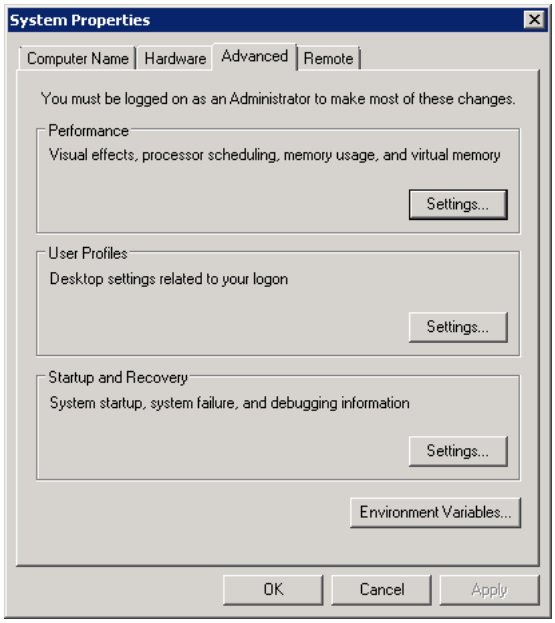
Procedure steps

Step	Action
1	Log on to the server using an administrator account.
2	Choose **Start**, **Control Panel**, **System and Security**.

3 Click **System**.

4 In the **System** window, click **Advanced system settings**.

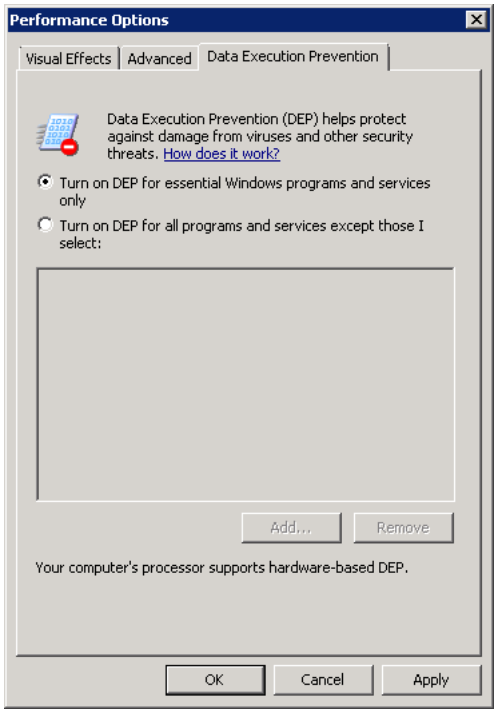
5 In the **System Properties** dialog box, click the **Advanced** tab.



6 Under **Performance**, click **Settings**.

7 In the **Performance Options** dialog box, click the **Data Execution Prevention** tab.

8 On the **Data Execution Prevention** tab, select **Turn on DEP for essential Windows programs and services only**.



9 Click **OK**.

10 On the **System Properties** dialog box, click **OK**.

11 Click **OK** to restart the computer.

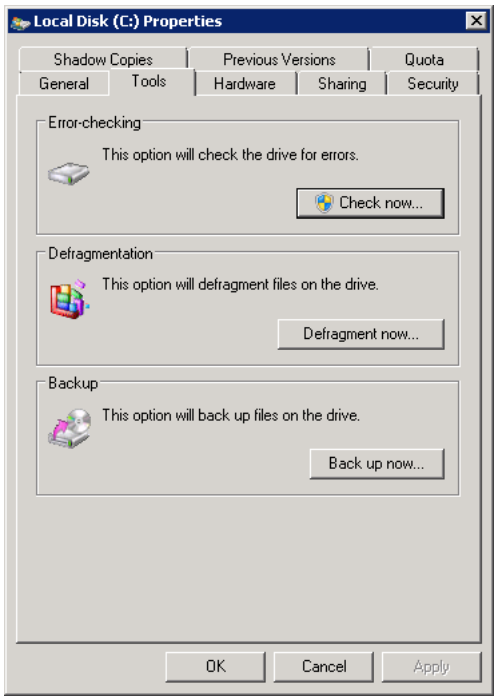
--End--

Scheduling Weekly Disk Defragmentation

Schedule weekly Disk Defragmentation for drive C: and drive D: to optimize performance and avoid potential outages.

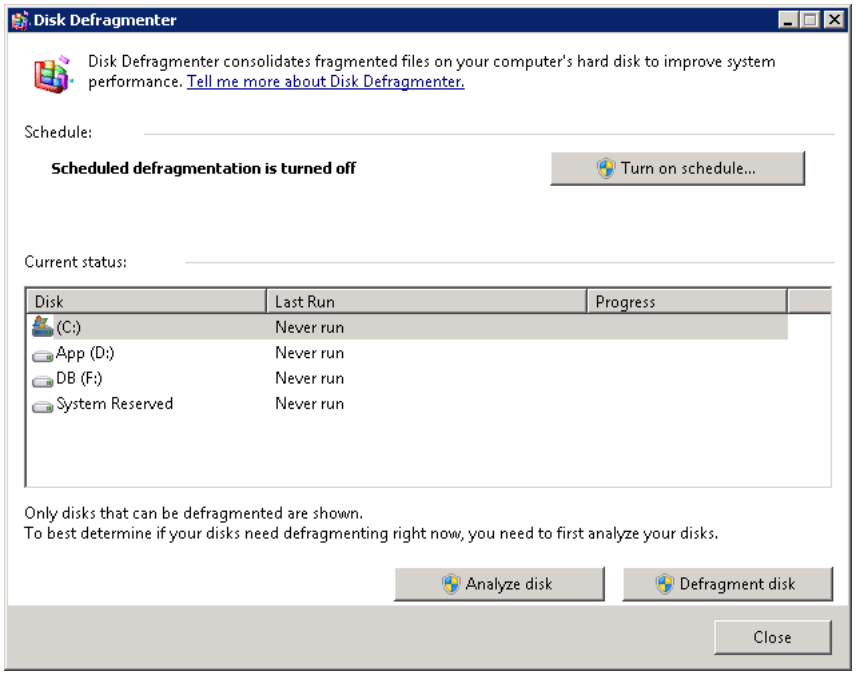
Procedure steps

Step	Action
1	Click **Start**, **Computer**.
2	Right-click drive C: and select **Properties**.
3	Click the **Tools** tab.



4 Select **Defragment Now**.

5 Click **Turn on Schedule**.



6 Select **Run on a schedule (recommended)**.

7 Under **Frequency**, select **Weekly**.

8 Under **Day**, select the day you want to schedule the defragmentation process.

9 Under **Time**, select an off-peak time at which you want to schedule the defragmentation process.

10 Click **Select Disks**.

11 In the **Disk Defragmenter: Select Disks for Schedule** window, select drive C: and drive D:.

12 Click **OK**.

13 Click **OK**.

14 Click **Close**.

15 On the **Properties** dialog box, click **OK**.

--End--

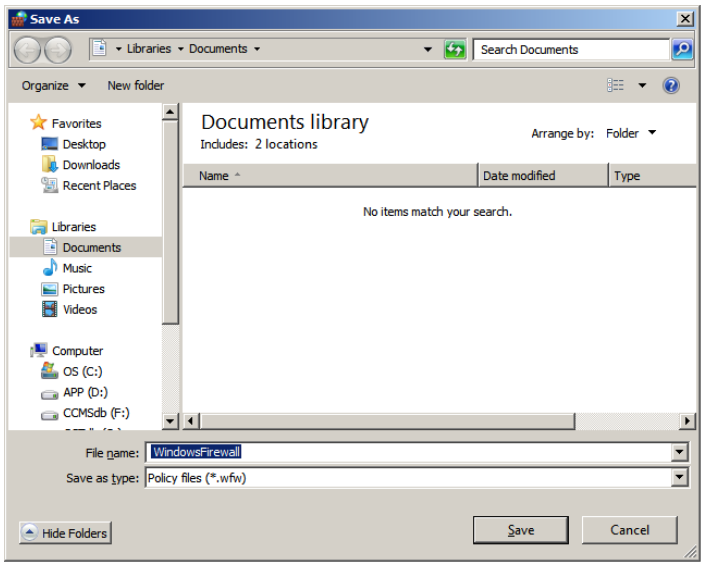
Importing the Contact Center Firewall Security policy

Import the Avaya Aura® Contact Center Firewall Security policy to ensure all contact center servers in the solution can communicate.

Export and backup your existing firewall security policy before importing the Avaya Aura® Contact Center Firewall Security policy. You can use this backup policy to rollback the Avaya Aura® Contact Center Firewall Security policy.

Procedure steps

Step	Action
1	Download the most recent Avaya Aura® Contact Center Firewall Security policy from www.avaya.com/support.
2	Log on to the server using an administrator account.
3	Choose **Start**, **Administrative Tools**, **Windows Firewall with Advanced Security**.
4	Choose **Action**, **Export Policy**.
5	In the **File name** box, type the name for the backup policy, for example type WindowsFirewall.



6 Click **Save**.

Windows exports the existing policy. You can use this backup policy to rollback the Avaya Aura® Contact Center Firewall Security policy, if you ever need to.

7 On the **Policy successfully exported** message box, click **OK**.

8 Choose **Action**, **Import Policy**.

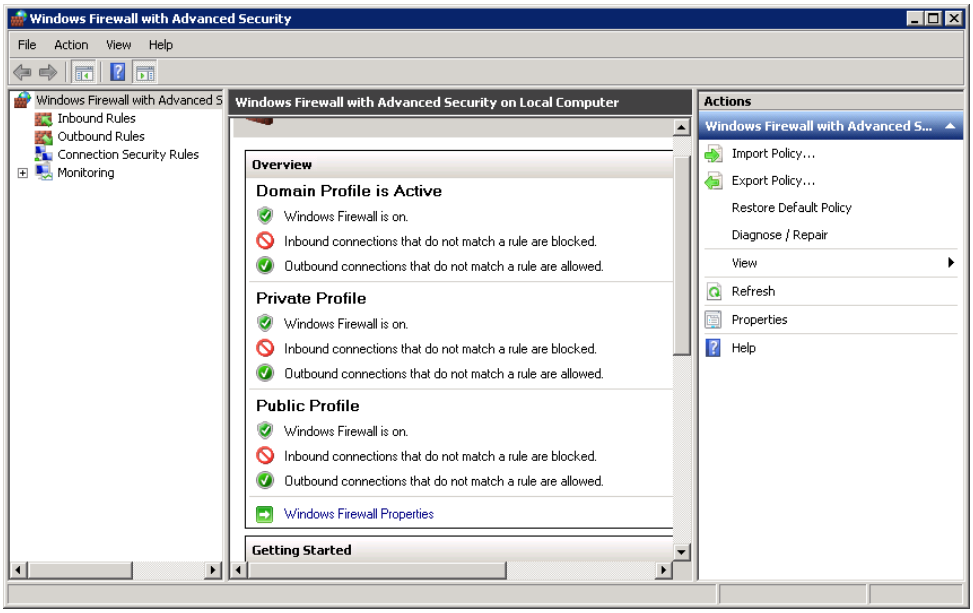
9 On the policy overwrite message box, click **Yes**.

10 Navigate to the folder containing the Avaya Aura® Contact Center Firewall Security policy and select the policy.

11 Click **Open**.

Windows imports the Avaya Aura® Contact Center Firewall Security policy.

12 On the **Policy successfully imported** message box, click **OK**.



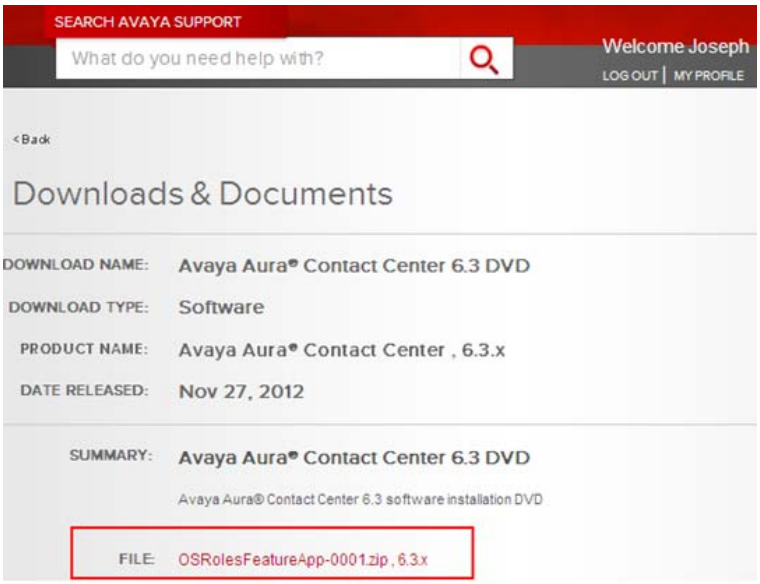
--End--

Downloading the Roles and Features Installer

The Avaya Aura® Contact Center Roles and Features Installer utility configures your Windows Server 2008 operating system. You must download the Roles and Features Installer from the support Web site http://support.avaya.com.

Procedure steps

Step	Action
1	Log on to http://support.avaya.com.
2	Navigate to the Avaya Aura® Contact Center Release 6.3.x section of the Avaya Support Web site.
3	Under Downloads and Documents, click on the file to download the Avaya Aura® Contact Center Roles and Features Installer.



4 Save the OSRolesFeatureApp-0001 folder to a location on your server.

--End--

Installing the required Windows roles and features

The Avaya Aura® Contact Center Roles and Features Installer is a new utility that configures your Windows Server 2008 operating system. The Roles and Features Installer installs the following required Windows Server 2008 roles and features:

- Active Directory Lightweight Directory Services
- Application Server
- Web Server (IIS)
- SNMP Services
- Windows Server Backup Features

Prerequisites

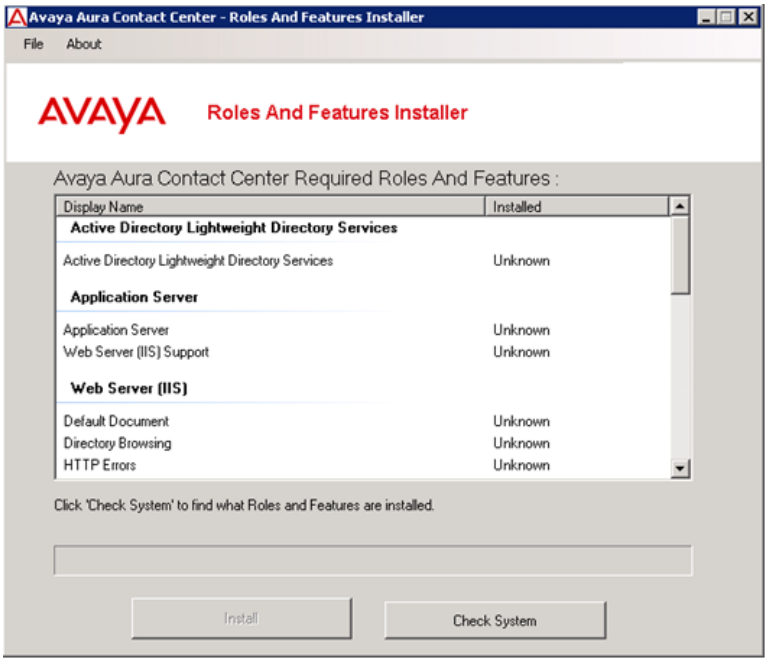
- Download the Avaya Aura® Contact Center Roles and Features Installer from the Avaya support website and save the application to a location on your server.

Procedure steps

Step	Action
1	Log on to the server.
2	Open the OSFeatureRolesApp-0001 folder.

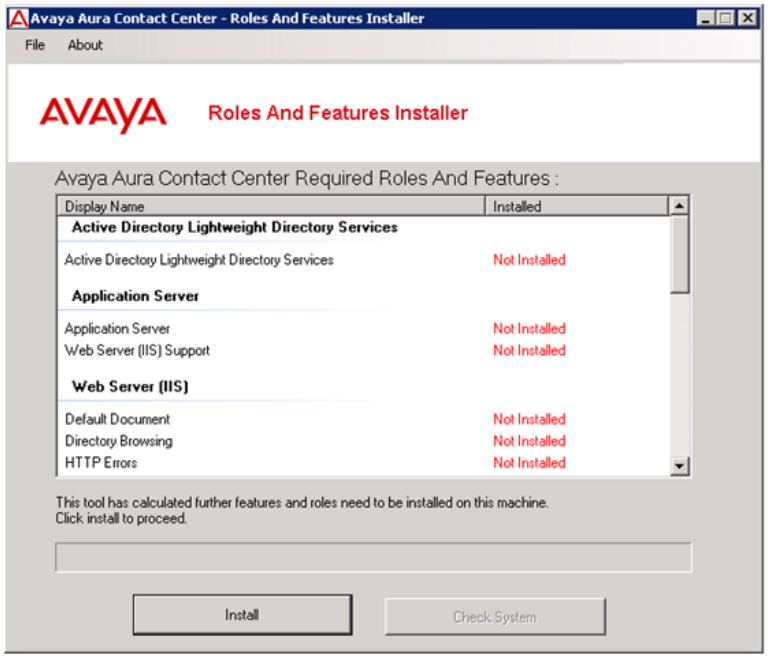
3 Open the APP folder and double-click **InstallWindowsFeatures**.

The Avaya Aura® Contact Center Roles and Features Installer appears.



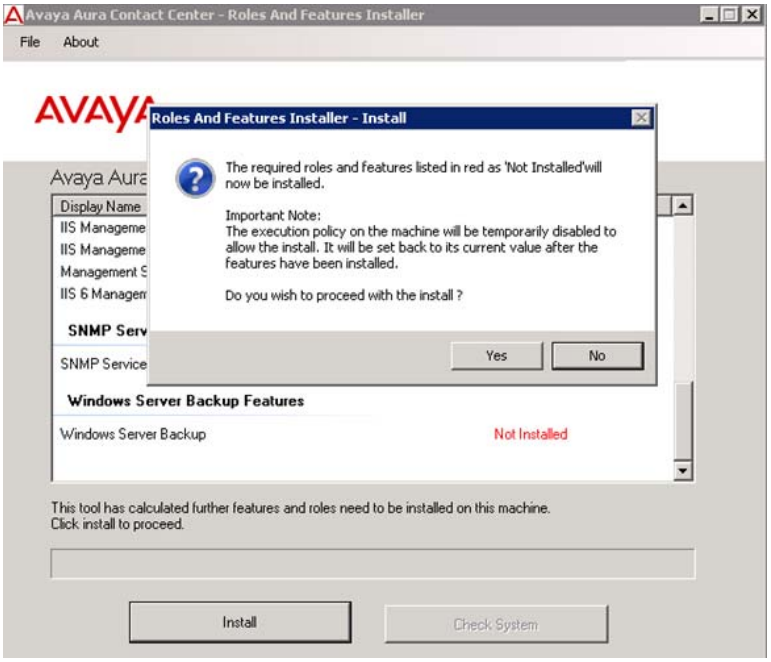
4 Click **Check System**.

The Avaya Aura® Contact Center Roles and Features Installer checks if the required roles and features are installed.



5 If all of the required roles and features are not installed, click **Install**.

6 Click **Yes**.



7 After the installation is complete, click **OK**.

--End--

Configuring Windows Server 2008

Before you install Contact Center software on your server, create a repair disk and back up the operating system configuration.

Prerequisites

- Install Microsoft Windows Server 2008 64-bit Release 2 on your server.

Procedure steps

Step	Action
1	Log on to the Windows Server 2008 server using an administrator account.
2	Select the **Don't display this screen on startup** check box.
3	Choose **Start**, **All Programs**, **Accessories**, **System Tools**, **Windows Server Backup**.
4	Follow the on-screen instructions to select what files you want to back up.

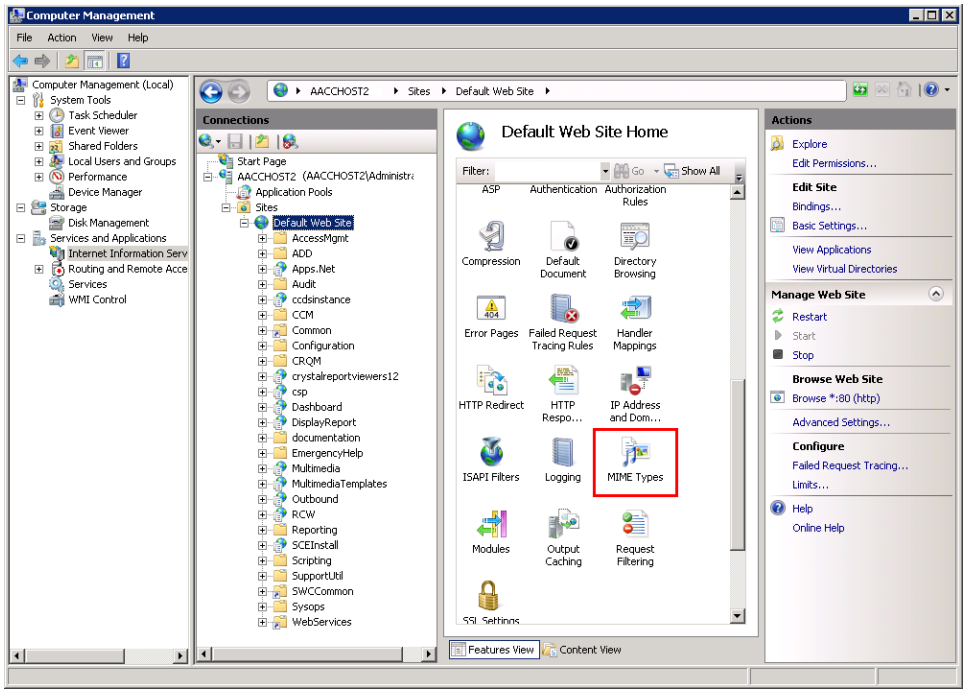
--End--

Configuring MIME types to support Microsoft updates

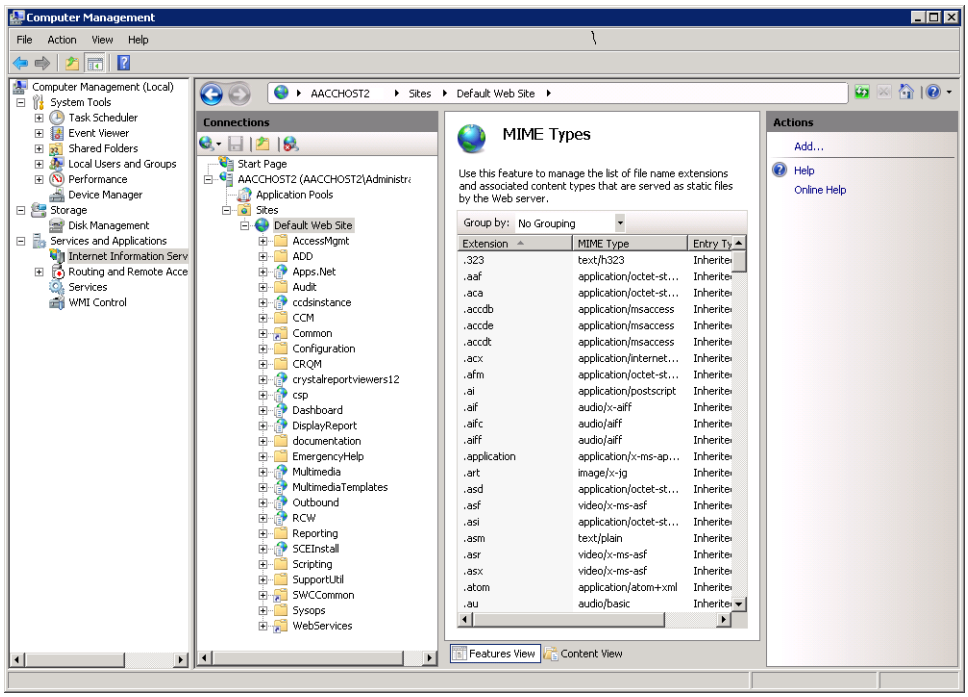
Configure the Multipurpose Internet Mail Extension (MIME) types to support Microsoft updates and patches.

Procedure steps

Step	Action
1	Log on to the server using an Administrator account.
2	Click **Start**, **Administrative Tools**, **Computer Management**.
3	In the **Computer Management** dialog box, expand **Services and Applications**, **Internet Information Services (IIS Manager)**.
4	Under **Connections**, expand **AACCHOST2**, **Sites**, **Default Web Site**.
5	Select **Default Web Site**.



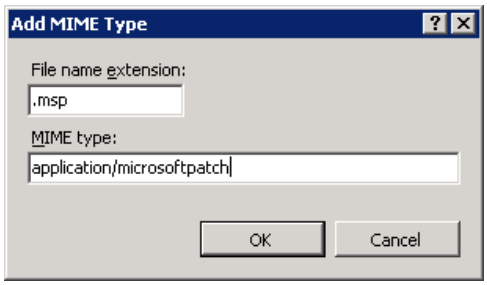
6 In the **Default Web Site Home** pane, under **IIS**, double-click **MIME Types**.



7 On the **Actions** list in the right pane, click **Add**.

8 In the **File name extension** box, type **.msp**.

9 In the **MIME Type** box, type **application/microsoftpatch**.

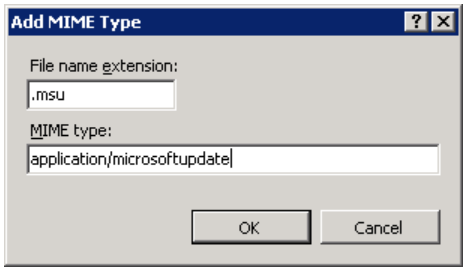


10 Click **OK**.

11 On the **Actions** list in the right pane, click **Add**.

12 In the **File name extension** box, type **.msu**.

13 In the **MIME Type** box, type **application/microsoftupdate**.

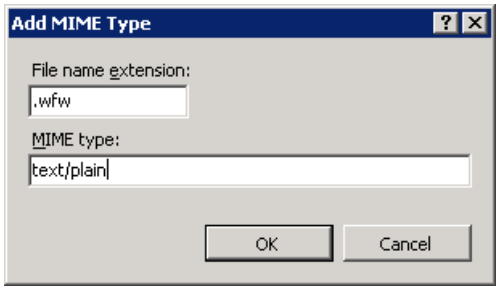


14 Click **OK**.

15 On the **Actions** list in the right pane, click **Add**.

16 In the **File name extension** box, type **.wfw**.

17 In the **MIME Type** box, type **text/plain**.



18 Click **OK**.

19 Close the **Computer Management** window.

--End--

Adding the domain AD-LDS replication account to the backup administrators and replicator group

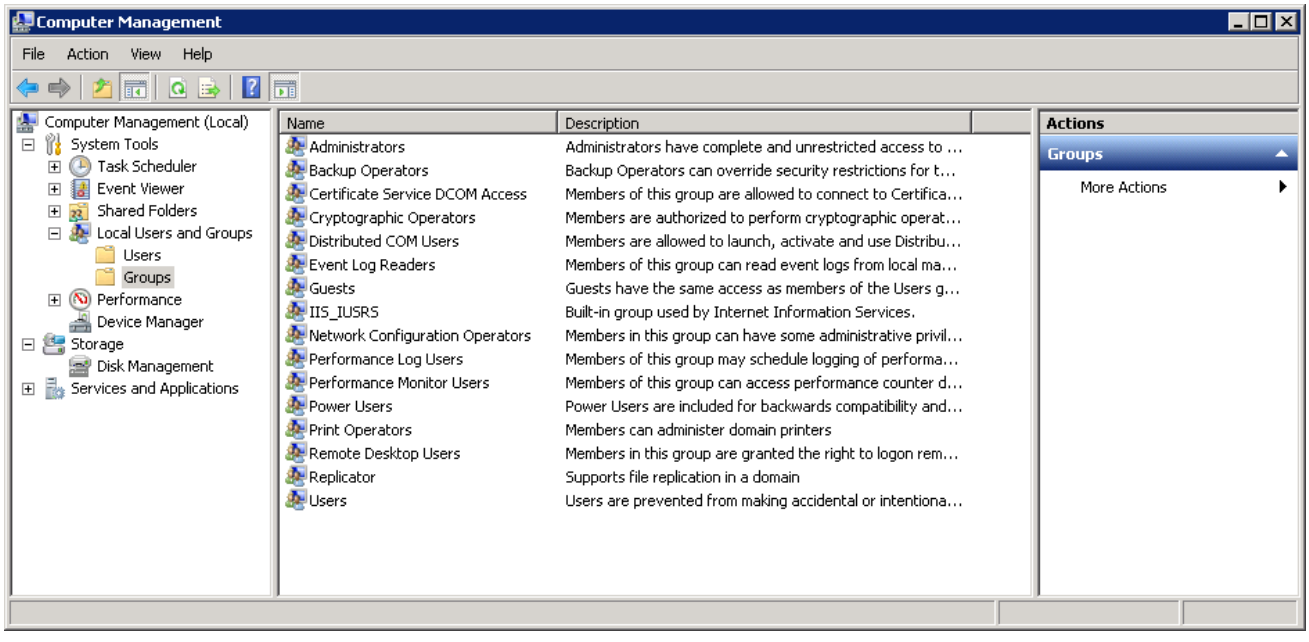
Add the AD-LDS replication account to the local Administrators and replicator group on the backup CCMA server.

Request this AD-LDS replication account from your Network or Domain Administrator. The primary and standby replicating Contact Center Manager Administration servers must both be added to the same domain.

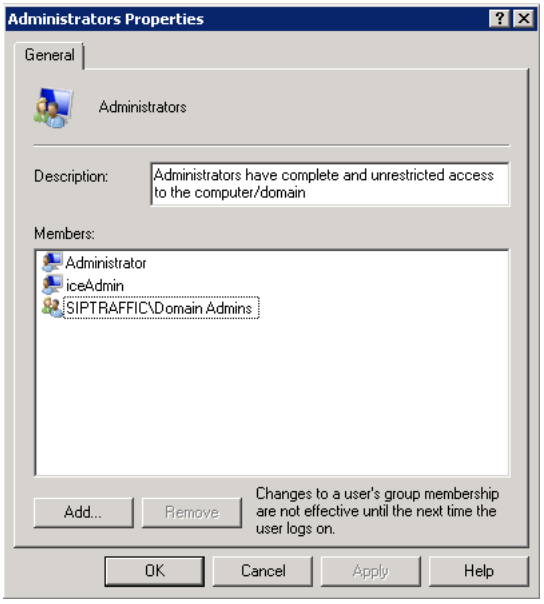
For this procedure, the name of the AD-LDS replication account is "siptraffic\AACCReplication". You can choose another name for the account.

Procedure steps

Step	Action
1	Log on to the standby server.
2	Click **Start**, **Administrative Tools**, **Computer Management**.
3	In the **Computer Management** window, expand **Local Users and Groups**.
4	Click the **Groups** folder.

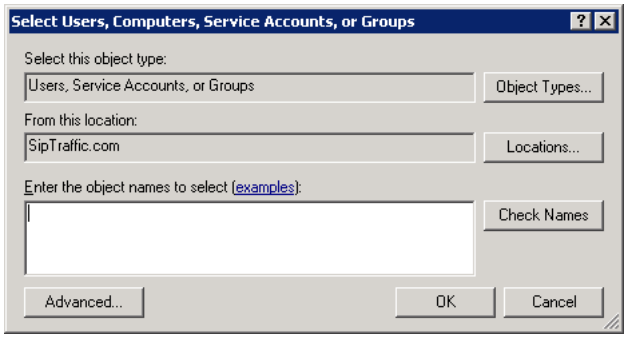


5 Double-click on **Administrators** group.

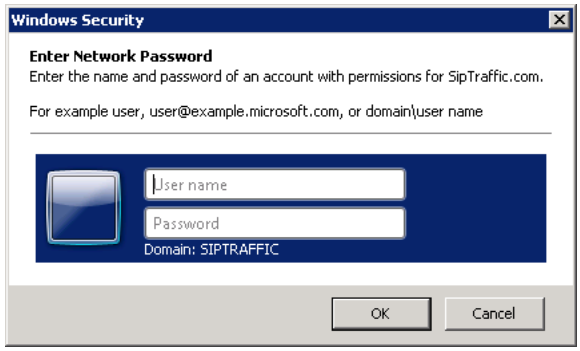


6 On the **Administrators Properties** window, click **Add**.

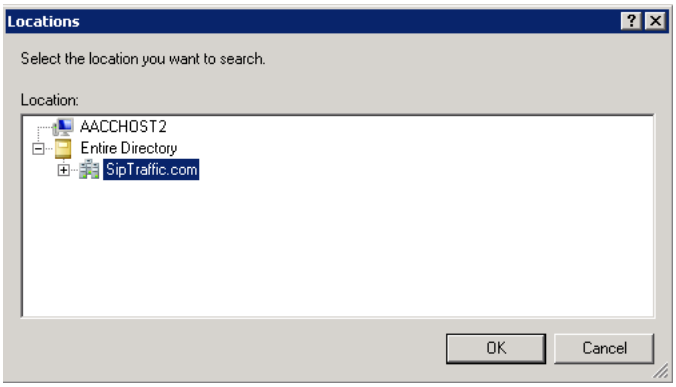
7 On the **Select Users, Computers, Service Accounts, or Groups** window, **click Locations**.



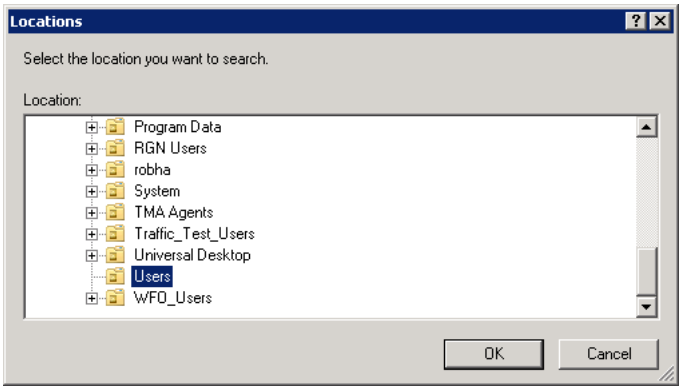
8 If a **Windows Security** dialog box appears, type a domain user account name and password for the domain.



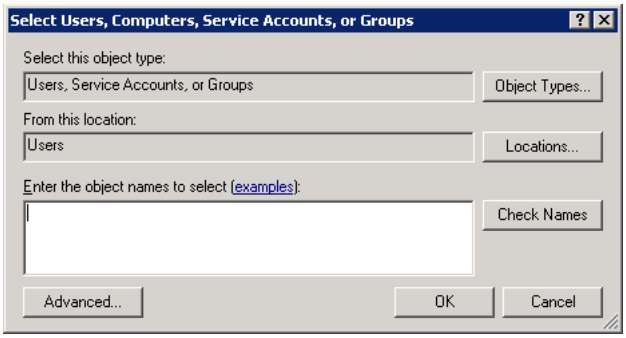
9 On the **Locations** dialog, select the domain to be used by CCMA replication, for example siptraffic.com.



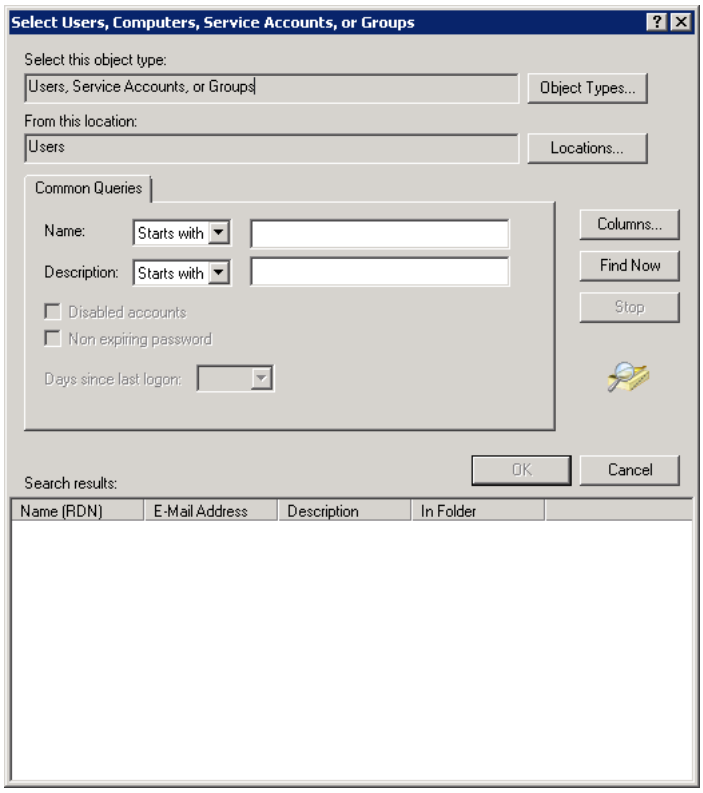
10 Expand the domain folder, scroll down and select **Users**.



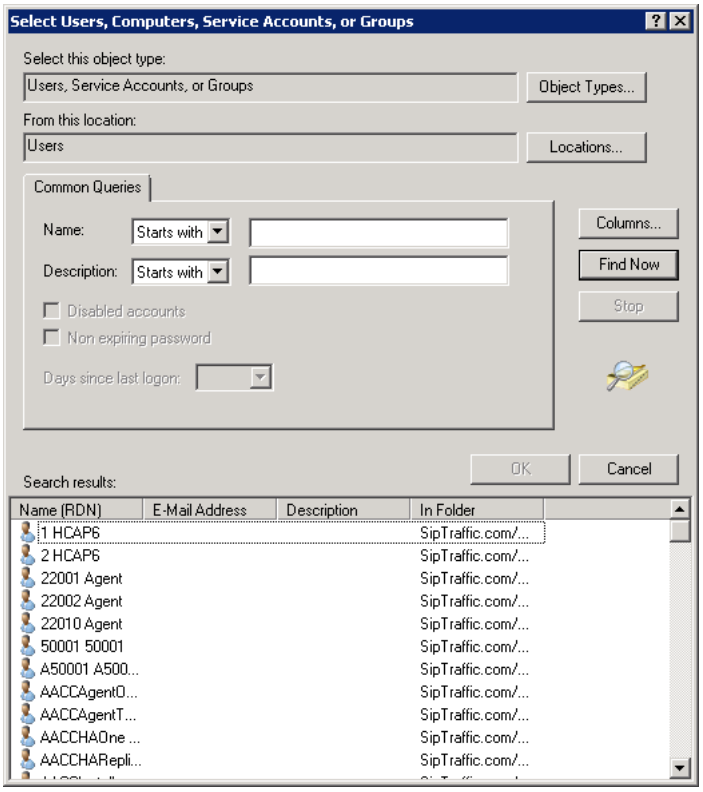
11 Click **OK**.



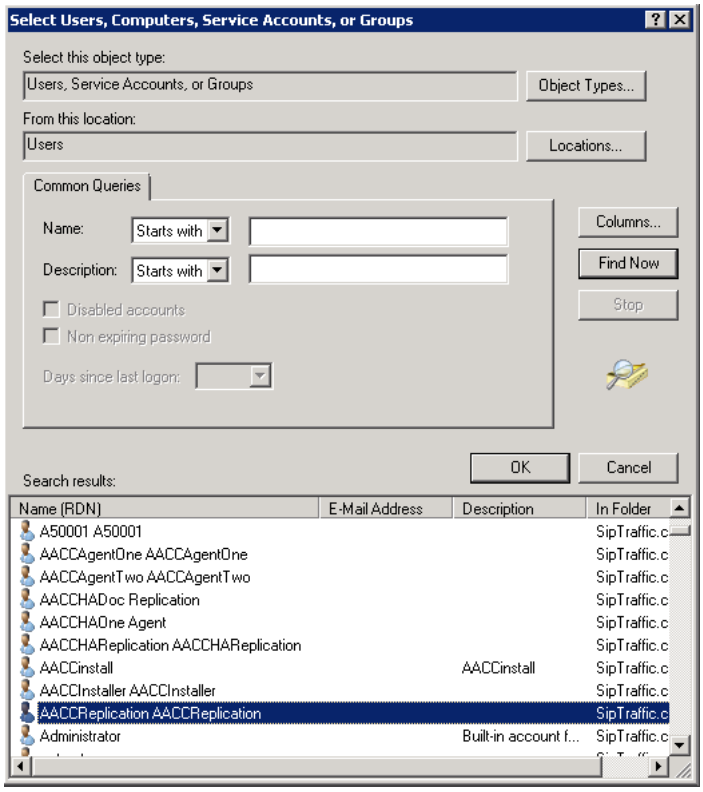
12 Click **Advanced**.



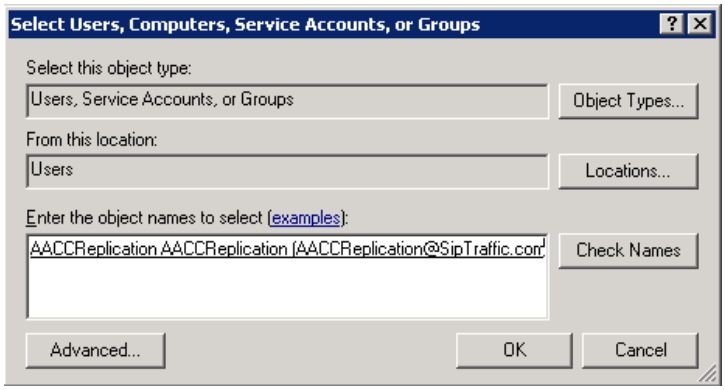
13 Click **Find Now**, to display domain users.



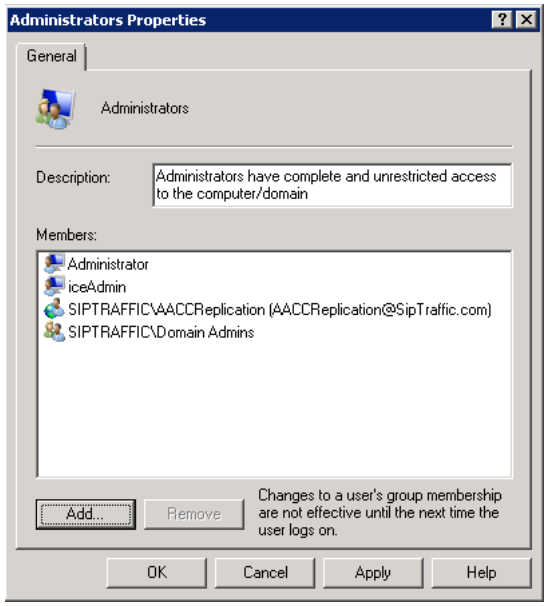
14 From the list of users select the CCMA replication domain user account, for example select the "siptraffic\AACCReplication" user account.



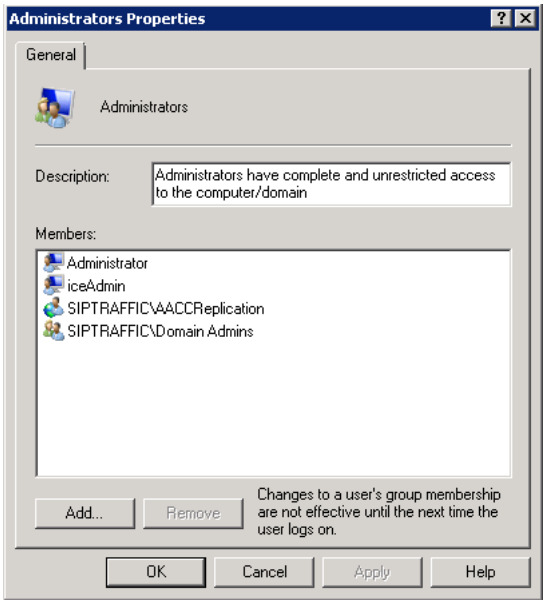
15 Click **OK**.



16 Click **OK**.

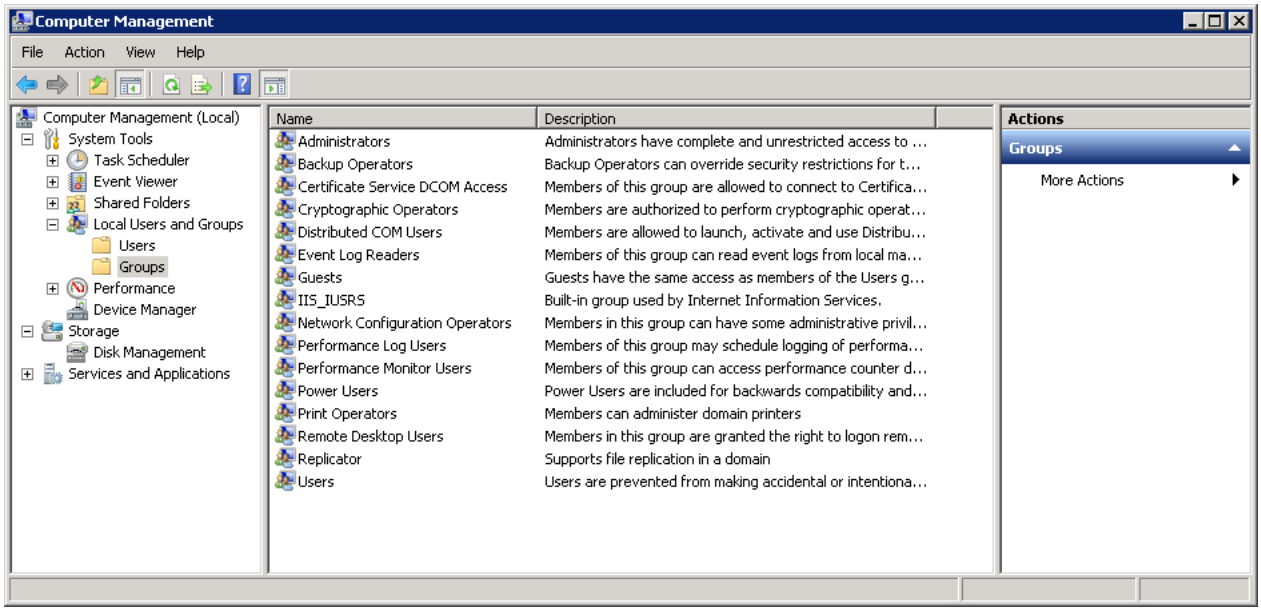


17 Click **Apply**.

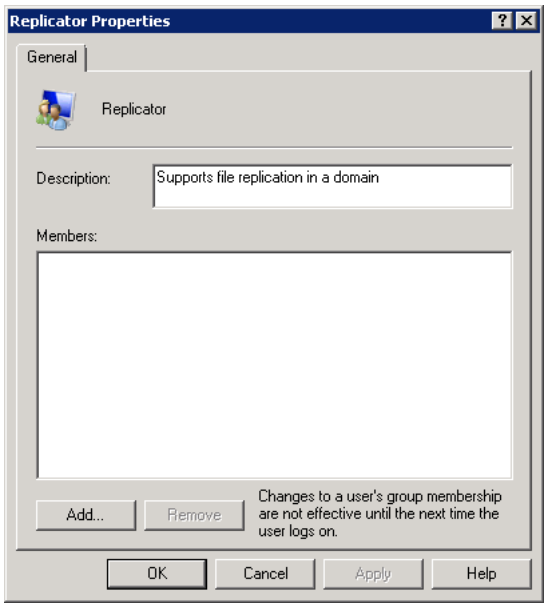


18 Click **OK**.

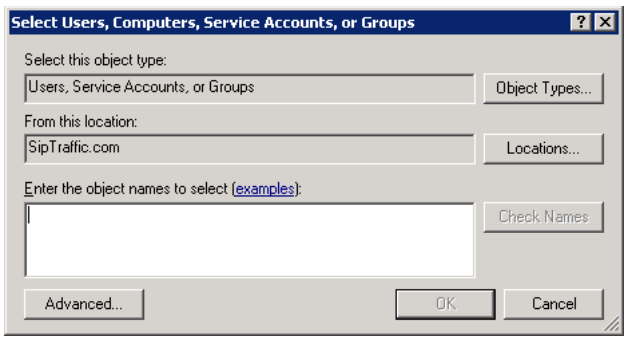
19 Click the **Groups** folder.



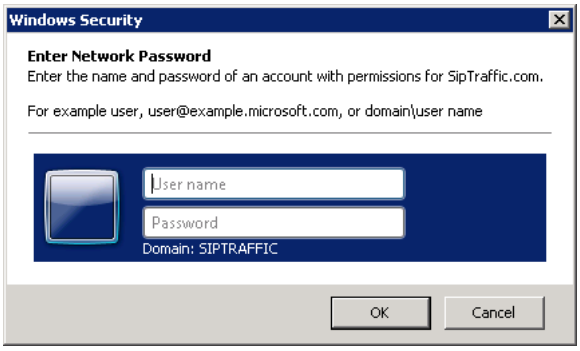
20 Double-click on **Replicator** group.



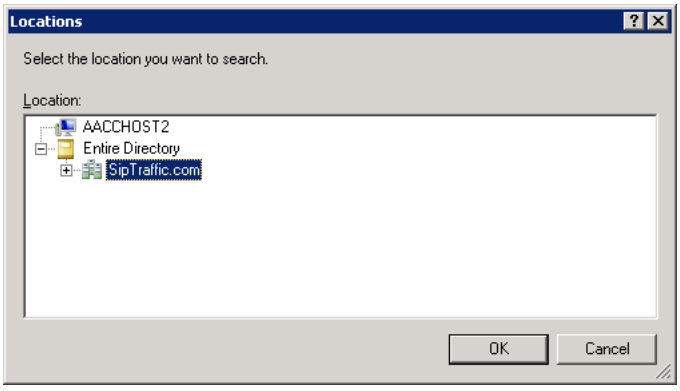
21 Click **Add**.



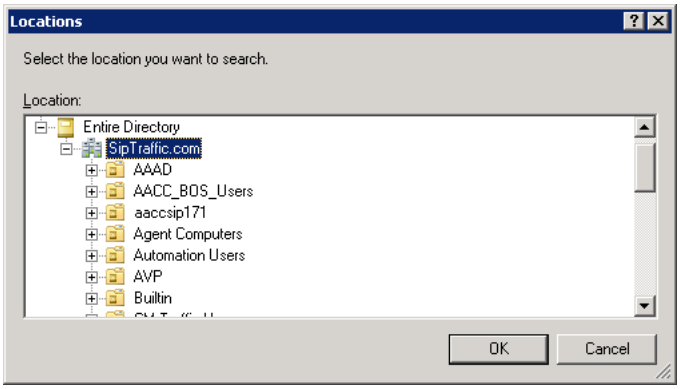
22 Click **Locations**.



23 If a **Windows Security** dialog box appears, type the domain account logon details.

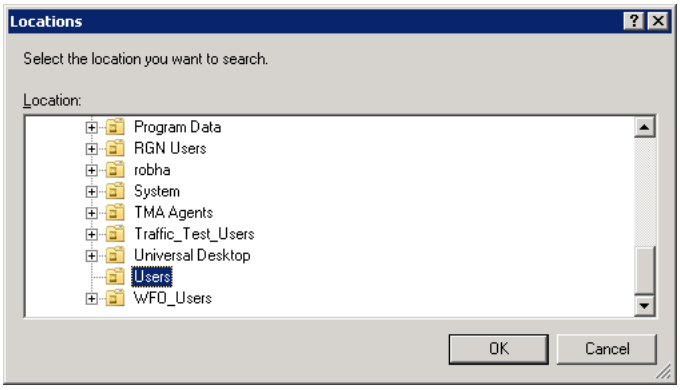


24 On the **Locations** dialog, select the domain to be used by CCMA replication. For example, select siptraffic.com.

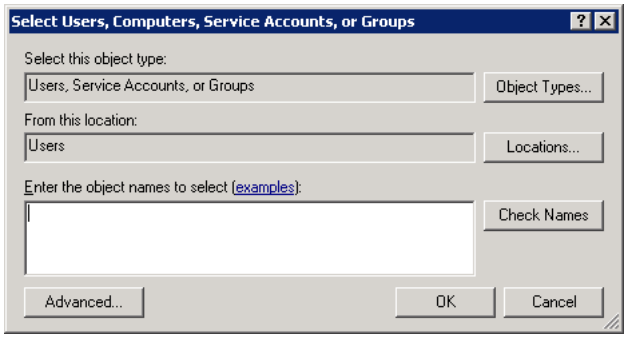


25 Expand the domain folder to display domain users.

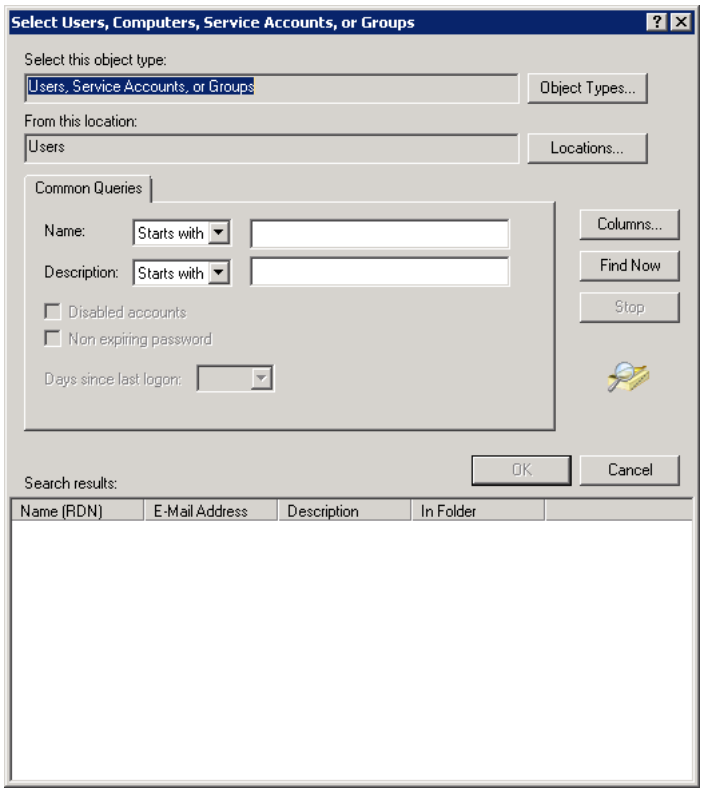
26 Click **Users**.



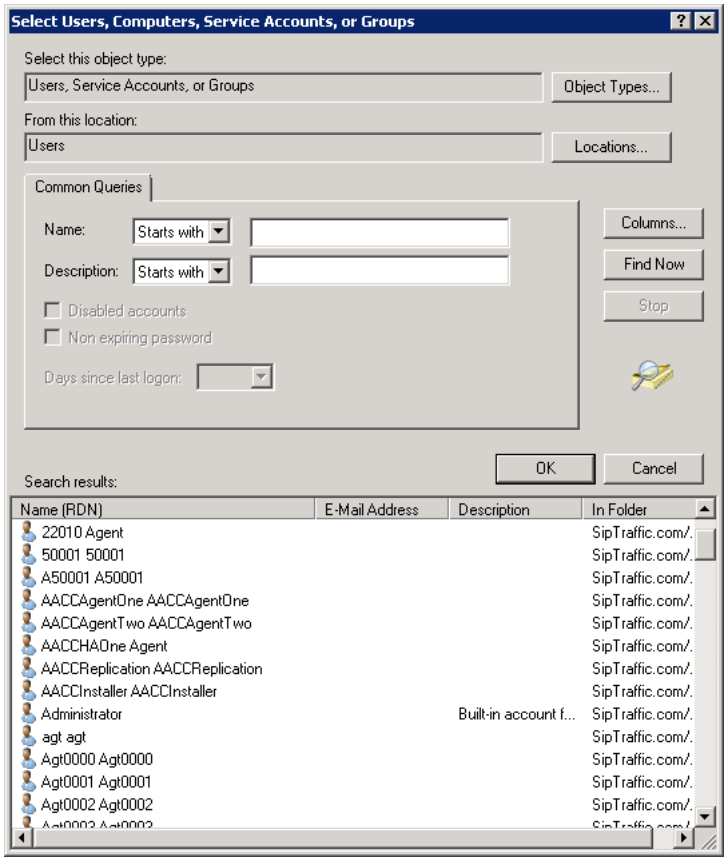
27 Click **OK**.



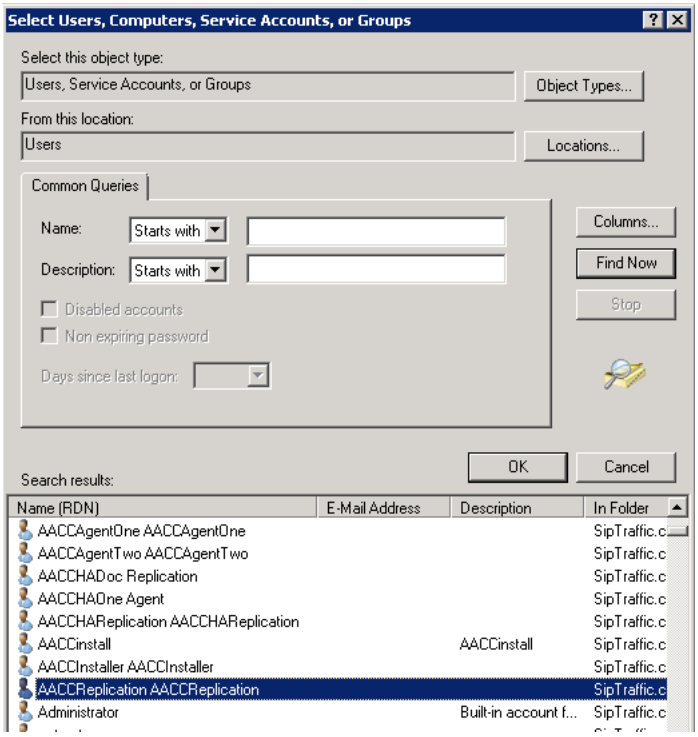
28 Click **Advanced**.



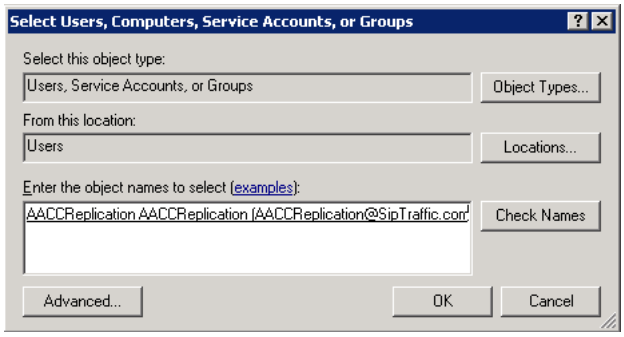
29 Click **Find Now**, to display domain users.



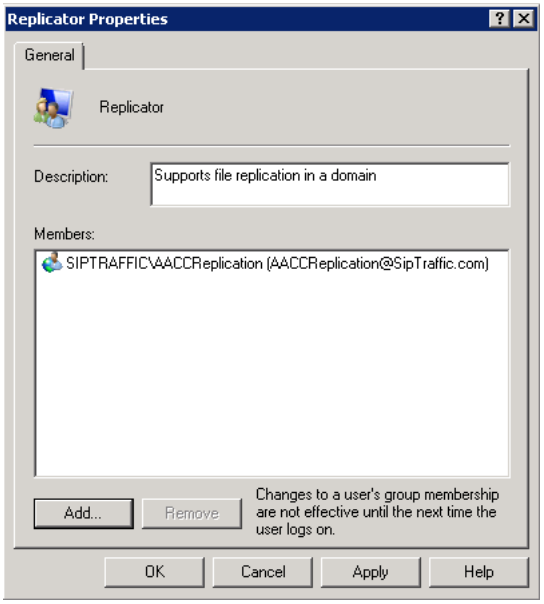
30 From the list of users select the CCMA replication domain user account. For example select the "siptraffic\AACCReplication" domain user account.



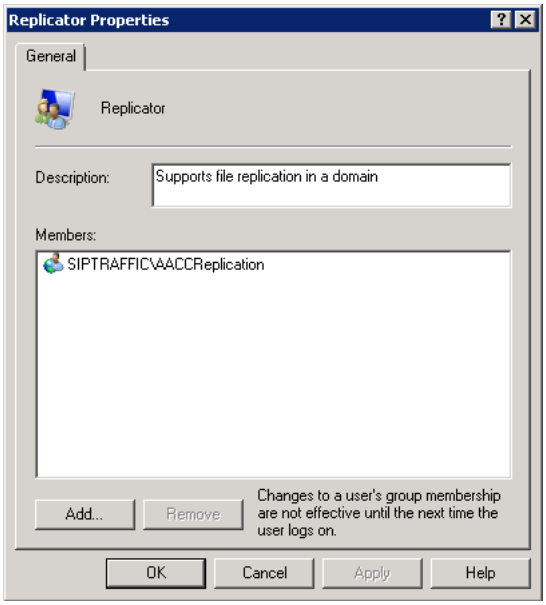
31 Click **OK**.



