Avaya Aura® Contact Center

Multimedia Complement to Call Center Elite–Deployment Guide

Document status: Standard
Document issue: 01.01
Document date: 06 April 2012
Product release: Release 6.2
Job function: Installation
Type: Technical Publication
Language type: English

Copyright © 2012 Avaya Inc.
All Rights Reserved.

Notices
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
Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree 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 Web sites referenced within this site or documentation(s) 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 this product. 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 Web site: http://www.avaya.com/support
Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

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, AND 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").

Copyright
Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) 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. 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
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks
The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents
For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support

Contact Avaya Support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

Introduction **9**
Overview 9
Unified Agent Desktop 11
How to use this book 11
System Overview 12
Overview of the components in the example solution without High Availability 12
Contact Center configuration without High Availability 13
Call Center Elite configuration without High Availability 14
Overview of the components in the example solution with High Availability 14
Contact Center configuration with High Availability 15
Call Center Elite configuration with High Availability 16
Overview of the e-mail contact workflow 16
Configuration data worksheets 17
Windows server preparation 18
Contact Center server software installation 19
Post-install Contact Center Server Commissioning 19
Contact Center Manager Server configuration 20
Contact Center Multimedia configuration 21
Preparing the Windows Domain for the Call Center Elite Integration with Contact Center 23
Configuring Contact Center to Integrate with Call Center Elite 23
Supervisor and Agent Configuration 24
Agent Desktop client software installation 25
Testing contacts using Agent Desktop 26
High Availability pre-install configuration 26
Windows server preparation—Standby server 27
Standby Contact Center server software installation 28
Standby Server Post-install Commissioning 29
High Availability server commissioning 30
Agent Desktop client software installation for High Availability 31
Testing High Availability 32
Recovering High Availability 32

Contact Center Server Installation Section **35**
Windows server preparation **37**
Installing Windows Server 2008 Release 2 37
Configuring Windows Server 2008 43
Installing the latest operating system service packs 44
Disabling the Remote Access services 45
Configuring SNMP on your server 47
Creating an account for installing and maintaining Contact Center 48
Downloading the most recent Contact Center patches to the server 57

Disabling Internet Protocol version 6 57
Disabling unused Network Adapters 59
Enabling Microsoft Remote Desktop connection 60
Configuring Data Execution Prevention 61
Importing the Contact Center Firewall Security policy 62
Contact Center server software installation 65
Installing operating system components for Contact Center Manager Administration 65
Configuring MIME types to support Microsoft updates 73
Installing the server software on the co-resident server 78
Disabling Java Runtime Environment updates on the co-resident server 93
Post-install Contact Center Server Commissioning 95
Applying Post-installation Patches 95
Confirming that the Contact Center services start 99
Scheduling Weekly Disk Defragmentation 105
Configuring the Multicast controller 107
Configuring Real-Time Reporting 110
Configuring Internet Explorer on the Contact Center server 113
Verifying the Web Services 115
Changing the default sysadmin password 116
Logging on to Contact Center Manager Administration for the first time 119
Adding the CCT Server in CCMA 122
Adding the CCMM Server in CCMA 124
Installing the Orchestration Designer client 128
Providing local users with the Log on as a service right 130
Verifying the Multimedia database installation 131
Verifying that Contact Center Multimedia services start 132
Logging on to the Multimedia Administration tool for the first time 134
Verifying and configuring server settings in the CCMM Administration client 135
Verifying the multimedia license type 140

Configuration Section 143
Contact Center Manager Server configuration 145
Configuring Contact Center Manager Server Global Settings 145
Adding a route point for e-mail skillsets 146
Creating a skillset threshold class 149
Configuring activity codes 152
Creating a call presentation class 155
Adding the e-mail skillset 156
Contact Center Multimedia configuration 161
Configuring the multimedia skillsets 161
Adding administrators 164
Checking the status of the multimedia configuration 165
Configuring office hours 166

Creating a keyword group 172
Creating a Rule Group and a Rule 177
Configuring the Inbound e-mail recipient address 187
Configuring the Outbound e-mail recipient address 194
Configuring the outbound e-mail settings 197
Configuring the e-mail general settings 201
Checking the status of the Multimedia e-mail configuration 202
Configuring MIME types to support e-mail attachments 203
Preparing the Windows Domain for the Call Center Elite Integration with Contact Center 209
Creating Domain users and groups for agents 209
Assigning a group policy for embedded softphone settings 212
Configuring Contact Center to Integrate with Call Center Elite 219
Checking the Elite agent and station settings 219
Configuring the default template with Reason Codes 225
Adding an agent template 230
Supervisor and Agent Configuration 239
Adding a supervisor 239
Adding an agent 244
Adding an agent profile 255

Client Installation Section 263
Agent Desktop client software installation 265
Modifying the agent settings in CCMM Administration client 265
Installing the Agent Desktop client software 269
Agent Desktop installation troubleshooting 285
Troubleshooting a Windows Security Alert when you install Agent Desktop 285
Troubleshooting an Existing Login Detected warning 286
Troubleshooting an Elite Agent Logout error 287
Testing contacts using Agent Desktop 289
Logging on to Agent Desktop 289
Opening the Multimedia Dashboard 295
Sending a test e-mail to the Contact Center e-mail inbox 296
Making the agent Ready and accepting the e-mail contact 298
Replying to and closing the e-mail contact 301
Testing a Call Center Elite voice call by answering it on Agent Desktop 305
Accepting a Multimedia Contact while on the voice call 306
Making the agent not ready 308

High Availability Section 311
High Availability pre-install configuration 313
Adding High Availability to a CCMM Complement solution 313
Overview of the components in the example solution with High Availability 313

Contact Center configuration with High Availability 314
Call Center Elite configuration with High Availability 315
CCMA Replication 315
Active Directory - Lightweight Directory Services data store 316
Domain environments 317
Licensing for High Availability 317
Adding the domain AD-LDS replication account to the Active server administrators and replicator group 319
Updating the license file on the Active server 332
Updating the site name on the Active server 336
336
Windows server preparation—Standby server 339
Installing Windows Server 2008 Release 2 339
Configuring Windows Server 2008 345
Installing the latest operating system service packs 346
Disabling the Remote Access services 347
Configuring SNMP on your server 349
Configuring the server to use the Contact Center installer account 350
Downloading the most recent Contact Center patches to the server 359
Disabling Internet Protocol version 6 359
Disabling unused Network Adapters 361
Enabling Microsoft Remote Desktop connection 362
Configuring Data Execution Prevention 363
Importing the Contact Center Firewall Security policy 364
Adding the domain AD-LDS replication account to the Standby server administrators and replicator group 366
Standby Contact Center server software installation 381
Installing operating system components for Contact Center Manager Administration 381
Configuring MIME types to support Microsoft updates 389
Installing the Contact Center server software on the Standby server 394
Disabling Java Runtime Environment updates on the co-resident server 420
Standby Server Post-install Commissioning 423
Applying Post-installation Patches 423
Confirming that the Contact Center services start 424
Troubleshooting if the LM and CCMS services do not start on the Standby server 430
Scheduling Weekly Disk Defragmentation 433
Configuring the Multicast controller 435
Configuring Real-Time Reporting 438
Configuring Internet Explorer on the Contact Center server 440
Verifying the Web Services 443
Changing the default sysadmin password 444
Providing local users with the Log on as a service right 447
Verifying the Multimedia database installation 448
Verifying that Contact Center Multimedia services start 449

Configuring MIME types to support e-mail attachments 451
High Availability server commissioning 457
Installing the latest Contact Center software patches on the Active server 459
Installing the latest Contact Center software patches on the Standby server 462
Resolving the Managed name to the Managed IP Address 464
Installing a third-party utility to support High Availability on the Active server 465
Installing a third-party utility to support High Availability on the Standby server 468
Verifying services are ready for High Availability on the active server 471
Verifying services are ready for High Availability on the standby server 473
Configuring High Availability on the Active Server 474
Configuring E-mail notification on the Active Server 476
Configuring service monitoring on the Active Server 478
Backing up the Contact Center Manager Administration component on the Active server 481
Backing up the Contact Center databases on the Active Server 486
Restoring the Contact Center databases on the Standby Server 491
Creating a drive mapping to the network backup location from the Standby server 500
Restoring CCMA data to the Standby server 503
Verifying the server details and restarting the Standby Server 507
Configuring High Availability on the Standby Server 508
Checking the server configuration on the Standby Server 511
Starting High Availability on the Active Server 513
Starting High Availability on the Standby Server 518
Verifying shadowing is running on the Active Server 523
Changing server details in Contact Center Manager Administration 527
Updating server names in CCMM Dashboard 533
Using the Contact Center Manager Administration server Managed name 537
Configuring CCMM General Administration 540
Configuring e-mail attachment file locations 545
Agent Desktop client software installation for High Availability 547
Uninstalling Agent Desktop 547
Installing the Agent Desktop client software using the HA Managed name 550

Testing and Troubleshooting High Availability Section 559
Testing High Availability 561
Logging on to Agent Desktop using the HA Managed name 561
Sending a test e-mail to the Contact Center e-mail inbox 562
Making the agent Ready and accepting the e-mail contact 562
Checking the e-mail contact status in Multimedia Dashboard 564
Reviewing the Active server status before switchover 565
Reviewing the Standby server status before switchover 566
Forcing a switchover and monitoring the results 567
Closing Agent Desktop 571
Checking the e-mail contact status in Multimedia Dashboard after the switchover 574

Logging on the agent and resuming processing of contacts 575

High Availability and Switchover Troubleshooting 577

Cannot start the HA utility on a server that has had a failure 577

A Multimedia contact that was active before a switchover does not offer to an agent after switchover 579

A switchover does not occur on the Standby server when the Active fails 581

Recovering High Availability 583

Fixing the cause of the failure on the Active server 583

Backing up the Contact Center Manager Administration component on the Standby server 583

Backing up the Contact Center databases on the Standby Server 587

Restoring the Contact Center databases on the Active Server 590

Creating a drive mapping to the network backup location from the Active server 597

Restoring CCMA data to the Active server 600

Verifying the server details and restarting the Active server 604

Verifying that the Active server is running in standby mode and shadowing data 606

Introduction

This guide provides a complete set of procedures to implement an installation of the Avaya Aura® Contact Center (CC) Multimedia Complement to support an existing Avaya Aura® Call Center Elite voice contact center.

Adding Avaya Aura® CC multimedia capabilities to an Avaya Aura® Call Center Elite contact center increases the number of communication channels with customers, offers flexibility, and is cost-effective.

Overview

Avaya Aura® CC Release 6.2 supports integration with Avaya Aura® Call Center Elite. In such a solution Avaya Aura® CC offers a Multimedia Complement to an Avaya Aura® Call Center Elite voice-based contact center. The contact center processes voice calls through Call Center Elite, and processes multimedia contacts through Avaya Aura® CC. The contact center agents use a single desktop application to answer and manage both their calls and their multimedia contacts.

Avaya Aura® CC supports the following multimedia contact types:

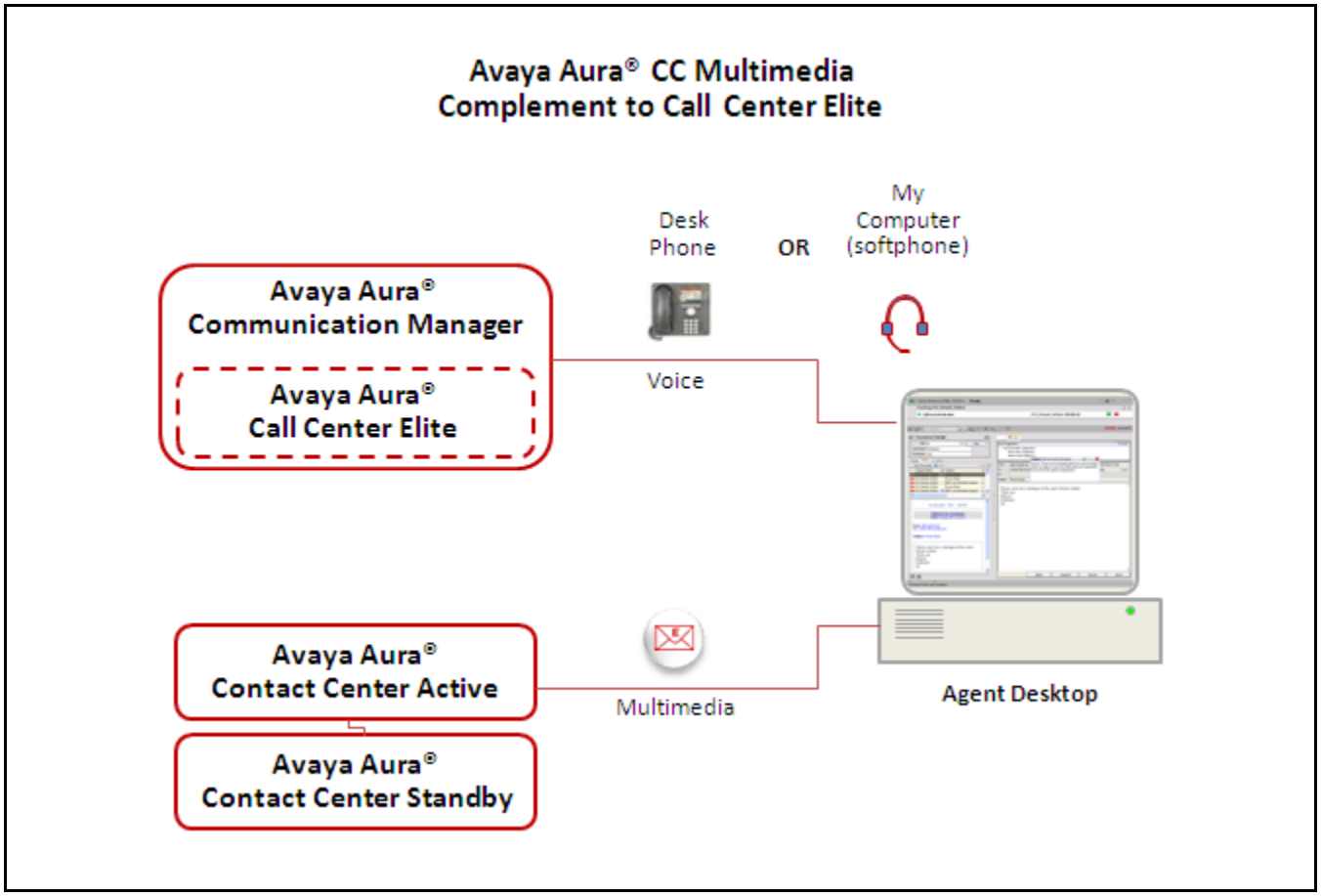
- E-mail
- SMS text messages
- Fax messages
- Scanned documents
- Voice mail messages
- Web Communications

A combined Avaya Aura® CC and Avaya Aura® Call Center Elite contact center solution provides:

- a unified agent desktop
- unified reporting and performance management, with the optional Avaya IQ product
- unified agent administration, with the optional Avaya Contact Center Control Manager product

You can install Avaya Aura® CC to add multimedia-enabled capabilities to new or existing Avaya Aura® Call Center Elite contact center solutions.

Example of a Call Center Elite and Contact Center integrated solution



Adding Avaya Aura® CC multimedia capabilities to a Call Center Elite contact center initially requires a single additional server, plus some additional backoffice infrastructure to handle, for example, e-mail based multimedia contacts and Web communications. Adding Avaya Aura® CC multimedia capabilities to a Call Center Elite call center does not impact the Call Center Elite voice call processing. Adding a second Contact Center server, configured as a Standby server, provides High Availability (HA). High Availability provides redundancy and resiliency in case of a failure on the Active Contact Center server.

The following table shows the supported Avaya Aura® Communication Manager–Call Center Elite system versions.

Platform	Supported Releases	Concurrent voice agents	Concurrent multimedia agents
Avaya Aura® Call Center Elite	3.x, 4, 5.x, 6.x	Per Avaya Aura® Call Center Elite on Avaya Aura® Communication Manager release limit	3000

An Avaya Aura® Call Center Elite and Avaya Aura® CC solution does not support the following:

- Instant Message (IM) contact type
- Outbound (OB) contact type
- Open Queue (not supported for voice)
- Video

A Call Center Elite and Contact Center solution enables enterprises to deliver a rich customer experience across many forms of contact and social media. The contact center solution communicates with customers using the customer's choice of media. Existing voice customers are maintained and continue to receive the familiar and personal phone experience. Existing and new customers can choose voice, e-mail, and web communication channels. Multimedia-aware customers can choose a communication media that suits their business needs or lifestyle, and experience the modern interactive and responsive service to which they are accustomed.

Unified Agent Desktop

In a combined Avaya Aura® Call Center Elite and Avaya Aura® CC solution, agents can process only voice contacts, only multimedia contacts, or both. However, all agents can use Avaya Aura® Agent Desktop to answer and manage their voice calls and multimedia contacts.

Avaya Aura® Agent Desktop provides a single unified agent client-side software application that supports all contact types including voice, e-mail, SMS text messages, fax messages, scanned document messages, voice mail messages and Web communications.

How to use this book

This book uses a sample solution to describe how to configure Avaya Aura® CC to support basic voice and e-mail contact types. It covers only the concepts and procedures required to install and configure a sample Contact Center Multimedia Complement to Call Center Elite on the Avaya Aura® Unified Communications platform. The examples in this document are specific to this sample solution.

This document 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

complete Avaya Aura® CC documentation on www.avaya.com/support. This guide assumes that you follow the procedures in sequence. If you skip procedures or choose to follow a different sequence, then it is likely that the detail of the procedure steps and sample screenshots in this guide will not match your installation.

The sample solution in this guide uses a PLIC license file, generated using the Media Access Control (MAC) address of the Contact Center server. If you have a WebLM .xml file, your system requires extra installation steps. For more information on installing Contact Center with a WebLM .xml file, see *Avaya Aura® Contact Center Installation* (NN44400-311).

Depending on the Windows Server versions in your solution, the steps in some documented Windows procedures can differ in detail from your system.

The diagrams and screenshots in the book use sample configuration values, and the procedures suggest these values whenever a step requires them. You can use the worksheets in this chapter to record the configuration values for your solution next to the sample values. When a procedure step suggests a sample value, you can substitute your solution value.

System Overview

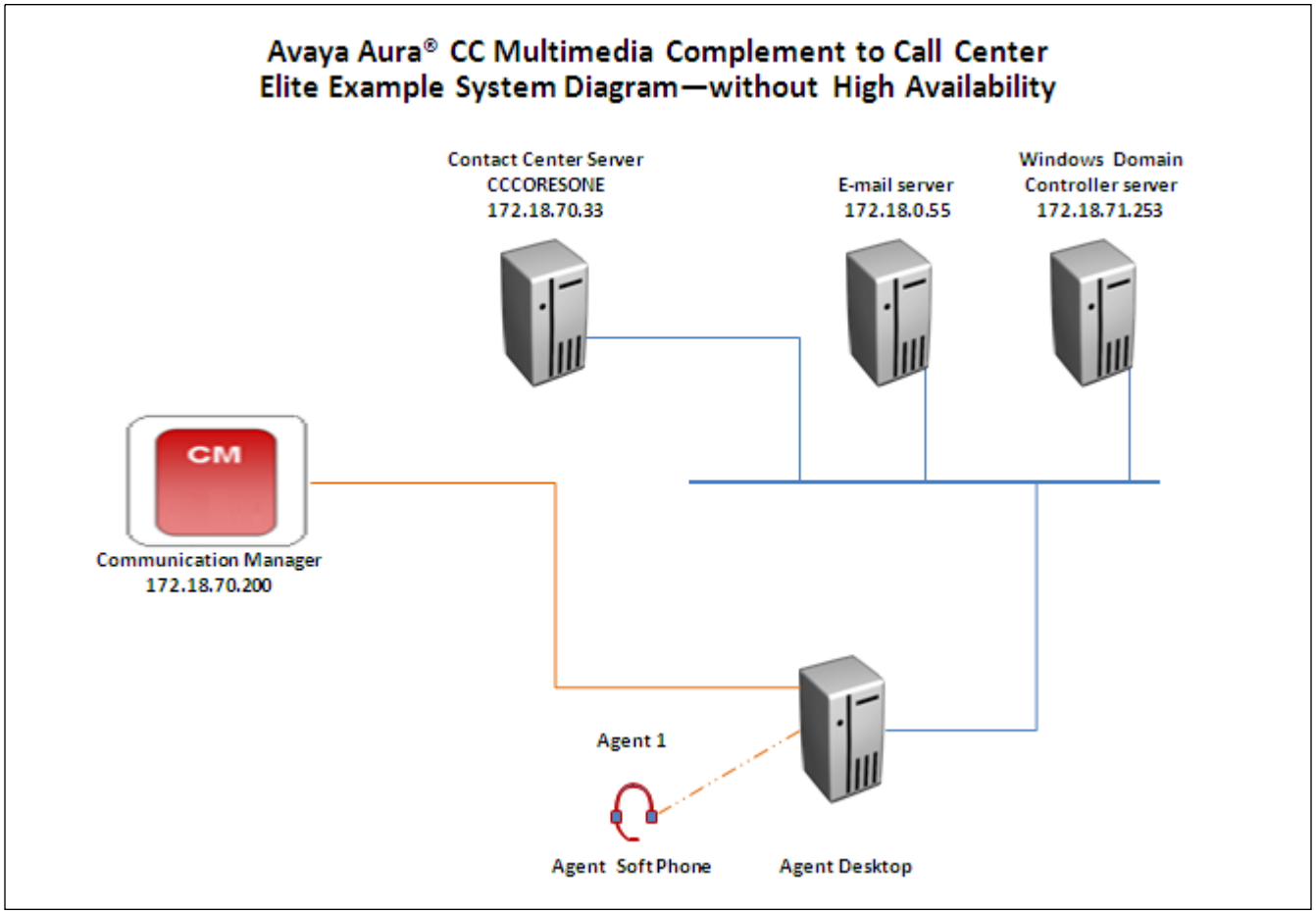
The following topics outline the example systems that this book describes. The first four sections of this Deployment Guide detail how to install a CCMM Complement to Call Center Elite without High Availability. The final two sections detail how to add High Availability to the example system

Overview of the components in the example solution without High Availability

In the example solution described in this Deployment Guide, the contact center is based on an existing Call Center Elite voice call center. The Avaya Aura® CC Multimedia Complement, when installed, provides contact center agents with the ability to answer e-mail contacts from Avaya Aura® CC as well as voice contacts from Call Center Elite.

It is also possible to add any other supported Multimedia type, but this guide covers only the e-mail contact type. For instructions on configuring other multimedia contact types, see *Avaya Aura® Contact Center Server Administration* (NN44400-610).

Contact Center Multimedia Complement without HA system diagram



Contact Center configuration without High Availability

The Contact Center server, CCCORESONE, has a specification to support the core assignment, management, licensing, CTI, and Multimedia software applications, as follows:

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

Call Center Elite configuration without High Availability

The existing Call Center Elite voice call center is fully operational and already has the full configuration for handling voice calls. It is licensed to support both desktop stations and soft phones.

Overview of the components in the example solution with High Availability

To add HA to the example solution described in this Deployment Guide, an additional server is required.

This solution supports Contact Center High Availability, implementing a Standby server to give resiliency for the Contact Center server. The Standby Contact Center server monitors and shadows the Active Contact Center server but does not process contacts. If the Active server fails, the Standby server recognizes the failure. It initiates a switchover, changes to active mode, and starts processing multimedia contacts.

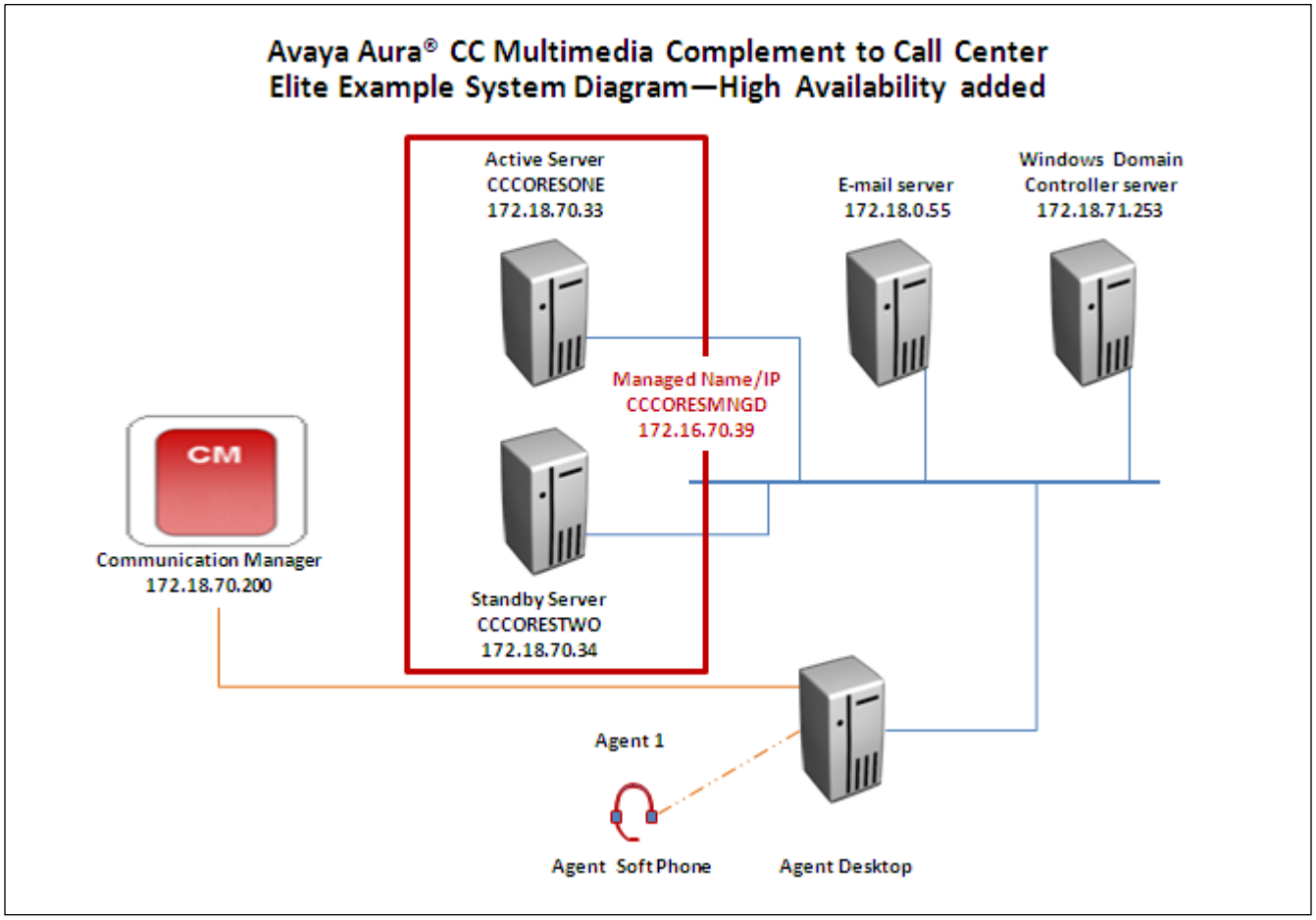
A Multimedia Complement to Call Center Elite allows for Warm Standby High Availability. In a Warm Standby HA solution, when the Standby server initiates a switchover, all agents must log off Agent Desktop, and log back in again. Contact Center re-queues all in-progress Multimedia contacts so that they become available to agents when they log back in. For more information on Warm Standby High Availability, and other types of High Availability available in different solutions, see the High Availability chapter in *Avaya Aura® Contact Center Fundamentals* (NN44400-110).

The Active and Standby servers are part of the same Contact Center, and they must be in the same IP subnet for campus High Availability resiliency to work.

This guide uses the term Active server for the original server, and Standby server for the additional server. When a server is processing contacts it is in active mode, and when it is monitoring and shadowing, it is in standby mode. Thus, after a switchover, the Standby server is in active mode.

When the Active server failure is corrected, the Active server can start in standby mode and monitor and shadow the Standby server.

Contact Center Multimedia Complement with High Availability system diagram



Contact Center configuration with High Availability

High Availability requires an additional Contact Center server, CCCORESTWO, configured to exactly match the original Contact Center server. The Standby server has the same applications as the Active server, as follows:

- Contact Center Manager Server
- Contact Center Manager Administration
- Communication Control Toolkit
- Contact Center Multimedia
- Contact Center License Manager
- Orchestration Designer
- Contact Center Manager Server Utility

High Availability also requires an additional IP address and virtual computer name, termed the Managed IP address and the Managed Name. In this example the Managed IP address is 172.18.70.39, and the Managed Name is CCCORESMNGD. All applications connecting to a High Availability Contact Center connect using the Managed IP address or the Managed Name. The server that is in active mode communicates with all other network hosts using the Managed IP address and Managed Name.

You complete the initial configuration of the Standby server using the server's unique name and IP address, CCCORESTWO and 172.18.70.34 respectively. You configure the Managed IP address and the Managed Name when you commission HA.

Call Center Elite configuration with High Availability

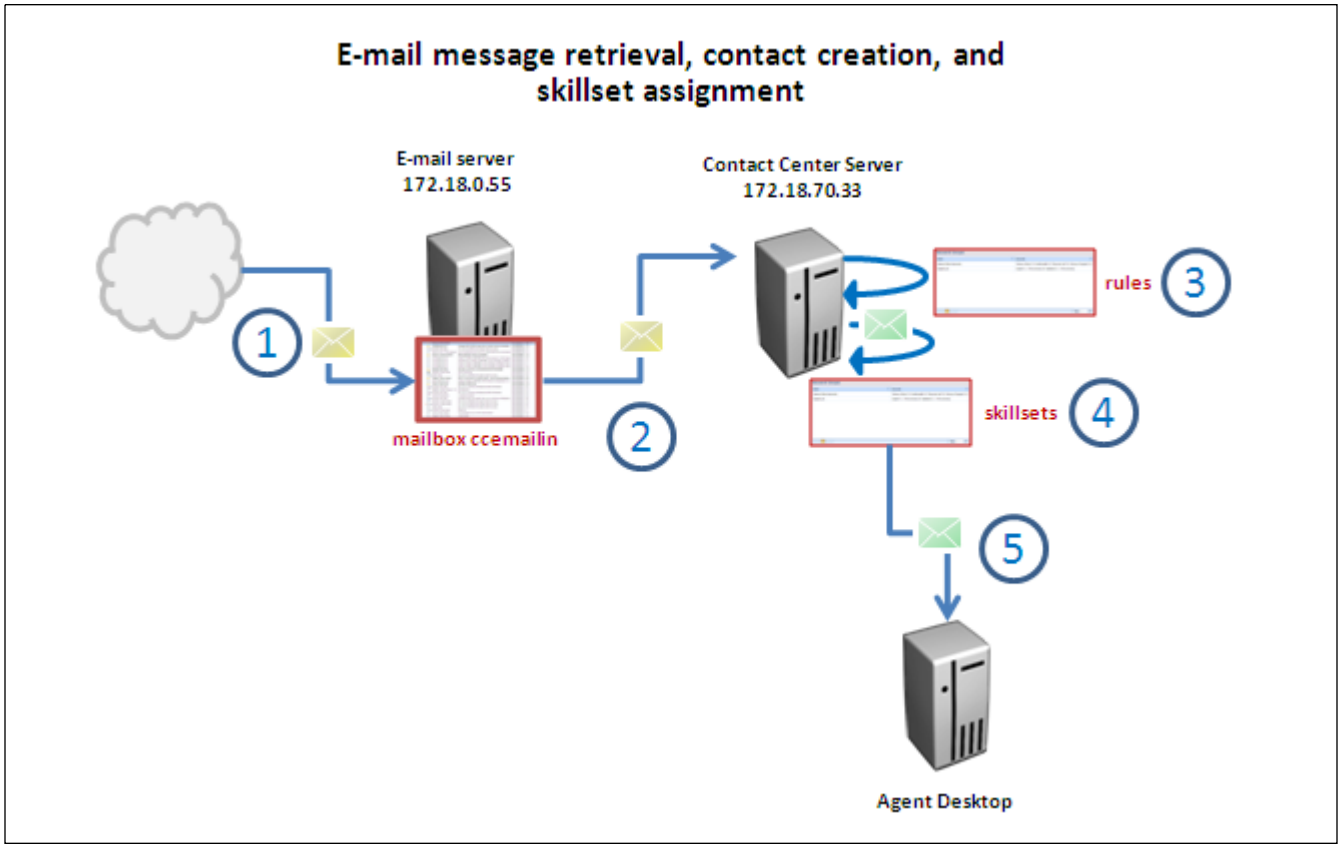
The Contact Center HA configuration does not affect the Call Center Elite configuration. The scope of the Contact Center HA feature includes only the Contact Center servers.

Overview of the e-mail contact workflow

In the solution described in this Deployment Guide, Contact Center monitors a specific e-mail address, from which it retrieves e-mail messages from customers. Contact Center checks the e-mail message content for specific keywords, and assigns the contacts to agents based on whether it finds the keywords or not.

In the example solution, the mailbox that Contact Center monitors is ccemailin, on a POP3 mailserver with an IP address 172.18.0.55. When Contact Center retrieves messages from the ccemailin, it searches them for the keywords "support" and "assistance". If the e-mail message includes either or both of these words, Contact Center creates the e-mail contact and assigns it to the EM_EM_Support skillset. If the e-mail message does not include either or of these words, it matches the System Default Rule. Contact Center creates the e-mail contact and assigns it to the default e-mail skillset, EM_Default_Skillset.

Contact Center Multimedia Complement e-mail retrieval, contact creation, and assignment



1. A customer sends an e-mail message to the ccemailin mailbox.
2. Contact Center retrieves the message from ccemailin.
3. Contact Center checks the e-mail contents for keywords that match the rules, for example "support" and "assistance".
4. Contact Center creates an e-mail contact and, based on the rule it matched, assigns it to a skillset, for example EM_EM_Skillset.
5. Contact Center assigns the e-mail contact to an available agent on that skillset.

Configuration data worksheets

The following pages provide all the data that the installer needs to enter during installation and configuration. The tables allow you to enter matching values for your own system: you can use these to map the correct values to enter in your own system if you use this manual to complete an installation.

Windows server preparation

The following table lists all the values that the installer needs to enter when installing the Contact Center servers in Windows server preparation (page 37).

Windows server preparation values

Configuration item	Worked example value	Equivalent value for your system
Contact Center server operating system drive size	61440 Mb	
Contact Center server operating system local administrator username	Administrator	
Contact Center server operating system local administrator password	MultiMpassw1	
Contact Center server IP address	172.18.70.33	
Local Area Network Mask	255.255.248.0	
Local Area Network Gateway	172.18.71.254	
DNS server IP address	172.18.71.253	
Contact Center server name	CCCORESONE	
domain name	siptraffic.com	
Domain administrator username	Administrator	
Domain administrator password	DomPass1	
Application drive letter and size	D:, 80Gb	
CCMS database drive letter and size	F:, 60Gb	
CCMM database drive letter and size	G:, 300Gb	
CCT database drive letter and size	H:, 5Gb	
Trace logs drive letter and size	I:, 5Gb	
Avaya Aura® CC installer domain username	AACCinstaller	
(1 of 2)		

Windows server preparation values

Configuration item	Worked example value	Equivalent value for your system
Avaya Aura® CC installer domain password	AACCInstPass1	
Support download location	C:\Avaya_Support\	
(2 of 2)		

Contact Center server software installation

The following table lists all the values that the installer needs to enter when installing the Contact Center server in Contact Center server software installation (page 65).

Contact Center server installation values

Configuration item	Worked example value	Equivalent value for your system
Contact Center operating system local administrator username	Administrator	
Contact Center operating system local administrator password	MultiMpassw1	
Avaya Aura® CC installer domain username	AACCinstaller	
Contact Center server name	CCCORESONE	
Support download location	C:\Avaya_Support\	
Customer Name	Sample Customer	
Company Name	Sample Company	
Site Name	CC_ELITESITE	
Contact Center server IP address	172.18.70.33	
CCMA service account (ICEAdmin) password	ICEpassw1	
POP3 mail server IP address (incoming e-mail messages)	172.18.0.55	
SMTP mail server IP address (outgoing e-mail messages)	172.18.0.55	

Post-install Contact Center Server Commissioning

The following table lists all the values that the installer needs to enter when installing the Contact Center servers in Post-install Contact Center Server Commissioning (page 95).

Contact Center server installation values

Configuration item	Worked example value	Equivalent value for your system
Support download location	C:\Avaya_Support\	
Off peak day for running disk defragmentation	Saturday	
Off peak hour for running disk defragmentation	01:00	
Real Time Display (RTD) Multicast address	204.5.6.10	
CCMA RTD incoming Multicast address	234.5.6.10	
Contact Center server name	CCCORESONE	
Contact Center sysadmin new password	sample1	
CCMA Administrator new password	nimdabew	
Contact Center server display name (for CCMA)	MM_Elite_CC_Single_Server	
CCT server display name (for CCMA)	cccoresone	
CCMM server display name (for CCMA)	CCElite_CCMM	
Inbound POP3 mail server IP address	172.18.0.55	
Outbound SMTP mail server IP address	172.18.0.55	
Web Statistics server IP address	172.18.70.33	

Contact Center Manager Server configuration

The following table lists all the values that the installer needs to enter when configuring the Contact Center Manager Server in Contact Center Manager Server configuration (page 145).

Contact Center server configuration sample values

Configuration item	Worked example value	Equivalent value for your system
Contact Center server display name (for CCMA)	MM_Elite_CC_Single_Server	
Route point for multimedia contacts	E-mailsContactsRP	
Threshold class for the e-mail skillsets	E-mailSkillsetTC	
Office hours template name	Sample Customer	
Threshold Class Calls Waiting: Level 2	5	
Threshold Class Longest wait since last call: Level 1	35	
Threshold Class Longest wait since last call: Level 2	65	
Threshold Class Agent Not Ready: Level 1	2	
Threshold Class Agent Not Ready: Level 2	5	
Call Center Elite Aux Work code number	10	
Call Center Elite Aux Work code name	Coffee Break	
Contact Center activity code display name	CoffeeBreak	
Contact Center activity code number	110	
Contact Center activity code name	Taking a CoffeeBreak	
Call presentation class name	Email_CPC	
Agent break after closing a contact	30 (seconds)	
E-mail skillset name	EM_Support	
E-mail skillset comment	SK for E-mail	

Contact Center Multimedia configuration

The following table lists all the sample values that the installer can enter when configuring the CCMM server in Contact Center Multimedia configuration (page 161).

Contact Center Multimedia configuration sample values

Configuration item	Worked example value	Equivalent value for your system
CCMM server display name (in CCMA)	CCElite_CCMM	
Multimedia E-mail skillset name	EM_EM_support	
E-mail route point	E-mailsContactsRP	
Mon-Fri office hours start	07:00	
Mon-Fri office hours end	18:00	
Sat-Sun office hours	Closed	
Keyword Group name	Support_KG	
Keyword (first in group)	support	
Keyword (second in group	assistance	
Rule Group name	Support_RG	
Rule (first in Rule Group)	Support_Rule	
Recipient mailbox name	ccemailin	
Recipient mailbox domain	labmail.com	
Recipient mailbox display name	CC_e-mail_IN	
Recipient mailbox POP server	172.18.0.55	
Recipient mailbox mail threshold	100	
Recipient mailbox SMTP server	172.18.0.55	
Recipient mailbox name	ccemailin	
Recipient mailbox domain	labmail.com	
Recipient mailbox display name	CC_e-mail_IN	
Recipient mailbox password	Passw0rd1	
Recipient mailbox POP server	172.18.0.55	
Recipient mailbox mail threshold	100	
Recipient mailbox SMTP server	172.18.0.55	
Outbound mailbox name	ccemailout	
(1 of 2)		

Contact Center Multimedia configuration sample values

Configuration item	Worked example value	Equivalent value for your system
Outbound mailbox domain	labmail.com	
Outbound mailbox display name	CC_e-mail_OUT	
Outbound mailbox password	Passw0rd2	
Outbound mailbox POP server	172.18.0.55	
Outbound mailbox mail threshold	100	
Outbound mailbox SMTP server	172.18.0.55	
(2 of 2)		

Preparing the Windows Domain for the Call Center Elite Integration with Contact Center

The following table lists all the values that the installer needs to enter when installing the Contact Center servers in Preparing the Windows Domain for the Call Center Elite Integration with Contact Center (page 209).

Windows Domain preparation values

Configuration item	Worked example value	Equivalent value for your system
Windows domain	siptraffic.com	
Windows Domain Organization Unit (for agent desktop computers)	EliteDesktops	
Download temporary folder on Windows Domain controller	C:\Temp\AACCGroupPolicy	
Group Policy name (for agent desktop computers)	EliteDesktopGroupPolicy	

Configuring Contact Center to Integrate with Call Center Elite

The following table lists all the values that the installer needs to enter when preparing Contact Center for integration with Elite in Configuring Contact Center to Integrate with Call Center Elite (page 219).

Contact Center integration with Call Center Elite values

Configuration item	Worked example value	Equivalent value for your system
Elite agent Login ID	6305	
Elite agent password	1234	
Agent feature button 04 assignment	aux-work	
Agent feature button 05 assignment	auto-in	
Agent feature button 06 assignment	manual-in	
Agent feature button 07 assignment	after-call	
Agent feature button 08 assignment	release	
CCMM server display name (for CCMA)	CCElite_CCMM	
Reason code mapping name	Elite_CoffeeBreak	
Elite Aux Work code	10	
Contact Center activity code	Coffee_Break	
Agent Template name	EliteAgentTemplate	
Elite Communication Manager IP address	172.18.70.200	
Follow up timer period	30 seconds	

Supervisor and Agent Configuration

The following table lists all the values that the installer needs to enter when creating and configuring Contact Center supervisors and agents in Supervisor and Agent Configuration (page 239).

Supervisor and Agent configuration values

Configuration item	Worked example value	Equivalent value for your system
CCMS display name (in CCMA)	MM_Elite_CC_Single_Server	
Supervisor first name	John	
Supervisor last name	Doe	
Supervisor title	Mr.	
(1 of 2)		

Supervisor and Agent configuration values

Configuration item	Worked example value	Equivalent value for your system
Supervisor department	E-mail Support	
Supervisor Login ID	1001	
Agent title	Mr.	
Agent department	E-mail Support	
Agent Login ID	2001	
Domain for agent's Windows logon name	siptraffic.com	
Avaya Aura® CC installer account	AACCinstaller	
Avaya Aura® CC installer password	AACCpass1	
Agent's Windows domain logon name	ccagentone	
Agent's call presentation class	EmailCPC	
Agent's e-mail skillset	EM_EM_Support	
Agent's profile template	EliteAgentTemplate	
(2 of 2)		

Agent Desktop client software installation

The following table lists all the values that the installer needs to enter when installing the Agent Desktop software in Agent Desktop client software installation (page 265).

Agent Desktop client software installation values

Configuration item	Worked example value	Equivalent value for your system
CCMM server display name (for CCMA)	CCElite_CCMM	
Callback Time:Maximum Time	2 (days)	
Attachment Upload Size:Maximum Size	1024 (Kb)	
Switch Type	Sip Avaya Aura 5.2	
Agent's Windows domain logon name	ccagentone	
Agent's Windows domain logon name	AG1_pass~2	
(1 of 2)		

Agent Desktop client software installation values

Configuration item	Worked example value	Equivalent value for your system
Agent Desktop installer URL	http://cccoresone/agentdesktop	
Agent Contact Center login ID	2001	
Agent Contact Center login password	2001	
(2 of 2)		

Testing contacts using Agent Desktop

The following table lists all the values that the installer needs to enter when testing contacts in Testing contacts using Agent Desktop (page 289).

Testing contacts using Agent Desktop

Configuration item	Worked example value	Equivalent value for your system
Agent's Windows domain logon name	ccagentone	
Agent's Windows domain logon name	AG1_pass~2	
Agent Desktop installer URL	http://cccoresone/agentdesktop	
Agent Contact Center login ID	2001	
Test e-mail To: address	ccemailin@labmail.com	
Test e-mail Subject	"Need Support on ProductX"	
Test e-mail Body	"Could I please have support on V2.1 of ProductX"	
Test agent reply	"Reply to customer"	
Test agent note	"Test reply - Contact Center install test"	
Not Ready reason code	Elite_CoffeeBreak	

High Availability pre-install configuration

The following table lists all the values that the installer needs to enter when configuring the Active server replication in High Availability pre-install configuration (page 313).

High Availability pre-install configuration values

Configuration item	Worked example value	Equivalent value for your system
Avaya Aura® CC installer domain account	AACCinstaller	
Windows domain for CCMA replication	siptraffic.com	
Windows domain account for CCMA replication	EliteReplication	
Active server name	CCCORESONE	
License file download location	C:\Avaya_Support\	
New license file for High Availability	elite_campus_WarmHA.lic	
New site name for High Availability	CC_ELITESITE	

Windows server preparation—Standby server

The following table lists all the values that the installer needs to enter when installing Windows Server 2008 on the Standby Contact Center server in Windows server preparation—Standby server (page 339).

Windows server preparation—Standby server values

Configuration item	Worked example value	Equivalent value for your system
Contact Center server operating system drive size	61440 Mb	
Contact Center server operating system local administrator username	Administrator	
Contact Center server operating system local administrator password	MultiMpassw1	
Contact Center server IP address	172.18.70.34	
Local Area Network Mask	255.255.248.0	
Local Area Network Gateway	172.18.71.254	
DNS server IP address	172.18.71.253	
Contact Center server name	CCCORESTWO	
domain name	SipTraffic.com	
(1 of 2)		

Windows server preparation—Standby server values

Configuration item	Worked example value	Equivalent value for your system
Domain administrator username	Administrator	
Domain administrator password	DomPass1	
Application drive letter and size	D:, 80Gb	
CCMS database drive letter and size	F:, 60Gb	
CCMM database drive letter and size	G:, 300Gb	
CCT database drive letter and size	H:, 5Gb	
Trace logs drive letter and size	I:, 5Gb	
Avaya Aura® CC installer domain username	AACCinstaller	
Avaya Aura® CC installer domain password	AACCInstPass1	
Support download location	C:\Avaya_Support\	
(2 of 2)		

Standby Contact Center server software installation

The following table lists all the values that the installer needs to enter when installing the Standby Contact Center server in Standby Contact Center server software installation (page 381).

Standby Contact Center server software installation values

Configuration item	Worked example value	Equivalent value for your system
Contact Center operating system local administrator username	Administrator	
Contact Center operating system local administrator password	MultiMpassw1	
Avaya Aura® CC installer domain username	AACCinstaller	
Contact Center server name	CCCORESONE	
Support download location	C:\Avaya_Support\	
(1 of 2)		

Standby Contact Center server software installation values

Configuration item	Worked example value	Equivalent value for your system
Customer Name	Sample Customer	
Company Name	Sample Company	
Site Name	CC_ELITESITE	
Contact Center server IP address	172.18.70.34	
CCMA service account (ICEAdmin) password	ICEpassw1	
POP3 mail server IP address (incoming e-mail messages)	172.18.0.55	
SMTP mail server IP address (outgoing e-mail messages)	172.18.0.55	
Active server Fully-Qualified Domain Name (FQDN)	CCCORESONE.siptraffic.com	
AD-LDS Replication LDAP Port	389 (default)	
Windows domain account for CCMA replication	EliteReplication	
(2 of 2)		

Standby Server Post-install Commissioning

The following table lists all the values that the installer needs to enter when commissioning the Standby Contact Center server in Standby Server Post-install Commissioning (page 423).

Standby Server Post-install commissioning values

Configuration item	Worked example value	Equivalent value for your system
Support download location	C:\Avaya_Support\	
Off peak day for running disk defragmentation	Saturday	
Off peak hour for running disk defragmentation	01:00	
Real Time Display (RTD) Multicast address	204.5.6.10	
CCMA RTD incoming Multicast address	234.5.6.10	
Contact Center server name	CCCORESTWO	
(1 of 2)		

Standby Server Post-install commissioning values

Configuration item	Worked example value	Equivalent value for your system
Contact Center sysadmin new password	sample1	
Windows domain for CCMA replication	siptraffic.com	
Windows domain account for CCMA replication	EliteReplication	
(2 of 2)		

High Availability server commissioning

The following table lists all the values that the installer needs to enter when commissioning the Contact Center servers for High Availability in High Availability server commissioning (page 457).

High Availability server commissioning values

Configuration item	Worked example value	Equivalent value for your system
Avaya Aura® CC installer domain username	AACCinstaller	
Active server patch download folder	C:\Avaya_Support	
Standby server patch download folder	C:\Avaya_Support	
Active server name	CCCORESONE	
Active server IP address	172.18.70.33	
Standby server name	CCCORESTWO	
Standby server IP address	172.18.70.34	
Managed IP address	172.18.70.39	
Avaya Aura® CC installer domain username	AACCinstaller	
Avaya Aura® CC installer domain password	AACCInstPass1	
Trusted host IP address	172.18.71.253	
SMTP server IP address (for HA e-mail notification)	172.18.0.55	
SMTP server user ID (for HA e-mail notification)	MailAdmin	
(1 of 2)		

High Availability server commissioning values

Configuration item	Worked example value	Equivalent value for your system
SMTP server user password (for HA e-mail notification)	MApass~1	
HA e-mail notification From address	vdhanote1@labmail.com	
HA e-mail notification To address	vdhanote2@labmail.com	
Host server for network backup	172.18.71.253	
Host server Windows share for network backup	CC_Backup	
Windows domain for network backup	siptraffic.com	
Active server backup drive letter	N:	
Standby server backup drive letter	P:	
Managed name	CCCORESMNGD	
(2 of 2)		

Agent Desktop client software installation for High Availability

The following table lists all the values that the installer needs to enter when re-installing the Agent Desktop in Agent Desktop client software installation for High Availability (page 547).

Agent Desktop client software installation for High Availability values

Configuration item	Worked example value	Equivalent value for your system
Agent's Windows domain logon name	ccagentone	
Agent's Windows domain logon name	AG1_pass~2	
Agent Desktop installer URL	http://coresmngd/ agentdesktop	
Agent Contact Center login ID	2001	
Agent Contact Center login password	2001	

Testing High Availability

The following table lists all the values that the installer needs to enter when testing High Availability in Testing High Availability (page 561).

Testing High Availability values

Configuration item	Worked example value	Equivalent value for your system
Agent's Windows domain logon name	ccagentone	
Agent's Windows domain logon name	AG1_pass~2	
Agent Desktop installer URL	http://cccoresmngd/agentdesktop	
Agent Contact Center login ID	2001	
Agent Contact Center login password	2001	
Test e-mail To: address	ccemailin@labmail.com	
Test e-mail Subject	"Need Support on ProductX"	
Test e-mail Body	"Could I please have support on V2.1 of ProductX"	

Recovering High Availability

The following table lists all the values that the installer needs to enter recovering the High Availability system after a switchover in Recovering High Availability (page 583).

Recovering High Availability procedure values

Configuration item	Worked example value	Equivalent value for your system
Avaya Aura® CC installer domain username	AACCinstaller	
Host server for network backup	172.18.71.253	
Host server Windows share for network backup	CC_Backup	
Windows domain for network backup	siptraffic.com	
Active server backup drive letter	N:	
(1 of 2)		

Recovering High Availability procedure values

Configuration item	Worked example value	Equivalent value for your system
Standby server backup drive letter	P:	
Managed server name	CCCORESMNGD	
(2 of 2)		

Contact Center Server Installation Section

Windows server preparation

This chapter provides the common procedures to prepare the Windows server on which you plan to install the Avaya Aura® Contact Center server software. You must perform the procedures in this chapter on each Windows Server 2008 64-bit Release 2 server in the solution.

Prerequisites to server preparation

- Ensure all server hardware meets the requirements described in *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).

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.

  Do not upgrade your operating system from a previous release. Remove the drive partitions and reformat the hard drives on the server.
- Configure all servers for RAID as described in *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
- 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. This partition must be a minimum of 61440 Mb. You can either change it now or expand it after the installation.

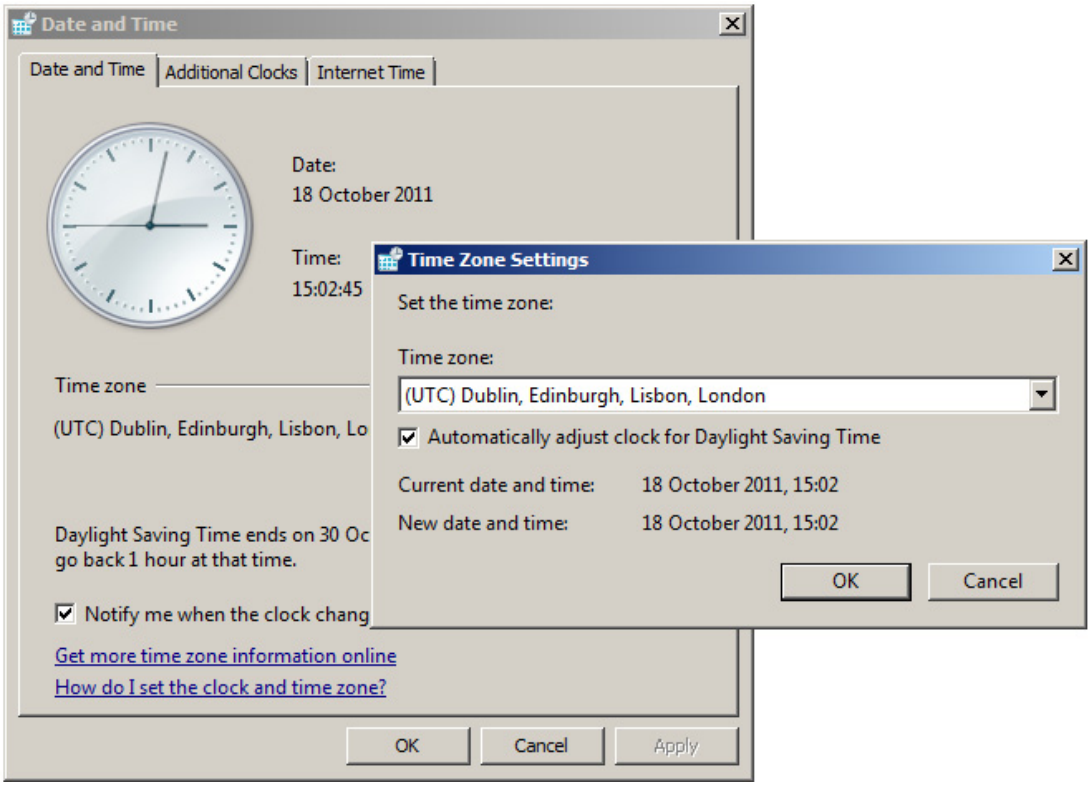
16 Click **Next**.

The install proceeds and automatically restarts the server several times.

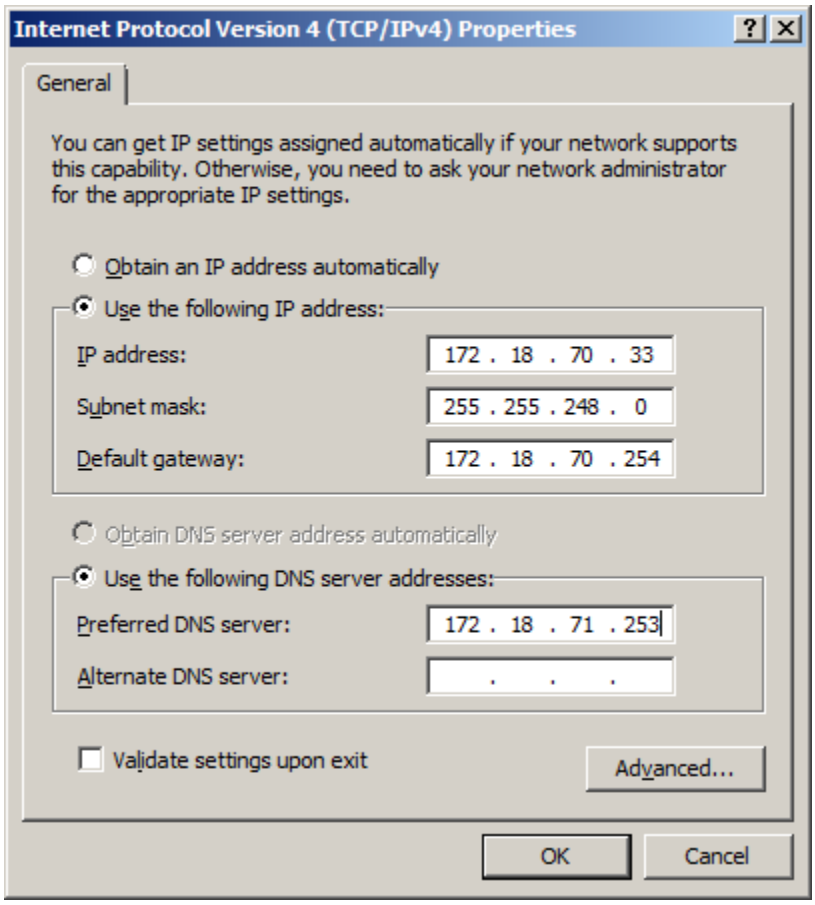
17 After completing the installation, log on to the server as Administrator. Enter and confirm the local Administrator password, for example **MultiMpassw1**.