32 Click **OK**.



33 Click **Apply**.



34 Click **OK**.

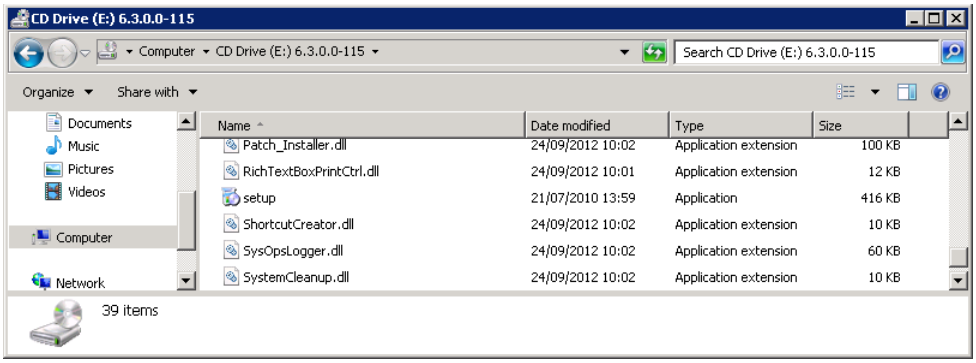
--End--

Installing the standby Voice and Multimedia Contact Server software

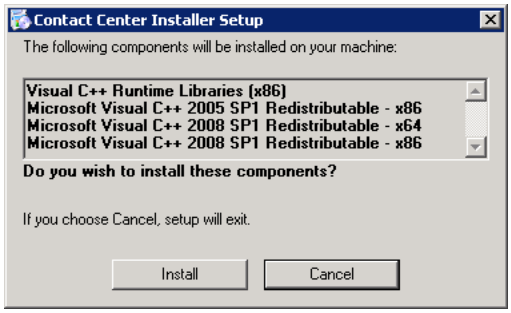
Install the Voice and Multimedia Contact Server software on the standby server. You must install the same Contact Center applications as installed on the active Voice and Multimedia Contact Server.

Procedure steps

Step	Action
1	Log on to the standby server using an administrator account.
2	Insert the Contact Center DVD into the DVD drive of your server.
3	If the installation does not automatically start, double-click **Setup.exe**.

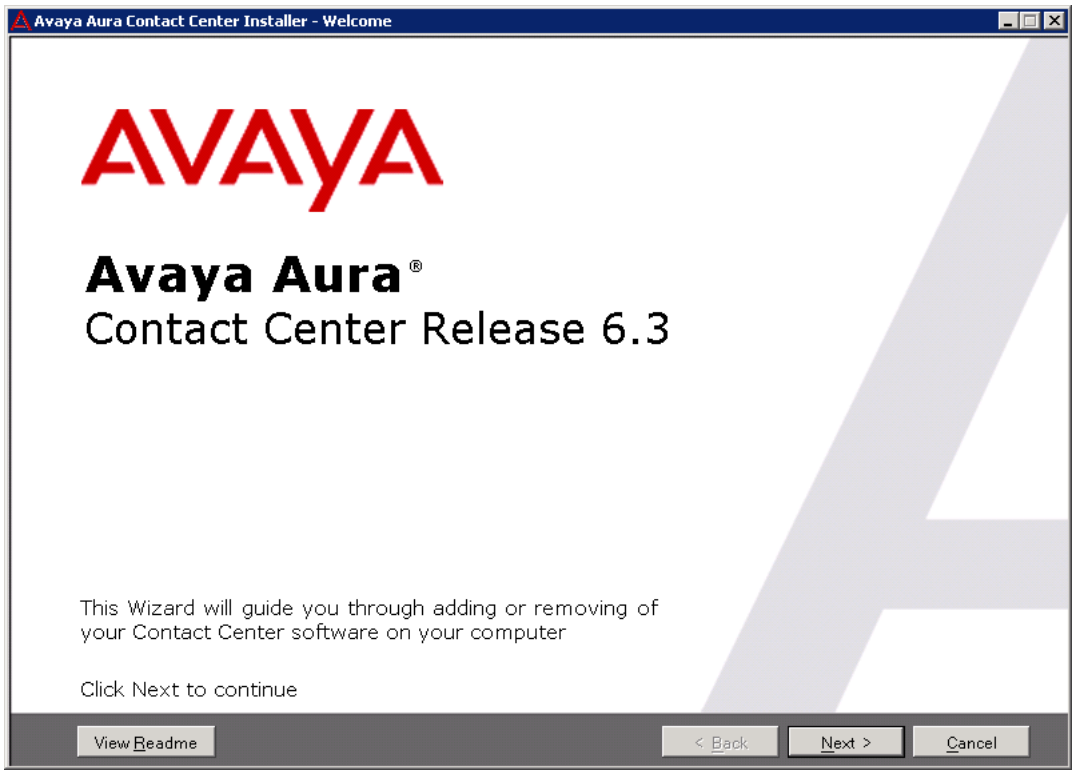


4	Click **Install** to install the Visual C++ runtime libraries on the server.



If you are prompted to restart the server, click **Yes** and repeat step 3.

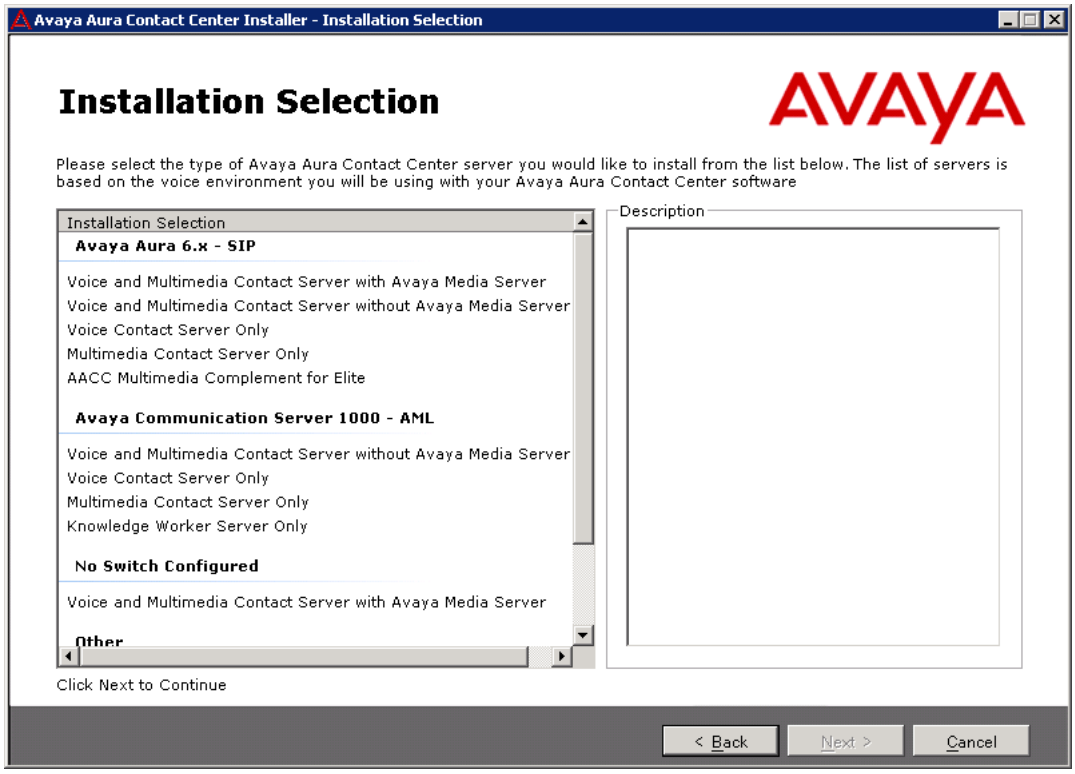
5	On the **Welcome** window, click **Next**.



6 On the **License Agreement** window, read the terms of the agreement.

7 Click **I ACCEPT the Terms of the End-User License Agreement**.

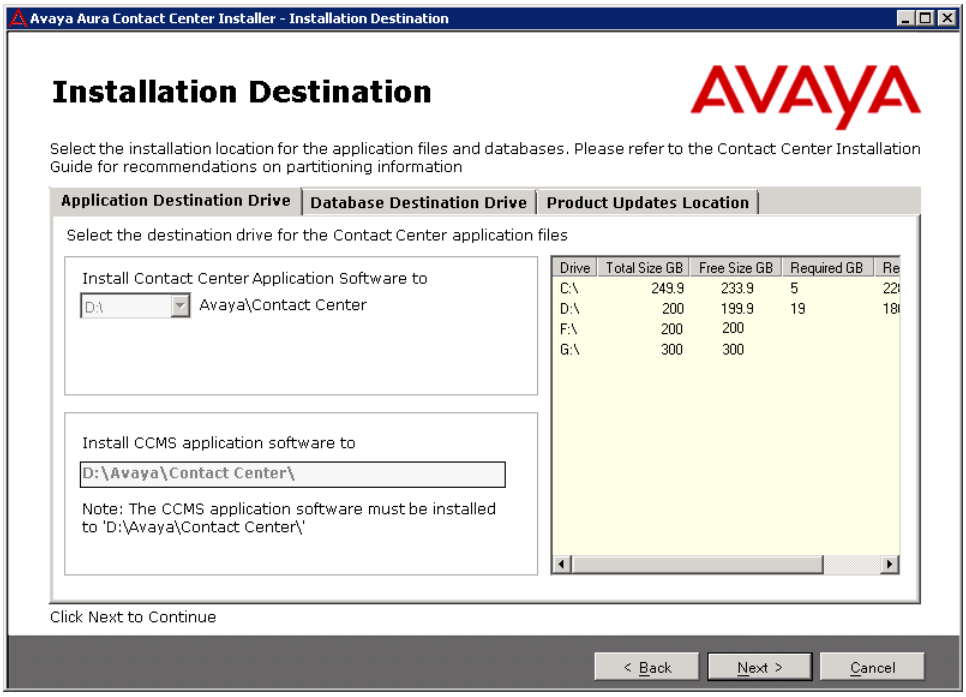
8 Click **Next**.



9 On the **Installation Selection** window, under **Avaya Aura 6.x - SIP**, select **Voice and Multimedia Contact Server without Avaya Media Server**.

10 Click **Next**.

11 On the **Installation Destination** window, on the **Application Destination Drive** tab, from the **Install Contact Center Application Software to** list, select **D:**.

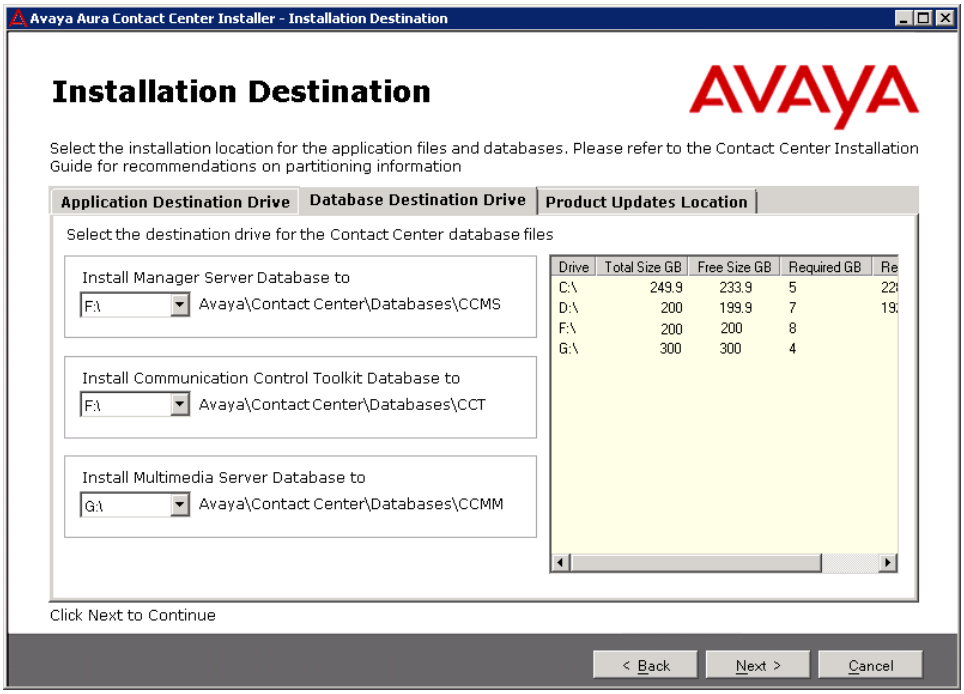


12 Click the **Database Destination Drive** tab.

13 From the **Install Manager Server Database to list**, select the drive for the Contact Center Manager Server database. select **F:**.

14 From the **Install Communication Control Toolkit Database to** list, select **F:**.

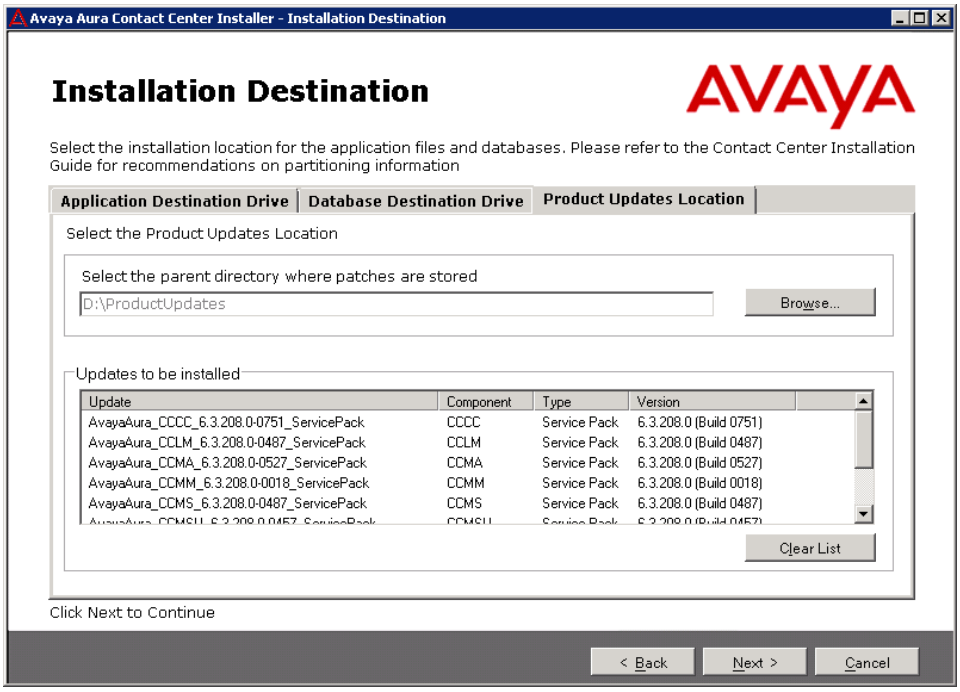
15 From the **Install Multimedia Server Database to** list, select **G:**.



16 Click the **Product Updates Location** tab.

17 Under **Select the parent directory where patches are stored**, click **Browse**.

18 Select the **D:\ProductUpdates** folder.



19 Click **Next**.

The System Readiness Check runs on the server.

20 If you have followed the previous instructions in this guide, the **System Readiness Checks** returns a Pass.

You can ignore warnings, if you understand the potential impact to the operation of the contact center and decide it is not applicable.

21 Click **Next**.

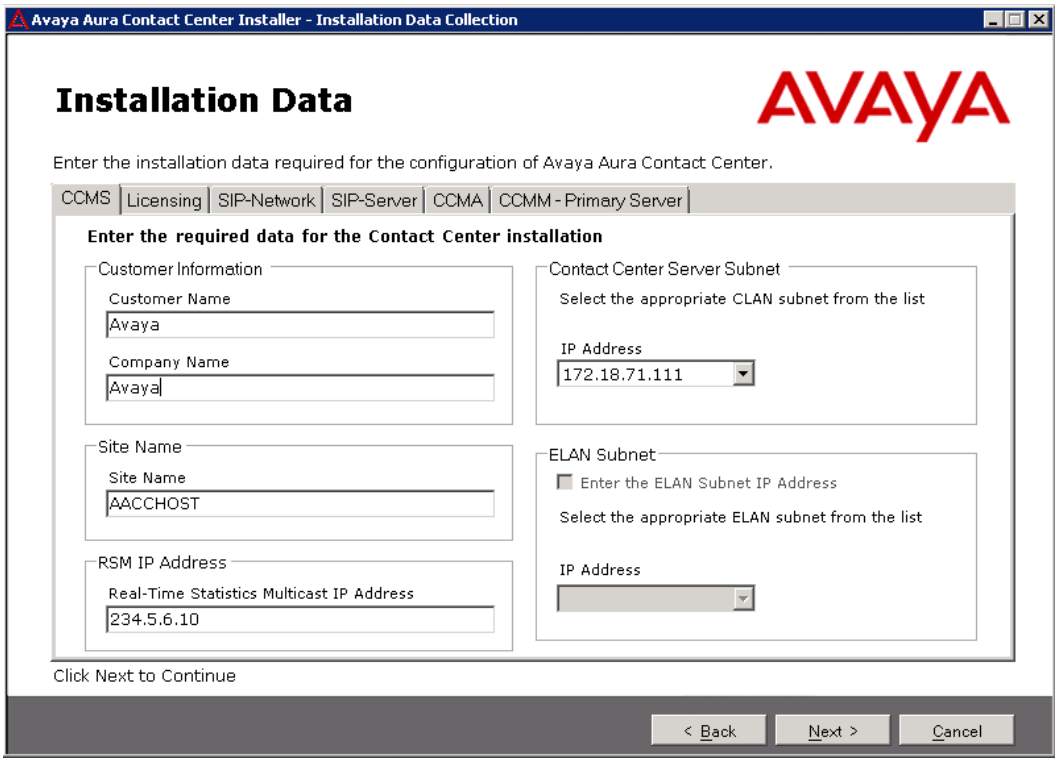
22 On the **Installation Data** window, select the **CCMS** tab. Complete the fields as follows:

Customer Name — Type the name of the contact center company, for example Avaya.

Company Name — Type the name of the contact center company, for example Avaya.

Site Name — Type the name of site, for example AACCHOST. The site name of the standby server must match the site name of the active server. Do not enter the active server name or the standby server name here. The site name must not contain spaces or nonalphabetical characters except hyphen (-) and underscore (_). The first character must be a letter. The site name can consist of 6 to 15 characters.

Contact Center Server Subnet IP Address — Select the standby Voice and Multimedia Contact Server IP address, for example 172.18.71.111.



23 Select the **Licensing** tab.

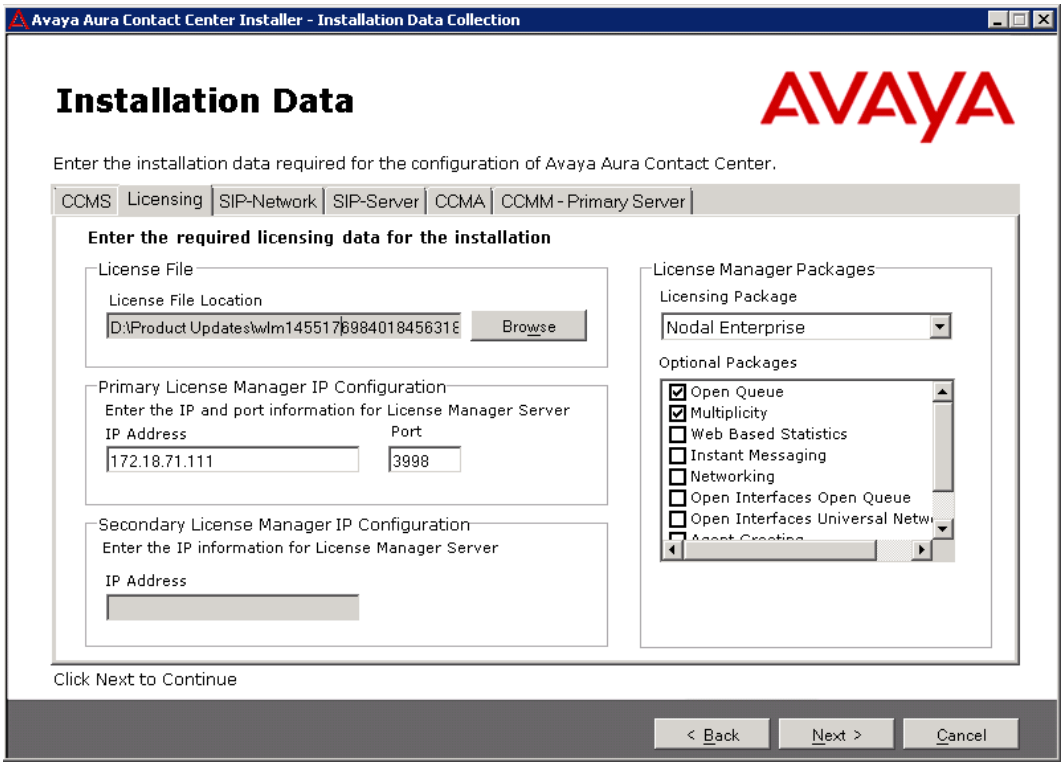
24 Complete the **Licensing** tab fields as follows:

License File Location — Use the **Browse** button to find and select the license file that you downloaded to the server. This sample solution uses a WebLM license file obtained from the Avaya Product Licensing and Delivery System (PLDS).

IP Address — Type the IP address of the license server, in this case the Voice and Multimedia Contact Server, for example 172.18.71.111.

CCMS Package List — Select **Nodal Enterprise**.

Optional Packages — Select **Open Queue** and **Multiplicity**.

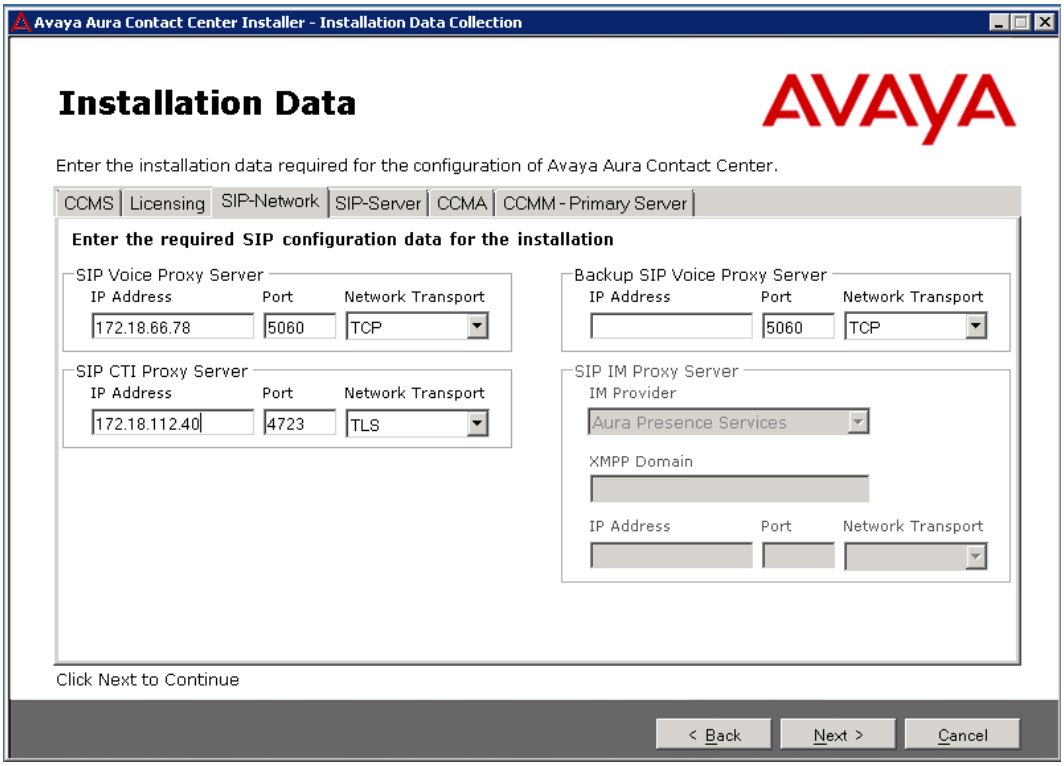


25 Select the **SIP-Network** tab.

26 Complete the **SIP-Network** tab fields as follows:

SIP Voice Proxy Server - IP Address — Type the IP address of the Session Manager SIP entity, for example 172.18.66.78.

SIP CTI Proxy Server - IP Address — Type the IP address of the Application Enablement Server, for example 172.18.112.40.



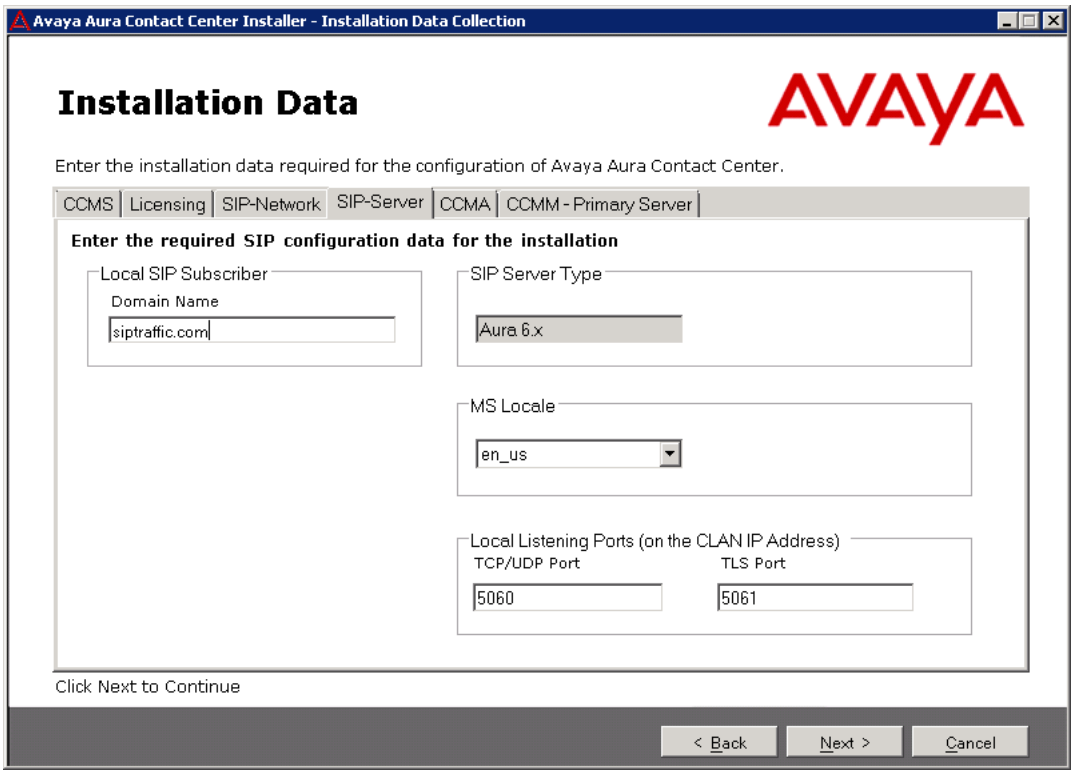
27 Select the **SIP-Server** tab.

28 Complete the **SIP-Server** tab fields as follows:

Local SIP Subscriber - Domain Name — Type the SIP domain name, for example siptraffic.com.

MS locale — Select **en_us**.

For the remaining boxes and lists, accept the defaults.

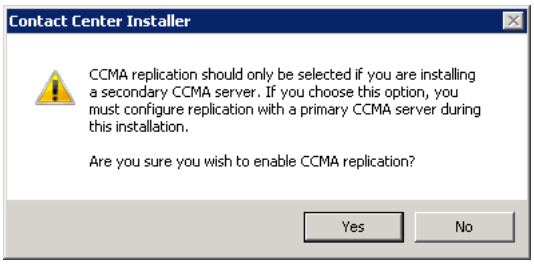


29 Select the **CCMA** tab.

30 Complete the **CCMA** tab fields as follows:

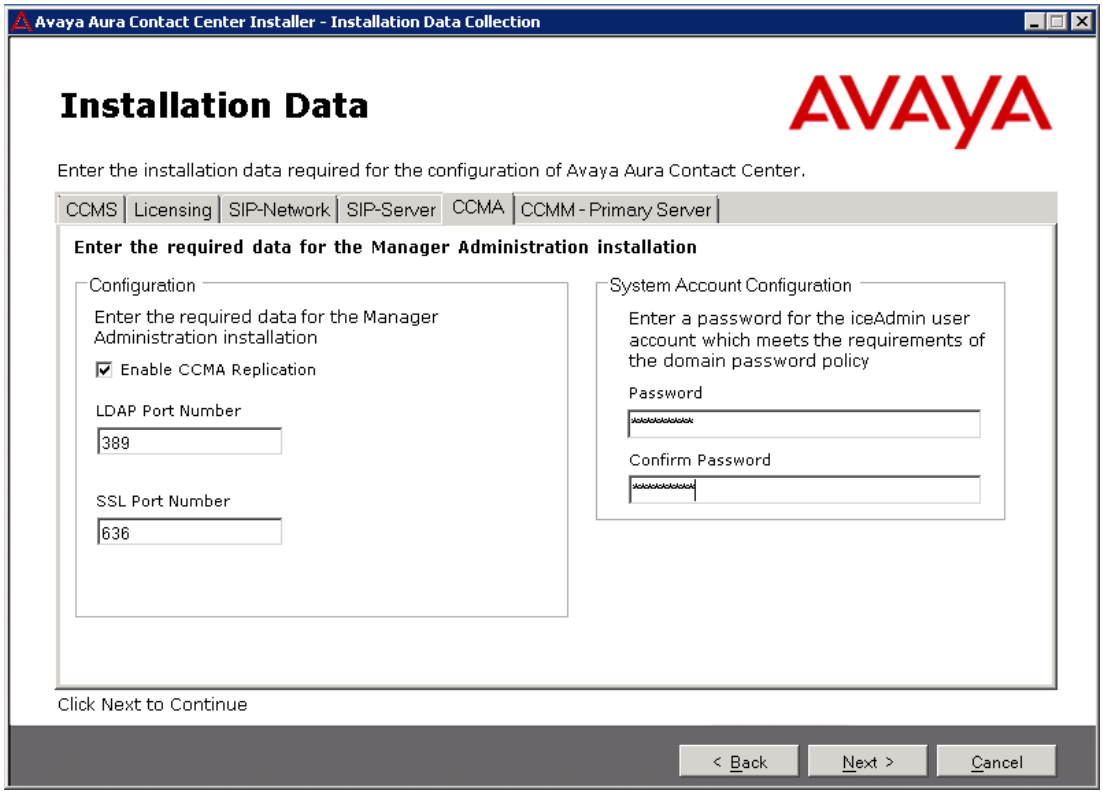
Configuration - Enable CCMA Replication — Select the **Enable CCMA Replication** check box.

On the **Contact Center Installer** message box, click **Yes**.



System Account Configuration - Password — Type the password for the CCMA System Account (iceAdmin). Enter a complex password which meets the requirements of your domain policy.

System Account Configuration - Confirm Password — Retype the password for the CCMA System Account (iceAdmin). Enter a complex password which meets the requirements of your domain policy.



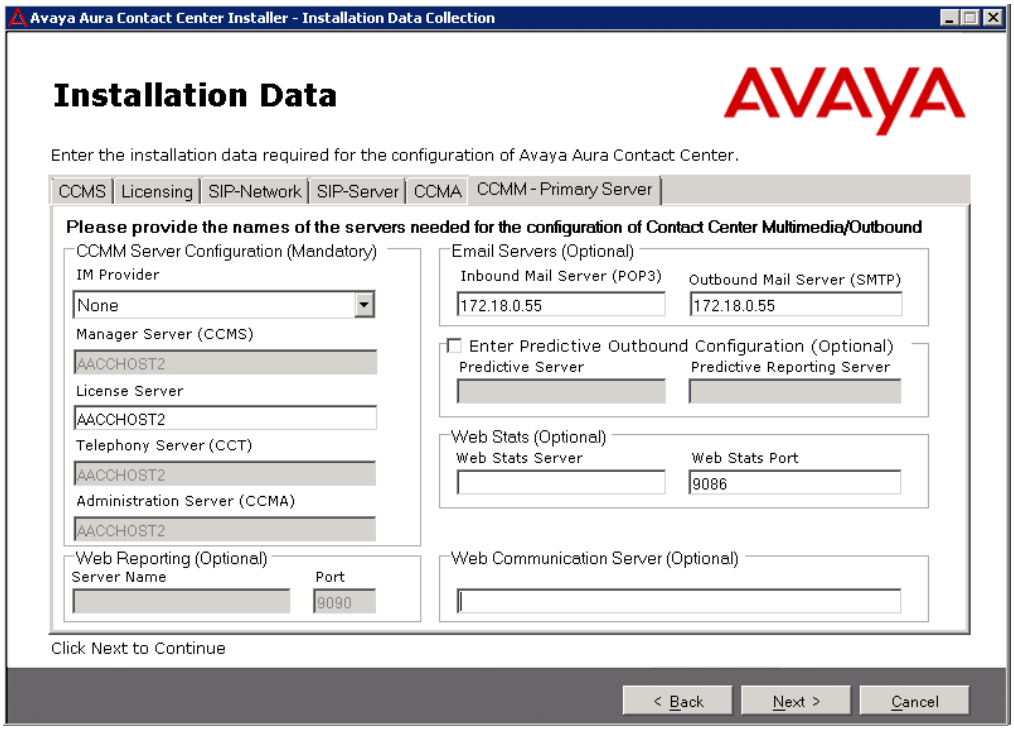
31 Select the **CCMM** tab, and configure the Contact Center Multimedia details.

32 From the **IM Provider** list, select either None, Microsoft OCS or Aura Presence Services. IM and presence features are supported for Avaya Aura® Presence Services server and Microsoft Office Communications Server. Instant Messaging is supported only in SIP-enabled contact center solutions.

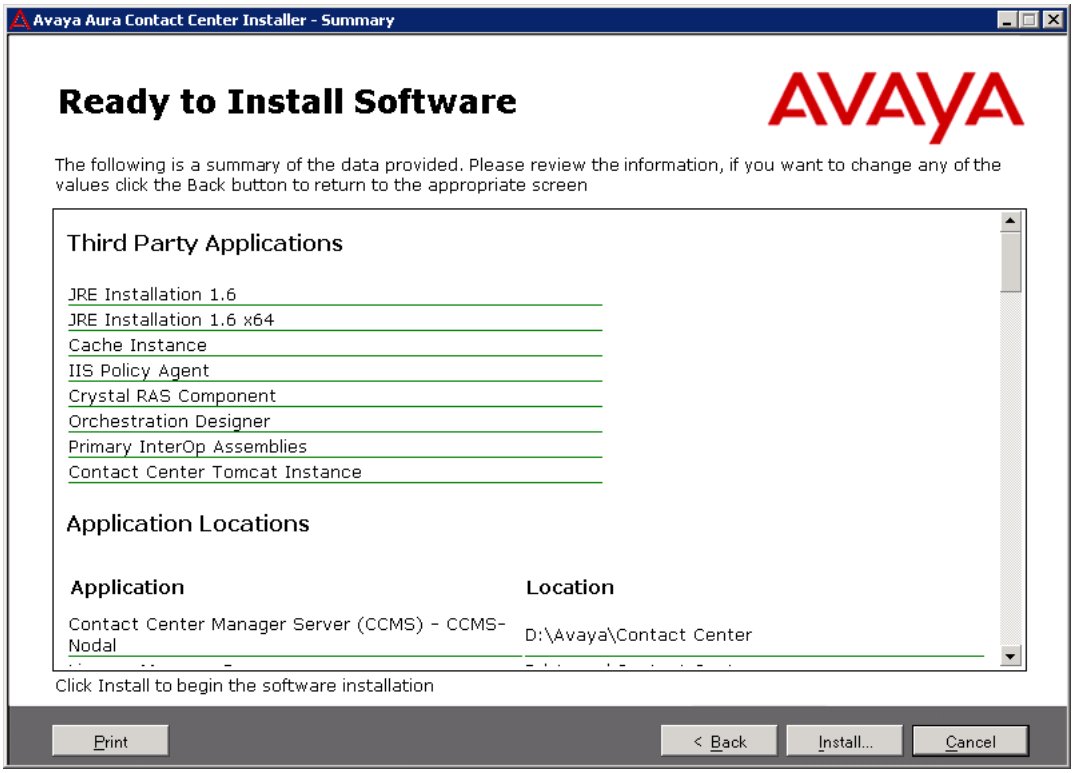
33 In the **License Server** box, type the name of the server on which the Contact Center License Manager software is installed. For example, type AACCHOST2.

34 In the **Inbound Mail Server (POP3)** box, type the IP address of the server on which email messages are received in your network. For example, type 172.18.0.55.

35 In the **Outbound Mail Server (SMTP)** box, type the IP address of the server from on which email messages are sent. Your inbound and outbound mail servers can have the same name. For example, type 172.18.0.55.



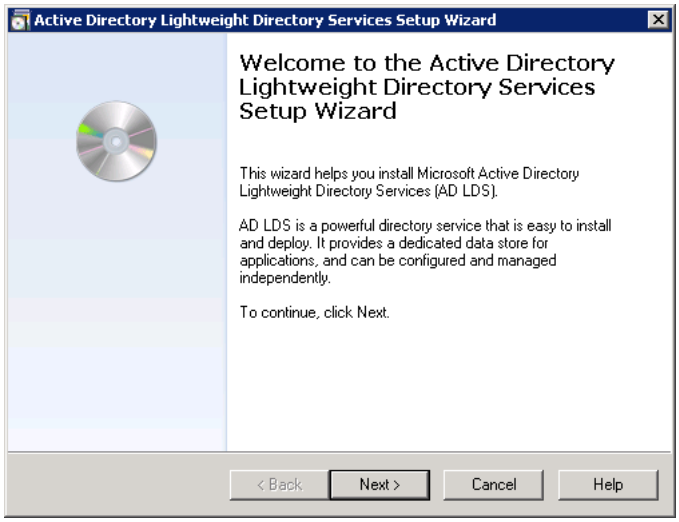
36 Click **Next**.



37 On the **Summary** window, review and verify the information.

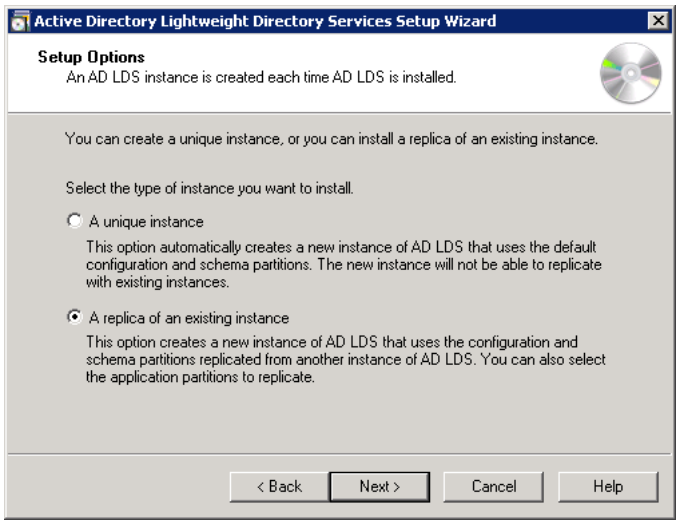
38 Click **Install**.

The install continues for some time until the AD-LDS setup wizard appears.



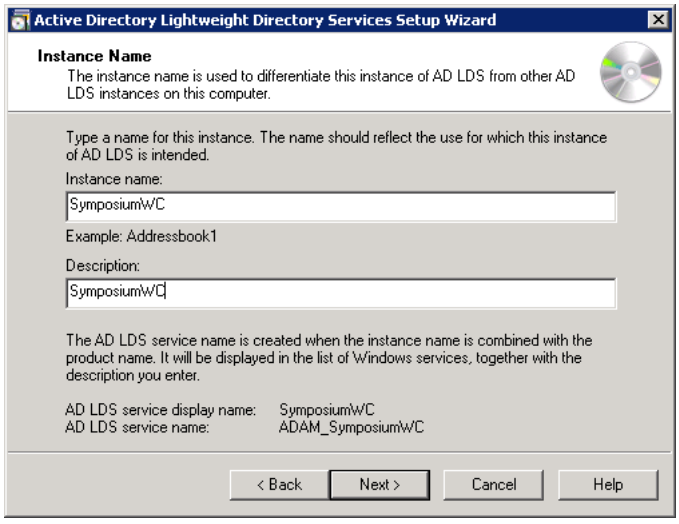
39 Select **Next**.

40 In the **Setup Options** dialog box, select **A replica of an existing instance**.



41 Select **Next**.

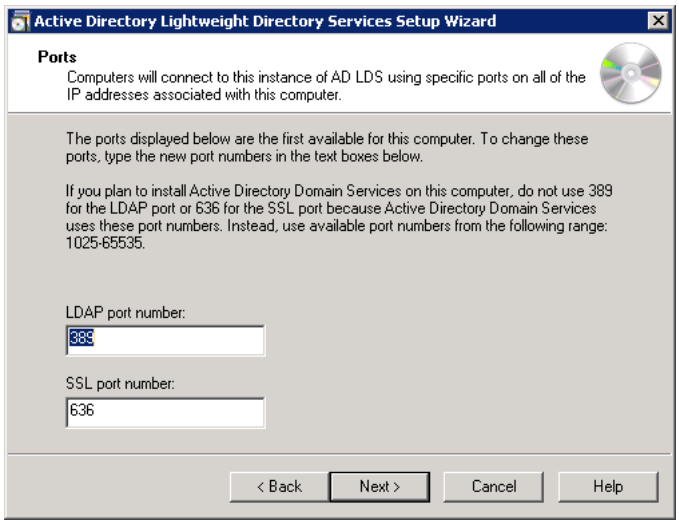
42 On the **Instance Name** dialog box, in the **Instance name** box, type the AD-LDS instance name. Type **SymposiumWC**.



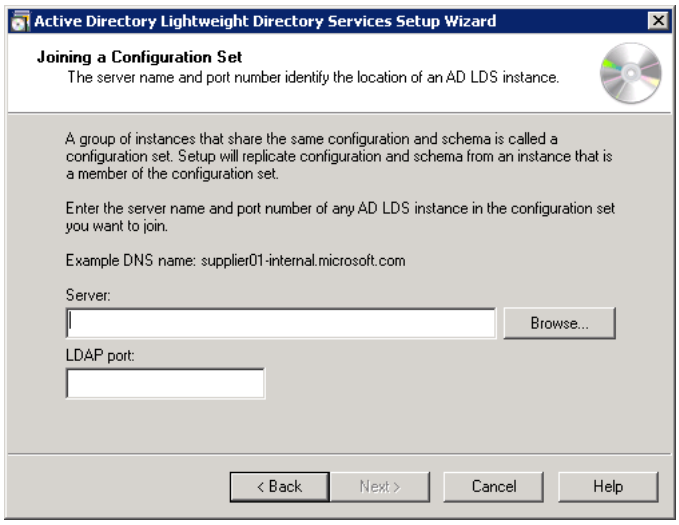
43 In the **Description** box, type **SymposiumWC**.

44 Click **Next**.

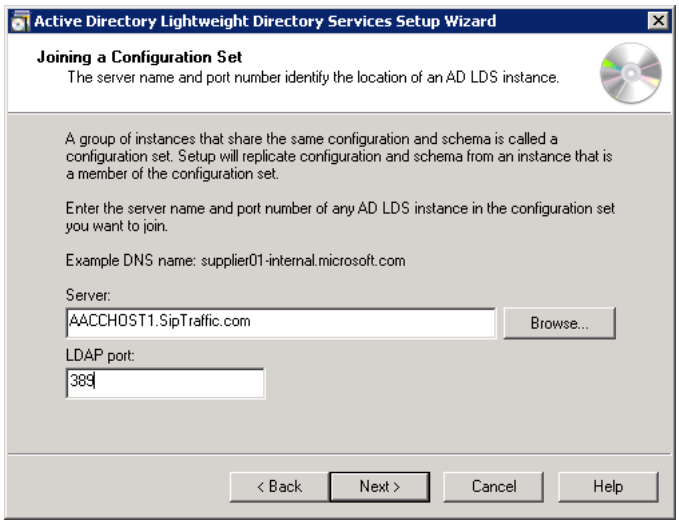
45 On the **Ports** dialog box, accept the default values in the LDAP port number and SSL port number boxes.



46 Click **Next**.

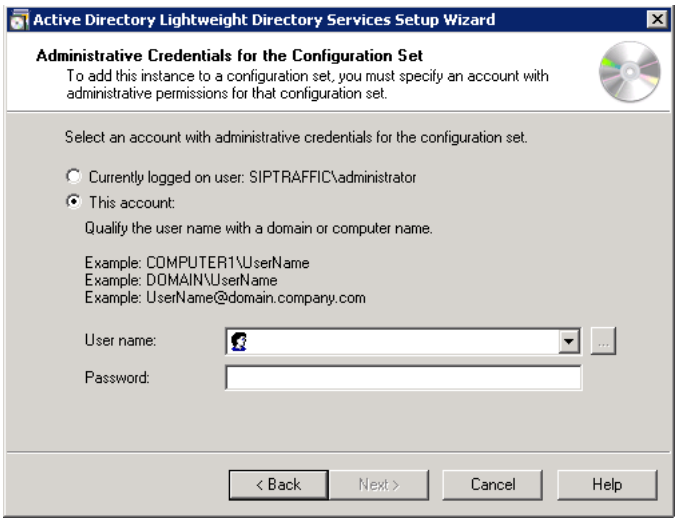


47 On the **Joining a Configuration Set** dialog box, in the **Server** box, type the FQDN name of the primary Contact Center Manager Administration server to replicate. For example type AACCHOST1.siptraffic.com.



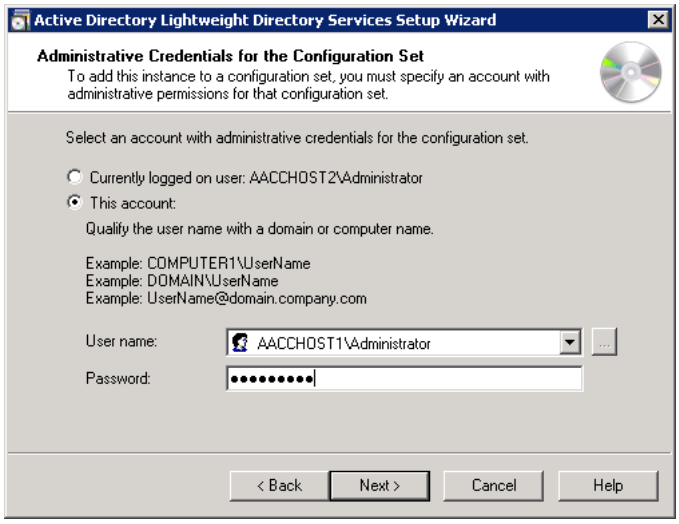
48 On the **Joining a Configuration Set** window, in the **LDAP Port** box, type the port number on the AD-LDS instance on the primary CCMA. The default is port number 389.

49 Click **Next**.



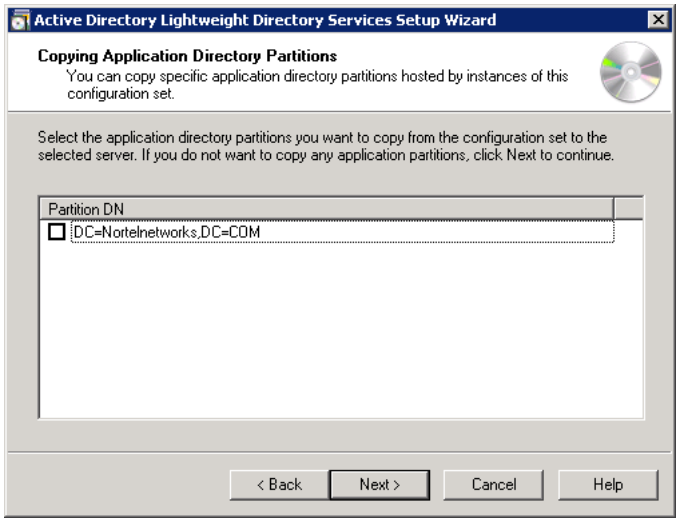
50 On the **Administrative Credentials for the Configuration Set** window, select **This account**.

51 In the **User name** box, type the primary CCMA server name followed by its Administrator name in the format <primary CCMA name>\Administrator. For example enter AACCHOST1\Administrator. If you have created another administrator account for Contact Center, then enter the details (name and password) for that Primary CCMA server administrator account here. Your administrator account must have full administrative privileges. Example of entering the administrative credentials.

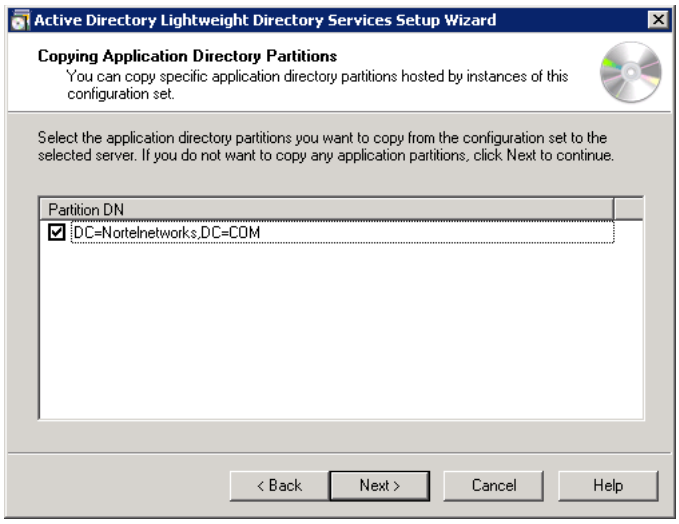


52 In the **Password** box, type the password for this user account.

53 Click **Next**.

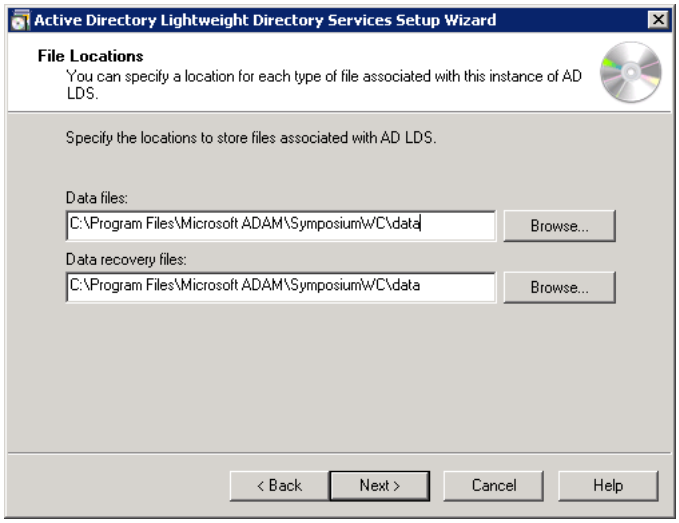


54 In the **Copying Application Directory Partitions** dialog box, in the Partition DN list, select the partition **DC=Nortelnetworks,DC=COM**.

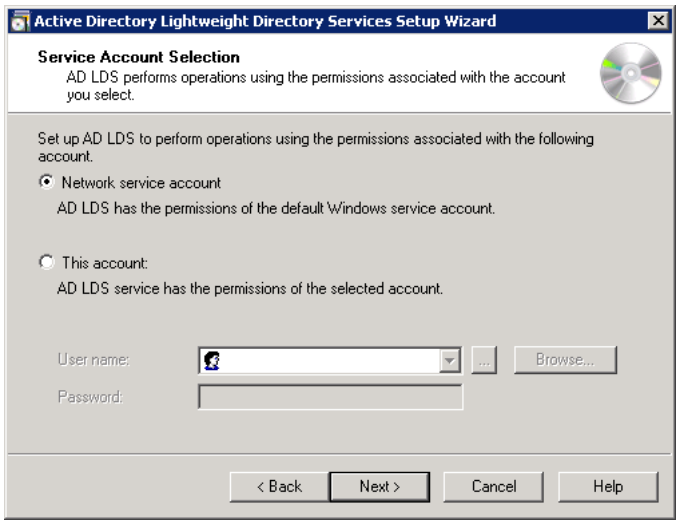


55 Select **Next**.

56 In the **File Location** dialog box, accept the default values.

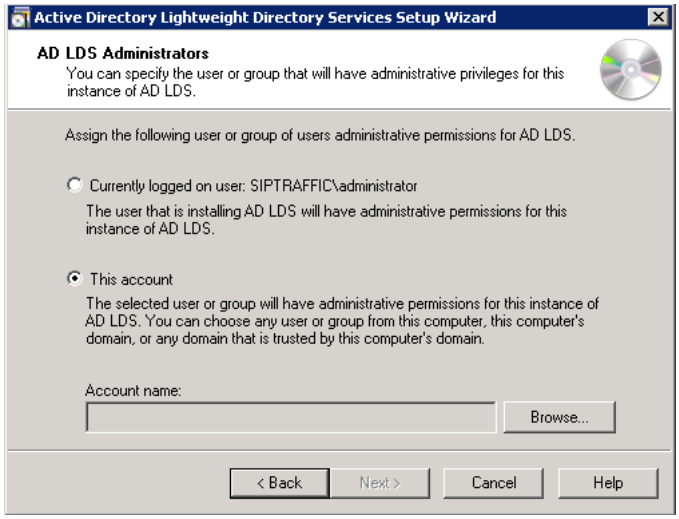


57 Click **Next**.

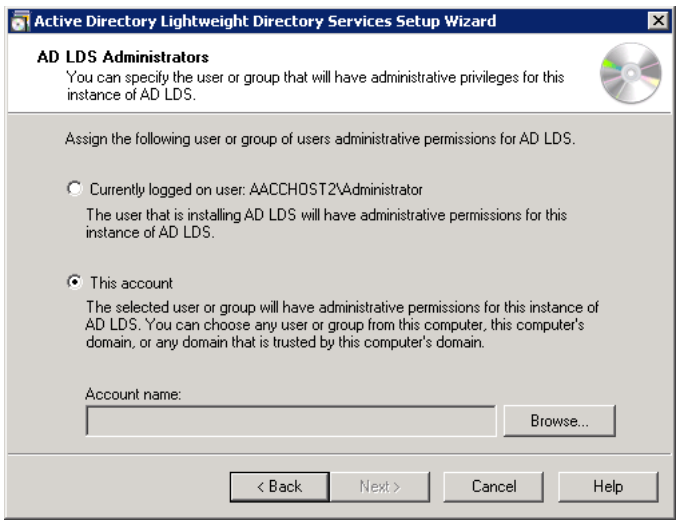


58 In the **Service Account Selection** dialog box, select **Network service account**.

59 Click **Next**.

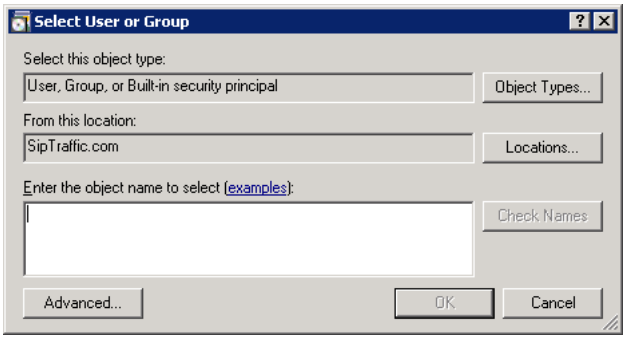


60 In the **AD LDS Administrators** dialog box, select **This account**.



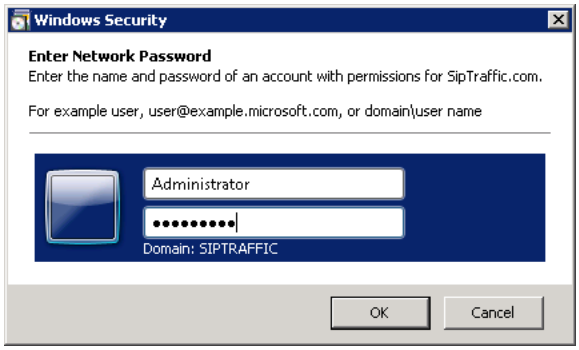
61 Select **Browse** to locate the CCMA AD-LDS replication account.

The Select User or Group dialog box appears. Note that the location is the local domain.



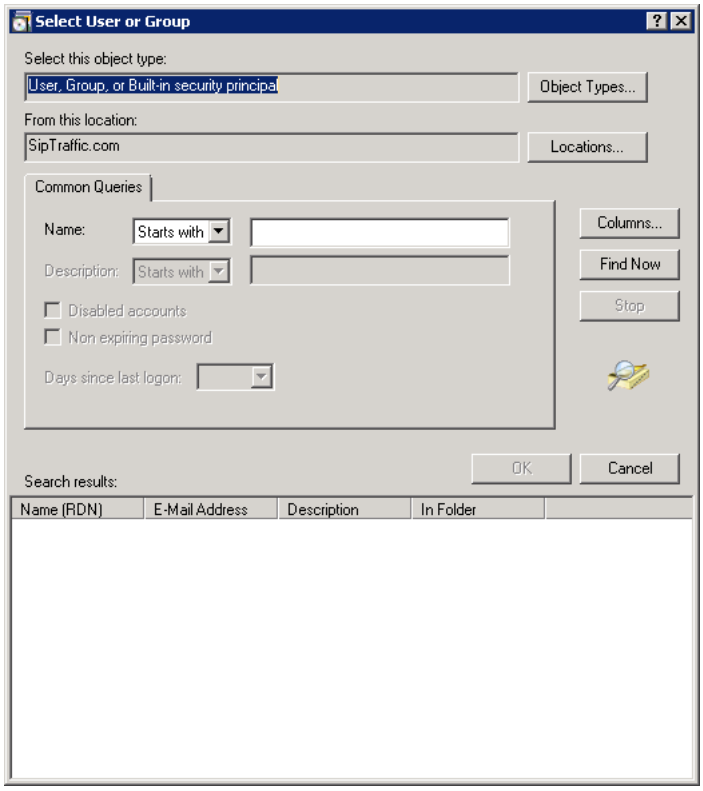
62 In the **Select User or Group dialog** box, click **Advanced**.

63 In the **Windows Security** dialog box, type a logon name and password of an account with permissions to access your domain.

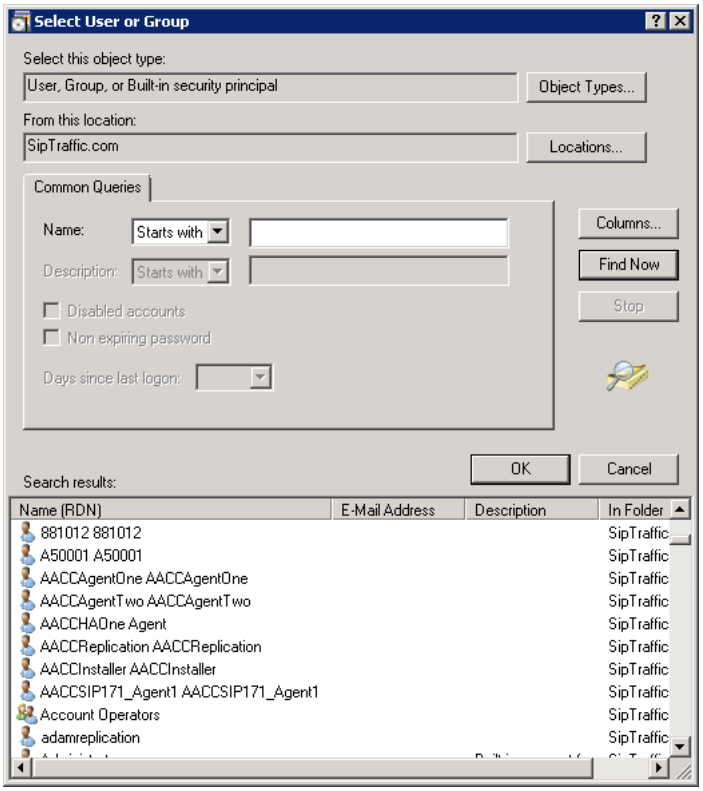


64 Click **OK**.

The advanced Select User or Group dialog box appears.

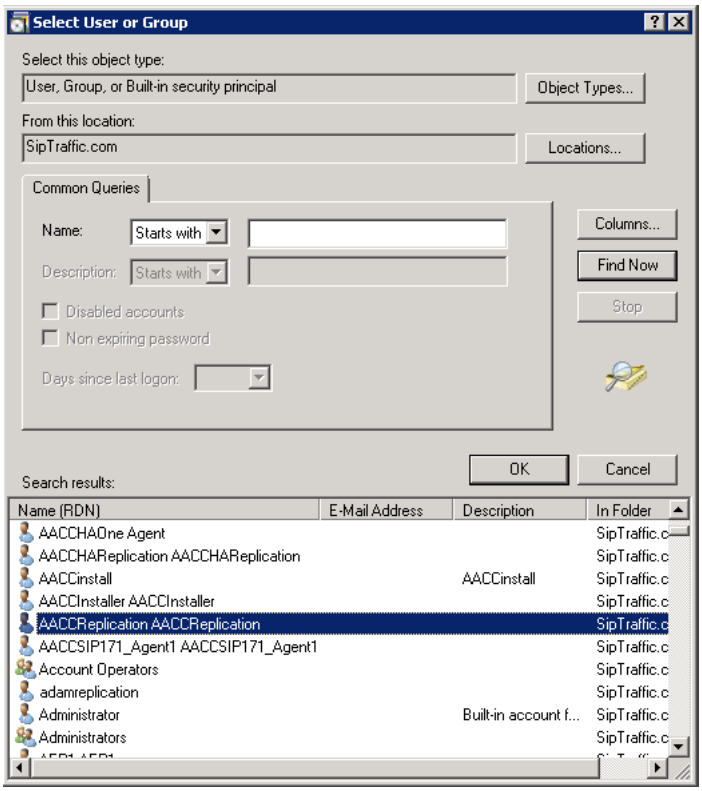


65 In the advanced **Select User or Group** dialog box, click **Find Now**.



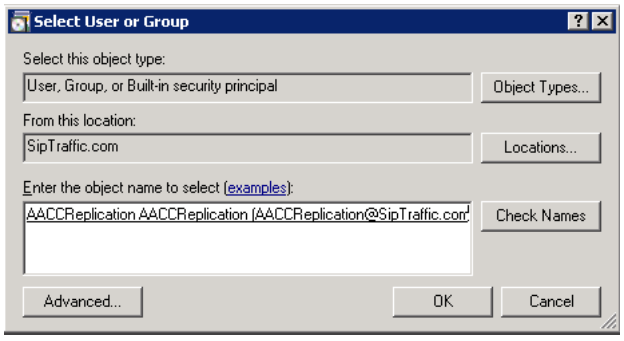
66 From the **Search results** list, select the CCMA replication account. For example, select the "AACCReplication" account.

Example of selecting a domain CCMA replication account:



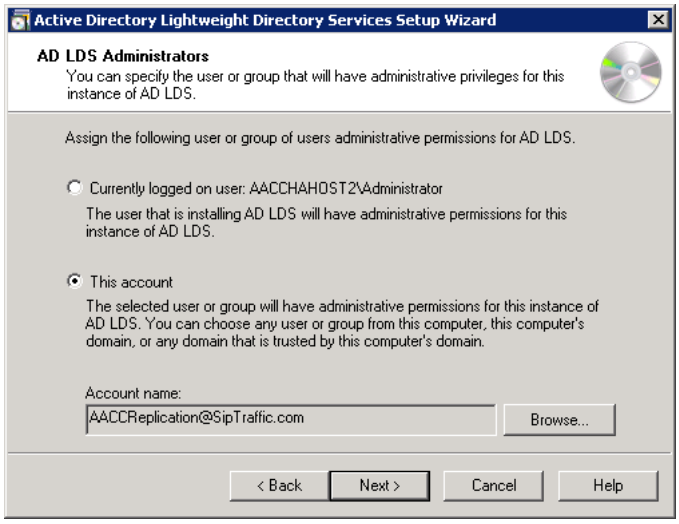
67 In the advanced **Select User or Group** dialog box, click **OK**.

Example of selecting a CCMA replication account:

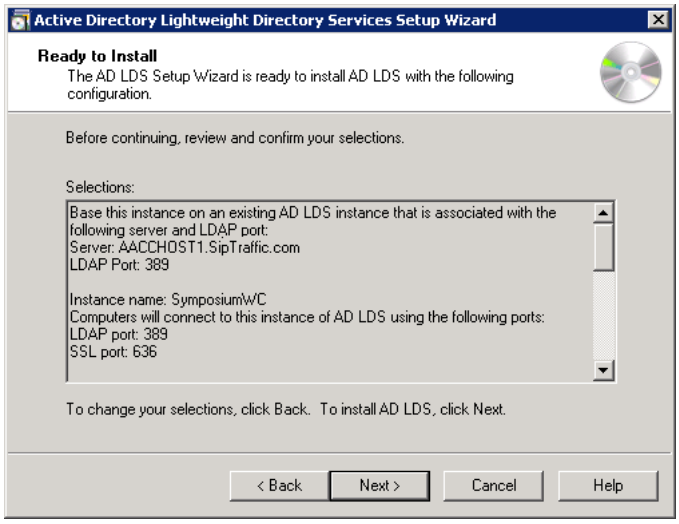


68 In the **Select User or Group** dialog box, click **OK**.

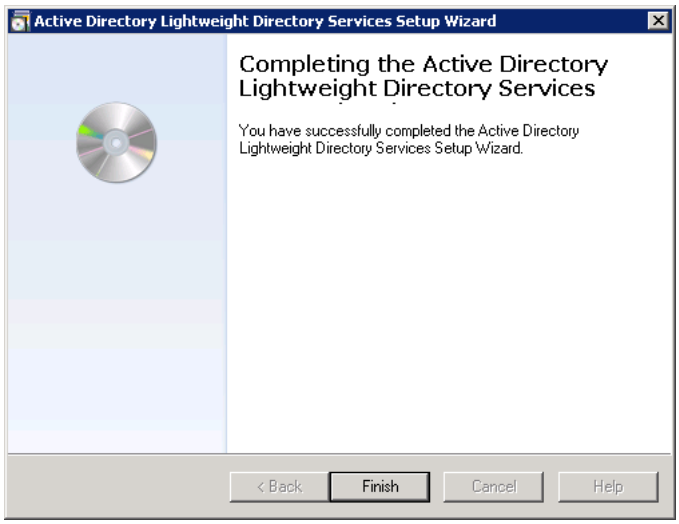
Example of using a domain CCMA replication account:



69 Click **Next**.



70 Confirm the installation components, and click **Next**.



71 Click **Finish**.

The Avaya Aura® Contact Center standby server installation continues.

72 After the installation is complete, if prompted, click **Yes** to restart the server.

--End--

Installing Voice and Multimedia Contact Server software patches

Install the most recent Voice and Multimedia Contact Server software service patches on the standby server to ensure that you have the most current development updates.

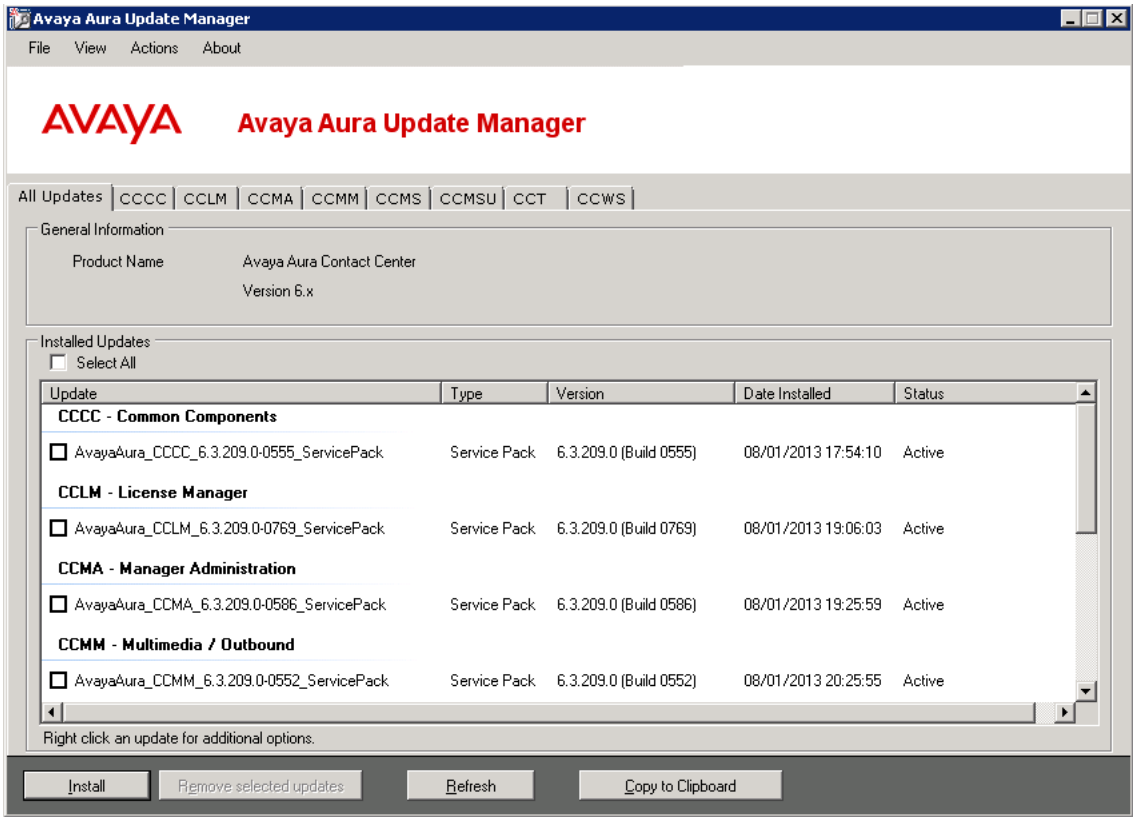
During a patch installation, all System Management and Monitoring Component (SMMC) services and the SMMC System Tray application stop to allow Contact Center files to be patched. After patching the server, if the patch does not require a server reboot, you must start the SMMC applications manually.

Prerequisites

- Download the most recent Avaya Aura® Contact Center patches.

Procedure steps

Step	Action
1	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Common Utilities**, **Contact Center Patch Manager**.



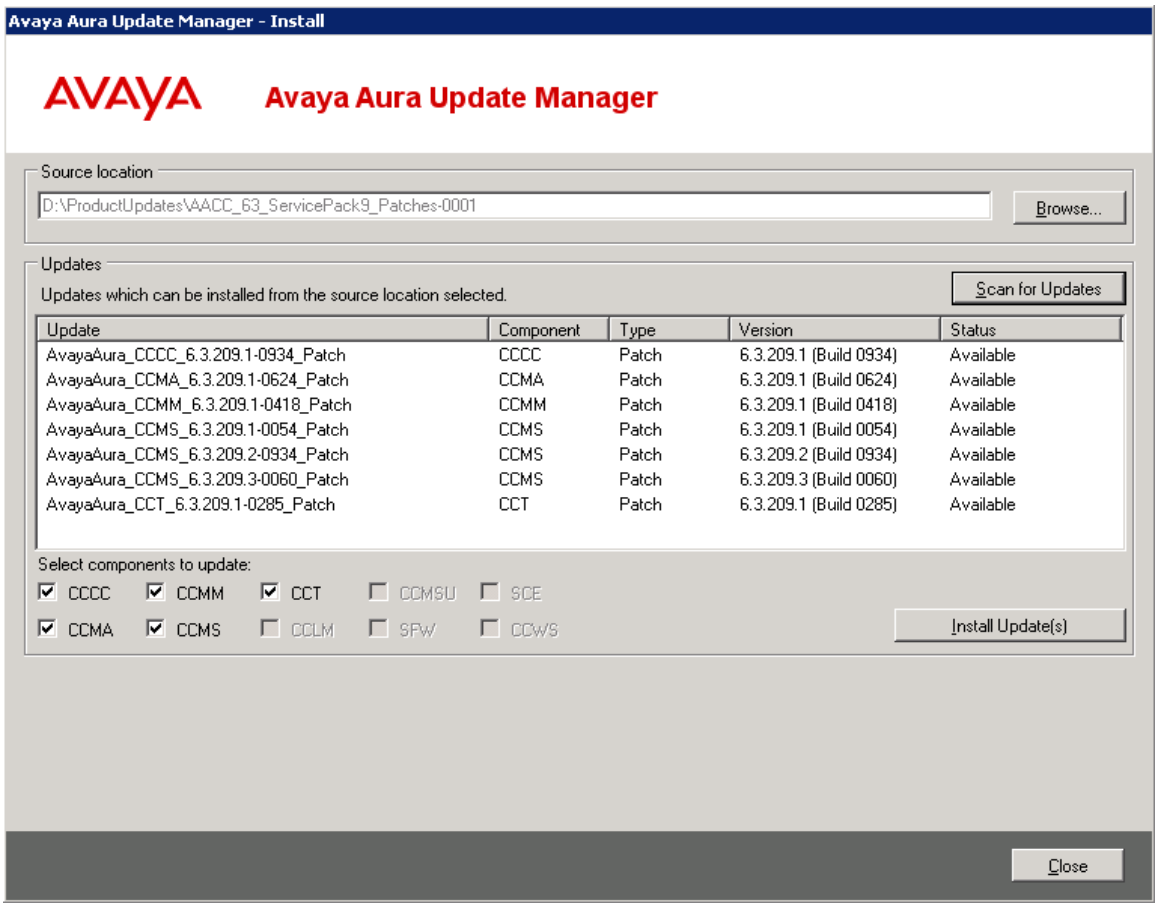
2 Click **Install**.

3 Click **Browse** and navigate to the folder where you have downloaded the server packs.

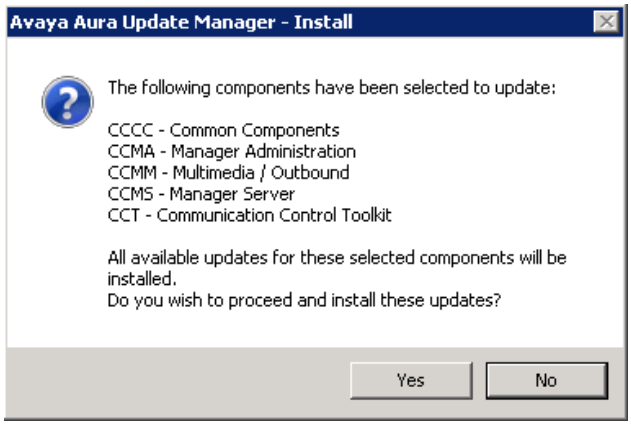
4 Click **Scan for Updates**.

The Contact Center Updates section displays the available patches.

5 Select the appropriate patch.



6 Click **Install Update(s)**.



7 Click **Yes**.

The Patch Manager installs the patch and displays a confirmation message.

8 If prompted to reboot your server, click **Close** and restart your server.

9 If the Voice and Multimedia Contact Server is not restarted, click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Common Utilities**, **SMMC SystemTray**.

10 On the Windows system tray, right-click the SMMC system tray icon, and select **Start SMMC**.

--End--

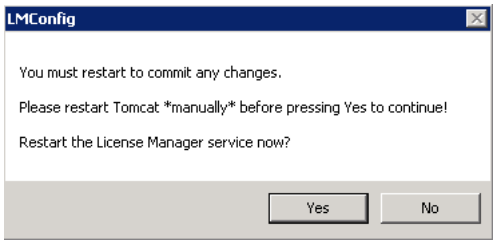
Configuring the WebLM license file

Configure Contact Center License Manager to use a WebLM file. Then restart the Contact Center Tomcat Instance on the Contact Center License Manager server to commission the WebLM license file for the first time.

When you install Contact Center License Manager, an instance of Apache Tomcat Server is also installed on the same server. The default port number for Apache Tomcat is 8081. If you need to change the port number to avoid conflicts with third-party software, see your Apache Tomcat documentation.

Procedure steps

Step	Action
1	Log on to the Voice and Multimedia Contact Server.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **License Manager**, **Configuration**.
3	View the type of license file currently used, and then click **OK**.
4	On the Configuration page, click **Browse**.
5	Navigate the file system and locate the WebLM license file.
6	Click **Open**.
7	Click **Apply**. *An LM dialog box appears, which you must ignore for now.*
8	On the Start menu, choose **All Programs** > **Administrative Tools** > **Services**.
9	Right-click the **Contact Center Tomcat Instance** service, and click **Stop**.
10	Right-click the **Contact Center Tomcat Instance** service, and click **Start**.
11	Close the services window.
12	On the LM dialog box, click **Yes** to restart the Contact Center License Manager services.



13 Click **OK** to close the window.

14 Click **Exit**.

--End--

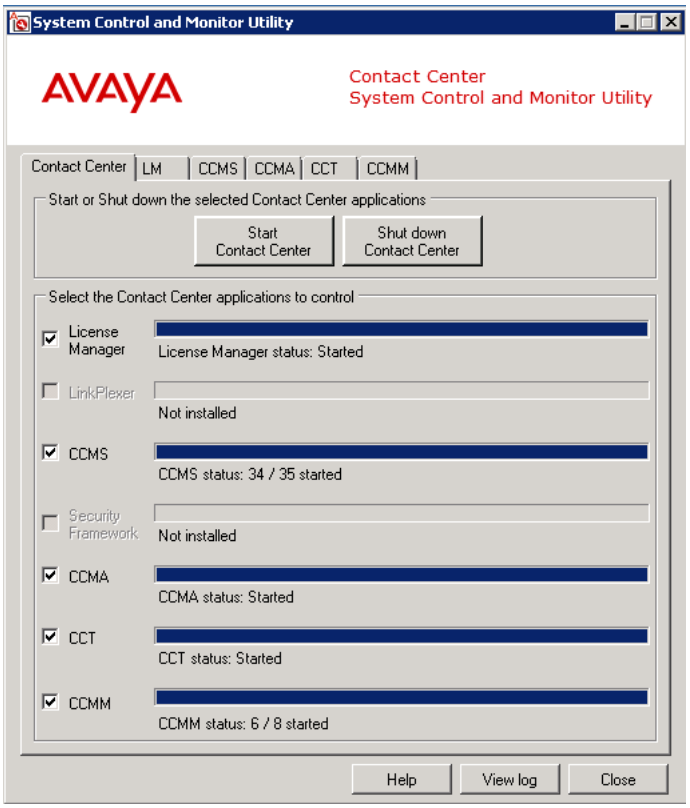
Confirming that the Contact Center services start

Confirm that all appropriate Contact Center services start on the Contact Center server.

Use the System Control and Monitor Utility to start and stop all Contact Center applications including the license manager. The System Control and Monitor Utility can also start, stop, or monitor the services.

Procedure steps

Step	Action
1	Log on to the standby Voice and Multimedia Contact Server.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Common Utilities**, **System Control and Monitor Utility**.
3	Click the **Contact Center** tab.
4	Select the applications to start on the current server by selecting the application name check boxes.

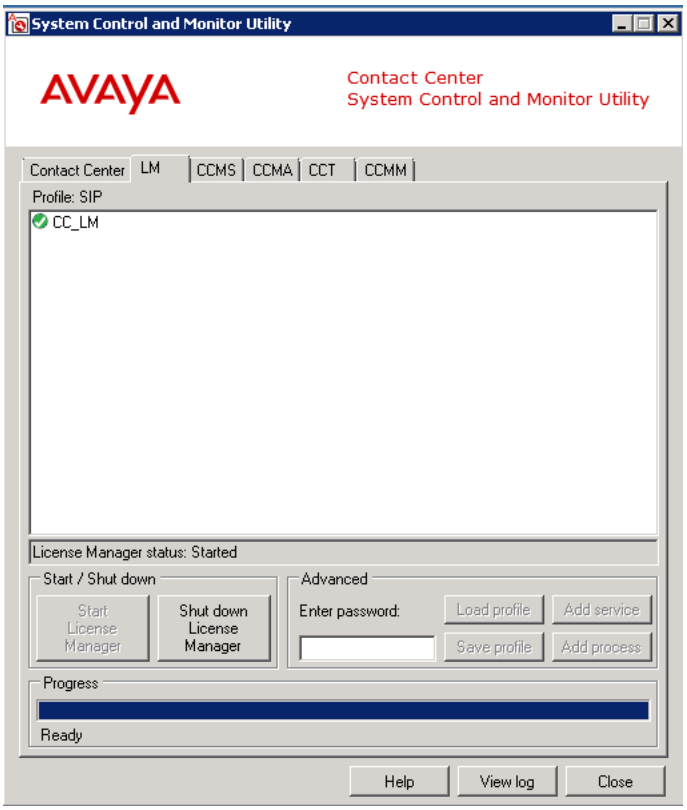


5 Click **Start Contact Center**.

6 Click **OK**.

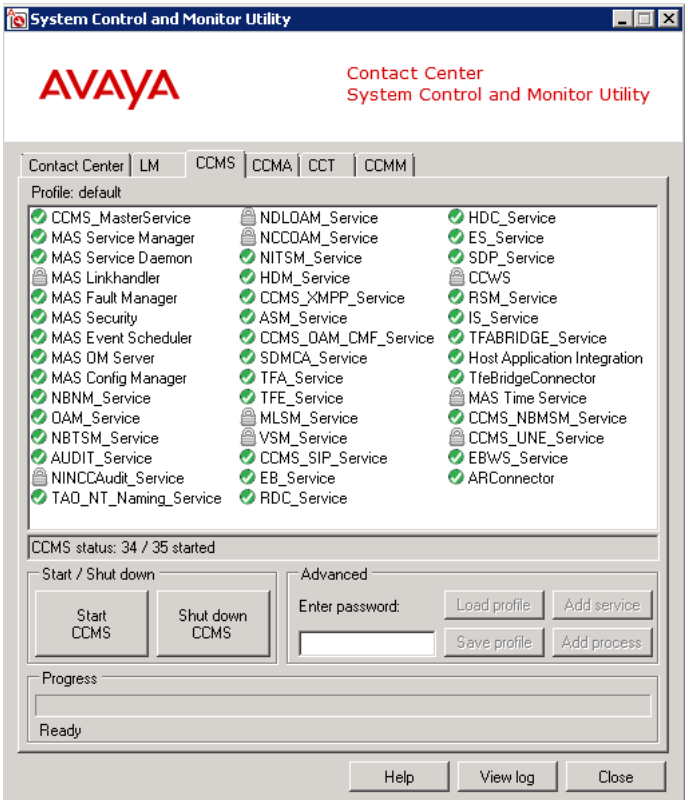
7 Click the **LM** tab.

8 Ensure that all services in the **Profile** box have a green circle next to them.



9 Click the **CCMS** tab.

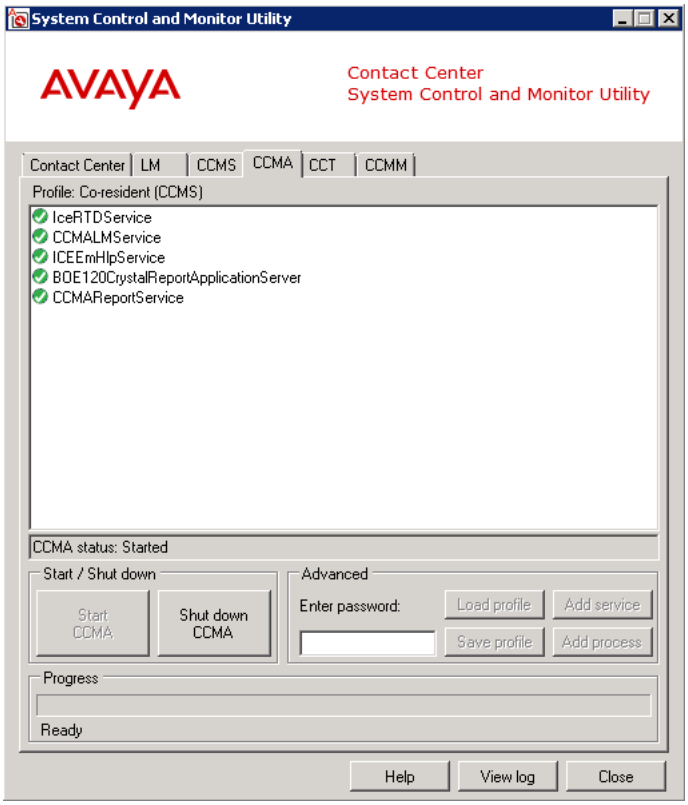
10 Ensure that the main CCMS services in the **Profile** box have a green circle next to them. CCMS services with a padlock icon are not licensed and therefore do not start.



11 If some of the services are not started, click **Start CCMS**.

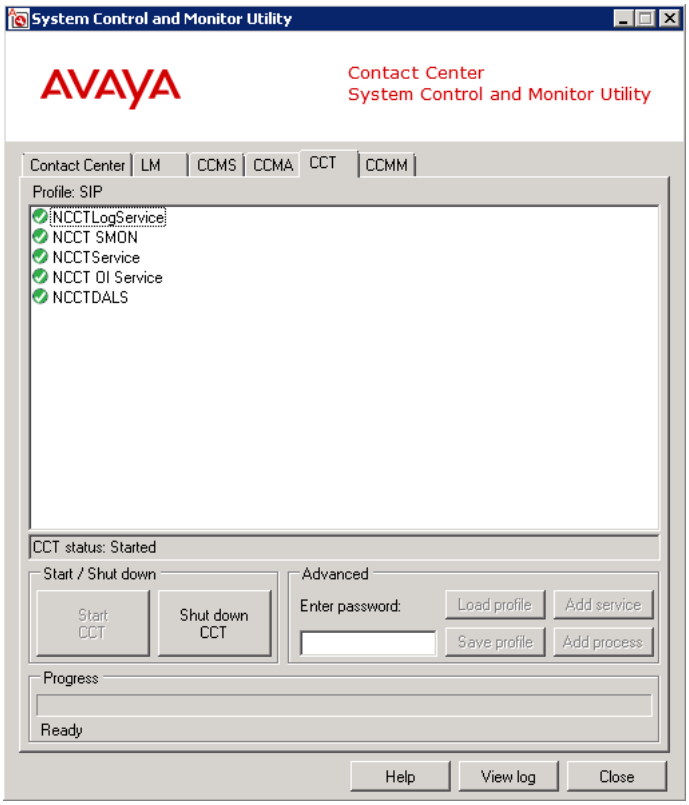
12 Click the **CCMA** tab.

13 Ensure that all services in the **Profile** box have a green circle next to them.



14 Select the **CCT** tab.

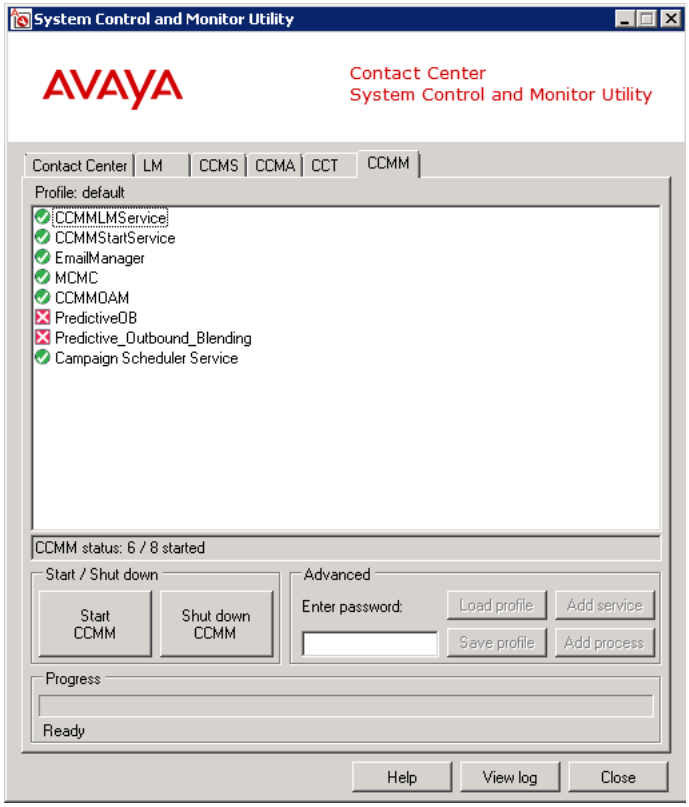
15 Confirm that the Communication Control Toolkit services are running.



16 If a Communication Control Toolkit service is not running, click **Start CCT**.

17 Select the **CCMM** tab.

18 Confirm that the Contact Center Multimedia services are running. Predictive Outbound Blending is not licensed or enabled on this server.



19 If a Contact Center Multimedia service is not running, click **Start CCMM**.

20 Click **Close**.

--End--

Updating the CCMA Administration user password

Update the CCMA Administration account password on your Contact Center Manager Administration server using the iceAdmin Password Change utility.

The CCMA Administration account is an administrator account for the Contact Center Manager Administration server.

Procedure steps

Step	Action
1	Log on the server on which you installed the standby Contact Center Manager Administration server software.

2 Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Manager Administration**, **Configuration**.

3 In the **Avaya Applications Configuration** window, in the left pane, expand **Avaya**, **Applications**, **iceAdmin Password Change**.

4 In the right pane, click the **iceAdmin Password Change** icon.

5 In the **New Password** box, type a password for the CCMA Admin user account. Enter a complex password which meets the requirements of your domain policy.

6 In the **Confirm Password** box, type the password again.

7 Click **OK**.

--End--

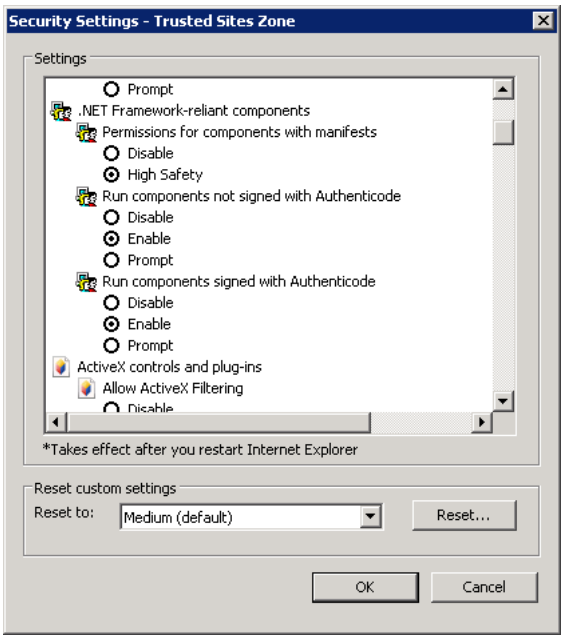
Configuring Internet Explorer on the Contact Center server

Configure Internet Explorer on the Contact Center server to access Contact Center Manager Administration for the first time.

Install Microsoft Internet Explorer 7.0, 8.0 or 9.0 (32 bit version only). Contact Center Manager Administration supports only the 32 bit version of Microsoft Internet Explorer.

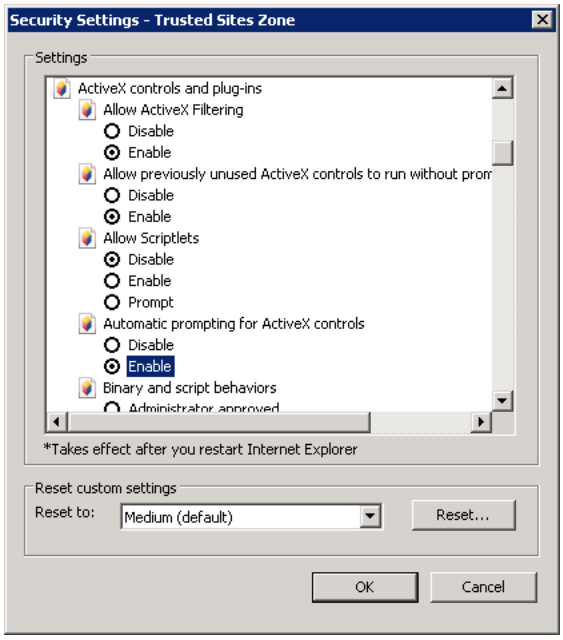
Procedure steps

Step	Action
1	On the Contact Center server, start Internet Explorer.
2	From the menu, select **Tools, Internet Options**.
3	In the **Internet Options** dialog box, click the **Security** tab.
4	Click the **Trusted Sites** icon.
5	Click **Custom Level**.
6	In the **Security Settings** dialog box for trusted sites, under the **.NET Framework-reliant components** heading, select **Enable** for the following: • **Run components not signed with Authenticode** • **Run components signed with Authenticode**



7 Under the **ActiveX controls and plug-ins** heading, select **Enable** for the following:

- **Automatic prompting for ActiveX controls**
- **Run ActiveX Controls and plug-ins**
- **Script ActiveX Controls marked safe for scripting**

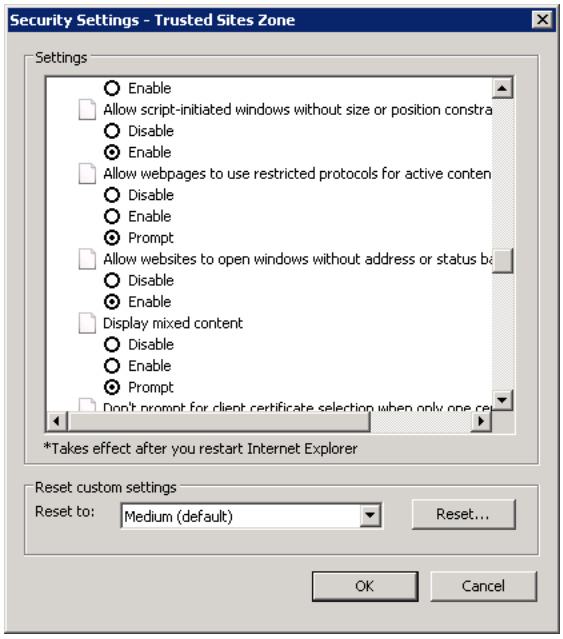


8 Under the **Downloads** heading, select **Enable** for the following:

- **Automatic prompting for file downloads**
- **File download**

9 Under the **Miscellaneous** heading, for **Allow script-initiated windows without size or position constraints**, select **Enable**.

10 Under the **Miscellaneous** heading, for **Allow websites to open windows without address or status bars**, select **Enable**.



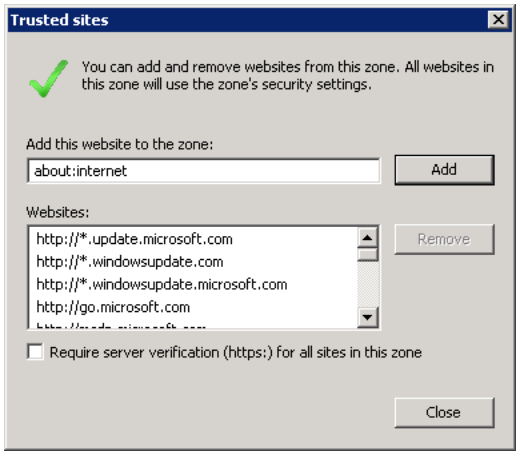
11 Click **OK**.

12 If you have enabled ActiveX options, when a message appears asking you to confirm your choice, click **Yes**.

13 Click the **Trusted Sites** icon.

14 Click **Sites**.

15 In the **Trusted sites** dialog box, clear the **Require server verification (https:) for all sites in this zone** check box.



16 In the **Add this Web site to the zone** box, type the server name (not the IP address) for your standby Voice and Multimedia Contact Server.

OR

If you used the fully qualified domain name when you installed the standby Voice and Multimedia Contact Server, in the **Add this Web site to the zone** box, type the fully qualified domain name.

17 Click **Add**.

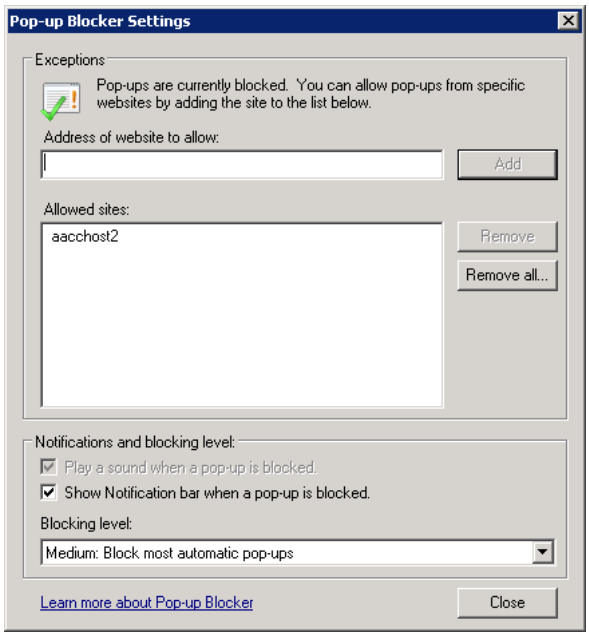
18 Click **Close** to return to the **Internet Options** dialog box.

19 Click the **Privacy** tab.

20 In the **Pop-up Blocker** section, select the **Turn on Pop-up Blocker** check box.

21 Click **Settings**.

22 In the **Pop-up Blocker Settings** dialog box, in the **Address of website to allow** box, type the standby Contact Center Manager Administration URL, for example http://AACCHOST2.

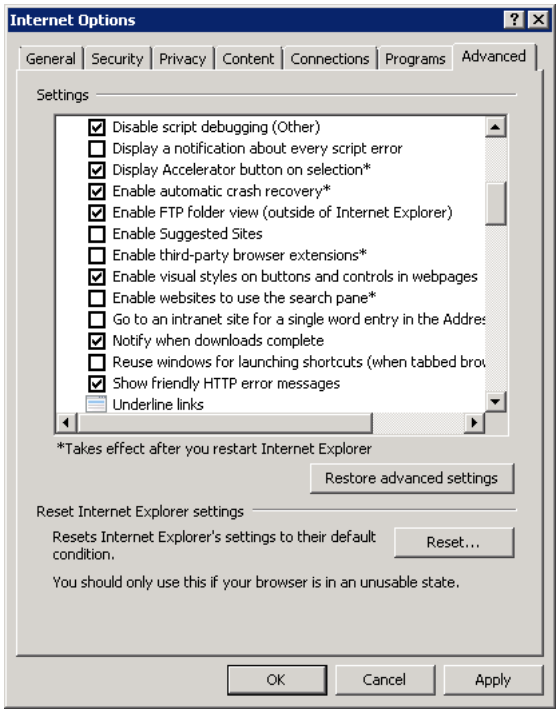


23 Click **Add**.

24 Click **Close**.

25 In the **Internet Options** dialog box, click the **Advanced** tab.

26 Under **Browsing**, clear the **Reuse windows for launching shortcuts** check box.



27	Click **Apply**.
28	Click **OK** to exit the **Internet Options** dialog box.
29	Restart Internet Explorer to activate your changes.

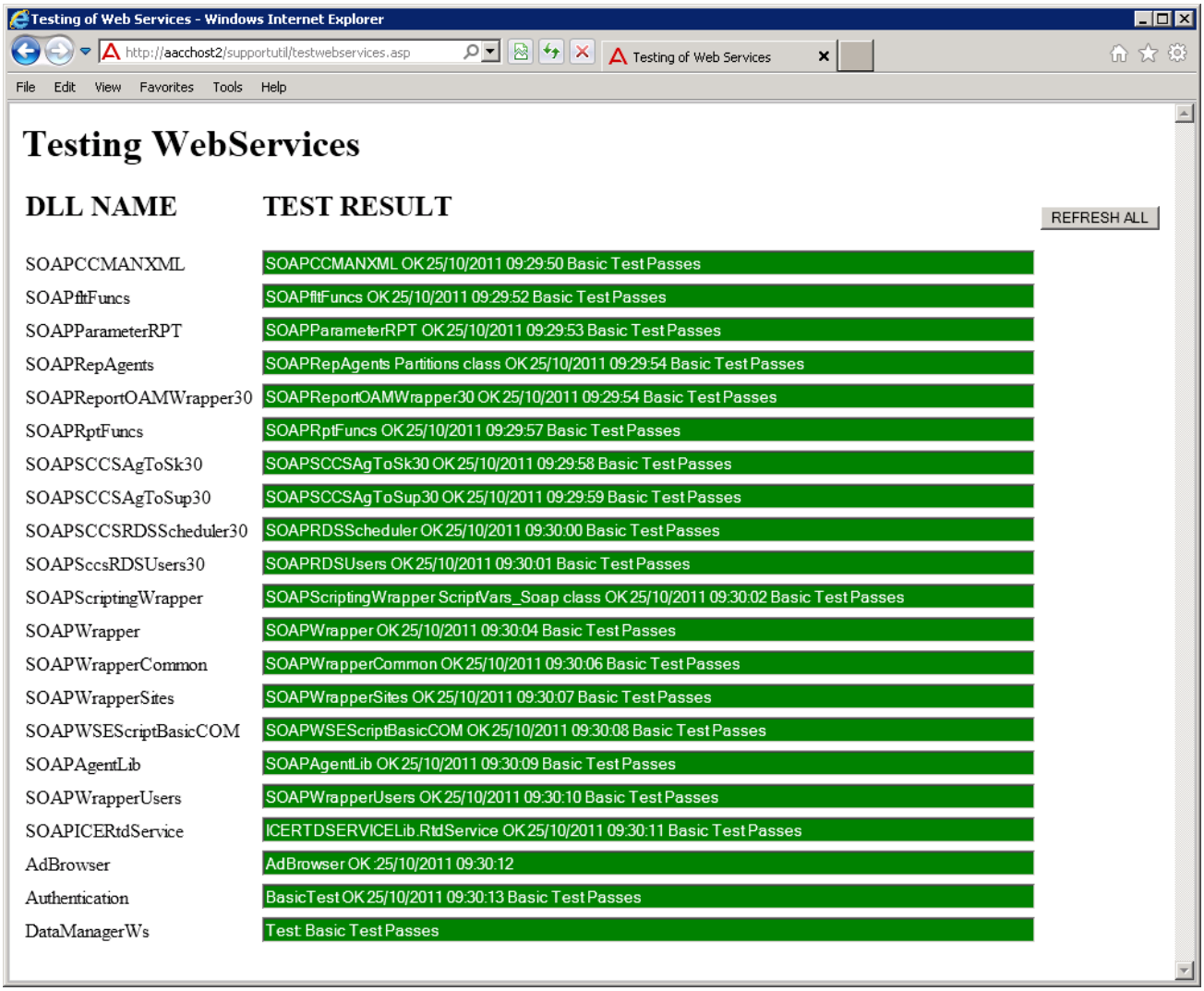
--End--

Verifying the Web Services

Test the Web Services to ensure CCMA web services are running correctly.

Procedure steps

Step	Action
1	Start Internet Explorer.
2	Enter the following: http://<SERVER NAME>/supportutil/testwebservices.asp Where SERVER NAME is the name of the Voice and Multimedia Contact Server. For example, enter the following: http://AACCHOST2/supportutil/testwebservices.asp The web services that appear in green are running correctly.


Testing of Web Services - Windows Internet Explorer
http://aacchost2/supportutil/testwebservices.asp
Testing of Web Services
File Edit View Favorites Tools Help
Testing WebServices
DLL NAME
TEST RESULT
REFRESH ALL
SOAPCCMANXML SOAPCCMANXML OK 25/10/2011 09:29:50 Basic Test Passes
SOAPfltFuncs SOAPfltFuncs OK 25/10/2011 09:29:52 Basic Test Passes
SOAPParameterRPT SOAPParameterRPT OK 25/10/2011 09:29:53 Basic Test Passes
SOAPRepAgents SOAPRepAgents Partitions class OK 25/10/2011 09:29:54 Basic Test Passes
SOAPReportOAMWrapper30 SOAPReportOAMWrapper30 OK 25/10/2011 09:29:54 Basic Test Passes
SOAPRptFuncs SOAPRptFuncs OK 25/10/2011 09:29:57 Basic Test Passes
SOAPSCCSAgToSk30 SOAPSCCSAgToSk30 OK 25/10/2011 09:29:58 Basic Test Passes
SOAPSCCSAgToSup30 SOAPSCCSAgToSup30 OK 25/10/2011 09:29:59 Basic Test Passes
SOAPSCCSRDSScheduler30 SOAPRDSScheduler OK 25/10/2011 09:30:00 Basic Test Passes
SOAPSccsRDSUsers30 SOAPRDSUsers OK 25/10/2011 09:30:01 Basic Test Passes
SOAPScriptingWrapper SOAPScriptingWrapper ScriptVars_Soap class OK 25/10/2011 09:30:02 Basic Test Passes
SOAPWrapper SOAPWrapper OK 25/10/2011 09:30:04 Basic Test Passes
SOAPWrapperCommon SOAPWrapperCommon OK 25/10/2011 09:30:06 Basic Test Passes
SOAPWrapperSites SOAPWrapperSites OK 25/10/2011 09:30:07 Basic Test Passes
SOAPWSEScriptBasicCOM SOAPWSEScriptBasicCOM OK 25/10/2011 09:30:08 Basic Test Passes
SOAPAgentLib SOAPAgentLib OK 25/10/2011 09:30:09 Basic Test Passes
SOAPWrapperUsers SOAPWrapperUsers OK 25/10/2011 09:30:10 Basic Test Passes
SOAPICERtdService ICERTDSERVICELib.RtdService OK 25/10/2011 09:30:11 Basic Test Passes
AdBrowser AdBrowser OK :25/10/2011 09:30:12
Authentication BasicTest OK 25/10/2011 09:30:13 Basic Test Passes
DataManagerWs Test: Basic Test Passes

--End--

Verifying Contact Center Manager Administration replication

Verify that Contact Center Manager Administration Active Directory - Lightweight Directory Services (AD-LDS) replication is working.

Attention: Normally you must log on to Contact Center Manager Administration using the hostname of the active CCMA or the Managed name of the High Availability Voice and Multimedia Contact Server pair. This procedure uses the hostname of the backup CCMA server for AD-LDS verification purposes only.

Procedure steps

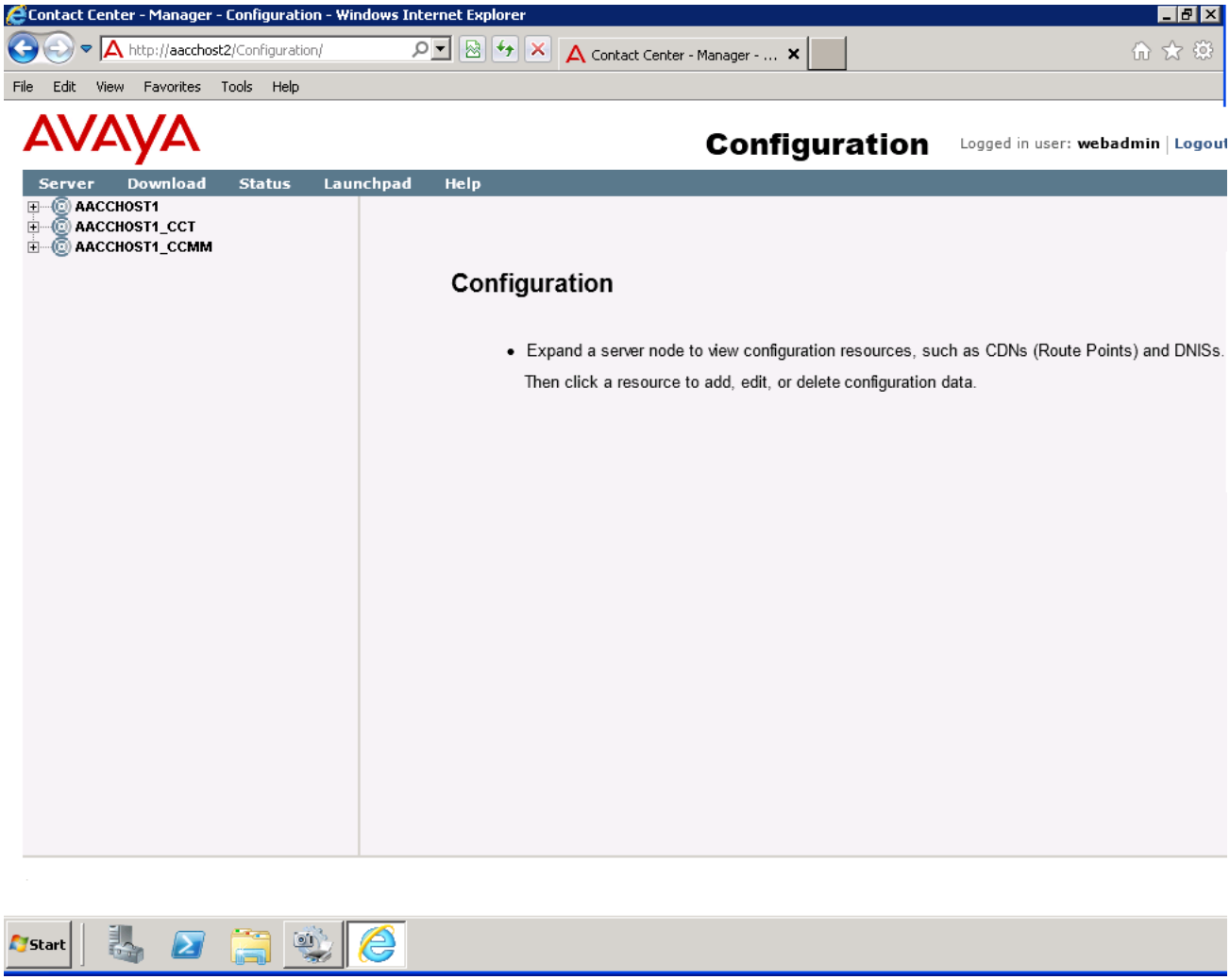
Step	Action
1	Start Internet Explorer.
2	In the **Address** box, type the following: **http://AACCHOST2**
3	Press **Enter**.
4	In the CCMA main log on window, enter the User ID and password for the CCMA on your active server. The default User ID is webadmin. The default password is webadmin.
5	Click **Login**.
6	Click **OK**.
7	Verify that the server details and data displayed in the standby Contact Center Manager Administration match the details entered on the active server.

--End--

Procedure job aid

Log on to the standby CCMA Web administration utility to verify that the data and server details match the data in the active (primary) CCMA.

In the following example, the Web browser is directed at the hostname of the standby CCMA server (AACCHOST2), but the server details shown in the browser are the active server details (AACCHOST1). This verifies that CCMA Active Directory - Lightweight Directory Services (AD-LDS) replication is working. Data entered on the primary CCMA is replicated to the standby CCMA.

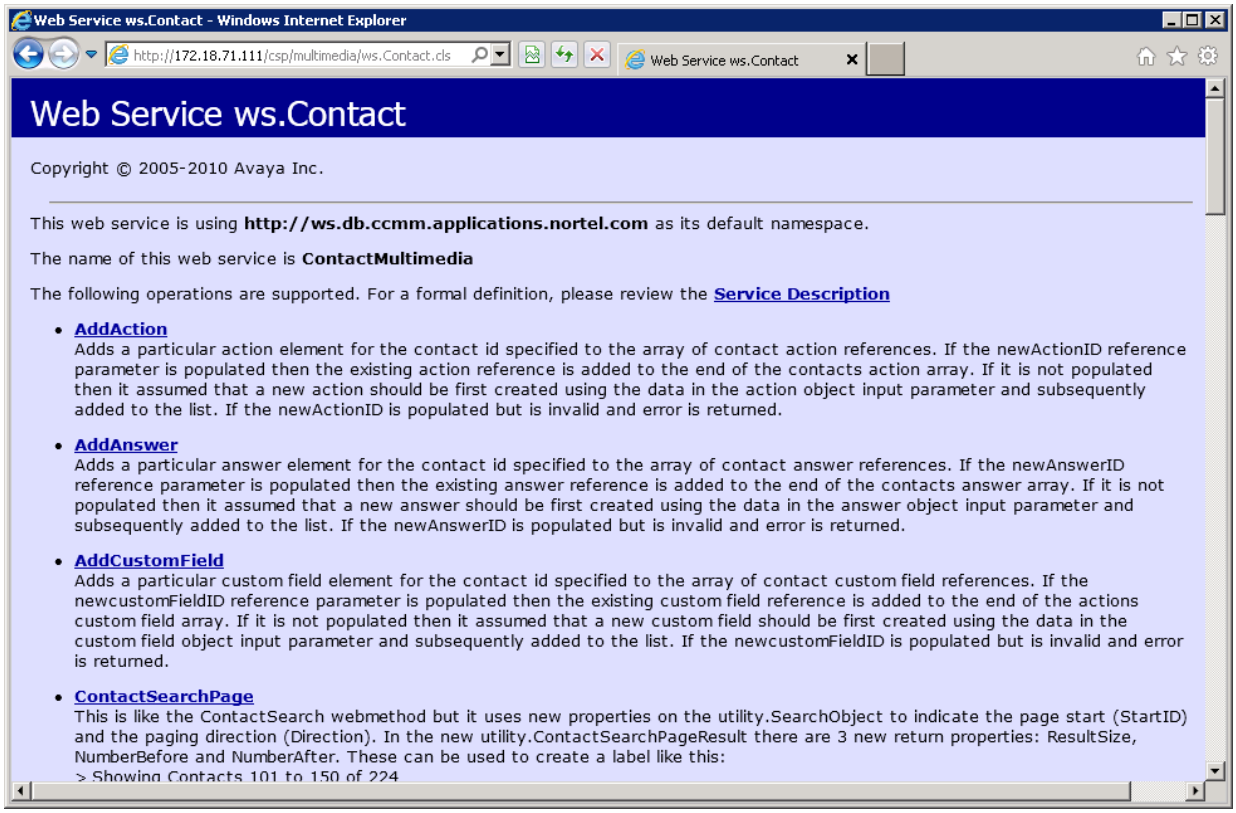


Verifying the Multimedia database installation

Verify that the Multimedia database is installed and configured correctly.

Procedure steps

Step	Action
1	On the standby Voice and Multimedia Contact Server, open Internet Explorer.
2	Browse to the following location: **http://172.18.71.111/csp/multimedia/ws.Contact.cls**



3 If a Web page does not appear, contact your Avaya technical support prime.

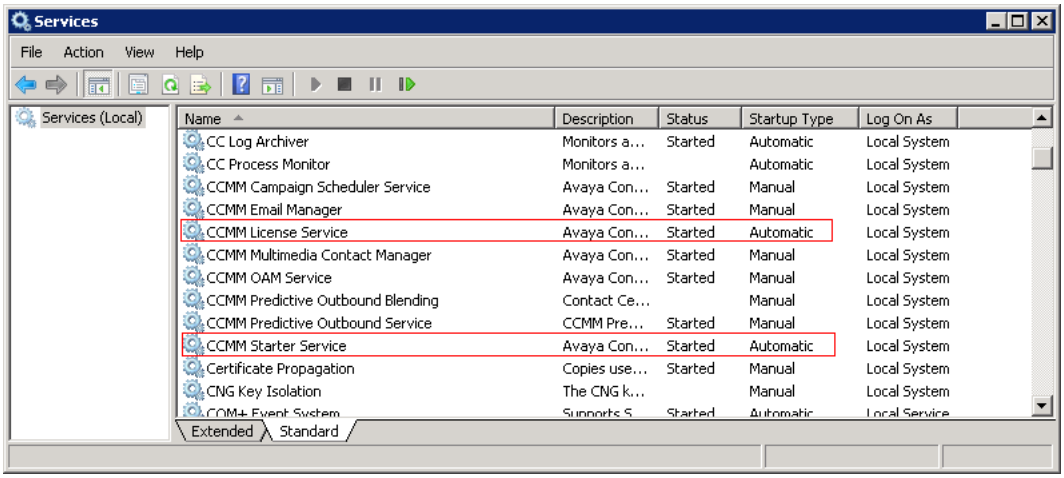
--End--

Verifying that Contact Center Multimedia services start

Verify that Contact Center Multimedia services start to ensure that contacts are routed immediately after the server restarts for any reason.

Procedure steps

Step	Action
1	On the standby Voice and Multimedia Contact Server, click **Start**, **Administrative Tools**, **Services**.
2	In the **Services** window, verify that the **CCMM License Service** status is **Started** and the startup type is **Automatic**.
3	In the **Services** window, verify that the **CCMM Starter Service** status is **Started** and the startup type is **Automatic**.



4 Verify that the following services started:

- CCMM Multimedia Contact Manager
- CCMM OAM service
- CCMM Campaign Scheduler service
- CCMM Email Manager

5 If any service does not start, in the **Services** window, right-click the service name, and click **Start**.

--End--

Providing local users with Log on as a service right

Provide local users with log on as a service right to ensure that administrators and the agents in your Contact Center have access to the Contact Center Agent Desktop application.

Procedure steps

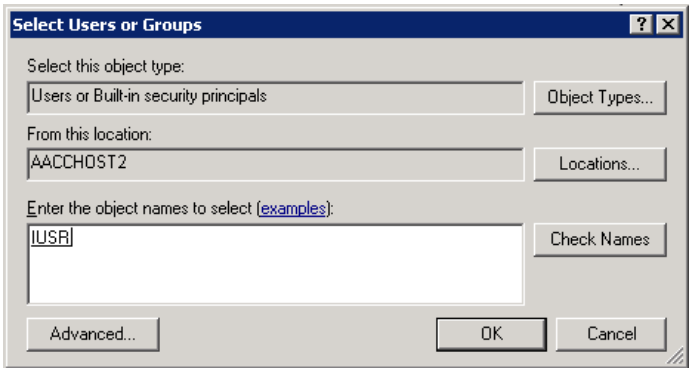
Step	Action
1	Click **Start**, **Administrative Tools**, **Local Security Policy**.
2	Under **Security Settings**, in the left pane, double-click **Local Policies**.
3	In the left pane, click **User Rights Assignment**.
4	In the right pane, double-click **Log on as a service**.
5	Click **Add User or Group**.
6	Click **Locations**.

7 In the **Locations** dialog box, select the Voice and Multimedia Contact Server name from the list.

8 Click **OK**.

9 In the **Enter the object name to select** box, type **IUSR**.

10 Click **Check Names** to verify that the user name exists on the local computer.



11 Click **OK**.

12 Click **Apply** to save the changes.

13 Click **OK**.

14 Close the **Local Security Settings** window.

--End--

Configuring the MIME types

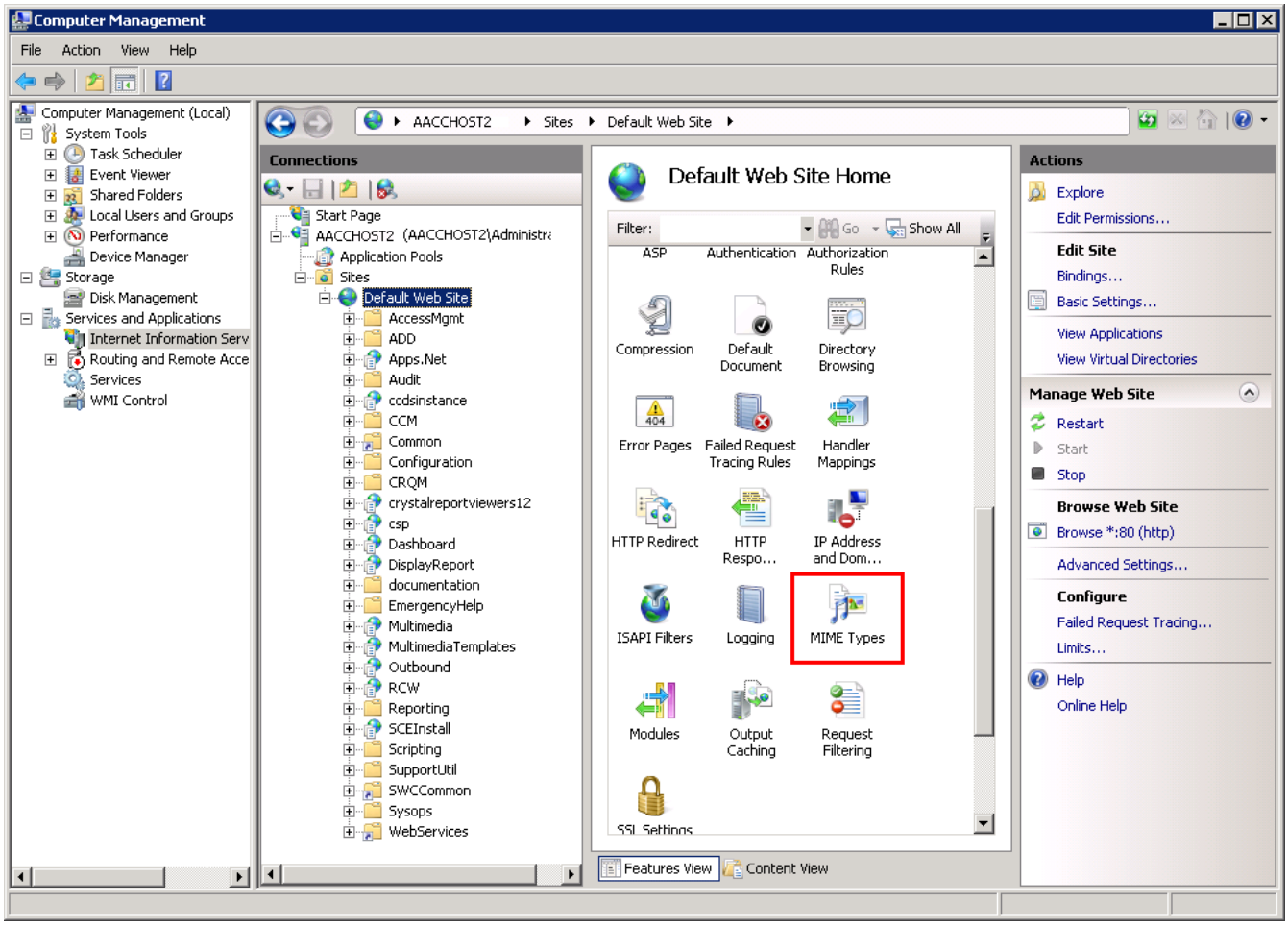
Configure the Multipurpose Internet Mail Extension (MIME) types to ensure that agents can access email message attachments.