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

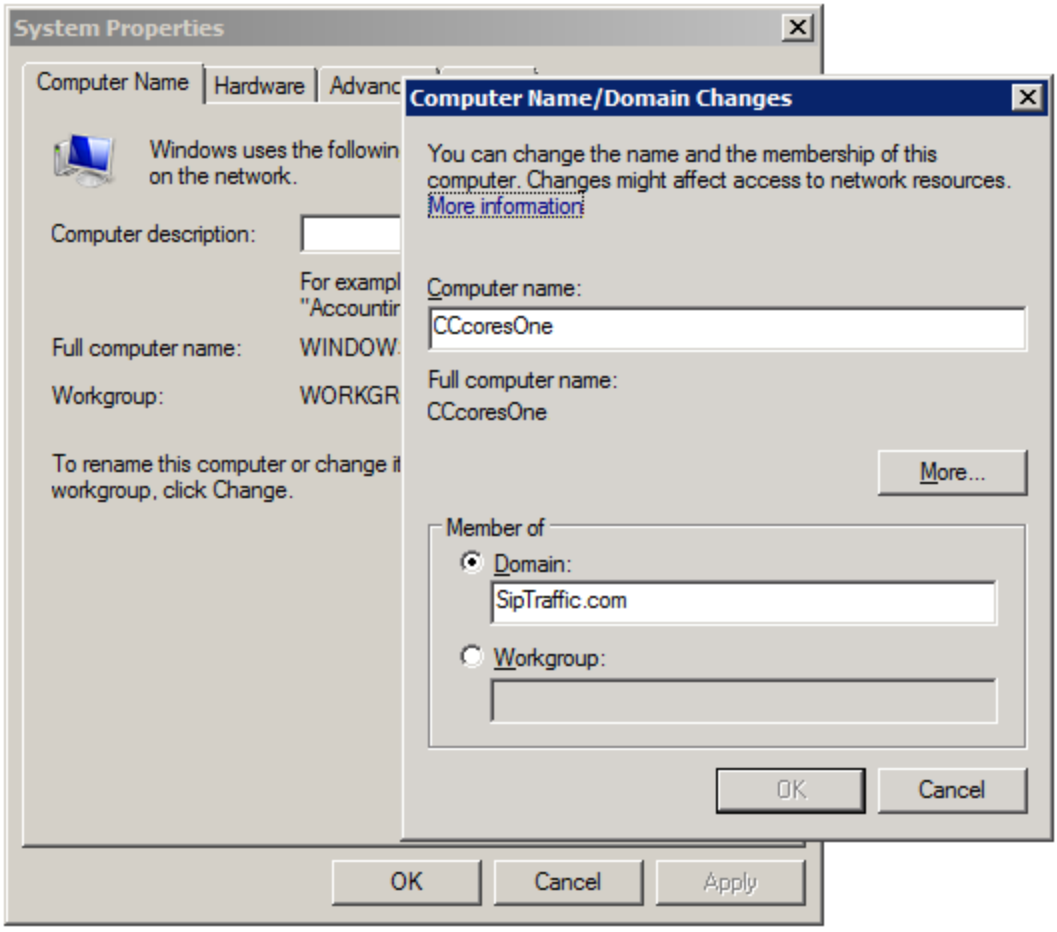
19 Select **Set time zone** and complete the information as required for your system. Ensure you select **Automatically adjust clock for Daylight Saving Time**: CCMM does not support manual DST time changes.



20 Select **Configure Networking** and complete the information for your Network Interface Card (NIC) with the server IP address, subnet mask, default gateway, and DNS server. For example use **172.18.70.33, 255.255.248.0, 172.18.70.254,** and **172.18.71.253** respectively for the primary server.



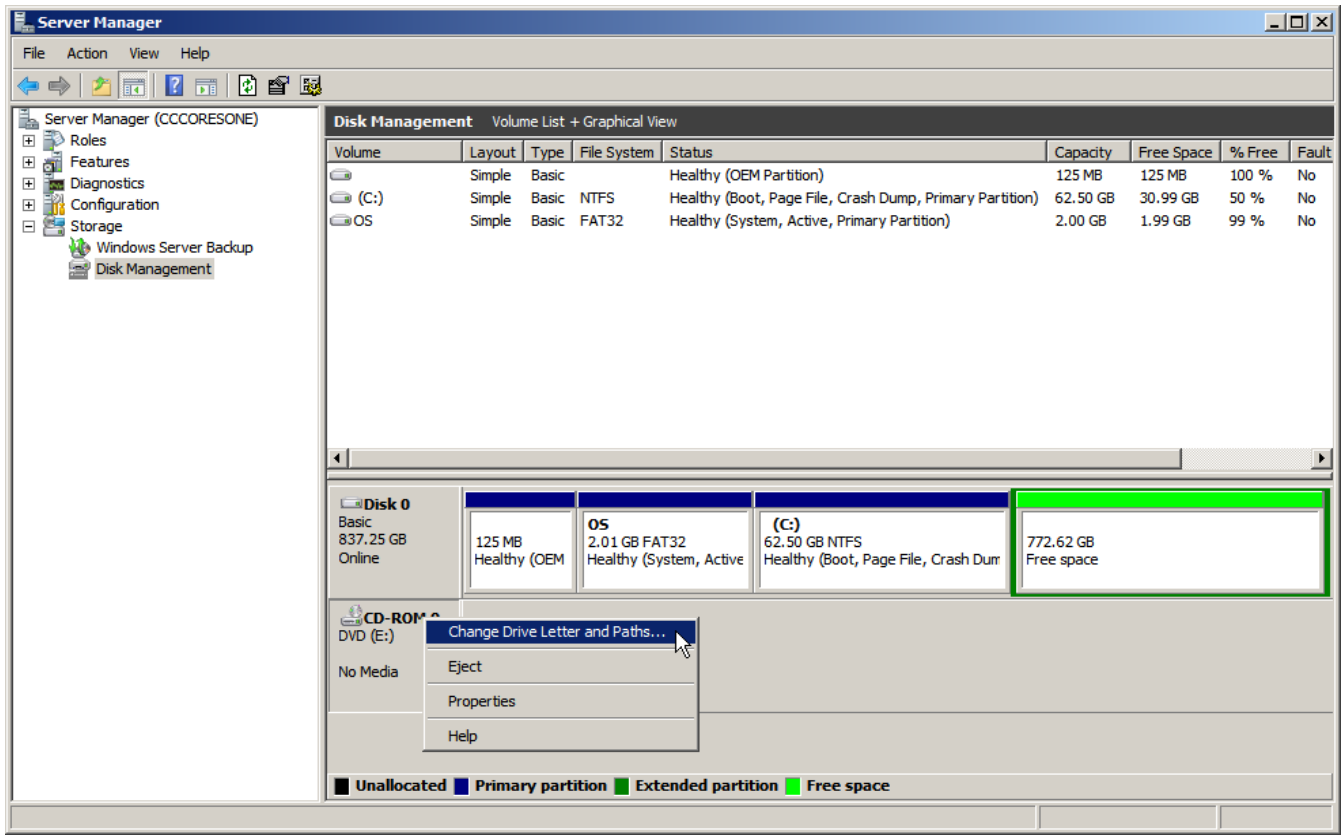
21 Select **Provide computer name and domain** and complete the information for your server name and domain settings. For example, use **CCCORESONE** in the domain **siptraffic**.



22 Choose Restart Later when prompted to restart the computer, and log back in as a local administrator, for example **CCCORESONE\Administrator**.

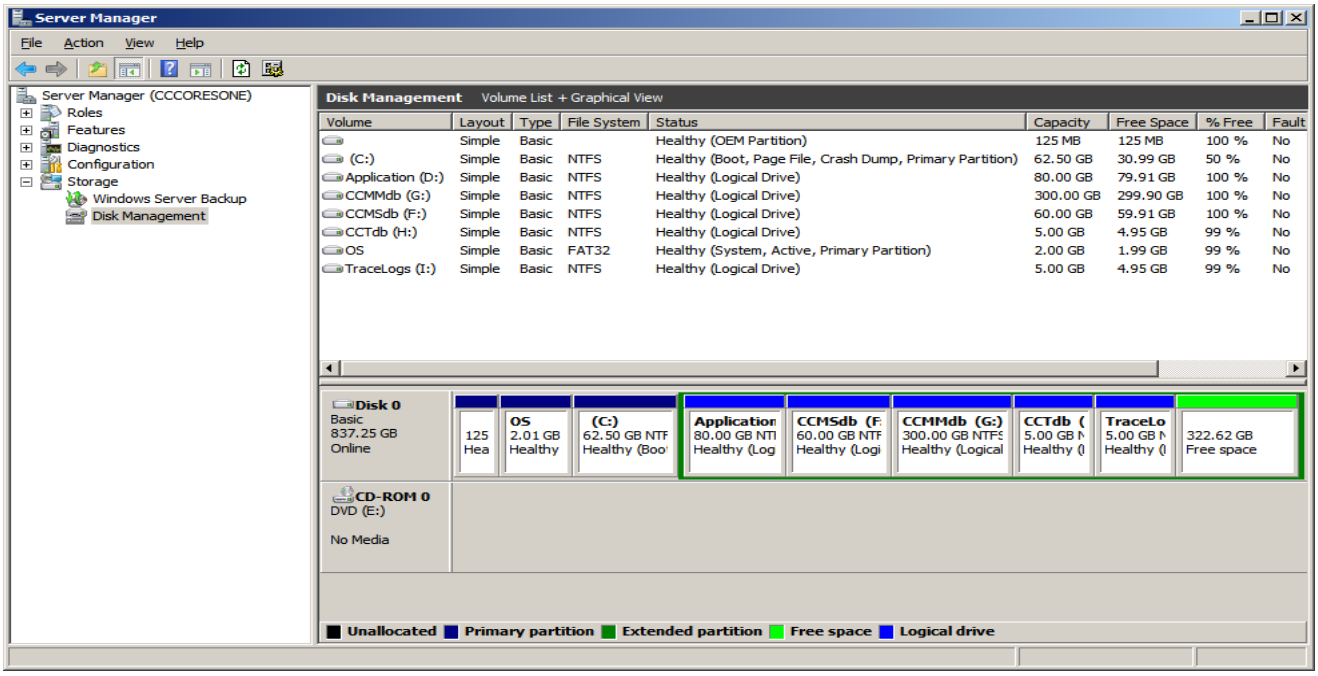
23 Configure disk drive C: to be the only primary partition on your hard drive. Ensure that it is at least 60Gb in size; if drive C: is less than 60Gb, expand the volume.

24 Change the DVD drive letter to E:, to ensure the correct drive letters are free for the drives needed for the Avaya Aura® CC application components.



25 Configure the remaining drives for this server as follows:

— D: 80Gb Application drive
— F: 60Gb CCMS Database drive
— G: 300Gb CCMM Database drive
— H: 5Gb CCT Database drive
— I: 5Gb Trace logs drive



26 Install any drivers specifically required for your hardware configuration.

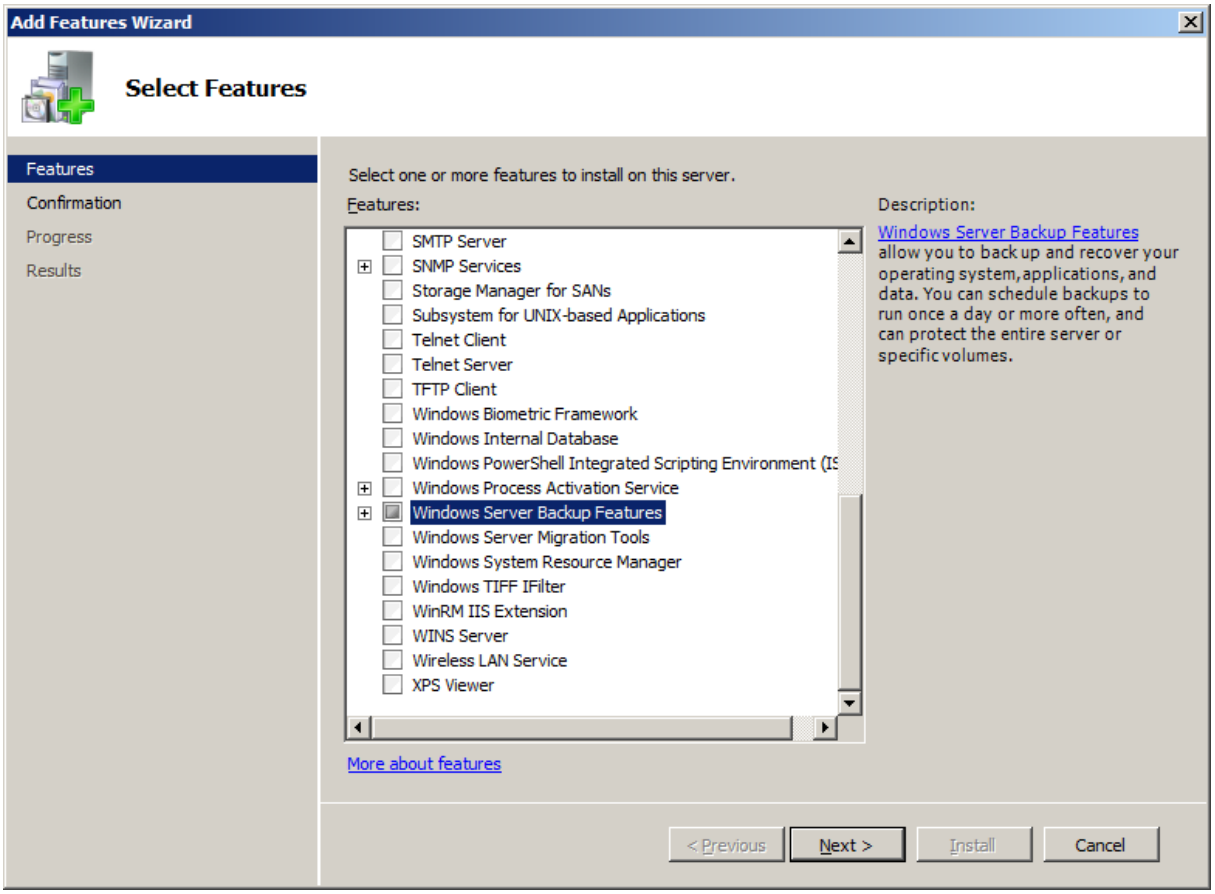
--End--

Configuring Windows Server 2008

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

Procedure steps

Step	Action
1	Log on to the Windows Server 2008 server as a local administrator, for example **CCCORESONE\Administrator**.
2	On the **Initial Configuration Tasks** window, select the **Don't display this screen on startup** check box and click **Close**.
3	Update the emergency repair disk to record the latest configuration data for the server.
4	Choose **Start, Administrative Tools, Server Manager**.
5	In the left pane, click **Features**.
6	Click **Add Features**.
7	Select **Windows Server Backup Features**.



8 Click **Next**.

9 Click **Install**.

10 Click **Close**.

11 Choose **Start, All Programs, Accessories, System Tools, Windows Server Backup**.

12 Follow the on-screen instructions to select what you want to back up.

--End--

Installing the latest operating system service packs

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

Before installing the latest recommended most recent supported operating system service packs, disable the Windows Update feature. Disabling the Windows Update feature prevents Windows Server 2008 from automatically applying operating system patches and potentially rebooting the server.

Prerequisites

- Log on to the server and disable the Windows Update feature. There are several methods for disabling the Windows Update feature, refer to the Windows Server 2008 documentation for a method suitable to your environment.
- Access the Avaya Contact Center Service Packs Compatibility and Hotfix Availability list on the support Web site http://www.avaya.com/support.
- Review the recommendations on operating system service updates in *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
- Install the Microsoft .NET Framework 3.5 and Microsoft .NET Framework 3.5 SP1.

Procedure steps

Step	Action
1	Review the Contact Center Service Packs Compatibility and Security Hotfixes Applicability list to determine the most recent supported patches or service packs.
2	Download the appropriate Microsoft Windows Server 2008 patches for the server software installed on this server.
3	Install the most recent Windows Server 2008 service pack that is validated with the server software by following the Microsoft installation instructions.

--End--

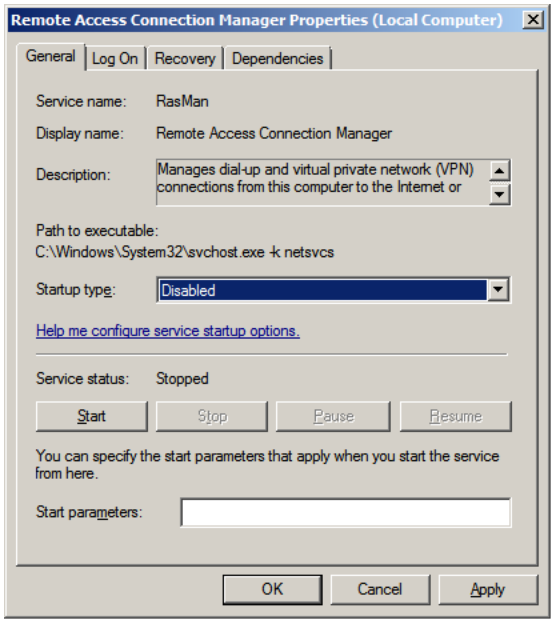
Disabling the Remote Access services

Disable the Remote Access services on the core contact center server, to support Communication Control Toolkit.

Attention: This procedure requires you to 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**.

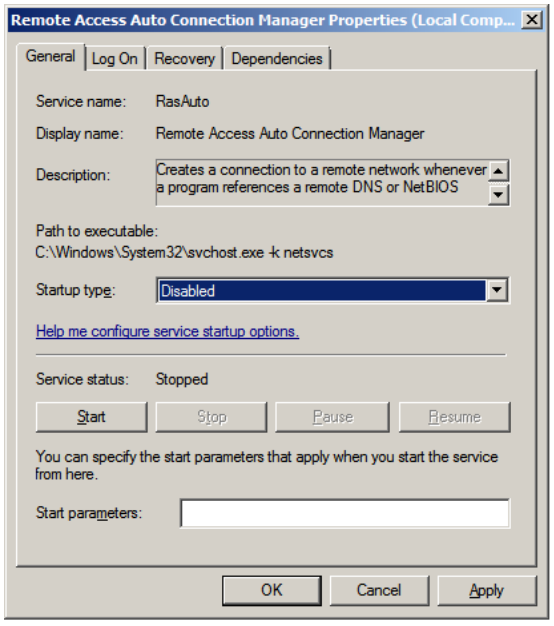


5 Click **OK**.

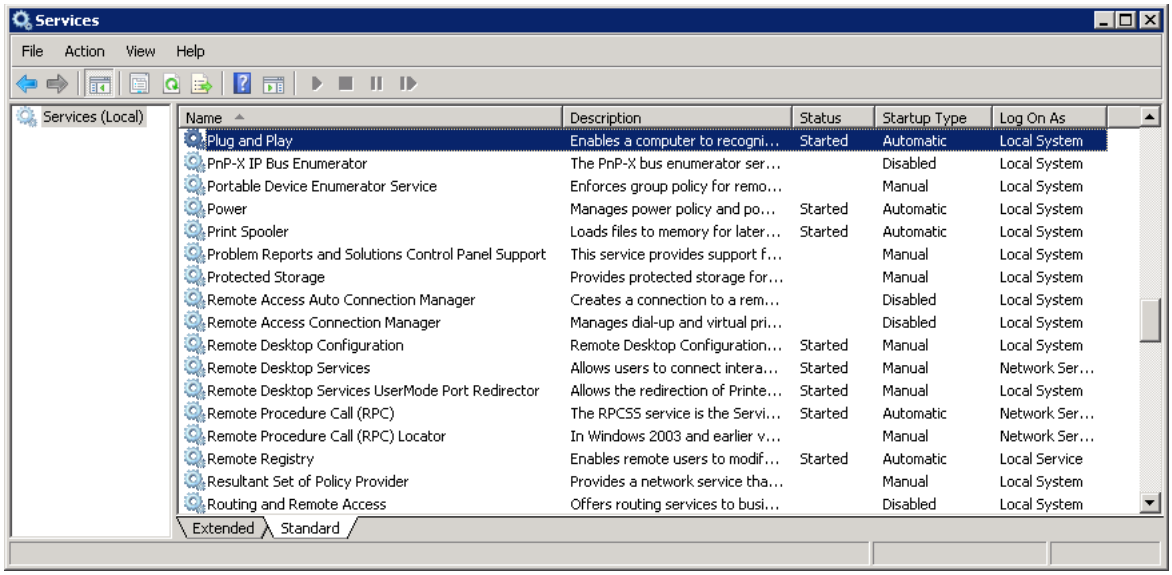
6 In the **Services** window, right-click the **Remote Access Auto Connection Manager** icon.

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.

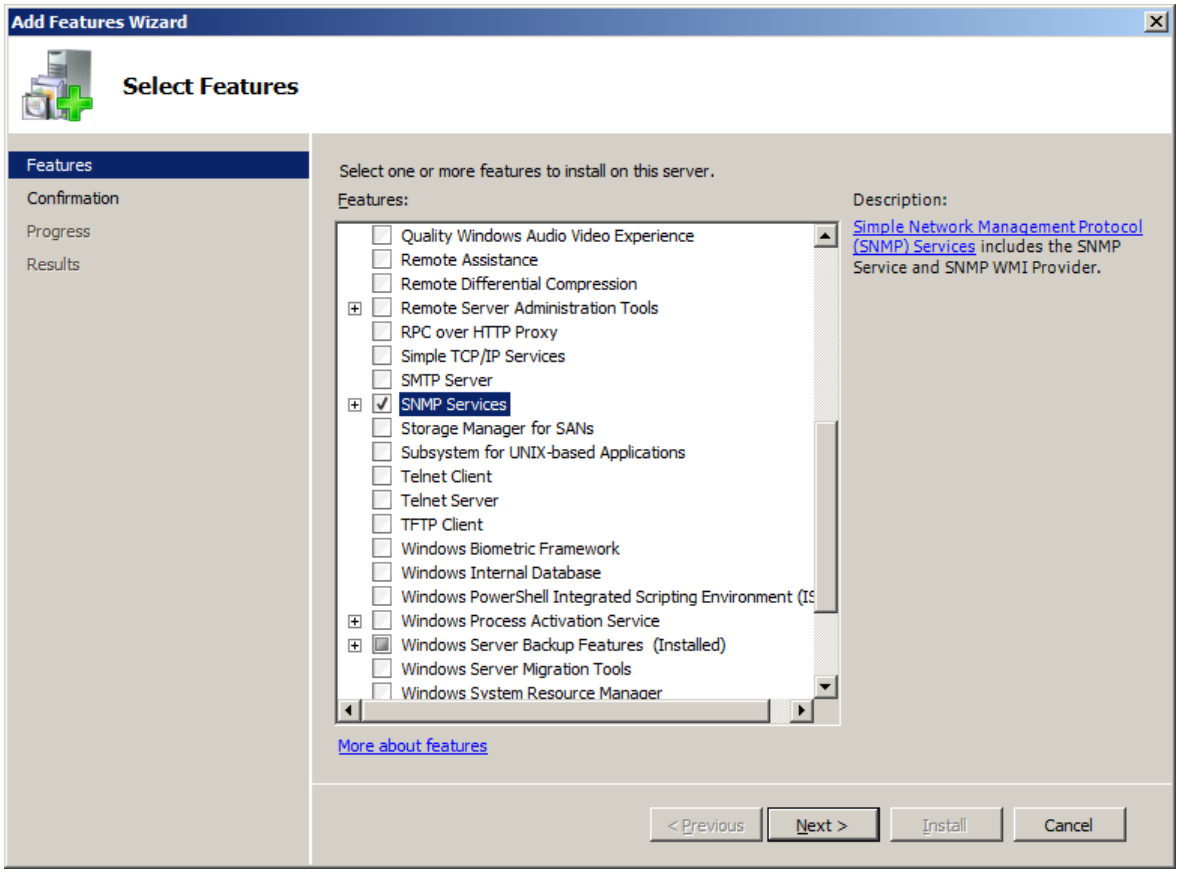
--End--

Configuring SNMP on your server

Configure Simple Network Management Protocol (SNMP) on your server to ensure you have all of the required components of the Internet Protocol for monitoring devices in your network. SNMP helps you manage data that describes the system configuration and errors that may occur between servers.

Procedure steps

Step	Action
1	Log on to the Windows Server 2008 server as a local administrator, for example **CCCORESONE\Administrator**.
2	Choose **Start**, **Control Panel**, **Programs**.
3	In the **Programs and Features** section, click **Turn Windows features on or off**.
4	In the **Server Manager** window, select **Features** and click **Add Features**.
5	Select **SNMP Services**.



6 Click **Next**.

7 Click **Install**.

8 If prompted, insert the Windows Server 2008 DVD.

9 Click **Close**.

--End--

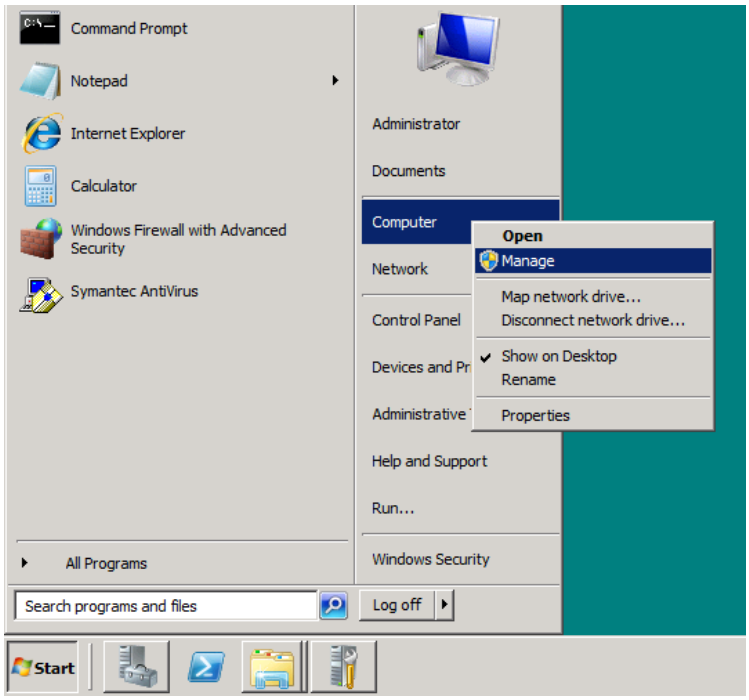
Creating an account for installing and maintaining Contact Center

Create a domain account that you can use to install Contact Center. You must never delete this account. After creating the account, you must add it to the Administrators group on the local server.

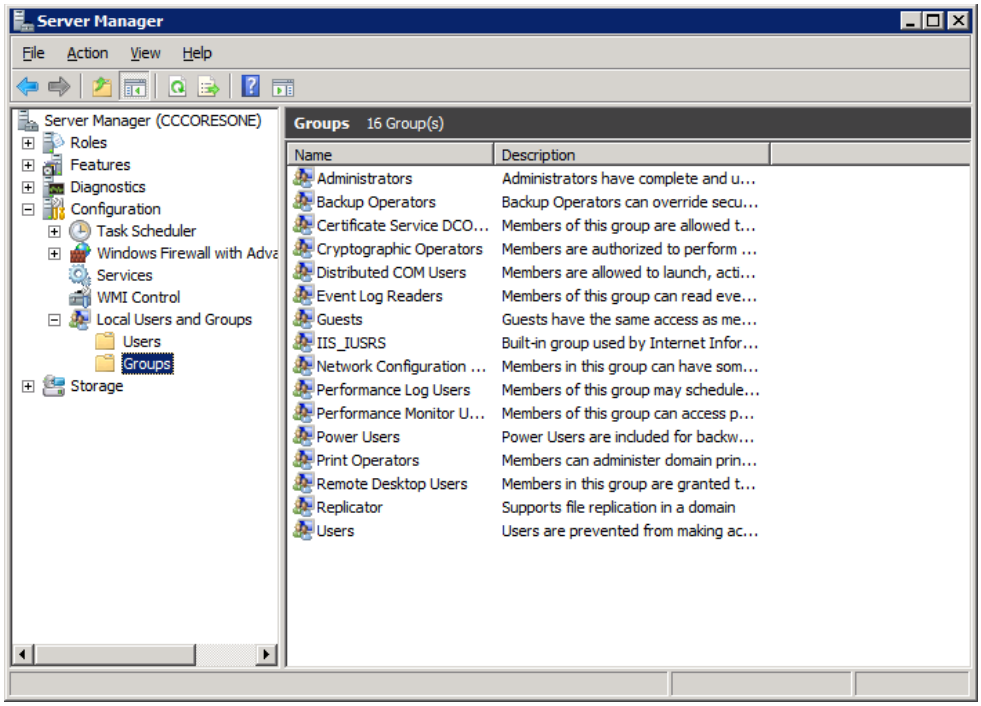
Attention: If you do not have privileges to create domain accounts, ask the domain administrator to create the domain account for you.

Procedure steps

Step	Action
1	Log on to the Active Directory Domain Server as a domain administrator.
2	Create a new user account, for example **AACCinstaller**.
3	Give the new user account normal user privileges on the domain–the precise privileges depend on your organization's domain settings.
4	Log on to the Contact Center server as a local administrator, for example **CCCORESONE\Administrator**.
5	Click **Start**.
6	Right-click **Computer** and select **Manage**.

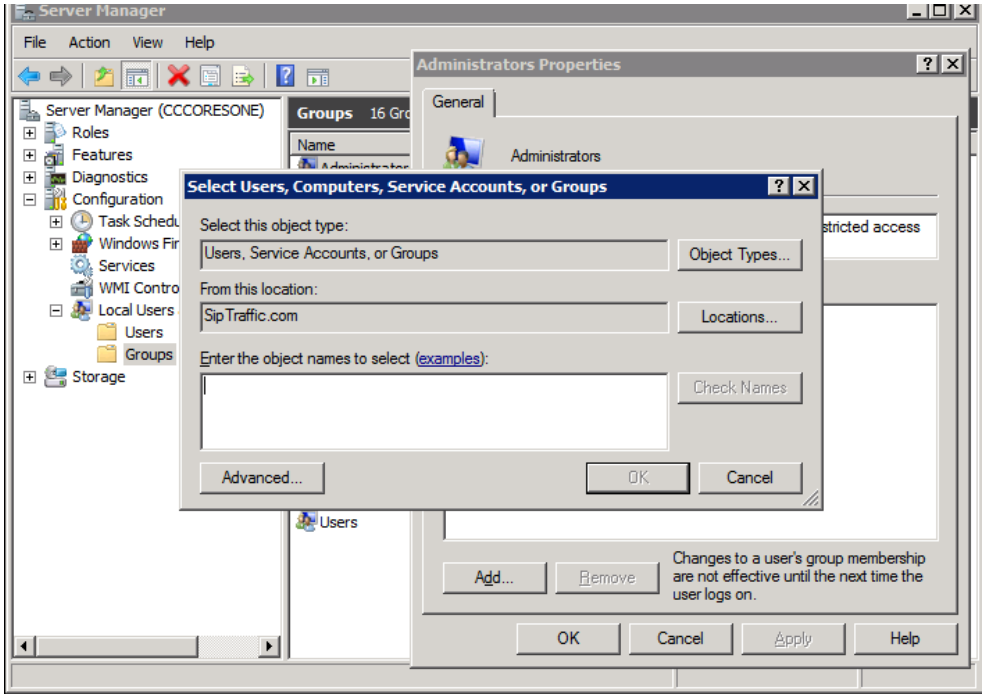


7	In the Server Manager window, in the left pane, expand **Configuration**, **Local Users and Groups**.
8	Select **Groups**.

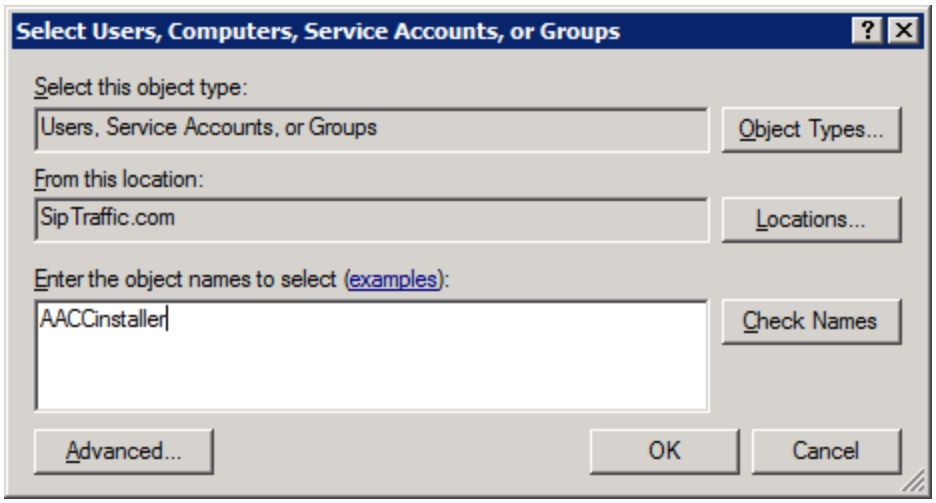


9 In the right pane, double-click **Administrators**.

10 In the **Administrators Properties** Window, click **Add**.



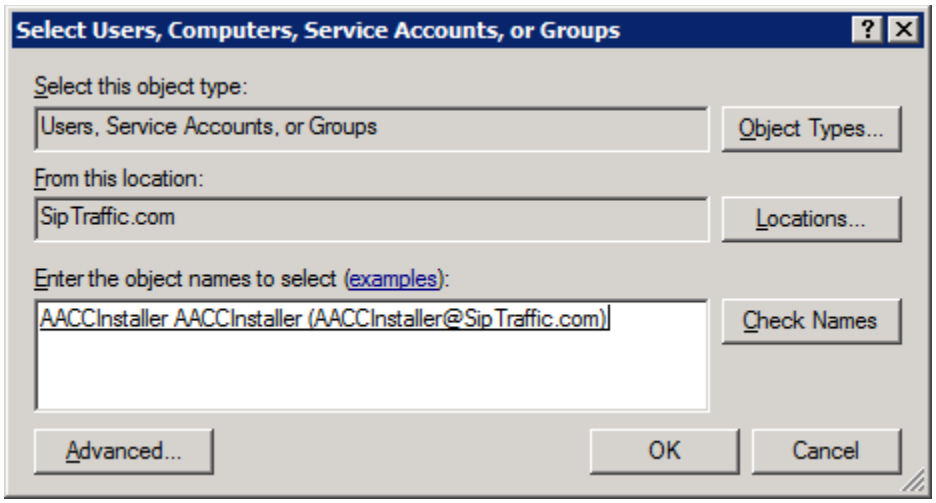
11 On the **Select Users, Computers, Service Accounts, or Groups** window, in the **Enter the object names to select (examples)** box, type the domain account that you created in Step 2, for example AACCinstaller.



12 Click **Check Names**.

13 When prompted, enter a domain administrator user name and password.

The system verifies the domain account.

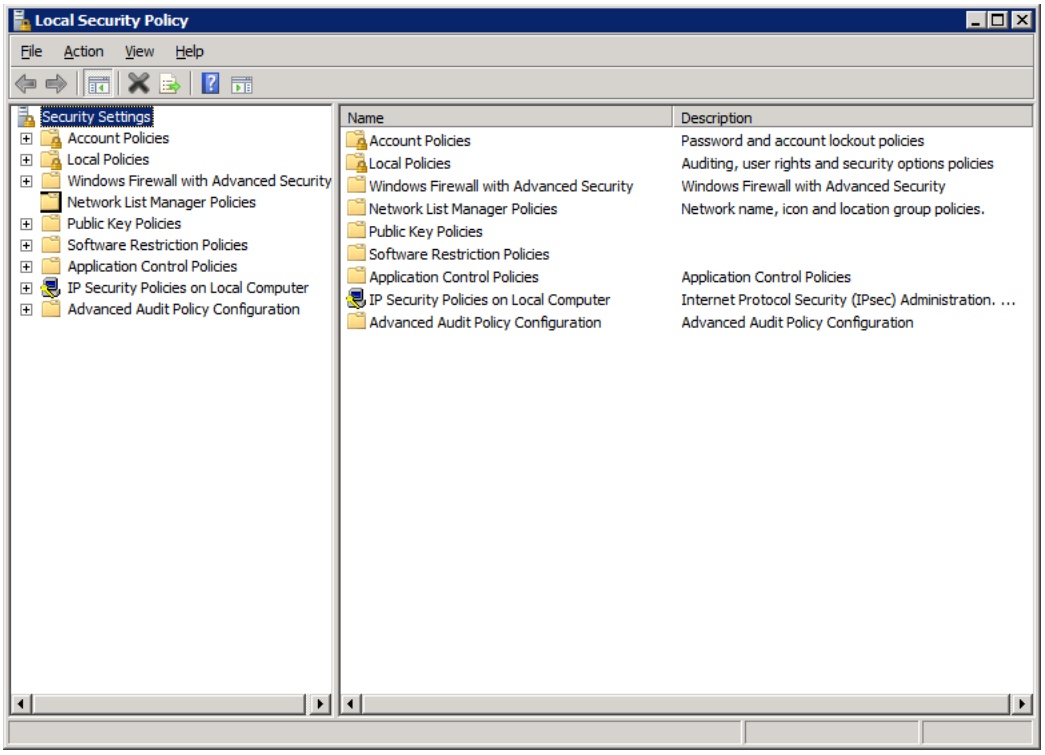


14 Click **OK**.

15 Click **OK**.

16 Exit the Server Manager window.

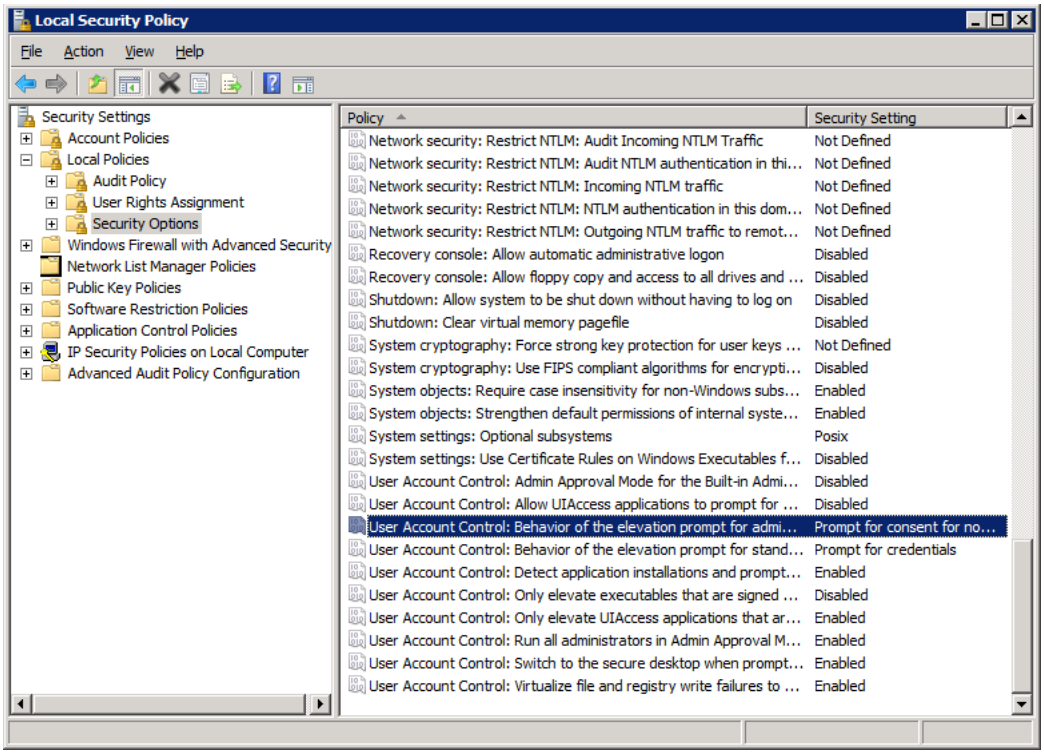
17 Select **Start, Administrative Tools, Local Security Policy**.



18 In the left pane, expand **Local Policies**.

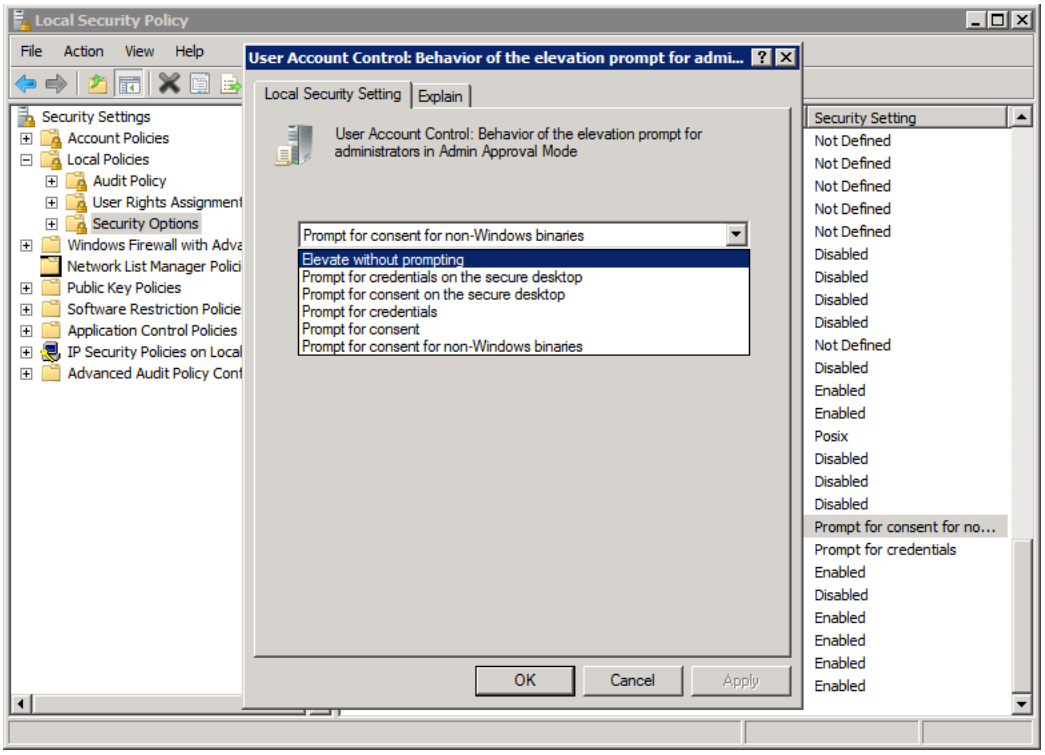
19 Select **Security Options**.

20 In the right pane, scroll down to find **User Account Control: Behavior of the elevation prompt for administrator**.

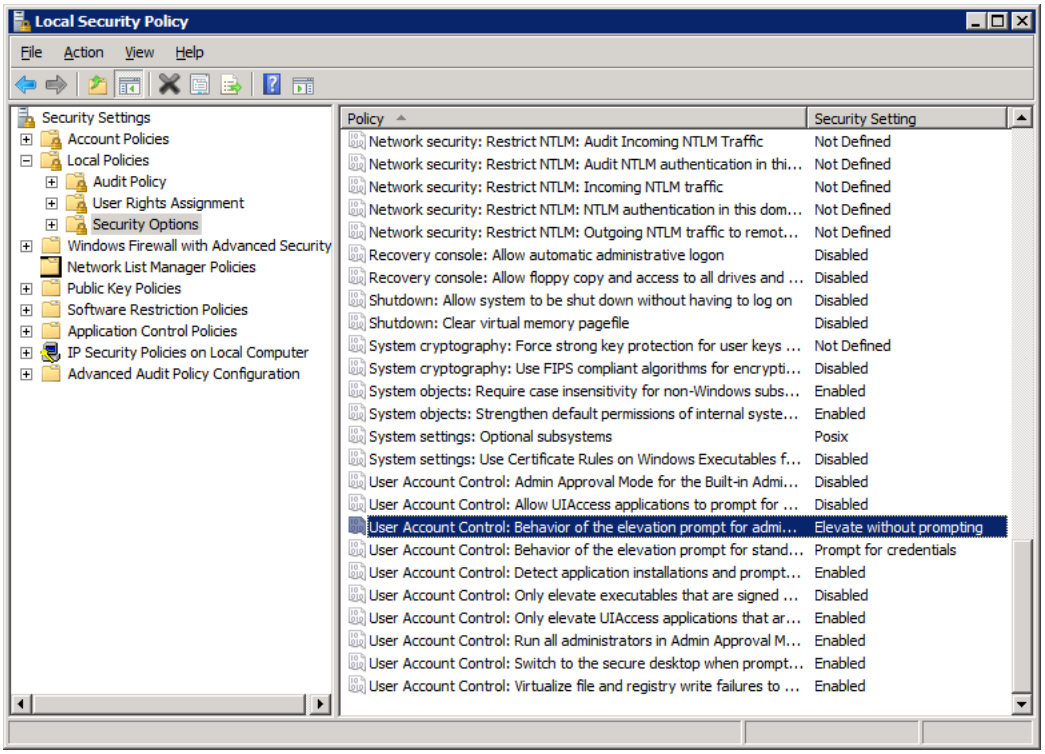


21 Double-click **User Account Control: Behavior of the elevation prompt for administrator**.

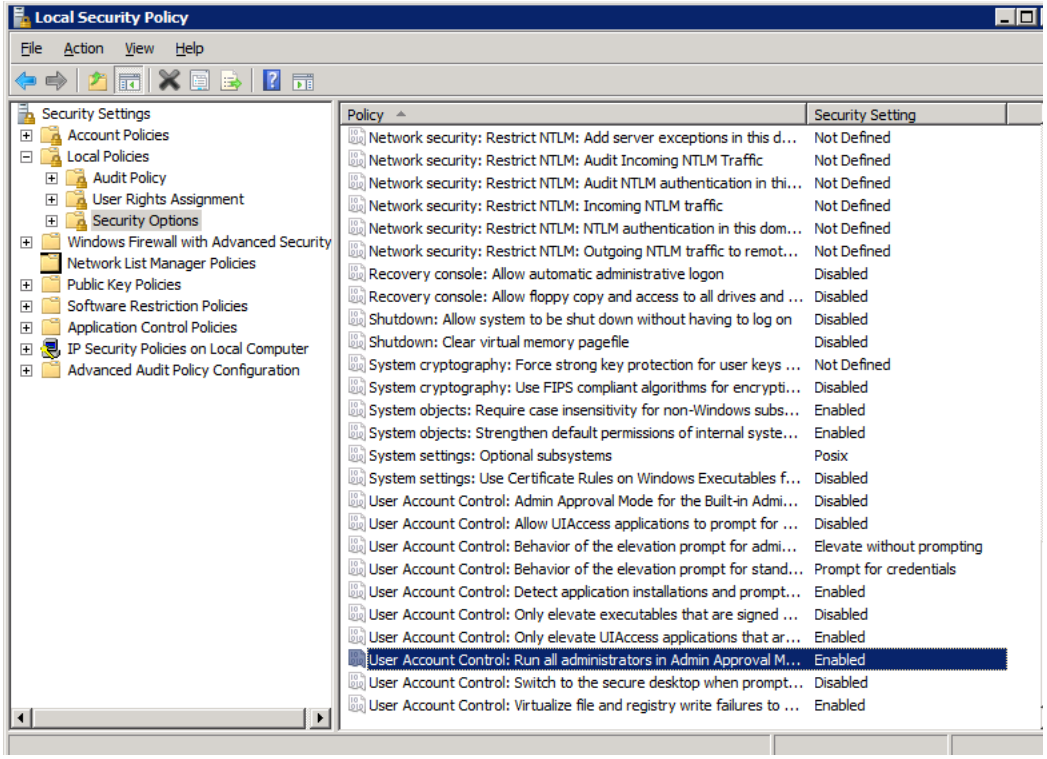
22 On the **Local Security Setting** tab, select **Elevate without prompting**.


Local Security Policy
File Action View Help
User Account Control: Behavior of the elevation prompt for admi...
Local Security Setting
Explain
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode
Prompt for consent for non-Windows binaries
Elevate without prompting
Prompt for credentials on the secure desktop
Prompt for consent on the secure desktop
Prompt for credentials
Prompt for consent
Prompt for consent for non-Windows binaries
OK
Cancel
Apply
Security Setting
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Adva
Network List Manager Polici
Public Key Policies
Software Restriction Policie
Application Control Policies
IP Security Policies on Local
Advanced Audit Policy Conf

23 Click **OK**.

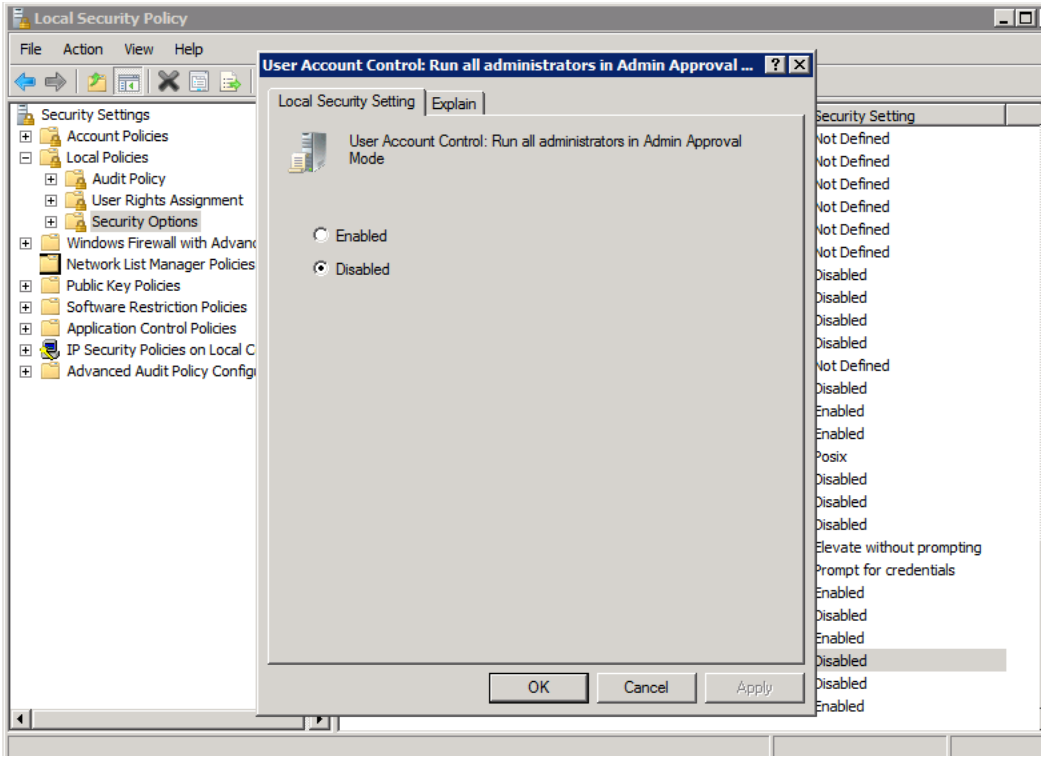

Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Policy
Security Setting
Network security: Restrict NTLM: Audit Incoming NTLM Traffic Not Defined
Network security: Restrict NTLM: Audit NTLM authentication in thi... Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic Not Defined
Network security: Restrict NTLM: NTLM authentication in this dom... Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to remot... Not Defined
Recovery console: Allow automatic administrative logon Disabled
Recovery console: Allow floppy copy and access to all drives and ... Disabled
Shutdown: Allow system to be shut down without having to log on Disabled
Shutdown: Clear virtual memory pagefile Disabled
System cryptography: Force strong key protection for user keys ... Not Defined
System cryptography: Use FIPS compliant algorithms for encrypti... Disabled
System objects: Require case insensitivity for non-Windows subs... Enabled
System objects: Strengthen default permissions of internal syste... Enabled
System settings: Optional subsystems Posix
System settings: Use Certificate Rules on Windows Executables f... Disabled
User Account Control: Admin Approval Mode for the Built-in Admi... Disabled
User Account Control: Allow UIAccess applications to prompt for ... Disabled
User Account Control: Behavior of the elevation prompt for admi... Elevate without prompting
User Account Control: Behavior of the elevation prompt for stand... Prompt for credentials
User Account Control: Detect application installations and prompt... Enabled
User Account Control: Only elevate executables that are signed ... Disabled
User Account Control: Only elevate UIAccess applications that ar... Enabled
User Account Control: Run all administrators in Admin Approval M... Enabled
User Account Control: Switch to the secure desktop when prompt... Enabled
User Account Control: Virtualize file and registry write failures to ... Enabled

24 In the right pane, scroll down to find **User Account Control: Run all administrators in Admin Approval mode**.

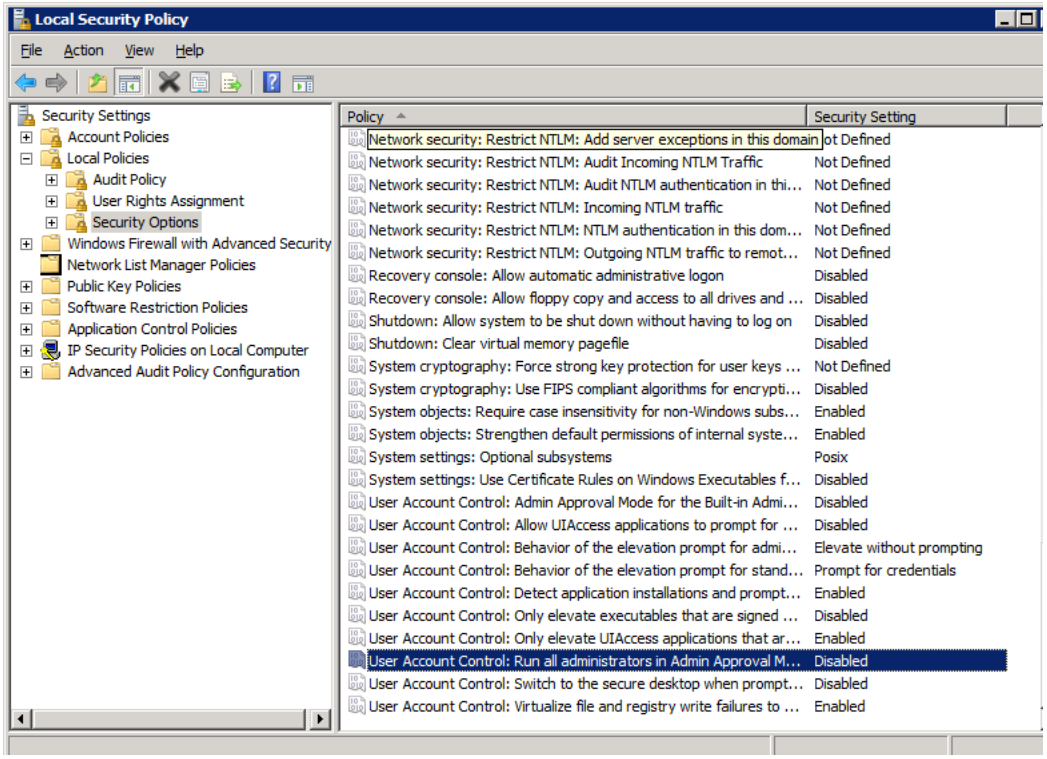


25 Double-click **User Account Control: Run all administrators in Admin Approval mode**.

26 On the **Local Security Setting** tab, select **Disable**.


Local Security Policy
File Action View Help
User Account Control: Run all administrators in Admin Approval ...
Local Security Setting
Explain
User Account Control: Run all administrators in Admin Approval Mode
Enabled
Disabled
OK
Cancel
Apply
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanc
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local C
Advanced Audit Policy Config
Security Setting
Not Defined
Not Defined
Not Defined
Not Defined
Not Defined
Not Defined
Disabled
Disabled
Disabled
Disabled
Not Defined
Disabled
Enabled
Enabled
Posix
Disabled
Disabled
Disabled
Elevate without prompting
Prompt for credentials
Enabled
Disabled
Enabled
Disabled
Disabled
Enabled

27 Click **OK**.


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Policy
Security Setting
Network security: Restrict NTLM: Add server exceptions in this domain
Network security: Restrict NTLM: Audit Incoming NTLM Traffic
Network security: Restrict NTLM: Audit NTLM authentication in thi...
Network security: Restrict NTLM: Incoming NTLM traffic
Network security: Restrict NTLM: NTLM authentication in this dom...
Network security: Restrict NTLM: Outgoing NTLM traffic to remot...
Recovery console: Allow automatic administrative logon
Recovery console: Allow floppy copy and access to all drives and ...
Shutdown: Allow system to be shut down without having to log on
Shutdown: Clear virtual memory pagefile
System cryptography: Force strong key protection for user keys ...
System cryptography: Use FIPS compliant algorithms for encrypti...
System objects: Require case insensitivity for non-Windows subs...
System objects: Strengthen default permissions of internal syste...
System settings: Optional subsystems
System settings: Use Certificate Rules on Windows Executables f...
User Account Control: Admin Approval Mode for the Built-in Admi...
User Account Control: Allow UIAccess applications to prompt for ...
User Account Control: Behavior of the elevation prompt for admi...
User Account Control: Behavior of the elevation prompt for stand...
User Account Control: Detect application installations and prompt...
User Account Control: Only elevate executables that are signed ...
User Account Control: Only elevate UIAccess applications that ar...
User Account Control: Run all administrators in Admin Approval M...
User Account Control: Switch to the secure desktop when prompt...
User Account Control: Virtualize file and registry write failures to ...
Not Defined
Not Defined
Not Defined
Not Defined
Not Defined
Not Defined
Disabled
Disabled
Disabled
Not Defined
Enabled
Enabled
Posix
Disabled
Disabled
Disabled
Elevate without prompting
Prompt for credentials
Enabled
Disabled
Disabled
Enabled

28 Select **File, Exit**.

29 Restart the Windows Server 2008 server.

--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 http://www.avaya.com/support to each server.

Procedure steps

Step	Action
1	Log on to the Contact Center server using the Avaya Aura® CC installer domain account, for example SIPTRAFFIC\AACCinstaller.
2	Create a folder **Avaya_Support** on the **C:** drive.
3	Download the most recent Contact Center service pack file and save it on the Contact Center server in the **Avaya_Support** folder.
4	Right-click the service pack .zip file and select **Extract All** from the context menu.

--End--

Disabling Internet Protocol version 6

Disable Internet Protocol version 6 (IPv6) to ensure correct operation of the contact center software.

Attention: This procedure requires modification of the Windows Server 2008 registry. This is an advanced administrator function: if you are not qualified to carry out edits to the registry, ask a qualified person to complete this procedure.

Attention: The published steps are extracted from Microsoft article 929852. Check the Microsoft support site to ensure that you use the most up to date procedure.

Step	Action
1	Search the Microsoft support site to locate the instructions to disable IPv6 in the Windows Server 2008 registry.
2	On the Windows server, click **Start**.
3	Type **regedit** in the **Start Search** box, and then click **regedit.exe** in the **Programs** list.
4	In the **User Account Control** dialog box, click **Continue**.

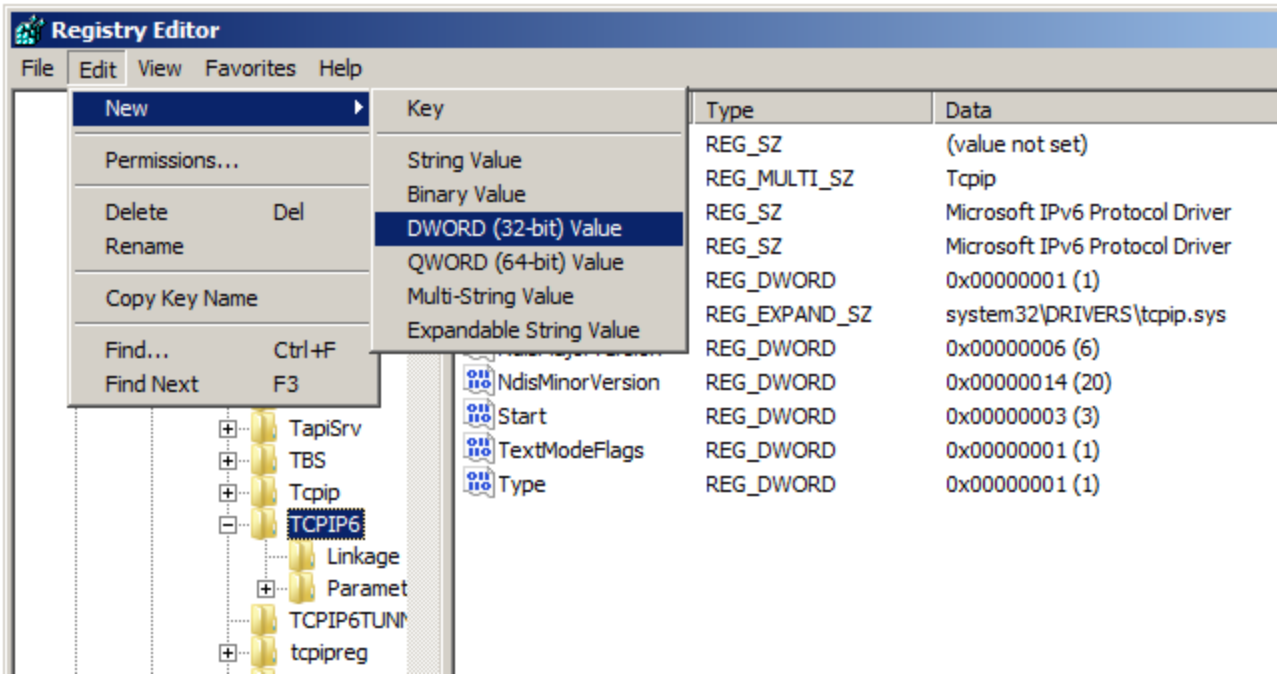
5 In Registry Editor, locate and then click the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP6\Parameters\

6 Double-click **DisabledComponents** to modify the **DisabledComponents** entry.

7 If the **DisabledComponents** entry is unavailable, you must create it by following steps 8 to 9. Otherwise go to step 10.

8 From the **Edit** menu, choose **New**, and select **DWORD (32-bit) Value**.

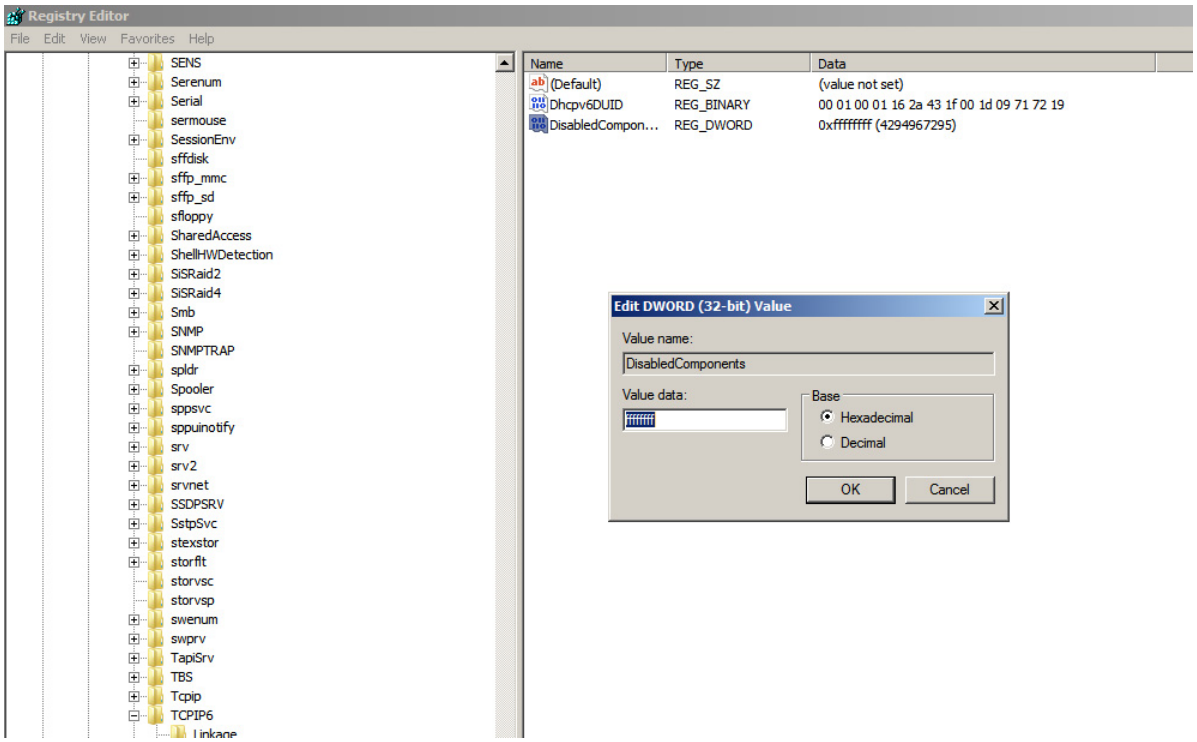


9 Type **DisabledComponents**, and then press **Enter**.

10 Double-click **DisabledComponents**.

11 Select **Hexadecimal**.

12 In the Value data: box type **ffffffff** to disable all IPv6 components.



13 Click **OK**.

14 Reboot the server, if required.

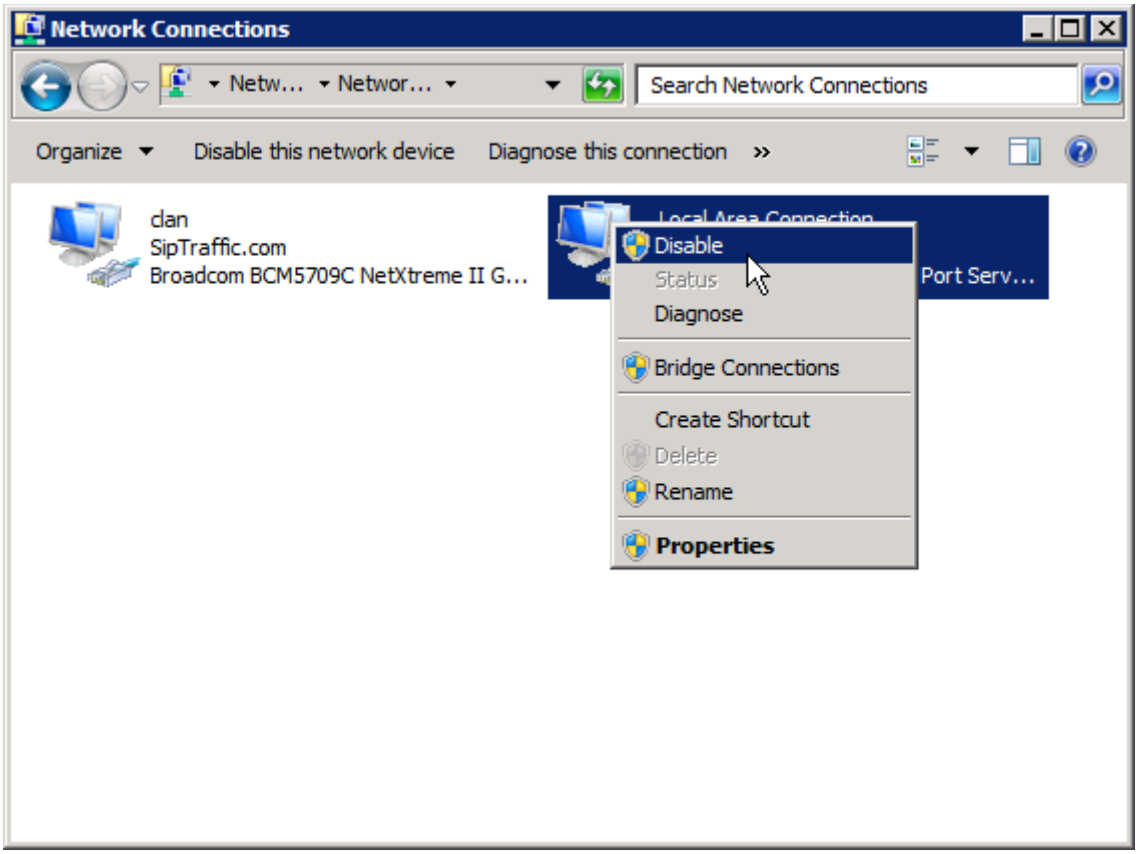
--End--

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 the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Click **Start**, **Control Panel**, **Network and Internet**, **Network and Sharing Center**, **Change Adaptor Settings**.
3	Right-click the unused Network Adaptor, and select **Disable**.



4 Repeat this procedure for all unused Network Adapters.

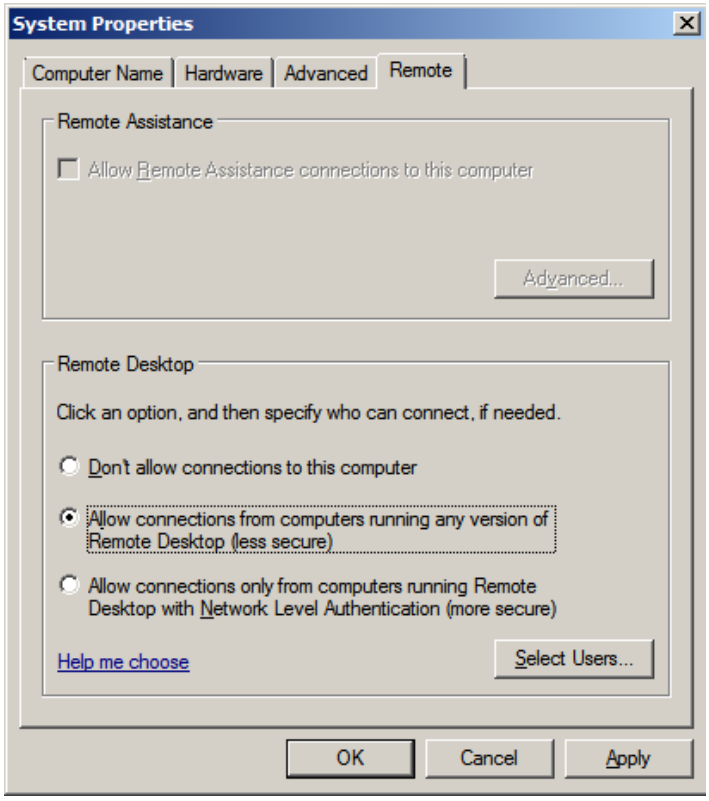
--End--

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	Choose **Start**, **Control Panel**, **System and Security**.
2	In the **System** section, select **Allow remote access**.
3	Click the **Remote** tab.
4	Select **Allow connections from computers running any version of Remote Desktop (less secure)**.



5 On the **Remote Desktop Connection** window, click **OK**.

6 Click **OK**.

--End--

Configuring Data Execution Prevention

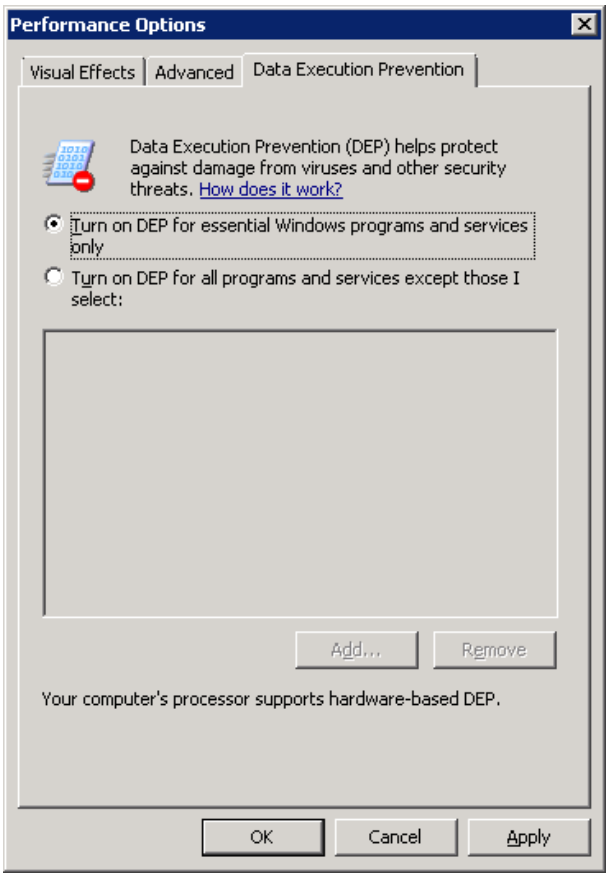
Configure the Data Execution Prevention (DEP) hardware and software to perform additional checks on memory that protect the Contact Center server against malicious code exploitation.

Procedure steps

Step	Action
1	Choose **Start, Control Panel, System and Security**.
2	Click **System**.
3	In the **System** window, click **Advanced system settings**.
4	In the **System Properties** dialog box, click the **Advanced** tab.
5	Under **Performance**, click **Settings**.

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

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



8 Click **OK**.

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

10 If prompted, click **OK** to restart the computer.

--End--

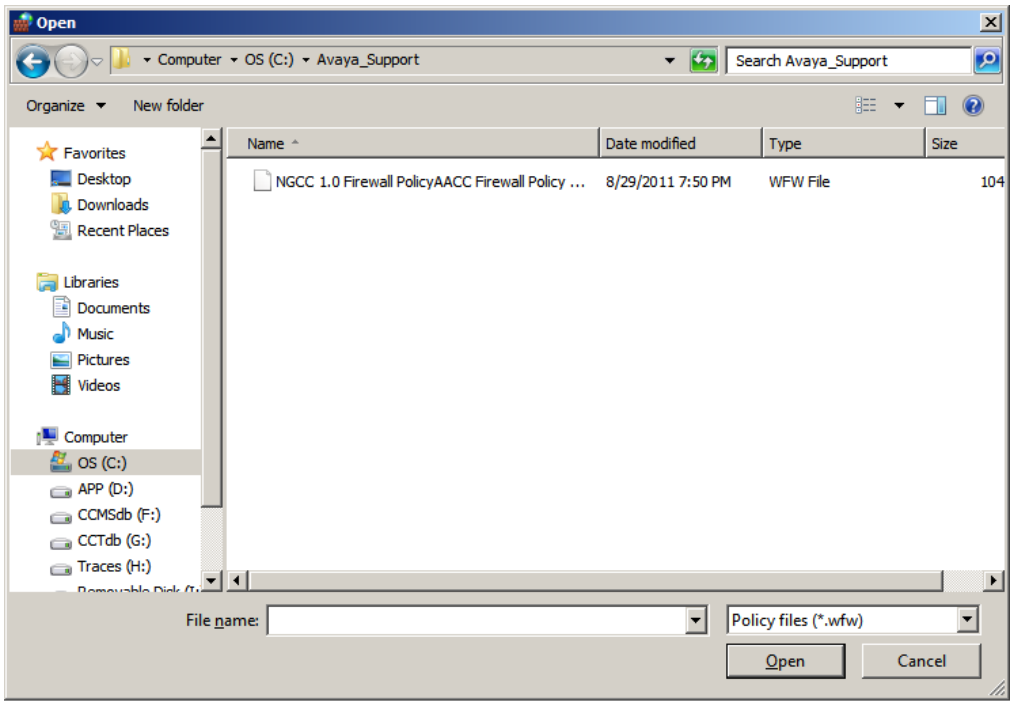
Importing the Contact Center Firewall Security policy

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.

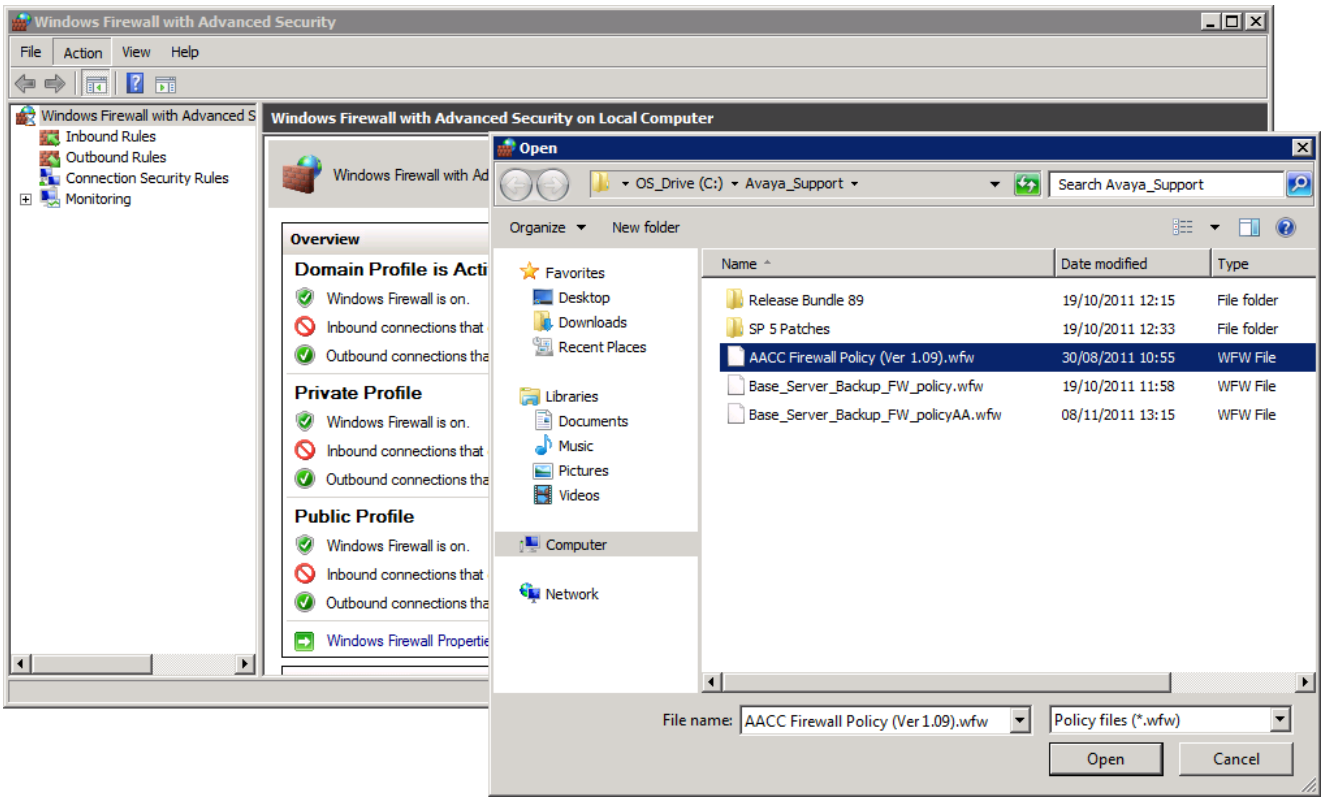
Procedure steps

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 the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
3	Choose **Start**, **Administrative Tools**, **Windows Firewall with Advanced Security**.
4	Choose **Action**, **Export Policy**.
5	In the **File name** box, type a name for the backup policy, for example **BaseOSFirewallPolicyBackup.wfw**.
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.



11 Select the Avaya Aura® CC Firewall Policy you downloaded, for example **AACC Firewall Policy (Ver 1.09).wfw**.

12 Click **Open**.

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

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

--End--

Contact Center server software installation

This chapter provides the steps to install the Avaya Aura® Contact Center server software on the server. This includes the following server software:

- Contact Center Manager Server
- Communication Control Toolkit
- Contact Center Multimedia
- Contact Center Manager Server Utility
- Contact Center License Manager
- Contact Center Manager Administration
- Orchestration Designer

Prerequisites to co-resident server software installation

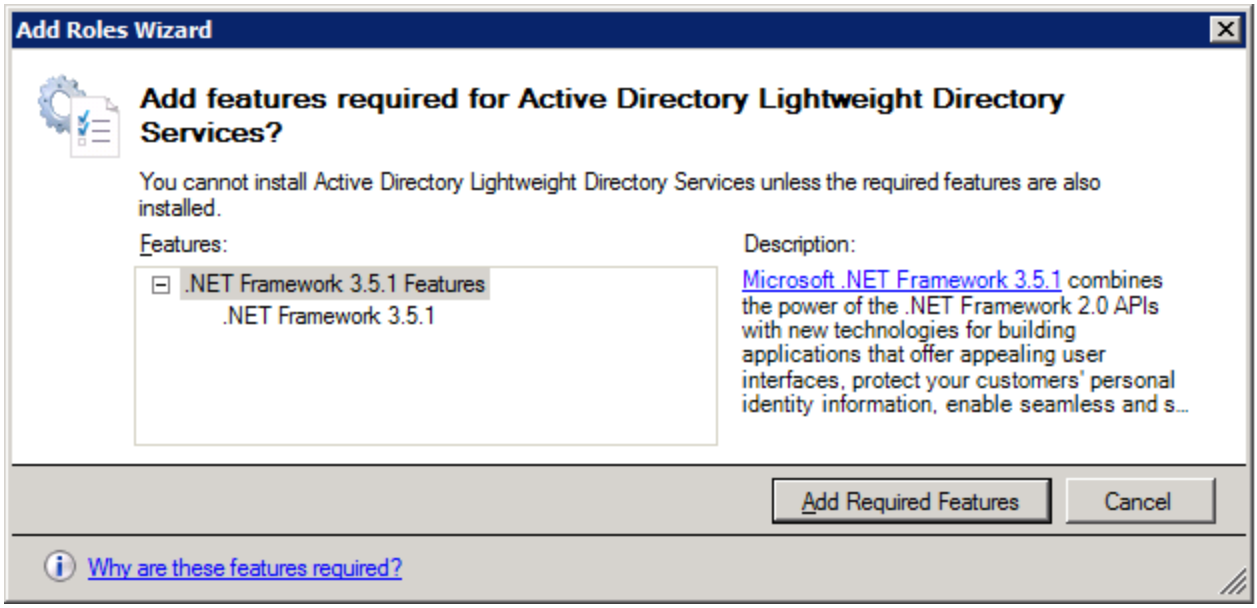
- Ensure that your have your new Contact Center license file.
- Ensure that you have the Contact Center Release 6.2 DVD.

Installing operating system components for Contact Center Manager Administration

Before installing Contact Center Manager Administration, you must install specific operating system software components such as Internet Information Services to integrate with the components in Contact Center.

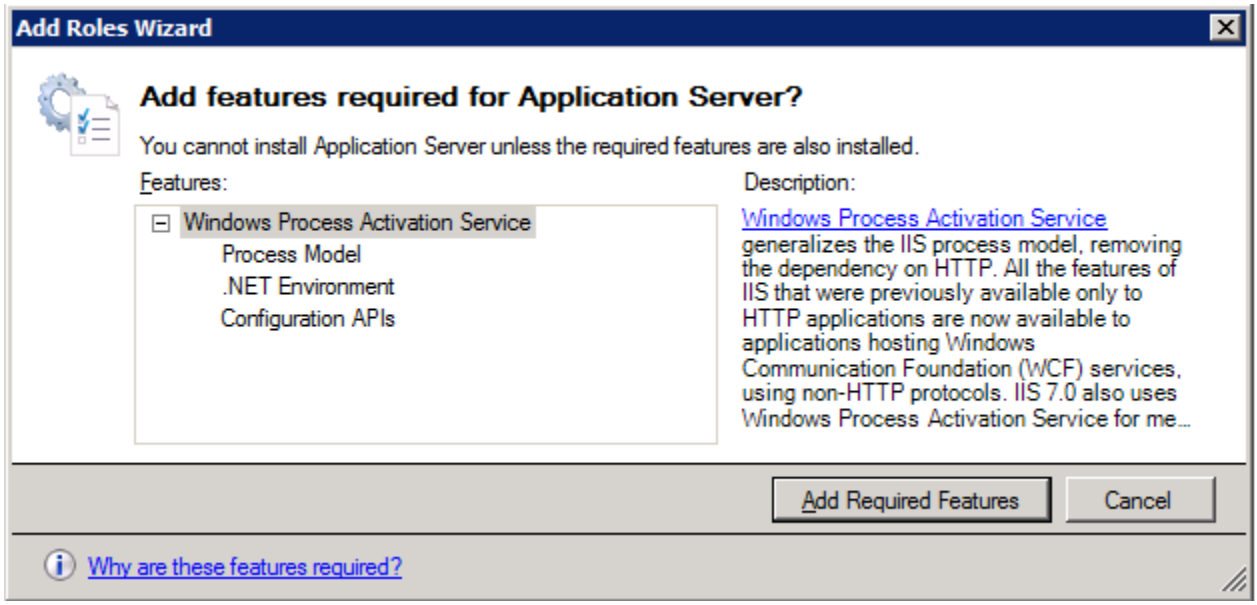
Procedure steps

Step	Action
1	Log on to the Contact Center server using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Choose **Start**, **Administrative Tools**, **Server Manager**.
3	In the left-hand column of the **Server Manager**, right-click **Roles** and select **Add Roles**.
4	Review the requirements for the new role, and click **Next**.
5	Under **Server Roles**, select **Active Directory Lightweight Directory Services**.
6	If an **Add Roles Wizard** message box that lists features required by Active Directory Lightweight Directory Services appears, click **Add Required Features**.



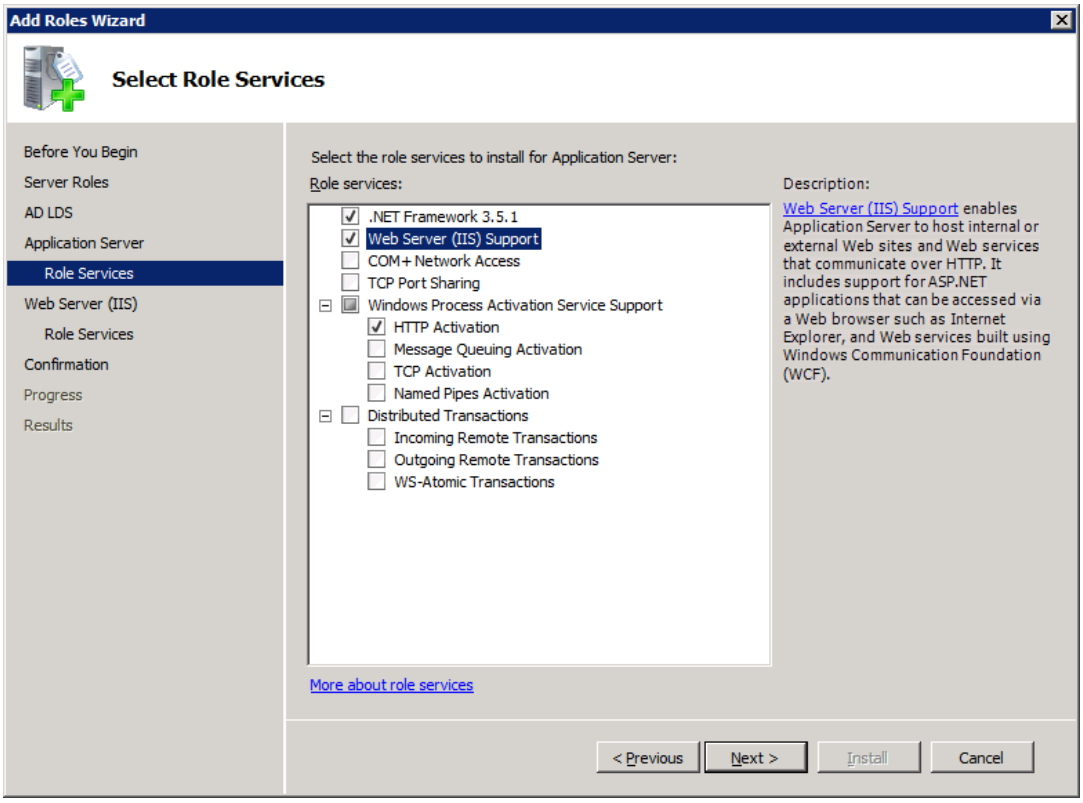
7 Under **Server Roles**, select **Application Server**.

8 If an **Add Roles Wizard** message box that lists features required by Application Server appears, click **Add Required Features**.

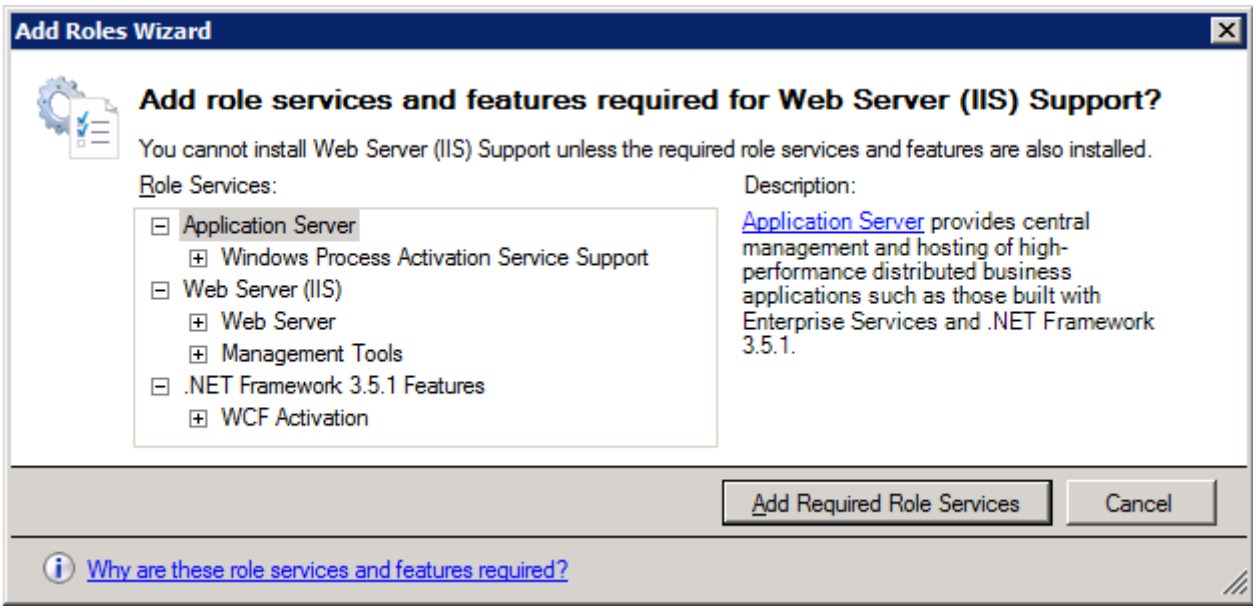


9 In the left pane, under **Application Server**, select **Role Services**.

10 Select **Web Server (IIS) Support**.



11 If an **Add Roles Wizard** message box appears, listing features required by Web Server (IIS) Support, click **Add Required Role Services**.



12 Click **Next**.

13 On the **Introduction to Web Server (IIS)** page, click **Next**.

14 On the **Select Role Services** page, under **Common HTTP Features**, select the following services:

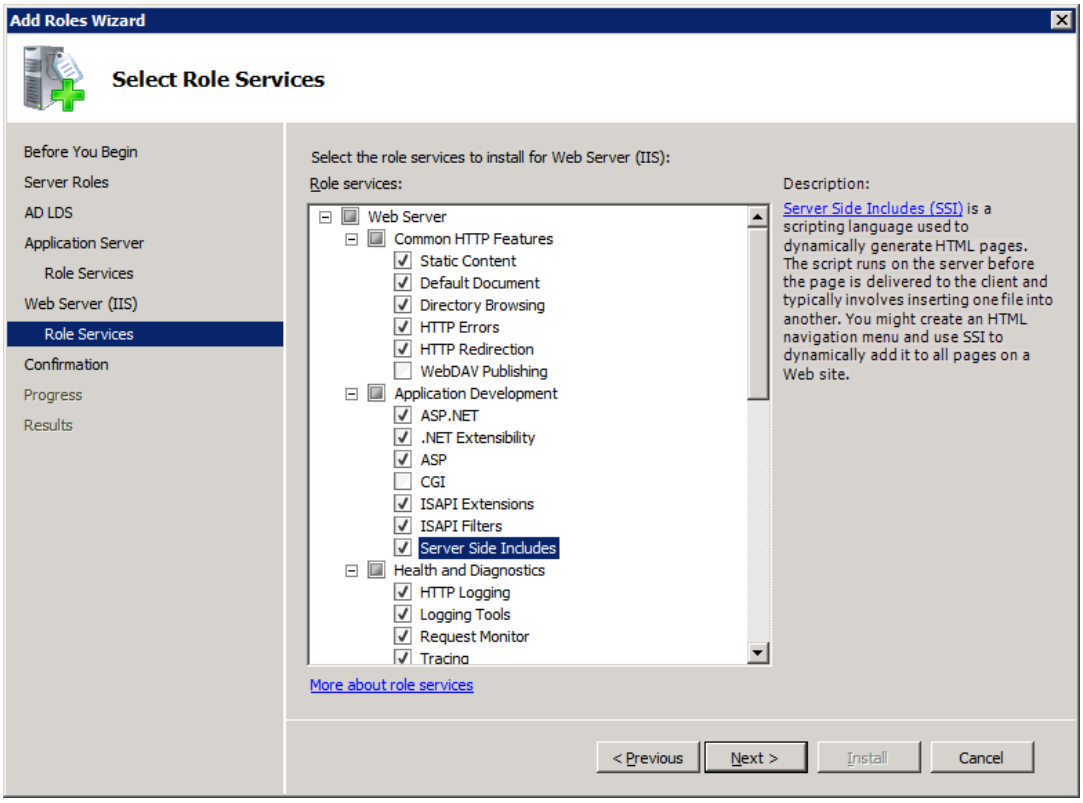
- Static Content
- Default Document
- Directory Browsing
- HTTP Errors
- HTTP Redirection

Attention: Clear the check boxes for all other services.

15 On the **Select Role Services** page, under **Application Development**, select the following services:

- ASP.NET
- .NET Extensibility
- ASP
- ISAPI Extensions
- ISAPI Filters
- Server Side Includes

Attention: Clear the check boxes for all other services.



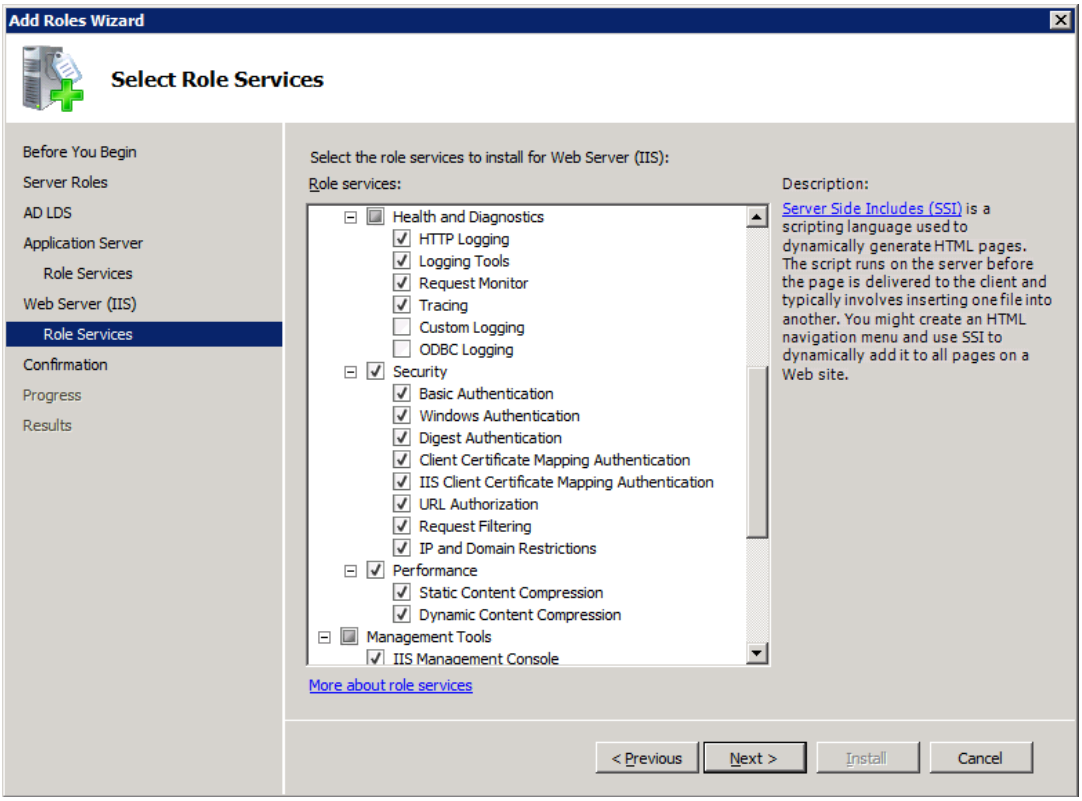
16 On the **Select Role Services** page, under **Health and Diagnosis**, select the following services:

- HTTP Logging
- Logging Tools
- Request Monitor
- Tracing

Attention: Clear the check boxes for all other services.

17 On the **Select Role Services** page, under **Security**, select all services.

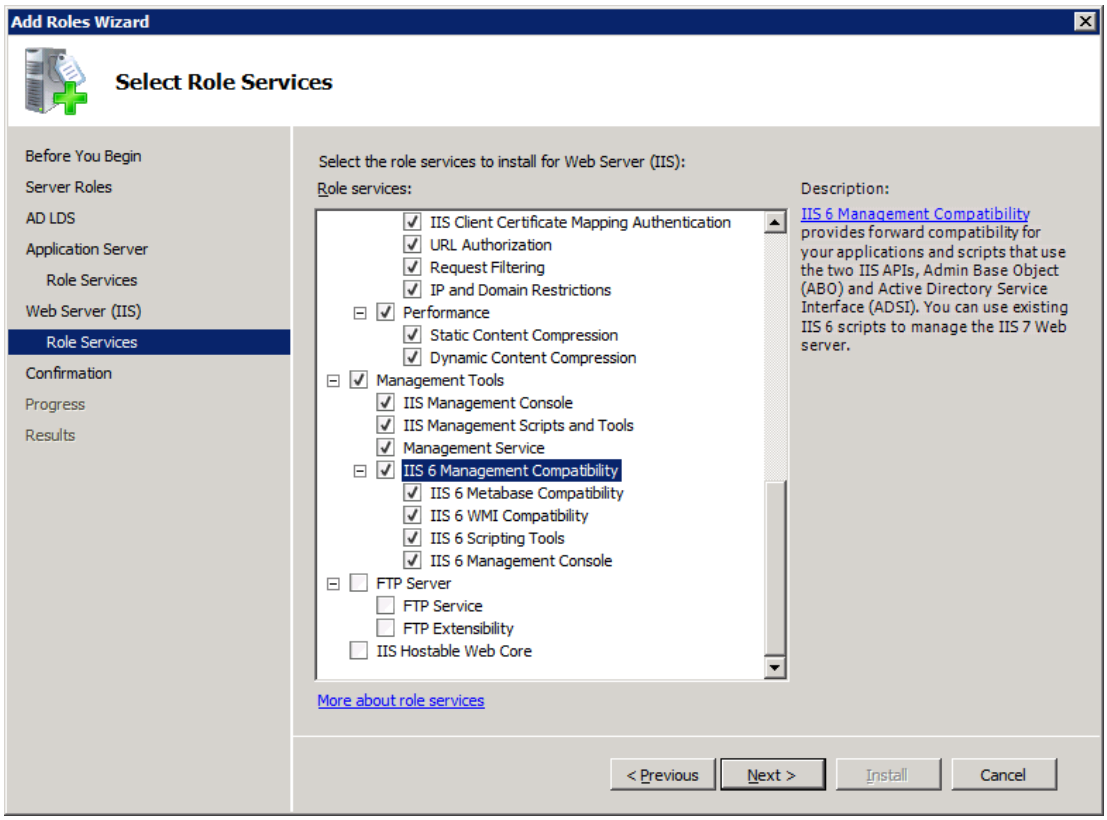
18 On the **Select Role Services** page, under **Performance**, select all services.



19 On the **Select Role Services** page, under **Management Tools**, select the following services:

- IIS Management Console
- IIS Management Scripts and Tools
- Management Service
- All items under IIS 6 Management Compatibility

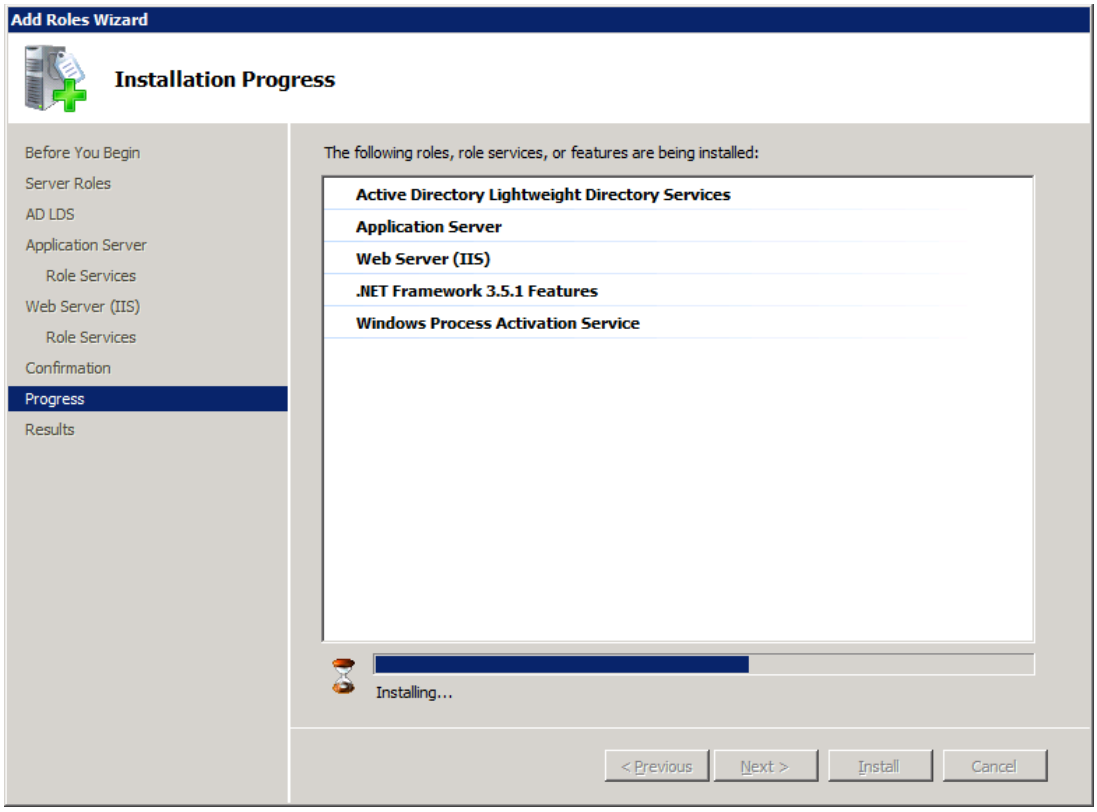
Attention: Clear the check boxes for all other services.



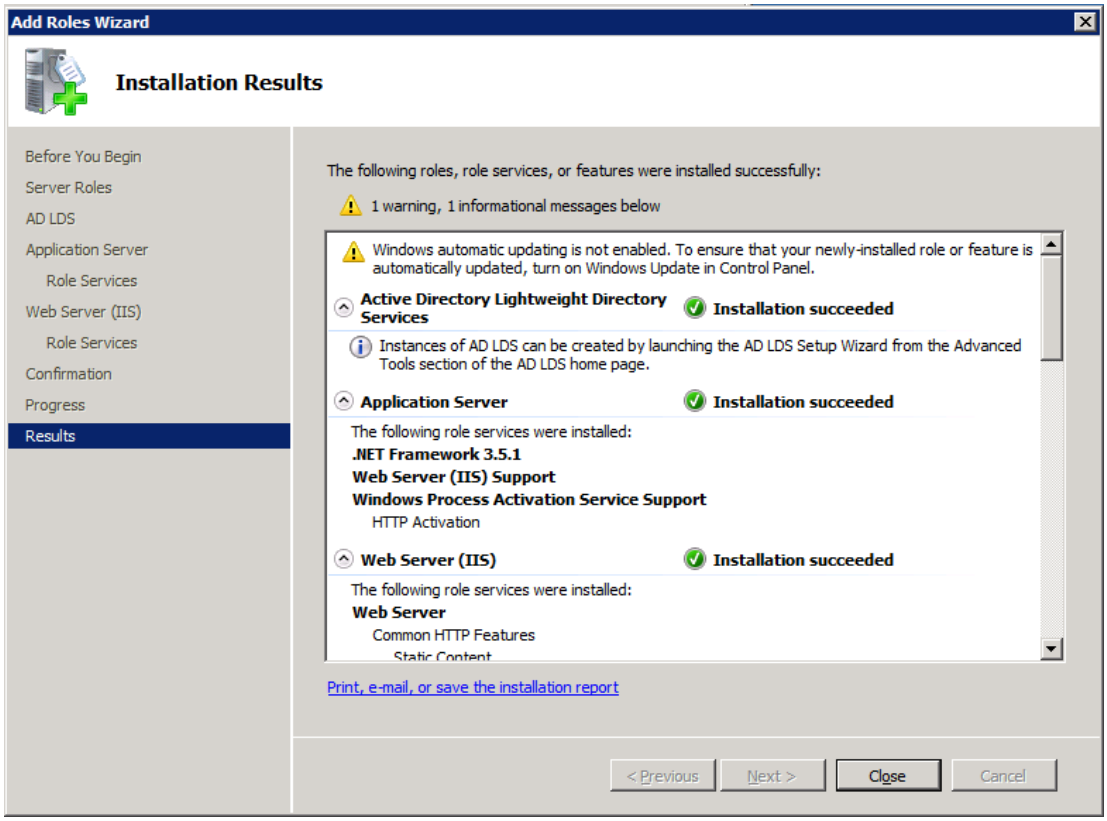
20 Click **Next**.

21 Review the installation information.

22 Click **Install**.



23 On the **Installation Results** page, click **Close**.



24 Restart the server if required.

--End--

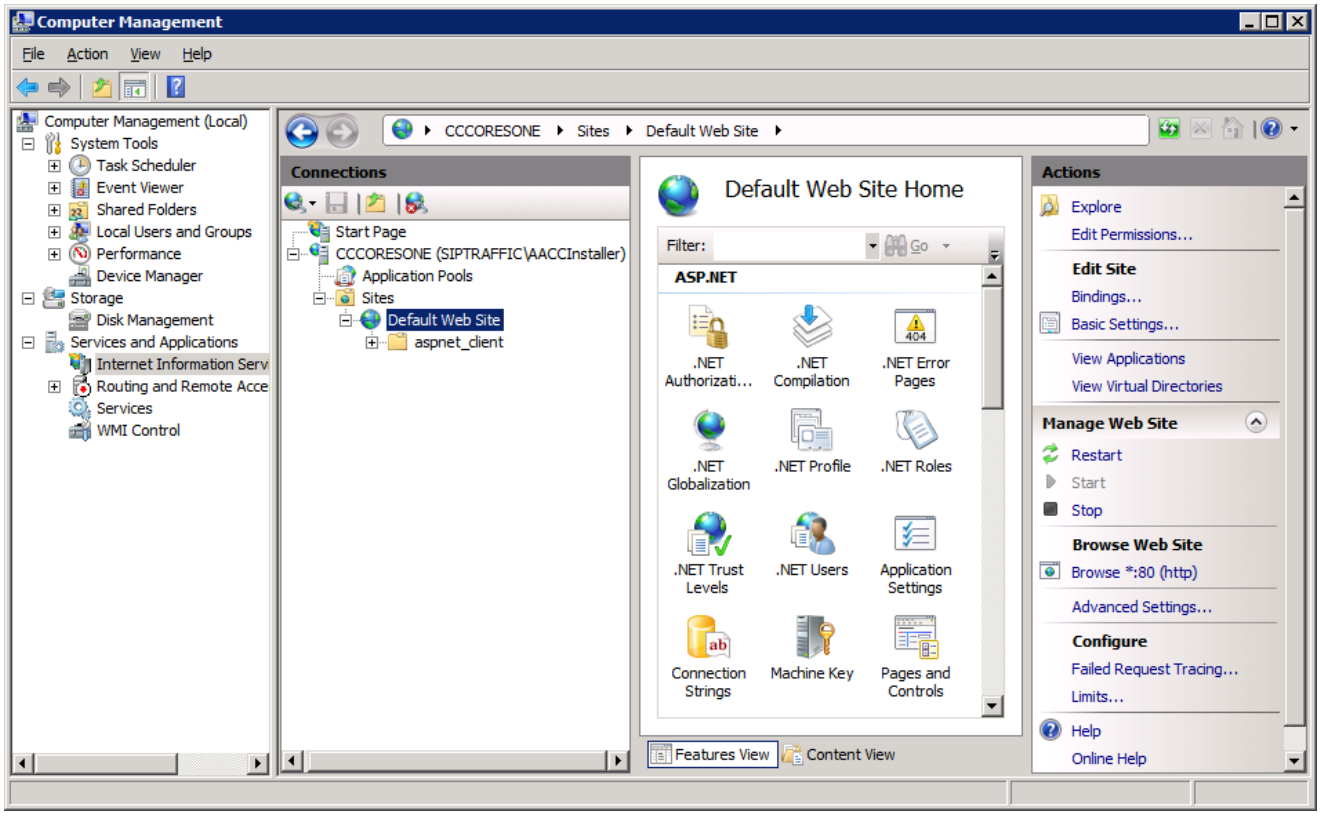
Configuring MIME types to support Microsoft updates

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

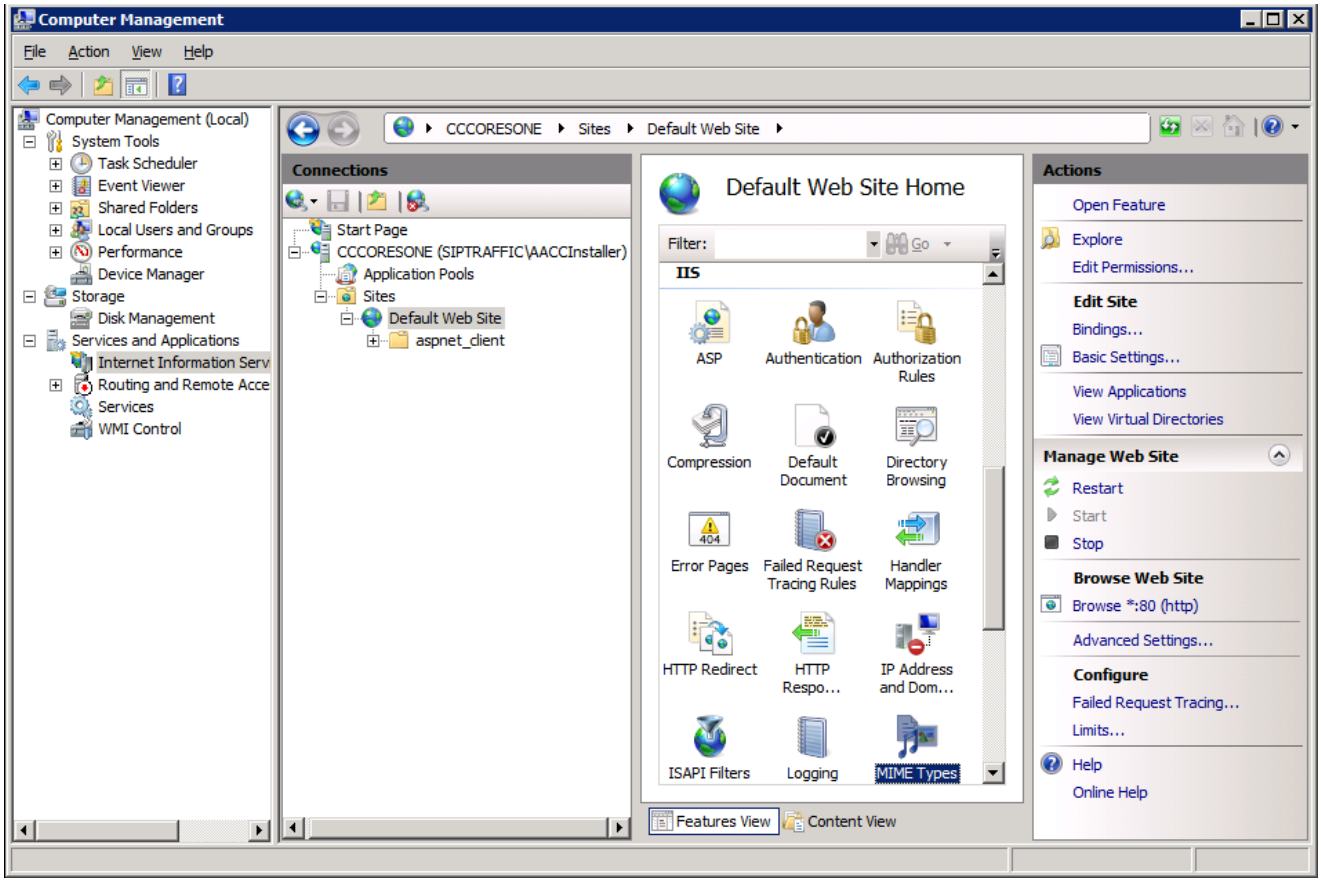
Procedure steps

Step	Action
1	Log on to the Contact Center server using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
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 the default site, for example **CCCORESONE**, **Sites**, **Default Web Site**.