If any of these MIME types are already configured, skip the configuration steps for that MIME type.

Procedure steps

Step	Action
1	On the Voice and Multimedia Contact Server, click **Start**, **Administrative Tools**, **Computer Management**.
2	In the **Computer Management** dialog box, expand **Services and Applications**, **Internet Information Services (IIS) Manager**.
3	In the **Connections** pane, under the Host Server (AACCHOST2) name, select **Sites**.
4	Select **Default Web Site**.

5 In the **Default Web Site Home** pane, under **IIS**, select **MIME Types**.

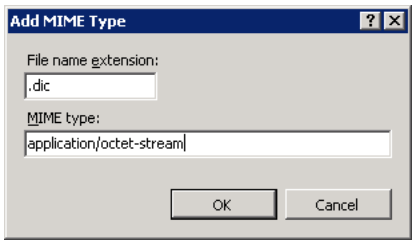


6 Double-click **MIME Types**.

7 On the **Actions** list on the right pane, click **Add**.

8 In the **File name extension** box, type **.dic**.

9 In the **MIME Type** box, type **application/octet-stream**.

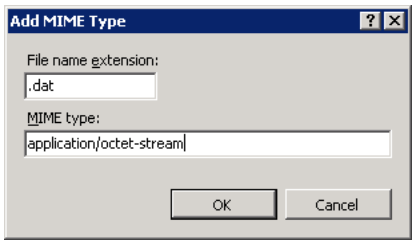


10 Click **OK**.

11 On the **Actions** list on the right, click **Add**.

12 In the **File name extension** box, type **.dat**.

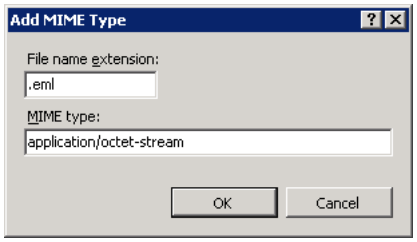
13 In the **MIME Type** box, type **application/octet-stream**.



14 Click **OK**.

15 From the **MIME Types** list, locate .eml and select **Edit** from the **Actions** list on the right.

16 In the **MIME Type** box, type **application/octet-stream**.



17 Click **OK**.

18 Close the **Computer Management** window.

--End--

High Availability – Voice and Multimedia Contact Server commissioning

This section describes how to configure Mission Critical High Availability (HA) resiliency for a pair of Voice and Multimedia Contact Servers in a campus SIP-enabled contact center environment that uses an Avaya Aura® Communication Manager and an Avaya Aura® Session Manager.

Both Voice and Multimedia Contact Servers have the following components installed:

- Contact Center Manager Server (CCMS)
- Contact Center License Manager (LM)
- Contact Center Manager Administration (CCMA)
- Communication Control Toolkit (CCT)
- Contact Center Multimedia (CCMM)
- Contact Center Orchestration Designer (OD)

Both Voice and Multimedia Contact Servers have the same disk drive partitions and the same Contact Center patches installed.

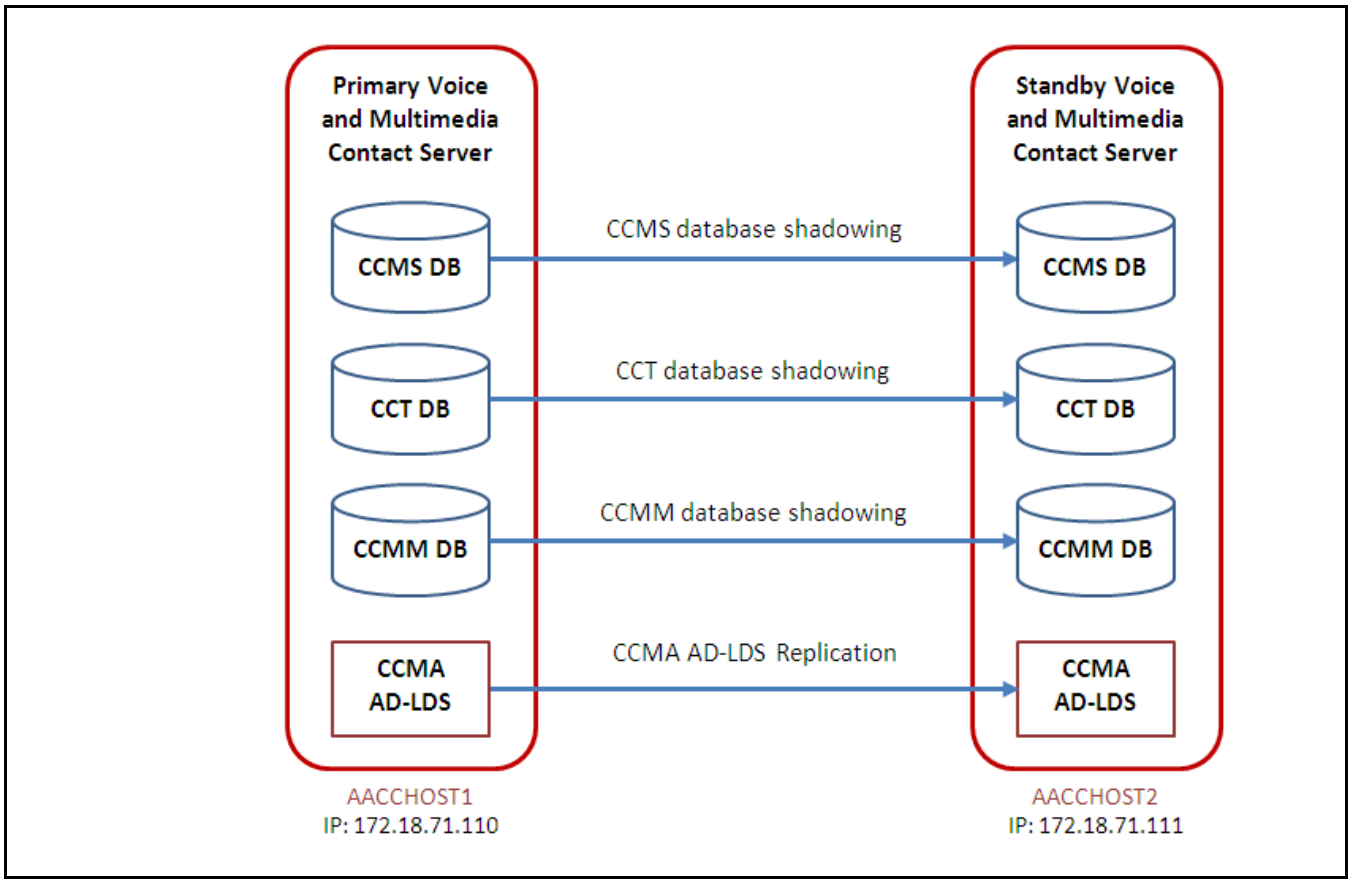
Example server details	
Active server name	AACCHOST1
Active server IP Address	172.18.71.110
Standby server name	AACCHOST2
Standby server IP Address	172.18.71.111
Managed name	AACCMANHOST
Managed IP Address	172.18.71.112

Ask your Domain Administrator to add a Domain Name System (DNS) static entry for the active and standby servers and one additional DNS static entry for each Managed name and associated Managed IP address.

Mission Critical High Availability campus overview

In a Voice and Multimedia Contact Server HA configuration, one server is the active server and one is the standby server. The active Voice and Multimedia Contact Server actively processes scripts and contacts, and records statistics. The standby server shadows the active server. The standby server copies all configuration changes made on the active server and monitors the active server status. If the active server fails, the standby server, running in Mission Critical standby mode, recognizes the failure and starts processing contacts. After the switchover, High Availability is disabled on the original active server.

Example of High Availability Voice and Multimedia Contact Servers



The active and standby Voice and Multimedia Contact Servers are part of the same Avaya Aura® Contact Center and they must be in the same subnet IP address range for campus High Availability resiliency to work.

The standby server must be configured exactly the same as the active server. The standby and active servers must have the same patch level and the same hard disk drive partitions. Configuration changes made to the active Voice and Multimedia Contact Server during normal operation are automatically copied to the standby server so that the standby server can take over processing from the active server when necessary.

If the Contact Center Administrator uses the Windows Service Control Manager (SCM) to stop a monitored service on an active server, a switchover occurs. If the Contact Center Administrator uses the System Control and Monitor Utility (SCMU) to stop a monitored service on an active server, a switchover does not occur.

If a critical service on the standby server stops or is stopped, the standby server stops all services and the contact center solution is no longer resilient. To reinstate High Availability resiliency, use SMMC to "Start HA System" on the standby server.

High Availability Utility

Configure High Availability resiliency for CCMS, CCT, and CCMM using the High Availability (HA) Utility in the Database Utilities. The High Availability Utility is used to configure which server is the active and which is the standby server. The HA utility also configures the Managed IP of the active server.

The High Availability Utility on an active server has the following dialogs under the Configuration tab:

- Server Mode
  - Configure the IP address for the active and standby servers.
  - Configure the IP address for Trusted servers.
  - Configure the IP address for the optional Remote Geographic Node.
  - Identify if the server is active or standby.
  - Enable Switchover.
  - Configure the switchover time-out. This is the wait time if a network outage occurs before an automatic switchover occurs.
- Notifications
  - Configure an email server for email notifications.
  - Configure where and how often to send email notifications.
  - Configure the email character set.
- System
  - Display information on the system status.
  - Verify that database shadowing is running.

SMMC system tray

The Contact Center System Management and Monitoring Component (SMMC) system tray gives quick access to action items in your High Availability environment, for example:

- Start HA System
- Stop HA System
- Disable Switchover
- Enable Switchover
- System Information
- Database Information

To access the SMMC system tray menu, right-click the SMMC icon on the Windows taskbar.

High Availability Utility and SMMC system tray

Use the High Availability Utility to configure High Availability IP addresses and to configure which server is the active server and which server is the standby server. Then use the System Management and Monitoring Component (SMMC) system tray to start database shadowing and High Availability functionality.

Determining the High Availability Network Timeout threshold

The level of Contact Center application High Availability you achieve depends on your complete enterprise contact center solution, including the underlying network infrastructure.

It is important that you determine the optimum High Availability SMMC Network Timeout threshold value for your contact center network. If the threshold is set too high, High Availability may not recognize network outages, switchover may not occur when necessary and call control may be lost. If the threshold is set too low, frequent and unnecessary switchovers may occur.

SMMC tests network connectivity between High Availability components and records the details of these connectivity tests in trace log files. The SMMC trace log files contain sufficient statistical data about SMMC communications in your network to characterize the network behavior for a High Availability contact center solution. You can use this SMMC statistical communications data to optimize your High Availability solution.

Avaya recommends that you analyse the SMMC trace log file and use the connectivity test results in it to optimize the High Availability settings for your network. For more information about optimizing your High Availability configuration settings to your network, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).

Prerequisites

- Ensure the Avaya Aura® Unified Communications platform is installed and patched to support Avaya Aura® Contact Center High Availability.
- Ensure that the standby server meets or exceeds the minimum hardware and platform requirements as specified in *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
- The active and standby servers must meet the planning and engineering specifications. For more information, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
- License Manager is installed on the active and the standby server.
- The active and standby server have a valid standby server license file.

Resolving the Managed name to the Managed IP Address

Complete the following procedure for the active and standby servers to resolve the Managed server name to the Managed IP address.

Attention: Avaya Aura® Contact Center High Availability solutions do not support Windows Server 2008 Dynamic DNS.

Ask your Domain Administrator to add a Domain Name System (DNS) static entry for the active and standby servers and one additional DNS static entry for each Managed name and associated Managed IP address.

A typical High Availability campus solution with a pair of servers requires three DNS static entries; one DNS static entry for the active server, one DNS static entry for the standby server, and one DNS static entry for the Managed name and associated IP address.

Perform this procedure for both the active and standby servers.

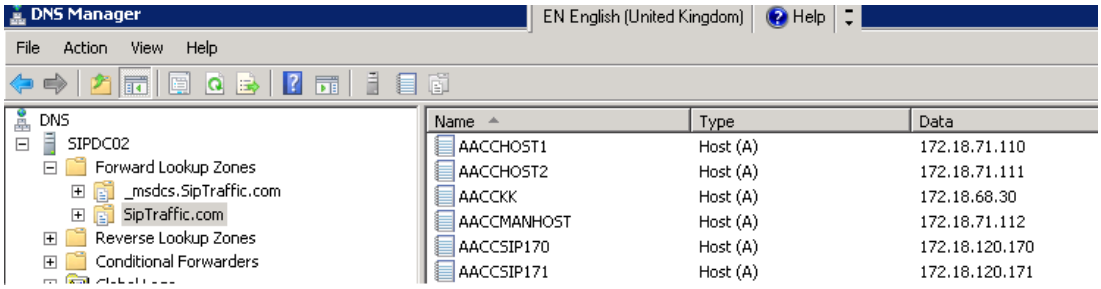
Procedure steps

Step	Action
1	Ask your Domain Administrator to add a Domain Name System (DNS) static entry for the active and standby servers and one additional DNS static entry for each Managed name and associated Managed IP address.

--End--

Procedure job aid

The following DNS window shows the three static entries in the siptraffic.com domain. The active (primary) server - hostname AACCHOST1 with an IP address 172.18.71.110. The backup (secondary) server - hostname AACCHOST2 with an IP address 172.18.71.111. And the Managed name and Managed IP - AACCMANHOST and 172.18.71.112.



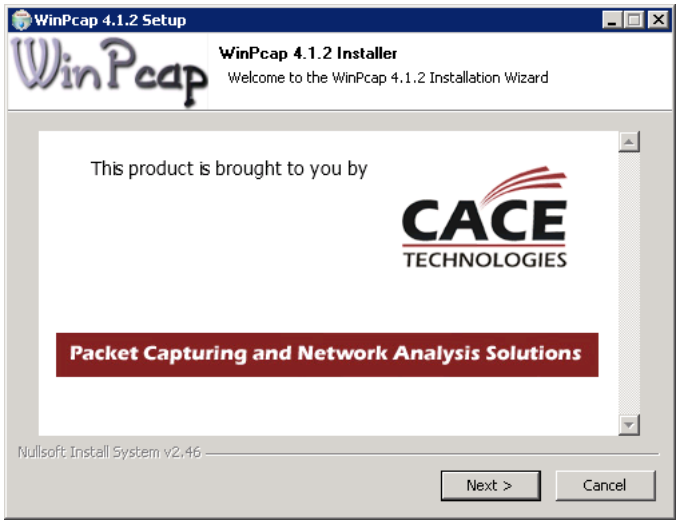
Installing a third-party utility to support High Availability

Install a third-party utility required by the Avaya Aura® Contact Center High Availability feature.

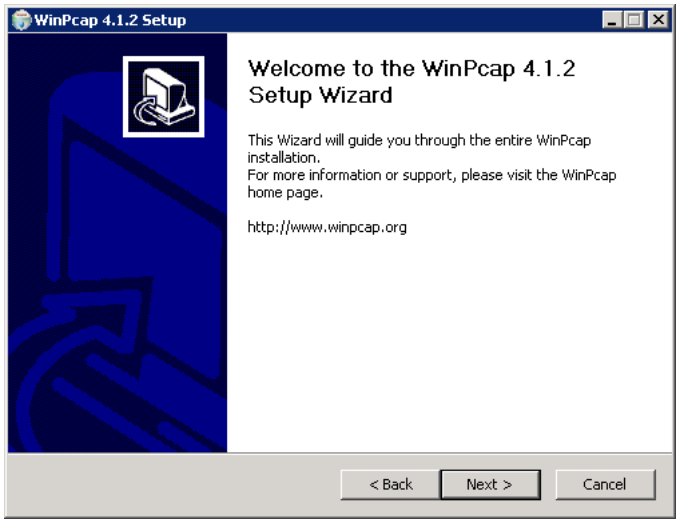
Perform this procedure on both the active and standby servers.

Procedure steps

Step	Action
1	Log on to the active server.
2	Using Windows Explorer, navigate to D:\Avaya\Contact Center\Manager Server\CCSMMC\thirdparty\winpcap.
3	Double-click **WinPcap_4_1_2.exe**.



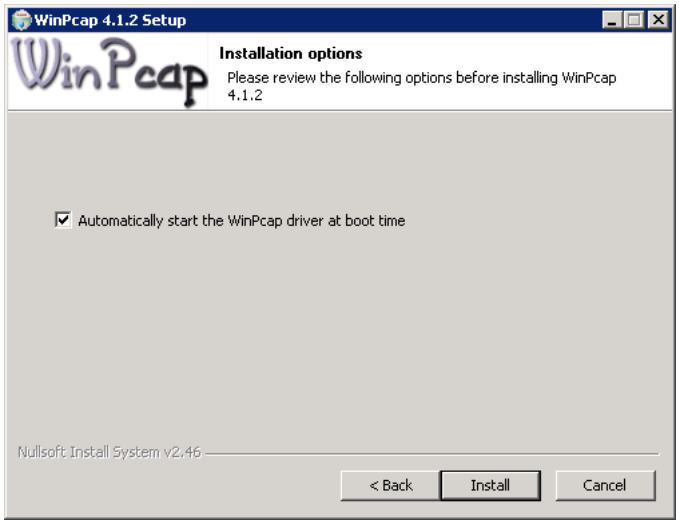
4	On the **WinPcap** installer dialog, click **Next**.



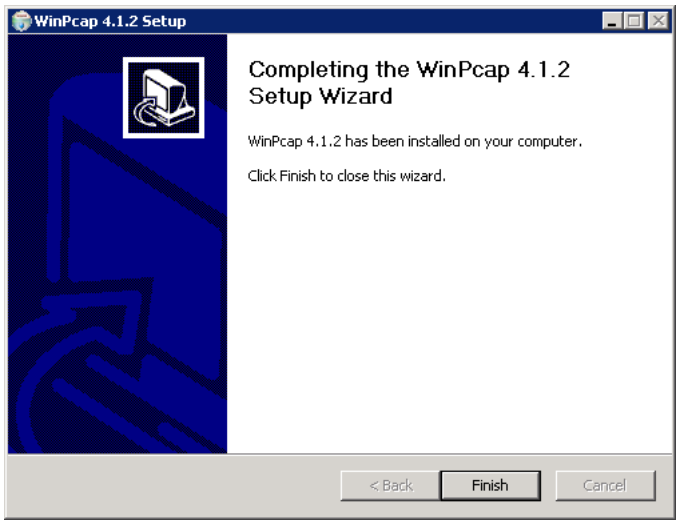
5 On the WinPcap installer **Setup Wizard** dialog, click **Next**.

6 On the WinPcap installer **License Agreement** dialog, click **I Agree**.

7 On the WinPcap installer **Installation options** dialog, click **Install**.



8 On the WinPcap installer dialog, click **Finish**.



9 Repeat this procedure on the standby server.

--End--

Configuring CCMM General Administration

In a multimedia-enabled solution Avaya Aura® Agent Desktop client software is typically downloaded from Contact Center Multimedia (CCMM). Avaya Aura® Agent Desktop then communicates with Contact Center Multimedia to handle email contacts. Avaya Aura® Agent Desktop also communicates with Communication Control Toolkit (CCT) to handle voice contacts.

In a multimedia-enabled High Availability solution use the CCMM Administration tool to configure the standby CCMM and CCT server details. Avaya Aura® Agent Desktop client software downloads the standby server details and communicates with the standby servers if it cannot communicate with the active CCMM or CCT servers.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration. For example, in the **Address** box in Internet Explorer, type: http://AACCHOST1
2	On the CCMA **Launchpad**, click **Multimedia**.
3	In the left column, select the server on which you want to configure server settings. For example select AACCHOST1.

4 In the right pane, click **Launch Multimedia Client**.

5 In the left column, select **General Administration**.

6 Click **Server Settings**.

7 Ensure that **Contact Center Manager Server** is configured with the Managed IP address of the Voice and Multimedia Contact Server High Availability pair. For example type 172.18.71.112.

8 Ensure that **Contact Center Manager Administrator** is configured with the Managed IP address of the Voice and Multimedia Contact Server High Availability pair. For example type 172.18.71.112.

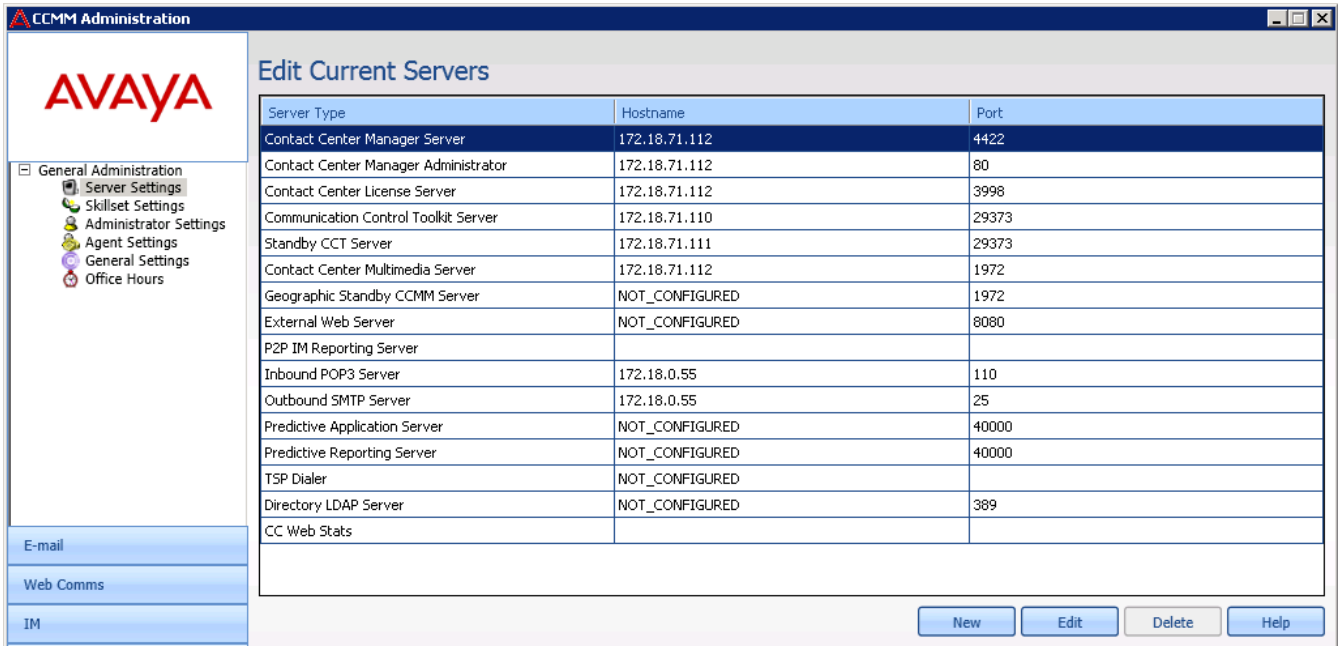
9 Ensure that **Contact Center License Server** is configured with the Managed IP address of the Voice and Multimedia Contact Server. For example type 172.18.71.112.

10 Ensure that **Communication Control Toolkit Server** is configured with the name or IP address of the active Voice and Multimedia Contact Server. For example type 172.18.71.110.

11 Ensure that **Standby CCT Server** is configured with the name or IP address of the standby Voice and Multimedia Contact Server. For example type 172.18.71.111.

12 Ensure that the **Standby CCT Server** port is 29373.

13 Ensure that **Contact Center Multimedia Server** is configured with the Managed IP address of the Voice and Multimedia Contact Server High Availability pair. For example type 172.18.71.112.



--End--

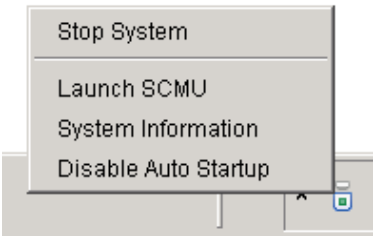
Verifying services are ready for High Availability

Verify that all services stop before you configure High Availability. This ensures that all resources are available to the active server when it starts.

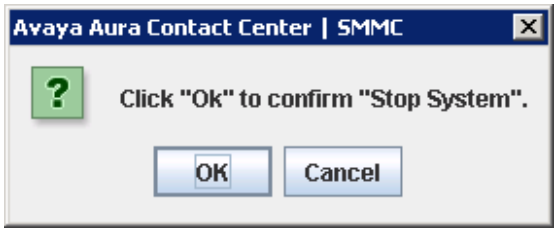
Perform this procedure using the System Management and Monitoring Component (SMMC) on both the active and standby servers.

Procedure steps

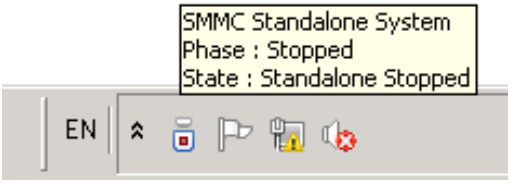
Step	Action
1	Log on to the active server.
2	On the Windows System Tray, right-click on the System Management and Monitoring Component (SMMC) system tray icon, and select **Stop System**.



3	On the SMMC message box, click **OK**.



4	Select the SMMC system tray to confirm the services have stopped.



5	Repeat this procedure on the standby server.

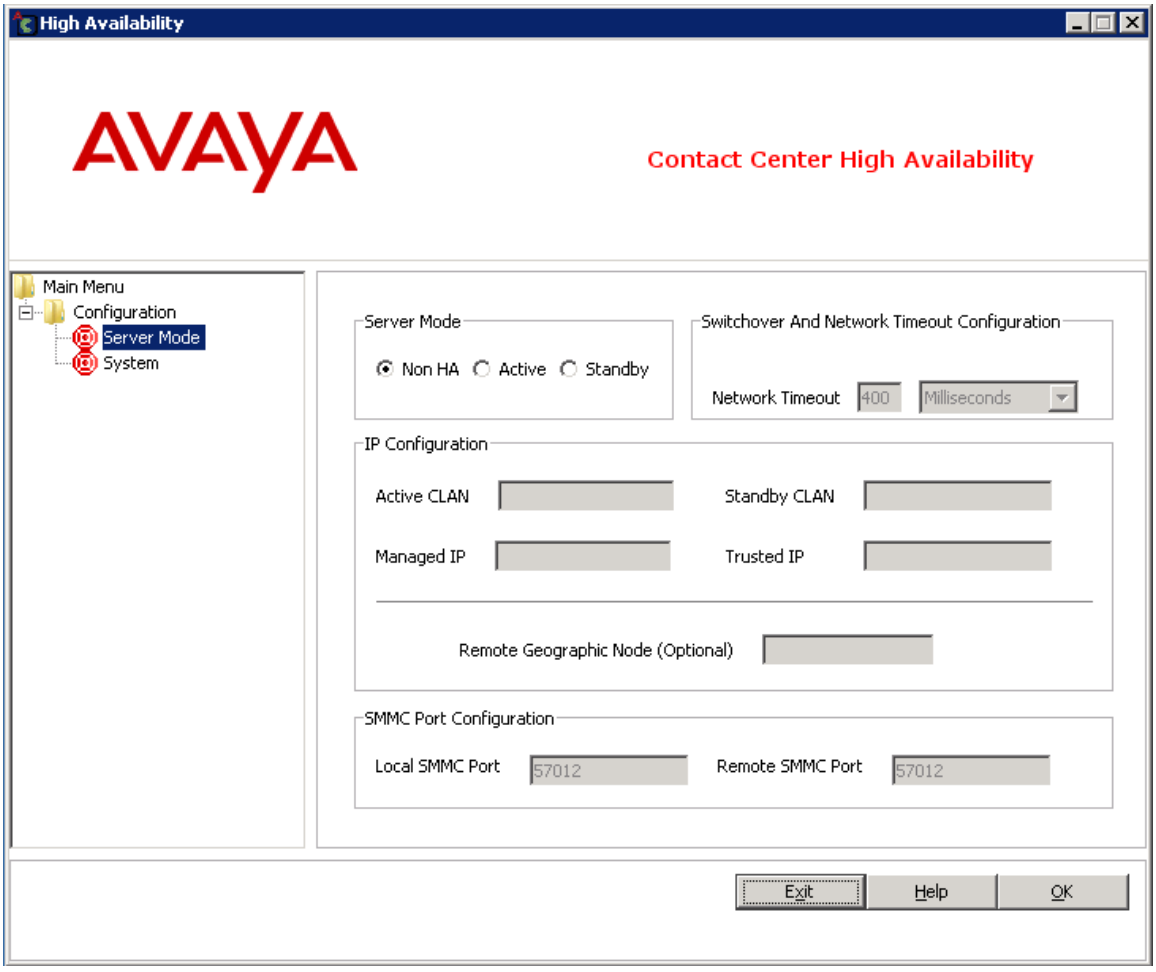
--End--

Configuring High Availability on the active server

Configure High Availability resiliency on the active server using the High Availability Utility. The active server is the Voice and Multimedia Contact Server that normally processes calls.

Procedure steps

Step	Action
1	Select one Voice and Multimedia Contact Server to be the active server and log on. Select AACCHOST1 to be the active Voice and Multimedia Contact Server.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Database Utilities**, **High Availability**.
3	Expand **Configuration**.



4 Double-click **Server Mode**.

5 Under **Server Mode**, select **Active**.

6 Under **IP Configuration**, in the **Active CLAN** box, type the IP address for the active server. For example, type 172.18.71.110.

7 Under **IP Configuration**, in the **Standby CLAN** box, type the IP address for the standby server. For example, type 172.18.71.111.

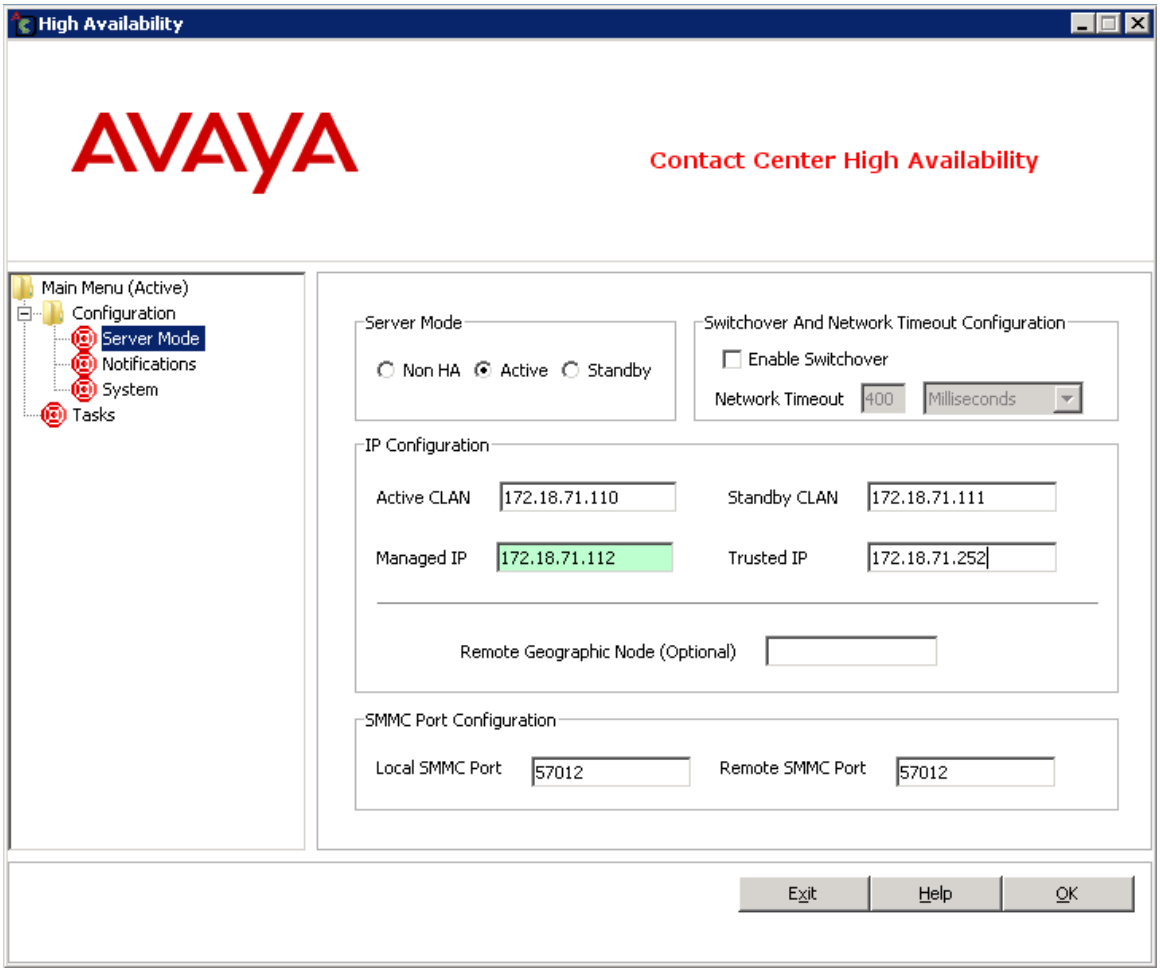
8 Under **IP Configuration**, in the **Managed IP** box, type the managed IP address. For example, type 172.18.71.112.

9 Under **IP Configuration**, in the **Trusted IP** box, type the IP address of a trusted server. For example, type 172.18.71.252.

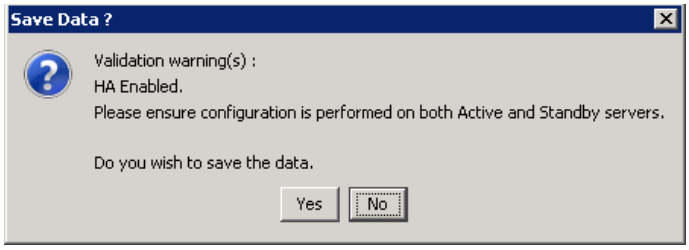
10 Leave the **Remote Geographic Node (Optional)** box blank.

11 Under **SMMC Port Configuration**, in the **Local SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the local (active) server. Accept the default 57012 value. The **Local SMMC Port** number must match the Avaya Media Server - **Failure Notification List** - **Server Port** number. For more information about Avaya Media Server and communication port alignment, see Configuring High Availability on the active server (page 555).

12 Under **SMMC Port Configuration**, in the **Remote SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the remote (standby) server. Accept the default 57012 value.



13 Click **OK**.



14 Click **Yes** on any **Save Data** confirmation dialog boxes that appear.

--End--

Variable definitions

Variable	Value
Network Timeout	The High Availability feature tests network connectivity between HA components by default every 100 milliseconds (100ms). The High Availability—Network Timeout value sets the maximum length of time these network connectivity tests can continue to fail consecutively before corrective action is considered. For example, if Network Timeout is set to 400ms, HA requires 4 consecutive failed network connectivity tests before the remote system is marked as unreachable. In this case, if switchovers are enabled, an attempt to switchover is made. Avaya recommends that you set Network Timeout high enough to be tolerant of normal network latency, but low enough to be responsive if a failure occurs.
Active CLAN	The IP address for the server initially configured in active mode.
Standby CLAN	The IP address for the server initially configured in standby mode.
Managed IP	The virtual Managed IP (MIP) address that is used by the active server for campus resiliency. A MIP is used only when the active and standby servers are in the same subnet.
Trusted IP	The active and standby servers use the Trusted IP address to verify network connectivity. If the active server cannot communicate with the standby server it attempts to communicate with the Trusted IP address. If the active server cannot communicate with the Trusted IP address, if shadowing and switchover are enabled, then the active server stops processing contacts and shuts down. The standby server starts processing contacts, if it cannot communicate with the active server but can communicate with the Trusted IP address. Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.

Configuring email notification on the active server

If an automatic switchover occurs, the High Availability utility can send email messages to configured users at a defined interval.

The default email notification character set is US_ASCII. The following character sets are also supported:

- ISO-8859-1

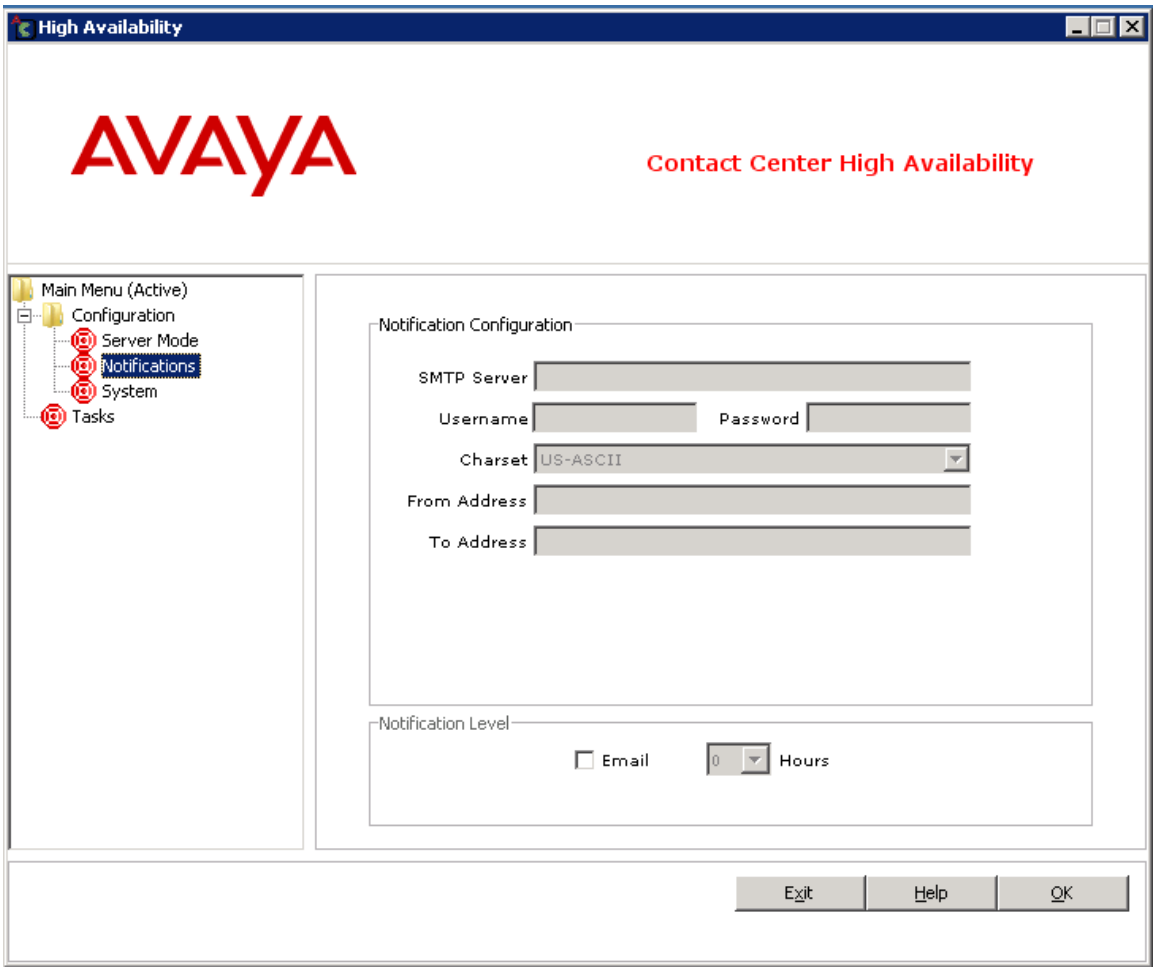
- UTF-16BE
- UTF-8
- UTF-8
- UTF-16BE
- UTF-16LE
- UTF-16

Prerequisites

- If anonymous users are allowed, a user name and password may not be required. Check with the Administrator of the email server for setup configuration.

Procedure steps

Step	Action
1	Log on to the active server.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Database Utilities**, **High Availability**.
3	Expand **Configuration**.
4	Double-click **Notifications**.



5 Select the **Email** check box.

6 In the **SMTP Server** box, type the name or IP address for your email server. For example type 172.18.0.55.

7 In the **Username** box, type an email server user log on name.

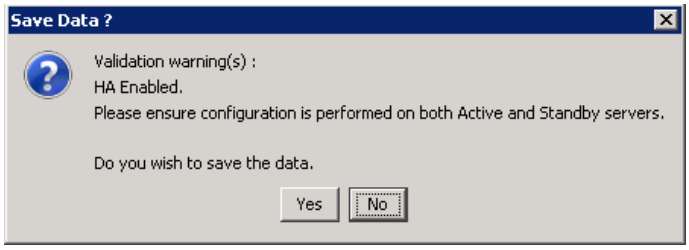
8 In the **Password** box, type email server user log on password.

9 Type the **From Address** email address. For example cust1@labmail.com.

10 Type the **To Address** email address.For example cust2@labmail.com.

11 Click **OK** to save the data.

12 Click **Yes** on any **Save Data** confirmation dialog boxes that appear.



--End--

Variable definitions

Variable	Value
Email	Enables or disables email notifications.
SMTP server	The SMTP server name, which is automatically verified when saving the data.
Username	E-mail User log on name.
Password	E-mail User log on password.
Charset	E-mail character set to use.
From Address	E-mail address to send notifications from.
To Address	E-mail address to send notifications to.

Backing up the active Contact Center Manager Administration

Back up Contact Center Manager Administration to a folder to create a snapshot of the preselected CCMA data files. You can create the folder on the same server or on another domain server.

The Backup and Restore utility is automatically installed on the CCMA server when you install the CCMA software.

You use this utility to back up the files located in the following folders (where D is the drive on which you installed CCMA):

- AD-LDS-specific data stored in the following folder:
  C:\Program Files (x86)\Microsoft ADAM\
- Historical reporting template files (both imported and custom) and Audit Trail event logs stored in the following folders:
  D:\Avaya\Contact Center\Manager Administration\Apps\Reporting\
  D:\Avaya\Contact Center\Manager Administration\Apps\Common\

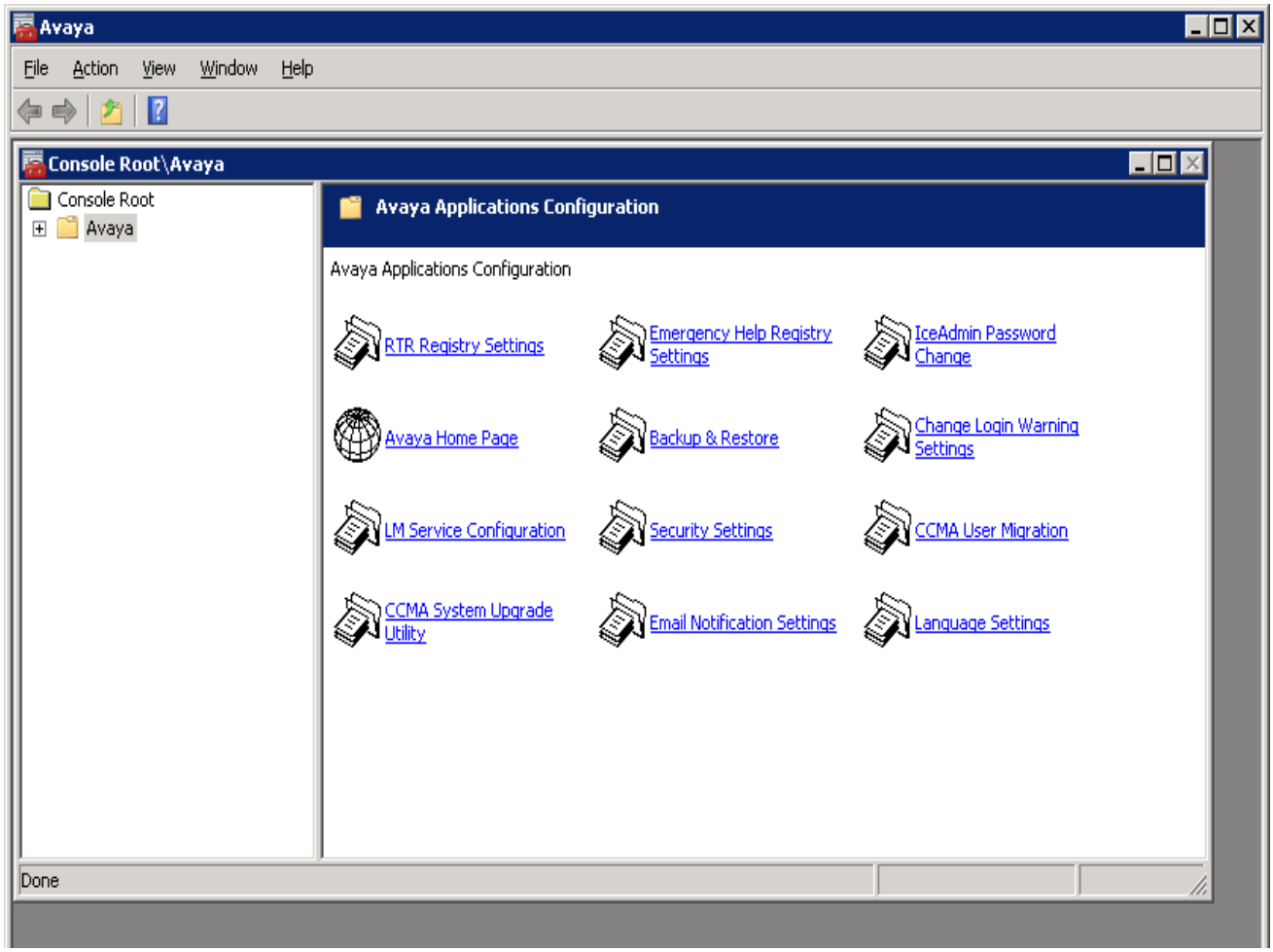
- The Report Creation Wizard database files stored in the following folder: D:\Avaya\Contact Center\Manager Administration\Server\RCW\Data
- A record of displays for real-time reporting exported to the following folder: D:\Avaya\Contact Center\Manager Administration\Apps\Reporting\
- A record of displays for Emergency Help exported to the following folder: D:\Avaya\Contact Center\Manager Administration\Apps\EmergencyHelp\

Prerequisites

- On a backup server, create a shared folder to store the CCMA backup data.
- Ensure that you have write privileges on the server where you want to store the CCMA data you are backing up.
- Log on to the CCMA server with administrative privileges.

Procedure steps

Step	Action
1	Log on to the active server.
2	On the active Voice and Multimedia Contact Server, click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Manager Administration**, **Configuration**.

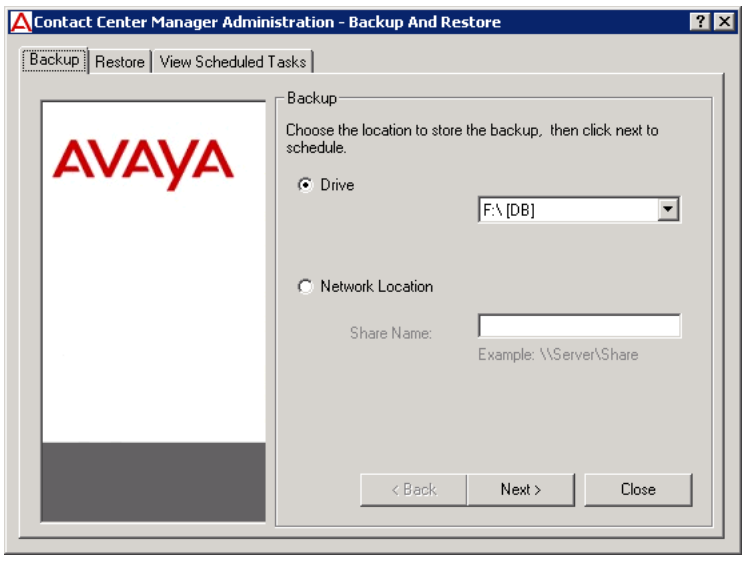


3 In the left pane of the Configuration window, expand **Avaya**, **Applications**.

4 In the **Avaya Applications Configuration** window, select **Backup & Restore**.

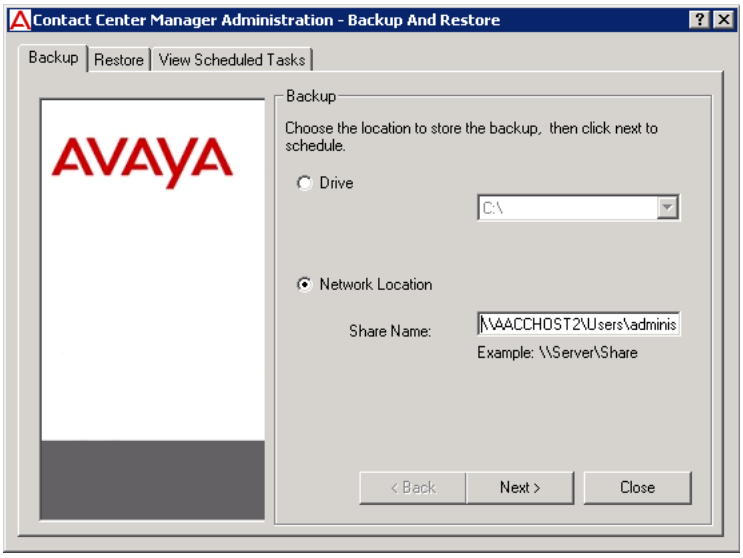
5 In the right-hand pane, click **Backup & Restore**.

6 In the **Contact Center Manager Administration - Backup and Restore** utility, select the **Backup** tab.

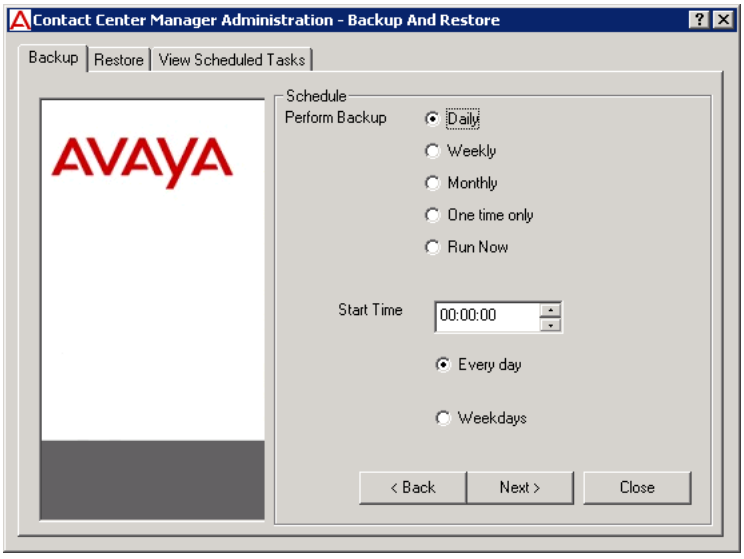


7 In the **Backup** window, select **Network Location**.

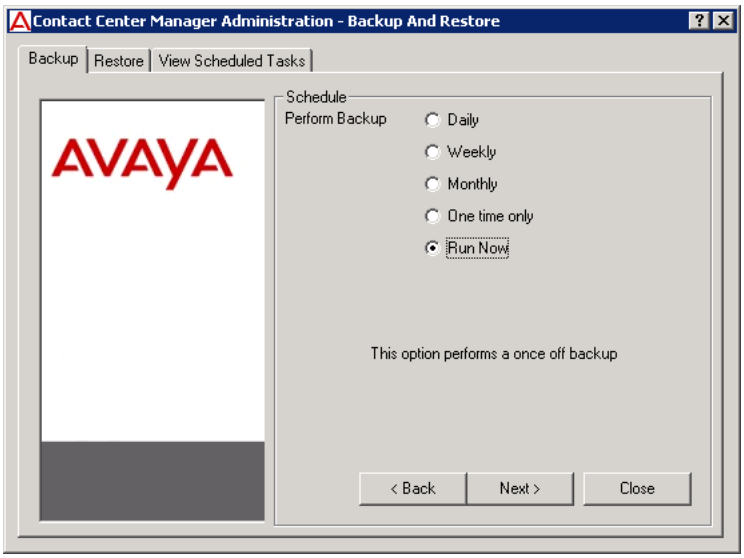
8 In the **Share Name** box, specify the Network Location where you want to store the backup. For example type \\AACCHOST2\Users\administrator\Desktop\DB_store. This is a shared folder on the standby server.



9 Click **Next**.



10 On the **Schedule** page, select **Run Now**.

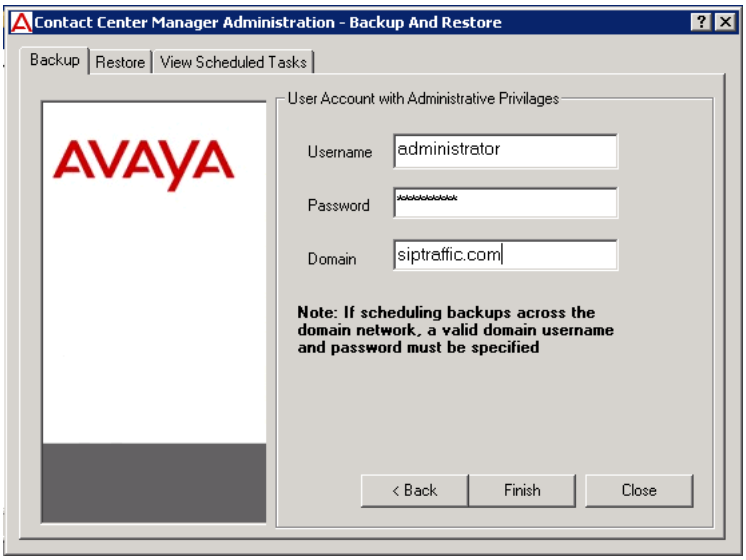


11 Click **Next**.

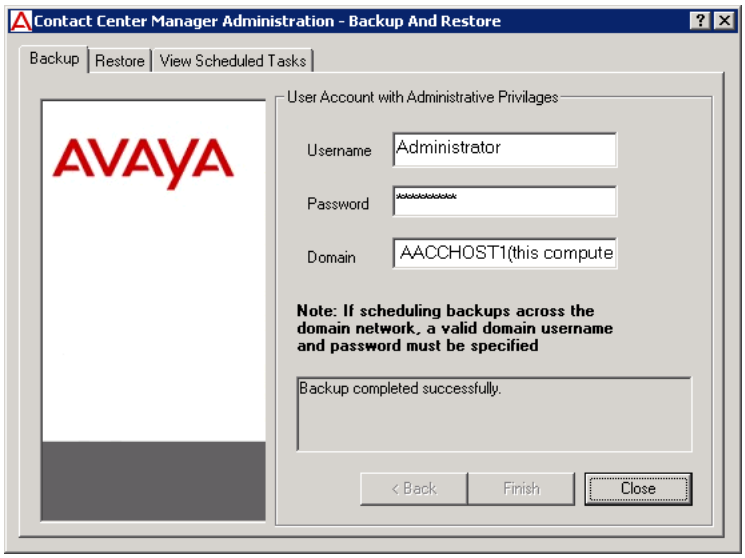
12 In the **Username** box on the **User Account with Administrative Privileges** page, type a valid administrator user name for the server on which you want to store the backup.

13 In the **Password** box, type a the password for the specified administrator user.

14 If you selected a backup location on another server in a domain, type the domain in the **Domain** field. The default option is **this computer** (that is, the Contact Center Manager Administration server on which you are creating the backup).



15 Click **Finish**.



16 Click **Close**.

All backups are saved as CCMAFilesBackup<BackupDateTime>.package.

--End--

Variable definitions

Variable	Value
Drive	The local hard drive where you choose to store the backup. This list shows available local hard drives and any network drives mapped on the server. Note that any drives included in the backup (typically C: and D:) do not appear in the list: these are not supported by the backup application. DVD drives do not appear in the list.
Network Location	The network location where you want to store the backup, in UNC format \\Computer Name\Folder.
Schedule options	The time interval for scheduled backups. This can be • Daily (to schedule recurring backups once a day) • Weekly (to schedule recurring backups once a week) • Monthly (to schedule recurring backups once a month) • One Time Only (to schedule a one-time-only backup at a time in the future) • Run Now (to back up files immediately after you enter a valid username and password) If you select Monthly, you can schedule a task only on the last day of the month that contains the least number of days. For example, if you want the backup to run every month, then you can schedule it to occur on day 28 only. However, if you clear February from the schedule, then the last possible day of a monthly schedule is 30. If you clear April, June, September, and November from the schedule, then the last possible day of a monthly schedule is 31.
Username and Password	You must configure a user name and password with write privileges on the server on which you want to store the backup.
Domain	If you selected a backup location on another server, type that server's domain. The username and password must be valid on this domain and have administrative privileges on the server specified in Network Location.

Procedure job aid

Data files stored on Contact Center servers

Contact Center server	Data files stored on server	Business consequence of CCMA server failure
Contact Center Manager Administration server	• Schedule information for historical reports • Partitions, access classes, report groups, and the Contact Center Manager Administration users • Real-time display configuration data and real-time display filters • Private historical reports • Contact Center Management scheduled assignment information	If the Contact Center Manager Administration server fails, your supervisors and administrators cannot access the Contact Center Manager Administration application. Therefore, access to real-time displays, agent desktop display, schedule information for historical reports, and all data stored on in the application is interrupted.
Contact Center Manager Server	• Agents, supervisors, skillsets and all their related assignments (accessed through Contact Center Management) • CDNs, DNISs and all other data items (accessed through the Configuration component)	If your stand-alone Contact Center Manager Administration server fails, calls continue to be routed according to your defined scripts and your contact center can still receive calls because all user and agent assignments, CDNs, and DNISs are stored on the Contact Center Manager Server.

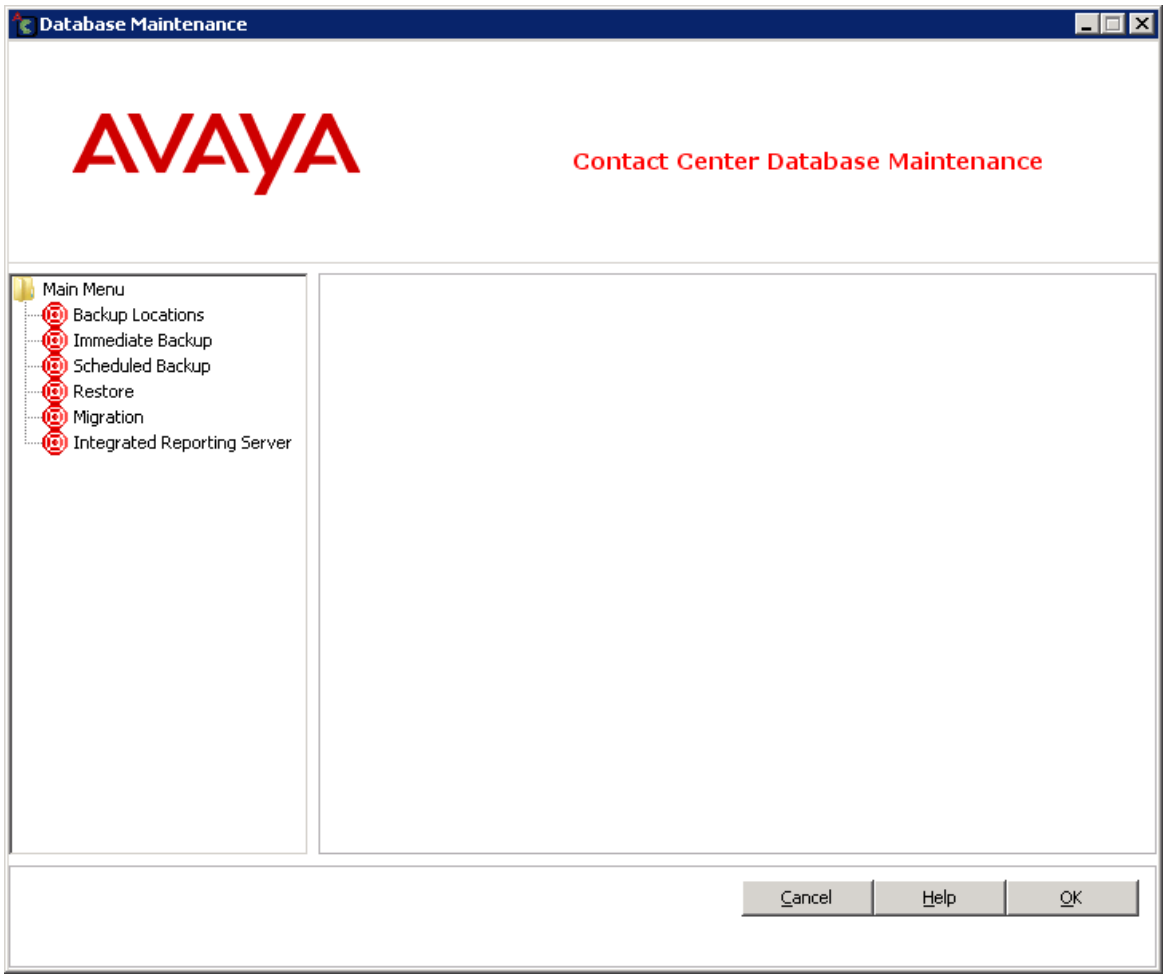
Backing up the database on the active server

The active server is configured for High Availability. Now the standby server must be prepared for High Availability resiliency. Back up the active server to create a snapshot of the database, which is then restored to the standby server. On the active Voice and Multimedia Contact Server all databases must be backed-up.

Attention: You must backup the active server database, restore it onto the standby server, and enable shadowing within 24 hours. If the difference in time between the active and standby server database content is greater than 24 hours, then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the active server database and restore it onto the standby server before re-enabling shadowing. Ensure that the system clock time on the active and standby servers are synchronized.

Procedure steps

Step	Action
1	Log on to the active server.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Database Utilities**, **Database Maintenance**.



3 Click **Backup Locations**.

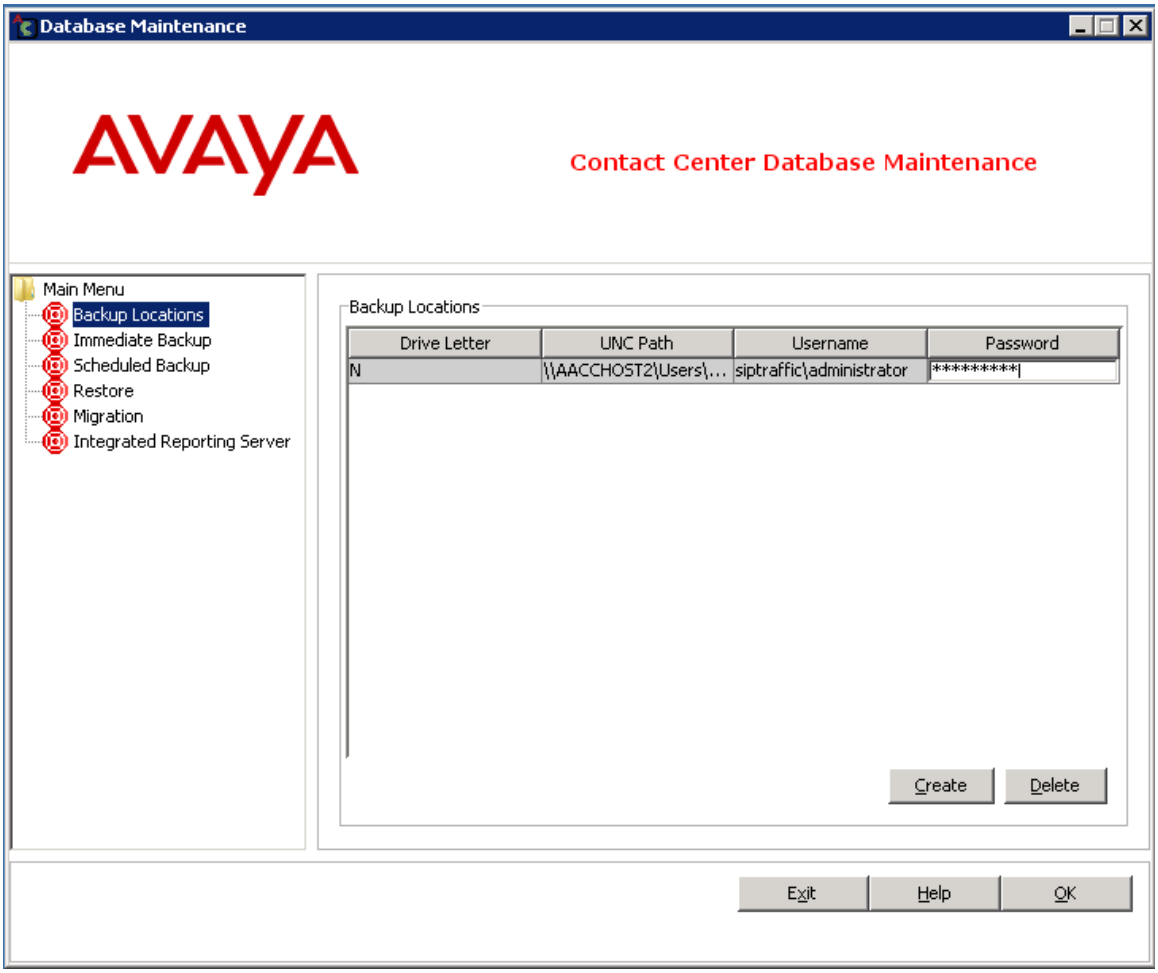
4 Click **Create**.

5 From the **Driver Letter** list, select the network drive on which you want to store the CCMS, CCT, CCMM, and ADMIN databases. For example select **N**.

6 In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Backup Location. This location must be a shared folder with correct permissions. For example, type \\AACCHOST2\Users\administrator\Desktop\DB_store, where "DB_store" is a shared folder on the standby server AACCHOST2.

7 In the **User Name** box, type the user name used to log on to the computer specified in the UNC Path box. For example siptraffic\Administrator.

8 In the **Password** box, type the password of the UNC backup location. For example type the Windows Administrator password for the account specified.



9 Click **OK**.

10 In the left pane, click **Immediate Backup**.

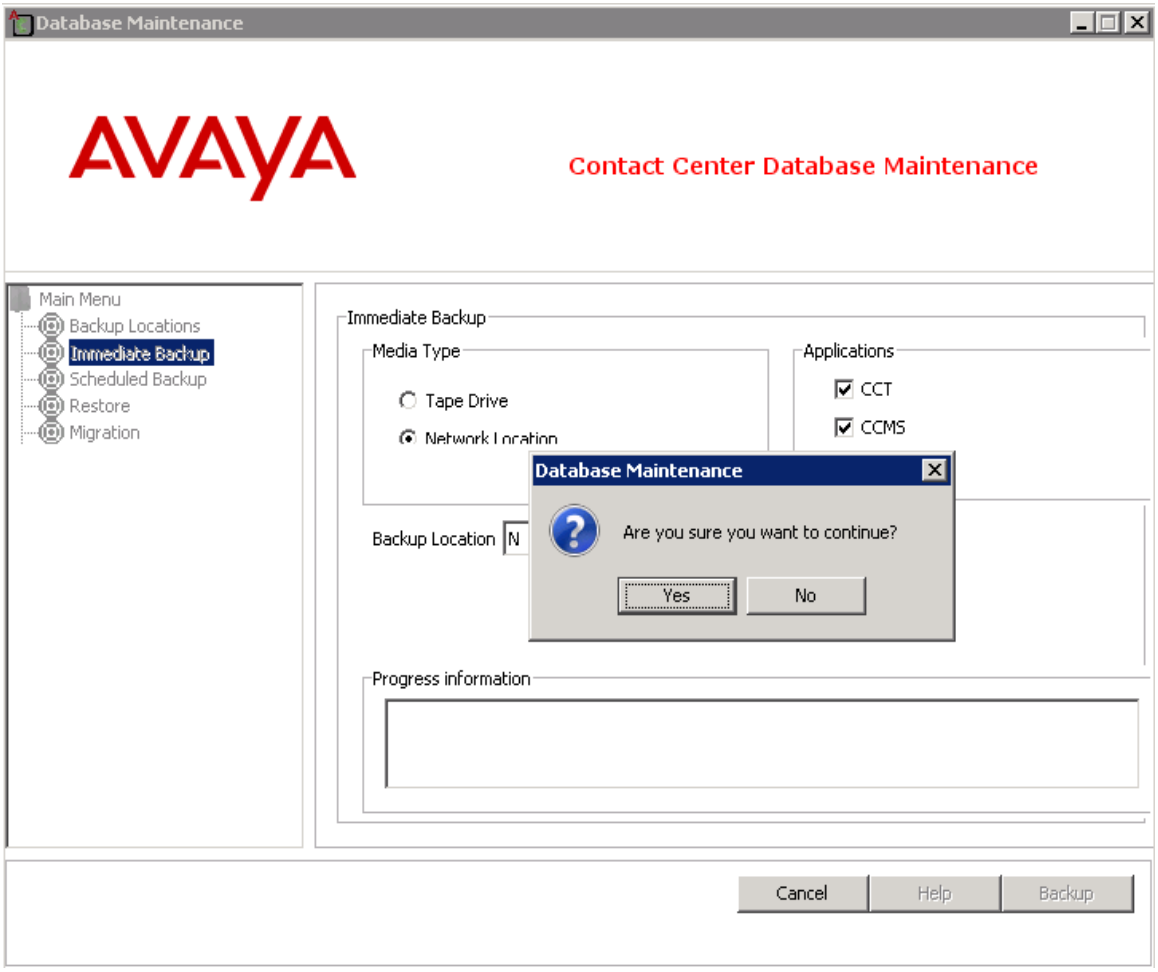
11 In the **Media Type** section, select **Network Location**.

12 In the **Applications** section, select **CCMS**, **CCT**, **CCMM**, and **ADMIN**.

13 From the **Backup Location** list, select the network drive on which to store the backup.

14 Click **Backup**.

15 Click **Yes**, to continue with the backup.



16 When the database backup completes, close the **Database Maintenance** window.

--End--

Restoring the database on the standby server

Restore the database from the active server to the standby server to ensure the databases are consistent. The Database Maintenance utility can restore only one application database at a time. Restore the data for the CCMS, CCT, CCMM, and ADMIN databases.

You must restore the CCMS, CCT, CCMM, and ADMIN database onto the standby server. You must restore the ADMIN database last.

Attention: You must backup the active server database, restore it onto the standby server, and enable shadowing within 24 hours. If the difference in time between the active and standby server database content is greater than 24 hours then database shadowing does not work. If shadowing is stopped for more than 24 hours, then you must backup the active server database and restore it onto the standby server before re-enabling shadowing. Ensure that the system clock time on the active and standby servers are synchronized.

Prerequisites

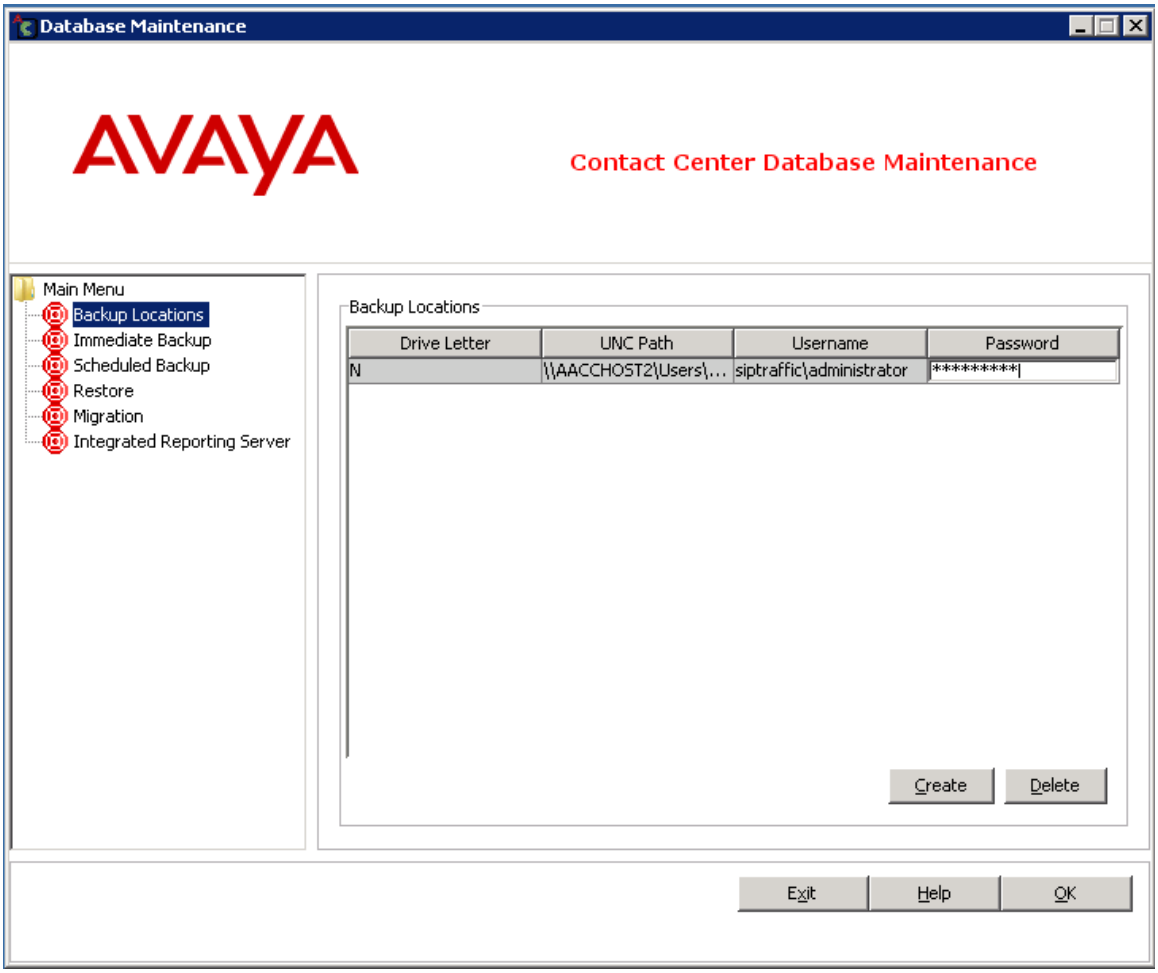
- Know the location of the backup database. Copy the database backups onto the standby server.

Attention: You must restore all databases on a Voice and Multimedia Contact Server. Restoring only CCMS and not CCT, CCMM or ADMIN may leave an inconsistent server and HA cannot shadow data correctly.

Attention: Restoring the Administration (ADMIN) database can change configuration of Backup locations on the standby server if the active server and standby server backup locations are different. Therefore, after you restore the ADMIN database, close and reopen the Database and Maintenance utility.

Procedure steps

Step	Action
1	Log on to the standby server.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Database Utilities**, **Database Maintenance**.
3	Click **Backup Locations**.
4	Click **Create**.
5	From the **Driver Letter** list, select the network drive on which you want to store the CCMS, CCT, CCMM, and ADMIN databases. For example select **N**.
6	In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Backup Location. This location must be a shared folder with correct permissions. For example, type \\AACCHOST2\Users\administrator\Desktop\DB_store, where "DB_store" is a shared folder on the standby server AACCHOST2.
7	In the **User Name** box, type the user name used to log on to the computer specified in the UNC Path box. For example type siptraffic\Administrator.
8	In the **Password** box, type the password of the UNC backup location. For example type the Windows Administrator password for the specified account.



9 Click **OK**.

10 In the **Database Maintenance** dialog box, in the left pane, click **Restore**.

11 In the right pane, under **Media Type**, select the media type on which the backup is restored. For example, select **Network Location**.

12 If the backup file is on the network drive, in the **Backup Location** list, select the backup location. For example, select **N**.

13 Under **Application**, select **CCT**.

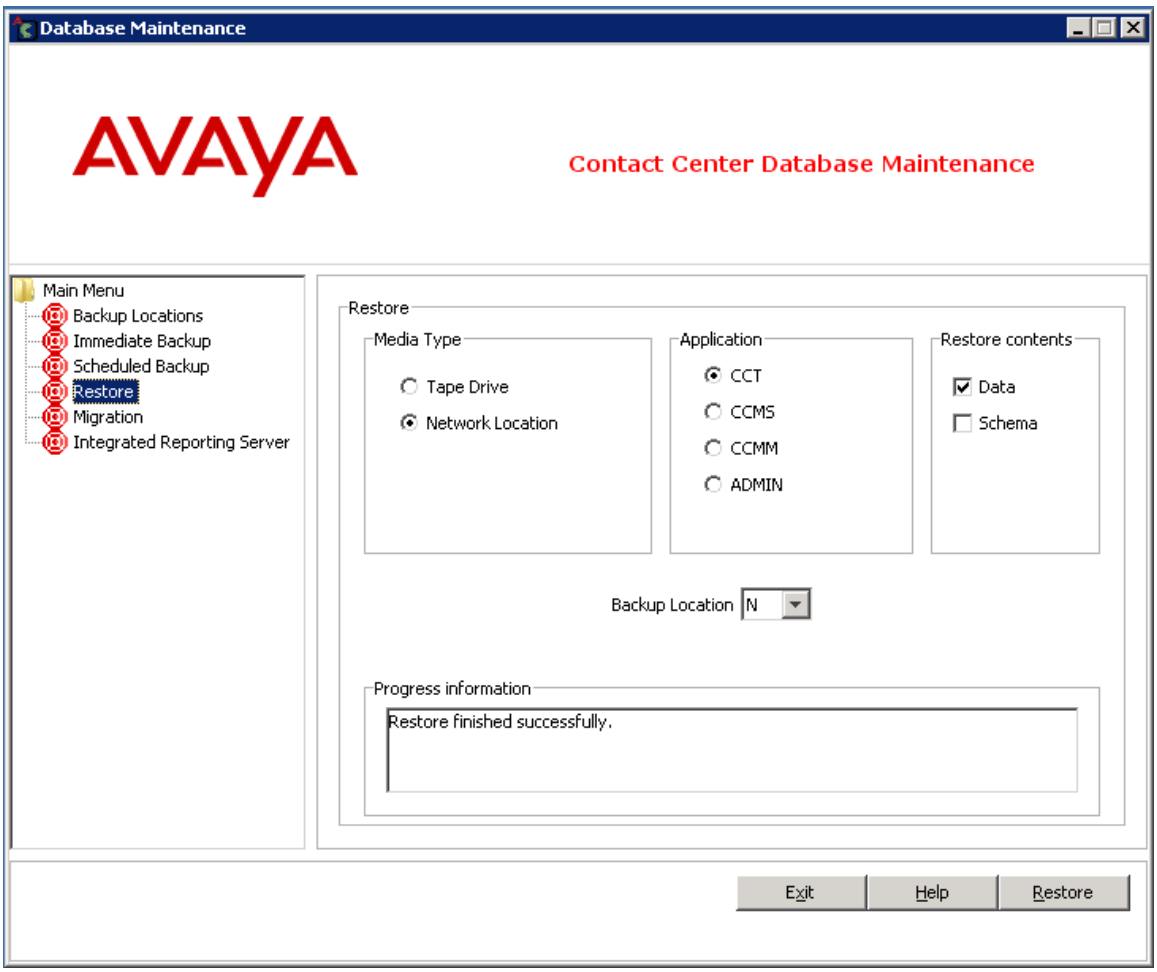
14 Under **Restore contents**, select **Data**.

15 Click **Restore**.

16 To overwrite contents, on the **Database Maintenance** dialog, click **Yes**.

17 Use the **Progress information** field to monitor the progress of the restoration.

18 Click **OK**.



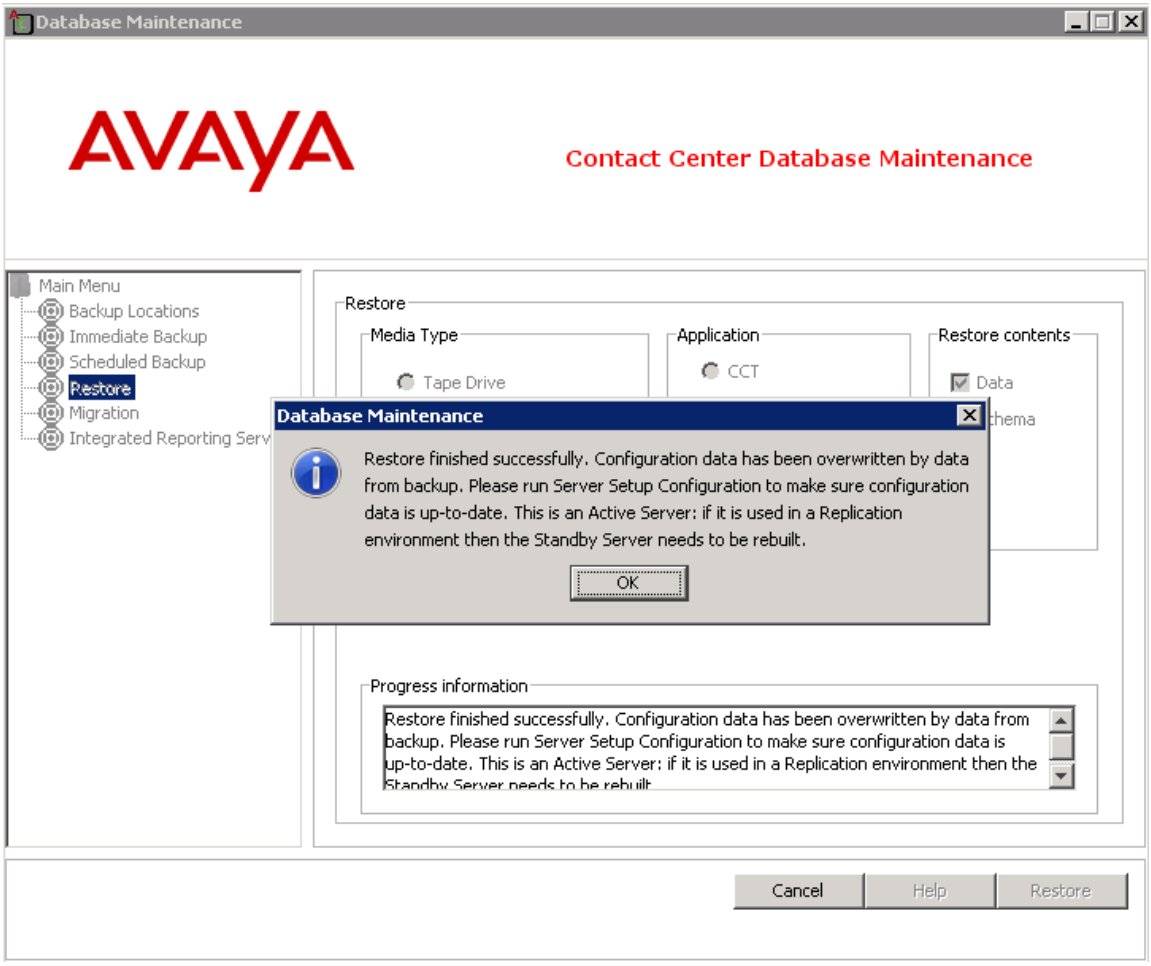
19 Under **Application**, select **CCMS**.

20 Under **Restore contents**, select **Data**.

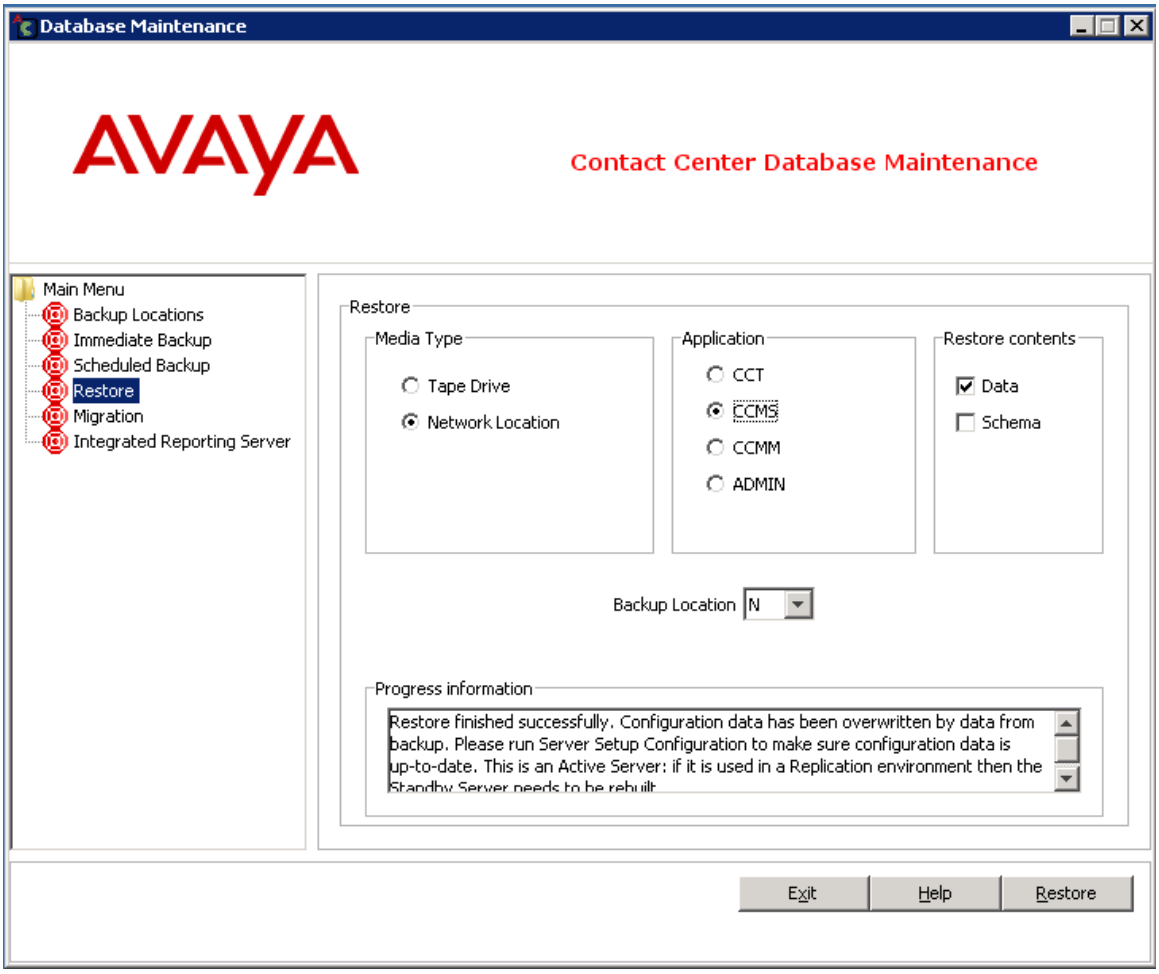
21 Click **Restore**.

22 To overwrite contents, on the **Database Maintenance** dialog, click **Yes**.

23 Use the **Progress information** field to monitor the progress of the restoration.


Database Maintenance
AVAYA
Contact Center Database Maintenance
Main Menu
Backup Locations
Immediate Backup
Scheduled Backup
Restore
Migration
Integrated Reporting Serv
Restore
Media Type
Tape Drive
Application
CCT
Restore contents
Data
thema
Database Maintenance
Restore finished successfully. Configuration data has been overwritten by data from backup. Please run Server Setup Configuration to make sure configuration data is up-to-date. This is an Active Server: if it is used in a Replication environment then the Standby Server needs to be rebuilt.
OK
Progress information
Restore finished successfully. Configuration data has been overwritten by data from backup. Please run Server Setup Configuration to make sure configuration data is up-to-date. This is an Active Server: if it is used in a Replication environment then the
Standby Server needs to be rebuilt
Cancel
Help
Restore

24 Click **OK**.



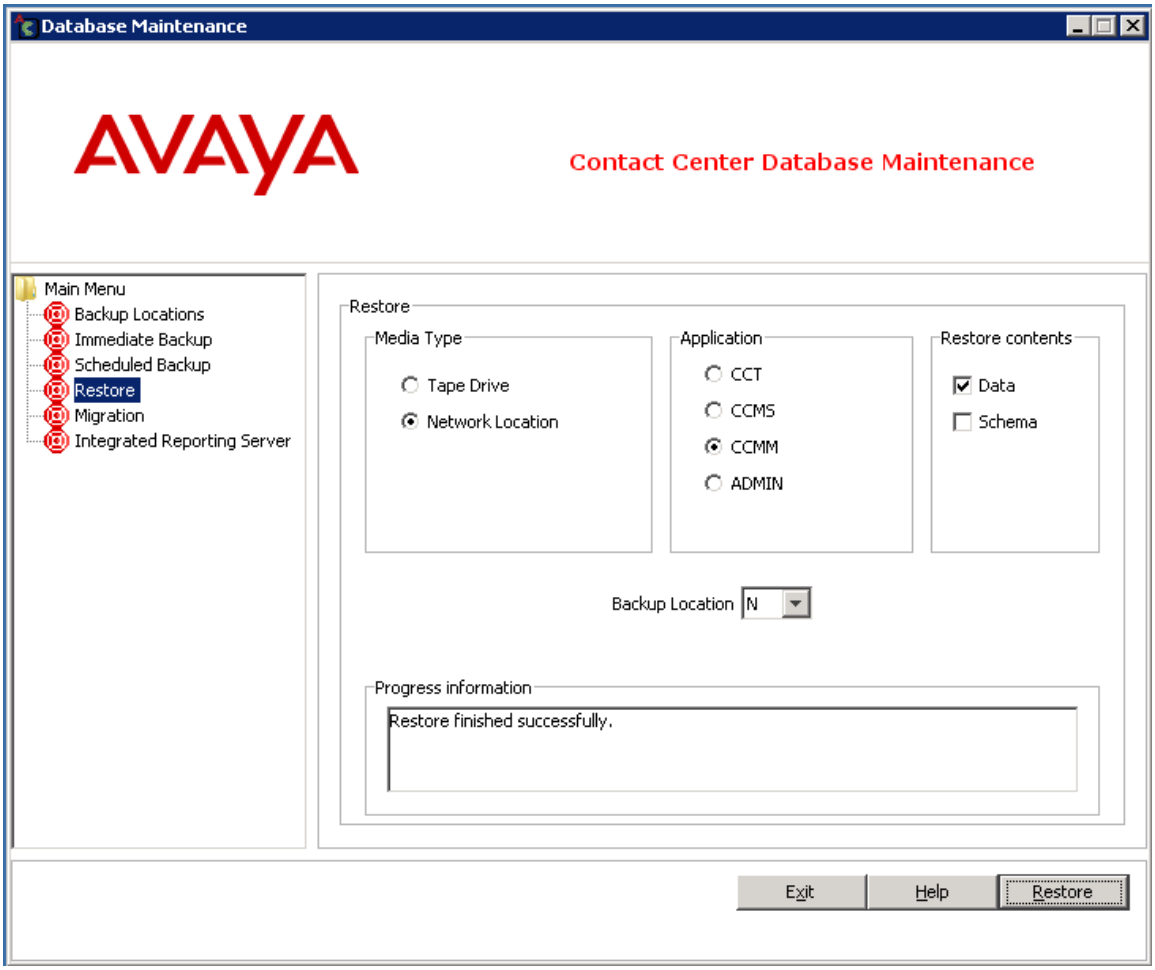
25 Under **Application**, select **CCMM**.

26 Under **Restore contents**, select **Data**.

27 Click **Restore**.

28 Click **OK** to overwrite contents.

29 Use the **Progress information** field to monitor the progress of the restoration.



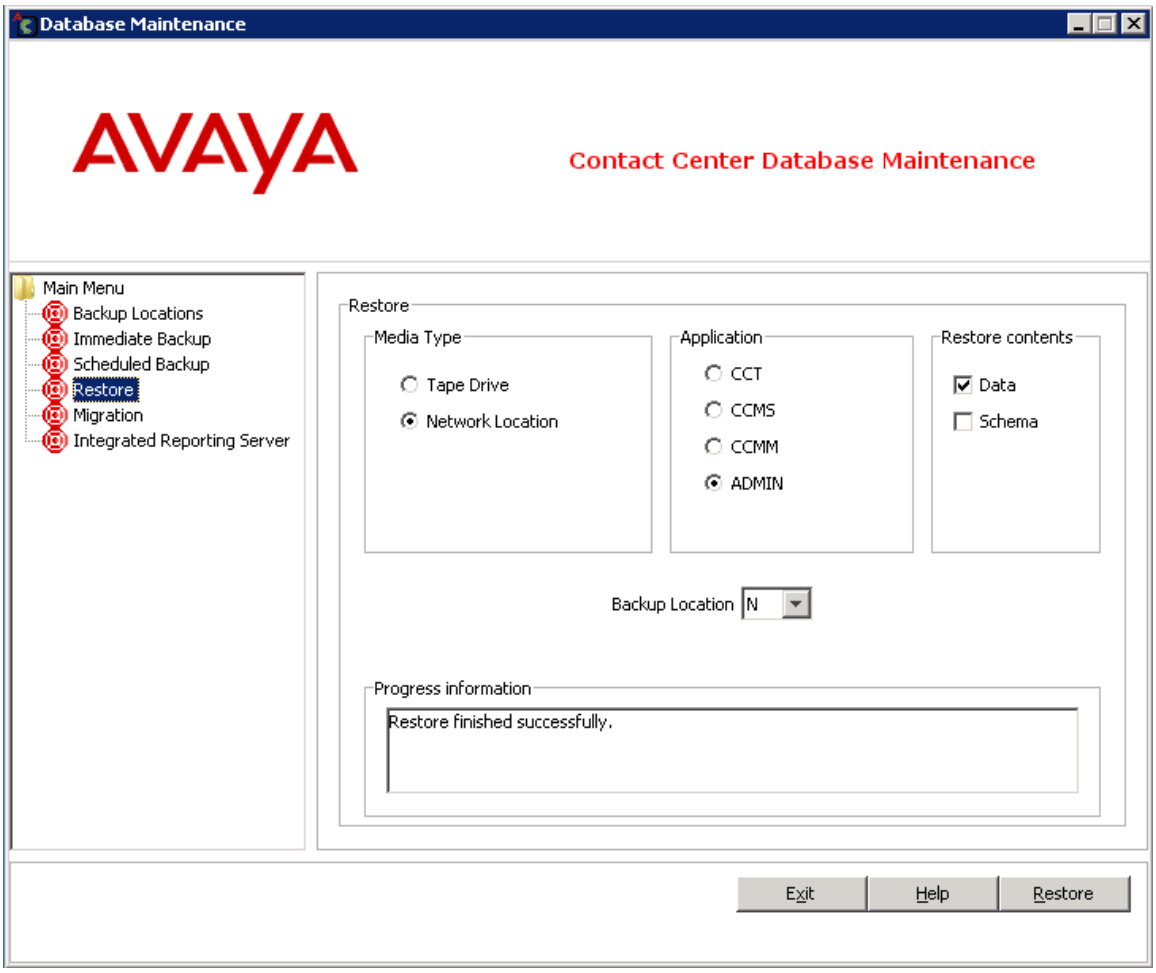
30 Under **Application**, select **ADMIN**.

31 Under **Restore contents**, select **Data**.

32 Click **Restore**.

33 Click **OK** to overwrite contents.

34 Use the **Progress information** field to monitor the progress of the restoration.



35 Click **Exit** to close the Database Maintenance utility.

--End--

Restoring CCMA data to the standby server

Restore the Contact Center Manager Administration data to the standby server.

Prerequisites

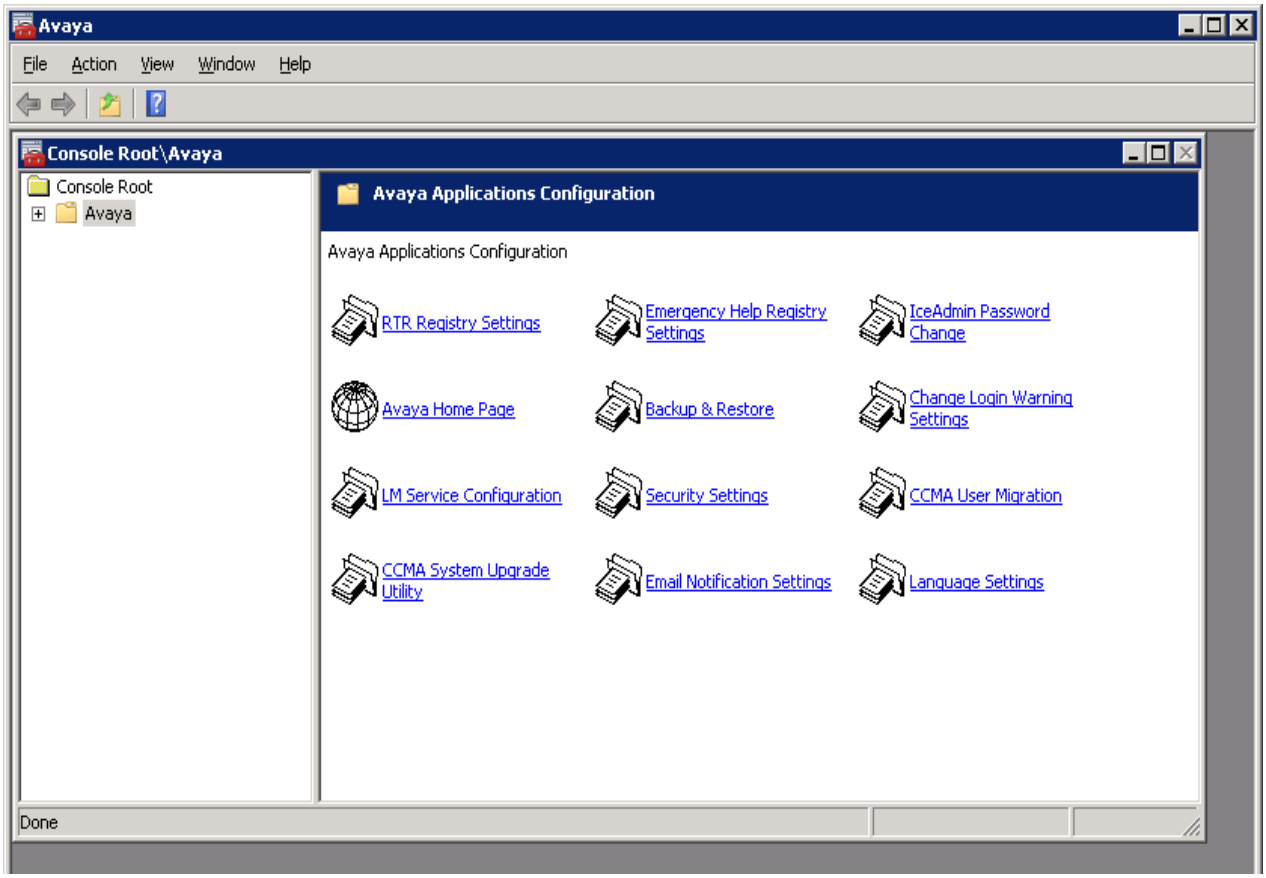
- Know the network location (in Universal Naming Convention (UNC) format) of the drive for the backed up database.

Attention: Ensure that the target server has the same patch level as the source server.

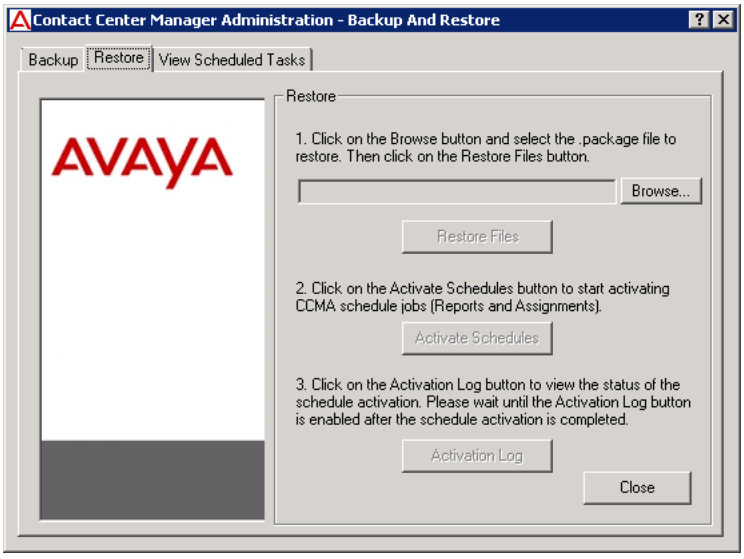
Attention: If you are restoring CCMA data to a Secondary CCMA server - In a High Availability environment, only non-AD-LDS data is restored. This is automatically detected by the Backup & Restore utility and only the required files are updated. This is because core CCMA AD-LDS data is automatically received through AD-LDS replication.

Procedure steps

Step	Action
1	On the standby Voice and Multimedia Contact Server, choose **Start**, **All Programs**, **Avaya, Contact Center**, **Manager Administration**, **Configuration**.



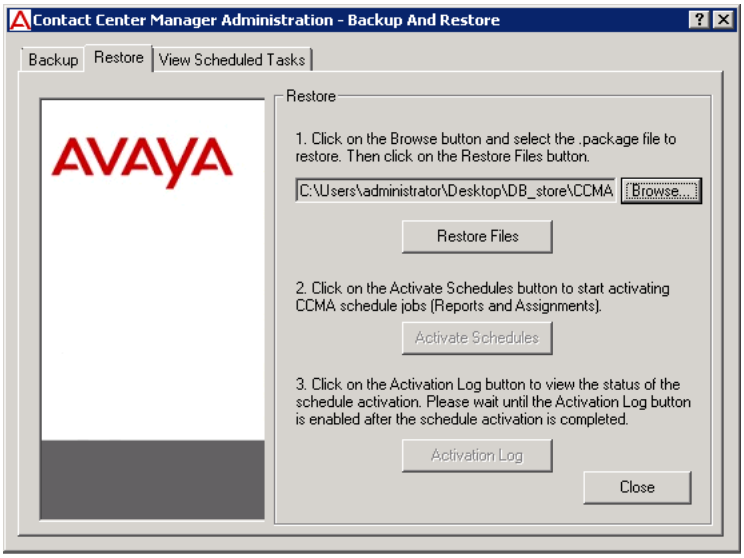
2	In the left pane of the **Avaya Configuration** window, expand **Avaya, Applications, Backup & Restore**.
3	In the right pane, click **Backup & Restore**.
4	In the **Contact Center Manager Administration - Backup And Restore** dialog box, click the **Restore** tab.



5 To select a backup file to restore from, click **Browse** and navigate to the backup folder.

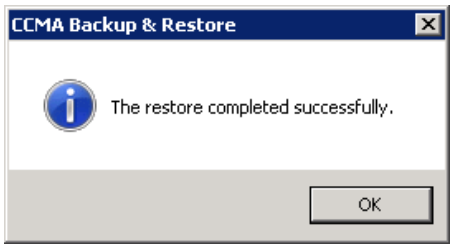
6 In the **Select a backup file** dialog box, select the required .package file.

7 Click **Open**.



8 To restore the backup file data into CCMA, click **Restore Files**.

The restore completed successfully *message box appears.*



9 Click **OK**.

--End--

Configuring server details on the standby server

After you restore the active server database on to the standby server, the standby server database contains the same agent and statistical data as the active server. However, the standby server details are now also configured exactly the same as the active server, therefore you must reconfigure the standby server with its own server details.

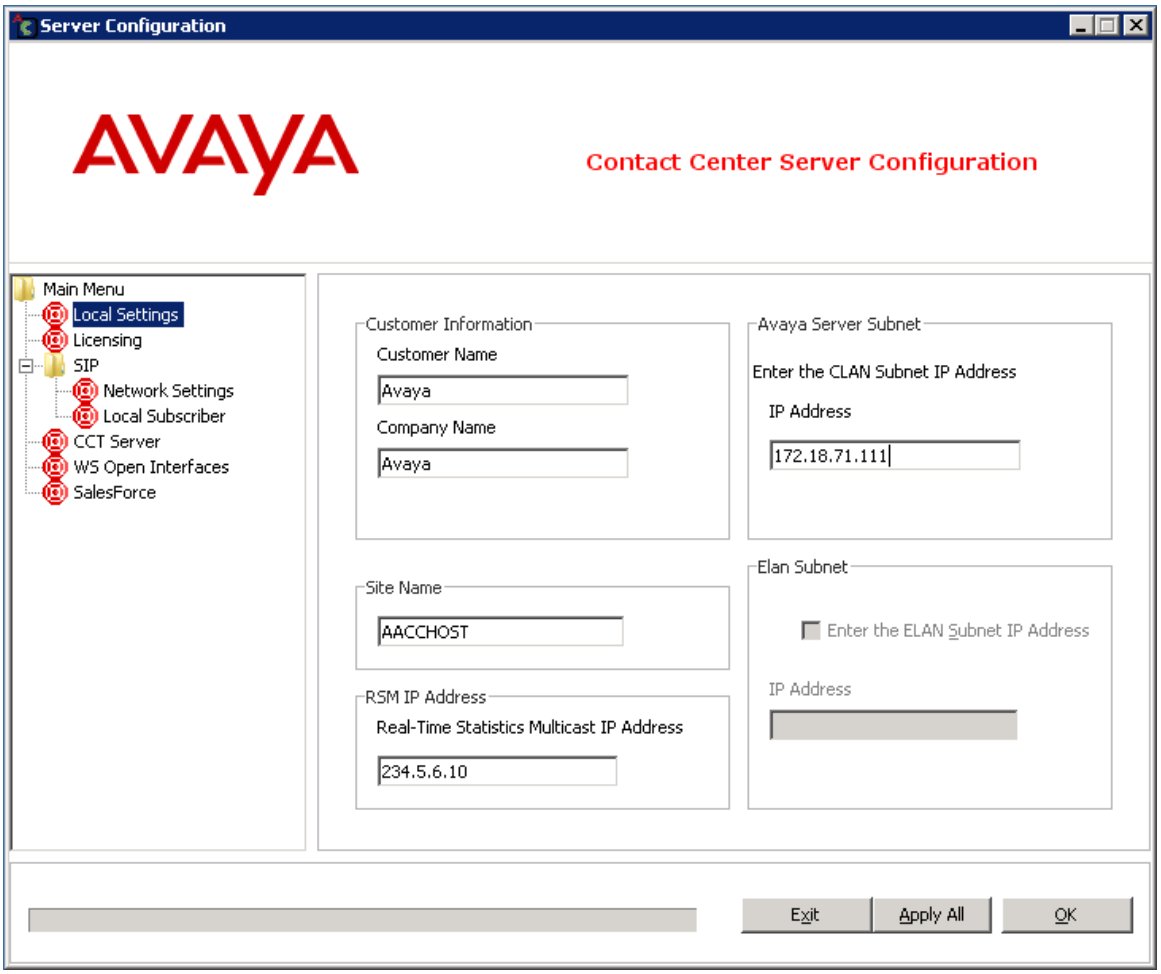
Attention: Changes to the SIP Local Subscriber data may require a Contact Center Manager Server restart. Changes to the SIP Local Subscriber data may require updates to other Avaya Aura® Contact Center components, such as Communication Control Toolkit and Contact Center Multimedia.

Prerequisites

- The active server databases are restored on to the standby server.

Procedure steps

Step	Action
1	Log on to the standby server.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Manager Server**, **Server Configuration**.
3	In the **Server Configuration** dialog box, click the **Local Settings** tab. *Because the active server database was restored on to the standby server, the standby server configuration details show the details for the active server. These server configuration details must be updated.*
4	Update the standby server local settings.
5	In the **Site Name** box, type the site name. For example type AACCHOST. Do not enter the CCMS server name here, use a site name.
6	In the **Avaya Server Subnet IP Address** box, type the IP address of the standby server. For example, type 172.18.71.111.



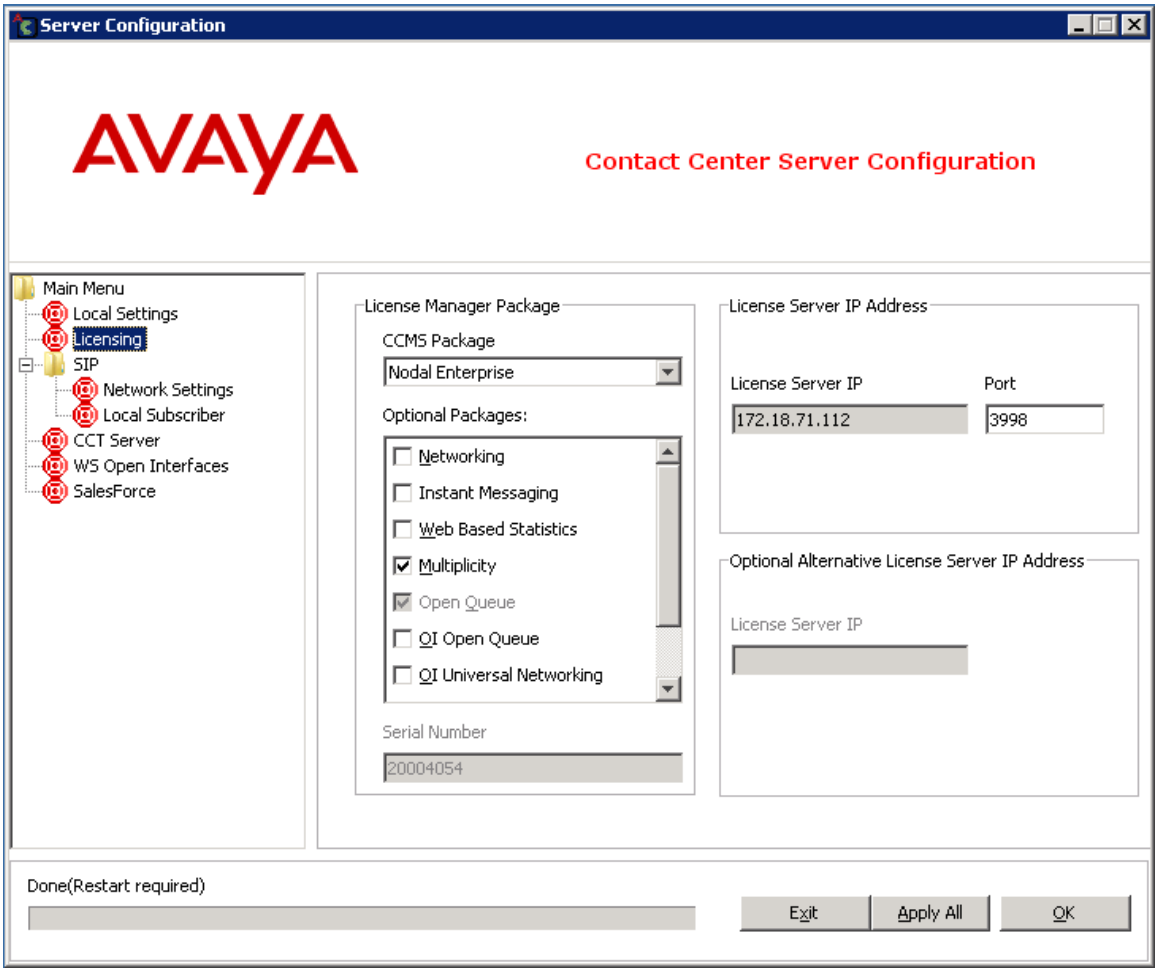
7 Click **Apply All**.

8 Click **OK**.

9 On the **Restart Required** dialog box, click **No**.

10 In the **Server Configuration** dialog box, click the **Licensing** tab.

11 Update the standby server licensing details, if necessary.



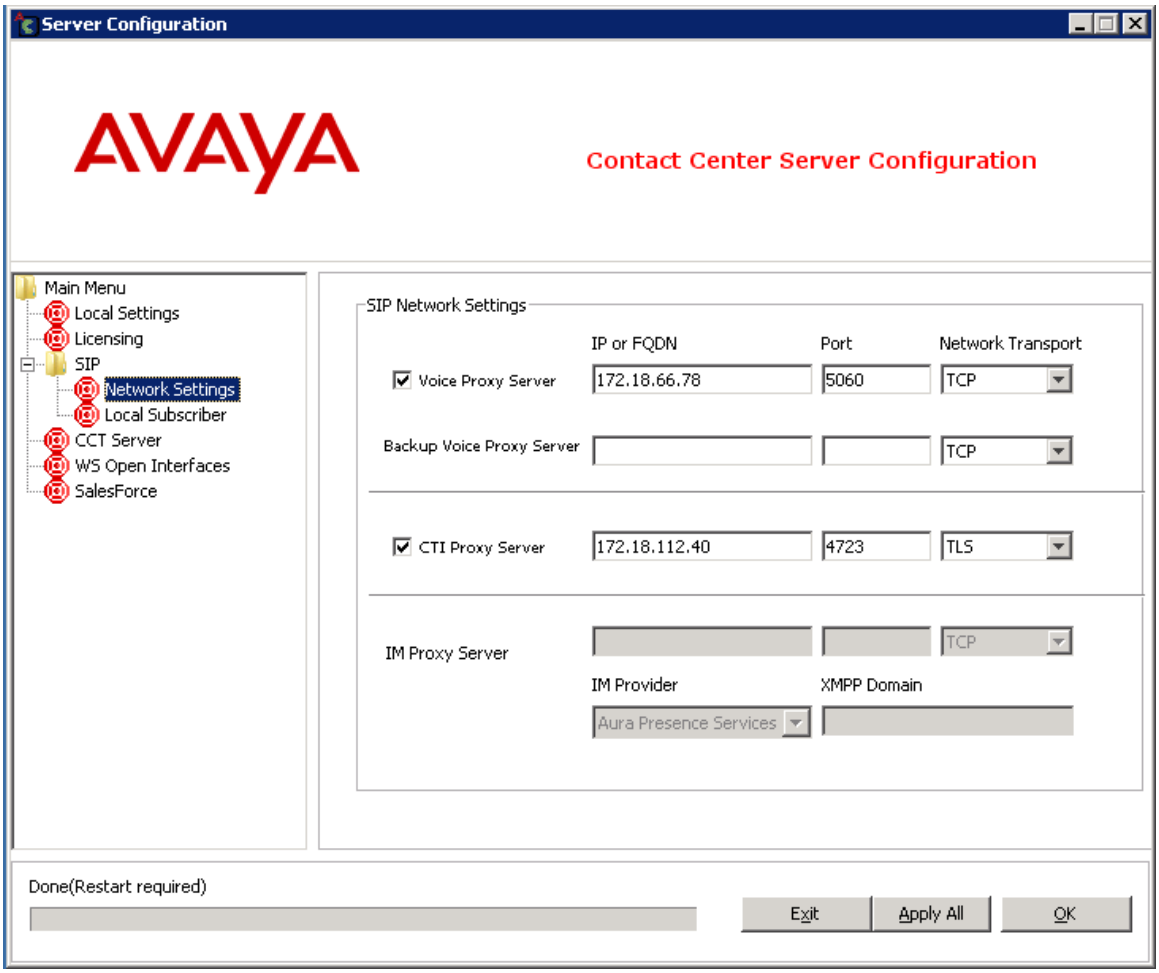
12 Click **Apply All**.

13 Click **OK**.

14 On the **Restart Required** dialog box, click **No**.

15 In the **Server Configuration** dialog box, under **SIP**, click the **Network Settings** tab.

16 Update the standby server **SIP Network Settings** details, if necessary.



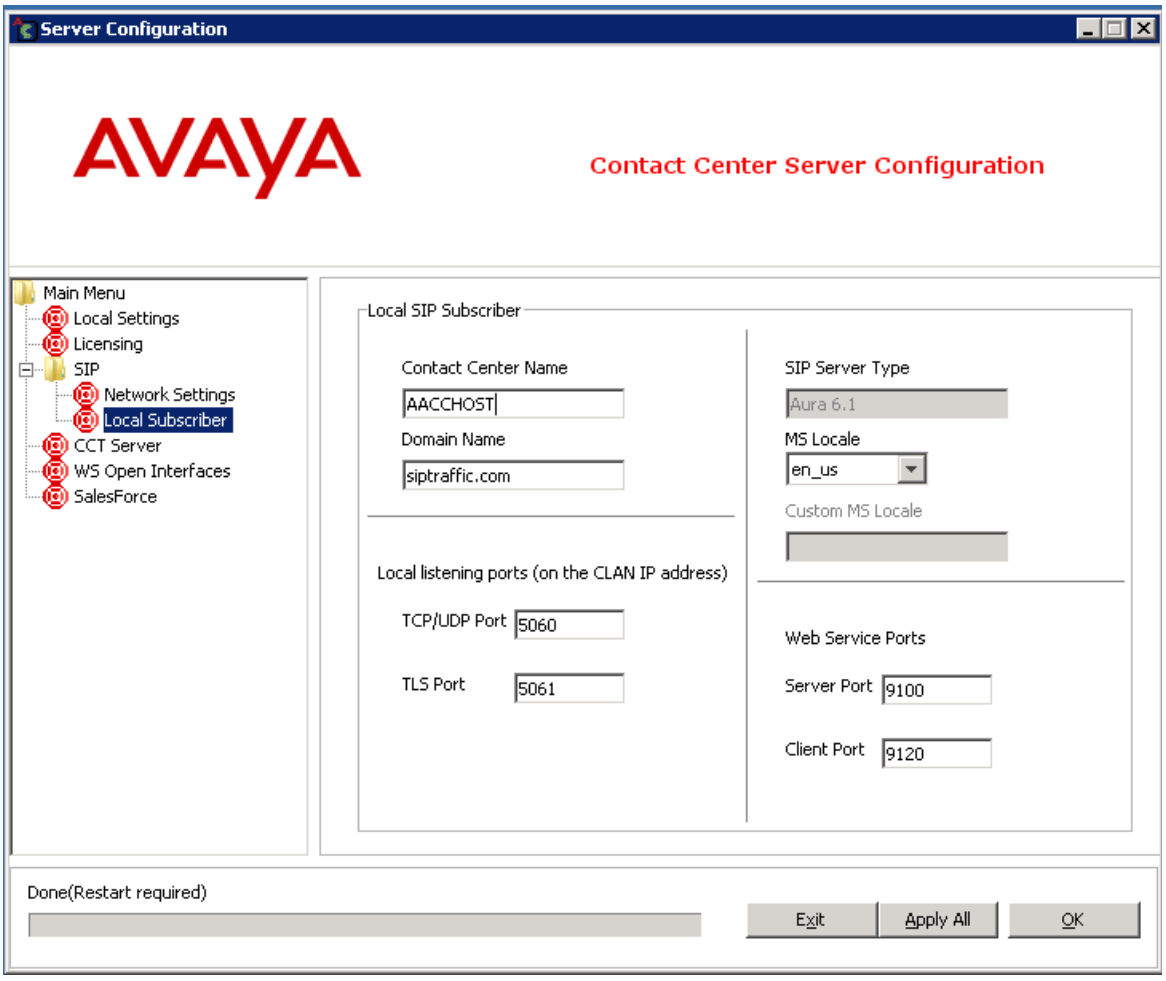
17 Click **Apply All**.

18 Click **OK**.

19 On the **Restart Required** dialog box, click **No**.

20 In the **Server Configuration** dialog box, under **SIP**, click the **Local Subscriber** tab.

21 Update the standby server **SIP Local Subscriber** details. Ensure the **Contact Center Name** box contains the Contact Center site name.