5 Select **Default Web Site**.



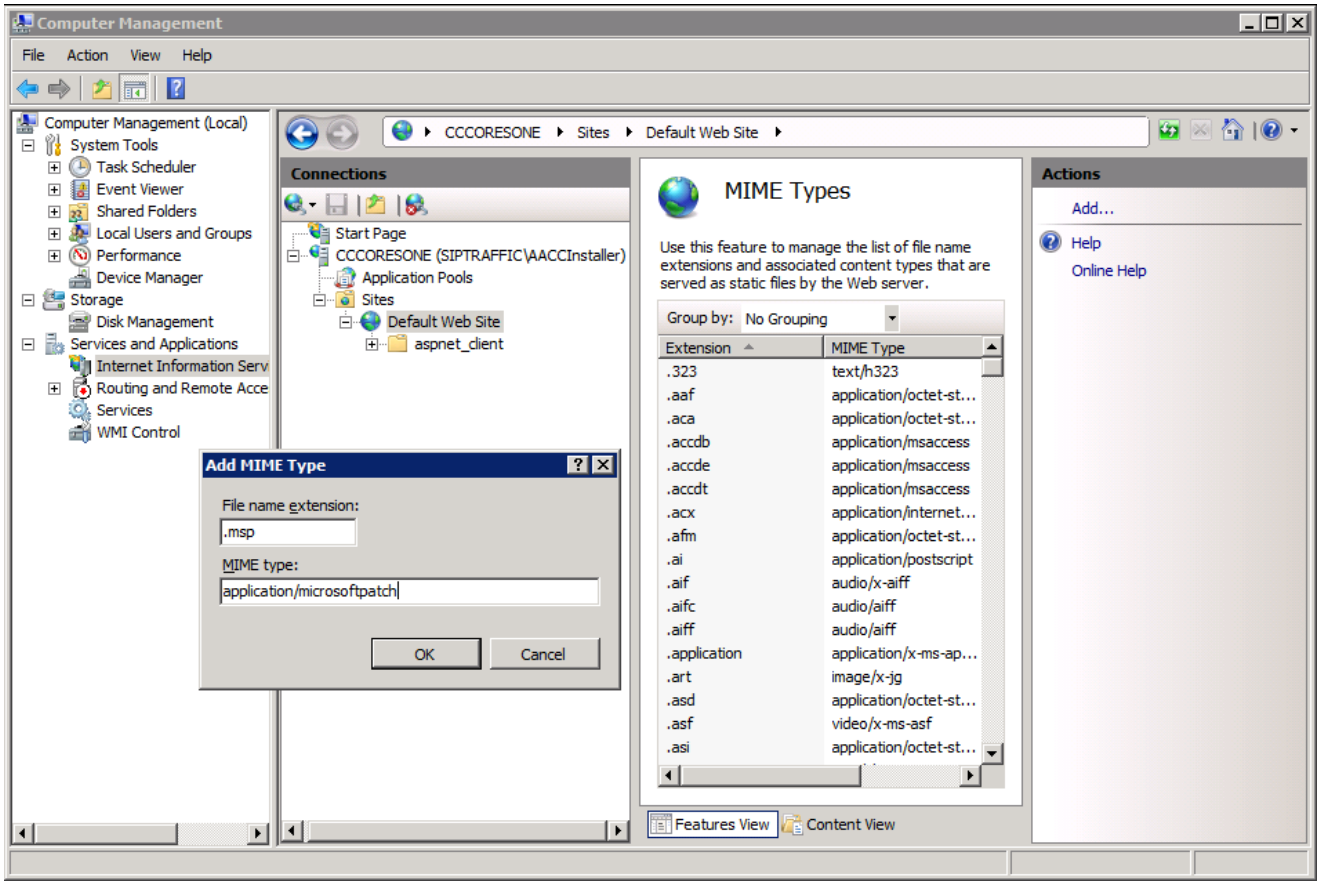
6 In the **Default Web Site Home** pane, under **IIS**, double-click **MIME Types**.



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**.

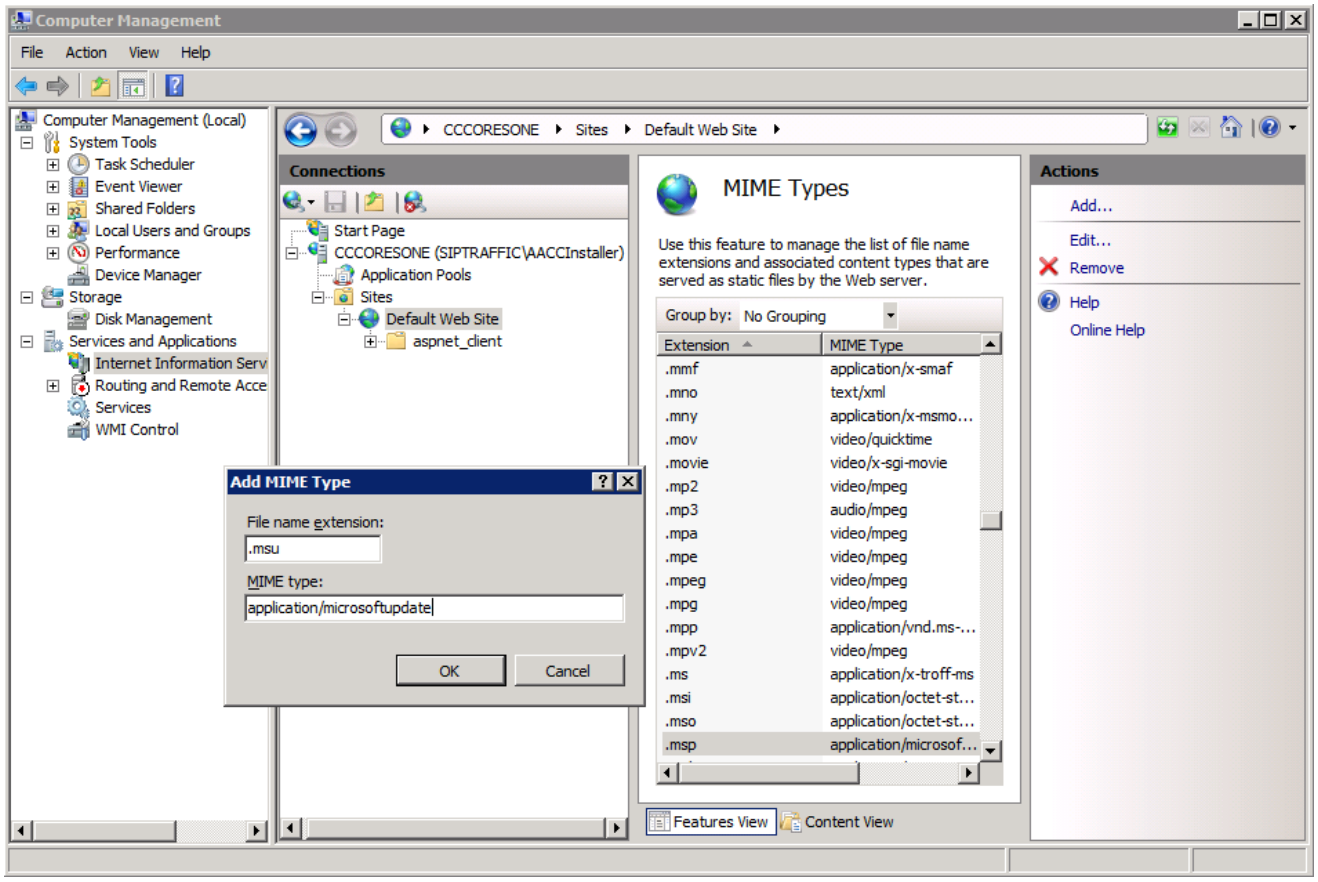


10 Click **OK**.

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**.

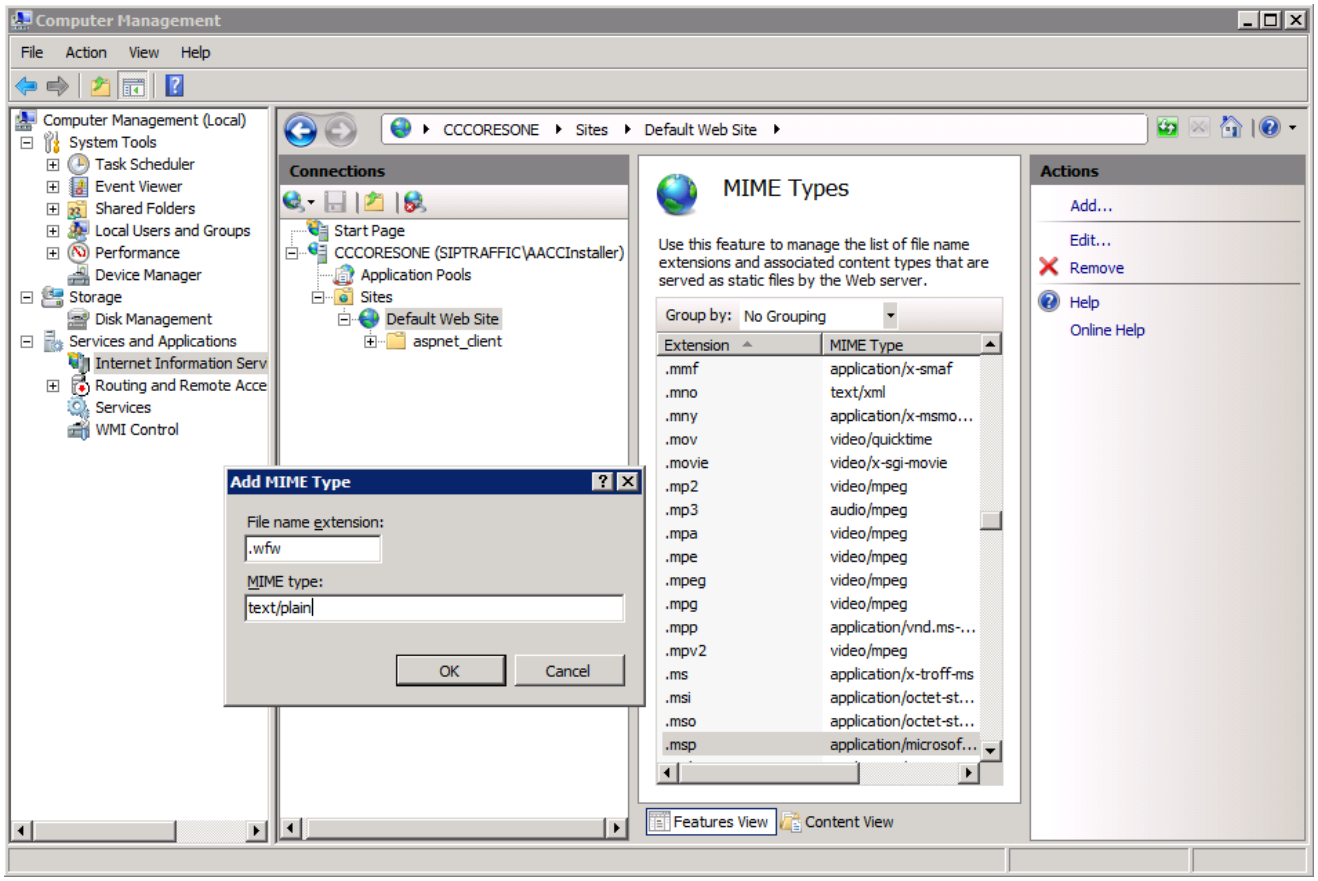


14 Click **OK**.

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.

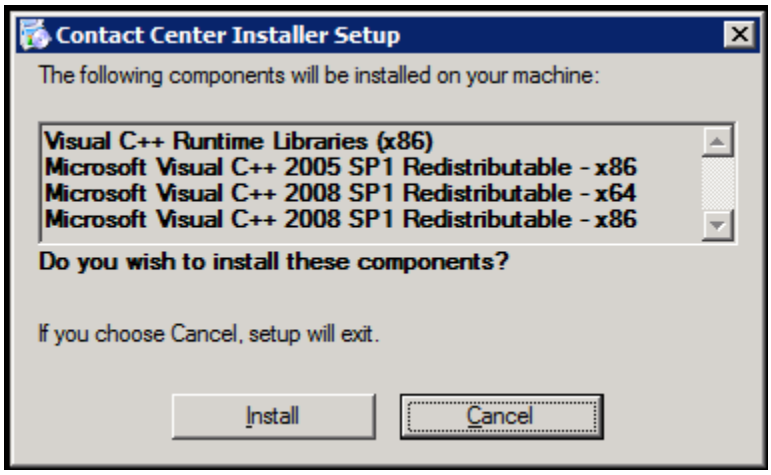
--End--

Installing the server software on the co-resident server

Install the Contact Center software and enable your contact center to route contacts.

Procedure steps

Step	Action
1	Log on to the Contact Center server using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
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.

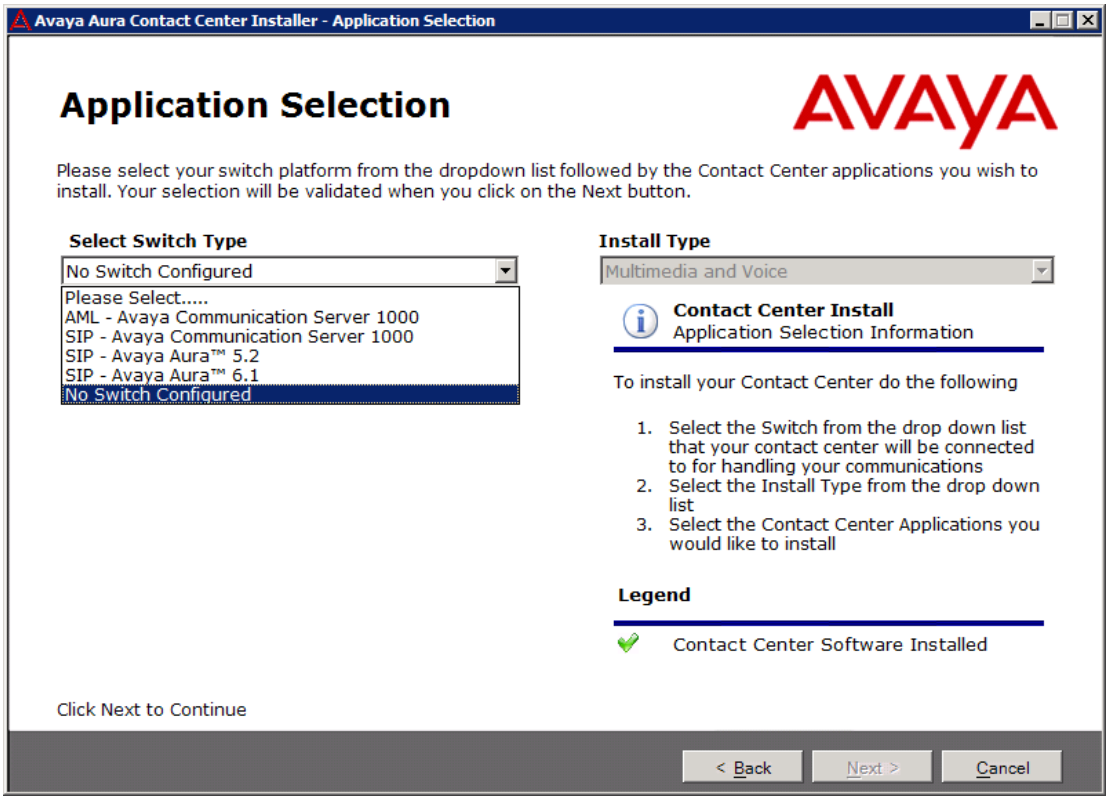
5 On the **Welcome** window, click **Next**.

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 **Application Selection** window, from the **Select Switch Type** list, select **No Switch Configured**.



10 Under **Contact Center Manager Server (CCMS)**, select **Nodal Server**.

In addition to installing Contact Center Manager Server, this selection installs the Open Queue Open Interface, the Open Networking Open Interface, and Multiplicity, which you can license and configure at a later time.

11 Under **Communication Control Toolkit (CCT)**, select **Contact Center Feature Set**.

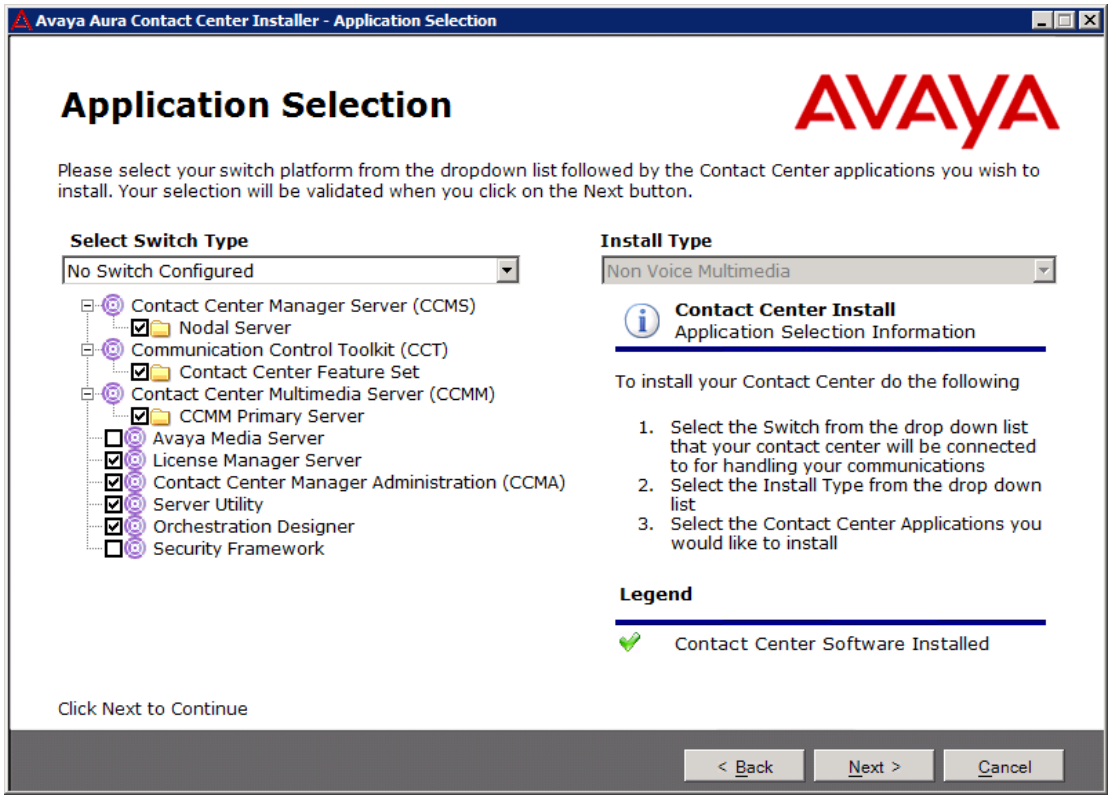
12 Under **Contact Center Multimedia Server (CCMM)**, select **CCMM Primary Server**.

13 Select **License Manager Server**.

14 Select **Contact Center Manager Administration (CCMA)**.

15 Select **Server Utility**.

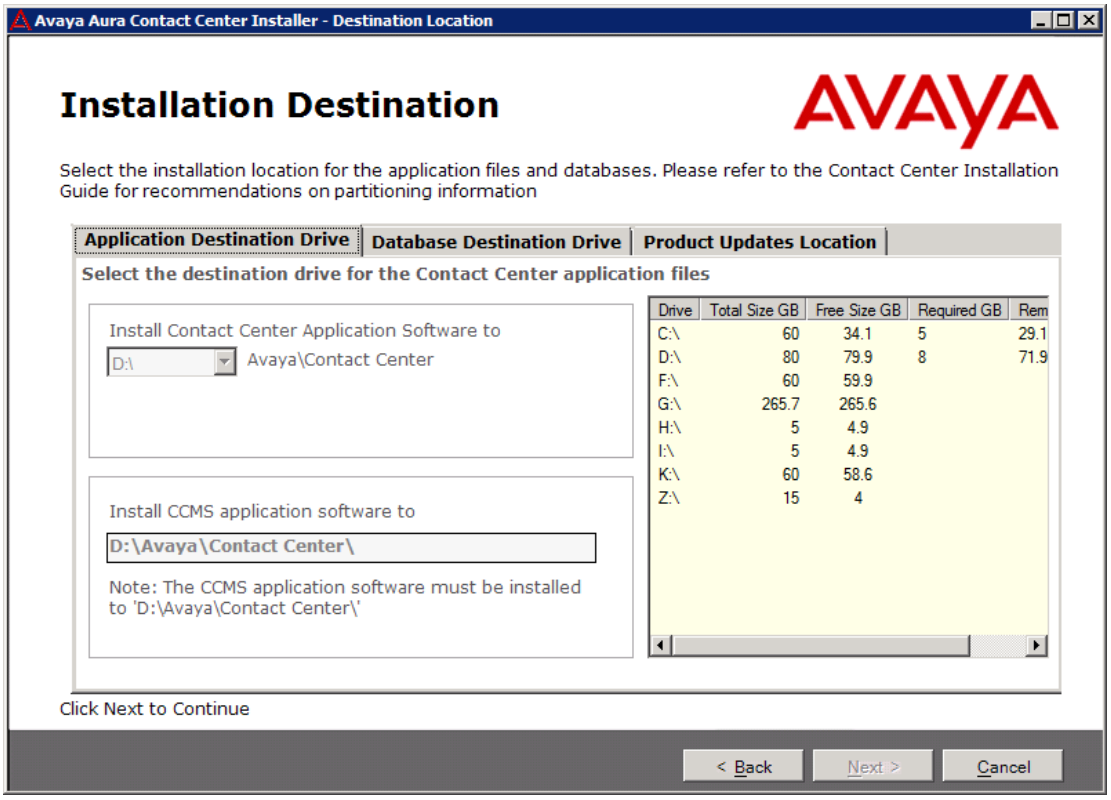
16 Select **Orchestration Designer**.



17 Click **Next**.

18 On the **Product Data Upgrade** window, click **Next**.

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

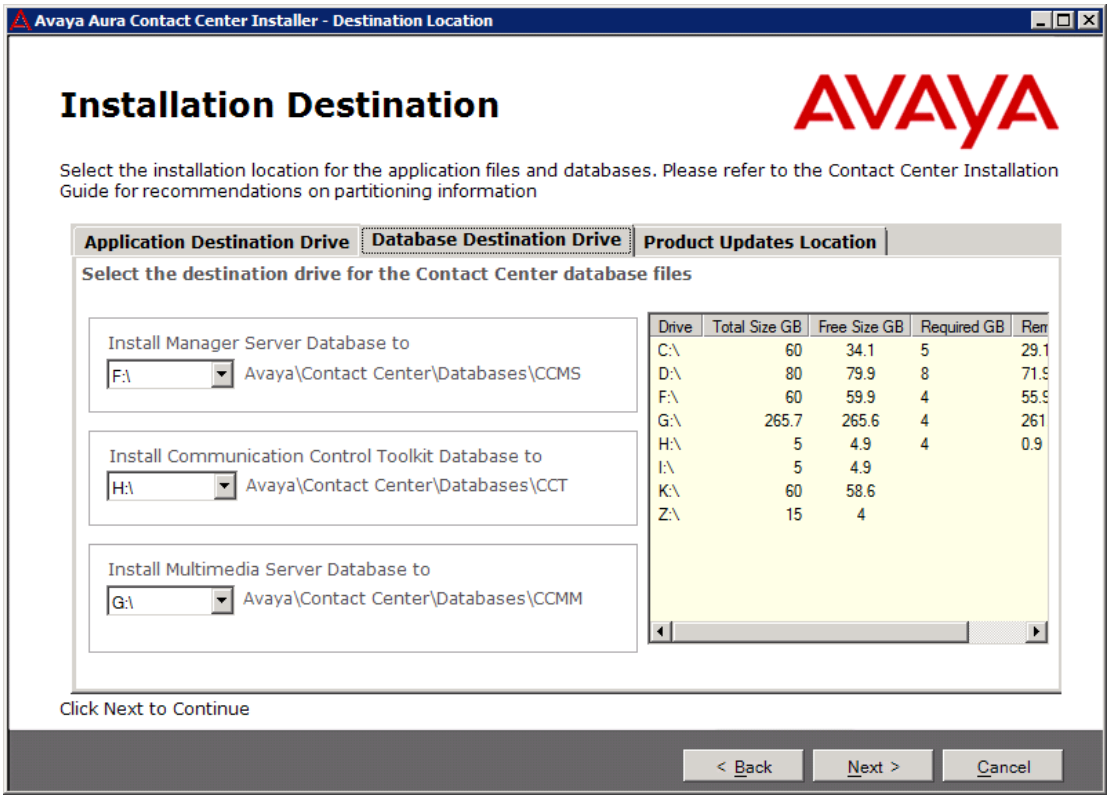


20 Select the **Database Destination Drive** tab.

21 From the **Install Manager Server Database to** list, select **F:**.

22 From the **Install Communication Control Toolkit Database to** list, select **H:**.

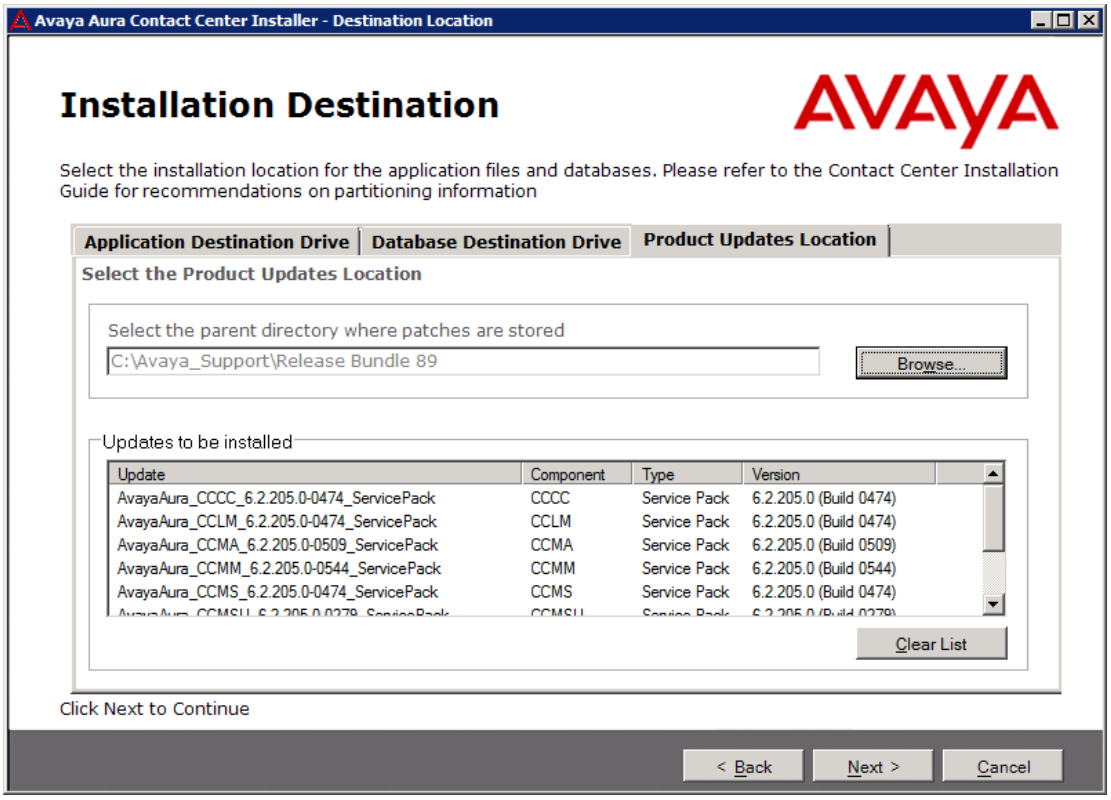
23 From the **Install Multimedia Server Database to** list, select **G:**.



24 Select the **Product Updates Location** tab.

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

26 Select the support directory you created, for example **C:\Avaya_Support**.

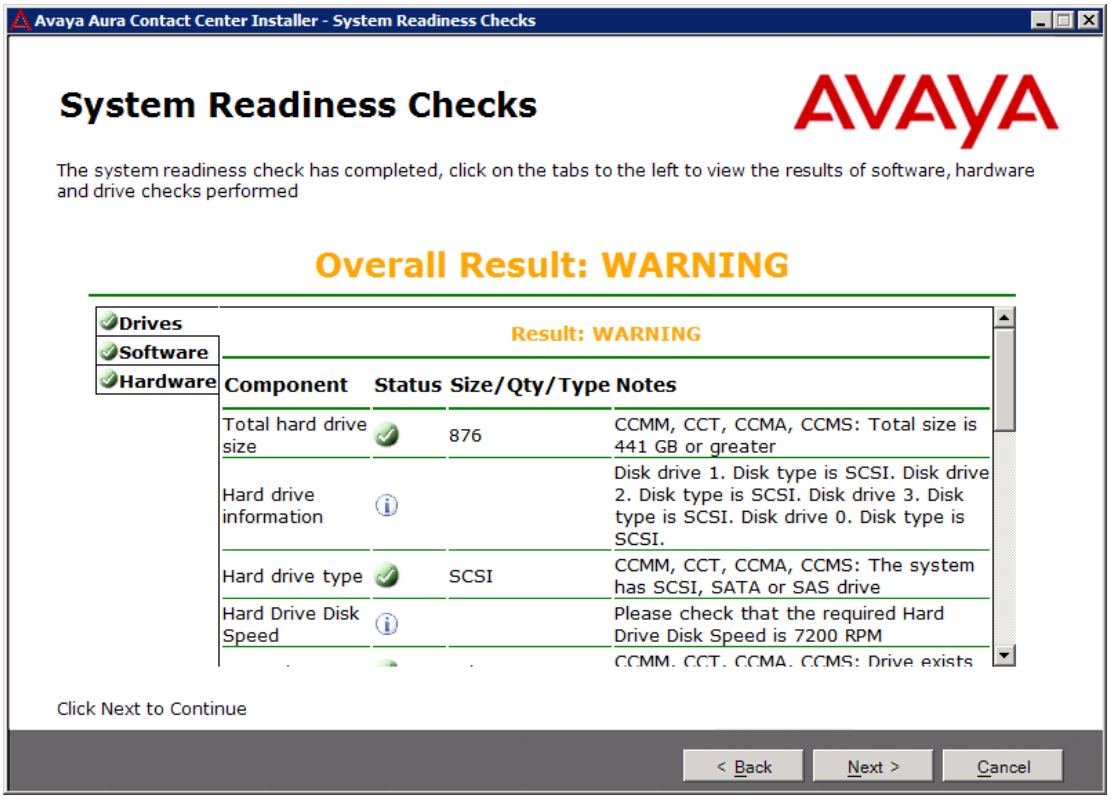


27 Click **Next**.

The System Readiness Check runs on the server.

28 If you have followed the previous instructions in this guide, and the server hardware meets the specifications in the *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210) 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.



29 Click **Next**.

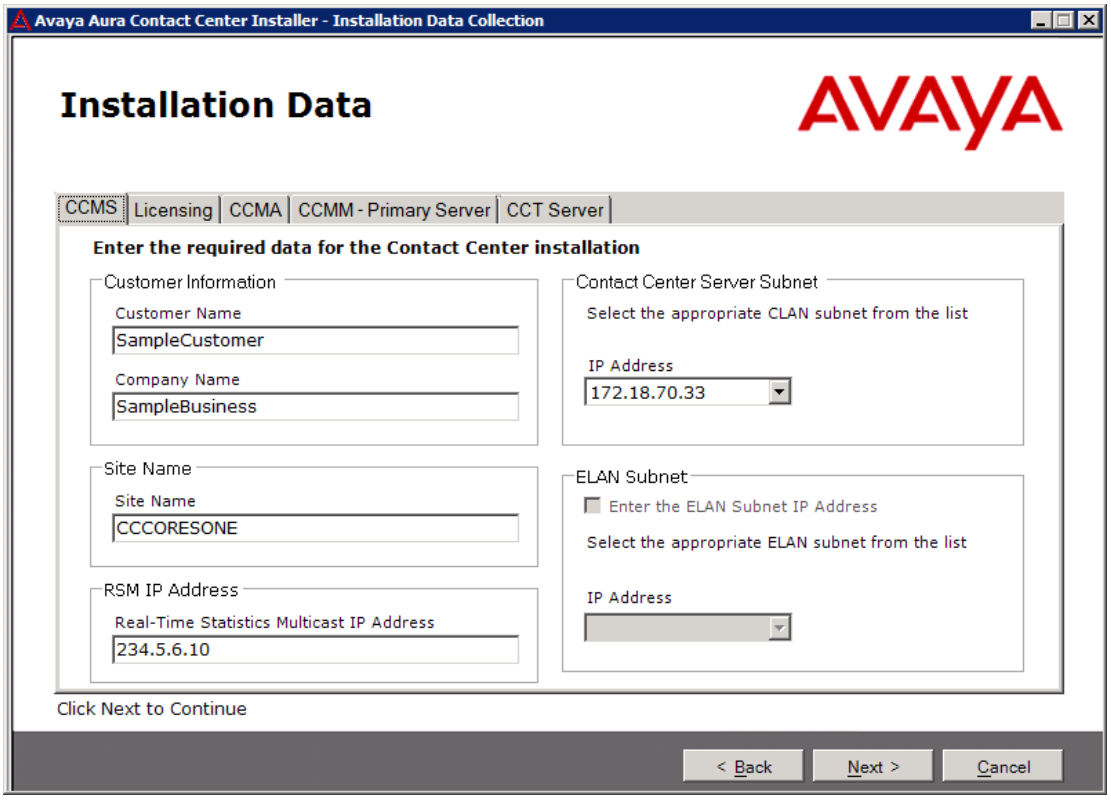
30 On the **Installation Data** window, select the **CCMS** tab. Complete the fields as follows:

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

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

Site Name — Type a site name for CCMS, for example **CC_ELITESITE**.

Contact Center Server Subnet IP Address — Select the Cores server IP address, for example **172.18.70.33**.



31 Select the **Licensing** tab.

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

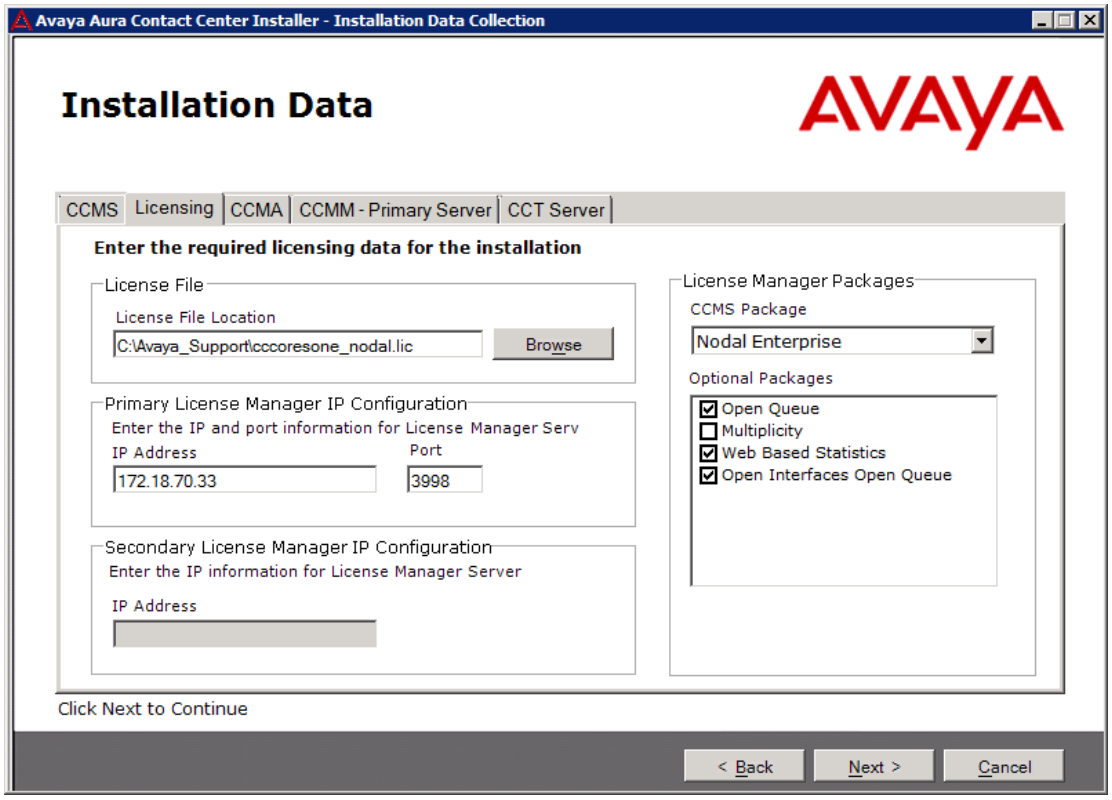
License File Location — Use the Browse button to find and select the license file that you downloaded to the server.

IP Address — The IP address of the license server, in this case the co-resident server itself, for example **172.18.70.33**.

Port — Accept the default port, **3998**.

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

Optional Packages — Select **Open Queue**, **Web Based Statistics**, and **Open Interfaces Open Queue**.



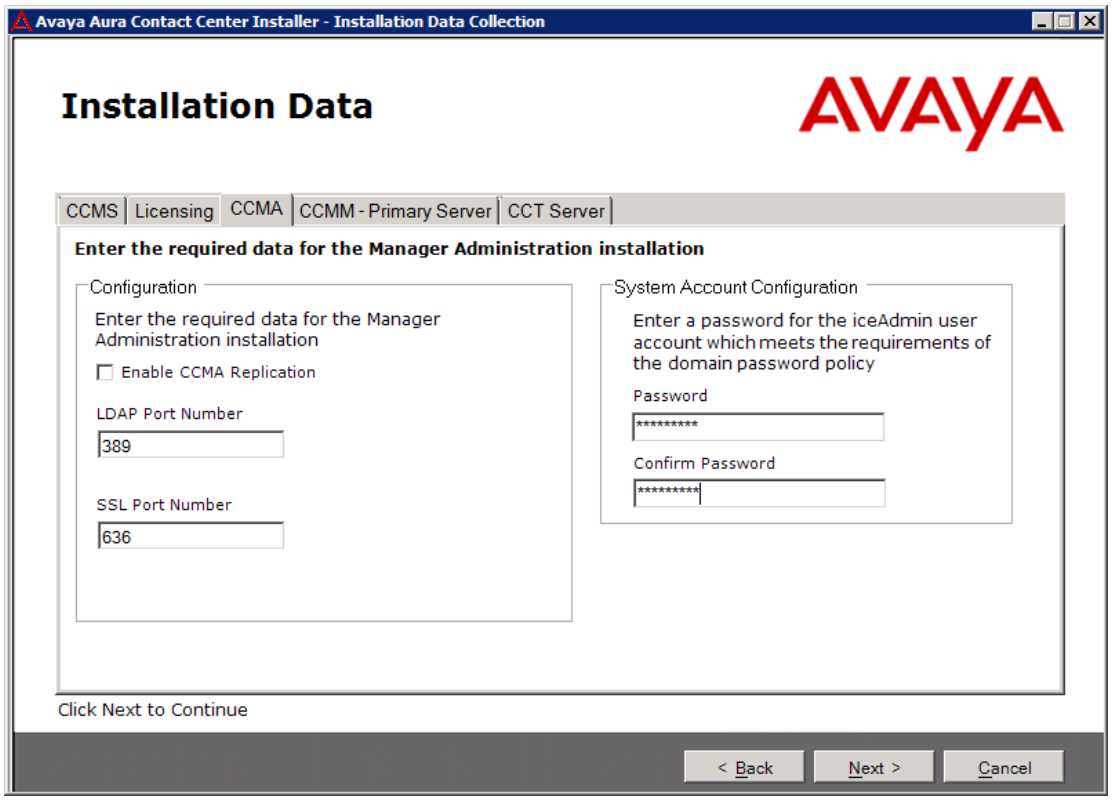
33 Select the **CCMA** tab.

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

Configuration - Enable CCMA Replication — Attention!: leave this box clear, you select this only when you set up the CCMA standby server.

System Account Configuration - Password — Type the password for the CCMA System Account (iceAdmin), for example ICEpassw1.
Attention! The password must conform to your domain password policy.

System Account Configuration - Confirm Password — Type the password for the CCMA System Account (iceAdmin), for example ICEpassw1.



35 Select the **CCMM - Primary Server** tab.

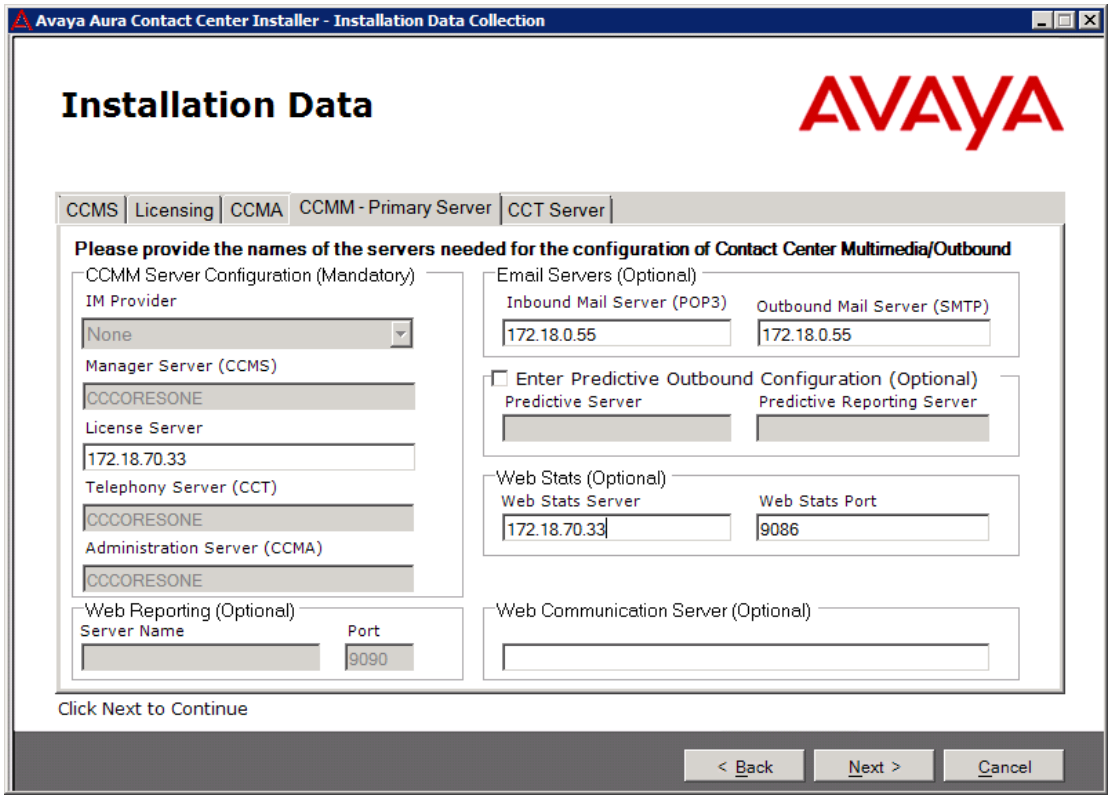
36 Complete the **CCMM - Primary Server** tab fields as follows:

License Server — Type the IP address of the License server, for example **172.18.70.33**.

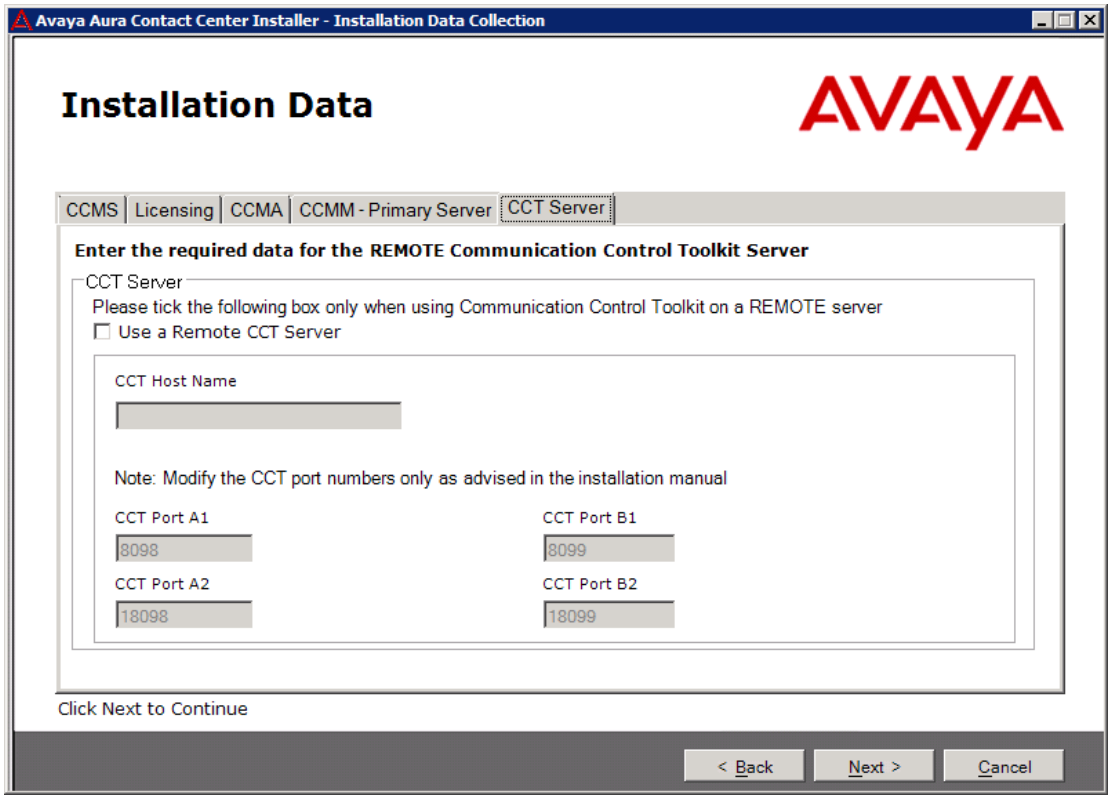
Inbound mail server (POP3) — Type the IP address of the e-mail server, for example **172.18.0.55**.

Outbound mail server (SMTP) — Type the IP address of the e-mail server, for example **172.18.0.55**.

Web Stats Server (Optional) — Type the IP address of the web statistics server, for example **172.18.70.33**.

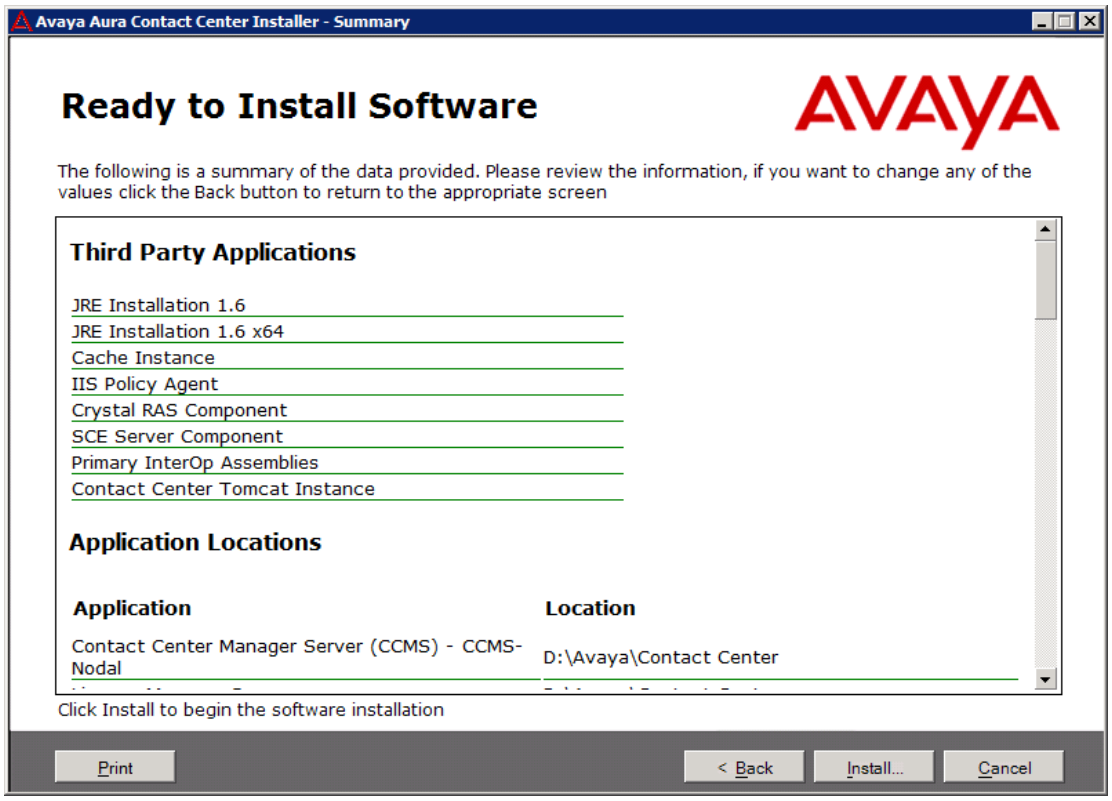


37 On the **Installation Data** window, in the **CCT Server** tab, you do not complete any configuration:



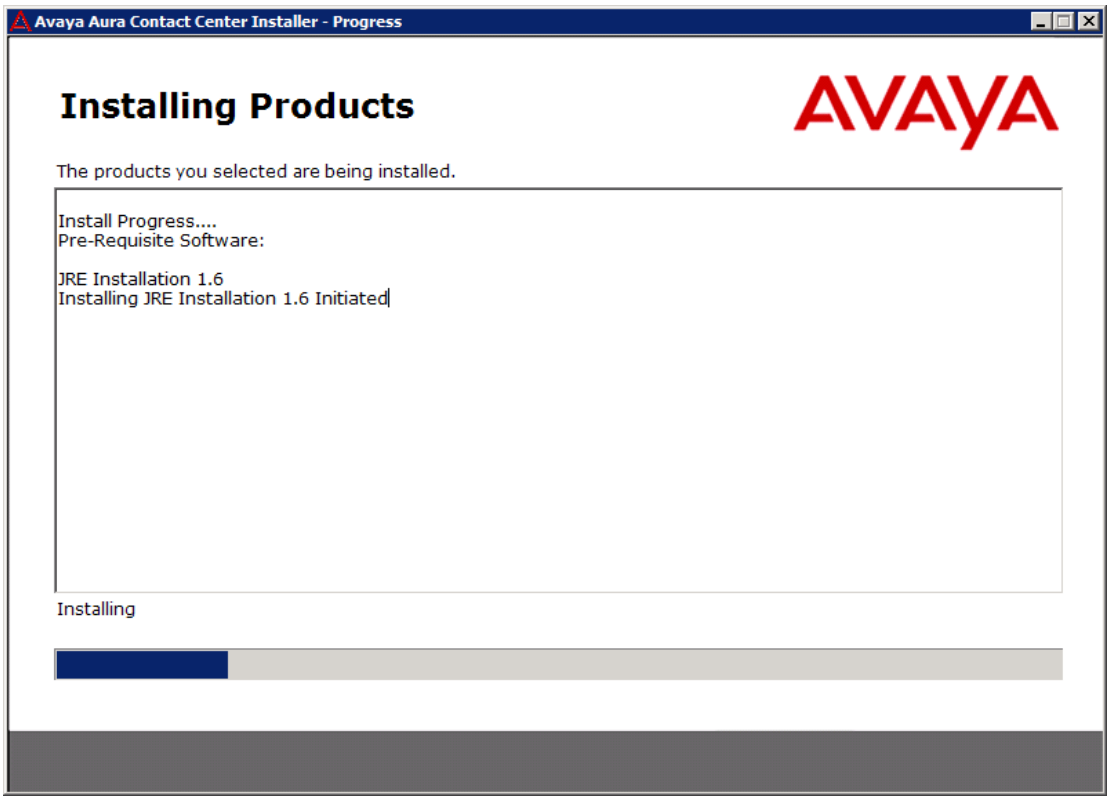
38 Click **Next**.

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



40 Click **Install**.

The system displays the Installing Products window, which updates you on the progress of the install.



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

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

43 After the server restarts, disable Java Runtime Environment (JRE) updates. See Disabling Java Runtime Environment updates on the co-resident server (page 93).

Attention: Updating to an unsupported version of JRE can cause the contact center to cease operation and may require the reinstallation of the contact center server.

--End--

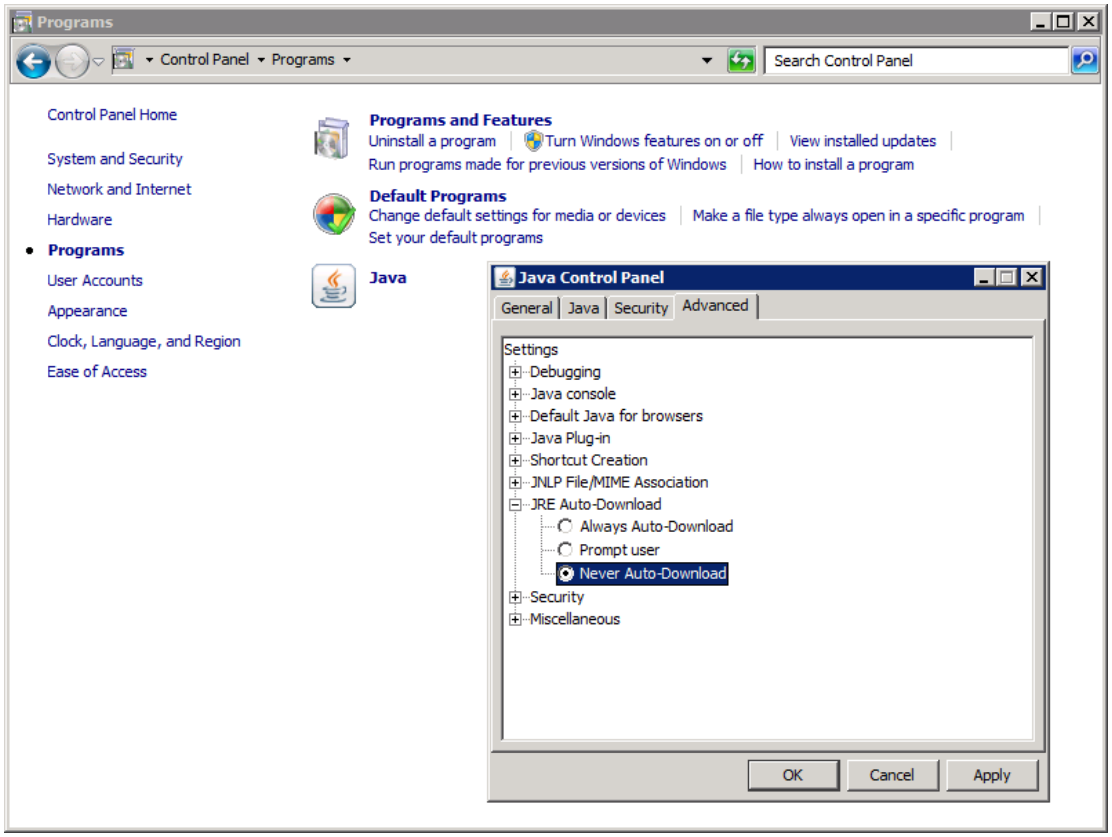
Disabling Java Runtime Environment updates on the co-resident server

Contact Center supports only specific versions of Java Runtime Environment (JRE). The Contact Center installer installs a supported JRE version, and Contact Center service packs install any required JRE updates. It is important that you disable JRE automatic updating in the Windows Control Panel on all contact center servers.

Attention: Updating to an unsupported version of JRE can cause the contact center to cease operation and may require the complete reinstallation of the contact center server.

Procedure steps

Step	Action
1	Log on to the Contact Center server using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Choose **Start**, **Control Panel**, **Programs**, **Java**.
3	On the **Java Control Panel**, select the **Advanced** tab.
4	Expand **JRE Auto-Download**.
5	Select **Never Auto-Download**.



6 Click **OK**.

--End--

Post-install Contact Center Server Commissioning

This chapter contains the procedures you must perform on the Primary Contact Center after installing the Contact Center applications.

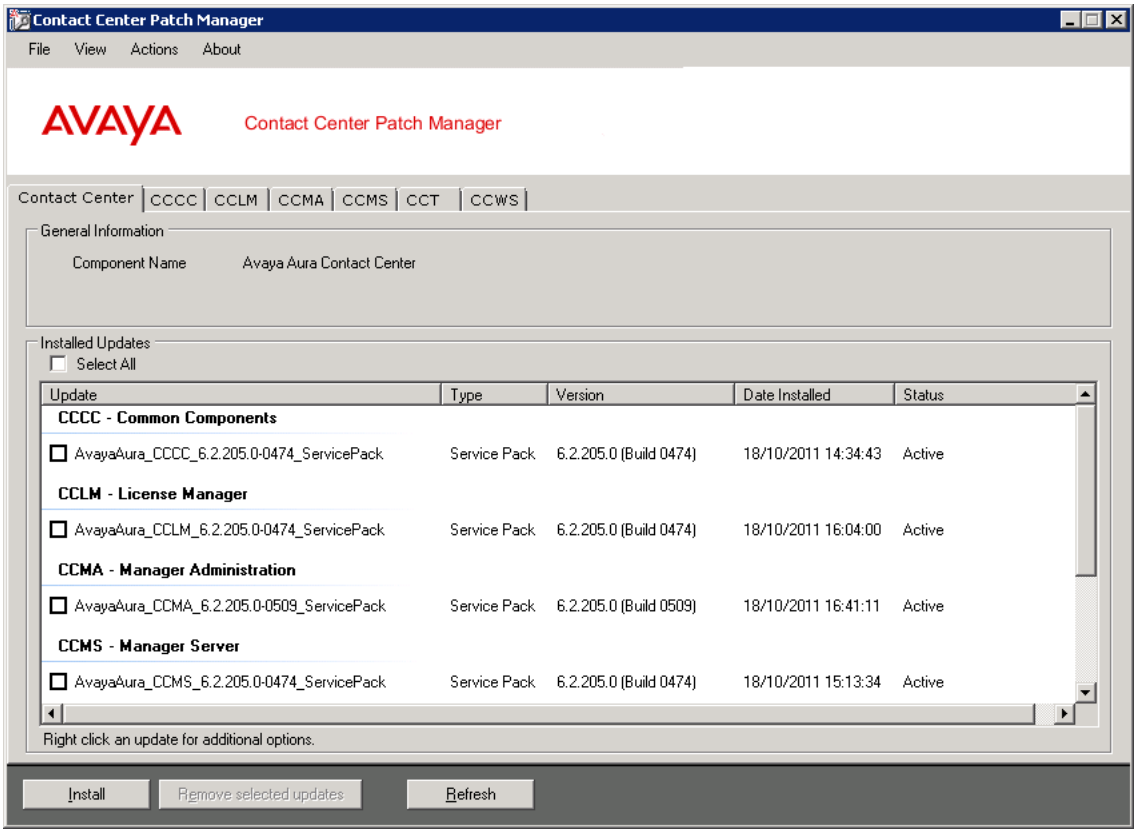
Applying Post-installation Patches

This is a general procedure for applying Contact Center patches after the initial installation. The Contact Center installer allows application only of service packs as part of the install.

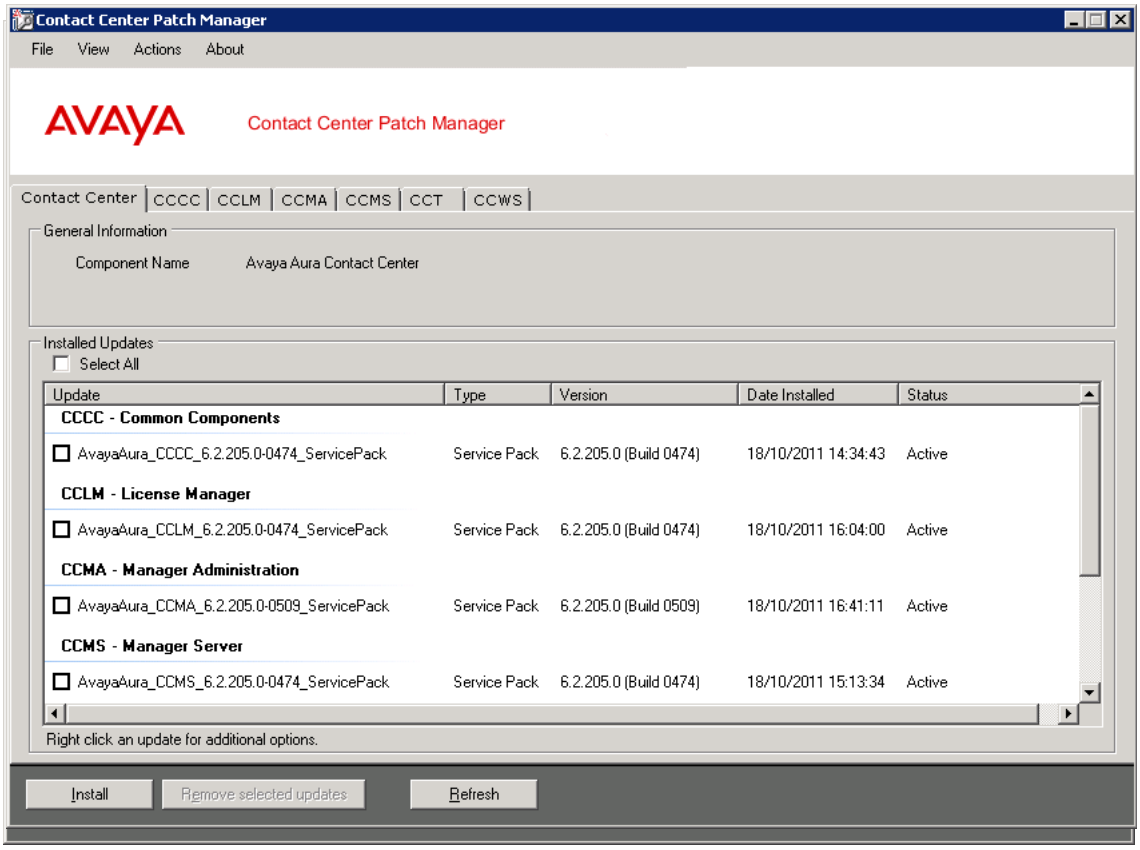
Attention: You must carefully review the README files for each patch you download. The precise steps for installation vary from patch to patch. For example, most patches require you to shut down Contact Center before application, but some do not. There can also be dependencies on the order of installation of patches.

Procedure steps

Step	Action
1	Log on to the Contact Center server using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Browse www.avaya.com/support to find the latest patches (if any) for Contact Center.
3	Download the patches to a folder on the Contact Center server, for example **C:\ Avaya_Support**.
4	Carefully review the patch README file(s) to determine installation pre-conditions and the order (if any) in which to apply them.
5	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Common Utilities**, **System Control and Monitor Utility**.
6	If required for the patches you are installing, click **Shut down Contact Center**.
7	Exit the System Control and Monitor Utility.
8	Click **Start, All Programs, Avaya, Contact Center, Common Utilities, Contact Center Patch Manager**.



9 Select **Actions, Install**.

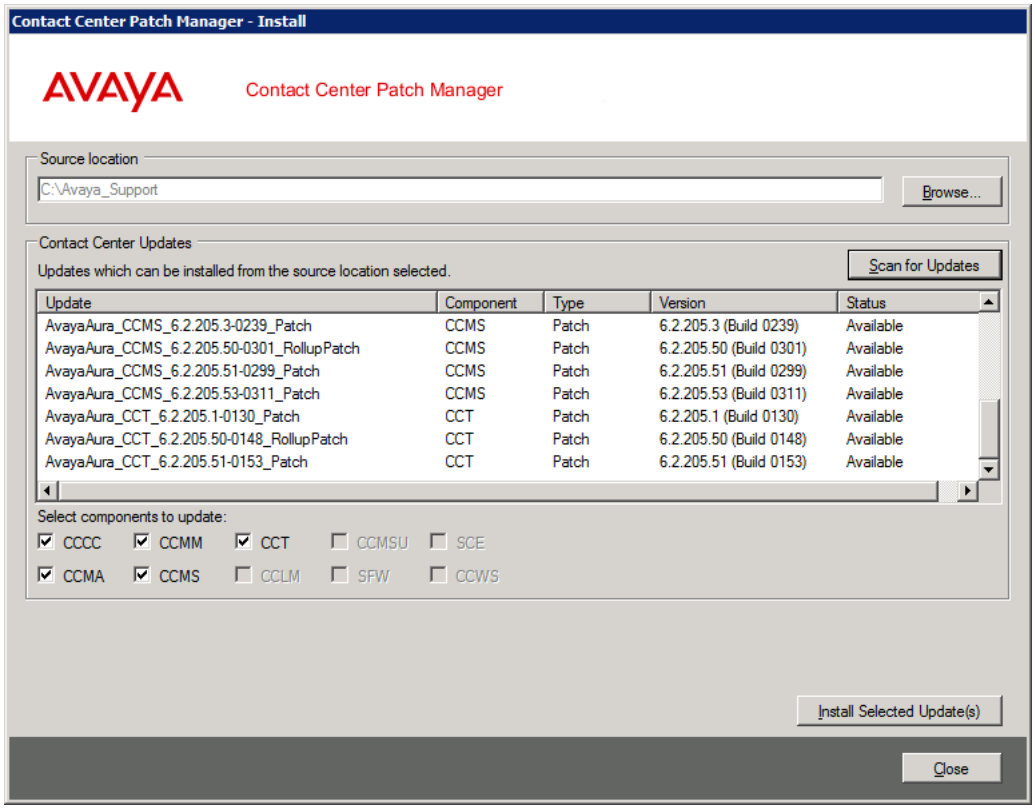


10 Click **Browse** and navigate to the folder where you have downloaded the patches, for example **C:\Avaya_Support**.

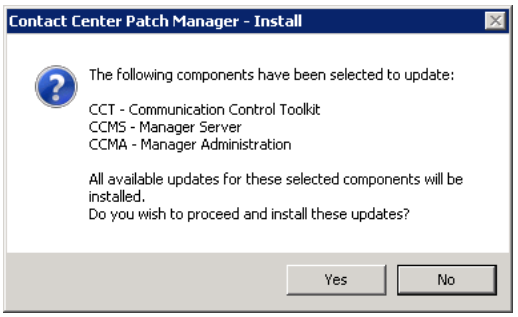
11 Click **Scan for Updates**.

The Contact Center Updates section displays the available patches.

12 Select the patches that you downloaded and extracted.



13 Click **Install Selected Updates**.



14 Click **Yes**.

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

15 Click **Close**.

16 Verify that the newly installed patch appears under **Installed Updates**.

--End--

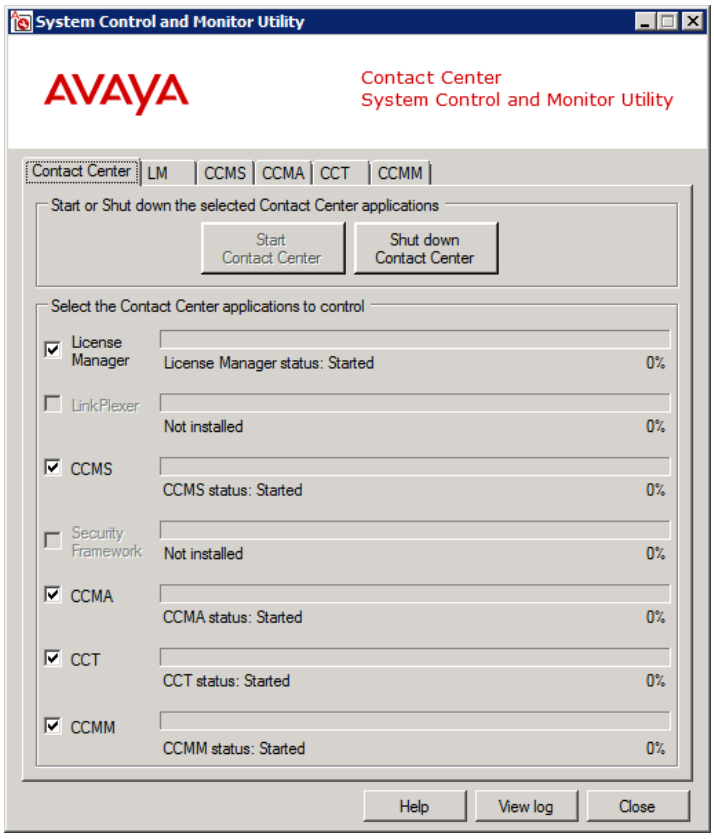
Confirming that the Contact Center services start

Confirm that all appropriate Contact Center Manager Server services start on the Contact Center Manager Server.

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

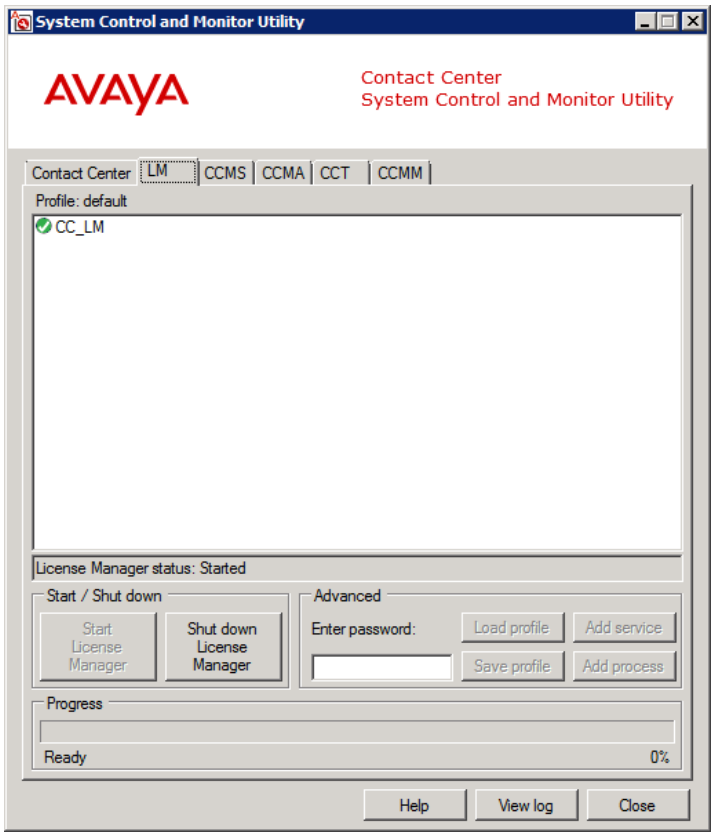
Procedure steps

Step	Action
1	Log on to the Contact Center server using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Common Utilities**, **System Control and Monitor Utility**.
3	Click the **Contact Center** tab.
4	Check that the following applications show a status of **Started**. License Manager CCMS CCMA CCT CCMM



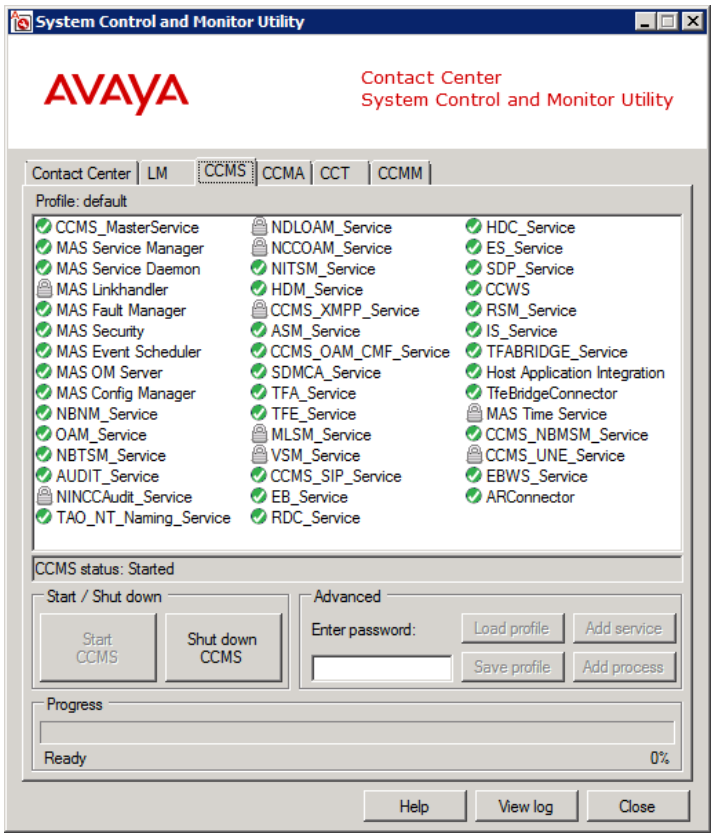
5 Click the **LM** tab.

6 Ensure that the CC_LM service in the **Profile** box has a green circle next to it.



7 Click the **CCMS** tab.

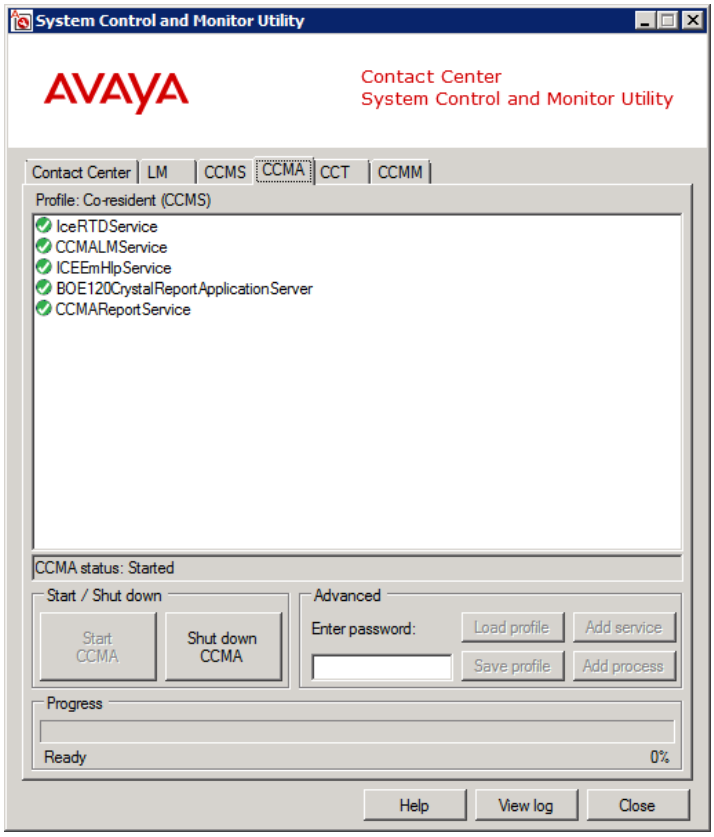
8 Ensure that all licensed services in the **Profile** box have a green circle next to them. (Unlicensed services show a lock icon; these do not require any action.)



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

10 Select the **CCMA** tab.

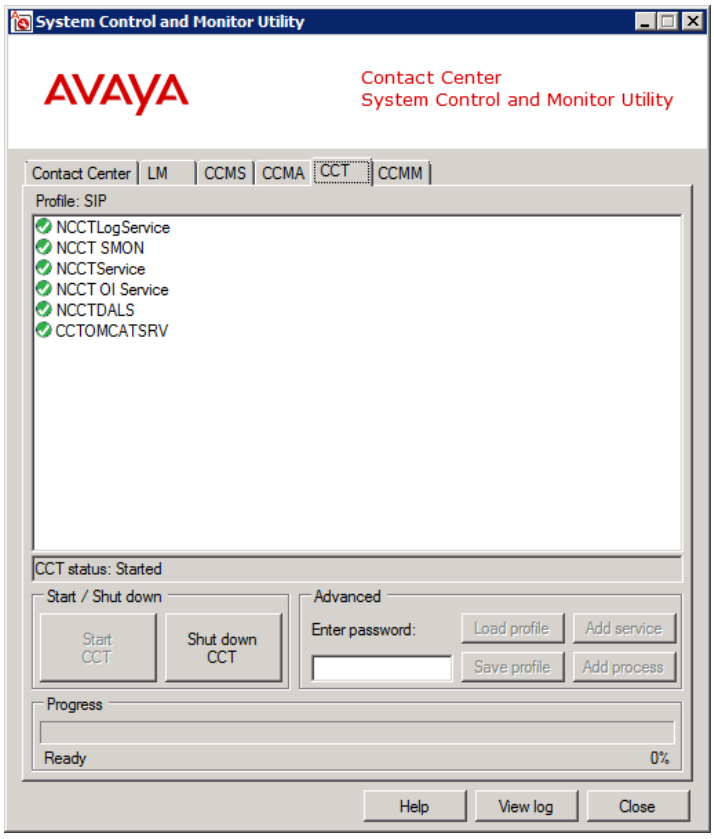
11 Confirm that the Contact Center Manager Administration services are running.



12 If a Contact Center Manager Administration service is not running, re-start CCMA.

13 Select the **CCT** tab.

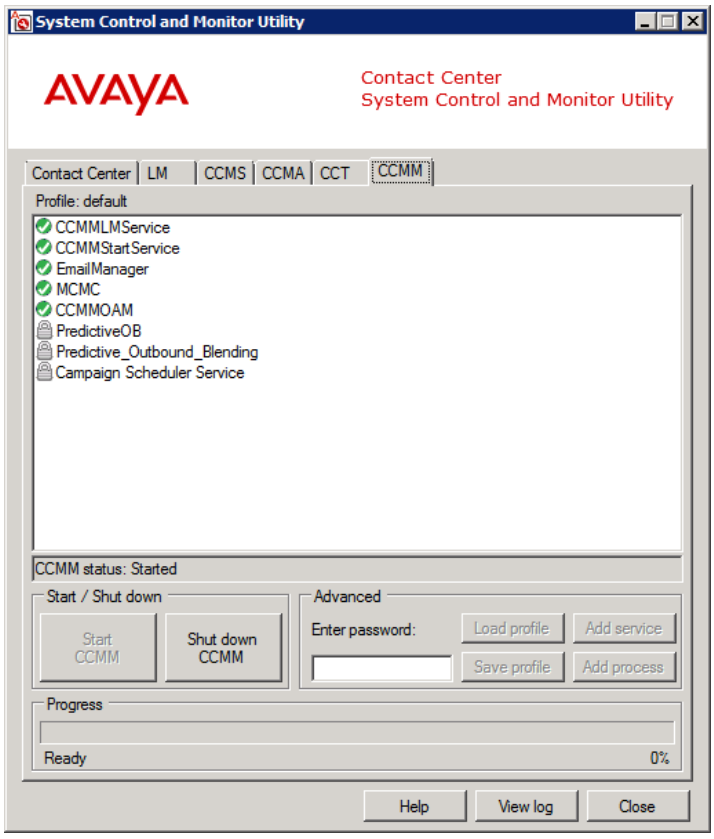
14 Confirm that the Communication Control Toolkit services are running.



15 If a Communication Control Toolkit service is not running, re-start CCT.

16 Select the **CCMM** tab.

17 Confirm that the Contact Center Multimedia services are running.



18 If a Contact Center Multimedia service is not running, re-start CCMM.

19 Click **Close**.

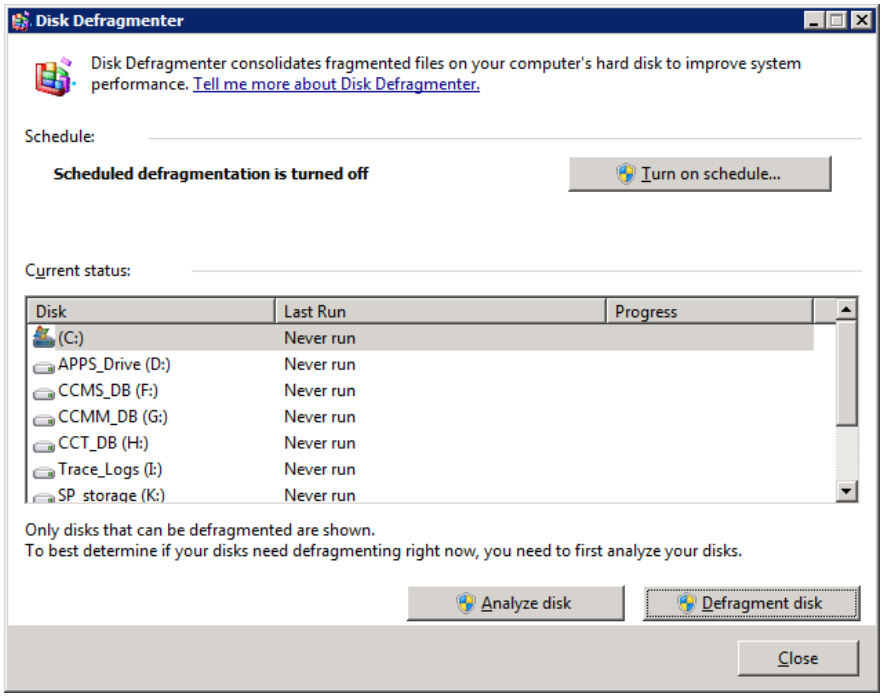
--End--

Scheduling Weekly Disk Defragmentation

Schedule Daily 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)**.

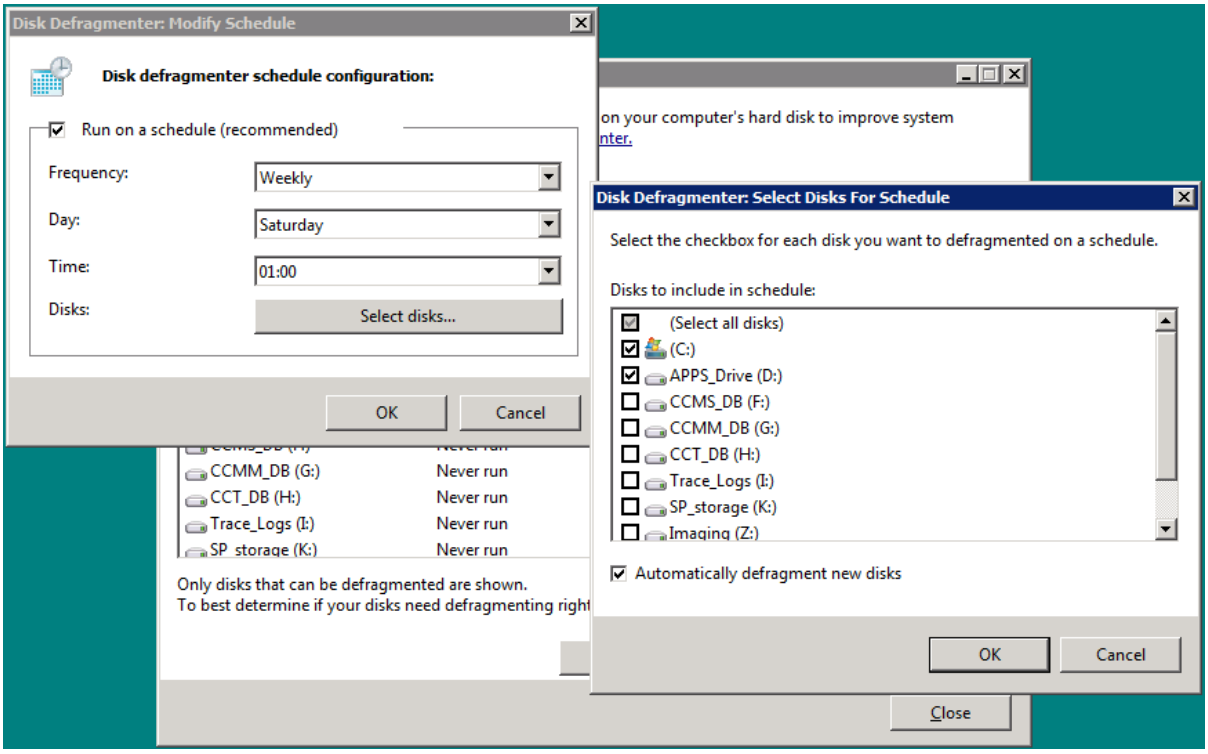
7 Under **Frequency**, select **Weekly**.

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

9 Under **Time**, select an off-peak time at which you want to schedule the defragmentation process, for example 01:00.

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**.

--End--

Configuring the Multicast controller

Configure the Multicast controller to use the IP Multicast delivery method to send Real Time Reporting data. Multicast is a network addressing method for delivering information to a group of destinations in a one-to-many distribution.

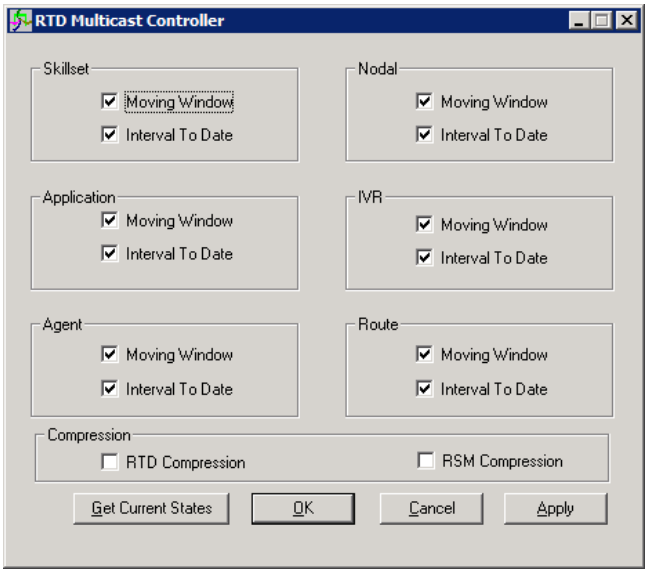
The default multicast addresses set at install time allow for correct multicast operation. You change these only if your network requires you to use different addresses. If you change the multicast addresses, you must configure the Contact Center Manager Administration (CCMA) IP Receive address to match the Contact Center Manager Server (CCMS) Multicast IP group.

If you plan to use the unicast delivery method, you do not need to configure CCMS, and you can skip this procedure. For Unicast delivery, only one user can log on at a time and you must ensure that you disconnect all terminal services sessions.

For more information about multicast and unicast, see *Avaya Aura® Contact Center Fundamentals* (NN44400-110).

Procedure steps

Step	Action
1	Log on to the Contact Center server using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Manager Server**, **Multicast Stream Control**.
3	In the **RTD Multicast Controller** dialog box, select the check boxes for the Real Time data to enable.

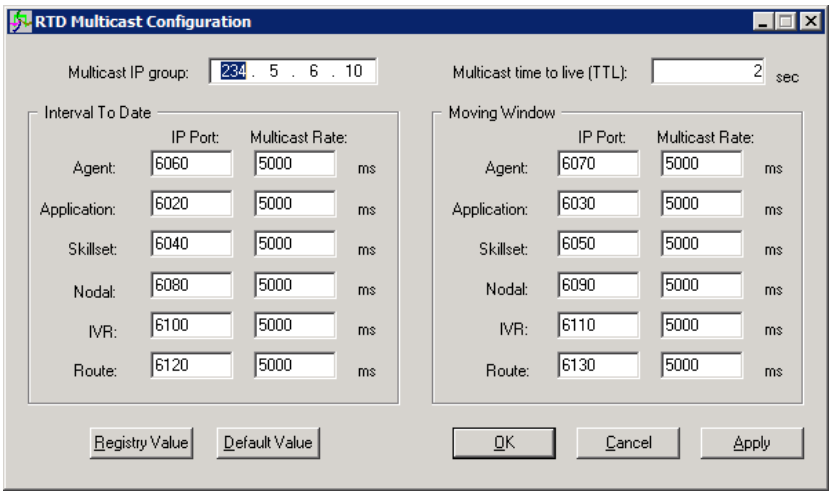


4	Click **OK**.
5	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Manager Server**, **Multicast Address and Port Configuration**.
6	In the **RTD Multicast Configuration** dialog box, in the **Multicast IP group** box, type the multicast IP address for Contact Center Manager Server to use to transmit the RTD, for example **234.5.6.10**. This is the same address as the Contact Center Manager Administration server receiving IP multicast address.
7	In the **Multicast Time To Live (TTL)** box, accept the default setting for the number of network hops packets can transition **OR**

Type a new value that matches your network topology.

Attention: Do not change the ports.

8 For the **Interval to Date, Moving Window IP Port**, and **Multicast Rate** boxes, accept the default values.

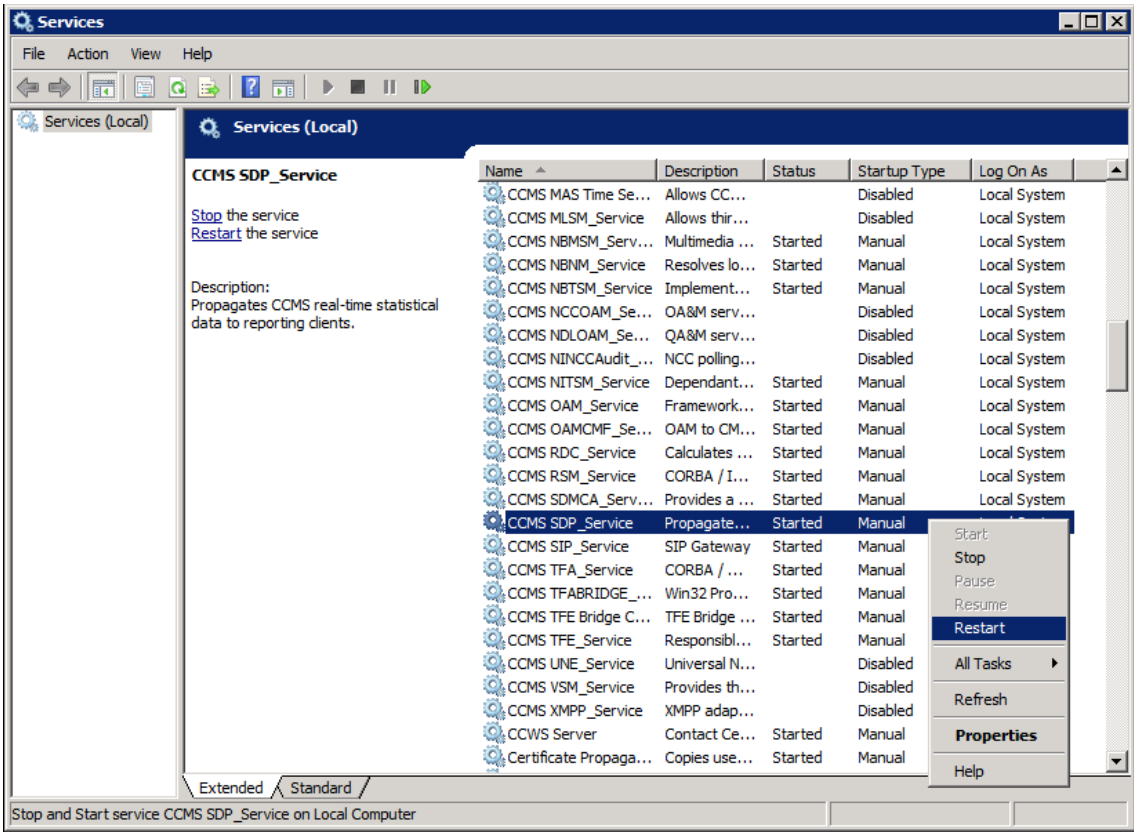


9 Click **OK**.

10 Click **Start**, **All Programs**, **Administrative Tools**, **Services**.

11 Scroll down to **CCMS SDP_Service**.

12 Right-click the **CCMS SDP_Service** and select **Restart**.



13 On the Restart Other Services dialog, click **Yes**.

--End--

Configuring Real-Time Reporting

Configure Real-Time Reporting if you plan to use multicast-based data transmission.

The default multicast addresses set at install time allow for correct multicast operation. You change these only if your network requires you to use different addresses. If you change the multicast addresses, you must configure the CCMA IP Receive address to match the CCMS Multicast IP group. You must ensure that the CCMA IP Send Address is different to the CCMA IP Receive address.

Multicast address and server	IP address	User Interface box name
CCMS send address	234.5.6.10	Multicast IP group
CCMA receive address	234.5.6.10	IP Receive Address
CCMA send address	234.5.6.2	IP Send Address

If you configure a replicating server, you must select multicast for the transmission options under the Real-time Reporting Configuration.

Prerequisites

- Ensure that the IP multicast addresses that you select for Real-time Statistics Multicast (RSM) sending and receiving are in the 224.0.1.0 to 239.255.255.255 range. Check with your network administrator for acceptable IP multicast addresses for your network.
- Ensure that the Contact Center Manager Administration server sending and receiving IP multicast addresses differ.

Procedure steps

Step	Action
1	Log on to the Contact Center server using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Click **Start, All Programs, Avaya, Contact Center, Manager Administration, Configuration**.
3	In the **Avaya Applications Configuration** window, in the left pane, navigate to **Avaya, Applications, Real-Time Reporting**.
4	In the right pane, click the **RTR Registry Settings** icon.
5	In the **RTR Properties** dialog box, in the **IP Receive Address** box, type the Contact Center Manager Administration server receiving IP multicast address, for example **234.5.6.10**.
6	In the **IP Send Address** box, type the Contact Center Manager Administration server sending IP multicast address, for example **234.5.6.2**.
7	For the **Output Rate** box and the **Transform Rate** box, accept the default values (5000 and 1000).

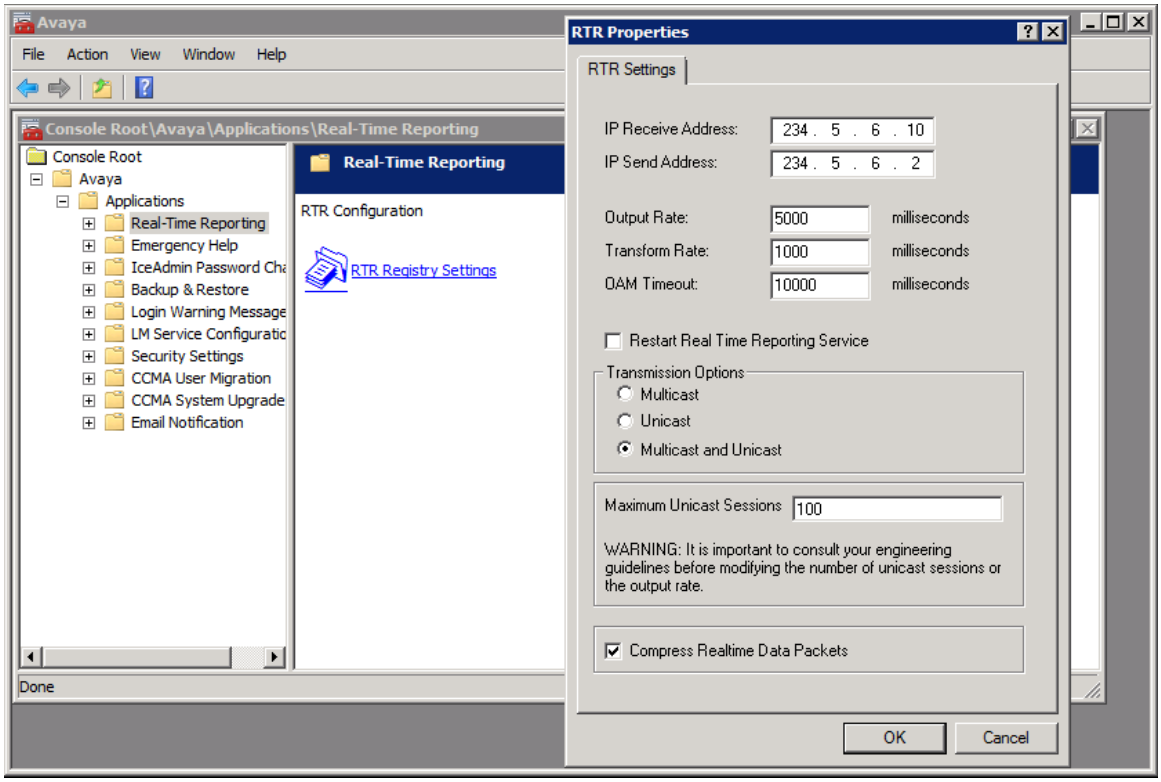
Attention: You can adjust the default values; however, reducing the Output Rate value and the Transform Rate value increases the workload on the Contact Center Manager Administration server.

8	For the **OAM Timeout** box, accept the default value (10 000).
9	Select the **Compress Realtime Data Packets** check box.

Attention: If you clear this check box, you disable real-time data packet compression.

10 In the **Transmission Options** area, select one of the following options:

- If your network supports multicast traffic, select **Multicast**. Avaya recommends this option.
- To support both transmission types, select **Multicast and Unicast**.



11 If you selected the **Multicast** option, proceed to step 14.

12 In the **Maximum Unicast Sessions** box, type the maximum number of simultaneous unicast sessions that you want the server to allow.

13 Select the **Restart Real Time Reporting Service** check box.

14 Click **OK**.

The Restart ICERtdService status window appears while the service is restarting, and closes after the service successfully restarts.

15 Close all windows to complete the procedure.

--End--

Configuring Internet Explorer on the Contact Center server

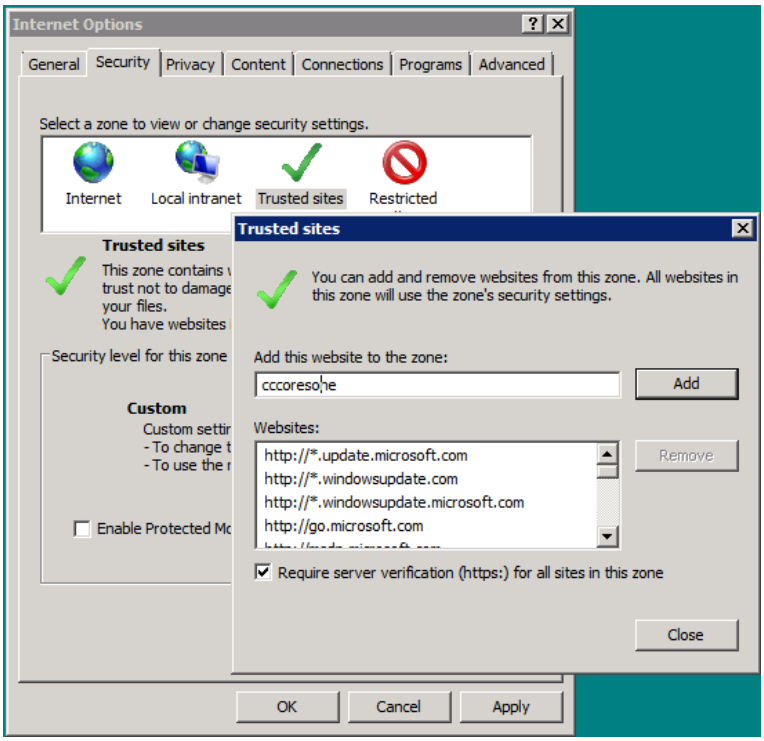
Configure Internet Explorer on the Contact Center server to access Contact Center Manager Administration for the first time.

Install Microsoft Internet Explorer 7.0 or later (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** • **Download signed ActiveX controls**
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 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) of the Contact Center server, for example CCCORESONE.



17 Click **Add**.

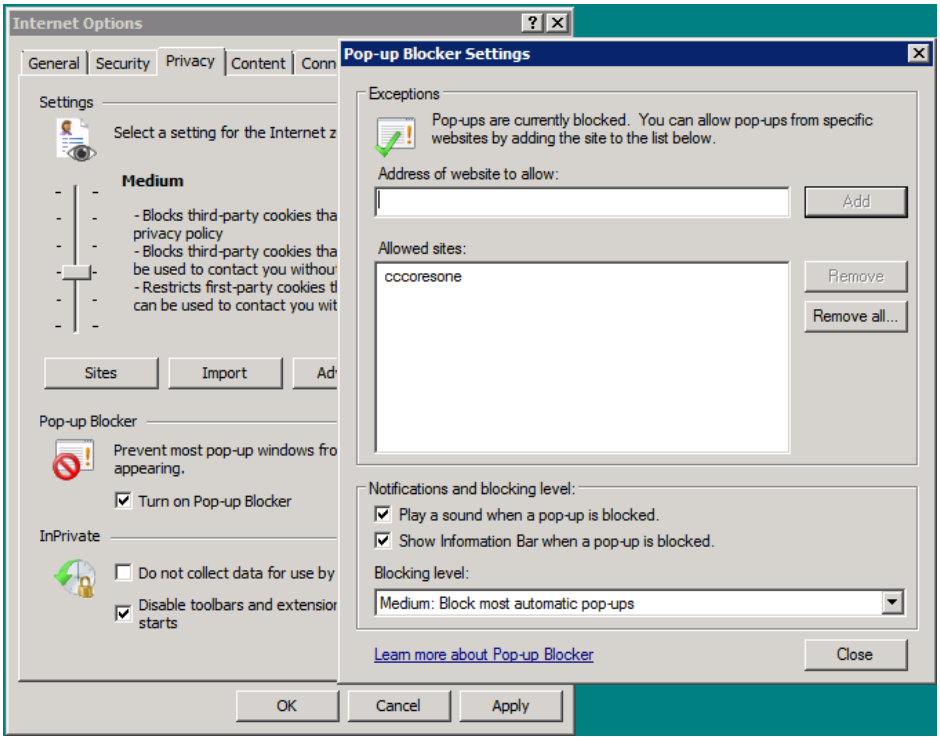
18 Click **Close** to return to the **Internet Options** dialog box.

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 Contact Center Manager Administration URL, for example http://cccoresone.



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.

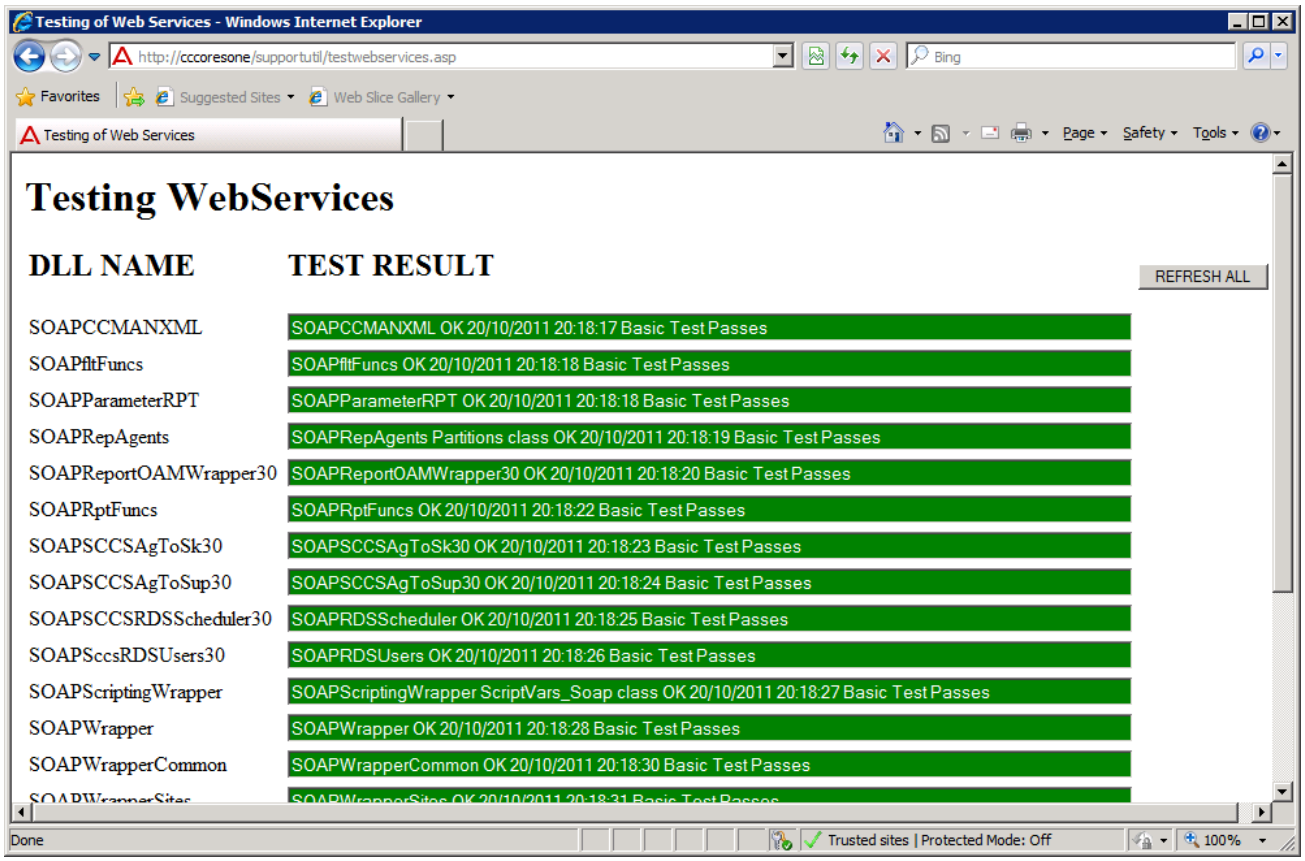
Procedure steps

Step	Action
1	On the Contact Center server, start Internet Explorer.

2 Enter the test URL in the format http://<Server name>/supportutil/testwebservices.asp, for example **http://CCCORESONE/supportutil/testwebservices.asp**.

3 Wait for the page to refresh.

The web services that appear in green are running correctly.



--End--

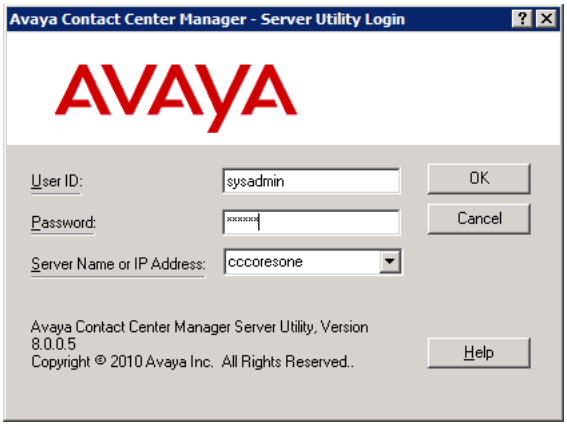
Changing the default sysadmin password

Change the sysadmin password from the default value. It is important to do this before logging on to CCMA for the first time and creating the CCMS server record in CCMA.

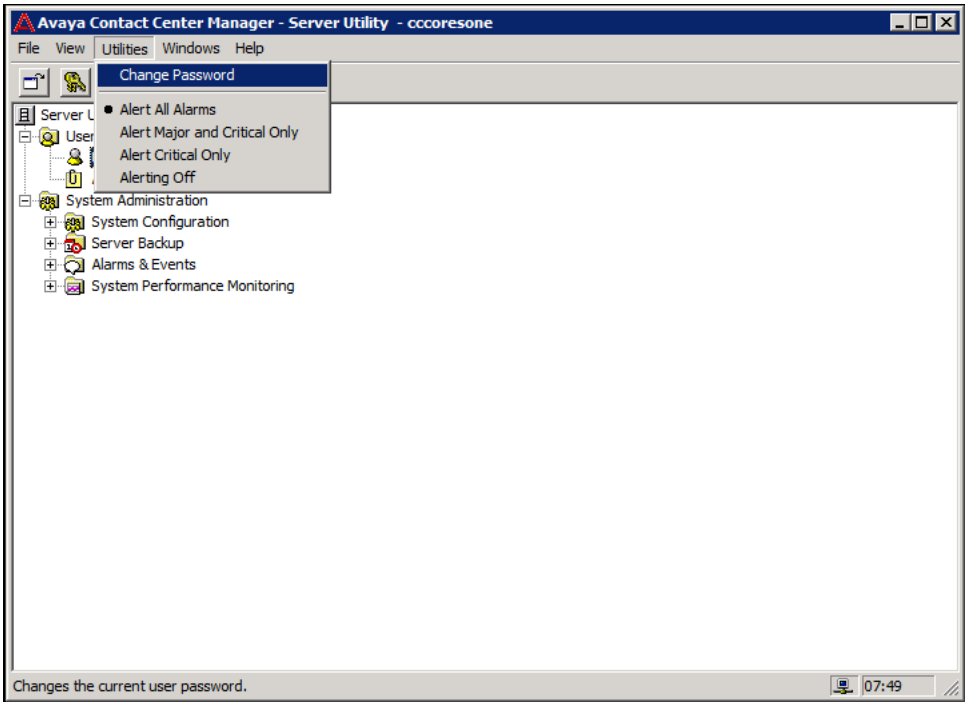
Attention: Ensure you keep a record of the sysadmin password. If you lose or forget this password, you are not able to carry out many important maintenance functions. There is no recovery mechanism for a lost sysdamin password–ultimately a lost sysadmin password requires a complete re-install of Contact Center.

Procedure steps

Step	Action
1	Log on to the Contact Center server using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Select **Start, All Programs, Avaya, Contact Center, Server Utility, Server Utility**.
3	In the **User ID** box, type the system administrator user name **sysadmin**.
4	In the **Password** box, type the default system administrator password **avaya1**.



Step	Action
5	Click **OK**.
6	Close the **Alarm Monitor** window.
7	Select **Utilities, Change Password**.



8 On the **Avaya Contact Center Manager - Server Utility** message box, click **OK**.

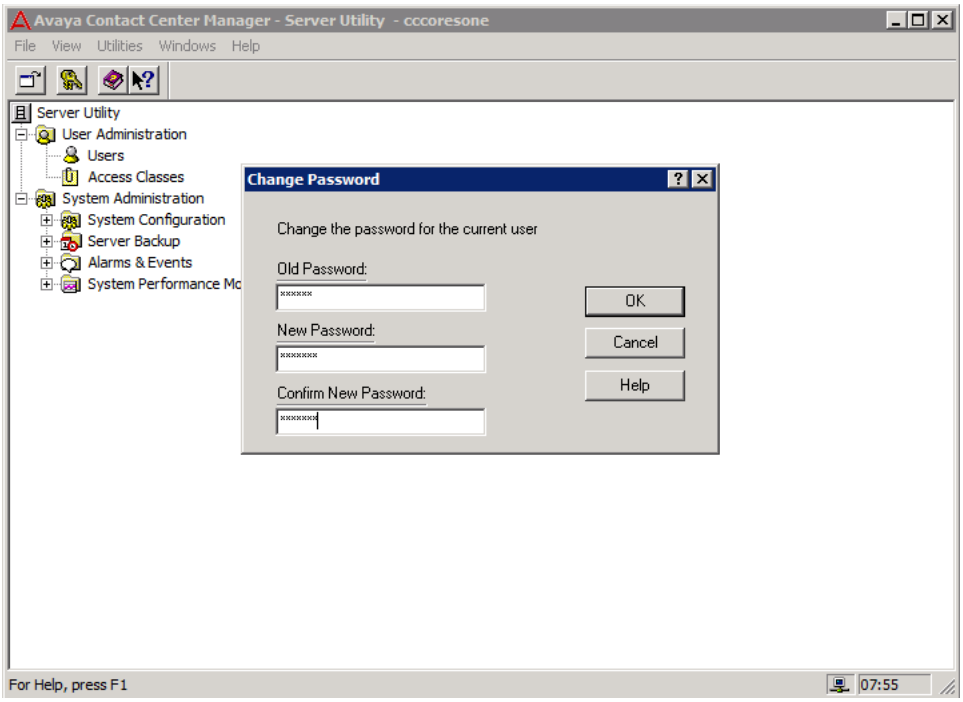
9 In the **Change Password** dialog box, in the **User name** box, type **sysadmin**.