22 Click **Apply All**.

23 Click **OK**.

24 On the **Restart Required** dialog box, click **No**.

25 Click **Exit**.

--End--

Variable definitions

Variable	Value
Avaya Server Subnet IP Address	The IP address of the subnet that connects the Contact Center servers (Contact Center Manager Server, Network Control Center, Contact Center Manager Administration, and Contact Center Multimedia are connected).
Voice Proxy Server	Information about the server that provides support for inbound and outbound calls, such as routing a call to an agent telephone.
• IP or FQDN	If the contact center uses an Avaya Aura® Session Manager, enter the IP address or Fully Qualified Domain Name (FQDN) for the primary Session Manager here.
• Port	The server listening port. The default port is 5060.
• Network Transport	The SIP Network Transport communication protocol.
CTI Proxy Server	Information about the server that provides support for SIP Computer Telephony Integration (CTI) so that Agent Desktop can acquire and control agent telephones for TR87.
• IP or FQDN	If the contact center uses an Avaya Aura® Session Manager server, enter the IP address or Fully Qualified Domain Name (FQDN) for it here.
• Port	For an Application Enablement Services server the default SIP CTI Proxy Server port is 4723.
• Network Transport	The SIP Network Transport communication protocol. For an Avaya Aura® Application Enablement Services server, the default Network Transport communication protocol is TLS.
IM Proxy Server	Information about the server that supports the deployment of Instant Message over SIP. From the IM Provider list, select the name of the instant messaging provider. Select either Avaya Aura® Presence Services or Microsoft OCS.
• IP or FQDN	The IP address or Fully Qualified Domain Name (FQDN) of the SIP IM Proxy Server.
• Port	The default SIP IM Proxy Server port is 5222.
• Network Transport	The IM SIP Proxy Server transport protocol.
IM Provider	Select your IM Provider, Microsoft OCS or Aura Presence Services.
XMPP Domain	If using an Avaya Aura® Presence Services server, enter the domain name of the Extensible Messaging and Presence Protocol (XMPP) server.

Variable	Value
Local SIP Subscriber	Information about the environment of the SIP-enabled contact center and how to identify the server within the network.
• Contact Center Name	The registration user name on the registration proxy. Use a suitable user name following the standards in your system.
• Domain Name	Associated domain name for the SIP-enabled contact center.
• Password	Password for the registration user name.
Web Service Ports	The Web Service Ports group box appears only if you select Avaya Aura® Presence Services as the IM Provider. Server Port default is 9100. Client Port default is 9120.
SIP Server Type	Type of SIP proxy for the contact center integration. Depending on the switch type you select in the Application Selection window, the system automatically sets the specific SIP Server Type as the default. • For SIP Avaya Aura® 6.1 switch type, the default SIP Server Type is Aura 6.1.
MS Locale	Locale (including language and dialects) of the system environment.
Local Listening Ports	The SIP Communication protocol accepted by the system for incoming calls. TCP/UDP Port default is 5060. TLS Port default is 5061.

Configuring High Availability on the standby server

Configure High Availability resiliency on the standby server using the High Availability utility. The standby server shadows the active server and takes over processing if the active server fails.

Prerequisites

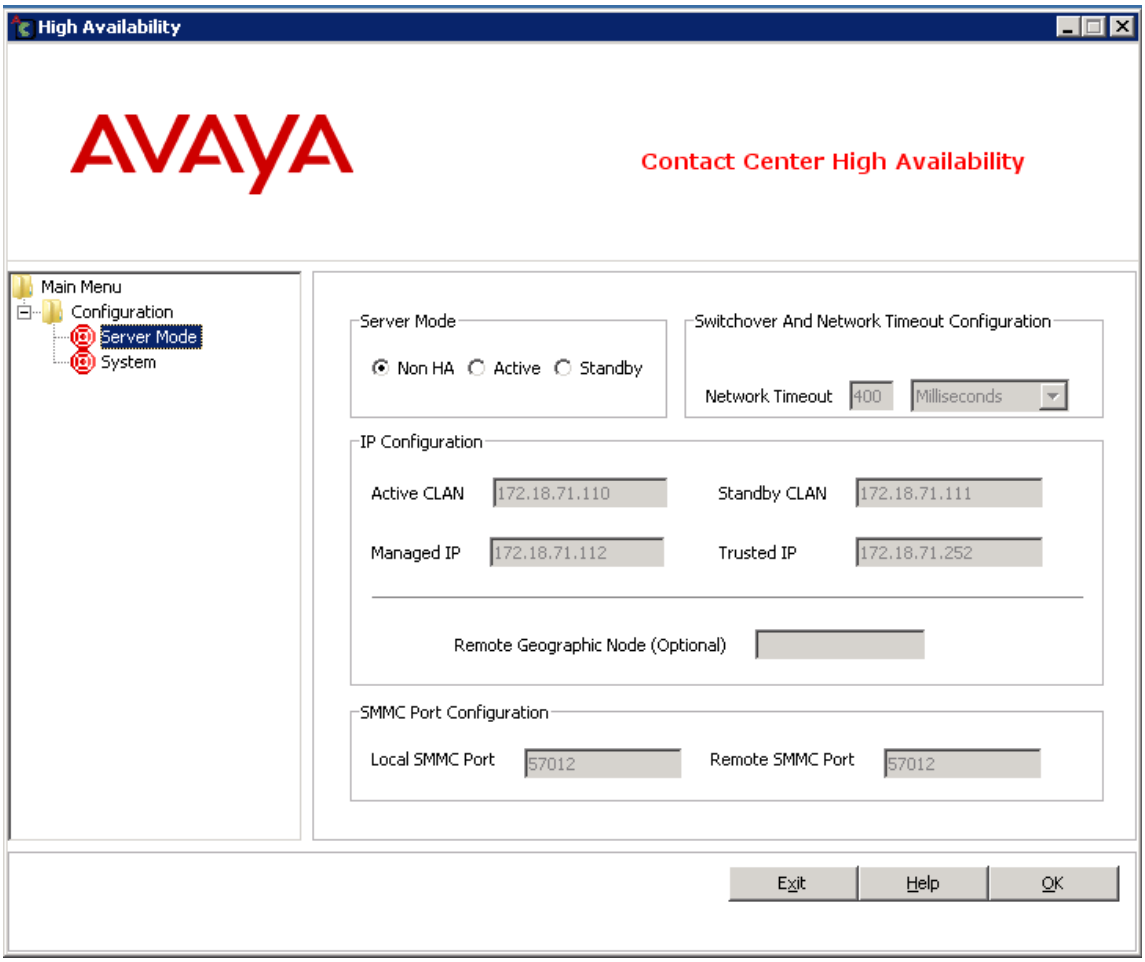
- The active server databases are restored on to the standby server.

Procedure steps

Step	Action
1	Log on to the standby server.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Database Utilities**, **High Availability**.

3 Expand **Configuration**.

4 Double-click **Server Mode**.



5 Under **Server Mode**, select **Standby**.

6 Under **IP Configuration**, in the **Active CLAN** box, type the IP address for the active server. For example, type 172.18.71.110.

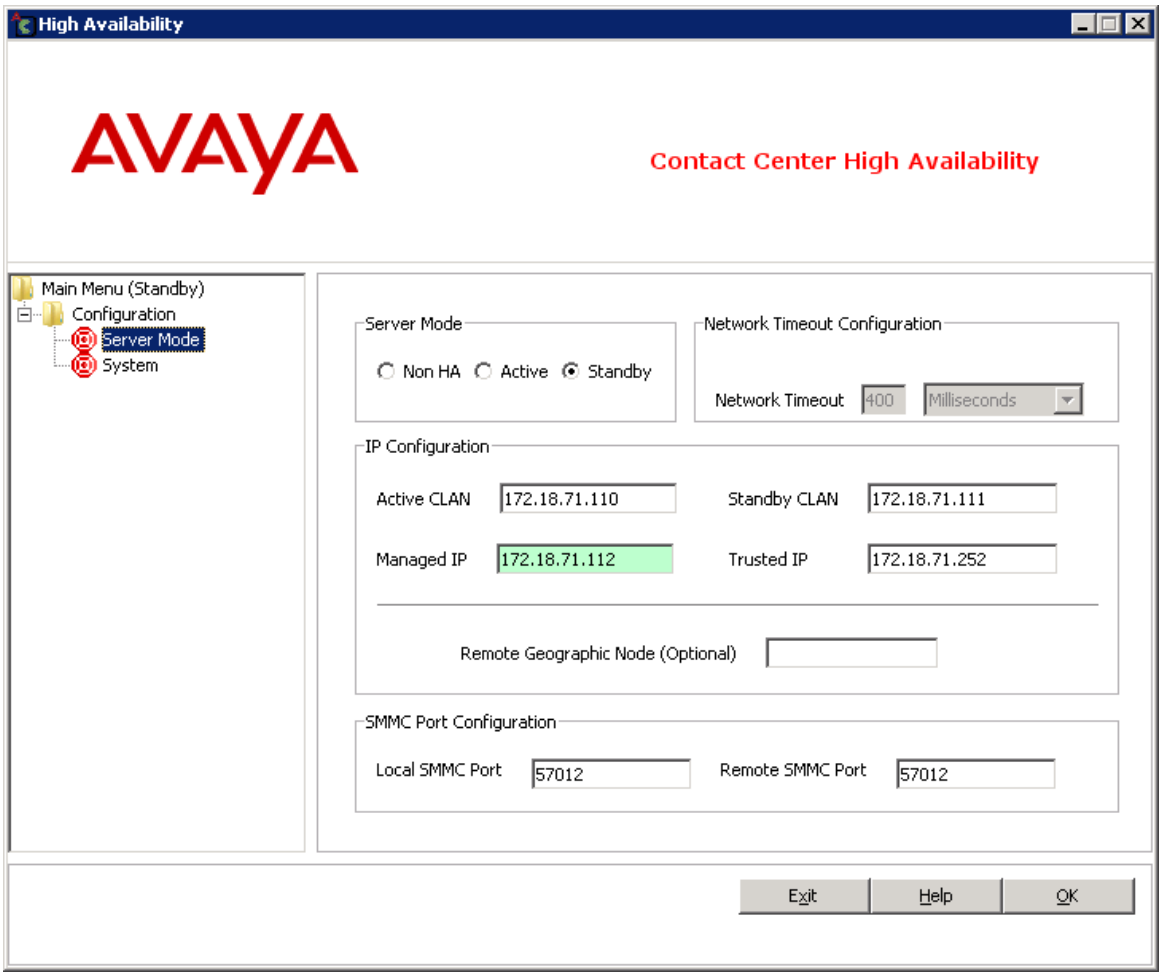
7 Under **IP Configuration,** in the **Standby CLAN** box, type the IP address for the standby server.For example, type 172.18.71.111.

8 Under **IP Configuration**, in the **Managed IP** box, type the managed IP address. For example, type 172.18.71.112.

9 Under **IP Configuration**, in the **Trusted IP** box, type the IP address of a trusted server. For example, type 172.18.71.252.

10 Under **SMMC Port Configuration**, in the **Remote SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the remote (active) server. Accept the default value.

11 Under **SMMC Port Configuration**, in the **Local SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the local (standby) server. Accept the default value.



12 Click **OK**.

--End--

Variable definitions

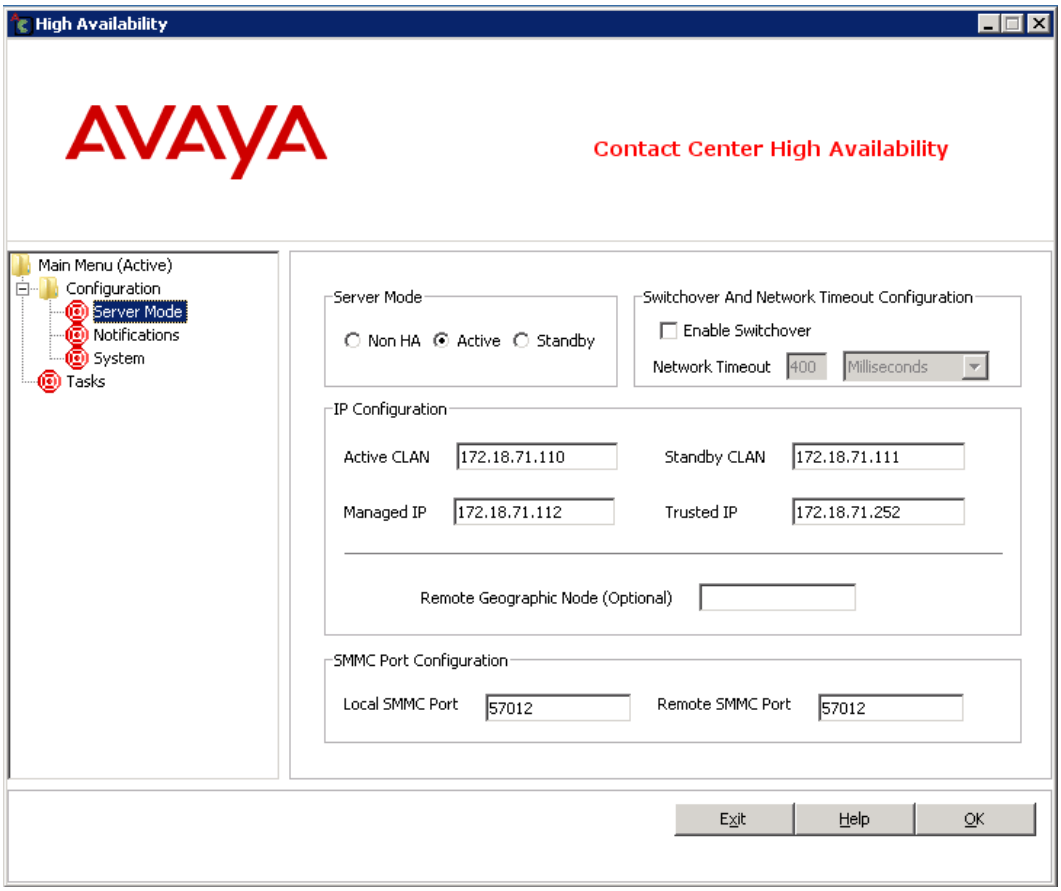
Variable	Value
Active CLAN	The IP address for the server initially configured in active mode.
Standby CLAN	The IP address for the server initially configured in standby mode.
Managed IP	The virtual Managed IP (MIP) address that is used by the active server for campus resiliency. A MIP is used only when the active and standby servers are in the same subnet.
Trusted IP	The active and standby servers use the Trusted IP address to verify network connectivity. If the active server cannot communicate with the standby server it attempts to communicate with the Trusted IP address. If the active server cannot connect to the Trusted IP address on startup then no Contact Center services start on that server. If the active server cannot communicate with the Trusted IP address, if shadowing and switchover are enabled, then the active server stops processing contacts and shuts down. The standby server starts processing contacts if it cannot communicate with the active server but can communicate with the Trusted IP address. Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.

Starting High Availability on the active server

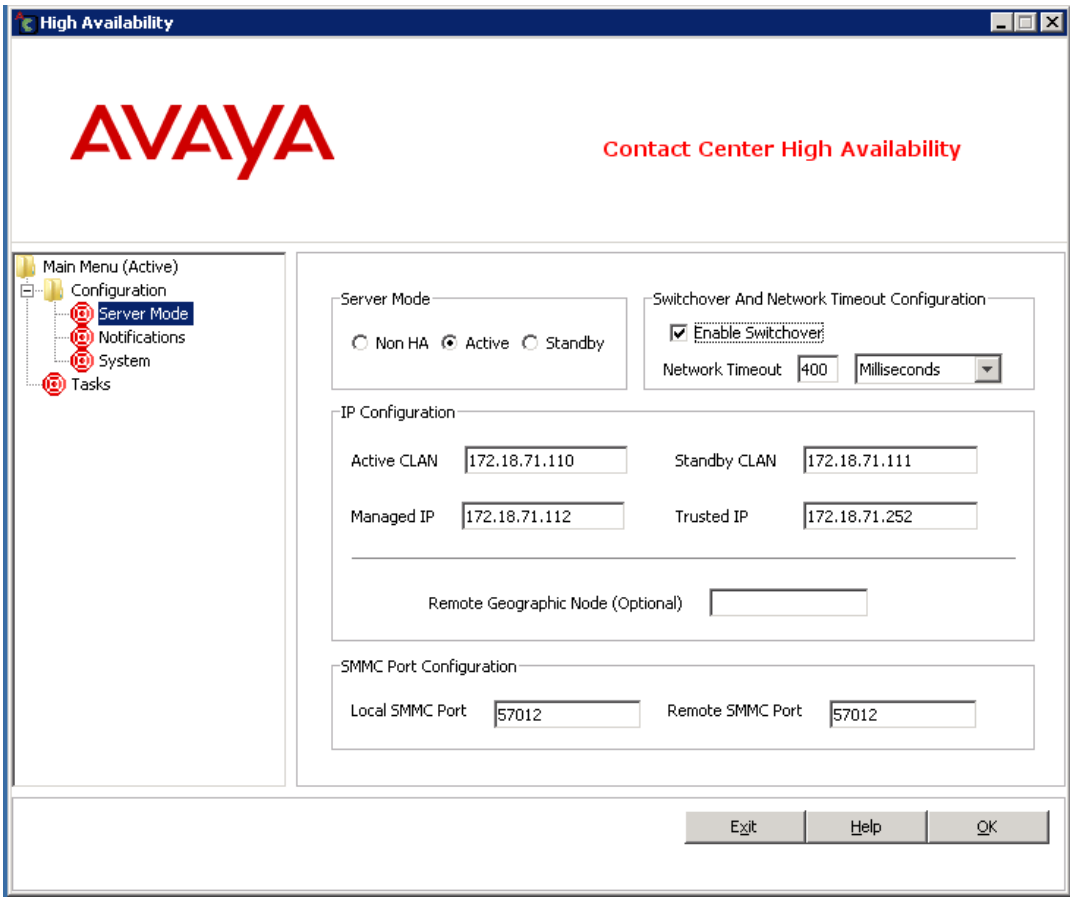
Start the active server using the System Management and Monitoring Component (SMMC) system tray. Starting the active server starts CCMS, CCT, CCMM, and system processes.

Procedure steps

Step	Action
1	Log on to the active server.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Database Utilities**, **High Availability**.
3	Expand **Configuration**.
4	Click **Server Mode**.



5 Under **Switchover And Network Timeout Configuration**, select **Enable Switchover**.

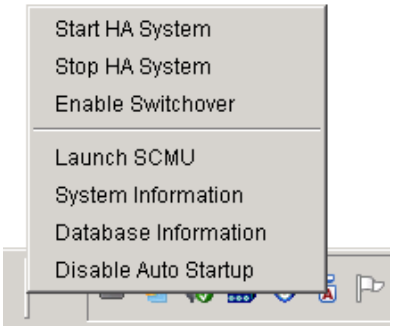


6 Under **Switchover And Network Timeout Configuration**, accept the default **Network Timeout** value (400 milliseconds). This is the maximum length of time the network connectivity tests can continue to fail consecutively before corrective action is considered. For more information about selecting a Network Timeout value appropriate for your contact center solution network, see High Availability Network Timeout optimization (page 37).

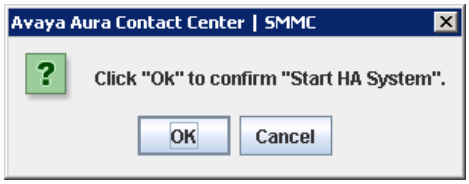
7 Under **Switchover And Network Timeout Configuration**, from the drop down list, select **Milliseconds**.

8 Click **OK**.

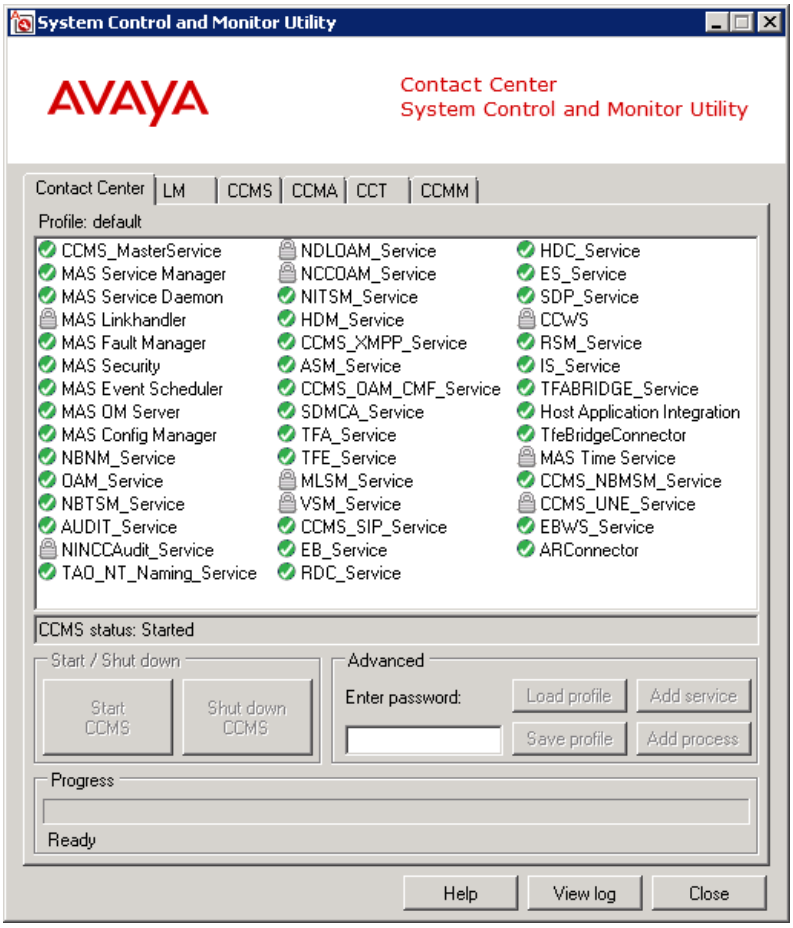
9 On the Windows taskbar of the active server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Start HA System**.



10 On the **SMMC** message box, click **OK**.



11 To verify that the Contact Center services are running using the SCMU, select **Avaya**, **Contact Center**, **Common Utilities**, **System Control and Monitor Utility**. Check that all Contact Center services are running.



--End--

Starting High Availability on the standby server

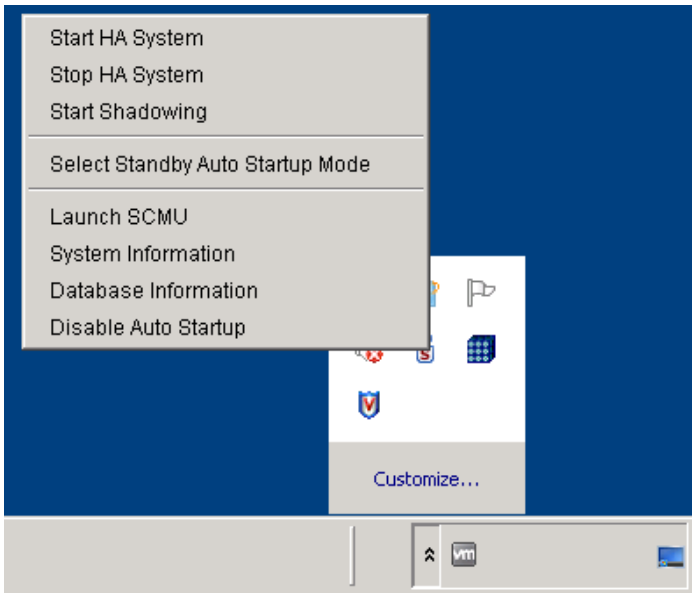
Start High Availability on the standby server using the System Management and Monitoring Component (SMMC) system tray.

The standby server shadows the active server, maintaining a near real-time local copy of the CCMS, CCT, CCMM, and Administration databases. Therefore, the standby server is configured with the most recent data and it can take over from the active server if necessary.

Procedure steps

Step	Action
1	Log on to the standby server.

2 On Windows taskbar of the standby server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Start HA System**.

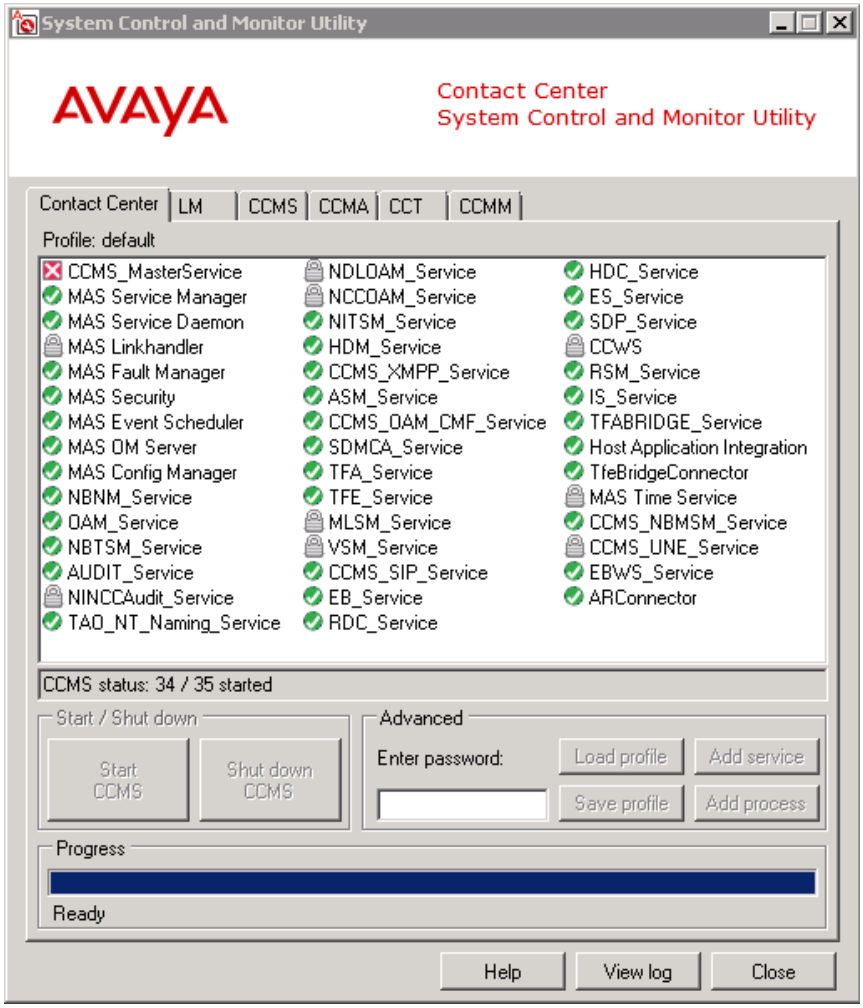


3 Click **OK** to confirm.

4 SMMC performs internal checks on the standby server. These checks may take a few minutes.

5 To verify that the Contact Center services are running using the SCMU, select **Start**, **Avaya**, **Contact Center**, **Common Utilities**, **System Control and Monitor Utility**. Check that Contact Center services are running.

Note: Now that High Availability is configured and functional, the CCMS_MasterService on the standby server is stopped.



--End--

Verifying High Availability is running on the active server

Verify that the active server is running in full High Availability mode.

Procedure steps

Step	Action
1	Log on to the active server.
2	On the Windows taskbar of the active server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **System Information**.

--End--

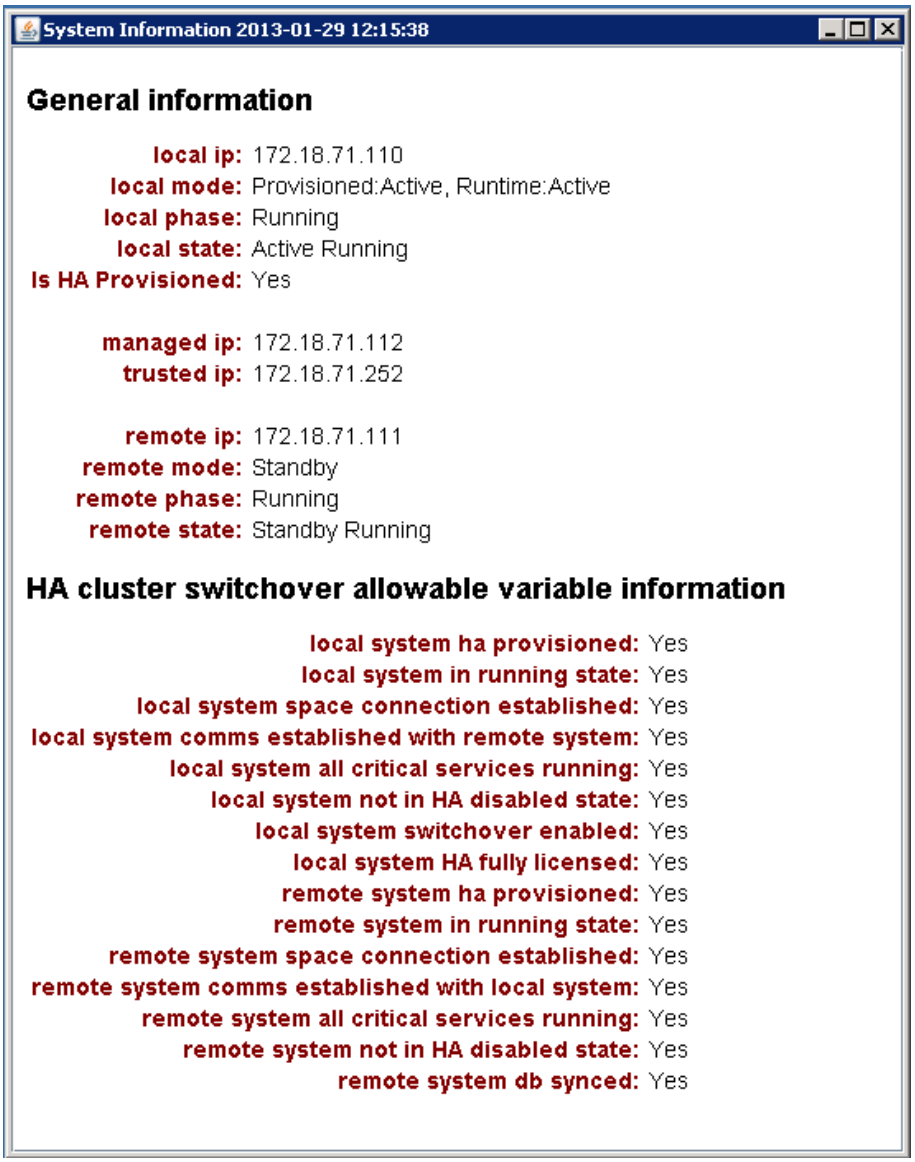
Procedure job aid

Examine the System Information dialog on the active server dialog to ensure it mirrors the System Information dialog on the standby server. The Trusted IP address and Managed IP address must be the same on both servers. Examine the "General Information" section to ensure that your High Availability solution is configured correctly, and to determine why High Availability last stopped. When in Stopped state, System Information displays a "Local last known stop reason".

The System Information dialog box displays the following information categories:

- Computer name and operating system version
- Server mode
- Server configuration type
- Port information
- Remote server connection status
- Remote server port information
- Local and remote information on system status, switchover, shadowing and network

On the active server, examine "local system switchover enabled" to confirm that switchover is supported and enabled.



When the active server is in full High Availability mode and communicating with the standby server, the active server SMMC icons appears as the following:



Note the letter "A" in the SMMC icon indicates that this is the active server. Also note the solid green bar to the right of the icon. This indicates that the active server is communicating with the standby server and that the databases are shadowing.

Verifying High Availability is running on the standby server

Verify that the standby server is running in full High Availability mode and is shadowing the active server.

Procedure steps

Step	Action
1	Log on to the standby server.
2	On the Windows taskbar of the standby server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **System Information**.

--End--

Procedure job aid

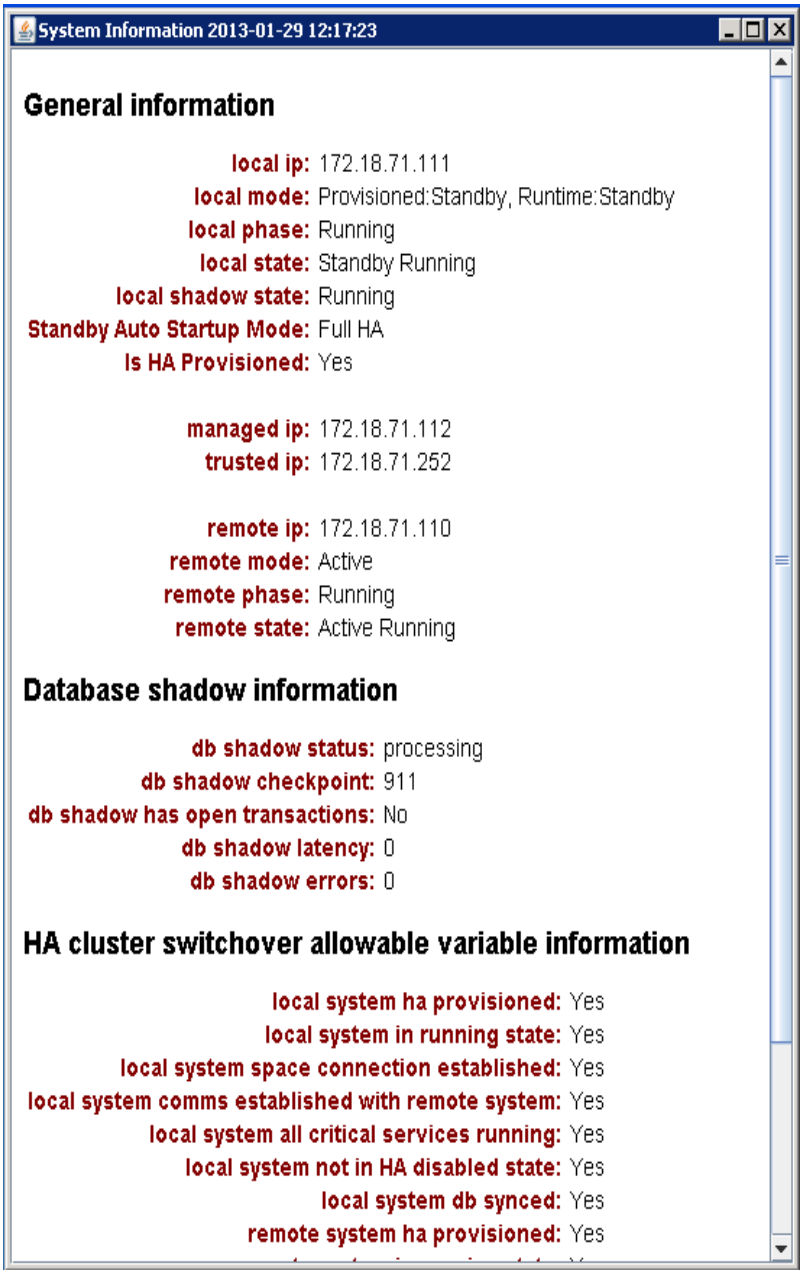
Examine the System Information dialog on the standby server dialog to ensure it mirrors the System Information dialog on the active server. The Trusted IP address and Managed IP address must be the same on both servers. Examine the "General Information" section to ensure that your High Availability solution is configured correctly, and to determine why High Availability last stopped. When in Stopped state, System Information displays a "Local last known stop reason".

The System Information dialog box displays the following information categories:

- Computer name and operating system version
- Server mode
- Server configuration type
- Port information
- Remote server connection status

- Remote server port information
- Local and remote information on system status, switchover, shadowing and network

On the standby server, examine "local system db synced" to confirm that database shadowing is working.



When the standby server is in full High Availability mode and shadowing the active server, the standby server SMMC icons appears as the following:



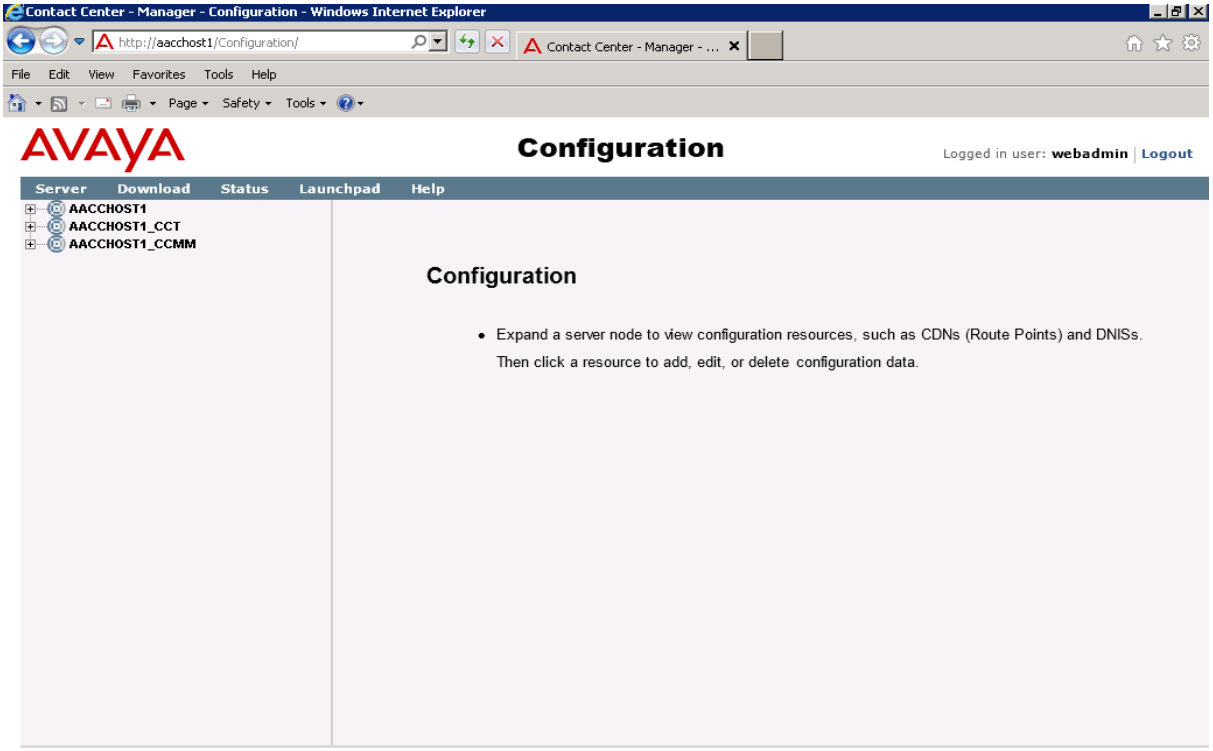
Note the letter "S" in the SMMC icon indicates that this is the standby server. Also note the solid green bar to the right of the icon. This indicates that the standby server is communicating with the active server and that the databases are shadowing.

Changing server details in Contact Center Manager Administration

In Contact Center Manager Administration, change the Contact Center Manager Server and Communication Control Toolkit server details to use the High Availability Managed IP address and Managed name details.

Procedure steps

Step	Action
1	Log on to the active server.
2	Log on to the Contact Center Manager Administration with administrative privileges.
3	On the **Launchpad**, click **Configuration**.

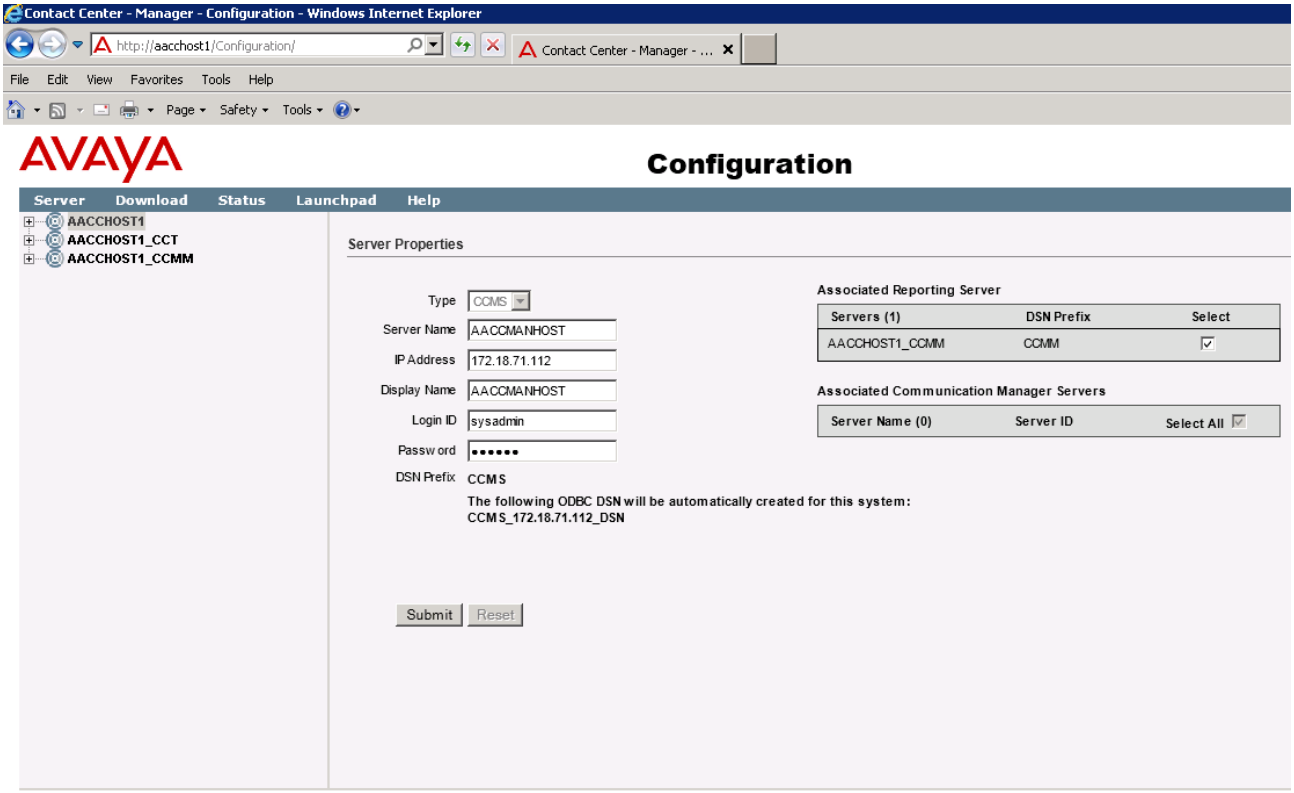


4 From the list of servers in the system tree, right-click on the active CCMS server, and select **Edit Properties**. For example, select AACCHOST1.

5 In the **Server Name** box, type the High Availability Managed name of the Voice and Multimedia Contact Server. For example, type AACCMANHOST.

6 In the **IP Address** box, type the High Availability Managed IP address of the Voice and Multimedia Contact Server. For example type, 172.18.71.112.

7 In the **Display Name** box, type the name of the Contact Center Manager Server as you want it to appear in the system tree of Contact Center Administration.
For example, type AACCMANHOST.



8 In the **Login ID** box, type the Login ID for Contact Center Manager Server. The Login ID corresponds to a user account created using the Contact Center Manager Server Utility. The default Login ID is **sysadmin**. For example, type sysadmin.

9 In the **Password** box, type the password for the Contact Center Manager Server. The default password is **avaya1**. For example, type avaya1.

10 Click **Submit**.

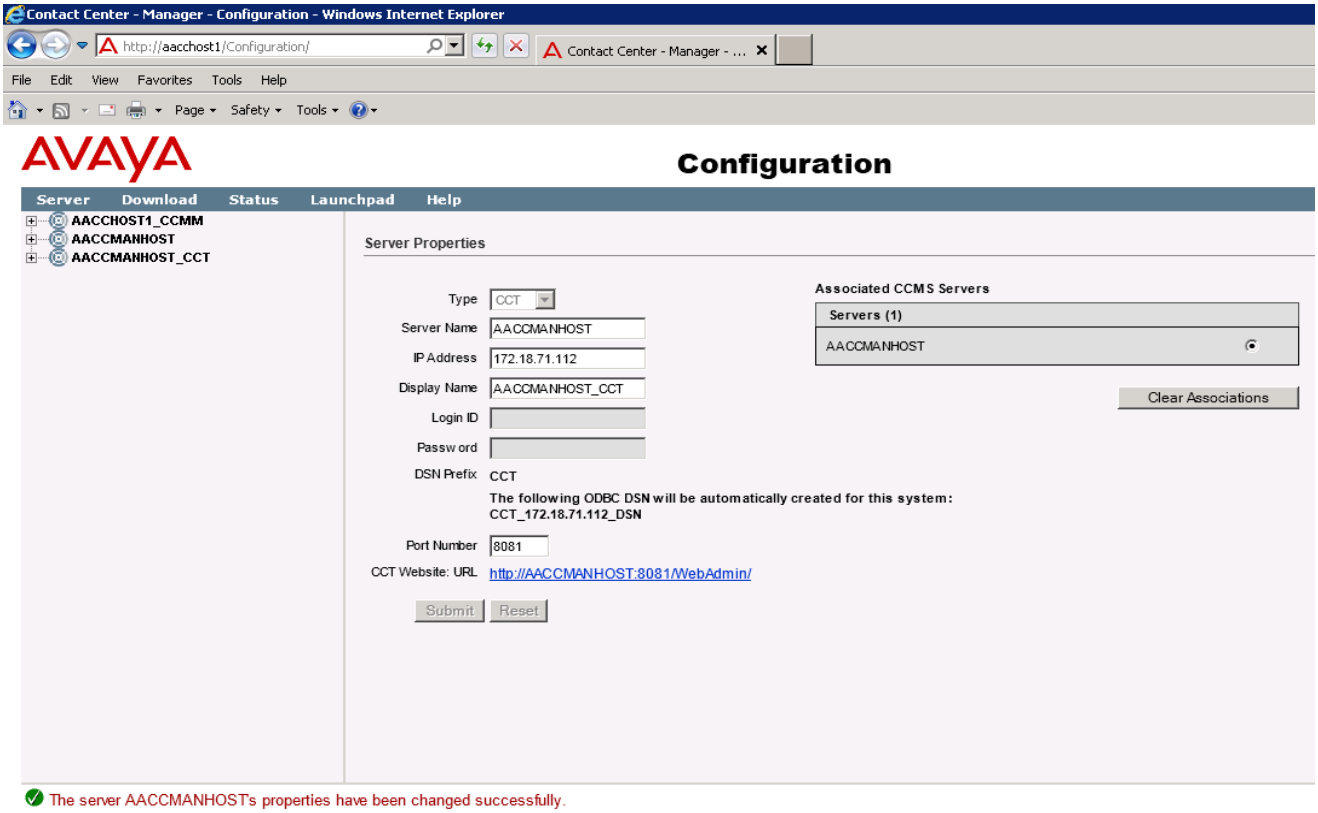
11 From the list of servers in the system tree, right-click on the active CCT server, and select **Edit Properties**. For example, select AACCHOST1_CCT.

12 In the **Server Name** box, type the High Availability Managed name of the Voice and Multimedia Contact Server. For example type AACCMANHOST.

13 In the **IP Address** box, type the High Availability Managed IP address of the Voice and Multimedia Contact Server. For example type 172.18.71.112.

14 In the **Display Name** box, type the name of Communication Control Toolkit as you want it to appear in the system tree of Contact Center Administration. For example type AACCMANHOST_CCT.

15 Click **Submit**.



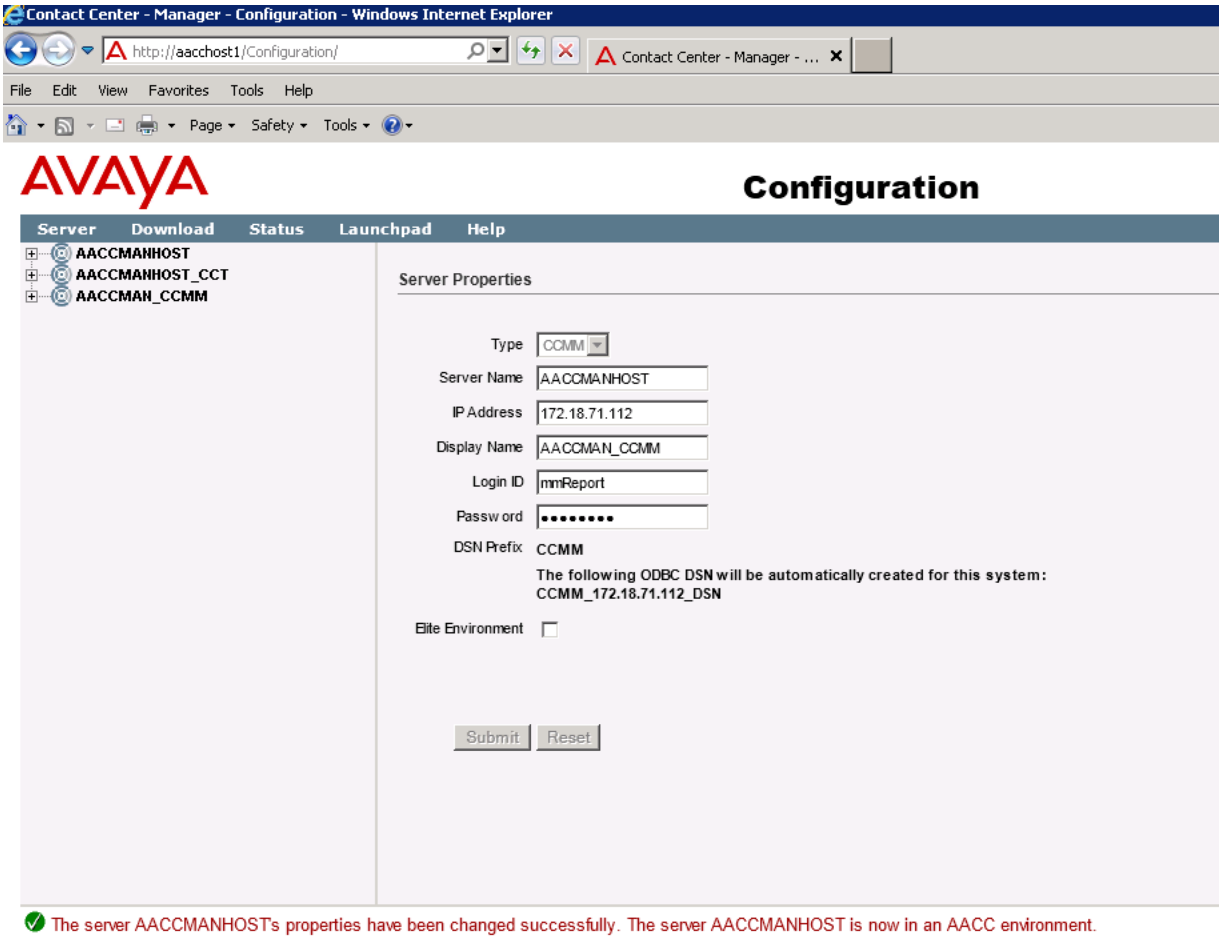
16 From the list of servers in the system tree, right-click on the CCMM server, and select **Edit Properties**.

17 In the **Server Name** box, type the High Availability Managed name of the Voice and Multimedia Contact Server.

18 In the **IP Address** box, type the High Availability Managed IP address of the Voice and Multimedia Contact Server.

19 In the **Display Name** box, type the name of Contact Center Multimedia as you want it to appear in the system tree of Contact Center Administration. For example, type AACCMAN_CCMM.

20 Click **Submit**.



--End--

Using the Contact Center Manager Administration server Managed name

Use the High Availability Managed name of Contact Center Manager Administration to access the CCMA application. When the Avaya Aura® Contact Center High Availability feature is configured and enabled, re-direct all Contact Center Manager Administration client Web browsers to use the Managed server name of the CCMA server.

If you have a High Availability campus solution Avaya recommends that you log onto the CCMA Web client using the Managed name of the Voice and Multimedia Contact Server. If an active application or server fails, the CCMA client Web browser continues to use the Managed name and you can continue working without interruption.

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

Prerequisites

- Configure High Availability on the active and standby servers.
- Change the server details in CCMA. For more information about changing the server details in CCMA, see Changing server details in Contact Center Manager Administration (page 602).
- Know the user ID and password to log on to the CCMA.

Procedure steps

Step	Action
1	Start Internet Explorer.
2	In the **Address** box, type the URL of the CCMA server. The default URL is http://<server name>; where <server name> is the Managed server name of the Voice and Multimedia Contact Server. For example, type **http://AACCMANHOST**
3	If you are prompted to add the managed name to the list of trusted hosts, accept the managed name.
4	In the **User ID** box, type your user ID.
5	In the **Password** box, type your password.
6	Click **Login**.

--End--

Procedure job aid



Configuring email attachment file locations

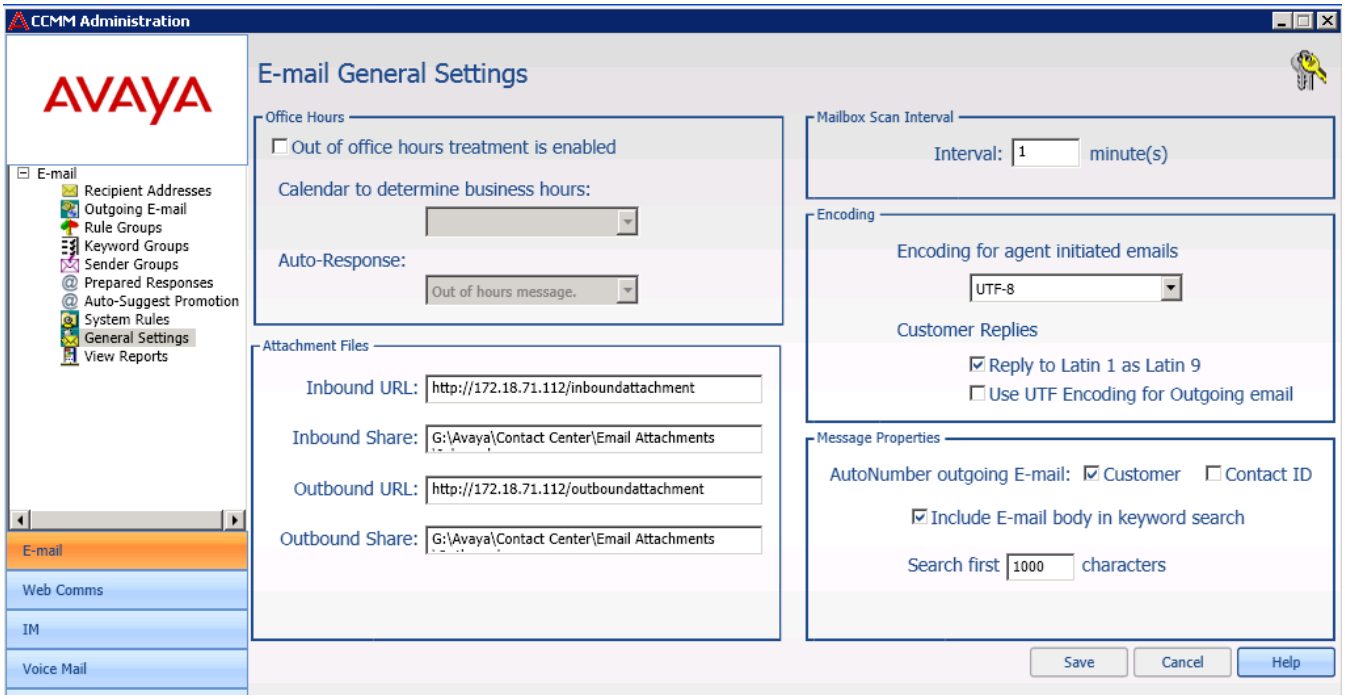
Update the locations for inbound and outbound email attachments. Update the locations to use the Managed IP address of the Voice and Multimedia Contact Server HA pair.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration, using the HA pair managed name, with administrator privileges.
2	On the CCMA **Launchpad**, click **Multimedia**.
3	In the left column, select the Multimedia server on which you want to configure server settings. For example select AACCMAN_CCMM.
4	In the right pane, click **Launch Multimedia Client**. *The CCMM Administration Tool opens.*
5	In the left column, select **E-mail**, **General Settings**.
6	Under **Attachment Files**, in the **Inbound URL** box, type the URL for files attached to inbound email messages. For example, type http://172.18.71.112/InboundAttachment.

7 Under **Attachment Files**, in the **Outbound URL** box, type the URL for files attached to outbound email messages. For example, type http://172.18.71.112/OutboundAttachment

8 Click **Save**.



--End--

Variable definitions

Variable	Value
Inbound URL	The URL for files attached to inbound email messages. For contact centers using the Avaya Aura® Contact Center High Availability feature, Avaya recommends using: http://managedIPAddress/InboundAttachment Where managedIPAddress is the managed IP address of the Voice and Multimedia Contact Server, for example 172.18.71.112.
Outbound URL	The URL for files attached to outbound email messages. For contact centers using the Avaya Aura® Contact Center High Availability feature, Avaya recommends using: http://<managedIPAddress>/OutboundAttachment Where managedIPAddress is the managed IP address of the Voice and Multimedia Contact Server, for example 172.18.71.112.

Verifying the Managed IP address on the active sever

Verify that the active server is running in full High Availability mode and that it is hosting the Managed IP address and Managed name.

Procedure steps

Step	Action
1	Log on to the active server.
2	Click **Start**, **Run**, and in the **Open** box, type **cmd**.
3	Enter **ipconfig**.
4	Verify that the Managed IP address is attached to the Network Interface on the active Voice and Multimedia Contact Server. Verify that the Managed IP address, for example 172.18.71.112 is attached to the Network Interface on the active server (172.18.71.110).

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 172.18.71.110
   Subnet Mask . . . . . . . . . . . : 255.255.248.0
   IPv4 Address. . . . . . . . . . . : 172.18.71.112
   Subnet Mask . . . . . . . . . . . : 255.255.248.0
   Default Gateway . . . . . . . . . : 172.18.71.254

C:\Users\administrator>_
```

--End--

Verifying server communication on the standby server

Verify that the standby server can resolve the Managed IP address and Managed name of the active server.

Procedure steps

Step	Action
1	Log on to the standby Voice and Multimedia Contact Server.
2	Click **Start**, **Run**, and in the **Open** box, type **cmd**.
3	Enter **ipconfig**.
4	Verify that the standby server can resolve the managed name of the active server to the Managed IP address of the active server. For example, if the standby Voice and Multimedia Contact Server pings the Managed name "AACCMANHOST", this resolves to the Managed IP address "172.18.71.112" of the Voice and Multimedia Contact Server HA pair.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\administrator>ping AACCMANHOST

Pinging AACCMANHOST.SipTraffic.com [172.18.71.112] with 32 bytes of data:
Reply from 172.18.71.112: bytes=32 time<1ms TTL=128
Reply from 172.18.71.112: bytes=32 time=2ms TTL=128
Reply from 172.18.71.112: bytes=32 time<1ms TTL=128
Reply from 172.18.71.112: bytes=32 time<1ms TTL=128

Ping statistics for 172.18.71.112:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Users\administrator>_
```

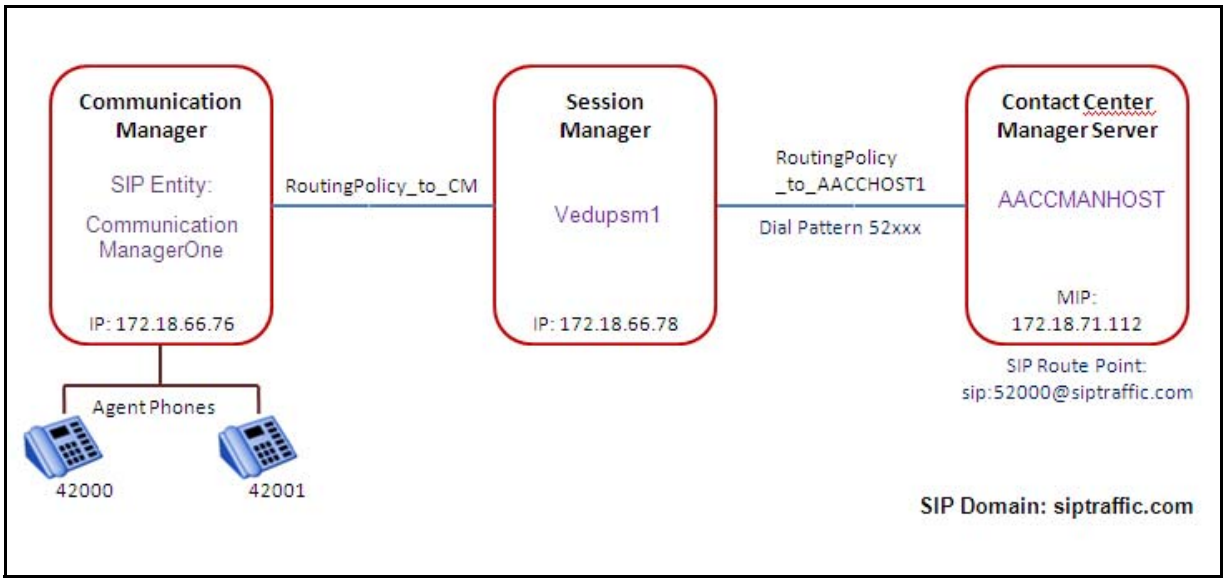
--End--

High Availability – Session Manager configuration

This section describes how to configure Avaya Aura® Session Manager Release 6.2 for use with High Availability Avaya Aura® Contact Center Release 6.3.