10 In the **Old password** box, type **avaya1**.

11 In the **New password** box, type a new password, for example **sample1**.

12 In the **Confirm password** box, type the new password again.

Attention: Ensure you keep a record of the changed sysadmin password. If you lose or forget the new sysadmin password, you cannot perform many important maintenance tasks. There is no recovery from losing the sysdamin password: it requires a complete re-install of Contact Center.



13 Click **OK**.

14 Exit Server Utility.

--End--

Logging on to Contact Center Manager Administration for the first time

When you log on to Contact Center Manager Administration (CCMA) 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. CCMA user passwords can contain only English characters and special characters.

Procedure steps

Step	Action
1	Start Internet Explorer.
2	In the **Address** box, type the CCMA URL in the format http://<Server name>, for example **http://CCCORESONE**.
3	Press **Enter**.
4	In the Contact Center Manager Administration main logon window, click **Change Password**.

5 In the **Change Password** dialog box, in the **User name** box, type **webadmin**.

6 In the **Old password** box, type **webadmin**.

7 In the **New password** box, type a new password, for example **nimdabew**.

8 In the **Confirm password** box, type the new password again.

You can modify the default password only. You cannot change the default user name.

Attention: If you lose or forget the new webadmin password, you cannot log on to Contact Center Manager Administration as the webadmin administrator. To avoid this scenario, in Access and Partition Management, you can create a new user account with administrator rights, such as tempadmin. If you forget or lose the new webadmin password, you can log on to the Contact Center Manager Administration server as tempadmin to change the password. If you forget all passwords for accounts with administrator rights, contact support to have the webadmin password reset.



9 Click **Submit**.

10 In the main logon window, in the **User ID** box, type webadmin.

11 In the **Password** box, type the new password, for example **nimdabew**.

12 Click **Login**.

13 Click **OK**.

The system displays the server configuration screen with default values for the current co-resident server.

14 In the **Display Name** box, type a descriptive name for the server; this is how the server appears in the system tree in Contact Center Manager Administration. For example, **MM_Elite_CC_Single_Server**.

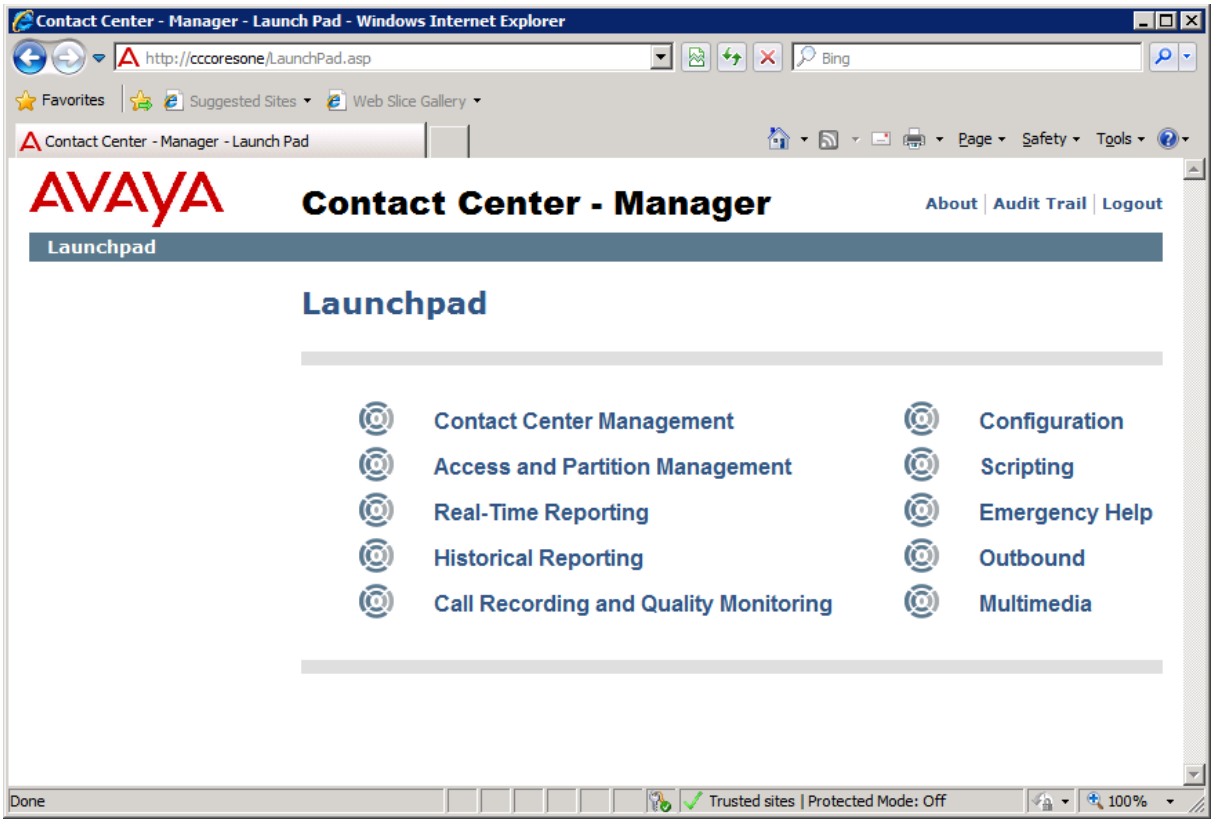
15 In the **Login ID** box, type sysadmin.

16 In the **Password** box, type the sysadmin password, for example sample1.



17 Click **Submit**.

The Contact Center Manager Administration launchpad appears.



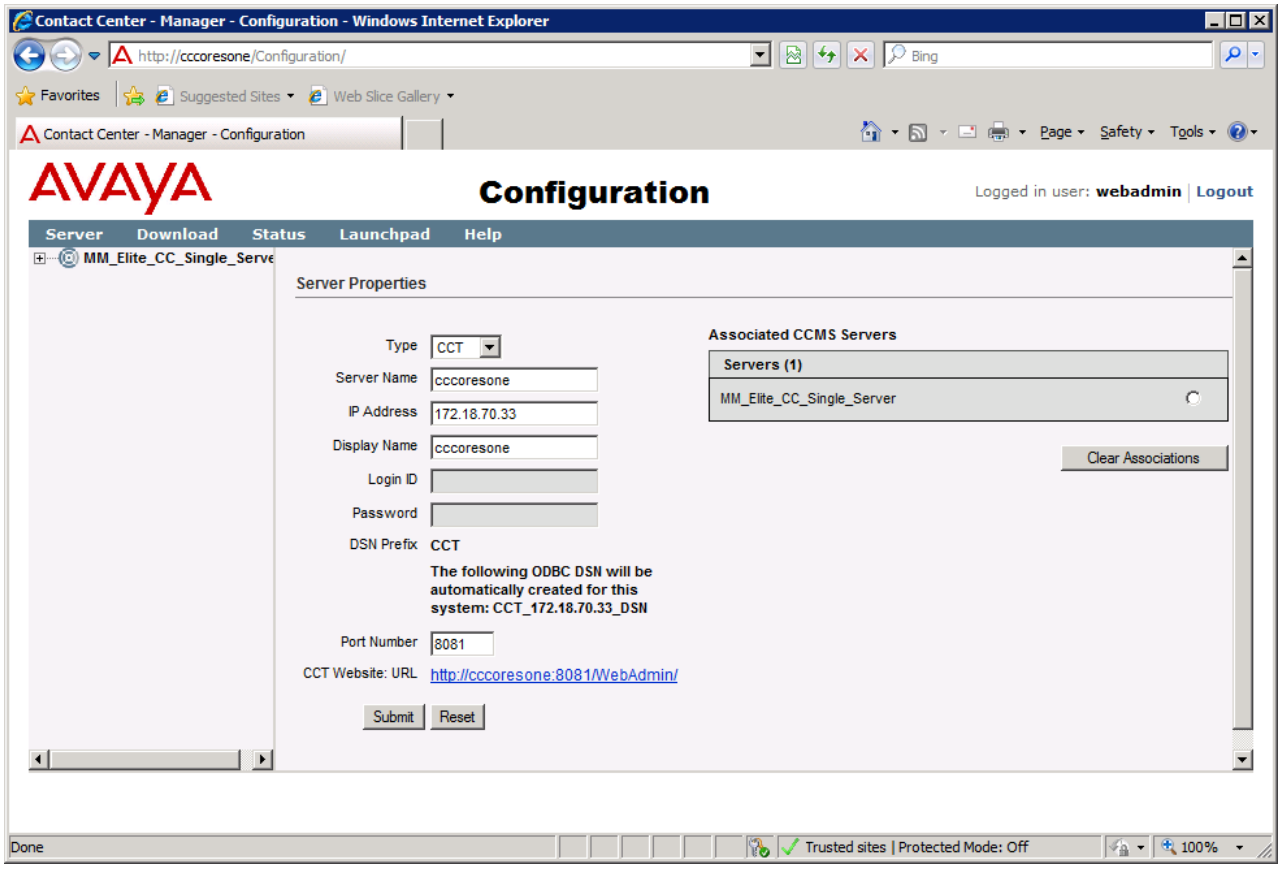
--End--

Adding the CCT Server in CCMA

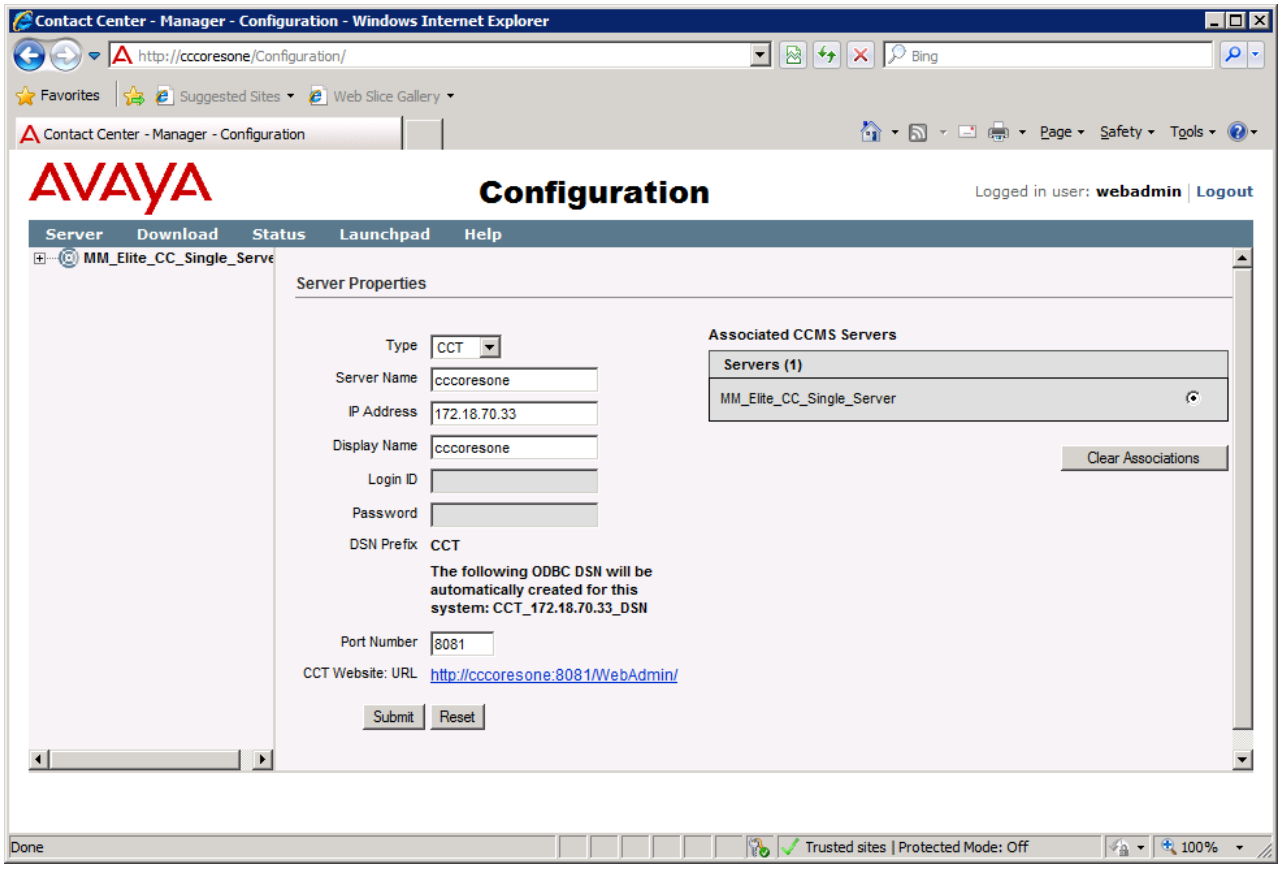
Add the CCT server to CCMA and associate it to a CCMS server.

Procedure steps

Step	Action
1	On the Launchpad, click **Configuration**.
2	From the **Server** menu, click **Add Server**.
3	From the **Type** list, select **CCT**.
4	In the **Server Name** box, type a descriptive name for the CCT server, for example cccoresone.
5	Press **Tab**. *The system populates the remaining boxes with the correct values for the server.*



6 In the Associated CCMS Servers list, select the CCMS server which you want to associate this CCT server, for example **MM_Elite_CC_Single_Server**.



7 Click **Submit**.

--End--

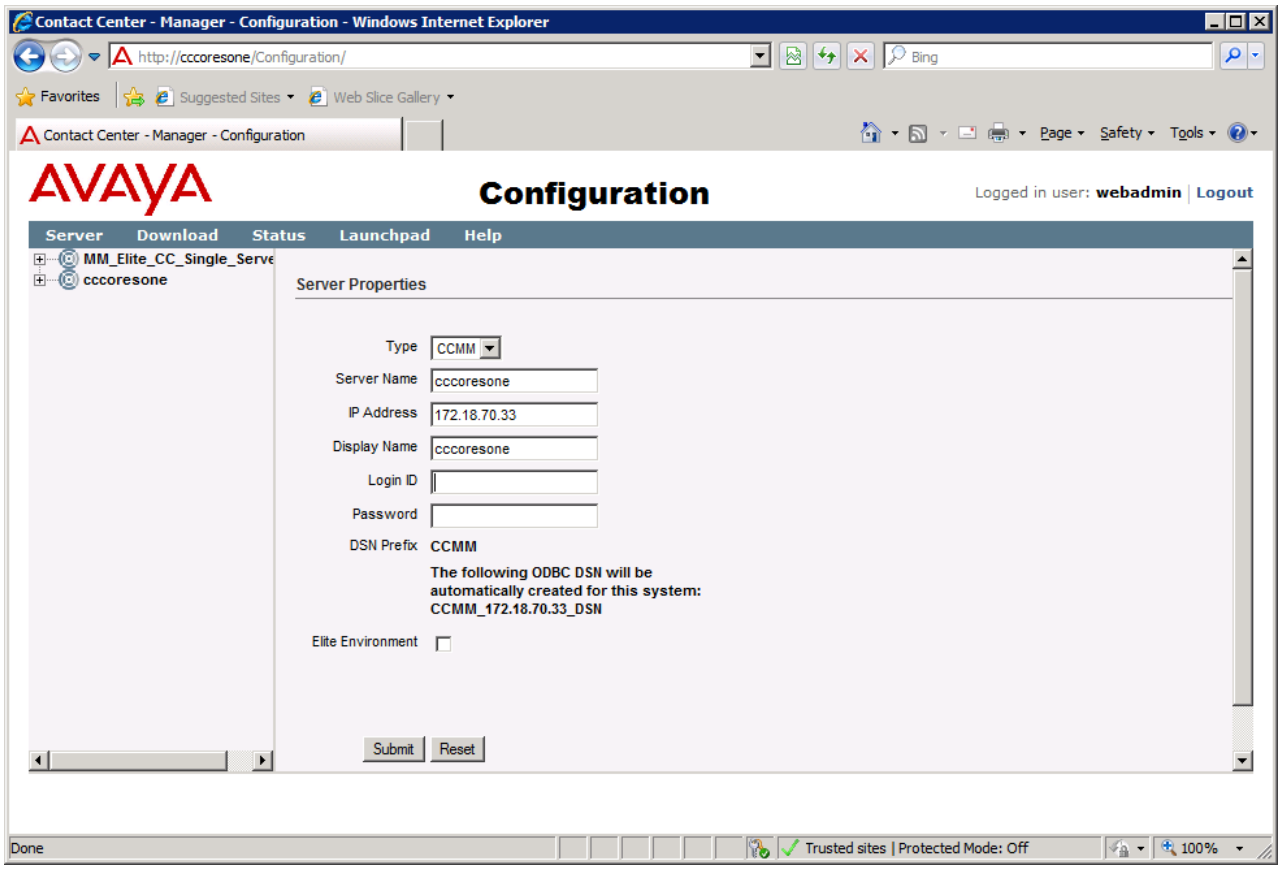
Adding the CCMM Server in CCMA

Add the CCMM server to CCMA and associate it to a CCMS server.

Procedure steps

Step	Action
1	On the Launchpad, click **Configuration**.
2	From the **Server** menu, click **Add Server**.
3	From the **Type** list, select **CCMM**.
4	In the **Server Name** box, type the name of the Contact Center server, for example **CCCORESONE**.
5	Press **Tab**.

The system populates the IP Address and Display Name boxes.



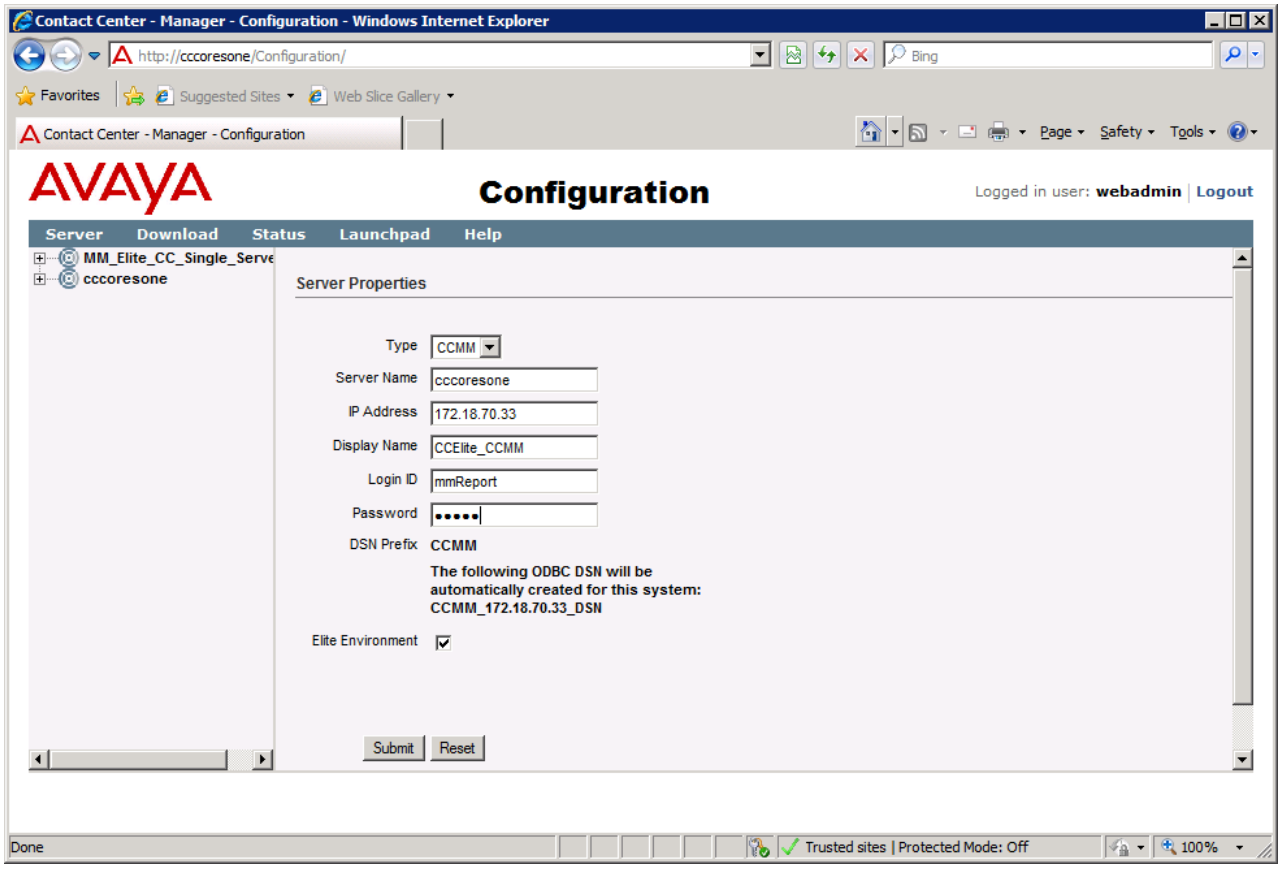
6 In the **Display Name** box, type a descriptive name for the CCMM server, for example CCElite_CCMM. (The display name cannot match an existing display name.)

7 In the **Login ID** box, type **mmReport**.

8 In the **Password** box, type **mmRep**.

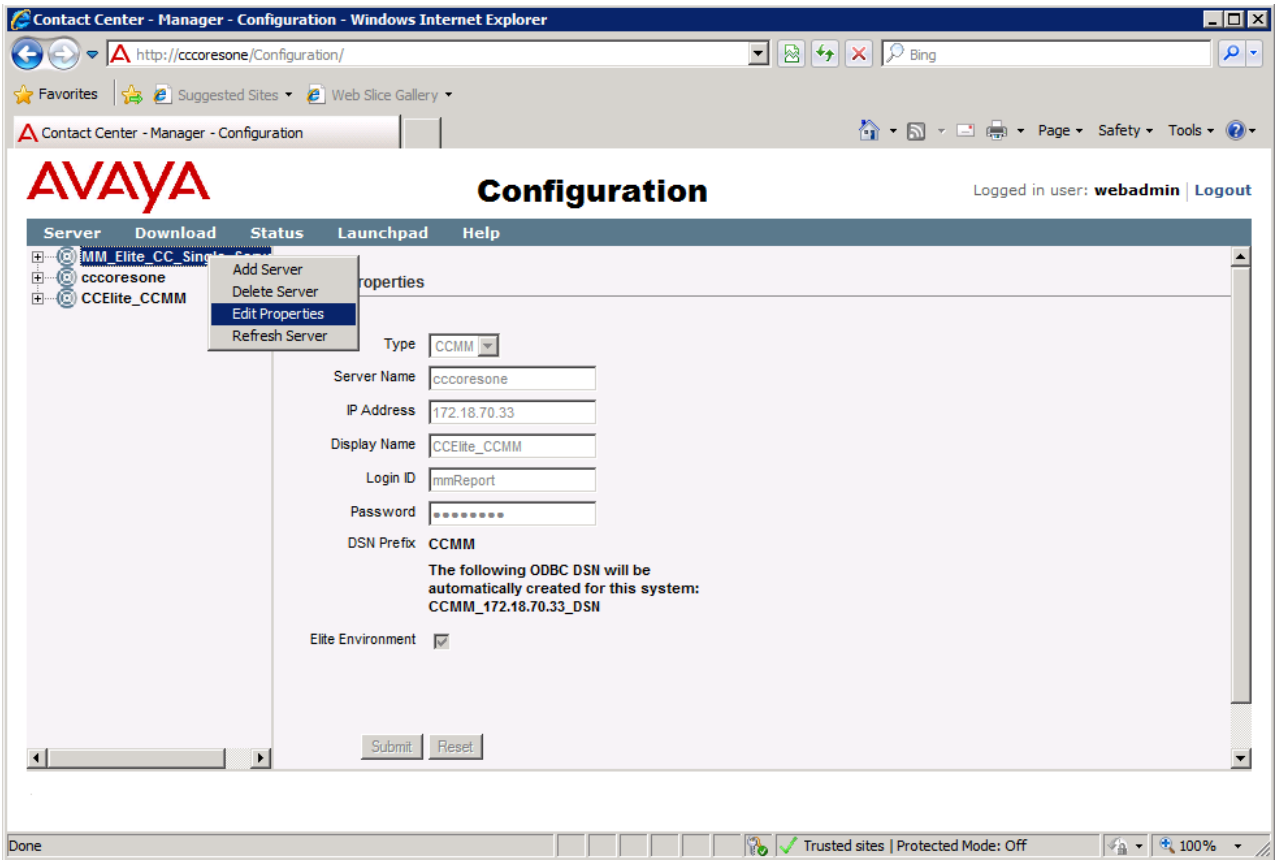
Attention: mmRep is the default Multimedia password, and you can change it using the CCMM Administration tool. If you change the password in the CCMM Administration tool, you must update this server record with the new password.

9 Select the **Elite Environment** checkbox.

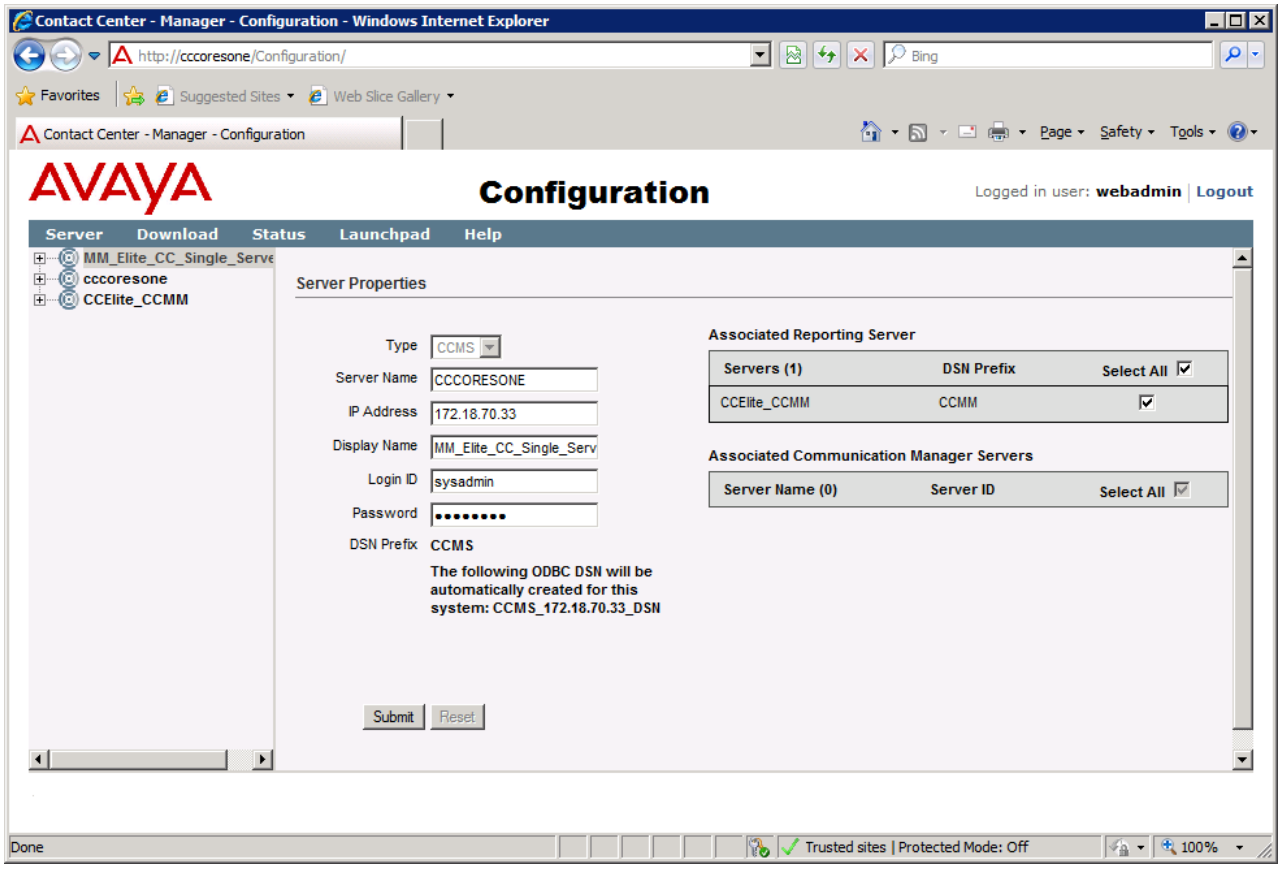


10 Click **Submit**.

11 In the left pane, right click the CCMS server, for example **MM_Elite_CC_Single_Server**, and select **Edit Properties**.



12 On the **Server Properties** screen, under **Associated Reporting Servers**, select the Multimedia Server display name, for example **CCElite_CCMM**.



13 Click **Submit**.

--End--

Installing the Orchestration Designer client

Install the Orchestration Designer client to manage Contact Center applications. Applications route contacts based on certain criteria from the contact such as skillset or customer name.

Procedure steps

Step	Action
1	On the **Launchpad**, click **Scripting**.
2	In the **Scripting** window, select **Orchestration Designer**, and click **Launch Orchestration Designer**.
3	In the message box requesting you to download the Orchestration Designer exe file, click **OK**.

4 In the dialog box, click **Run**.

5 In the **Orchestration Designer- InstallShield Wizard**, click **Next**.

6 In the **User Name** box, type a name.

7 In the **Organization** box, type your company name.

8 Select **Anyone who uses this computer (all users)**.

9 Click **Next**.

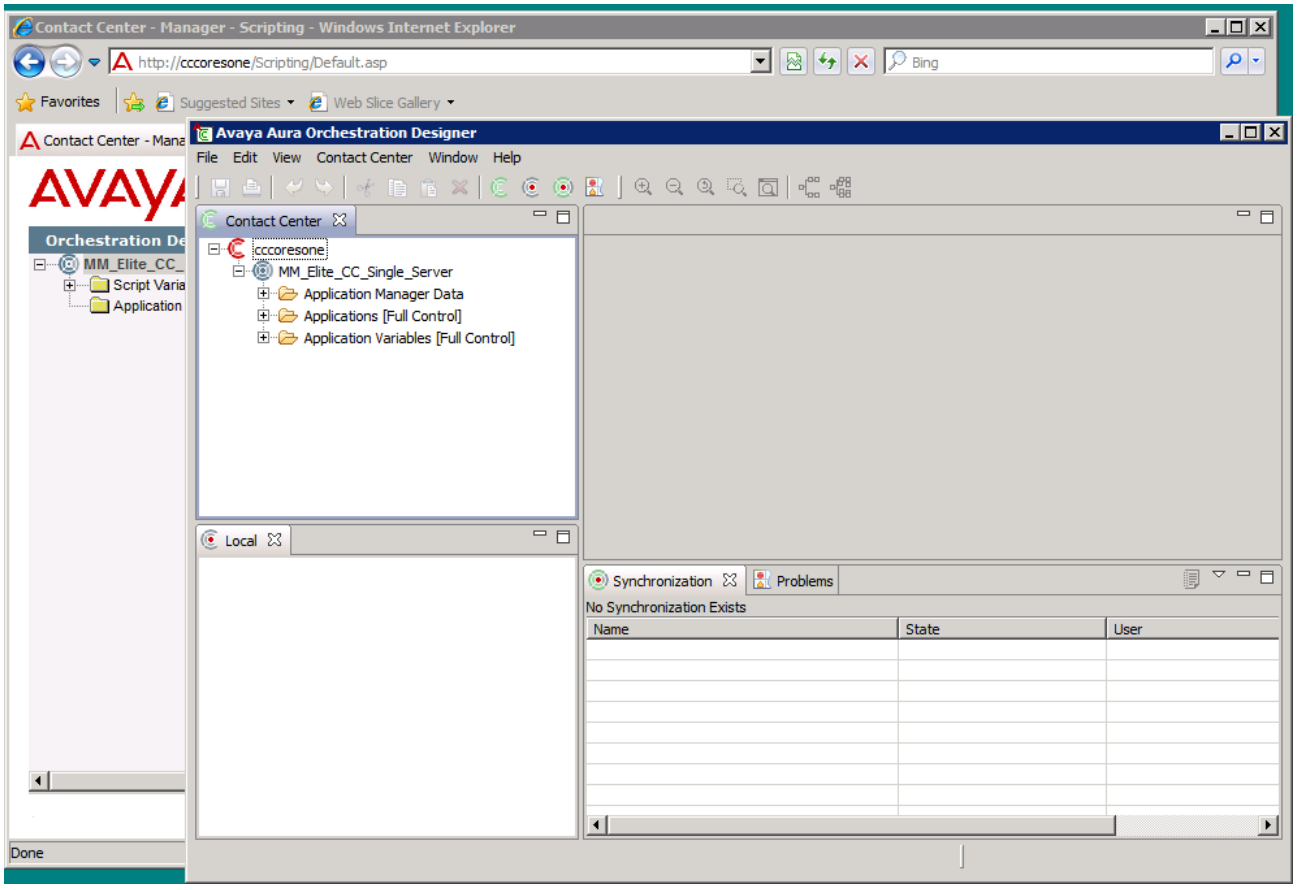
10 Accept the default **Destination Folder** and Click **Next**.

11 Click **Install**.

12 Click **Finish**.

13 In the **Scripting** window, select **Orchestration Designer**, and click **Launch Orchestration Designer**.

14 Verify that the Orchestration Designer client starts correctly.



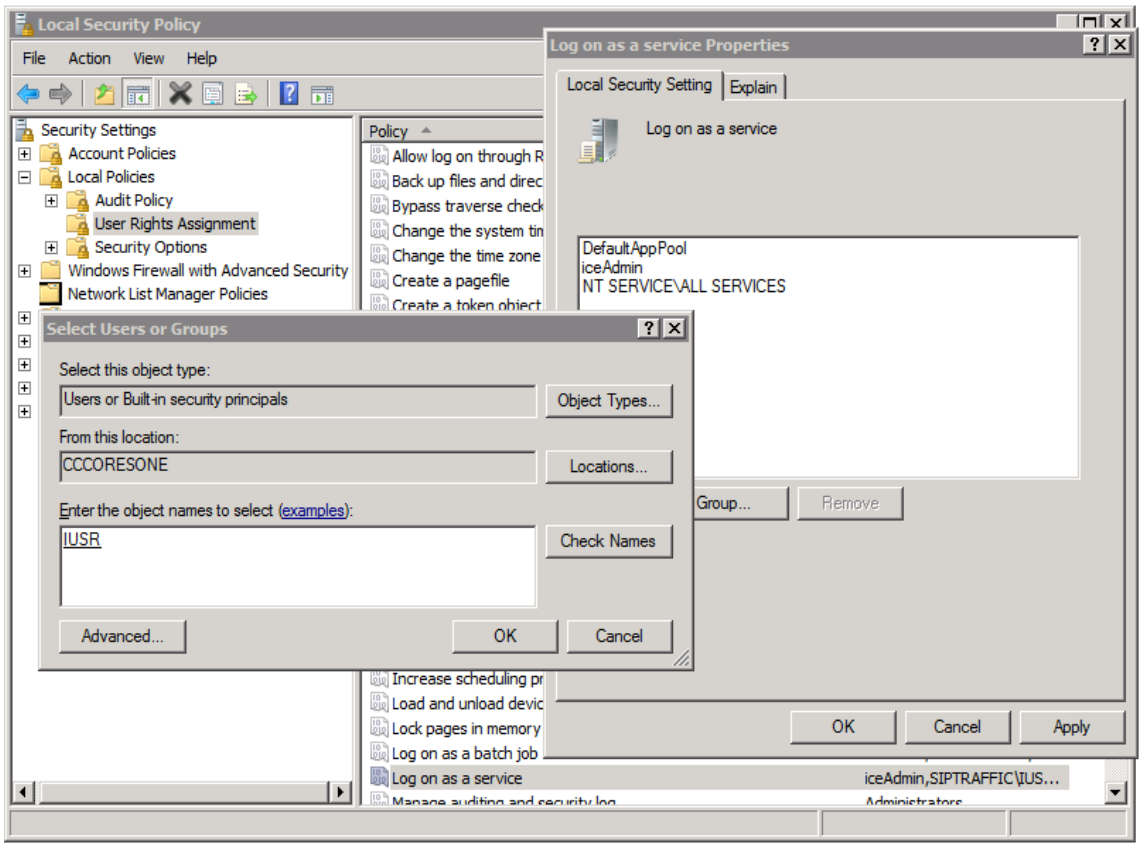
--End--

Providing local users with the Log on as a service right

Provide local users with the 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	In the left pane, under **Security Settings**, expand **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 Contact Center server name from the list, for example **CCCORESONE**.
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 On the **Log on as a service Properties** dialog, click **OK**.

13 Close the **Local Security Settings** window.

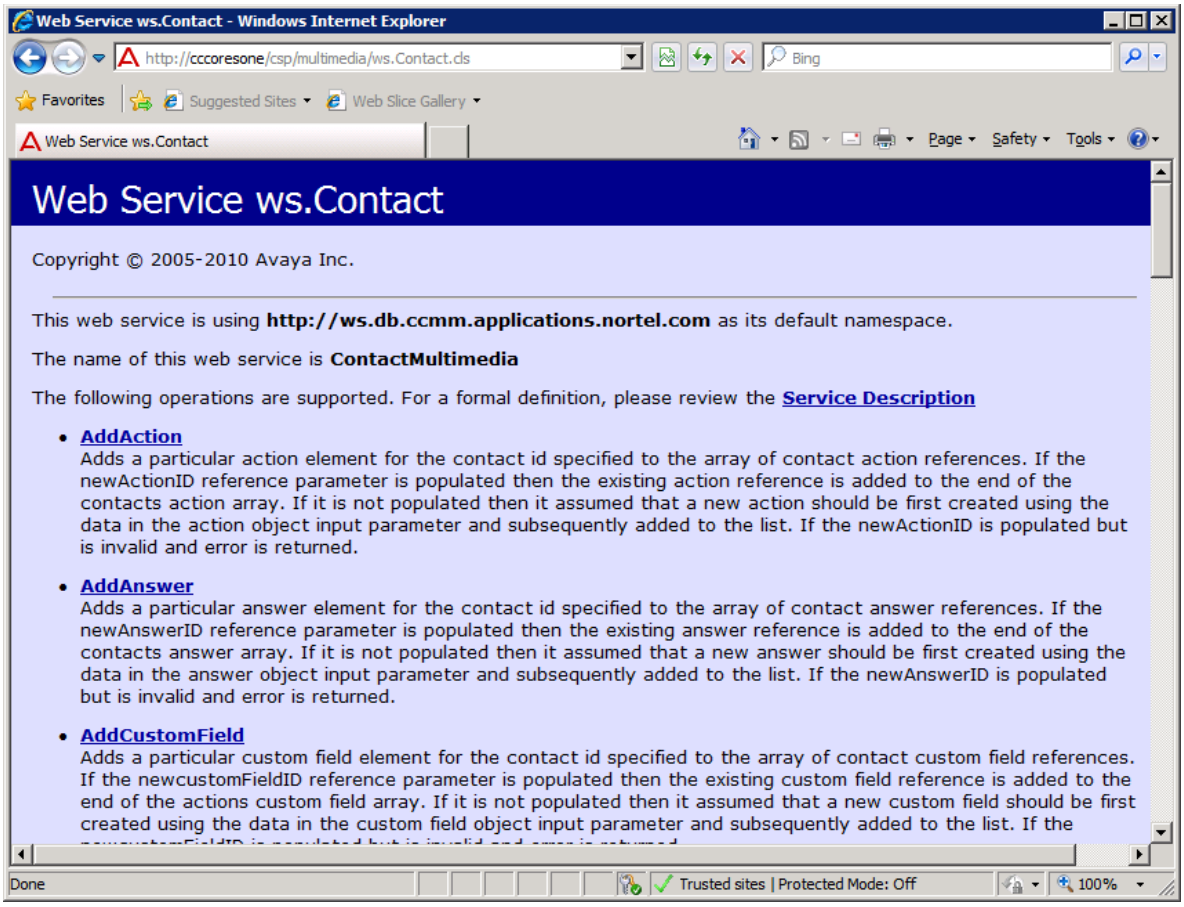
--End--

Verifying the Multimedia database installation

Verify that the Multimedia database is installed and configured correctly.

Procedure steps

Step	Action
1	On the Contact Center server, open Internet Explorer.
2	In the **Address** box, type the web service test URL in the format http://<Server name>/csp/multimedia/ws.Contact.cls, for example **http://CCCORESONE/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

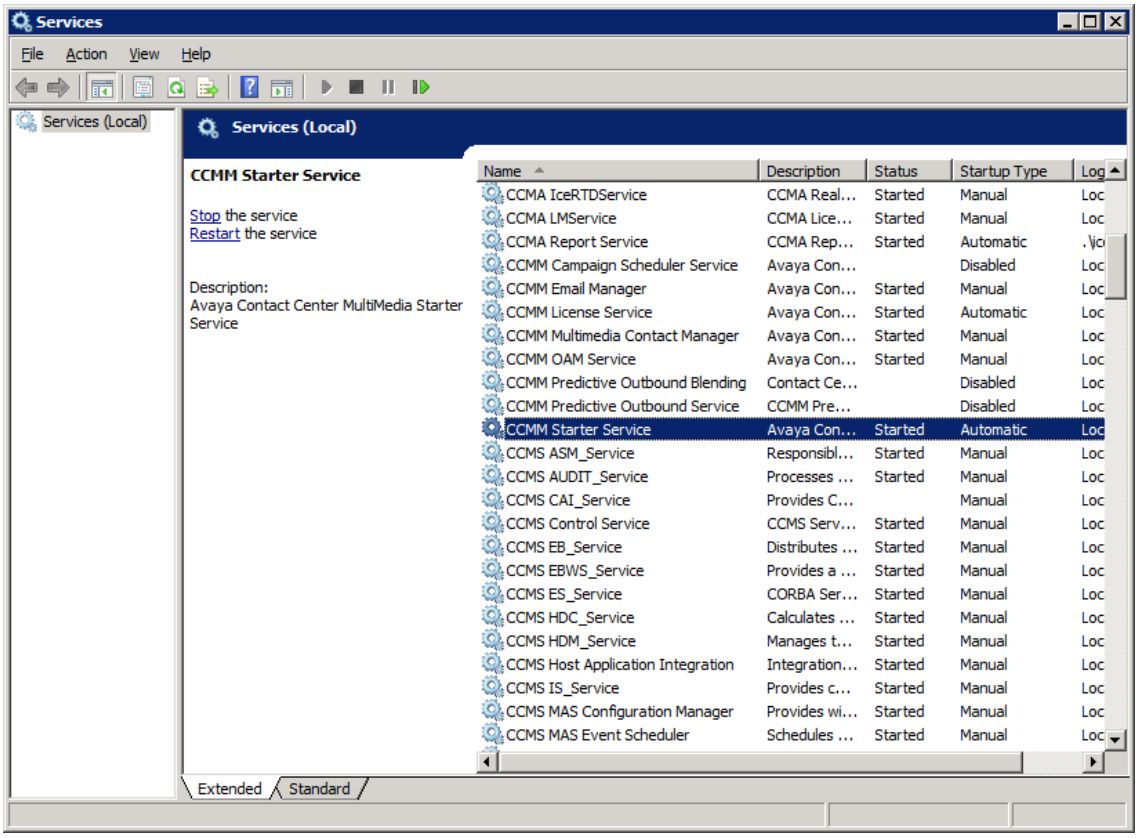
Verify that the Contact Center Multimedia services have the correct configuration to start automatically, to ensure that CCMM starts routing contacts immediately after a server restart.

Procedure steps

Step	Action
1	On the Contact Center server, click **Start**, **Administrative Tools**, **Services**.
2	Next to **CCMM License Service**, verify that the status is **Started** and the startup type is **Automatic**.

3 Next to **CCMM Starter Service**, verify that the Status is **Started** and the Startup Type is **Automatic**.

If either service does not have a startup type of **Automatic**, right-click the service and modify the properties to correct this.



4 Verify that the following services have a Status of **Started**:

- CCMM Multimedia Contact Manager
- CCMM OAM service
- CCMM Email Manager

5 If any service did not start, in the **Services** window, right-click the service name, and click **Start**.

6 Exit the **Services** window.

--End--

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.

Procedure steps

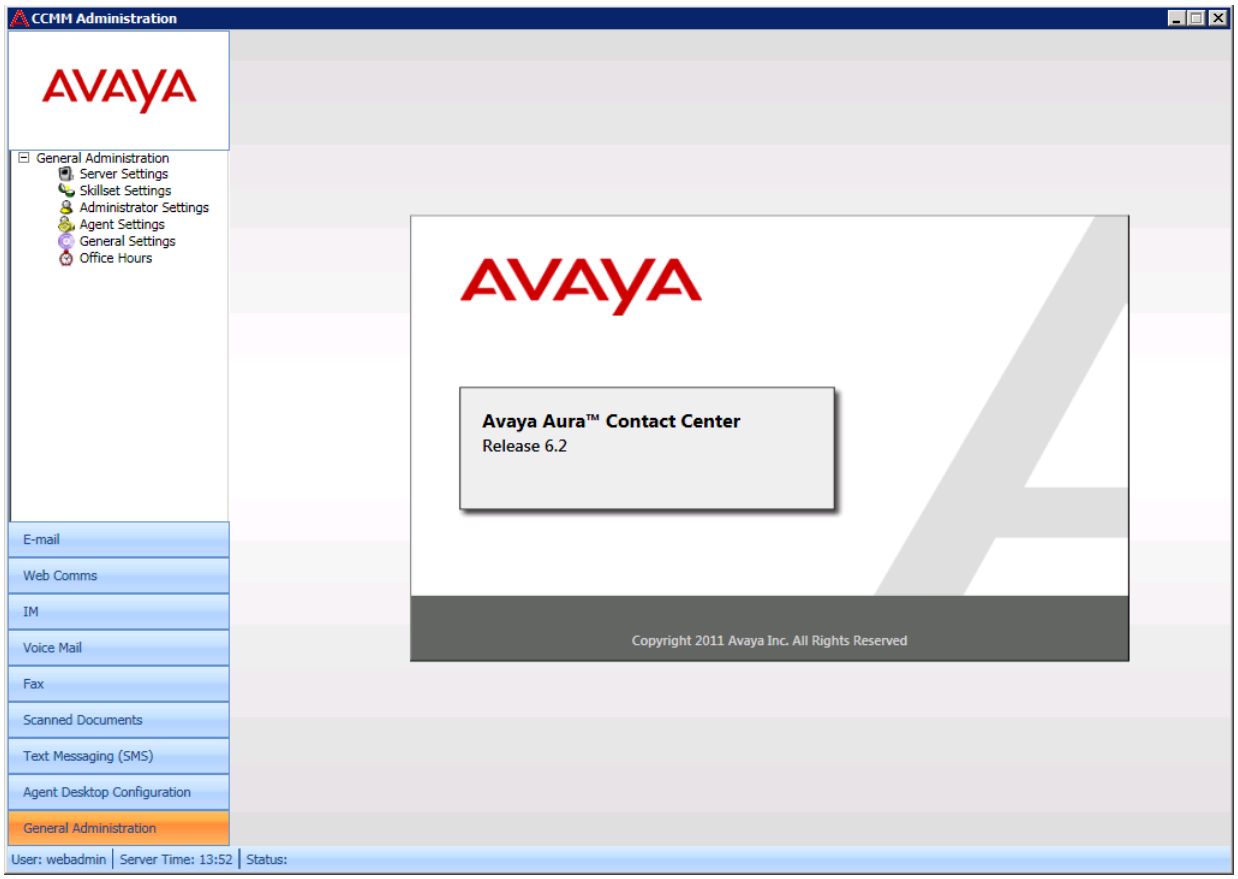
Step	Action
1	On the Contact Center server, start Internet Explorer.
2	In the **Address** box, type the CCMA URL in the format http://<Server name>, for example **http://CCCORESONE**.
3	Press **Enter**.
4	In the main logon window, in the **User ID** box, type **webadmin**.
5	In the **Password** box, type the password, for example **nimdabew**.
6	On the **Launchpad**, click **Multimedia**.
7	In the left pane, select the CCMM server by its display name, for example **CCElite_CCMM**.



8	Select **Install Prerequisite Software**, and click **Launch Multimedia Client**.
9	On the **File Download - Security Warning** window, click **Run**.

10 On the **Internet Explorer - Security Warning** window, click **Run**.

The Contact Center Multimedia Administration tool appears.



--End--

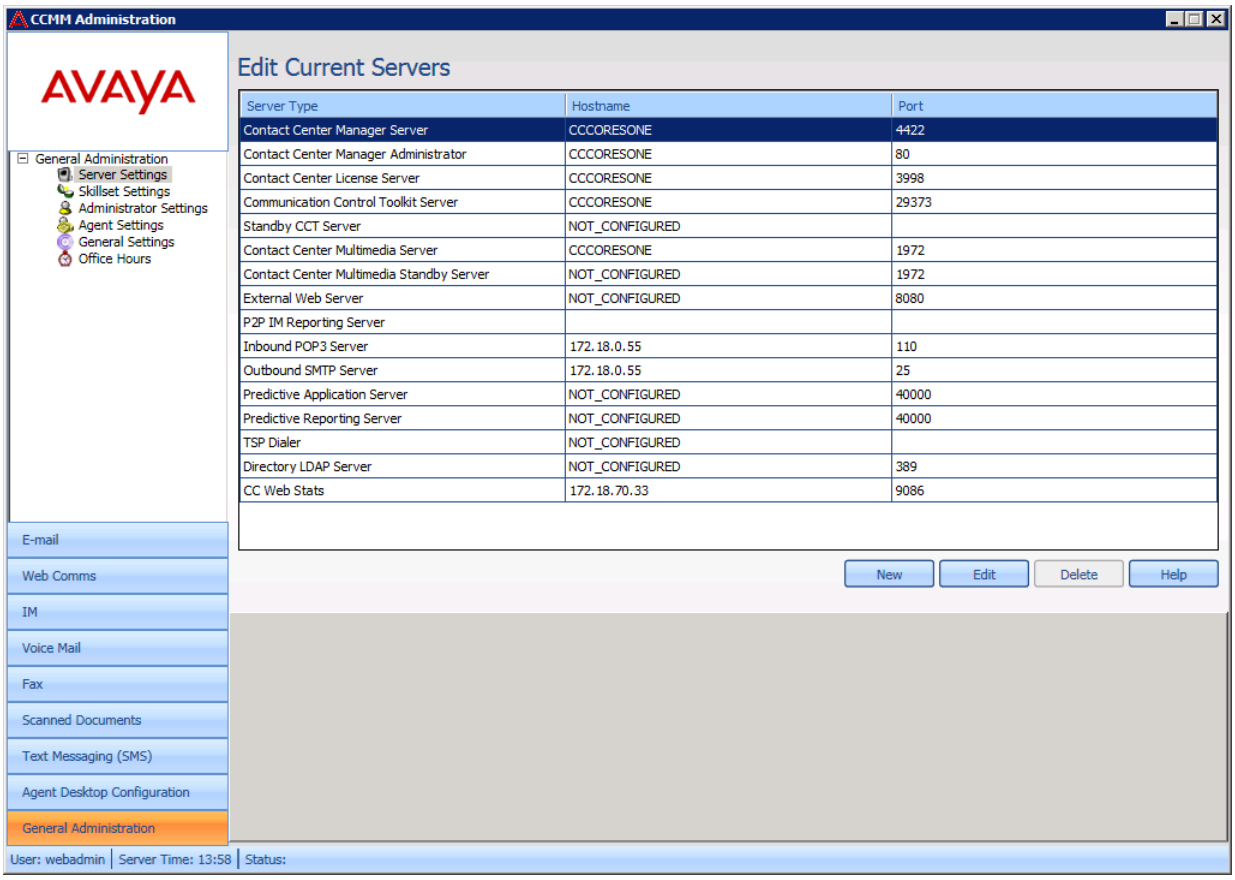
Verifying and configuring server settings in the CCMM Administration client

On a co-resident server, the installer automatically creates all required server records in the CCMM database. Verify that the Contact Center application servers and e-mail server details are correct by reviewing the information in the CCMM Administration client.

Add the Communication Manager that hosts Call Center Elite. This allows Agent Desktop to generate a local XML setting so that it can log on to the softphone even in the case of a Contact Center failure.

Procedure steps

Step	Action
1	Log on to the CCMM Administration client.
2	In the left column, select the Multimedia server by its display name, for example **CCElite_CCMM**.
3	In the left column, select **General Administration**.
4	Click **Server Settings**.



5	Verify the required servers are present and have the correct hostname and IP address, for example as follows: Contact Center Manager Server — CCCORESONE Contact Center Manager Administrator — CCCORESONE Contact Center License Server — CCCORESONE Communication Control Toolkit Server— CCCORESONE Contact Center Multimedia Server — CCCORESONE Inbound POP3 Server — 172.18.0.55 Outbound SMTP Server — 172.18.0.55

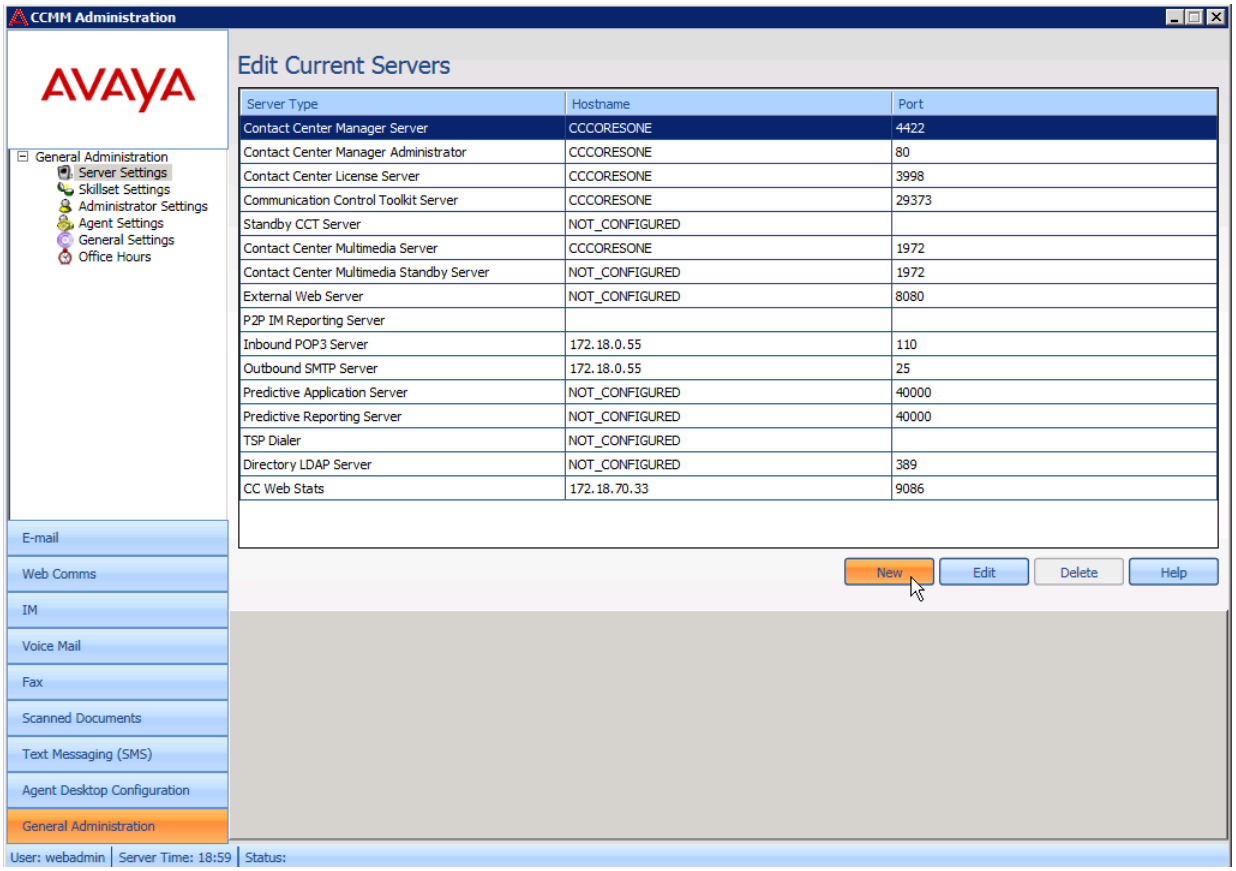
CC Web Stats — 172.18.70.33

6 If the details of any of the above servers are incorrect, select the server and click **Edit**.

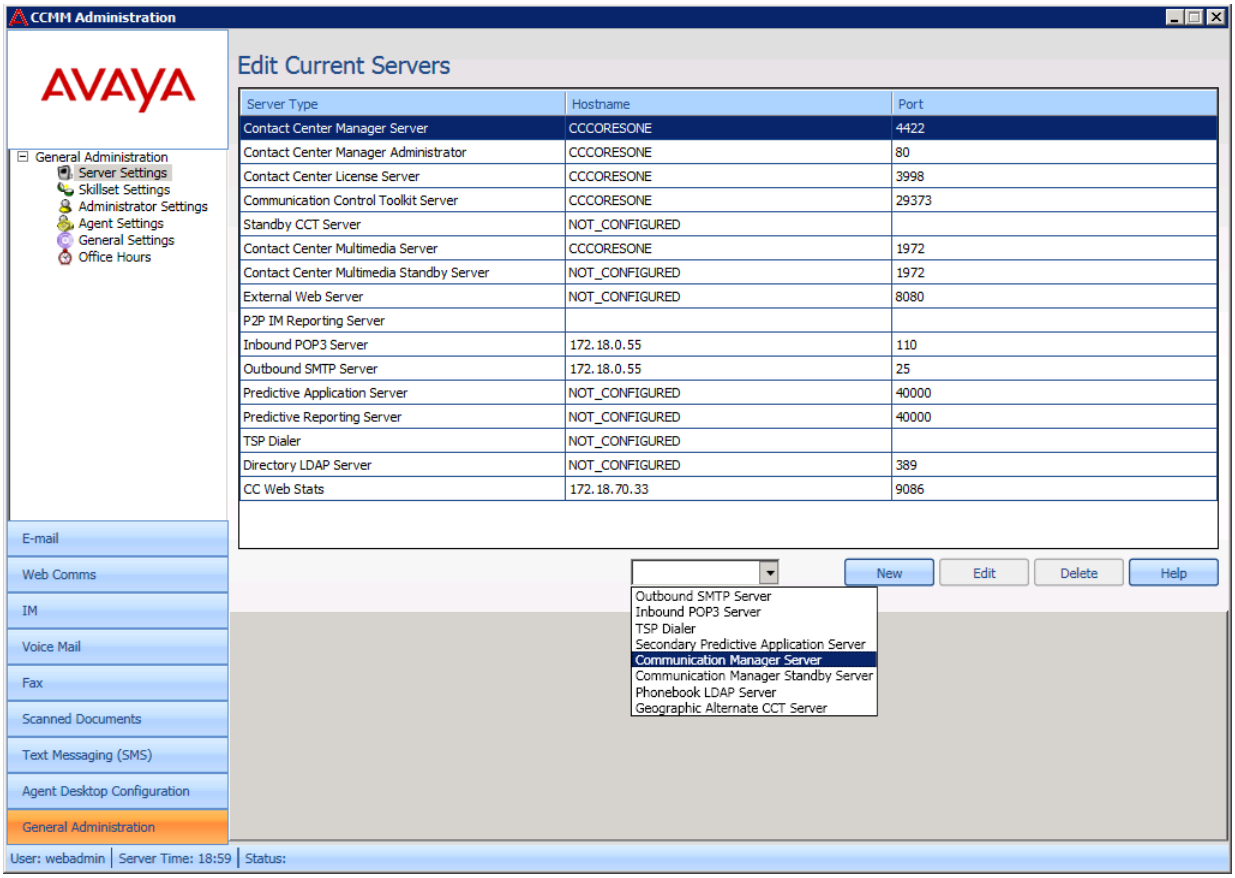
7 Under **Edit Server Details**, correct the server information, and click **Save**.

8 If any of the above servers are missing, click **New**, select the server type, complete the server details, and click **Save**.

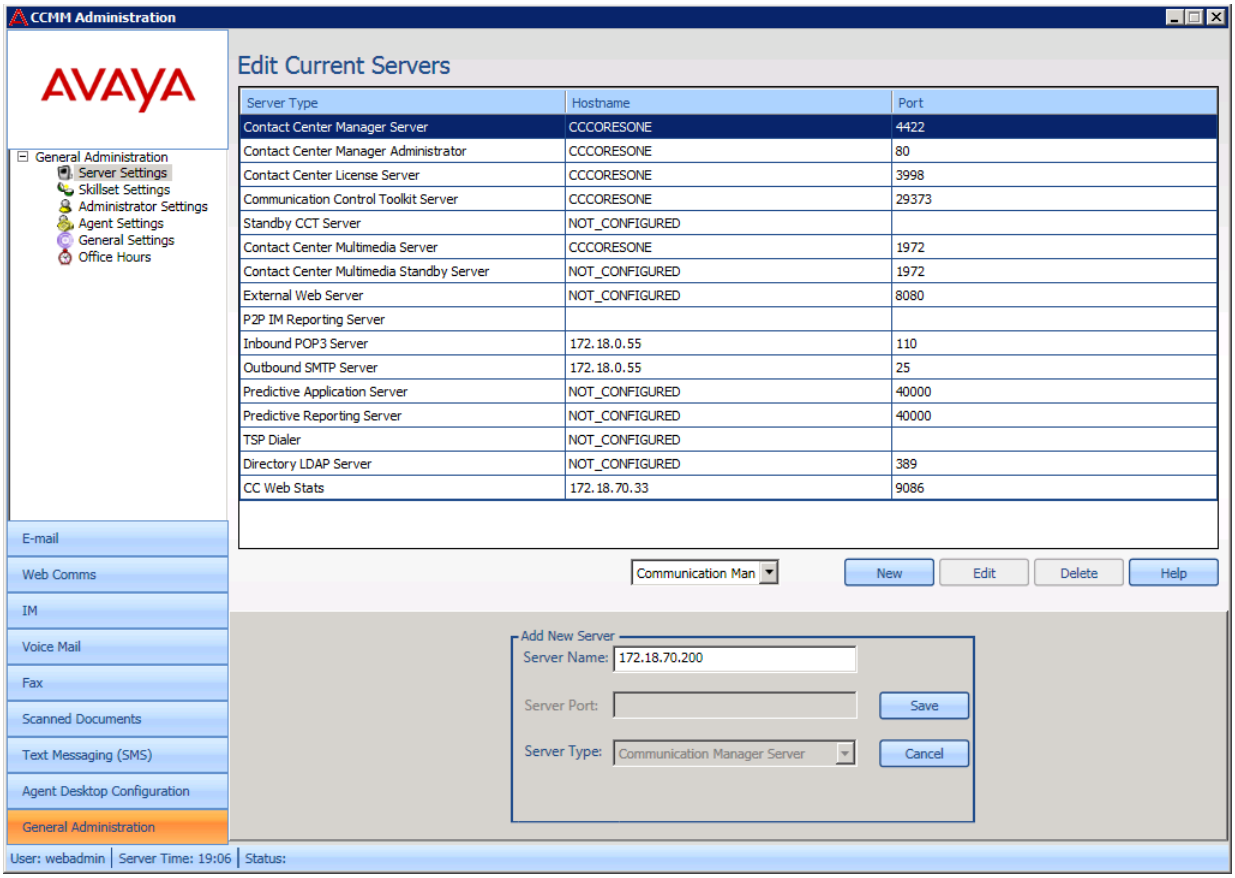
9 Click **New**.



10 From the list, select **Communication Manager Server**.



11 In the **Server Name** box, type the IP address of the Communication Manager server, for example **172.18.70.200**.



12 Click **Save**.



--End--

Verifying the multimedia license type

Verify that the license type for the Contact Center Multimedia server matches the system license for your contact center.

Nodal licensing is for single sites of Contact Center; corporate licensing enables multiple sites.

Procedure steps

Step	Action
1	In the CCMM Administration Client, in the left column, click **General Administration**.
2	Click **General Settings**.
3	Under **License Type**, verify that **Nodal** is the selected license type.
4	If the selected license type is not Nodal, select **Nodal** and click **Save**.

5 Click **Save**.

--End--

Configuration Section

Contact Center Manager Server configuration

This section describes how to configure Contact Center Manager Server as a Multimedia Complement to Call Center Elite. Perform these tasks using Contact Center Manager Administration.

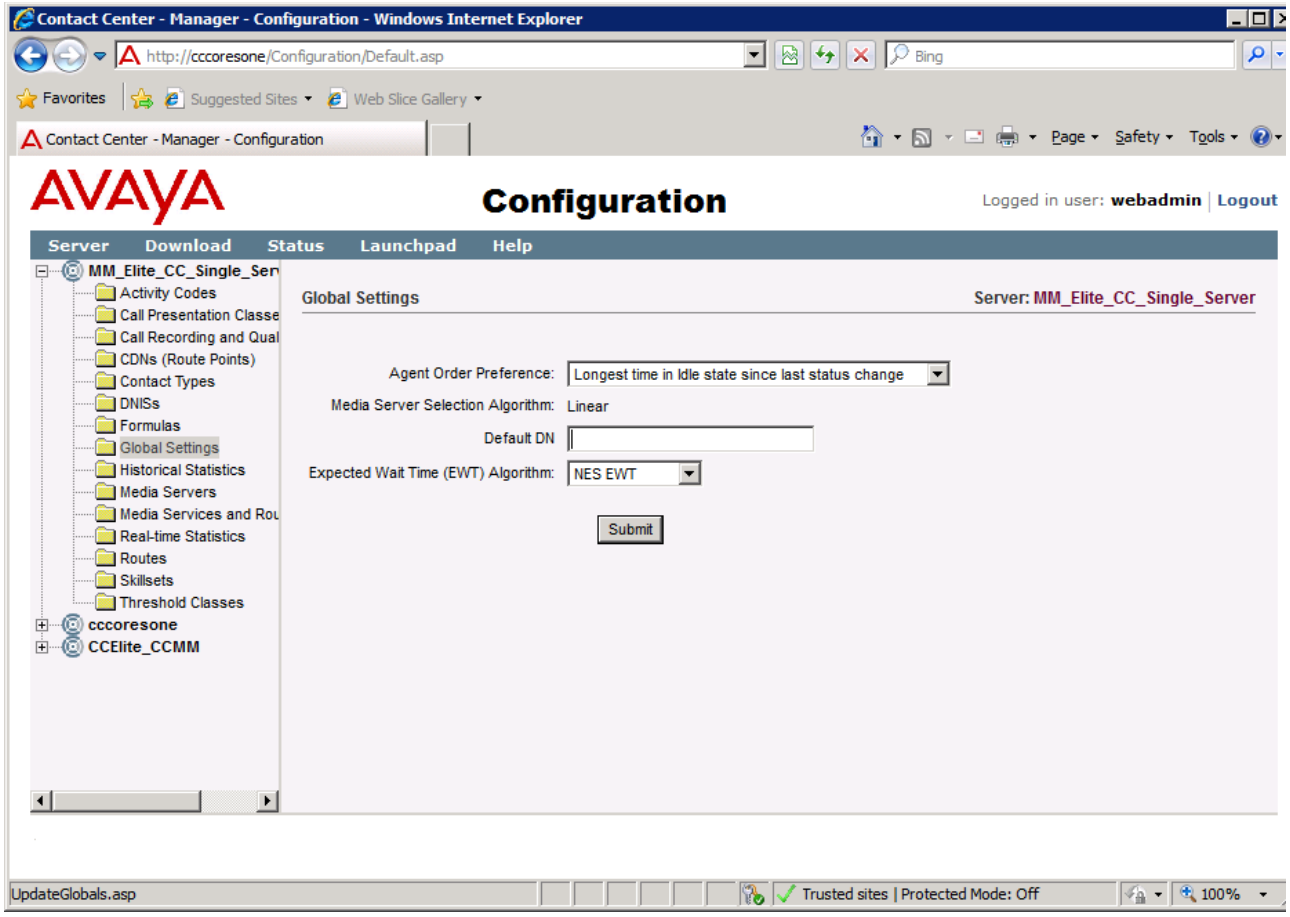
Configuring Contact Center Manager Server Global Settings

Configure Contact Center Manager Server Global Settings to setup Agent Order Preference, Default DN, Expected Wait Time algorithm, and the server designated for historical statistical data.

On the PABX, configure a number to which Contact Center Manager Server can send treated calls that a contact center script defaults, and to catch calls not answered by agents. Avaya recommends that you configure an attendant console as the Default DN.

Procedure steps

Step	Action
1	On the Contact Center server, start Internet Explorer.
2	In the **Address** box, type the CCMA URL in the format http://<Server name>, for example **http://CCCORESONE**.
3	Press **Enter**.
4	In the main logon window, in the **User ID** box, type **webadmin**.
5	In the **Password** box, type the password, for example **nimdabew**.
6	On the **Launchpad**, select **Configuration**.
7	In the left pane, expand the Contact Center server, for example **MM_Elite_CC_Single_Server**.
8	Select the **Global Settings** folder.
9	From the **Agent Order Preference** list, select **Longest time in Idle status since last status change**.
10	Clear the **Default DN** box; this is not relevant for an Elite Complement configuration.



11 Click **Submit**.

--End--

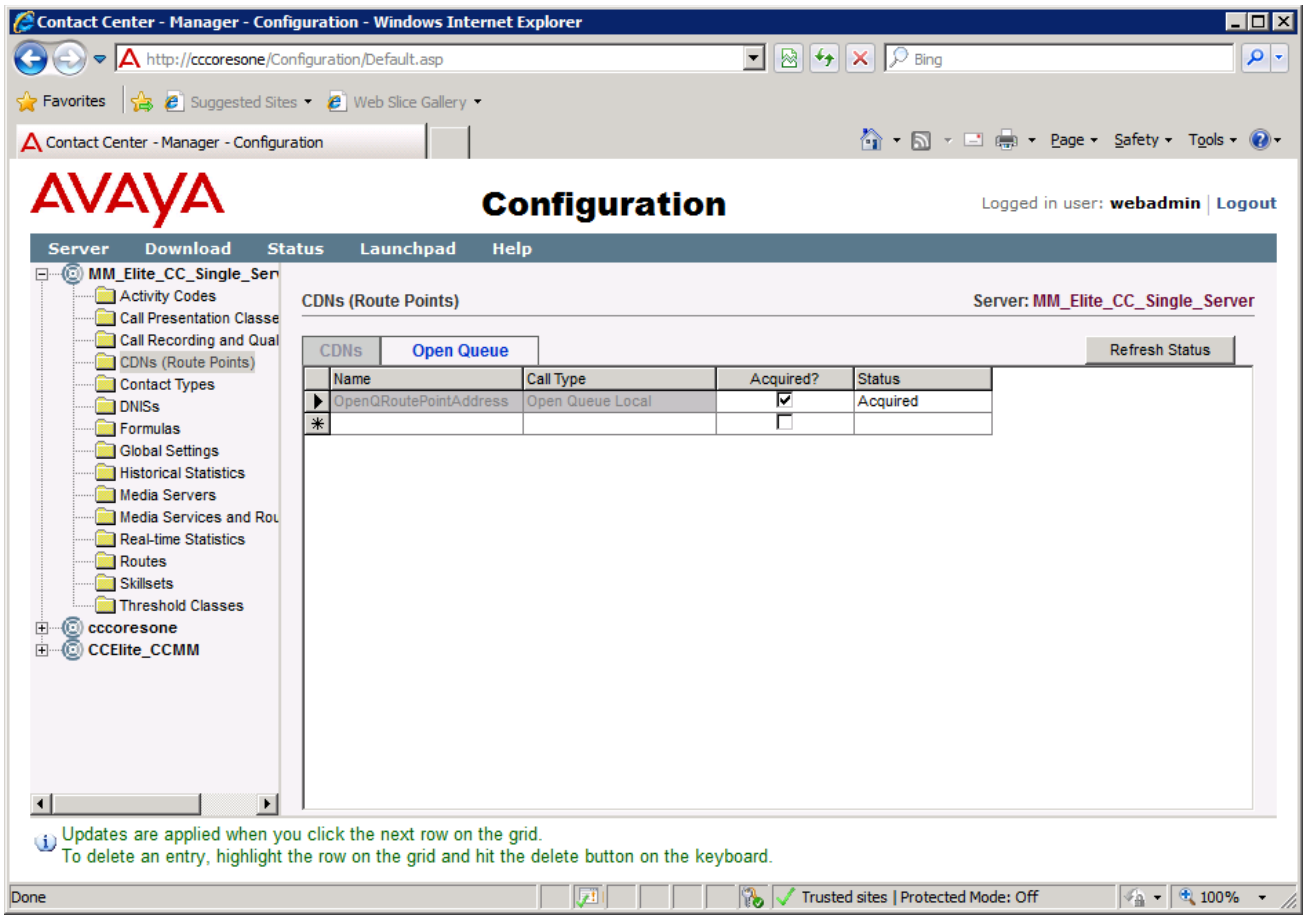
Adding a route point for e-mail skillsets

Add a route points for the e-mail skillsets.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration **Launchpad**, click **Configuration**.
2	In the left pane, expand the Contact Center server, for example **MM_Elite_CC_Single_Server**.
3	Select the **CDNs (Route Points)** folder.

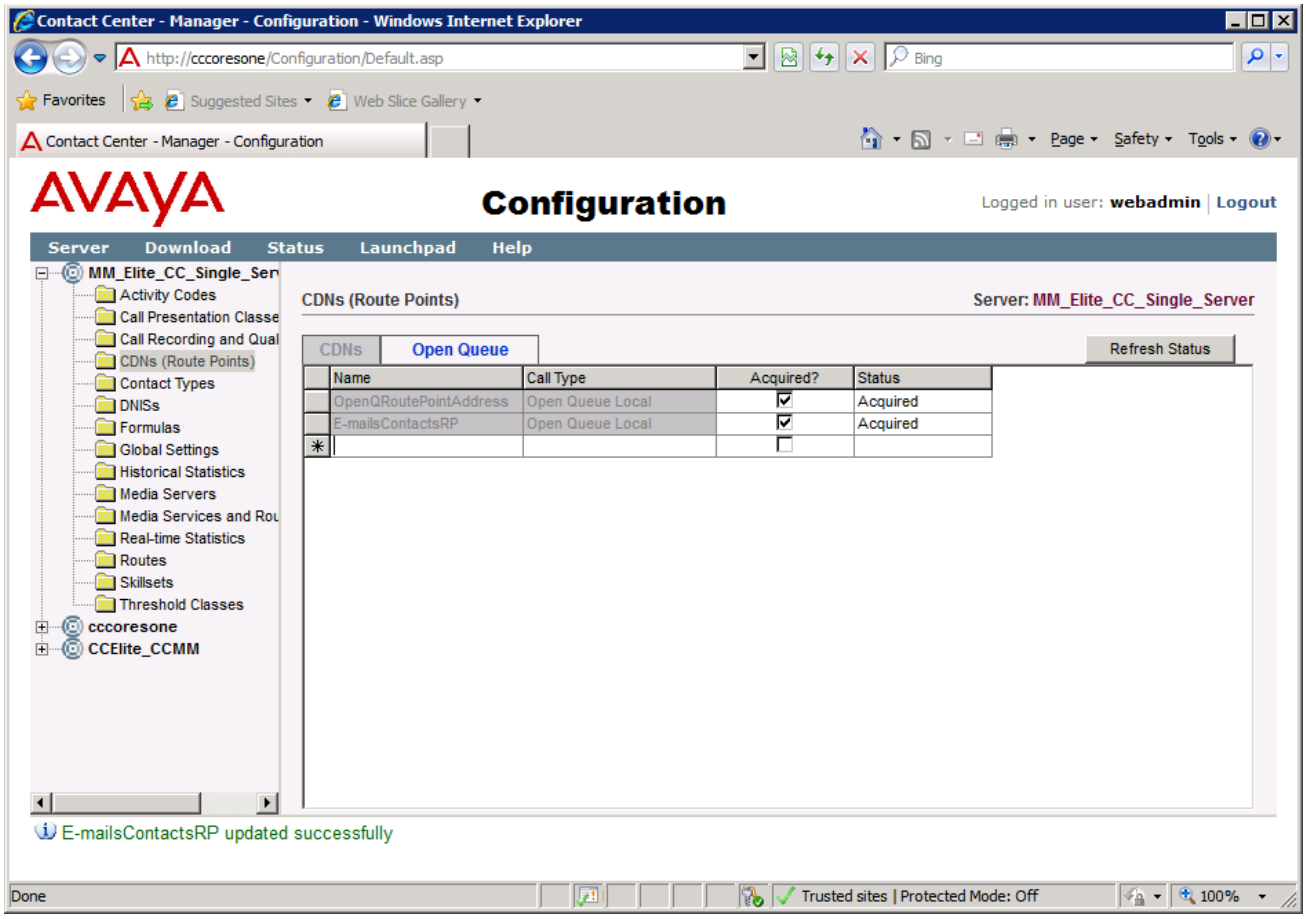
4 On the **CDNs (Route Points)** window, select the **Open Queue** tab.



5 In the **Name** box, type a name for the new route point, for example **E-mailsContactsRP**.

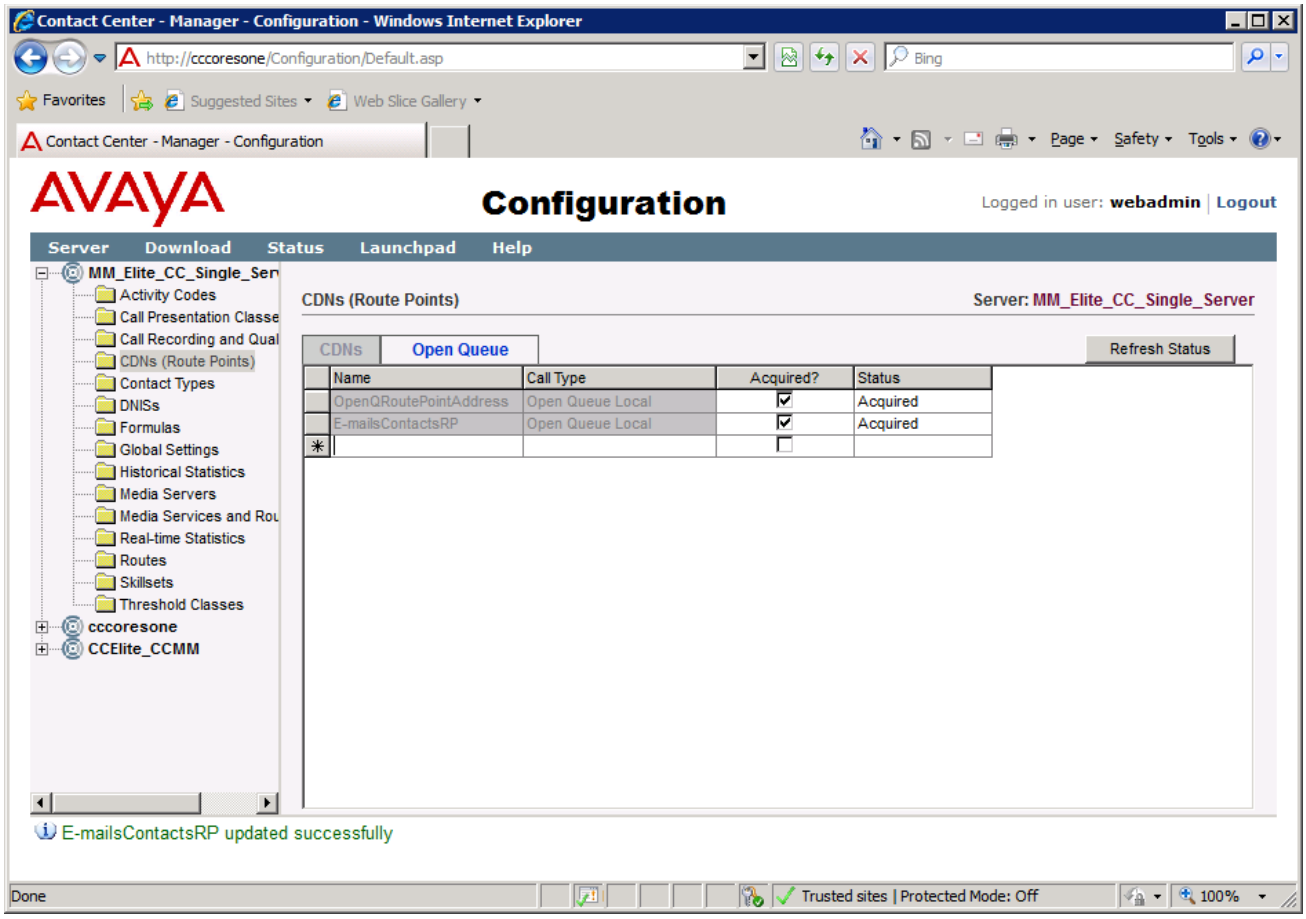
6 From the **Call Type** list, select **Open Queue Local**.

7 Select **Acquired**.



8 Press **Enter**.

The system saves the route point and automatically acquires it.



--End--

Creating a skillset threshold class

Create a threshold class for the e-mail skillset to specify how statistics appear in reports and real-time displays.

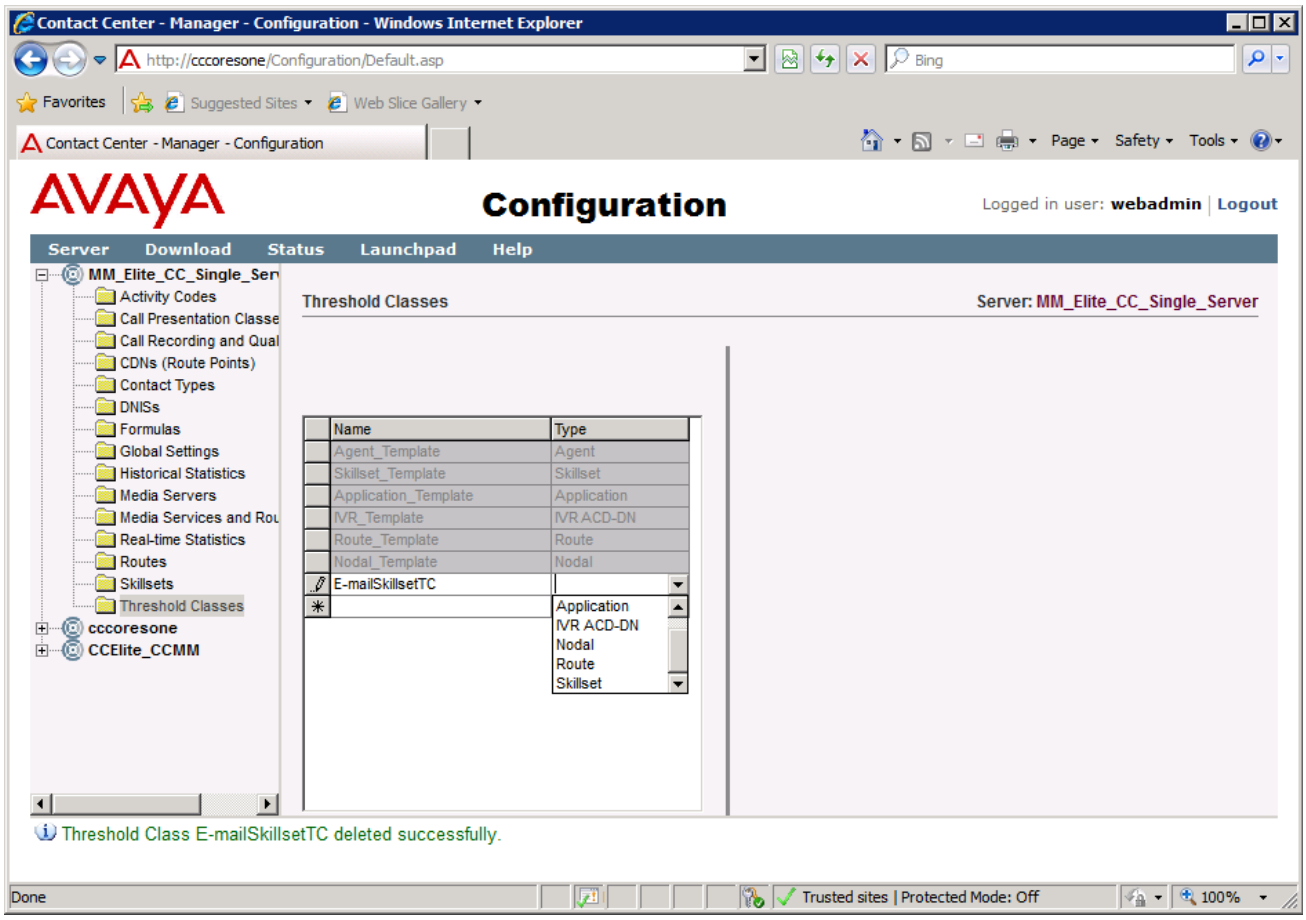
The threshold class for this skillset highlights thresholds on the number of contacts waiting, agents with the longest wait since last call, and agents not ready on the skillset.

This threshold class causes the skillset to show Yellow in Real Time Displays if the number of contacts waiting is greater than or equal to 2, if any agent's longest wait since the last contact is greater than or equal to 35, or if the number of agents Not Ready is greater than or equal to 3. It causes the skillset to show

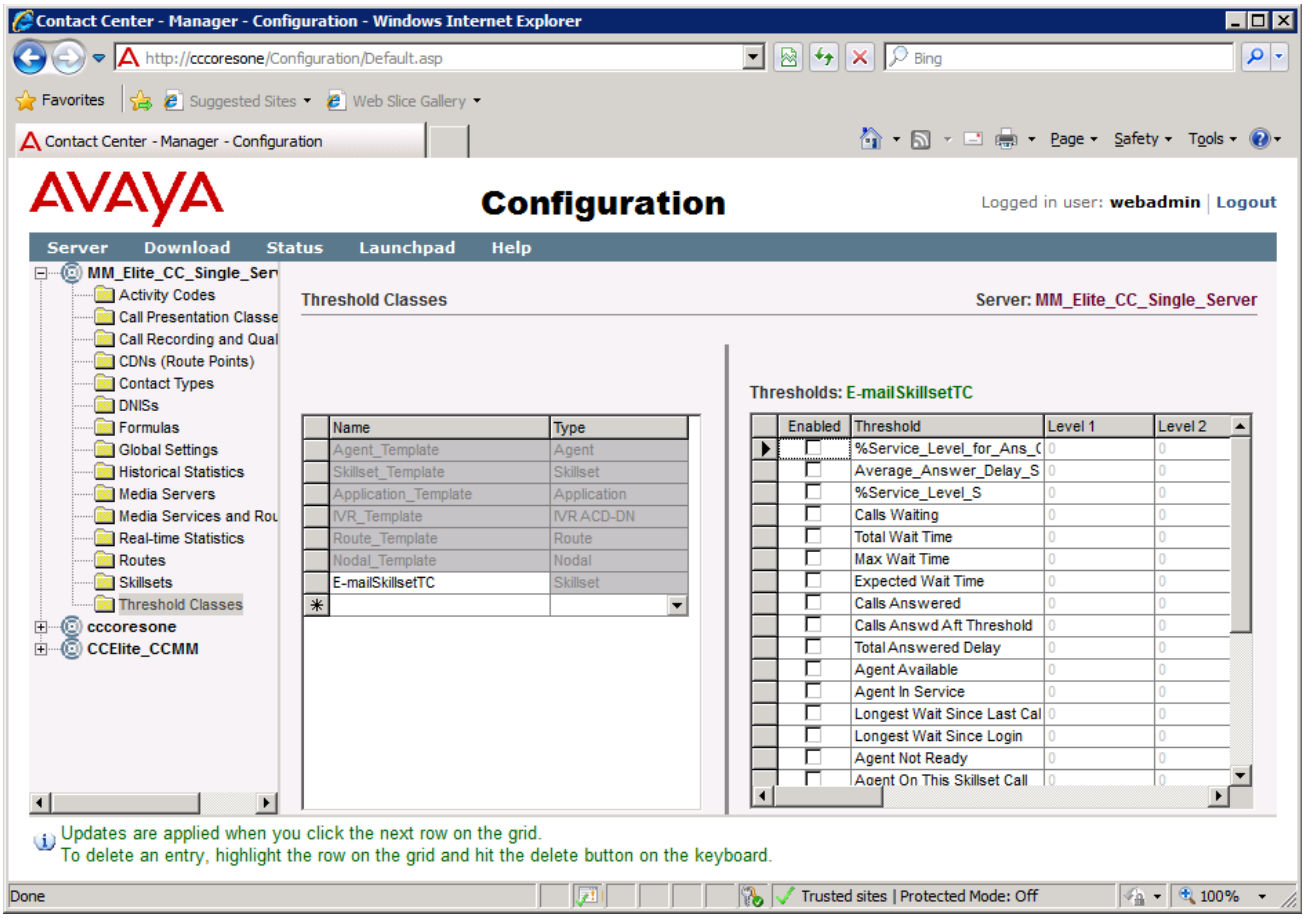
Red if the number of contacts waiting is greater than or equal to 5, if any agent's longest wait since the last contact is greater than or equal to 65, or if the number of agents Not Ready is greater than or equal to 5.

Procedure steps

Step	Action
1	In the left pane, expand the Contact Center server, for example **MM_Elite_CC_Single_Server**.
2	Select the **Threshold Classes** folder.
3	In the right pane, in the **Name** box, type the name of a new threshold class, for example E-mailSkillsetTC.
4	From the **Type** list, select **Skillset**.



Step	Action
5	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.*



6 In the **Thresholds** table, select **Calls Waiting**.

7 In the **Level 1** box, type the number of waiting e-mail messages that trigger the first threshold, for example 2.

8 In the **Level 2** box, type the number of waiting e-mail messages that trigger the second threshold, for example 5.

9 Select **Longest wait since last call**.

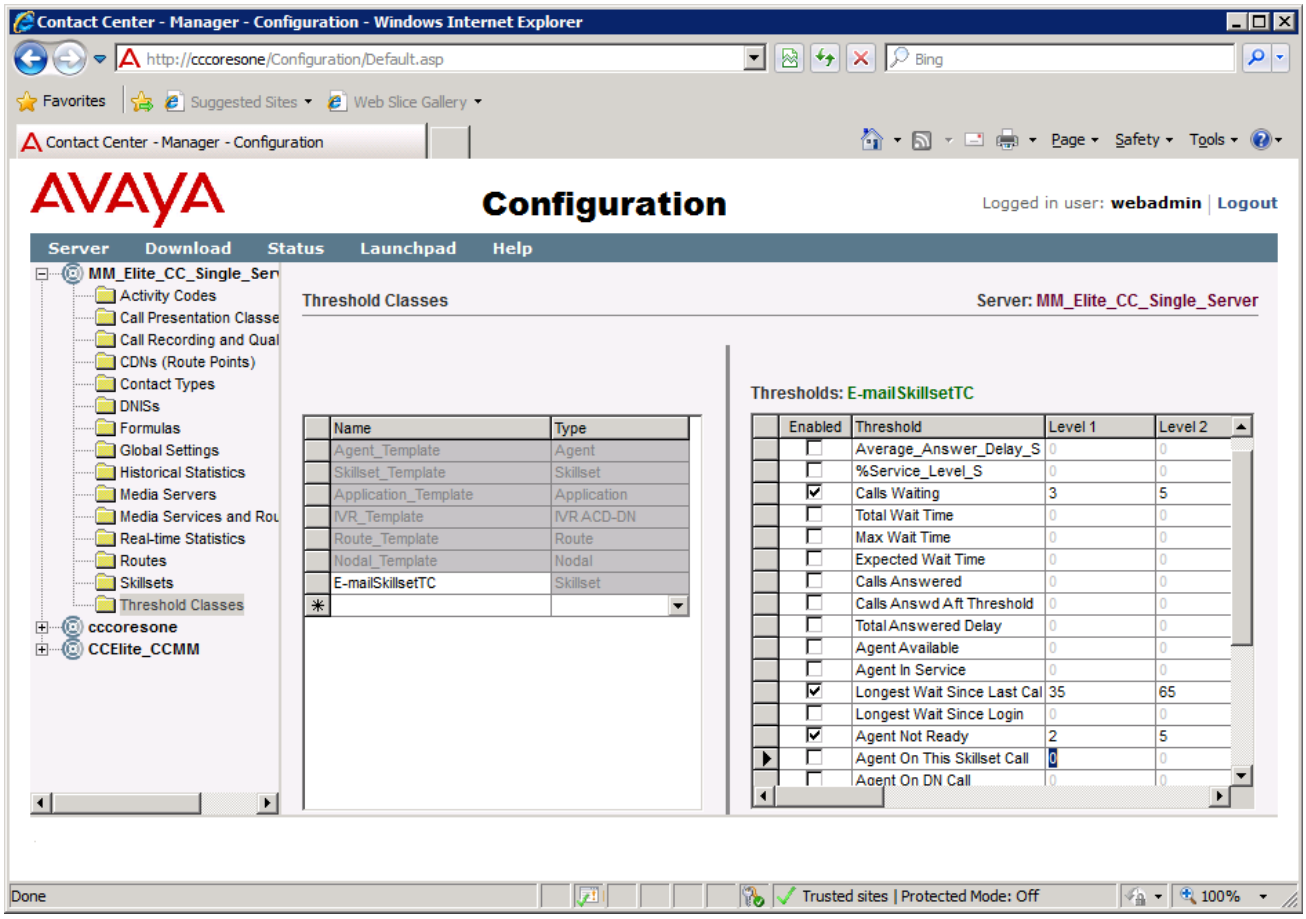
10 In the **Level 1** box, type the number of seconds an agent remains idle after closing a contact that trigger the first threshold, for example 35.

11 In the **Level 2** box, type the number of seconds an agent remains idle after closing a contact that trigger the second threshold, for example 65.

12 Select **Agent Not Ready**.

13 In the **Level 1** box, type the number of idle agents that trigger the first threshold, for example 2.

14 In the **Level 2** box, type the number of idle agents that trigger the second threshold, for example 5.



15 Click any other row in the grid to submit your changes.

--End--

Configuring activity codes

Configure a Contact Center activity code for each Aux Work reason code on Call Center Elite. You map the Contact Center codes to the Call Center Elite codes so that the agent can select a single option on Agent Desktop, which sends correct codes to both systems. You complete the mapping of the codes when you set up agent templates.

The Contact Center system already includes the following default activity codes:

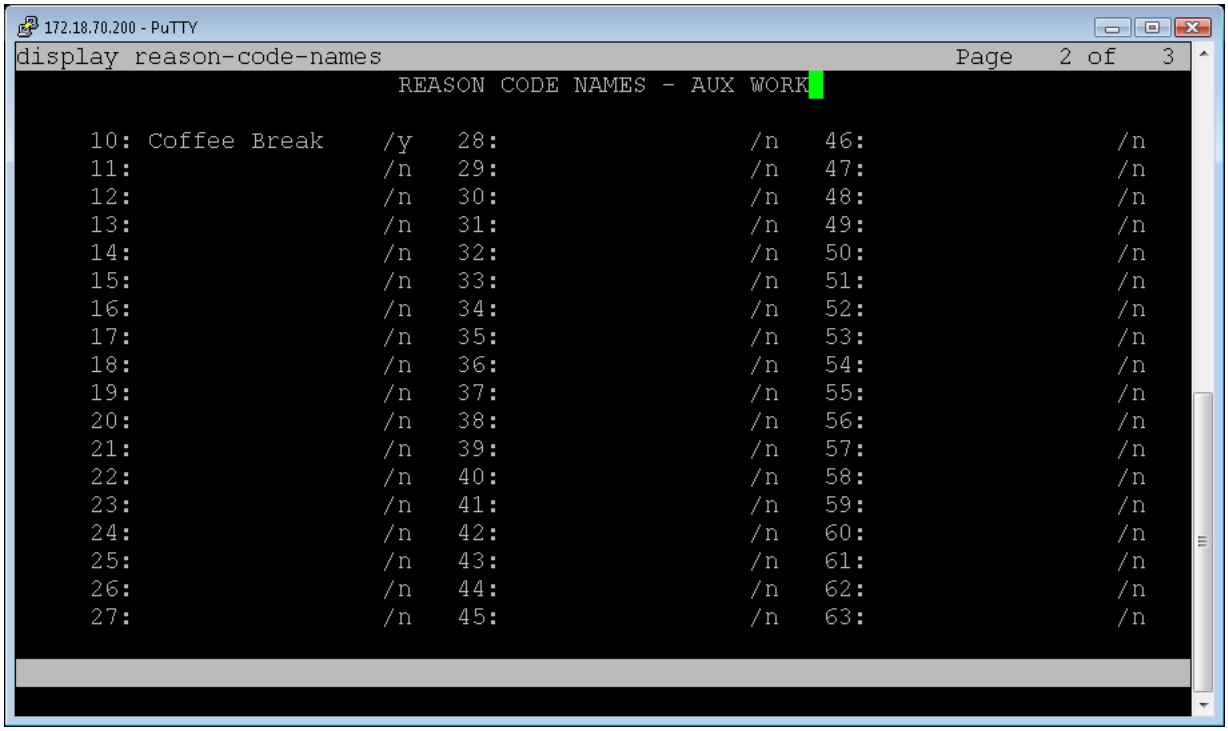
- activity code 000 (Not_Ready_Default_Reason_Code)

- activity code 00 (Skillset_Default_Activity_Code)
- activity code 0 (System_Default_Activity_Code)

Contact Center assigns a default activity code to a contact if the contact is not queued to a skillset and if no other activity code is assigned.

Procedure steps

Step	Action
1	Access the Call Center Elite administrative tool.
2	Navigate to the Aux Work reason codes screen.
3	Note all the Aux Work reason code numbers and names configured on Call Center Elite, for example **10: Coffee Break**.



4	On the Contact Center server, start Internet Explorer.
5	In the **Address** box, type the CCMA URL in the format http://<Server name>, for example **http://CCCORESONE**.
6	Press **Enter**.
7	In the main logon window, in the **User ID** box, type **webadmin**.
8	In the **Password** box, type the password, for example **nimdabew**.
9	On the **Launchpad**, select **Configuration**.

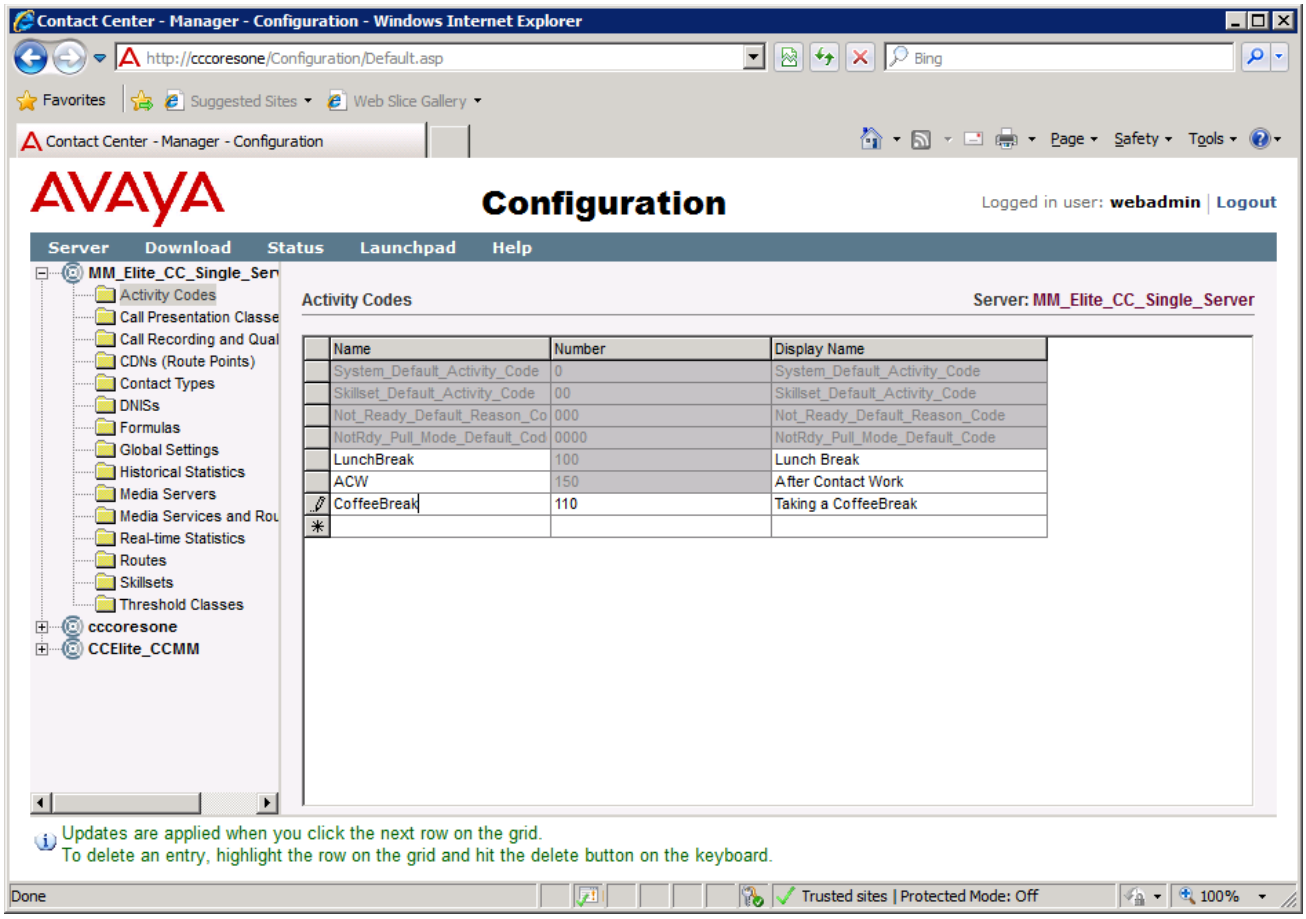
10 In the left pane, expand the contact center server, for example **MM_Elite_CC_Single_Server**.

11 Select the **Activity Codes** folder.

12 In the right pane, in the **Activity Codes** table, in **Name** box, type **CoffeeBreak**.

13 In the **Number** box, type a number for the code, for example **110**. This is the Contact Center activity code number agents select on Agent Desktop when they go on a coffee break.

14 In the **Display Name** box, type **Taking a CoffeeBreak**. This is how the activity code appears in Contact Center reports.



15 Click any other row to save your changes.

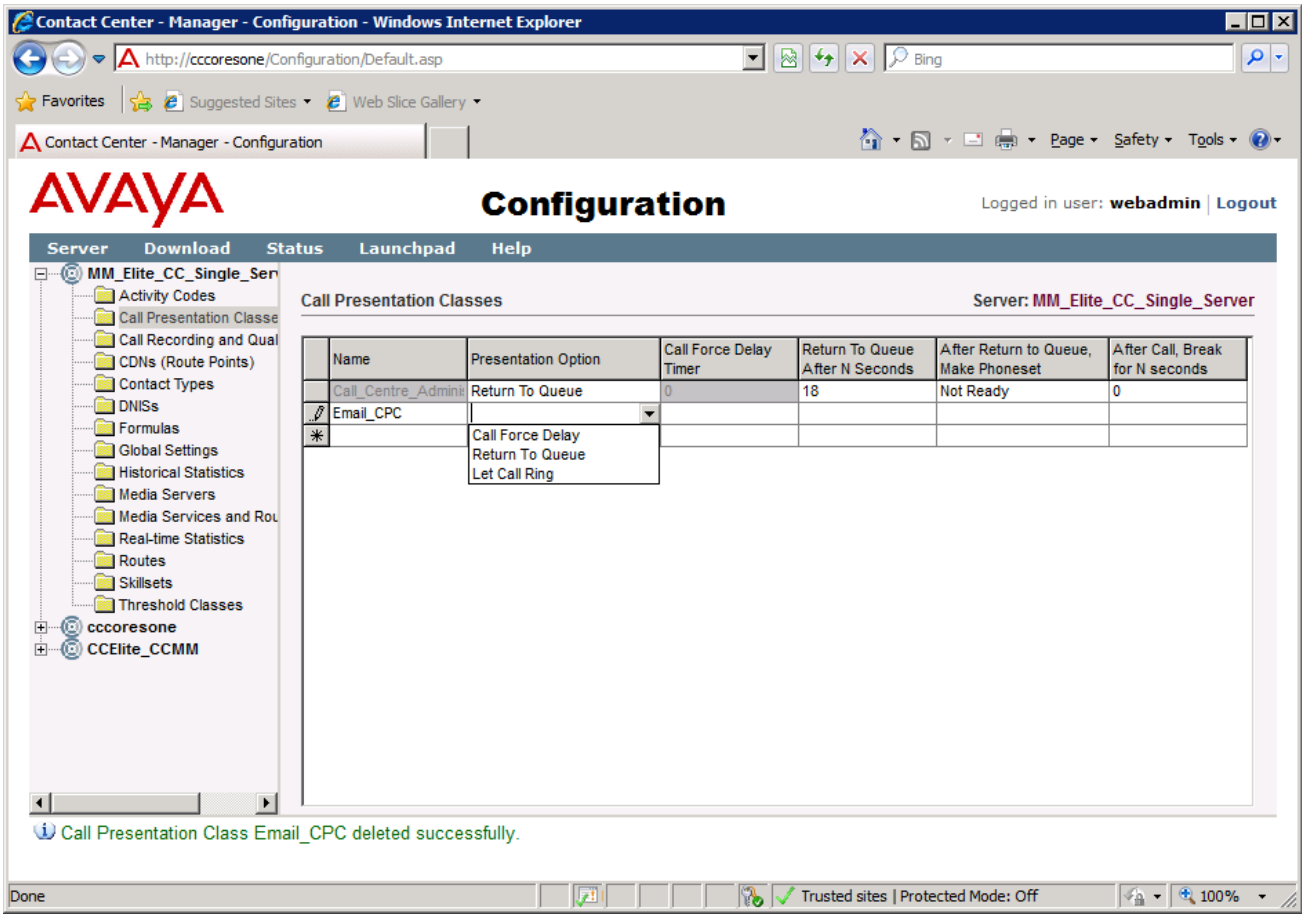
--End--

Creating a call presentation class

Create a call presentation class to determine how the system presents contacts to an agent. This call presentation class returns the contact to the queue if the agent does not answer it in 30 seconds, and allows the agent a 30 second period after closing the contact in which to complete post-contact tidy up work. If it returns the call to the queue, it also places the agent in a Not Ready status.

Procedure steps

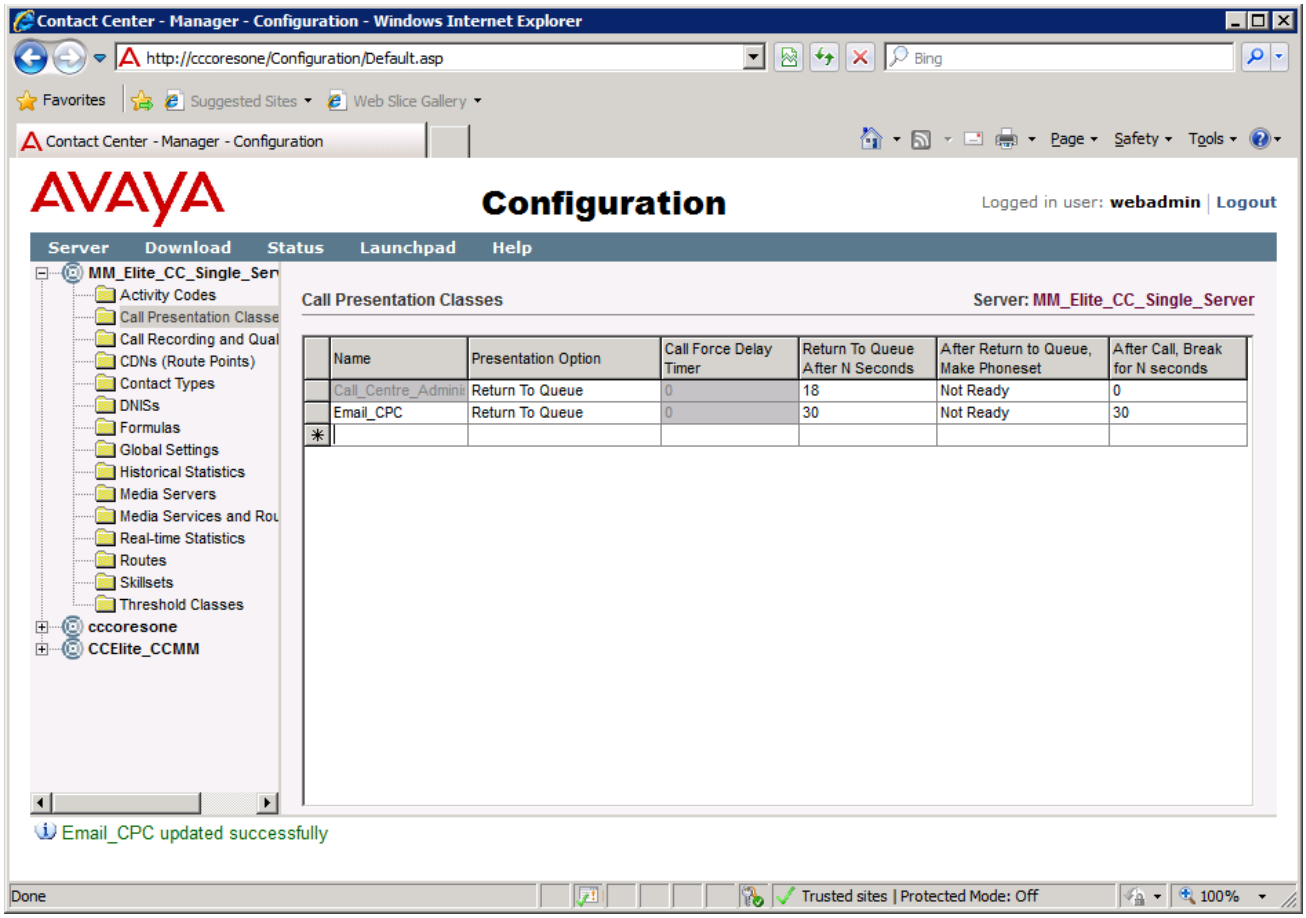
Step	Action
1	Select the **Call Presentation Classes** folder.
2	In the right pane, in the **Name** box, type the name for a new call presentation class, for example **Email_CPC**.
3	From the **Presentation Option** list, select **Return to Queue**.



Step	Action
4	In the **Return to Queue After N Seconds** box, type **30**. This is the time after which the contact returns to the queue if the agent does not open it.

5 From the **After Return to Queue, Make Phoneset** list, select **Not Ready**. This ensures the system makes the agent not ready if they fail to open a presented contact within 30 seconds.

6 In the **After Call, Break for N Seconds** box, type the amount of time that the agent is in break state after a call ends, for example **30**.