The following diagram shows a typical simplex Session Manager deployment and configuration to support Avaya Aura® Contact Center – High Availability.The procedures and SIP Entity names in this section are based on this typical routing configuration.

Example of a SM routing solution using Contact Center HA pair Managed IP address



Prerequisites

- Ensure that your Avaya Aura Unified Communications platform meets the minimum template requirements for integration with Avaya Aura® Contact Center.
- Ensure that your Avaya Aura® Session Manager is Release 6.2 or later.

Updating the Contact Center Manager Server SIP Entity

Update the SIP Entity for the Contact Center Manager Server to use the Managed IP address of the HA pair.

Procedure steps

Step	Action
1	On the System Manager console, select **Routing**, **SIP Entities**.
2	Select the existing Contact Center SIP Entity link and click **Edit**.
3	In the **Name** box, type the name of the Contact Center Manager Server SIP Entity, for example AACCHOST1.
4	In the **FQDN or IP address** box, type the Managed IP address of the Contact Center Manager Server HA pair, for example 172.18.71.112.
5	In the **Notes** box, update the description.
6	Click **Commit**.

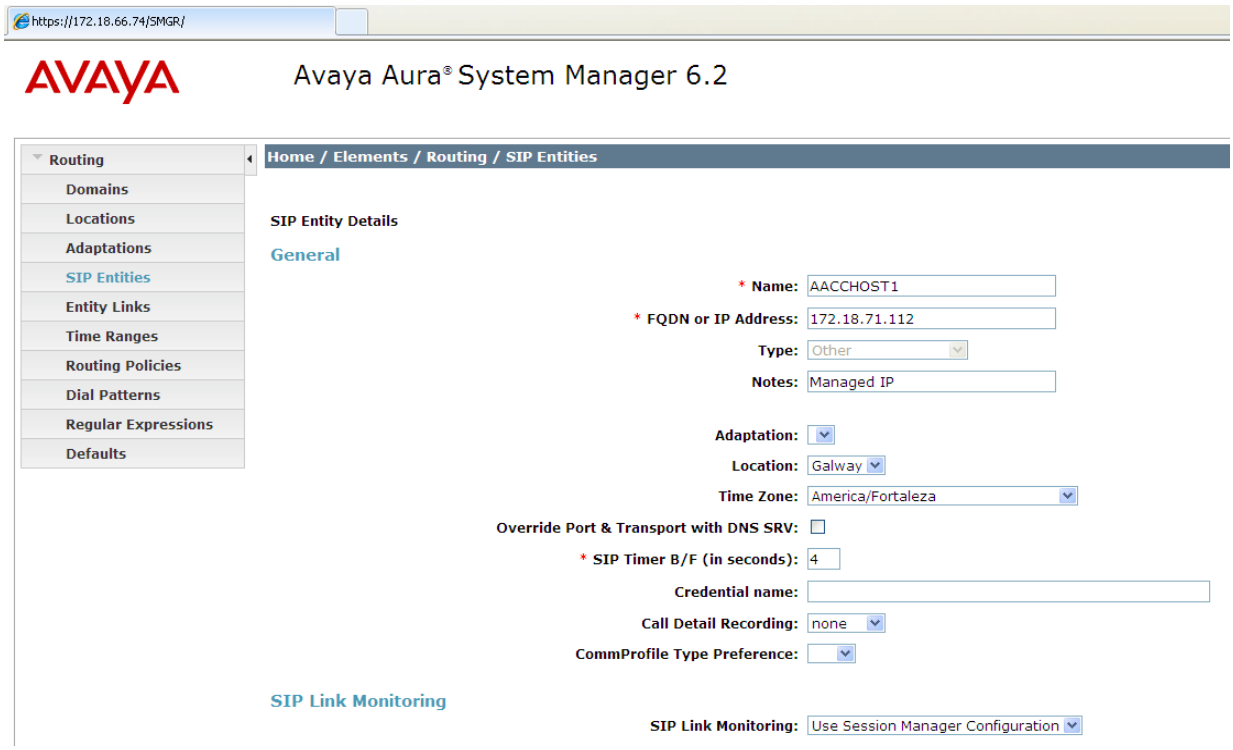
--End--

Variable definitions

Variable	Value
Name	SIP entity name. This name must be unique and can have between 3 and 64 characters.
FQDN or IP Address	Fully qualified domain name or IP address of the Avaya Aura® Contact Center SIP entity. If your Avaya Aura® Contact Center supports High Availability (HA) then the IP address for the Avaya Aura® Contact Center SIP Entity is the Avaya Aura® Contact Center HA cluster IP address. If your Avaya Aura® Contact Center does not support High Availability (HA) then the IP address for the Avaya Aura® Contact Center SIP Entity is the Contact Center Manager Server IP Address.
Type	SIP entity type, such as a Other.

Procedure job aid

The SIP Entity for the Contact Center Manager Server.


https://172.18.66.74/SMGR/
AVAYA
Avaya Aura® System Manager 6.2
Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults
Home / Elements / Routing / SIP Entities
SIP Entity Details
General
* Name: AACCHOST1
* FQDN or IP Address: 172.18.71.112
Type: Other
Notes: Managed IP
Adaptation:
Location: Galway
Time Zone: America/Fortaleza
Override Port & Transport with DNS SRV:
* SIP Timer B/F (in seconds): 4
Credential name:
Call Detail Recording: none
CommProfile Type Preference:
SIP Link Monitoring
SIP Link Monitoring: Use Session Manager Configuration

High Availability – Testing

This section describes how to test the Avaya Aura® Contact Center – High Availability feature in your solution.

Avaya Aura® Agent Desktop supports High Availability for fault tolerant and resilient contact center solutions. In High Availability (HA) contact centers, Avaya Aura® Agent Desktop connects to multiple Avaya Aura® Contact Center servers. If one of the Contact Center servers fails or is shut down for maintenance, your Agent Desktop software switches over to the remaining Contact Center servers and continues working.

Normally, agents do not notice a server switchover, agents remain logged on and continue handling customer phone calls without interruption. The Agent Desktop multimedia contacts list refreshes during a server switchover and this causes a short delay before new multimedia contacts arrive. In limited circumstances, Agent Desktop experiences a short delay during server switchover and if this occurs agents must log on again after the switchover. Phone calls in progress with a customer are not affected by a switchover.

The Agent Desktop – High Availability test procedure outline is as follows:

1 Uninstall the existing Agent Desktop client software.

2 Install the Agent Desktop software from the HA pair Managed IP address.

3 Launch the Agent Desktop software.

4 Log on one test agent, and change into the ready state.

5 Generate a test phone call.

6 On the Agent Desktop, answer the test phone call.

7 Send a test email.

8 On the Agent Desktop, accept the test email.

9 Trigger a switchover from the active server to the standby server.

10 Monitor the agent state, test call and test email during and after the switchover.

11 Verify the original active server has shut down correctly.

12 Verify the original standby server is now running in active mode.

13 Verify that the test email is still open and editable after the switchover.

14 Close the test email.

15 Verify the original standby server is now running in active mode.

16 Verify that the Agent Desktop retains call control by placing the test call on hold.

17 Outline of how to reinstate High Availability solution resiliency.

If you experience unnecessary or unexplained switchovers, consider increasing the High Availability Network Timeout value to match your network performance. For more information about tuning the High Availability feature to your solution, see High Availability Network Timeout optimization (page 37).

Uninstalling Agent Desktop client software

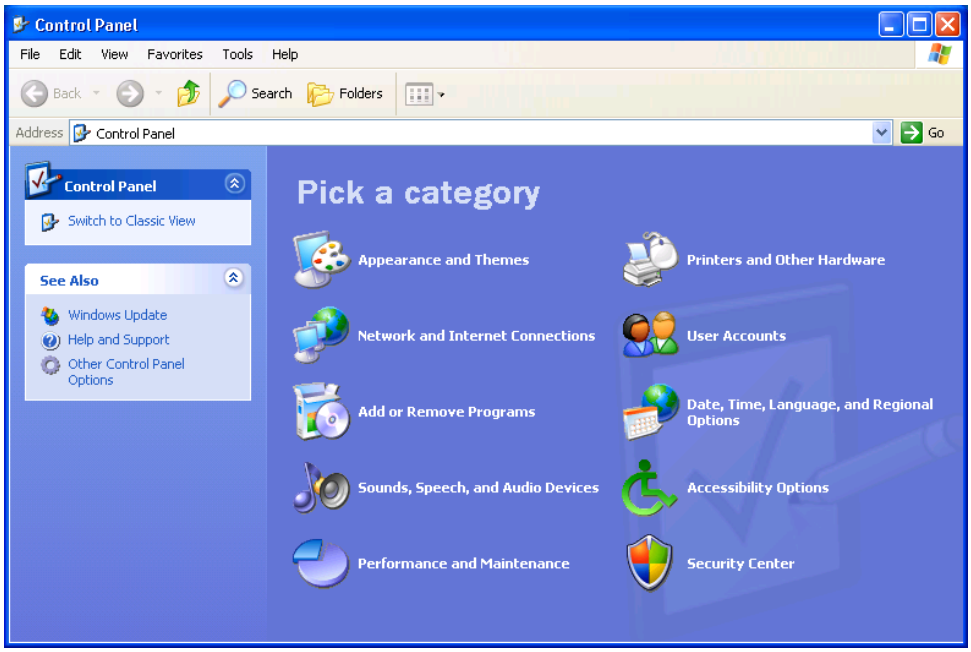
Uninstall the existing Agent Desktop client software from the client computers. In HA solutions, you must uninstall the Agent Desktop client software downloaded directly from the original Voice and Multimedia Contact Server. You must download the Agent Desktop client software from the Managed IP or Managed name of the HA pair. This ensures Agent Desktop – High Availability support and future software updates.

Prerequisites

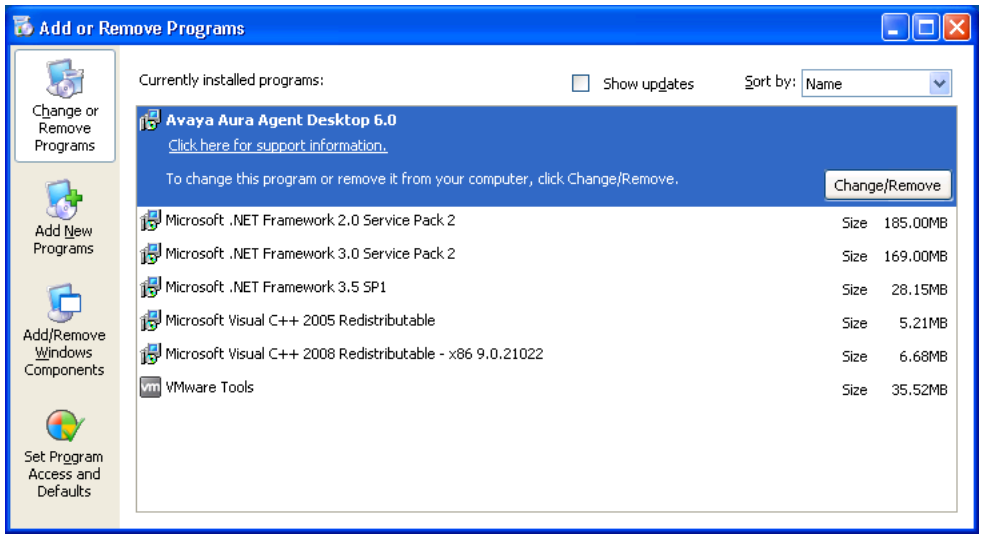
- Ensure that the Agent that uses the Agent Desktop computer is logged off.

Procedure steps

Step	Action
1	Log on to the Agent Desktop computer. For example, log on to XPClientDoc1 using the AACC_Agent1 agent account.
2	Click **Start**, **Control Panel**, **Add or Remove Programs**.

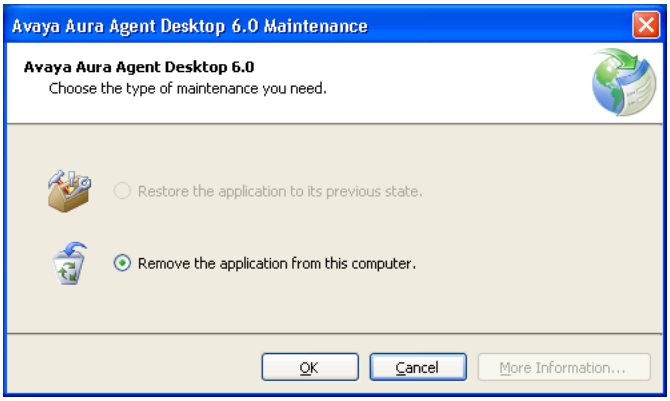


3 From the list of **Currently installed programs**, select **Avaya Aura Agent Desktop 6.0**.



4 Click **Change/Remove**.

5 On the **Avaya Aura Agent Desktop 6.0 Maintenance** dialog, select **Remove the application from this computer**.



6 Click **OK**.

7 Follow the on-screen instructions to uninstall Avaya Aura Agent Desktop 6.0 software.

--End--

Starting Agent Desktop

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

Prerequisites

- Ensure that High Availability is configured.

Procedure steps

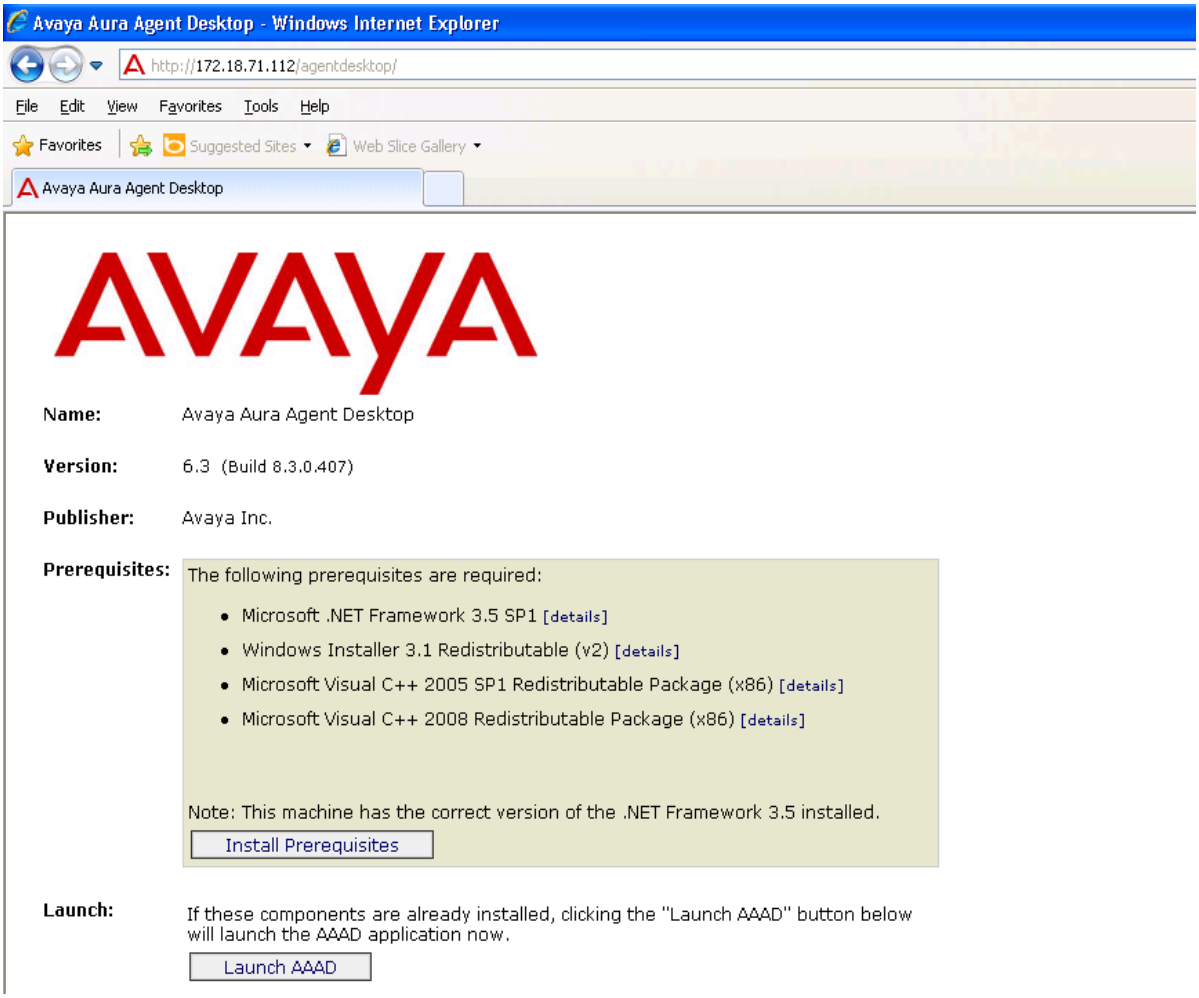
Step	Action
1	In Windows Explorer or Internet Explorer, enter the HTTP address (URL) provided by your Domain Administrator. The URL format is <HA pair Managed IP address>/agentdesktop. For example, type **http://172.18.71.112/agentdesktop**
2	Click **Launch AAAD**. Follow the on-screen instructions to download and install the Agent Desktop software.

--End--

Procedure job aid

In High Availability solutions you must launch the Agent Desktop software from the HA pair Managed IP address.

Example of launching Agent Desktop from the HA Managed IP address



Creating a shortcut to the Agent Desktop

Create a shortcut to the Agent Desktop to quickly access the application without manually entering the URL.

Prerequisites

- Ensure that you install Agent Desktop.

Procedure steps

Step	Action
1	Click **Start**, **Programs**, **Avaya**.
2	Right-click Avaya Aura Agent Desktop.

3 Select **Send To**, **Desktop (create shortcut)**.

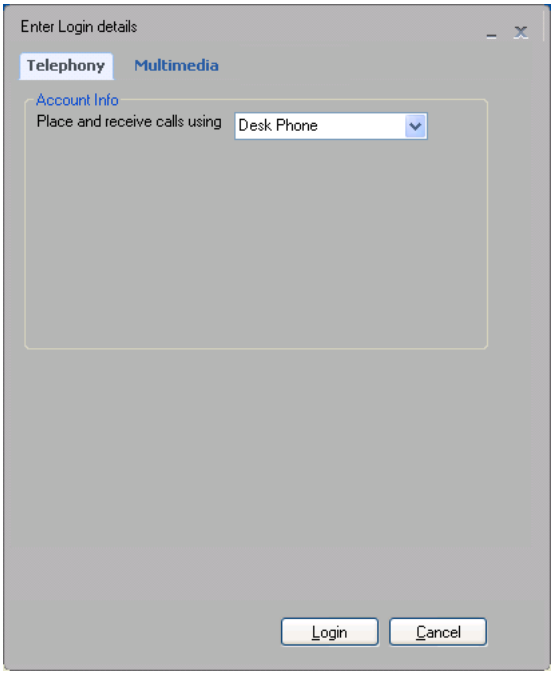
--End--

Logging on to Agent Desktop when using a desktop phone

Log on to Agent Desktop after you start the Agent Desktop application. The system automatically configures your status to Not Ready. Change your status to Ready to indicate that you are available to handle all media types for which you are licensed and configured. If you are assigned to a skillset for a particular contact type, you can receive and create contacts in that contact type.

Procedure steps

Step	Action
1	Start Agent Desktop.
2	On the Agent Desktop Top bar, from the **Status** list, select **Login**.
3	Click the **Telephony** tab.



4	From the **Place and receive calls using** drop-down list, select **Desk Phone**.
5	On the **Multimedia** tab, type your **ID** and **Password**. For example, type 42000 as the ID and 42000 as the password.
6	Click **Login**.

The status icon changes to the Not Ready status.

--End--

Variable definitions

Description	Value
ID (Multimedia)	Your logon ID appears in the ID box, based on your Communication Control Toolkit configuration.
Password (Multimedia)	Initially, for multimedia agents, your password is the same as your Agent Logon ID. The system verifies your password and logs you on to the Agent Desktop application. The Logged Out button changes to Logged In.

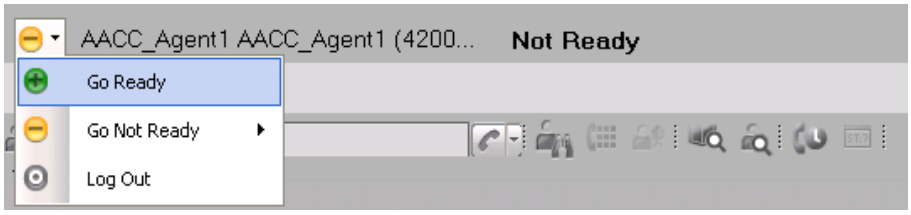
Changing your status to Ready

Change your status to Ready when you are available to create or receive contacts.

When you change your status to Ready in a SIP-enabled Contact Center, your Contacts Presence status automatically changes to Available.

Procedure steps

Step	Action
1	On the Agent Desktop Top bar menu, click the Status icon.
2	Select **Go Ready**.



Agent Desktop places you in Ready status. The status icon changes to green and the Top bar displays the Ready status.

--End--

Generating a test call

Accept and work with a test call. The relevant work item controls become active and the call timer appears in the work item.

Prerequisites

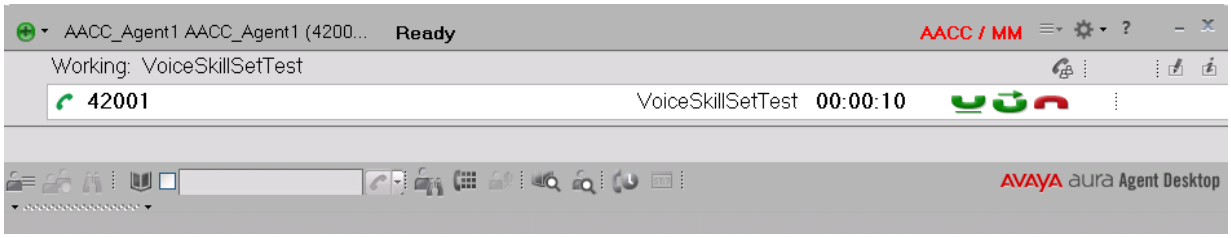
- Ensure that you are in Ready state.
- Ensure that you have a skillset designated to handle telephone calls.

Procedure steps

Step	Action
1	Generate a test call that resolves to the Agent skillset. For example, from another phone on the same Communication Manager, dial the contact center route point of 52000.
2	On the Agent Desktop, select the new alerting work item and click the **Accept** work item control. *The top pane of the Agent Desktop shows the customer details and history of all past calls with the contact.*

--End--

Procedure job aid



Generating a test email contact

Accept an incoming email contact to display customer details and begin contact with a customer. Agent Desktop expands to show the customer details and the call timer appears in the work item. The new incoming email is presented as a new work item in the work list window.

Procedure steps

Step	Action
1	Generate a test email. For example, create an email requesting support or assistance and send this email to mailbox99@labmail.com. The email must contain the keyword Assistance or Support.

The test email is presented to the logged on agent.

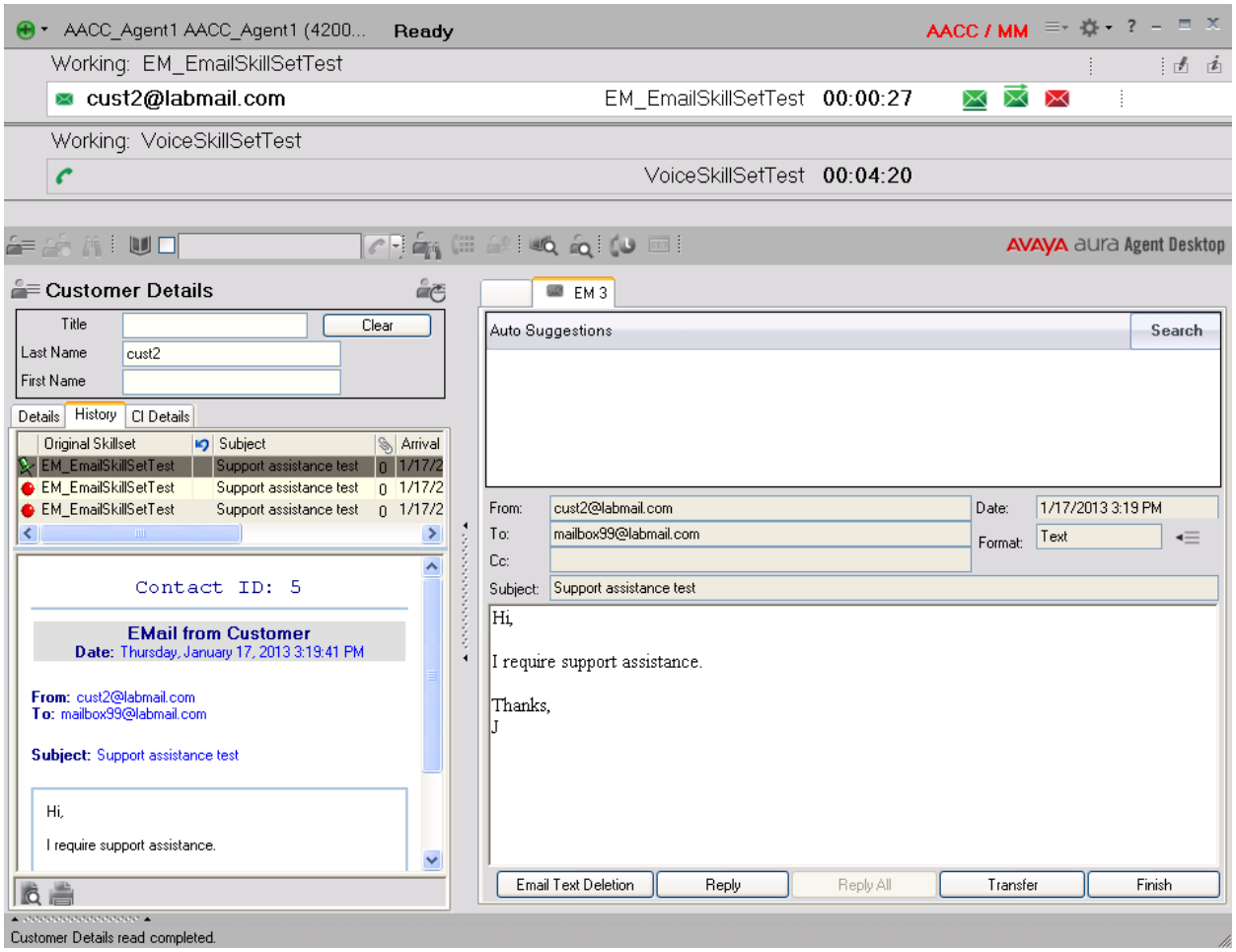
2 On the Agent Desktop, click **Accept**.

The email opens in the email Display panel.
The customer details for the email appears in the bottom left hand Customer Details panel.

--End--

Procedure job aid

Example of accepting a test email.



Testing voice and email resiliency by generating a Voice and Multimedia Contact Server switchover

Test the resiliency of the Avaya Aura® Contact Center – High Availability solution by generating a switchover on the active Voice and Multimedia Contact Server.

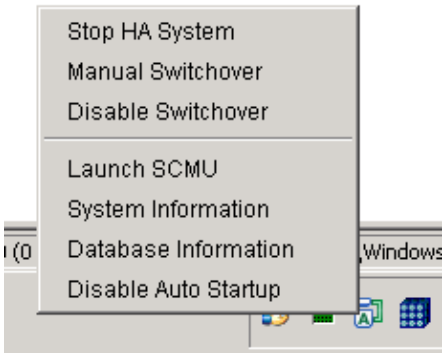
You can generate a switchover by disconnecting the network cable from the active Voice and Multimedia Contact Server. This procedure uses the High Availability manual switchover feature to verify High Availability phone call resiliency.

Prerequisites

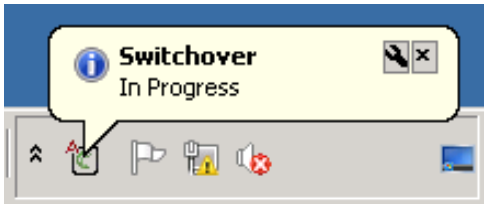
- Ensure an Agent Desktop agent has answered the test call and test email message.

Procedure steps

Step	Action
1	Log on to the active server (AACCHOST1 - 172.18.71.110).
2	On the Windows taskbar of the active server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Manual Switchover**.

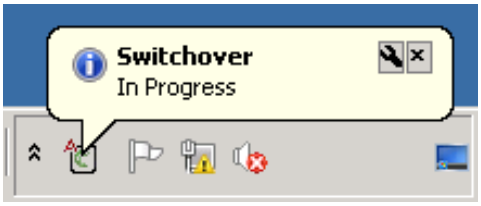


3	On the **SMMC** message box, click **OK**.
4	The active server begins to switchover.
5	On the active server the High Availability system tray icon displays a message box counting down the switchover.

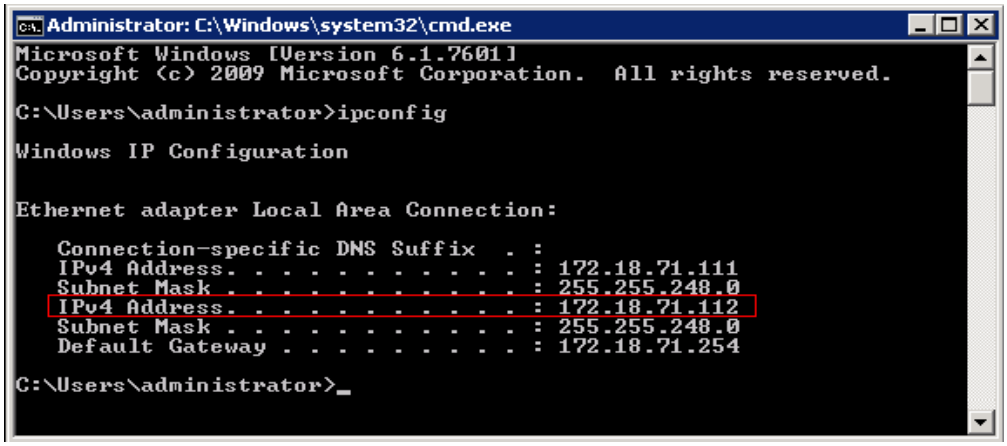


6 The standby (AACCHOST2 - 172.18.71.111) continues to shadow the active server (AACCHOST1 - 172.18.71.110).

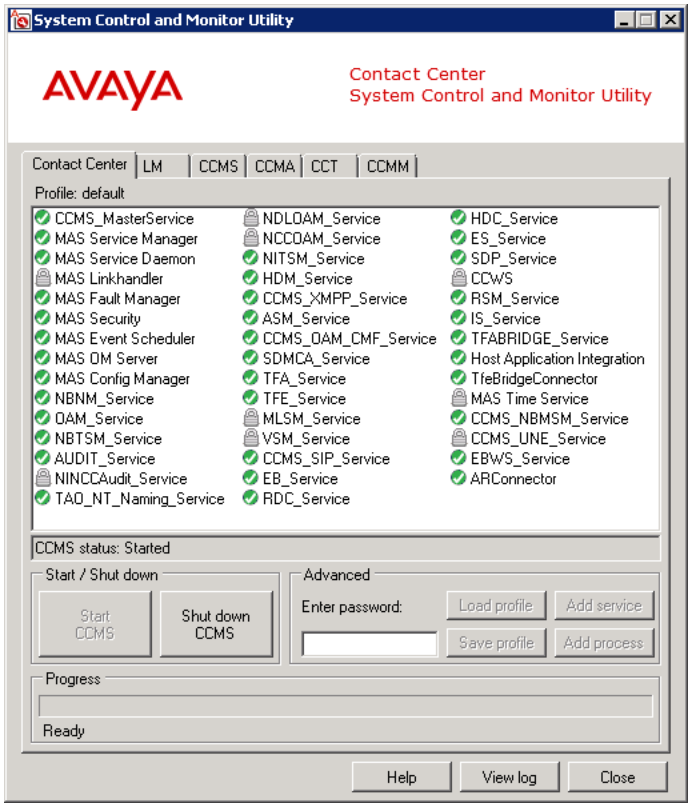
7 The standby server then recognizes that a switchover is in progress. The High Availability system tray icon on the standby server displays a message box indicating that a switchover is in progress.



8 After the switchover, the standby server is now hosting the Voice and Multimedia Contact Server HA pair Managed IP address. The Managed IP address is now attached to the network interface on the original standby server. The original standby server is now the active server. In this worked example the AACCHOST2 server (172.18.71.111) is now the active server.



9 The core CCMS, CCMA, CCMM and CCT services are now running on the new active server (AACCHOST2 - 172.18.71.111).



10 The new active server (AACCHOST2 - 172.18.71.111) is now processing customer contacts.

11 Verify that the Agent Desktop agent is still logged on and is in the ready state.

12 Verify that the voice contact is still open.

13 Verify that the email contact is still open and editable.

14 Verify that Agent Desktop still has call control by placing the call on hold.

--End--

Handling multimedia contact refreshes during a switchover

Agent Desktop software supports multimedia contacts such as email.

If a Contact Center server switchover occurs, you may notice that all of your Agent Desktop contacts refresh; they are removed and recreated in Agent Desktop after the switchover. This contact refreshing may take a few seconds, depending on the number of contacts you have open. During the contact refreshing period you cannot use Agent Desktop to handle multimedia contacts,

but you can continue to handle customer voice calls using your desk phone. When the contacts have refreshed, the contact open time is correct and typed contact information is still present. If you were typing an email reply when the switchover occurred, your unfinished email is preserved and you can continue typing from where you were interrupted. You can continue to handle customer contacts using Agent Desktop as normal.

Procedure steps

Step	Action
1	If Agent Desktop starts to refresh the contacts in your Work Item list, do not use Agent Desktop. Stop typing and allow Agent Desktop to completely refresh the contacts Work Item list.
2	If you are handling a customer voice contact, continue to handle the phone call using your desk phone.
3	When the contacts Work Item list has fully refreshed, confirm that all your contacts are still open and continue handling multimedia and voice contacts using Agent Desktop.

--End--

Handling loss of desk phone control

Normally you use Agent Desktop software to control your desk phone and to handle customer phone calls. If Agent Desktop is unable to control your desk phone, use your desk phone to continue handling customer phone calls. Do not attempt to use Agent Desktop to handle customer phone calls. When Agent Desktop regains control of your desk phone, a message box appears to inform you that Agent Desktop can now be used again for telephony operations.

Procedure steps

Step	Action
1	If Agent Desktop displays a **Please use your phone for telephony operations. A message will appear when AAAD control returns** message box, show the message to your supervisor.
2	On the message box, click **OK**.
3	Continue to handle customer phone calls using your desk phone. Do not attempt to use Agent Desktop to handle customer phone calls.
4	When the **AAAD can now be used again for telephony operations** message box appears, click **OK** and use Agent Desktop to handle customer phone calls.

--End--

Handling Server communication issues

Agent Desktop connects to multiple Contact Center servers. In the event that the connection to the servers is lost, Agent Desktop repeatedly attempts to reconnect. If you are forced to exit Agent Desktop as a result of server communication issues, all multimedia contacts such as email are lost. You can continue to handle phone calls using your desk phone, while server communication is lost.

Procedure steps

Step	Action
1	If Agent Desktop shows a **CCT Session Disconnected** message box, show the message to your Supervisor.
2	On the message box, click **Dismiss** and continue to handle phone calls using your desk phone.
3	If Agent Desktop shows a **Server Error - Failed to connect to the CCMM Server** message box, show the message to your Supervisor.
4	On the message box, click **Dismiss** and continue to handle voice contacts.
5	Agent Desktop continues attempting to reconnect with the server. On successful reconnect you may need to login again.
6	If Agent Desktop repeatedly fails to reconnect with the server, speak with your Supervisor, and if necessary click **Exit Application**.

--End--

Handling configuration issues when launching Agent Desktop

In multimedia solutions, Agent Desktop is downloaded from and connects to one or more Contact Center Multimedia (CCMM) servers. In voice-only solutions, install the Agent Desktop Telephony Toolbar on the Communication Control Toolkit (CCT) server. Agent Desktop is then downloaded from and connects to one or more CCT servers.

When launched, Agent Desktop attempts to connect to the default server and download the configuration file. In High Availability solutions, if Agent Desktop is unable to access the configuration file on the default server it attempts to access the configuration files on the other servers. If Agent Desktop can access the

configuration files on another server it displays a message box. The agent can choose to accept the configuration settings for that server or choose to attempt to connect to another server.

Procedure steps

Step	Action
1	If Agent Desktop displays a **Configuration Settings Error** message box, show the message to your Supervisor.
2	If you wish to accept the configuration settings from the server specified, on the **Configuration Settings Error** message box click **OK**.
3	If you do not wish to accept the configuration settings from the server specified, on the **Configuration Settings Error** message box click **Cancel**.
4	In the **CCMM Server Error** message box a list of available servers is displayed. Choose which server you want to connect to and click **Connect**.
5	If the problem persists, speak with your Supervisor.

--End--

Replying to the test email message

Reply to the test email message to verify that you can send an email after a High Availability switchover. Create a response to a customer in the same format as the original request.

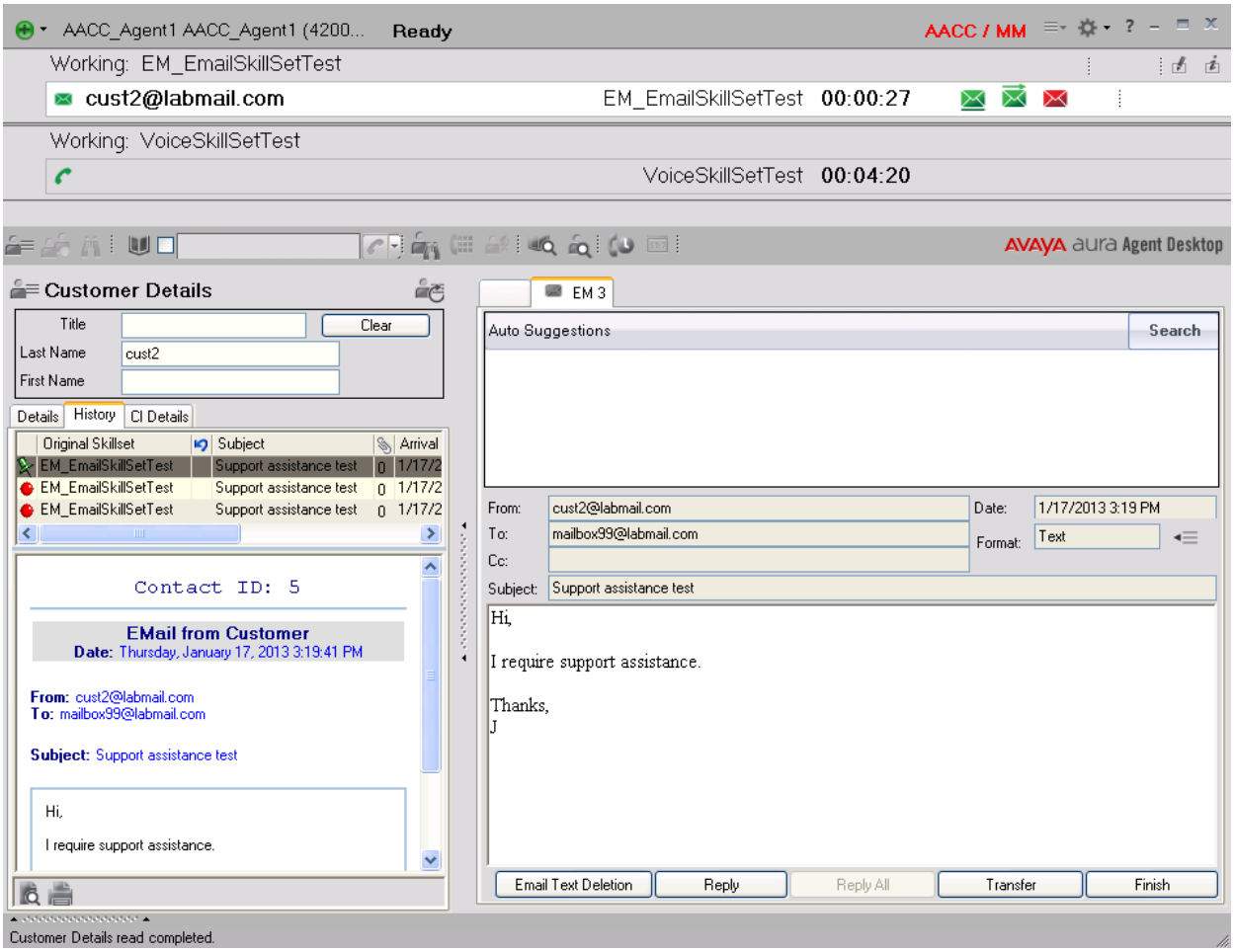
You can use several features in the Agent Desktop interface to create your email response in HTML or plain text:

- Auto suggestions
- the address book
- one or more response templates
- an automatic signature
- an attached file
- the spelling checker

You can also add a comment to an email message in the Agent Note box as a reference for later communications with the customer. The customer does not see the content of the Agent Note box.

Procedure steps

Step	Action
1	After you review the customer contact, click **Reply**.



2 In the **E-mail Response** window, accept the default **To** email address, with the same email address from which the message was sent.

3 In the **Subject** box, accept the subject currently displayed or edit the subject.

4 Add text to the reply using one or both of the following methods:

- Type the message text.
- Add a template response.

5 If you use HTML text and you want to bold, underline, or italicize any text, select the text and click the appropriate button to apply formatting. You cannot format plain text.

6 To change the text size, select the text and click the up arrow to increase the font size, or click the down arrow to decrease the font size.

7 To perform a spell check, click the Check Spelling icon.

8 To add an attachment to the email response, click Insert a file.

Step	Action
9	In the **Agent Note** box, type additional information about the contact or the customer. Only agents and supervisors can view the information in the **Agent Note** box.
10	Click **Send**.
11	Close the contact. If required, select a reason for closing the contact.

--End--

Ending the test call

End the test call when testing is completed. If you were in Ready status before the call, you automatically return to Ready when you terminate the call. If you require time to perform call wrap-up tasks before you accept another call, change your status to Not Ready and enter a Not Ready Reason Code in the Code field of the Top bar. Not Ready Reason codes are defined by the Administrator.

Procedure steps

Step	Action
1	On the work item, click **Release**.

--End--

Logging off from Agent Desktop

Log off from Agent Desktop when you are ready to exit the application.

A warning message appears asking you to confirm that you want to close the Agent Desktop and log off.

Prerequisites

Ensure that you do not have any contacts open. If a contact is open, you must close the contacts before you log off of the application.

Procedure steps

Step	Action
1	On the Agent Desktop Top bar menu, click the Status icon.
2	Click **Log Out**. *Agent Desktop logs you off. The status icon changes to red and the Top bar displays the Logged Out status.*

--End--

How to reinstate High Availability after a switchover

In campus solutions, if the active server fails the standby server starts processing contacts. The initially active server is now stopped, and the High Availability - Enable Switchover option is disabled. The standby server becomes the active server and it continues to process contacts. The High Availability SMTP feature sends an email to the Contact Center Administrator informing them about the switchover. The active server has no corresponding standby server at this point, and the solution is no longer resilient.

When the root cause of the failure has been addressed the Contact Center Administrator may re-instate High Availability resiliency using the following procedure.

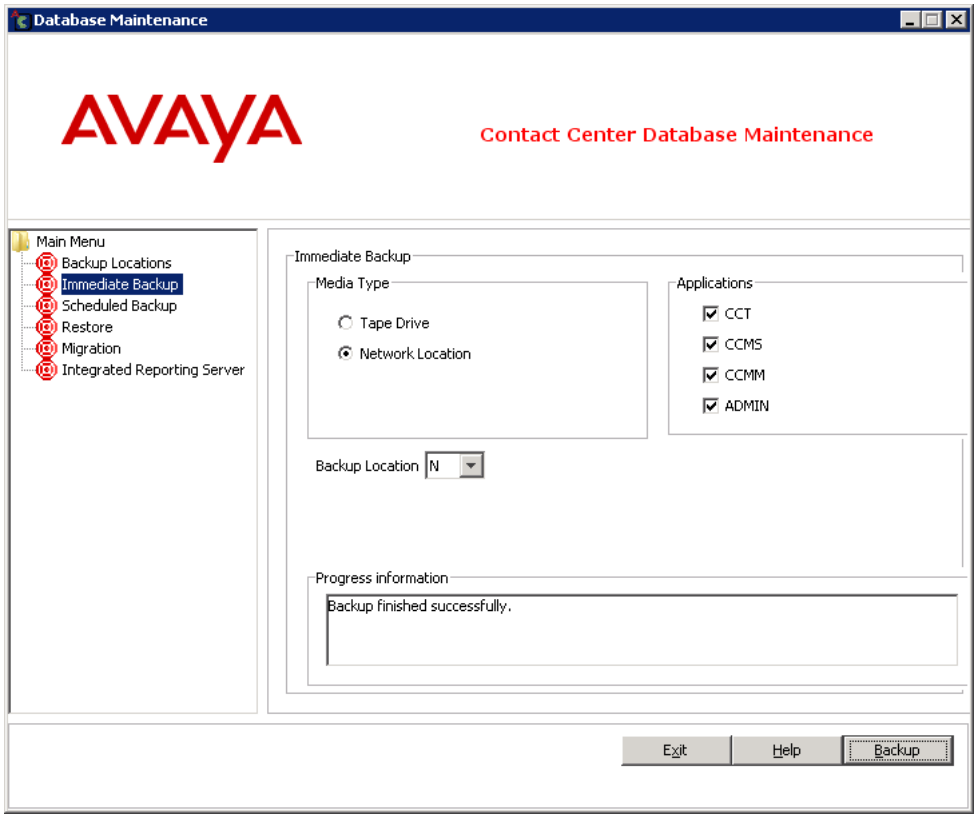
After the switchover, the standby server is now the current active server. The following tables list the current active server details used in this worked example.

Voice and Multimedia Contact Server details after a switchover:

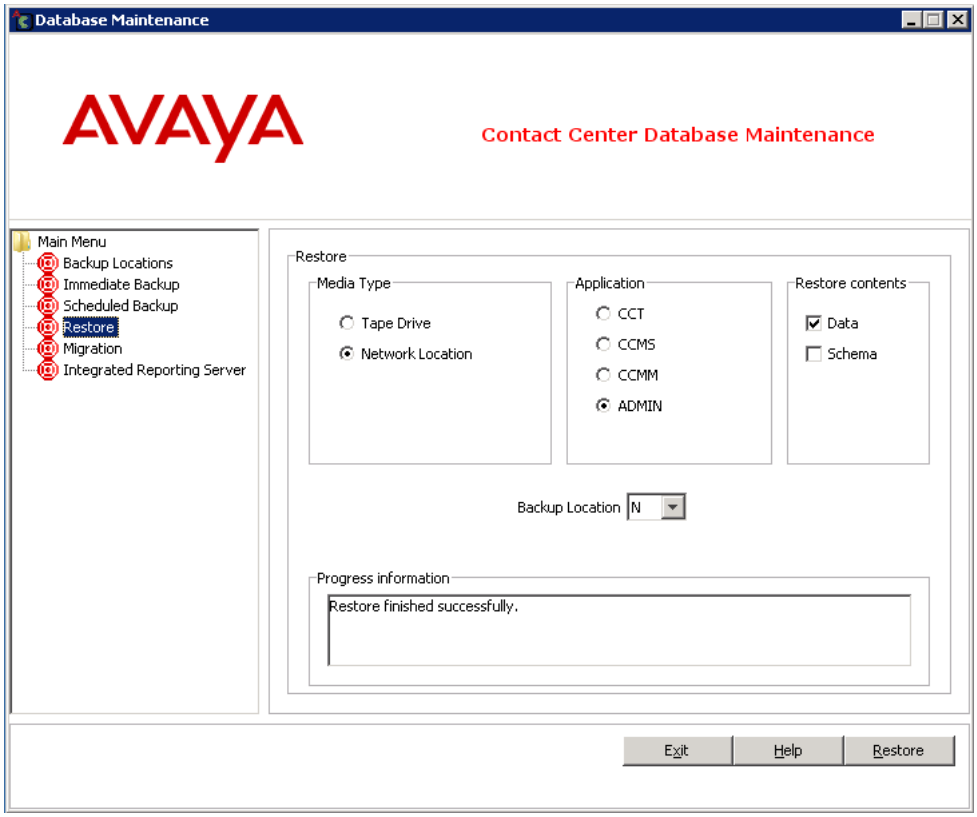
Example Voice and Multimedia Contact Server details	
Current active server name	AACCHOST2
Current active server IP Address	172.18.71.111
Previous active server name	AACCHOST1
Previous active server IP Address	172.18.71.110
Managed server name	AACCMANHOST
Managed IP Address	172.18.71.112

Procedure steps

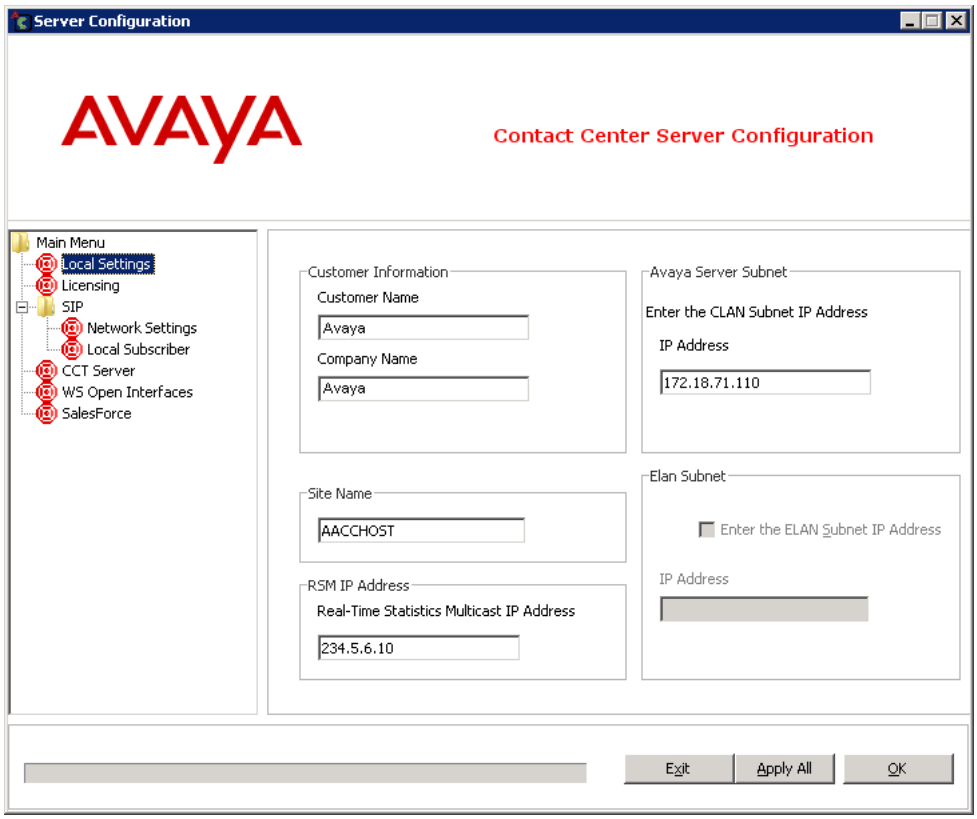
Step	Action
1	Backup the current active server CCMS, CCT, CCMM, and ADMIN databases. For example, backup the (AACCHOST2 - 172.18.71.111) server databases.



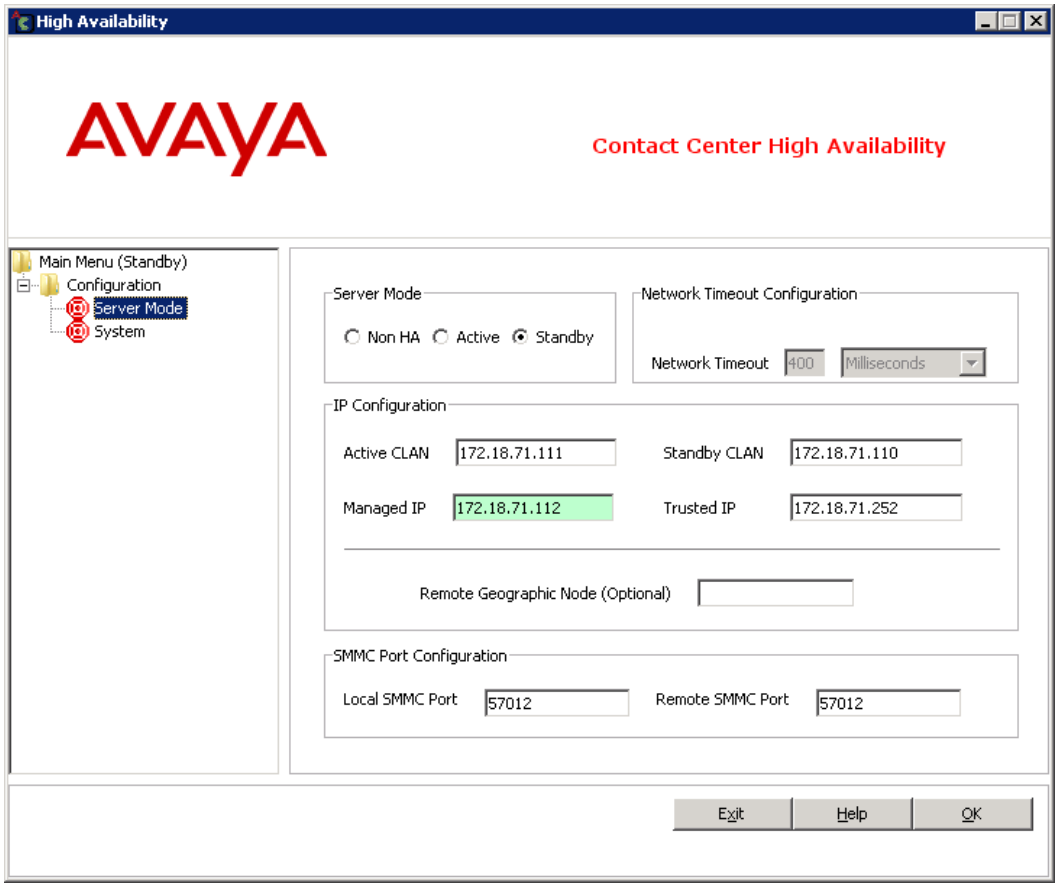
2 Restore these databases to the new standby server. Restore the ADMIN database last. For example, restore the server databases onto AACCHOST1 - 172.18.71.110.



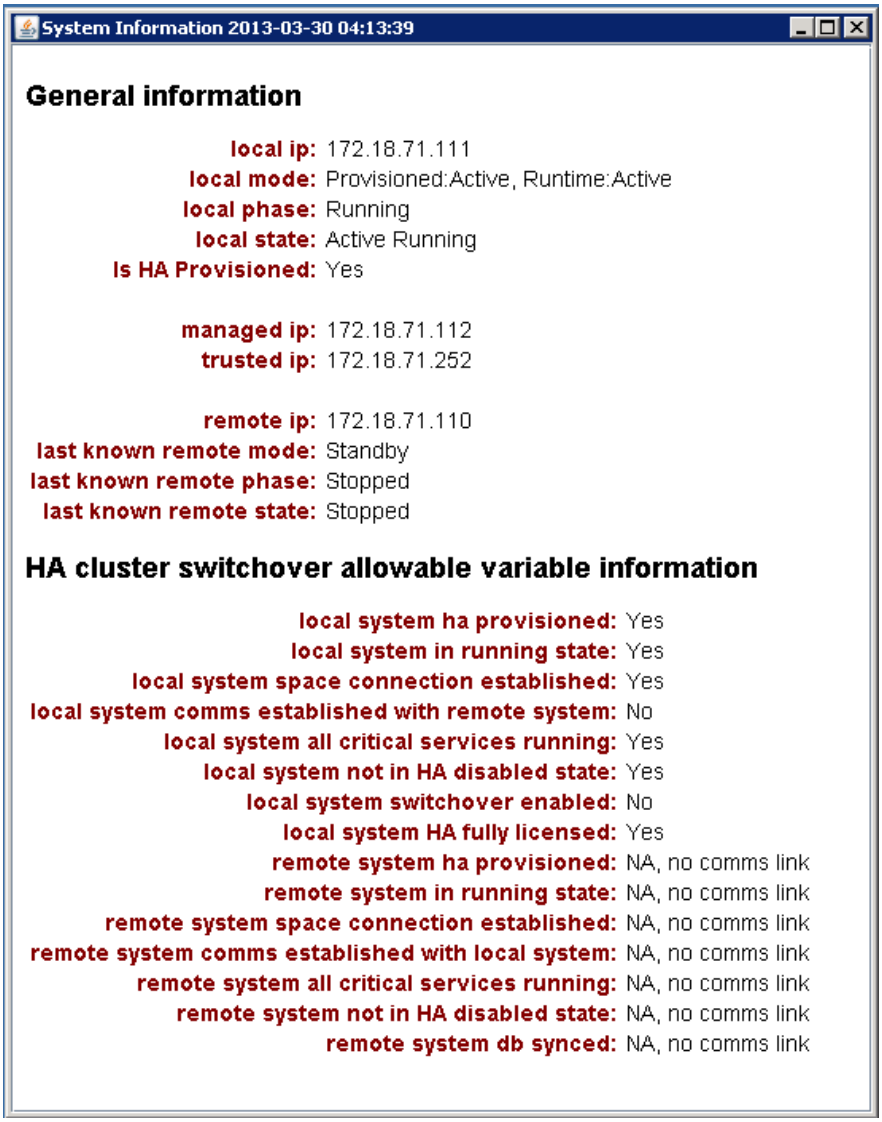
3 On the new standby server (AACCHOST1 - 172.18.71.110), reconfigure the server details using CCMS Server Configuration. Update the server details to match the standby server.



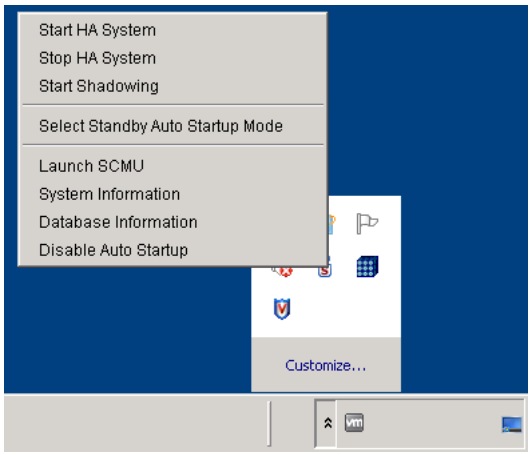
4 On the new standby server, configure a standby server using the High Availability utility. For example, configure High Availability on the AACCHOST1 (172.18.71.110) server.



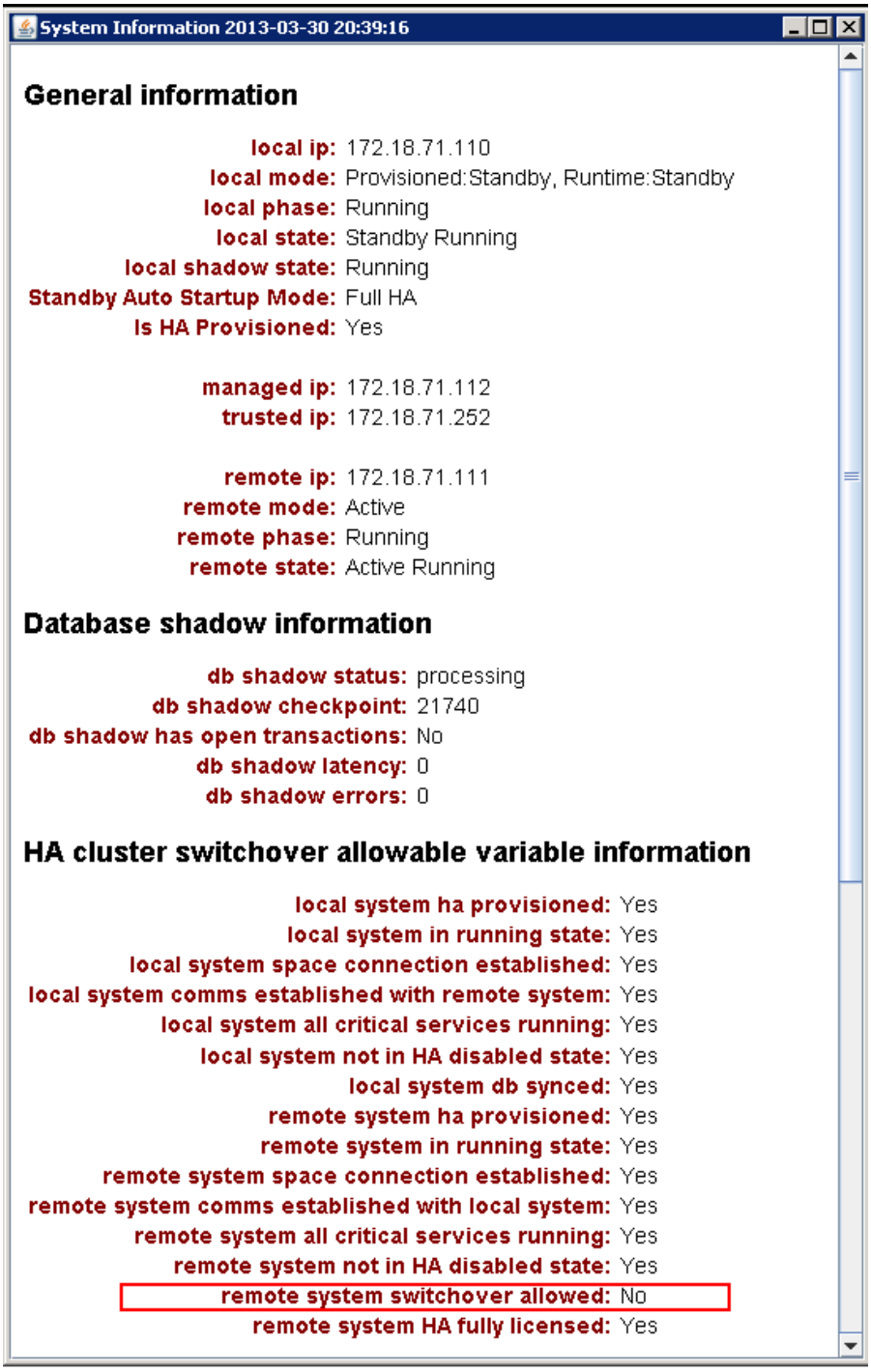
5 After the switchover, AACCHOST2 (172.18.71.111) is running in active mode.



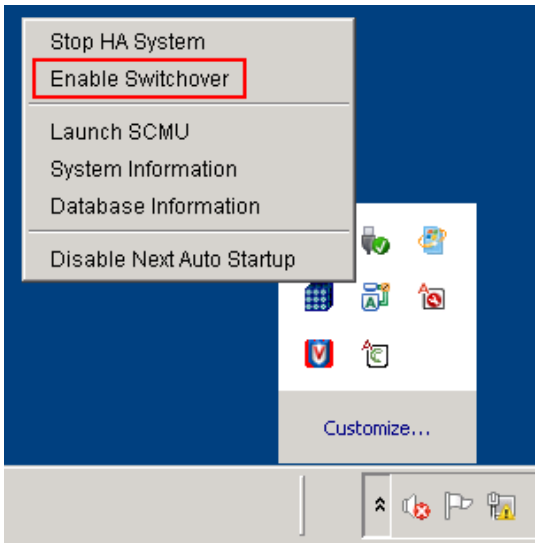
6 On the new standby server, use the System Management and Monitoring Component (SMMC) to start the HA System. For example, on the AACCHOST1 (172.18.71.110) server, use the SMMC system tray to **Start HA System**.



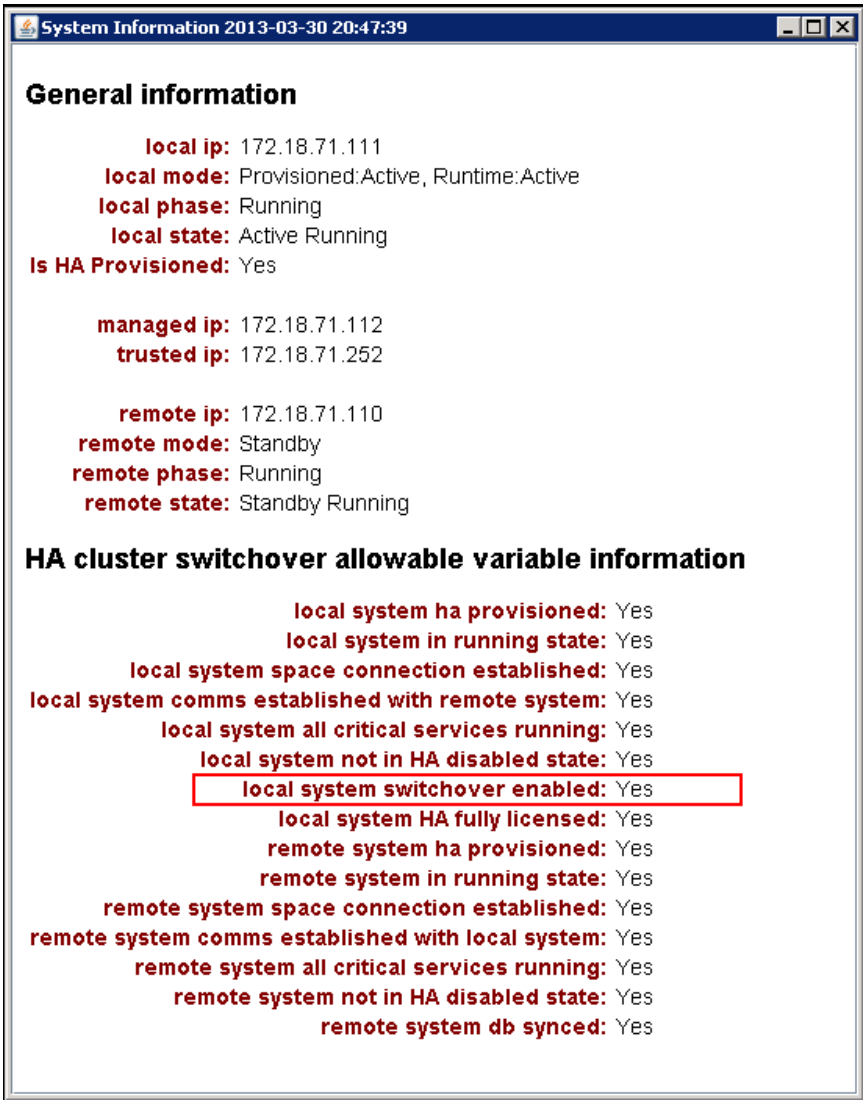
7 Contact Center services must restart on the standby server (AACCHOST1 - 172.18.71.110) before the standby server starts shadowing the active server. Switchovers are not yet re-enabled.



8 On the active server, enable HA switchover.



9 Switchover is now enabled on the active server. High Availability is now reinstated.


System Information 2013-03-30 20:47:39
General information
local ip: 172.18.71.111
local mode: Provisioned:Active, Runtime:Active
local phase: Running
local state: Active Running
Is HA Provisioned: Yes
managed ip: 172.18.71.112
trusted ip: 172.18.71.252
remote ip: 172.18.71.110
remote mode: Standby
remote phase: Running
remote state: Standby Running
HA cluster switchover allowable variable information
local system ha provisioned: Yes
local system in running state: Yes
local system space connection established: Yes
local system comms established with remote system: Yes
local system all critical services running: Yes
local system not in HA disabled state: Yes
local system switchover enabled: Yes
local system HA fully licensed: Yes
remote system ha provisioned: Yes
remote system in running state: Yes
remote system space connection established: Yes
remote system comms established with local system: Yes
remote system all critical services running: Yes
remote system not in HA disabled state: Yes
remote system db synced: Yes

--End--

Maintenance section

- Patching – Voice and Multimedia Contact Server software (page 647)

Patching – Voice and Multimedia Contact Server software

This chapter describes how to install patches on a Voice and Multimedia Contact Server. This includes the following server software:

- Contact Center Manager Server
- Contact Center License Manager
- Contact Center Manager Administration
- Communication Control Toolkit
- Contact Center Multimedia
- Orchestration Designer

If your Avaya Aura® Contact Center is licensed for standby servers, you can hot patch your software to minimize down-time. You must patch both the active and standby servers to the same patch level.

Installing Voice and Multimedia Contact Server software patches

Install the most recent Voice and Multimedia Contact Server software service patches to ensure that you have the most current development updates.

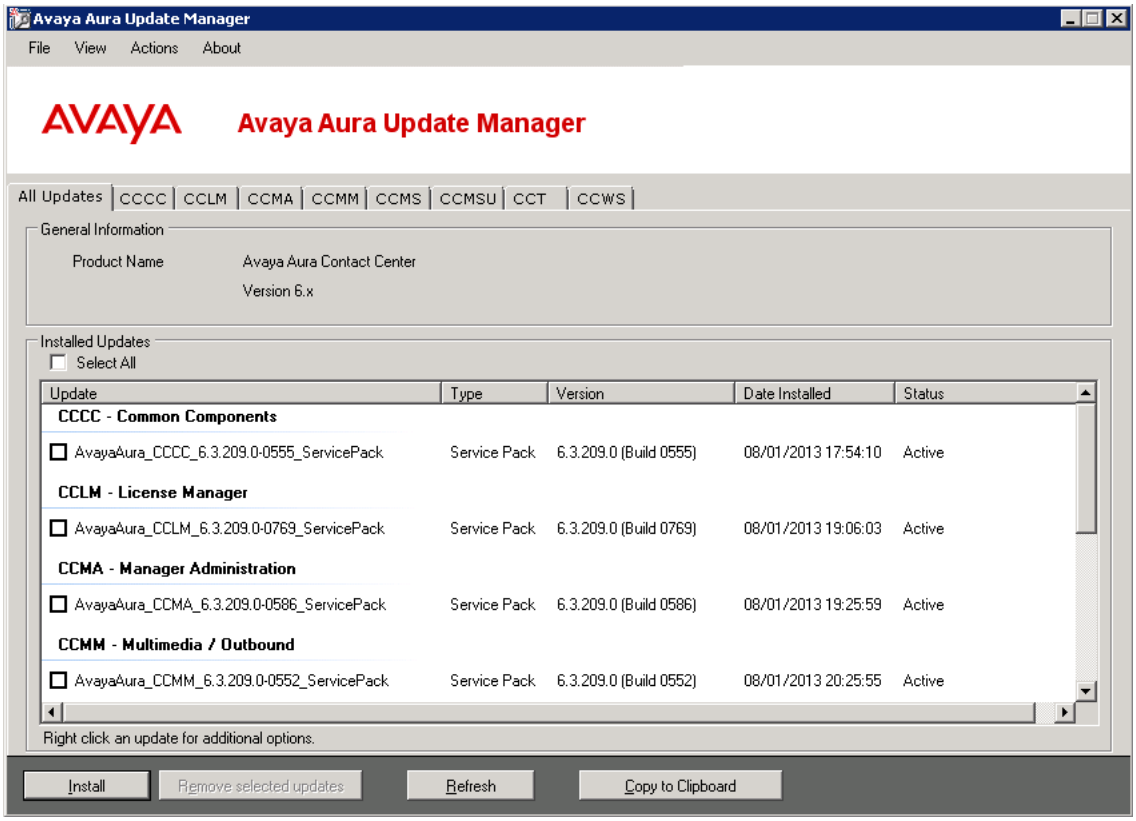
During a patch installation, all System Management and Monitoring Component (SMMC) services and the SMMC System Tray application stop to allow Contact Center files to be patched. After patching the server, if the patch does not require a server reboot, you must start the SMMC applications manually.

Prerequisites

- Download the most recent Avaya Aura® Contact Center patches.

Procedure steps

Step	Action
1	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Common Utilities**, **Contact Center Patch Manager**.



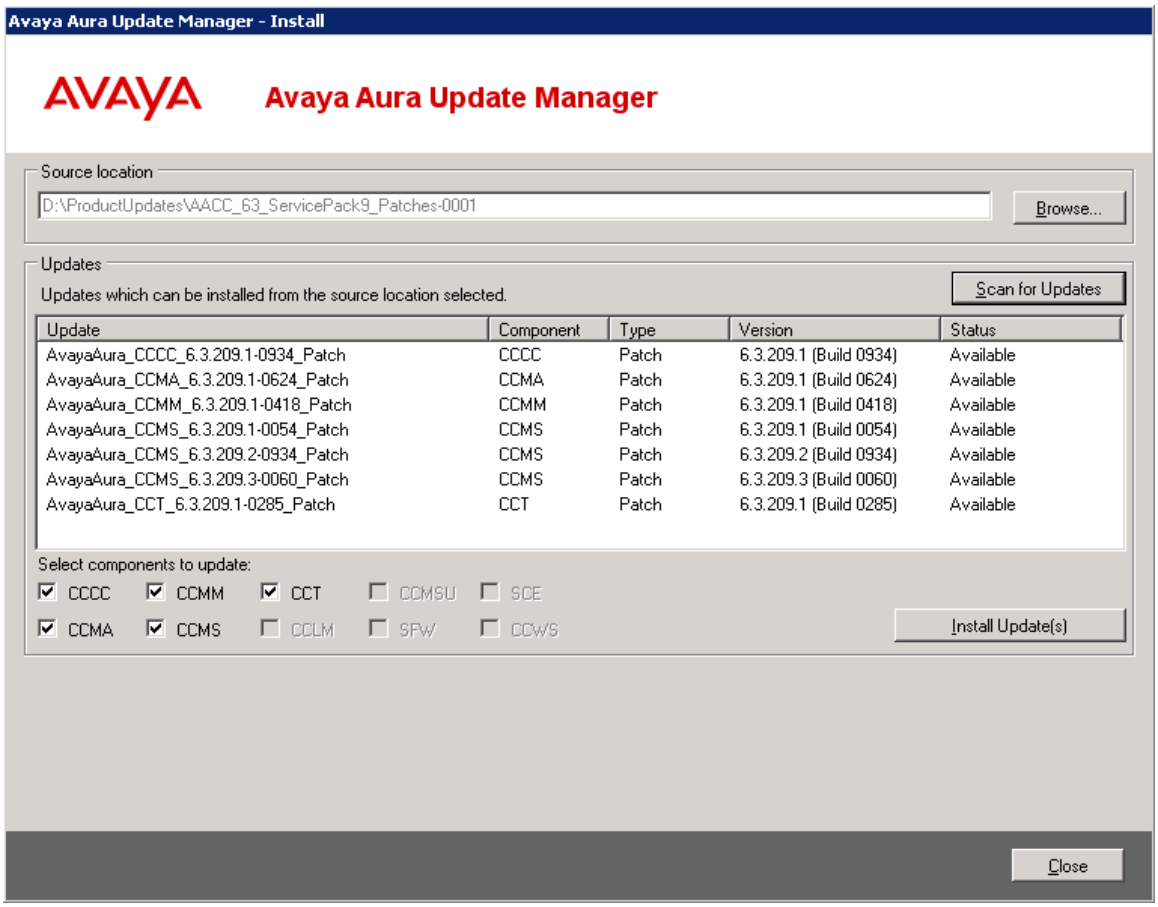
2 Click **Install**.

3 Click **Browse** and navigate to the folder where you have downloaded the server packs.

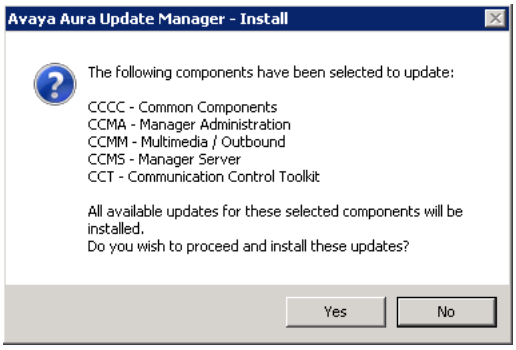
4 Click **Scan for Updates**.

The Contact Center Updates section displays the available patches.

5 Select the appropriate patch.



6 Click **Install Update(s)**.



7 Click **Yes**.

The Patch Manager installs the patch and displays a confirmation message.

8 If prompted to reboot your server, click **Close** and restart your server.

9 If the Voice and Multimedia Contact Server is not restarted, click **Start**, **Avaya**, **Contact Center**, **Common Utilities**, **SMMC SystemTray**.

10 On the Windows system tray, right-click the SMMC system tray icon, and select **Start SMMC**.

--End--

Troubleshooting section

- Troubleshooting – SIP Contact Center (page 653)
- Troubleshooting – High Availability (page 663)
- Troubleshooting – Avaya Aura platform (page 679)

Troubleshooting – SIP Contact Center

This section describes the troubleshooting procedures that you perform when handling SIP issues in an Avaya Aura® Contact Center.

Responding when dialing a Route Point

When a Route Point is dialed, the customer is placed on a conference call in the Avaya Media Server and ringback is the first treatment. If a Route Point is dialed and there is no audible response or error code, check the Route Point has been acquired on the Contact Center Manager Administration server.

Prerequisites

- Ensure the Contact Center Manager Administration server is configured.

Procedure steps

Step	Action
1	Check the Route Point is acquired. For more information, see Adding route points for voice contacts (page 201).

--End--

Logging on to Agent Desktop

When an agent cannot log on to Agent Desktop, the agent is presented with an internal server error message. There can be many reasons for this error, however one resolution is to check the transport type for the SIP CTI Proxy Server is correct. Ensure the SIP settings in the server configuration utility are correct.

Procedure steps

Step	Action
1	If your contact center uses an Avaya Aura® Application Enablement Services server, check the transport type for the SIP CTI Proxy setting in the Server Configuration utility is set to TLS.

--End--

Troubleshooting when hold/unhold causes calls to be dropped after seventy seconds

If hold/unhold causes calls to be dropped after seventy seconds, there is a problem with the SIP terminal configuration.

Procedure steps

Step	Action

Step	Action
1	Check the agent's SIP terminal configuration in Contact Center Manager Administration.

--End--

Playing ringback into an active call

If ringback or an announcement is played in an active call, there is a problem with the SIP terminal configuration.

Procedure steps

Step	Action
1	Check the agent's SIP terminal configuration in Contact Center Manager Administration.

--End--

Call processing fails due to suspected Avaya Media Server failure

If there is an issue with call processing which has been narrowed down to Media Application failure, follow these sequence of steps.

Procedure steps

Step	Action
1	Ping the Avaya Media Server to ensure it is on the network.
2	If it is on the network, log on to the Avaya Media Server and ensure there are no alarms in the Alarms window in Element Manager.
3	If there are no alarms, ensure the Avaya Media Server handled the INVITE correctly. Turn on logging and check the timestamp of the failed call in the sipmcDebug.txt file.
4	If there is no INVITE in the logs, there is a problem with the lower level components of the Avaya Media Server (i.e. the SIP stack).

--End--

Handling 486 Busy Here error messages

If there is no ringback on a call and message 486 Busy Here is in the CCMS_SGM_SIPMessages.log, the CCMS cannot establish communication with the Avaya Media Server.

Procedure steps

Step	Action
1	Ensure the Firewall is turned off on the Avaya Media Server. Avaya Media Server cannot function correctly with a Firewall turned on.
2	Ensure Domain policies are correct as per defined by your Domain Administrator.

--End--

Handling 404 Not Found error messages

If there is no ringback on a call and error message 404 Not Found is in the CCMS_SGM_SIPMessages.log, the CCMS cannot establish communication with the Avaya Media Server. This indicates that the Avaya Media Server services have not been installed correctly, or that Avaya Media Server is configured to use the wrong port. The Avaya Media Server port may be set at 5070 if, for example, Avaya Media Server is co-resident with Contact Center Manager Server.

Procedure steps

Step	Action
1	Verify the Contact Center Services (Announcement, Conference, Dialog) exist in Packaged Applications in the Element Manager. If they do not exist the Contact Center Services installer was not run, or failed to run successfully.
2	Run the Contact Center Services installer.
3	If Avaya Media Server is installed co-resident with Contact Center Manager Server and Contact Center Manager Administration, ensure the Avaya Media Server port is not set to 5060. For example, ensure the Avaya Media Server port is set to 5070.

--End--

Handling 480 Temporarily Unavailable error messages

If there is no ringback on a call and error message 480 Temporarily Unavailable is in the CCMS_SGM_SIPMessages.log file, the Contact Center Manager Server cannot establish communication with the Avaya Media Server. This is due to an one of the following license issues with Avaya Media Server:

- Not licensed
- Licensed incorrectly
- Licensed but the license is not saved and confirmed.

Procedure steps

Step	Action
1	To verify this look for any alarms in the Avaya Media Server Alarms window. If there are no issues there, use the Avaya Media Server logs to pinpoint the problem.
2	Apply a license to the Avaya Media Server, save and Confirm the license.

--End--

Handling 488 error messages

Error message 488 error (SDP fault) error message is in the CCMS_SGM_SIPMessages.log file. This is due to video codecs enabled on the Avaya Media Server.

Procedure steps

Step	Action
1	Remove all video codes from the Avaya Media Server.

--End--

Troubleshooting when digits entered for IVR Play and Collect are not recognized

Avaya Media Server collect digits and sends them to the Contact Center Manager Server, but the relevant IVR is not acted upon.

Procedure steps

Step	Action
1	On the Avaya Media Server, log on to Element Manager.

2 In the navigation pane, click **System Configuration**, **Media Processing**, **Digit Relay (DTMF)**.

3 On the **Digit Relay (DTMF)** page, select **RFC2833**.

4 On the **Digit Relay (DTMF)** page, select **INFO digits**. **INFO digits** must be enabled after enabling **RFC2833**, **RFC2833** must appear first on the list.

5 Click **Save**.

--End--

Troubleshooting when no terminals or addresses appear in Agent Desktop

No terminals or addresses appear in the Communication Control Toolkit reference client (RefClient) or in Avaya Aura® Agent Desktop and as a result, Agents cannot log on.

Procedure steps

Step	Action
1	In Contact Center Manager Administration, ensure every agent has a unique SIP URI.

--End--

Handling subscribed Resource Availability error messages

Agents cannot log on and a subscribedResourceAvailability CSTA error message is in the CCMS_SGM_SIPMessages.log file. This error suggests that the Avaya Aura® Application Enablement Services server has ran out of agent desktop licenses.

Procedure steps

Step	Action
1	Increase the Avaya Aura® Application Enablement Services **Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)** license count.

--End--

Handling TLS server certificate time zone issues

Signing a Transport Layer Security (TLS) security certificate on a server which is in a different time zone, especially ahead of the server which is to use the certificate, results in a failure in create a server certificate for Avaya Aura® Application Enablement Services.

Procedure steps

Step	Action
1	Ensure that the servers, including the Certificate Authorities and Avaya Aura® Application Enablement Services,are in the same time zone.

--End--

Handling missing TLS certificates

The Avaya Aura® Contact Center SIP Gateway Manager (SGM) Windows service fails to start and a "Failed to read or convert the security information - See previous logs for details" message is in the SGM_SIPSp.log file.

A possible cause of this is that the Certificate Manager steps which create a certificate store on the server has not been performed or the Transport Layer Security (TLS) security certificates have not been added to the store when created.

Procedure steps

Step	Action
1	Create a certificate store on the Contact Center Manager Server. For more information see, *Avaya Aura® Contact Center Commissioning* (NN44400-312).
2	Create the root and signed certificates. For more information see, *Avaya Aura® Contact Center Commissioning* (NN44400-312).

--End--

Troubleshooting CCMS and AES TLS communication issues

The Avaya Aura® Contact Center SIP Gateway Manager (SGM) windows service is running but agents cannot log on. A possible cause of this is that the Transport Layer Security (TLS) connection between the Contact Center Manager Server and Avaya Aura® Application Enablement Services is not functioning correctly.

Procedure steps

Step	Action

1. Create a certificate store on the Contact Center Manager Server. For more information see, *Avaya Aura® Contact Center Commissioning* (NN44400-312).
2. Create the root and signed certificates. For more information see, *Avaya Aura® Contact Center Commissioning* (NN44400-312).
3. Ensure the name entered when creating the certificate store or certificate name [FQDN] are the same as the one entered in the Application Enablement Services trusted server property.
4. Check the certificate name by launching the Certificate Manager, go to the templates tab and check the CN value. It must match the name of the server on which it resides and match the value that has been entered into the Application Enablement Services trusted server property. The Common Name (CN) is case sensitive.
5. Using Contact Center Manager Server - Server Configuration, ensure that TLS is selected, the port is 4723 and the correct IP address of the Application Enablement Services in the SIP-CTI box.

--End--

Troubleshooting when an agent goes not-ready to a presented call

When a call is routed to a Communication Control Toolkit reference client or Avaya Aura® Contact Center, the agent automatically goes to the Not-Ready state.

There are a number of possible causes for this problem.

Procedure steps

Step	Action
1	Ensure the agent is logged into the phone set or station.
2	Examine the SIP traces for the "P-Charging-Vector Required" error message. If this error message is present, log on to Avaya Aura® Communication Manager and on the Sat prompt, change the IMS field on the signaling-group to "n".
3	Examine the SIP traces for the "407 Proxy Authentication Required" error message. If this error message is present, and if you are using an Avaya Aura® Session Manager server, ensure the Contact Center Manager Server is added to the list of authorized list in the Session Manager. For more information, see *Avaya Aura® Contact Center Configuration – Avaya Aura® Unified Communications Platform Integration* (NN44400-521).

--End--

Troubleshooting – High Availability

Troubleshooting High Availability must be done to address errors that occur when active servers do not switchover as expected or when the standby server fails to shadow the active server.

The Windows events log contains extensive High Availability diagnostic information.

Prerequisites for High Availability troubleshooting

- Read *Avaya Aura® Contact Center Fundamentals* (NN44400-110).
- Read *Avaya Aura® Contact Center Installation* (NN44400-311).
- Read *Avaya Aura® Contact Center Commissioning* (NN44400-312).
- Read *Avaya Aura® Contact Center Server Administration* (NN44400-610).

Troubleshooting Mission Critical High Availability

Troubleshoot Mission Critical High Availability (HA) resiliency for a pair of Voice and Multimedia Contact Servers in a campus SIP-enabled contact center environment that uses an Avaya Aura® Communication Manager and an Avaya Aura® Session Manager.

In a Mission Critical campus High Availability solution, a CCMS or CCT critical service failure, or a CCMS, CCT or CCMM hardware, network, or database failure can initiate a switchover but only in the following situations:

- The active server is in the active mode.
- The active server is running. All the critical CCMS and CCT services are monitored and running.
- The active server has Enable Switchover enabled.
- The active and standby servers can communicate with the trusted server.
- The active server database and the standby server database are synchronized. The standby server database is shadowing the active server database, and is up-to-date.

If the Contact Center Administrator uses the Windows Service Control Manager (SCM) to stop a monitored service on an active server, a switchover occurs. If the Contact Center Administrator uses the System Control and Monitor Utility (SCMU) to stop a monitored service on an active server, a switchover does not occur.

High Availability Utility

Configure High Availability resiliency for CCMS and CCT using the High Availability (HA) utility in the Database Utilities. The High Availability utility is used to configure which server is the active server and which server is the standby server. The HA utility also configures the Managed IP of the active server.

SMMC system tray

The Contact Center System Management and Monitoring Component (SMMC) system tray gives quick access to action items in your High Availability environment. The SMMC system tray has the following main menu options and action items:

- Start HA System
- Stop HA System
- Disable Switchover
- Enable Switchover
- Launch SCMU
- System Information
- Database Information
- Disable Auto Startup

To access the SMMC system tray menu, right-click the SMMC icon on the Windows taskbar.

High Availability utility and SMMC system tray

To commission High Availability, use the High Availability utility to configure High Availability IP addresses and to configure which server is the active server and which server is the standby server. Then use the System Management and Monitoring Component (SMMC) system tray to start database shadowing and High Availability functionality.

Troubleshooting High Availability

To troubleshoot High Availability, use the System Management and Monitoring Component (SMMC) utility, Windows Events logs, and the System Control and Monitor Utility (SCMU) to diagnose High Availability issues. Then use the High Availability utility in to resolve the diagnosed issues.

Procedure steps

Step	Action
1	Log on to the active server.
2	On the Windows System Tray, right-click on the System Management and Monitoring Component (SMMC) system tray icon, and select **System Information**.
3	Examine the **System Information** dialog to determine the cause of High Availability related issues.

4 On the Windows System Tray, right-click on the System Management and Monitoring Component (SMMC) system tray icon, and select **Database Information**.

5 Examine the **Database Information** dialog to determine the cause of High Availability related issues.

6 Repeat these steps on the standby server.

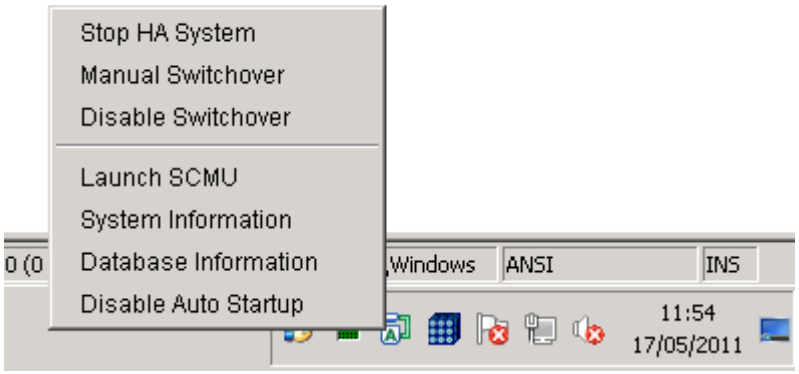
--End--

Procedure job aid

The following examples are from a functional High Availability pair of Voice and Multimedia Contact Servers.

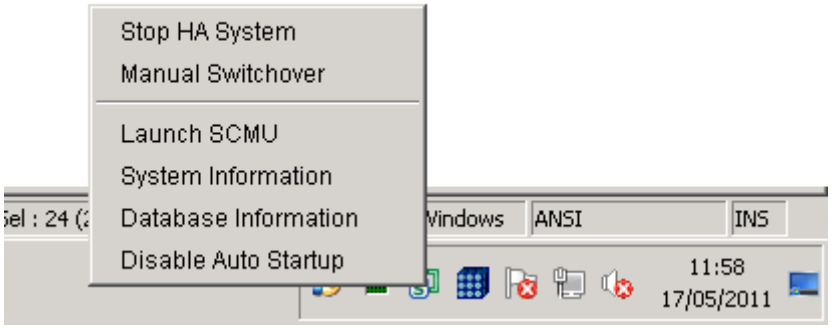
Use the System Management and Monitoring Component (SMMC) utility to diagnose High Availability issues. Use the High Availability (HA) Utility in the Database Utilities to resolve the diagnosed issues.

Example of using SMMC on a functional active server



In a High Availability solution, the SMMC system tray icon displays "A" to indicate that the server is configured as a High Availability active server. You can use SMMC on active server to perform a Manual Switchover to the standby server.

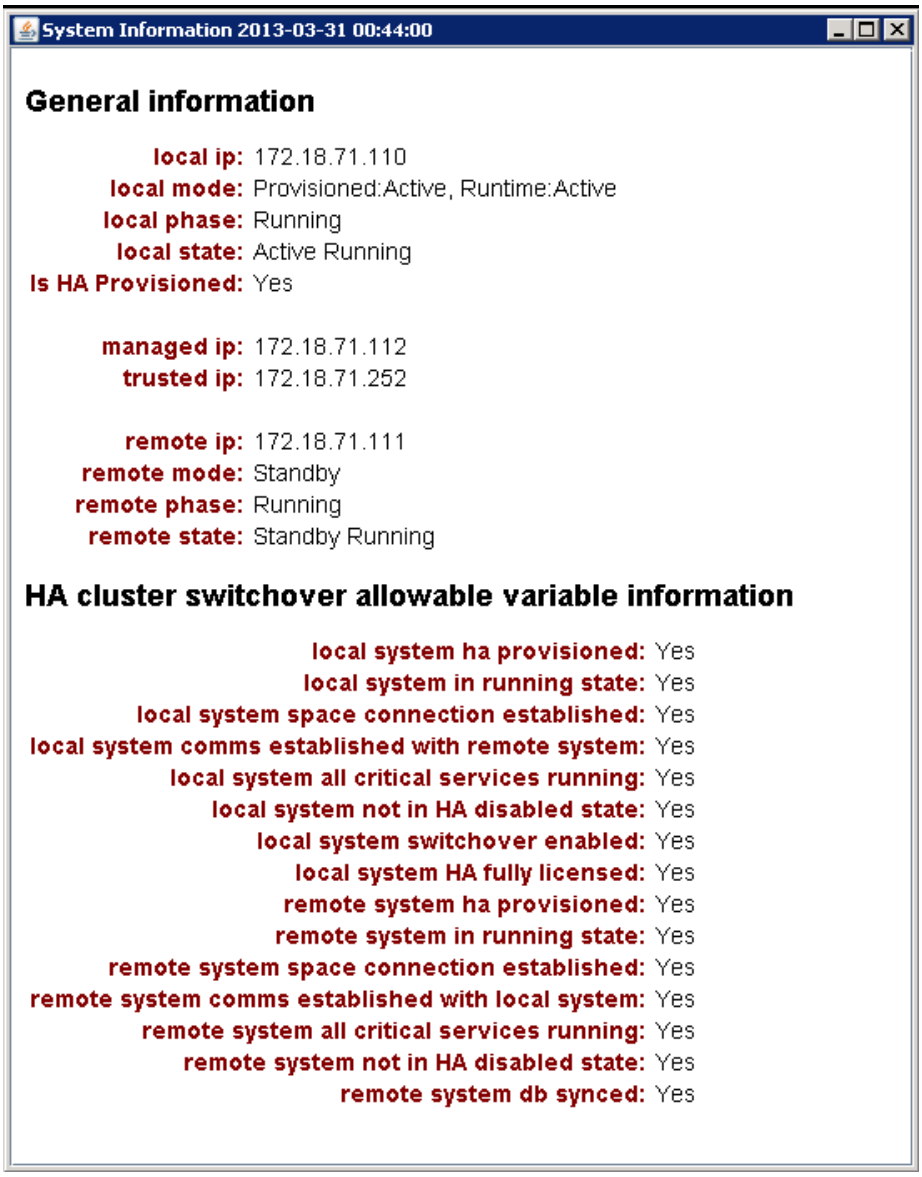
Example of using SMMC on a functional standby server



In a High Availability solution, the SMMC system tray icon displays "S" to indicate that the server is configured as a High Availability standby server. The standby server has different SMMC system tray menu options to the active server.

You can use SMMC system tray to display system and database information, and to diagnose High Availability related issues.

Example of a functional Mission Critical High Availability active server System Information dialog

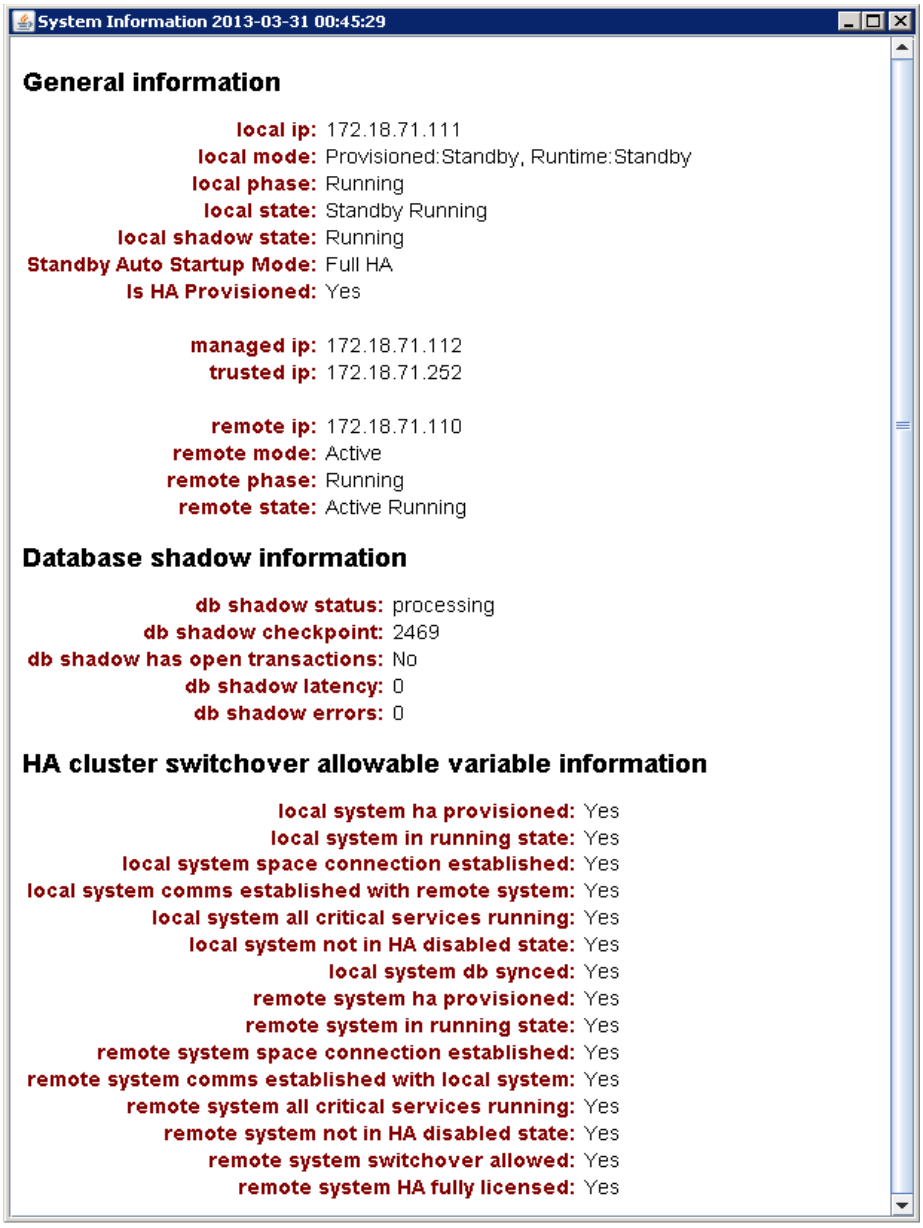


Examine the System Information dialogs on the active server and the standby server to ensure they mirror each other. The Trusted IP address and Managed IP address must be the same on both servers. Examine the "General Information" section to ensure that your High Availability solution is configured correctly, and to determine why High Availability last stopped. When in the Stopped state, the System Information dialog displays a "Local last known stop reason".

On the active server, examine "local system switchover enabled" to confirm that switchover is supported and enabled.

On the active server, examine "local system all critical services running" to confirm that all the necessary services are running. If any critical service is not running, use the System Control and Monitor Utility (SCMU) to investigate further.

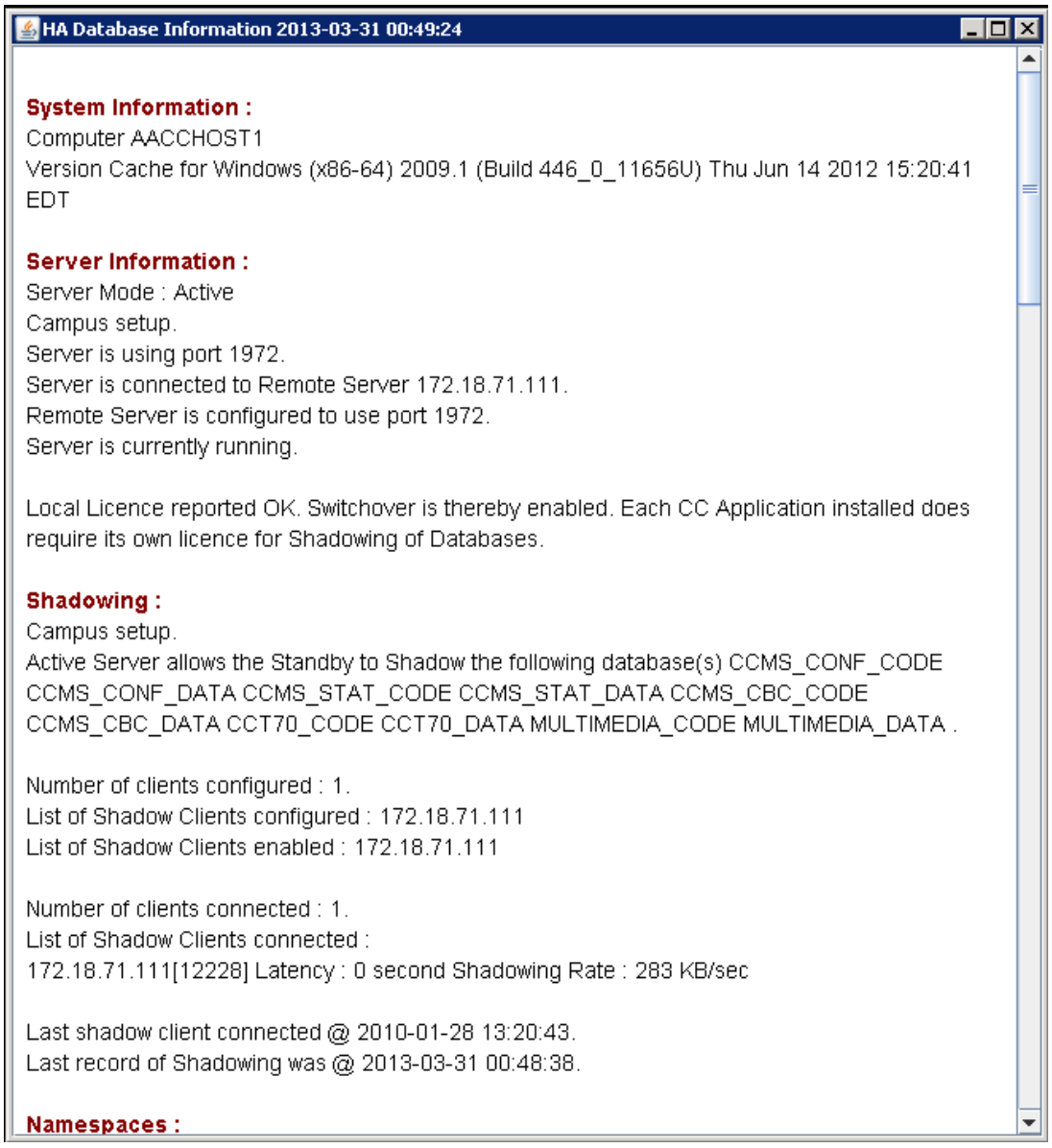
Example of a functional Mission Critical High Availability standby server System Information dialog



The standby server System Information dialog displays Database Shadowing information. Examine the "Database shadow information" section to determine if the network in your High Availability solution is causing shadowing issues.

Examine "local system comms established with remote system" to confirm that the SMMC on the standby server can communicate with the SMMC on the active server, and visa versa.

Example of a functional Mission Critical High Availability active server Database Information dialog



The Database Information dialog displays information about the database ports, namespaces, and the number of Shadow Clients connected to the High Availability server. On the active server a Shadow Client may also be a Remote Geographic Node server on a remote site, accessed using a Wide Area Network (WAN).

Troubleshooting when shadowing fails to start

You must backup the active server database, restore it onto the standby server, and enable shadowing within 24 hours. If the difference in time between the active and standby server database content is greater than 24 hours then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the active server database and restore it onto the standby server before re-enabling shadowing. Ensure that the system clock time on the active and standby servers are synchronized.

Procedure steps

Step	Action
1	Use the Database Maintenance utility to create a new backup of the active server database.
2	Use the Database Maintenance utility to restore the database to the standby server.
3	Re-commission High Availability on the standby server.
4	Use the High Availability utility to enable shadowing.

--End--

Troubleshooting when SMMC fails to start

The Contact Center System Management and Monitoring Component (SMMC) system tray provides quick access to action items in your High Availability environment.

To access the SMMC system tray menu, right-click the SMMC icon on the Windows taskbar. The SMMC system tray is a graphical interface for the underlying SMMC system. If the SMMC system fails or stops, the SMMC system tray may display a "No connection to SMMC" message. You can use the SMMC system tray menu to restart the SMMC system.

Procedure steps

Step	Action
1	Log on to the High Availability server.
2	On the Windows System Tray, right-click on the System Management and Monitoring Component (SMMC) system tray icon, and select **Start SMMC**.

--End--

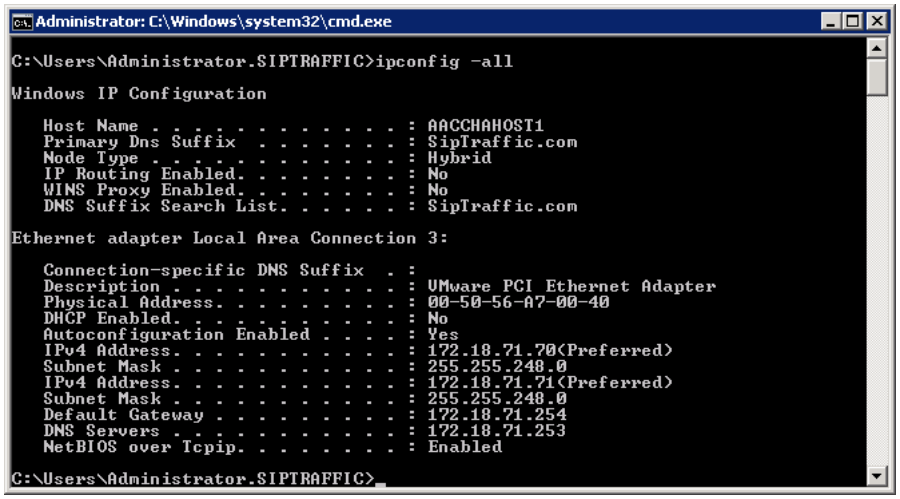
Troubleshooting Licensing issues

High Availability is a licensed feature. It is enabled when you purchase a standby server license.

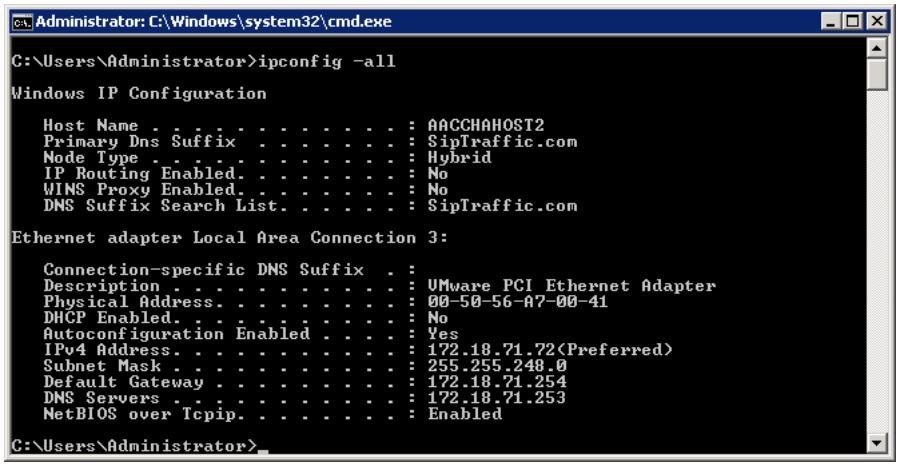
For campus High Availability, the license file is based on two MAC addresses, the MAC address of the active server and the MAC address of the standby server. The license file, containing the active and standby MAC addresses, is installed on both servers. If a switchover occurs, the standby server processes calls. The standby server has a High Availability license, and does not use the grace period mechanism.

Procedure steps

Step	Action
1	Log on to the active License Manager server.
2	Click **Start**, **Run**, and in the **Open** box, type **cmd**.
3	Enter **ipconfig -all**. *The IP Configuration details appear.*



4	Note the **Physical Address** identifier. For example, the MAC address of this active server is 00-50-56-a7-00-40.
5	Log on to the standby License Manager server.
6	Click **Start**, **Run**, and in the **Open** box, type **cmd**.
7	Enter **ipconfig -all**. *The IP Configuration details appear.*



8 Note the **Physical Address** identifier. For example, the Physical Address (MAC) address of this standby server is 00-50-56-a7-00-41.

9 Navigate to the folder containing the Avaya Aura® Contact Center license file.

10 Open the license file in Notepad.

11 Locate the **LM_STANDBYN** license key in the file. The **LM_STANDBYN** license key must appear twice in the license file, once for each High Availability server.

12 Confirm one instance of the **LM_STANDBYN** license key corresponds with the MAC address of the active server. For example;

xyz== # **LM_STANDBYN** 8.0 **00:50:56:a7:00:40** Identifier (1) 60 secs

13 Confirm the other instance of the **LM_STANDBYN** license key corresponds with the MAC address of the standby server. For example;

abc== # **LM_STANDBYN** 8.0 **00:50:56:a7:00:41** Identifier (1) 60 secs

14 If the MAC addresses in your license file do not match the MAC addresses of your servers, contact your Avaya technical support prime.

--End--

Troubleshooting when services fail to start

The active and standby servers use a Trusted IP address to verify network connectivity. If the active server cannot communicate with the standby server it attempts to communicate with the Trusted IP address.

Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.

Procedure steps

Step	Action
1	Verify the active and standby servers can communicate with the Trusted IP address.

--End--

Troubleshooting shadowing failures

Troubleshoot when the standby server does not shadow the active server. The standby set of Avaya Aura® Contact Center applications monitors and shadows the active applications in the system and does not process calls. The standby CCMS monitors the active CCMS. The standby CCT monitors the active CCT. The standby CCMM monitors the active CCMM. Each active and standby pair of applications forms a resilient or replication pair. If any of the active applications fail, the standby applications recognize the failure and start processing contacts.

Procedure steps

Step	Action
1	Verify that the standby server is installed exactly the same as the active server. The standby and active servers must have the exact same patch level and the same hard disk drive partitions.
2	Verify that the Cache service is running on the standby server.
3	Verify that you have installed a standby server license to enable High Availability.
4	Verify that the standby server can communicate with the active server by name and IP address.
5	Verify that you can ping the Managed IP address of the active server from the standby server and from a client computer.
6	Verify that the static IP address of the active and standby servers are configured correctly in the High Availability configuration utility.
7	Ensure that the standby server is configured exactly the same as the active server. Backup the active server database and restore this database onto the standby server.
8	If the contact center uses an Avaya Aura® Application Enablement Services and Avaya Aura® Session Manager, use the Contact Center System Management and Monitoring Component (SMMC) system tray System Information display to examine the status of the High Availability solution.
9	Verify that both the active and standby servers can ping the Trusted IP address.
10	Examine the Windows Event Viewer on the active and standby servers for High Availability, network, or Contact Center-related error messages.

--End--

Troubleshooting unnecessary switchovers

If you experience unnecessary or unexplained switchovers, consider increasing the High Availability Network Timeout value to match your network performance.

Procedure steps

Step	Action
1	For more information about tuning the High Availability feature to your solution, see High Availability Network Timeout optimization (page 37).

--End--

Troubleshooting switchover failure

Troubleshoot when the active server does not switchover to the standby server. Each active and standby pair of applications forms a resilient or replication pair. If any of the active applications fail, the standby applications recognize the failure and start processing contacts.

Attention: In a campus Voice and Multimedia Contact Server solution, a CCMS or CCT service failure, or a CCMS, CCT, or CCMM hardware, network, or database failure can initiate a switchover.

Procedure steps

Step	Action
1	Verify that the standby server can shadow the active server.
2	Verify that the switchover check box on both servers is selected.
3	Verify that the standby server is installed exactly the same as the active server. The standby and active servers must have the exact same patch level and the same hard disk drive partitions.
4	Verify that you have installed a standby server license to enable High Availability.
5	Verify that the standby server can communicate with the active server by name and IP address.
6	Verify that you can ping the Managed IP address of the active server from the standby server and from a client computer.

7 Verify that the static IP address of the active and standby servers are configured correctly in the High Availability configuration utility.

8 If the contact center uses an Avaya Aura® Application Enablement Services and Avaya Aura® Session Manager, use the Contact Center System Management and Monitoring Component (SMMC) system tray System Information display to examine the status of the High Availability solution.

9 Ensure that the standby server is configured exactly the same as the active server. Backup the active server database and restore this database onto the standby server.

10 Verify that both the active and standby servers can ping the Trusted IP address.

11 Examine the Windows Event Viewer on the active and standby servers for High Availability, network, or Contact Center related error messages.

--End--

Troubleshooting when network outages occur in a High Availability Contact Center

Troubleshoot when a Contact Center component or network link fails.

The High Availability-System Management and Monitoring Component (SMMC) monitors network communications, network latency, and contact center components. If the High Availability “Network Timeout” threshold value is not suitable for your network then outages may occur. You must configure the High Availability SMMC "Network Timeout" threshold value high enough to be tolerant of normal network latency, but low enough to be responsive if a network failure occurs. For more information on configuring the High Availability Network Timeout value, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210). You can determine what your current network threshold value is by performing the following steps.

Procedure steps

Step	Action
1	Log on to the High Availability server.
2	Retrieve the active server SMMC log files from Avaya\Logs\Common Components\SMMC\CC_SMMC_NM_x.log. X indicates a running numeric identifier between 1 and 9.
3	Copy the SMMC log files into the same folder as the Network Log Analyzer utility: D:\Avaya\Contact Center\Manager Server\CCSMMC\util
4	On the active server, open a command prompt and navigate to the folder that holds the Network Analyzer utility. • d: • cd \Avaya\Contact Center\Manager Server\CCSMMC\util

5 At the command prompt type:

NetworkLogAnalyser.exe CC_SMMC_NM_1.log CC_SMMC_NM_2.log...

6 The Network Log Analyzer utility processes the SMMC statistical network data in the log files and recommends a Network Timeout value. For example:

$> NetworkLogAnalyser.exe CC_SMMC_NM_1.log

....

....

===== OUTAGES PACKET DATA ANALYSIS END ====

Recommendation:

Network Timeout= 2x Max(Outage_Duration)= 2x 325ms = 650ms

While processing the statistical data, the Network Log Analyzer utility also produces a comma-separated file (network-analysis.csv) that can be imported in to Microsoft Excel using the "network-analysis.xlsm" spreadsheet.

7 Open the file 'network-analysis.xlsm' using Microsoft Excel and ensure that you have macros turned on. Follow the instructions given in the spreadsheet.

8 From the resulting chart and recommended Network Timeout value, determine what the suitable Network Timeout value for your network is and update it accordingly.

--End--

Troubleshooting contact issues that occur after a switchover

Troubleshoot when contacts that are in treatment during a High Availability switchover experience any of the following issues:

- calls are left stranded in a treatment after the switchover. They are never routed to an agent.
- calls that are in queue or in treatment (for example Music, IVR, Ringback), are disconnected soon after the switchover.
- email messages that were queuing at the time of the switchover are all disconnected. They are ultimately re-injected by CCMM and re-queued.

In all these cases, the root cause of the issue may be the programming in the Switchover Handling script.

You must configure the Switchover Handling script for the applications and skillsets in your contact center solution.

Procedure steps

Step	Action
1	Configure your Contact Center Orchestration Designer — Switchover Handling script. for more information about configuring the Switchover Handling script, see Configuring the Switchover Handling script (page 307).

--End--

Troubleshooting – Avaya Aura platform

Troubleshooting the Avaya Aura® Unified Communications platform must be done to address errors that occur when the Avaya Aura® Contact Center cannot control phone calls or route calls to agents.

Prerequisites for Avaya Aura platform troubleshooting

- Ensure that your servers, client computers, and network meet the minimum system requirements. For more information about hardware and network requirements, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
- Complete the Avaya Aura® Unified Communications platform pre-installation checklist. For more information about the checklist, see *Avaya Aura® Contact Center Installation Checklist* (NN44400-310).
- Complete the SIP-enabled Contact Center pre-installation checklist. For more information, see *Avaya Aura® Contact Center Installation Checklist* (NN44400-310).
- Ensure that you have installed Contact Center correctly. For more information about installing Contact Center, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- Read *Avaya Aura® Contact Center Commissioning* (NN44400-312).
- Read *Avaya Aura® Contact Center Configuration – Avaya Aura® Unified Communications Platform Integration* (NN44400-521).

Troubleshooting AES and CCMS communication issues

Log on to the Application Enablement Services (AES) server using Secure Shell (SSH) and confirm that AES is communicating with the Contact Center Manager Server (CCMS) on port 4723. Also confirm that there is an established connection between the AES and CCMS. The AES server uses port 4723 to listen to the TR87 SIP CTI link between AES and the CCMS.

Procedure steps

Step	Action
1	On the AES SSH console, enter **netstat -an | grep 4723** *The AES server console displays the network status of the AES.*
2	Confirm that the link to your Contact Center Manager Server is established.
3	Confirm that the Application Enablement Services server is listening on port 4723.

--End--

Procedure job aid

The following is an example of using the Application Enablement Services Secure Shell to check the connection to the Contact Center Manager Server.

[AES1admin@aes521svr01 ~]$ **netstat -an | grep 4723**
tcp 0 0 ::ffff:127.0.0.1:4723 :::* LISTEN
tcp 0 0 ::ffff:172.18.112.40:**4723** :::* **LISTEN**
tcp 0 0 ::ffff:172.18.112.40:4723 :ffff:172.18.71.110:65235 **ESTABLISHED**

In this example the AES IP address is 172.18.112.40 and the CCMS IP address 172.18.71.110. The AES server (172.18.112.40) is listening on port 4723. There is an ESTABLISHED link between the AES server (172.18.112.40) and CCMS (172.18.71.110).

Troubleshooting Communication Manager stations

To ensure proper integration and Contact Center control, Avaya Aura® Communication Manager stations (phones) must be configured as follows:

- A maximum of 2 Call Appearance lines per agent station
- Restrict Last Appearance must be enabled on all agent stations
- Call Forwarding is not supported on agent stations
- Priority call feature is not support on agent stations

Perform the following checks on each Communication Manager station to be controlled by Contact Center and used as an agent phone.

Procedure steps

Step	Action
1	Verify that each Communication Manager station has button number one configured for Call Appearance, for example; **BUTTON ASSIGNMENTS 1: call-appr**.
2	Verify that each Communication Manager station has button number two configured for Call Appearance, for example; **BUTTON ASSIGNMENTS 2: call-appr**.
3	Verify that Call Appearance is not set on the remaining buttons. Two Call Appearance buttons are supported. Disable Call Appearance on the other buttons.
4	Verify **Restrict Last Appearance** is enabled on all agent stations, for example; **Restrict Last Appearance? y**.
5	Verify IP Softphone is enabled on all agent stations, for example; **IP SoftPhone? y**.

--End--

Troubleshooting treatments when dialing the Contact Center Route Point Address

Add the Contact Center Manager Server to the list of trusted hosts on the Avaya Aura® Session Manager server. Add a Contact Center Manager Server (CCMS) routing entry to the Session Manager server. This indicates to Session Manager which host (SIP endpoint) to send calls to, based on the dialed number. Add contact details for the CCMS routing entry. This configures the Session Manager server to send calls to the CCMS when the calls match the map.

If you dial the Contact Center Route Point Address (RPA) and do not receive any treatments, perform the following checks.

Procedure steps

Step	Action
1	Verify that the Contact Center Manager Server is a trusted host of the Session Manager server.
2	Verify that the Session Manager server has a routing entry to the Contact Center Manager Server.
3	Verify that the Session Manager server has contact details for the Contact Center Manager Server routing entry.

--End--

Troubleshooting routing calls from Contact Center to agents on Communication Manager

If you cannot route calls from the Contact Center to agents on the Avaya Aura® Communication Manager, perform the following checks.

On the Session Manager server, add a route entry to the Communication Manager. The Session Manager re-directs SIP contacts that match the route entry pattern to the Communication Manager.

Add the Contact Center Manager Server to the list of trusted hosts on the Session Manager server. Session Manager does not authenticate SIP requests from trusted hosts.

Procedure steps

Step	Action
1	Verify that there is a routing entry from the Session Manager to the Communication Manager.
2	Verify that the Contact Center Manager Server is a trusted host of the Session Manager server.

--End--

Troubleshooting when agents cannot log on to Agent Desktop

If agents cannot log onto Avaya Aura® Agent Desktop, perform the following checks.

Procedure steps

Step	Action
1	Verify that TR87 is enabled on the Avaya Aura® Application Enablement Services (AES) server.
2	Verify that you imported certificates into the AES server.
3	Ensure that the Contact Center Manager Server is a trusted host on the AES server.
4	Ensure network connectivity is configured between the Avaya Aura® Unified Communications platform, CCMS, and Agent Desktop computers in the network and that all computers can ping each other.
5	Ensure that all Avaya Aura® Unified Communications platform and Contact Center servers can communicate with each other by host name, Fully Qualified Domain Name (FQDN), and IP address. Ensure that they can ping each other.

--End--