7 Click any other row in the grid to submit your changes and to save the call presentation class.

--End--

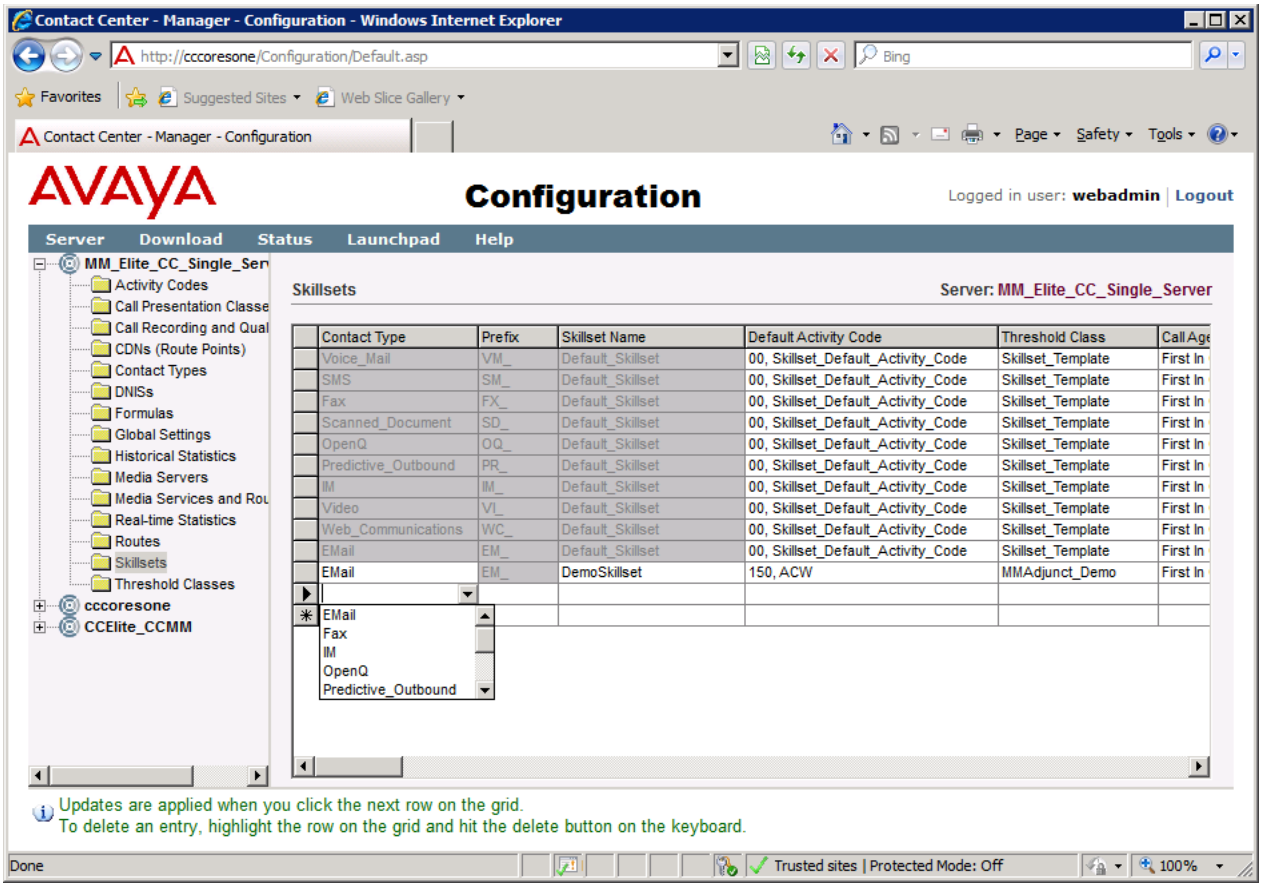
Adding the e-mail skillset

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. Contact Center uses skillsets to match callers with the agents who can best meet the

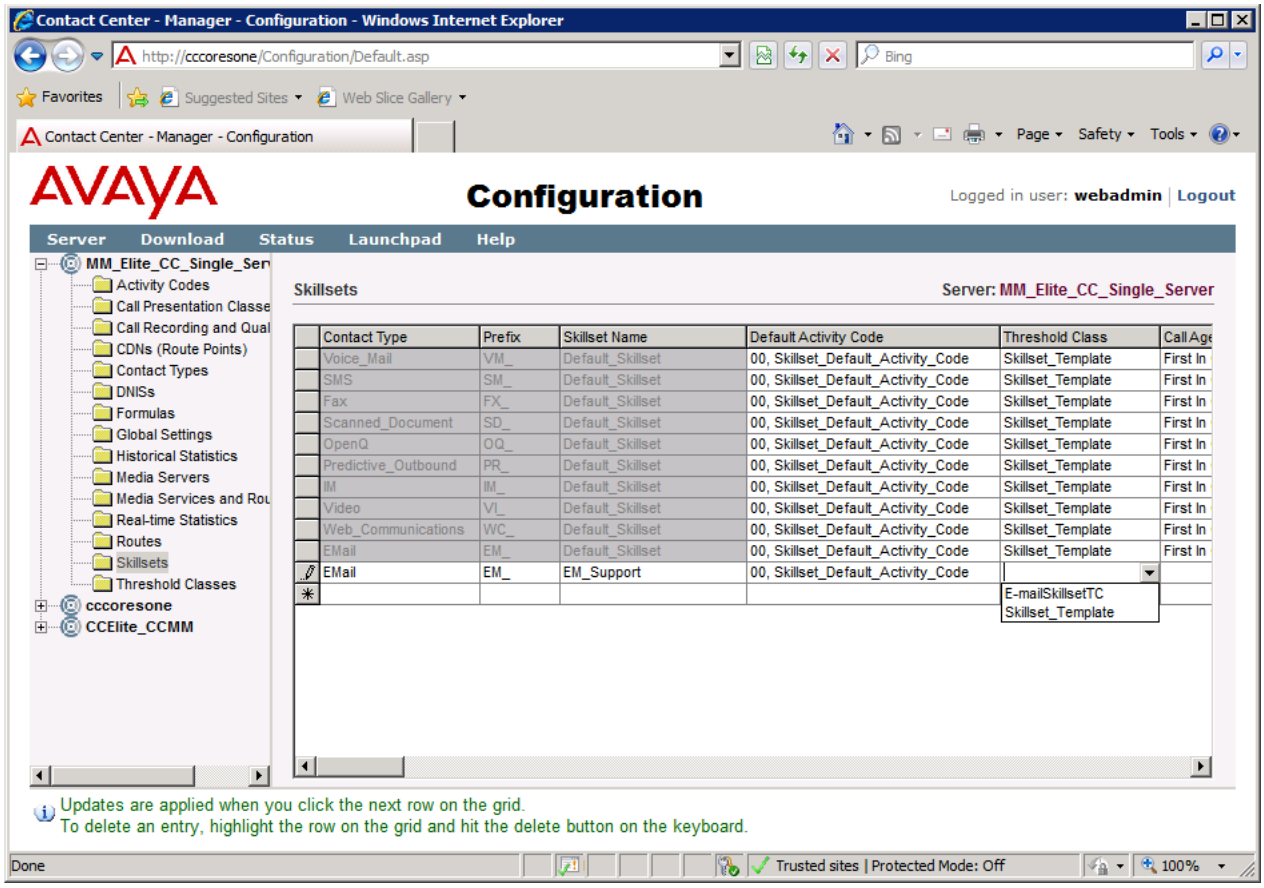
callers' needs. When you complete Multimedia configuration you link the skillset with the e-mail inbox: when you complete agent configuration you link the agent with the skillset.

Procedure steps

Step	Action
1	In the left pane, select the **Skillsets** folder.
2	From the **Contact Type** list, select **EMail**. CCMA automatically populates the **Prefix** field with the skillset name prefix **EM**.

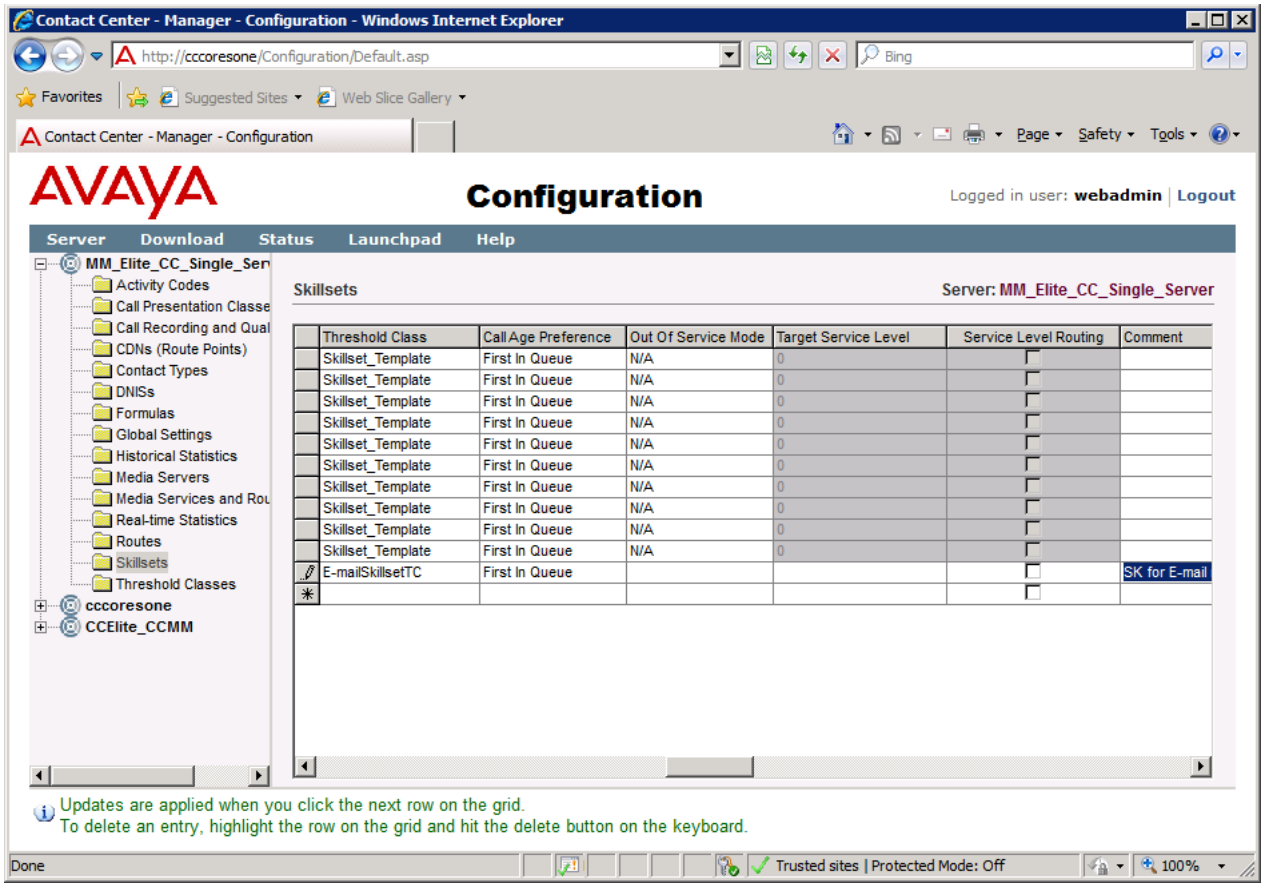


3	In the **Skillset Name** box, type a name for the skillset, for example **EM_Support**.
4	For **Default Activity Code**, accept the default, **00_Skillset_Default_Activity_Code**.
5	From the **Threshold Class** list, select the threshold class associated with this skillset, for example **E-mailSkillsetTC**.



6 From the **Call Age Preference** list, select the method to configure the order of contacts in the queue, for example select **First In Queue**. (This gives priority to the first contact in the queue).

7 In the **Comment** box, type any comments you have about the skillset, for example **SK for E-mail**.



8 Click any other row in the grid to save your changes.

--End--

Contact Center Multimedia configuration

This section describes how to configure Contact Center Multimedia to process e-mail messages. Perform these tasks using the CCMM Administration client, which you access through Contact Center Manager Administration.

In the example solution, the mailbox that Contact Center monitors is ccemailin, on a POP3 mailserver with an IP address 172.18.0.55. When Contact Center retrieves messages from the ccemailin, it searches them for the keywords "support" and "assistance". If the e-mail message includes either or both of these words, Contact Center creates the e-mail contact and assigns it to the EM_EM_Support skillset. If the e-mail message does not include either or of these words, it matches the System Default Rule. Contact Center creates the e-mail contact and assigns it to the default e-mail skillset, EM_Default_Skillset.

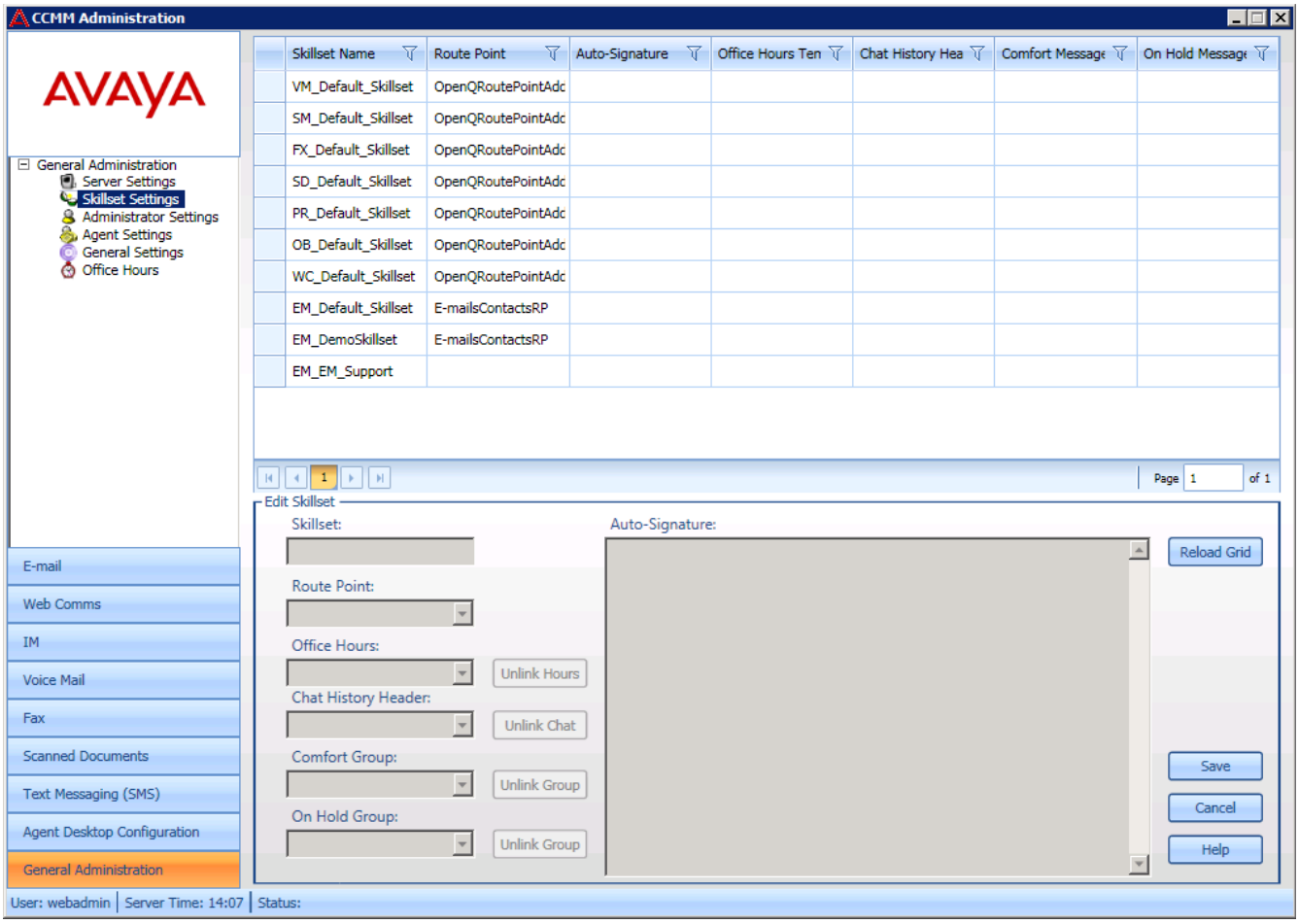
Configuring the multimedia skillsets

Configure the e-mail multimedia skillset in the CCMM Administration client to ensure that you can route e-mail contacts to agents. You must also configure a route point for each default skillset.

Attention: Depending on the performance of your Contact Center server CPU, it can take several minutes for the skillset you created in the CCMA Configuration component to appear in the CCMM Administration client.

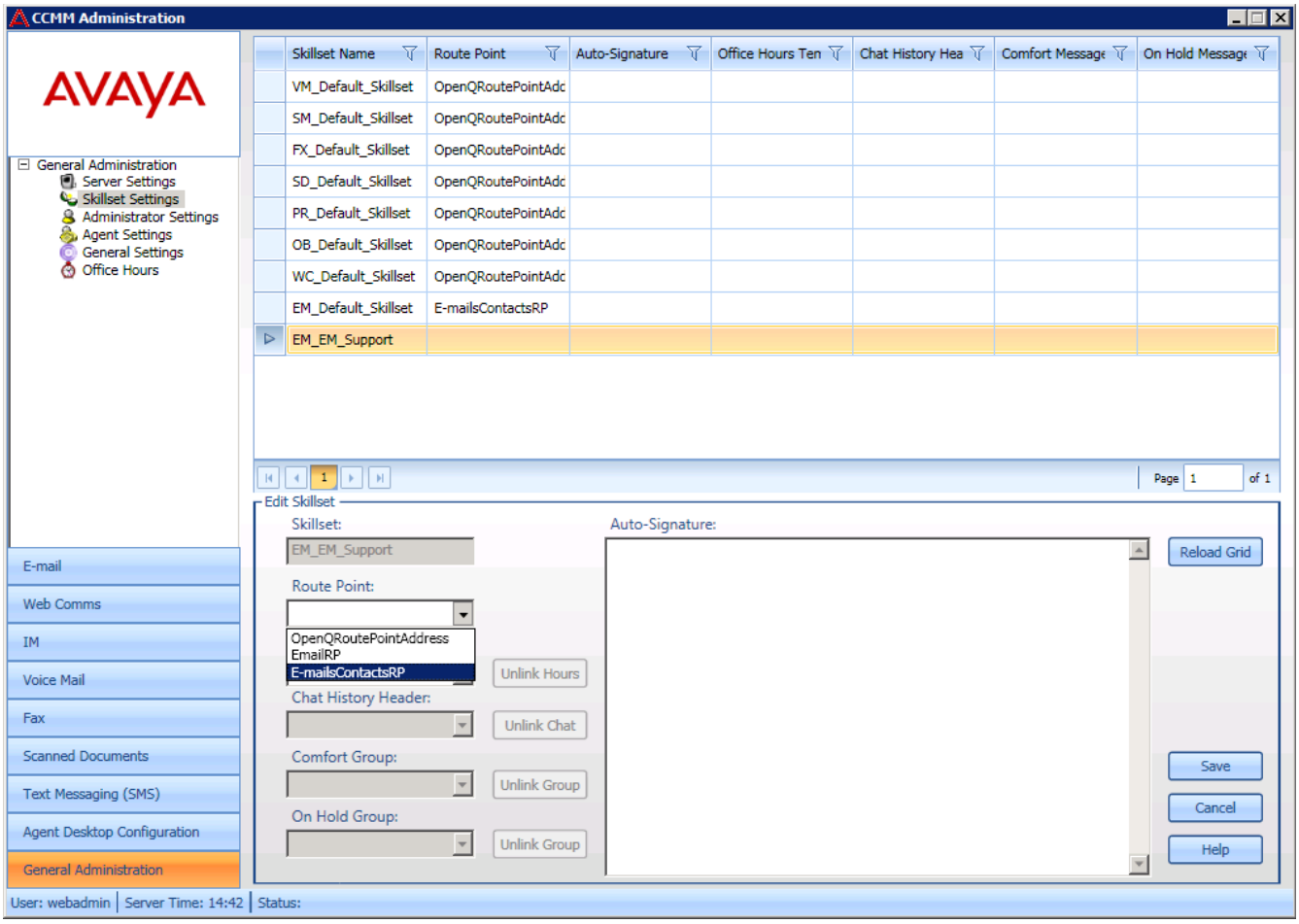
Procedure steps

Step	Action
1	On the CCMA Launchpad, click **Multimedia**.
2	In the left column, select the CCMM server, for example **CCElite_CCMM**.
3	In the right pane, click **Launch Multimedia Client**.
4	On any pop-up dialogs that appear, click **Run**.
5	In CCMM Administration, in the left pane click **Skillset Settings**.



6 In the right pane, select the e-mail skillset, for example **EM_EM_support**.

7 In the bottom pane, from the **Route Point** list, select the e-mail route point, for example **E-mailsContactsRP**.



8 Click **Save**.

9 In the right pane, select **EM_Default_Skillset**.

10 In the bottom pane, from the **Route Point** list, select the e-mail route point, for example **E-mailsContactsRP**.

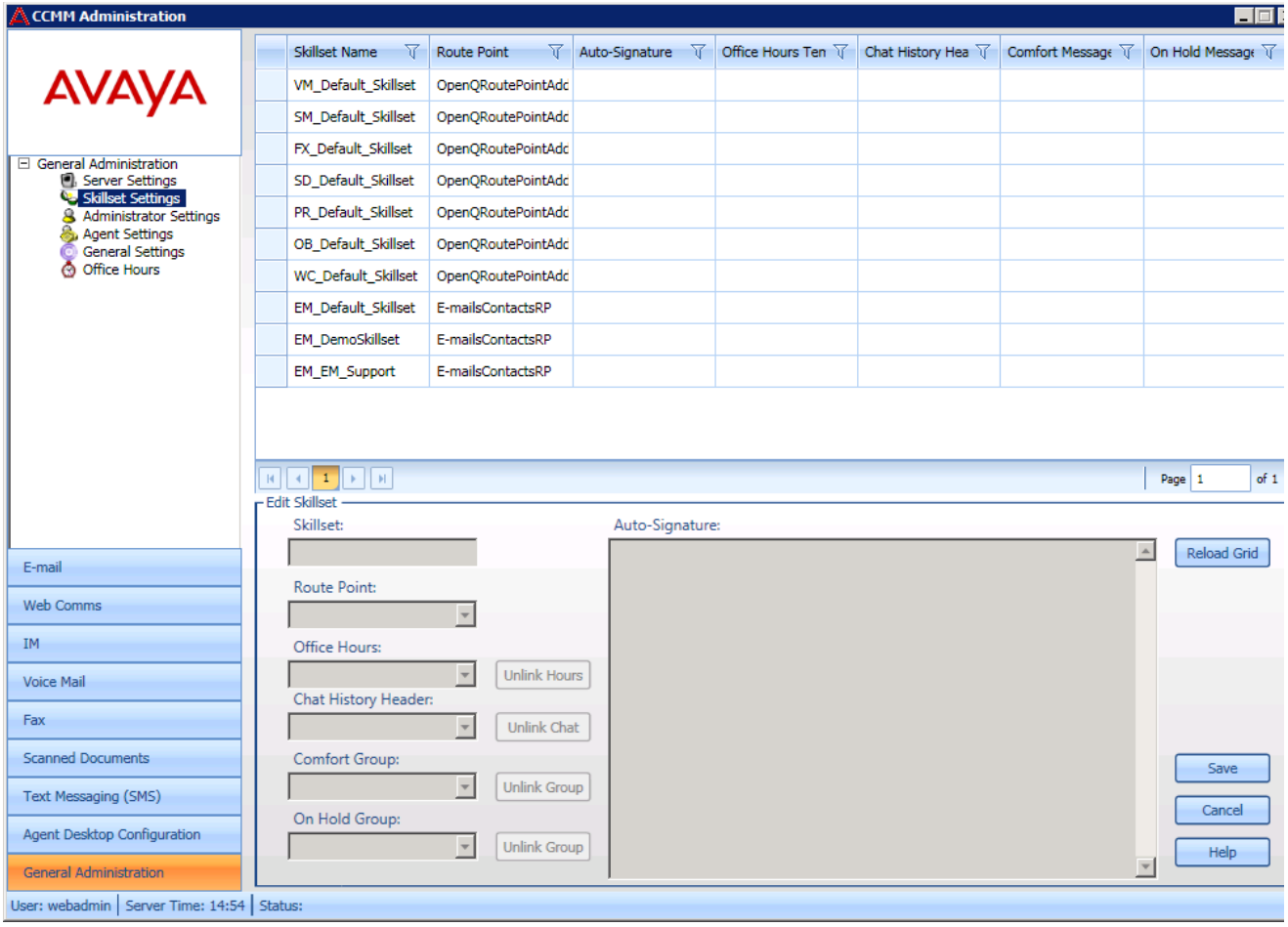
11 Click **Save**.

12 In the right pane, select **VM_Default_Skillset**.

13 In the bottom pane, from the **Route Point** list, select **OpenQRoutePointAddress**.

14 Click **Save**.

15 Repeat step 12 to step 14 for each default skillset. Although this contact center example does not use these contact types, this prevents errors showing in the Multimedia dashboard.



--End--

Adding administrators

Add administrators for the Contact Center Multimedia server to control access to configuration components in your contact center. It is good practise to have a backup administration account as well as the default account.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step **Action**

1. In the Contact Center Manager Administration application, on the Launchpad, click **Multimedia**.
2. In the left column, select the CCMM server, for example **CCElite_CCMM**.
3. In the right pane, click **Launch Multimedia Client**.
4. On any pop-up dialogs that appear, click **Run**.
5. In CCMM Administration, in the left pane click **General Administration**.
6. In the left column, click **General Administration**.
7. Click **Administrator Settings**.
8. Click **New**.
9. In the **General identification** section, type the last name, the first name, and the user name of the Administrator.
10. In the **Contact Details** section, add information about how to contact the Administrator, such as the phone number, fax number, and e-mail address.
11. In the **Password** section type a password and confirm it in the confirm password field.
12. Click **Save**.

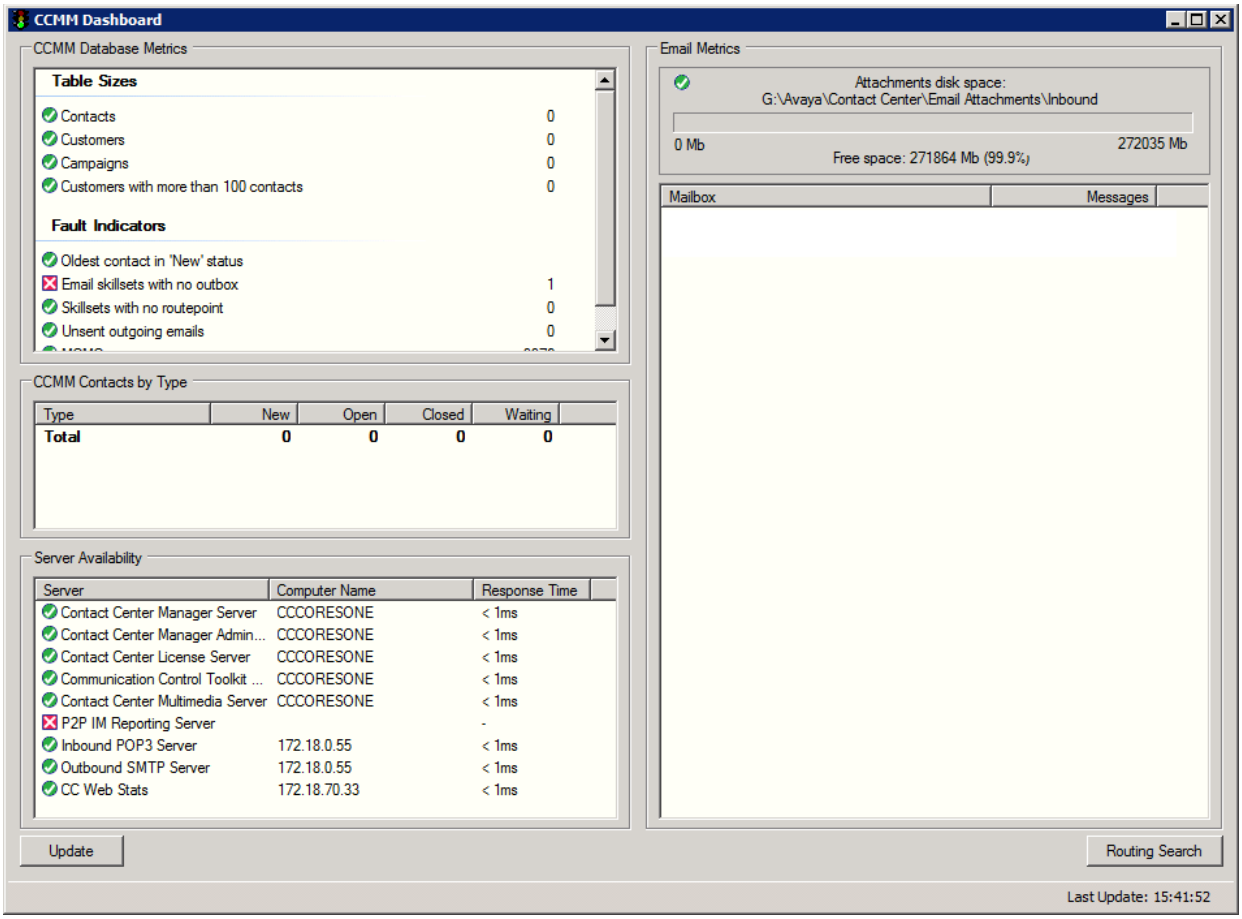
--End--

Checking the status of the multimedia configuration

Use the Multimedia dashboard to check the progress and status of the Multimedia configuration.

Procedure steps

Step	Action
1	Select **Start, All Programs, Avaya, Contact Center, Multimedia server, Multimedia Dashboard**.
2	Review the dashboard information in the **CCMM Database Metrics** box. You see only one error: **E-mail skillsets with no outbox**.



3 Review the dashboard information in the **Server availability** box. You see only one error: **P2P IM Reporting Server**.

4 Review the dashboard information in the **Email Metrics** box. You see no errors and no mailbox or message information.

--End--

Configuring office hours

Configure the days and hours that the contact center is open.

Configuring the office hours is important to determine accurate service levels for e-mail contacts, which may have a delayed response. 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.

The office hour calendar uses sliders to indicate closed times for your contact center.

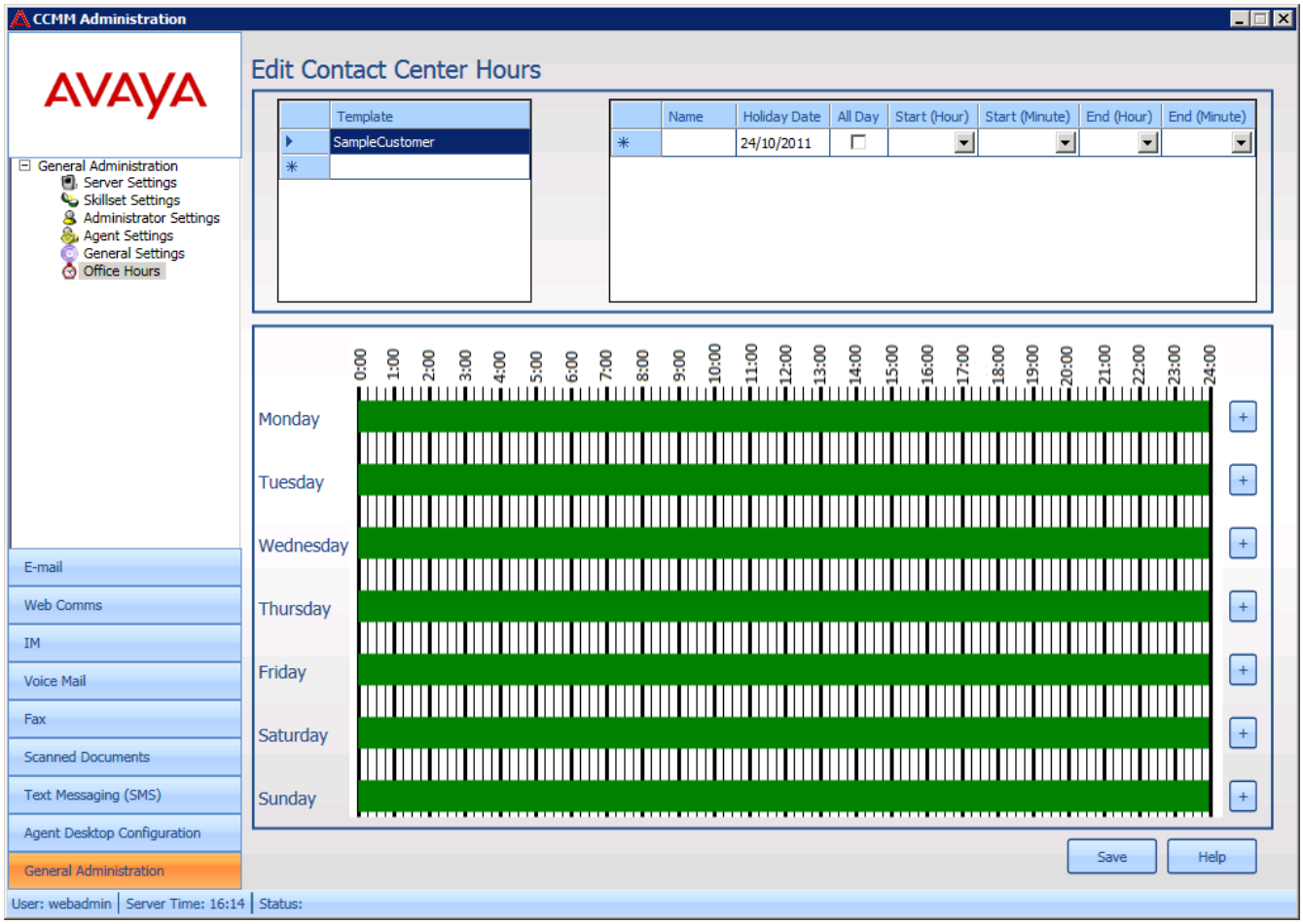
The Start Closed Period slider is a blue triangle ().

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 end of the closed office hours.

Procedure steps

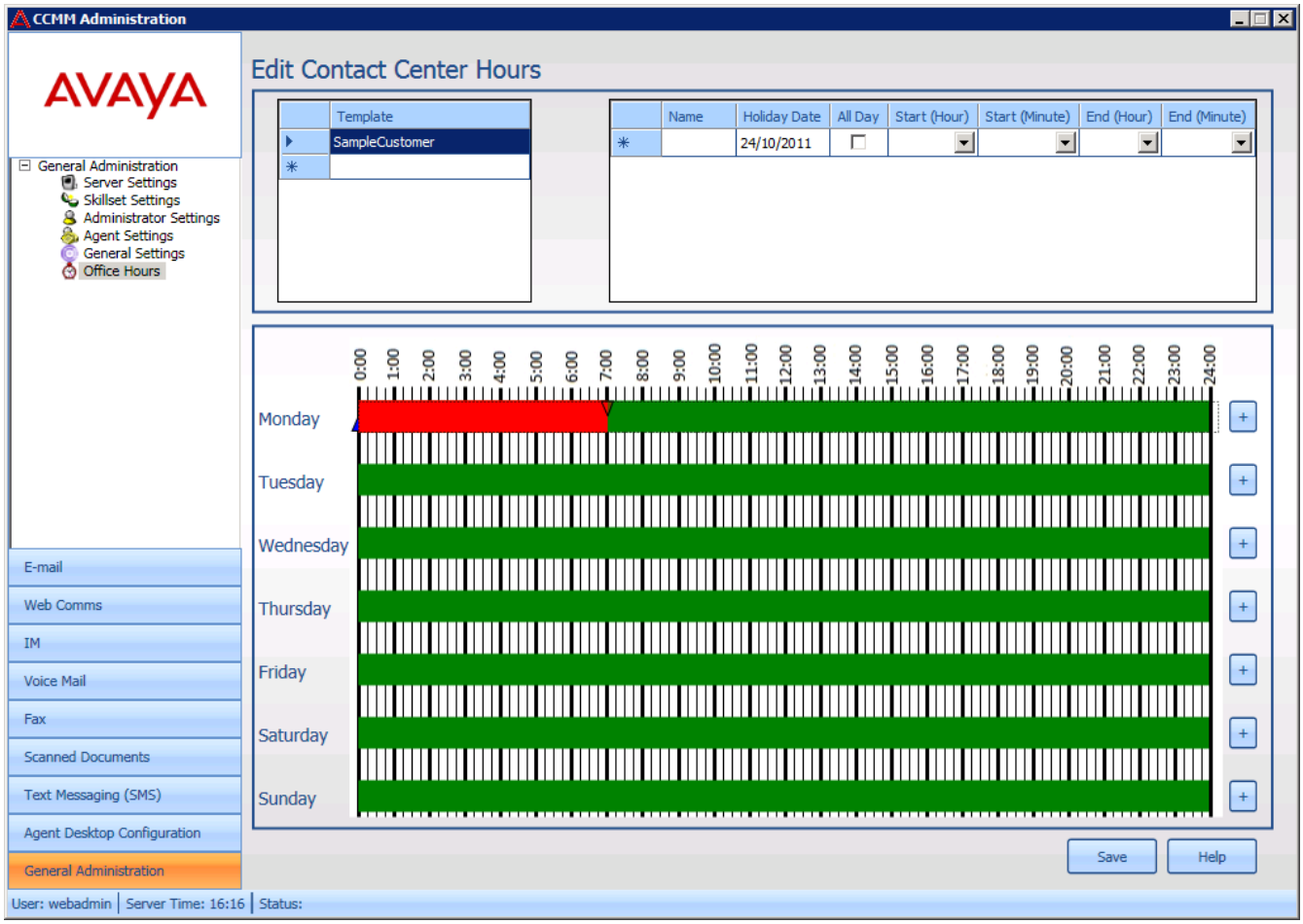
Step	Action
1	In the left column, click **General Administration**.
2	Click **Office hours**.
3	In the **Template** box, type a name for this office hours template, for example **Sample Customer**.



4 On the right of the Monday row, click the plus icon .

5 Move the End Closed Period slider to **7:00**.

The display shows the closed hours for the contact center in red.

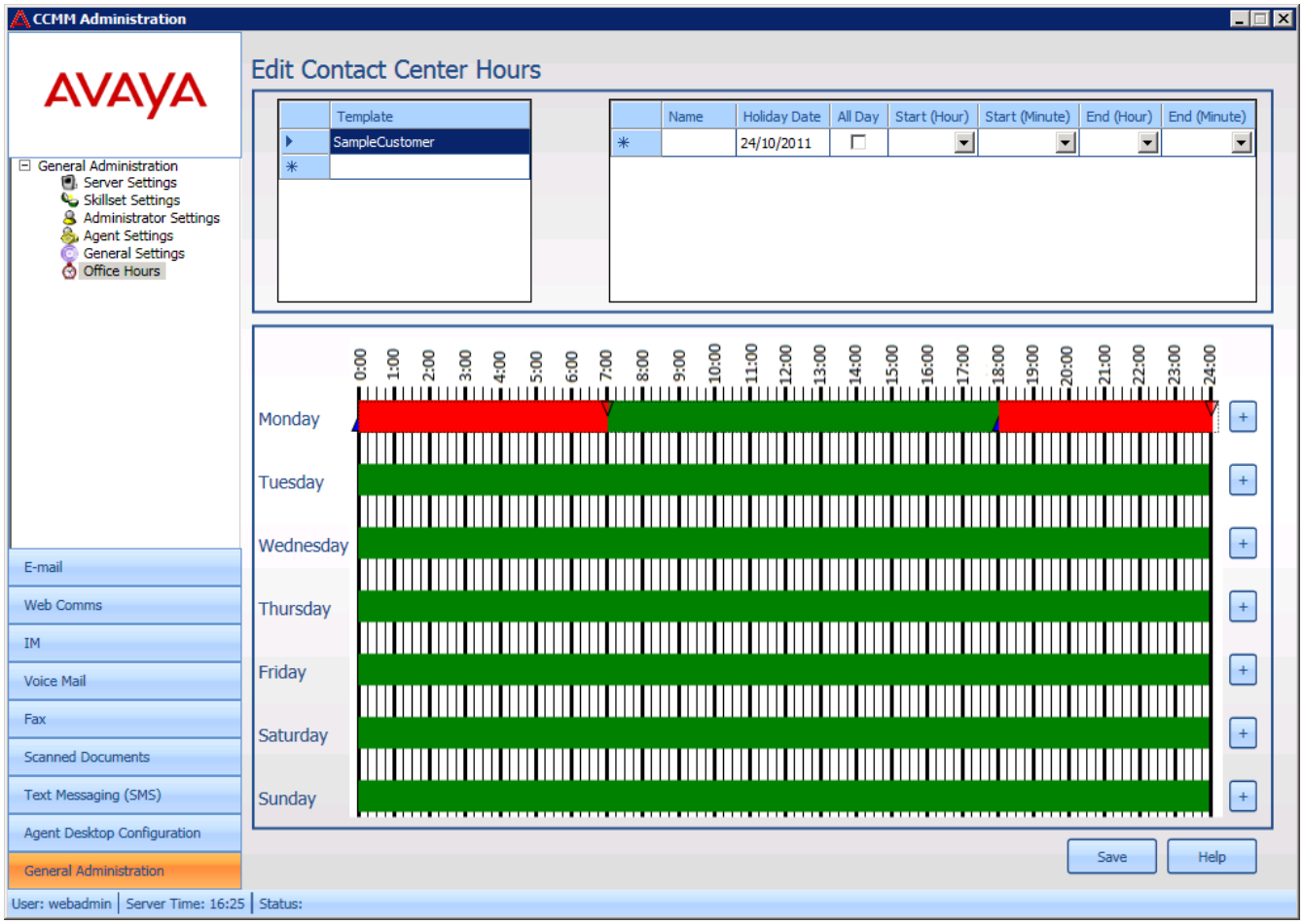


6 On the right of the Monday row, click the plus icon .

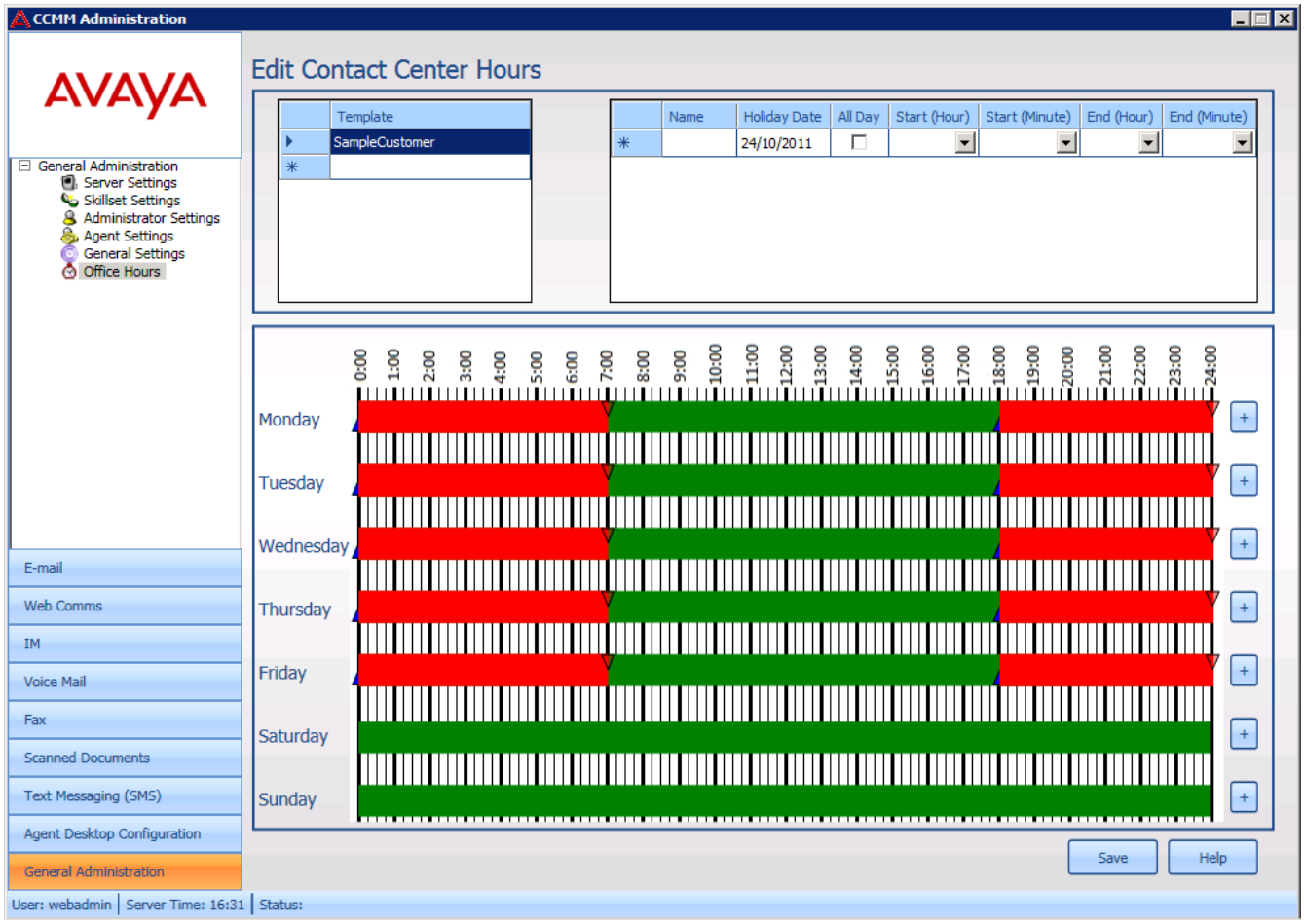
7 Move the Start Closed Period slider to **18:00**.

8 Move the End Closed Period slider to **24:00**.

The display shows the closed hours for the contact center in red.



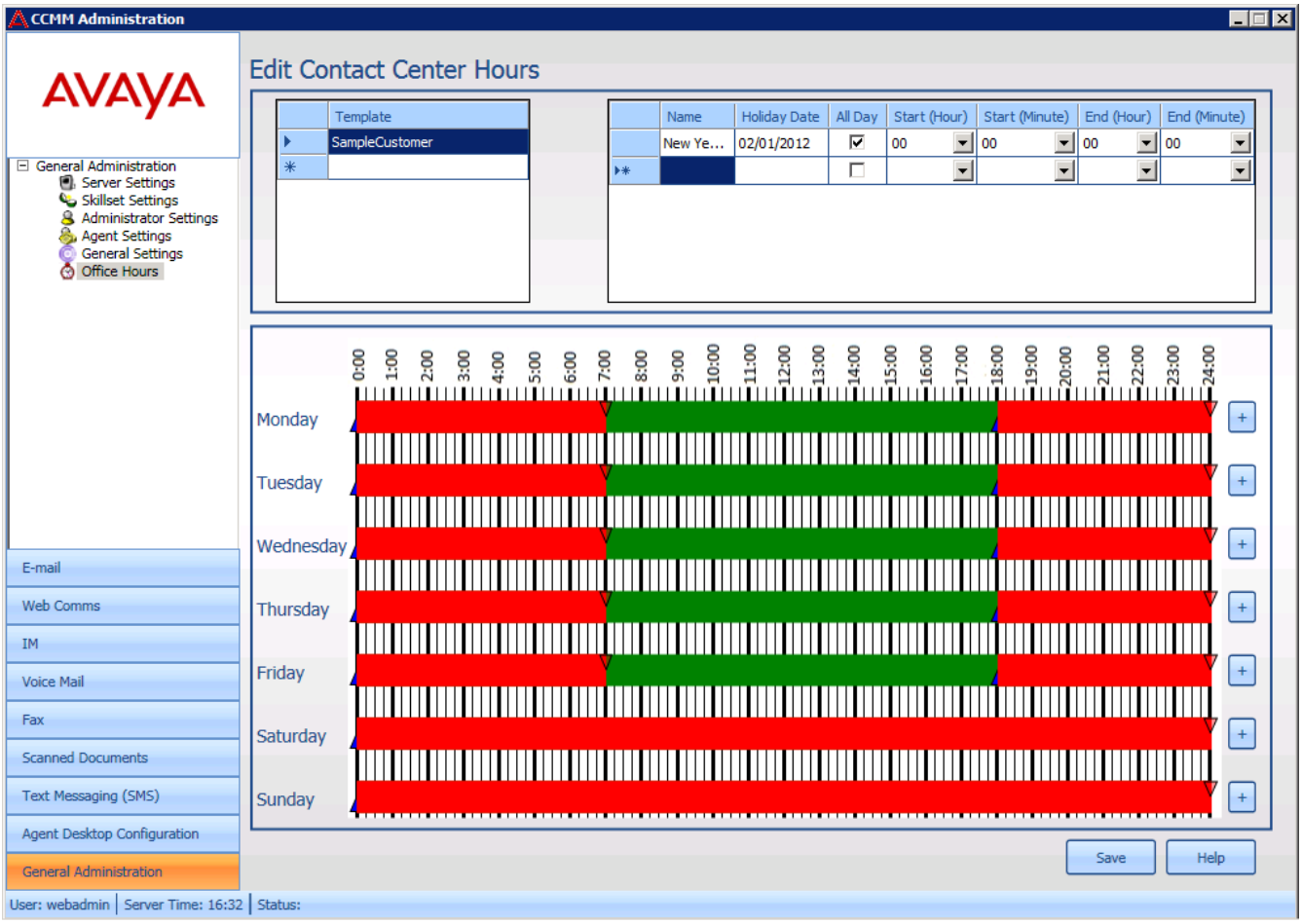
9 Repeat step 4 to step 8 for each week day.



10 On the right of the Saturday row, click the plus icon .

11 Move the End Closed Period slider to **24:00**.

12 Repeat step 10 and step 11 for the Sunday row.



13 Click **Save**.

--End--

Creating a keyword group

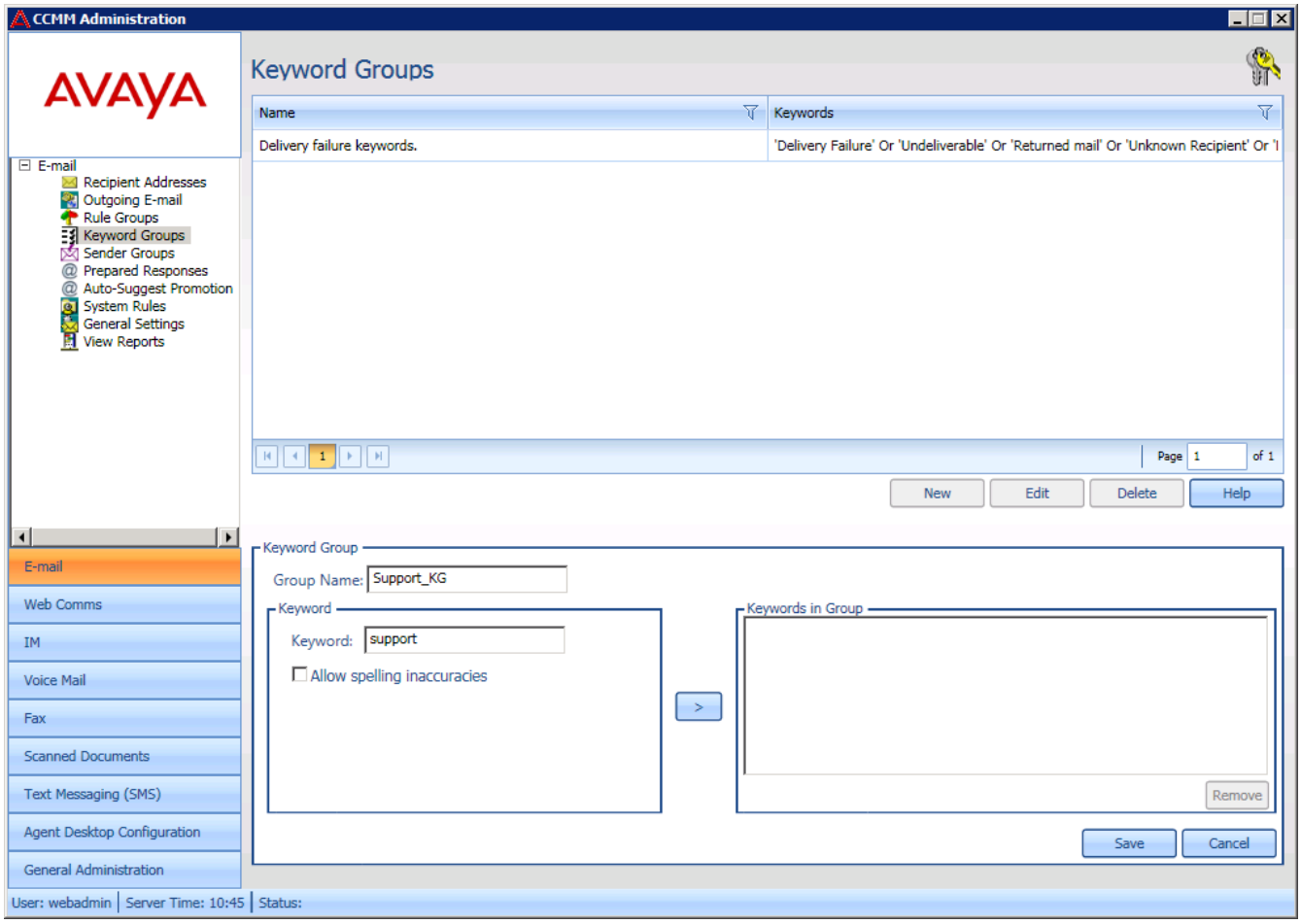
Create a keyword group that you can use to create a rule to route e-mail messages to skillsets. You must assign at least one keyword to a keyword group before you can save the keyword group.

The keyword search in an e-mail 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.

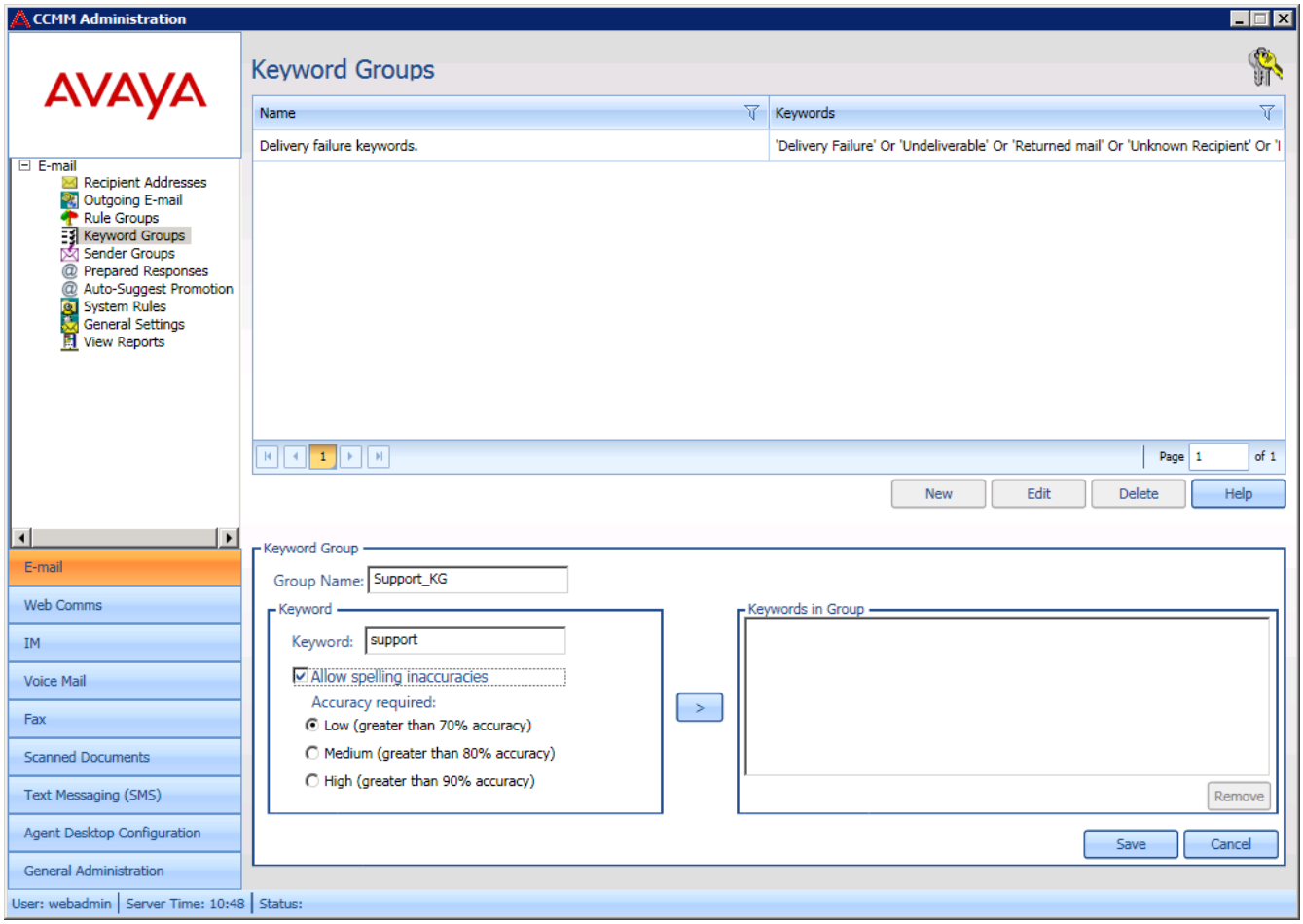
The Keyword box supports the Unicode UTF-8 character set.

Procedure steps

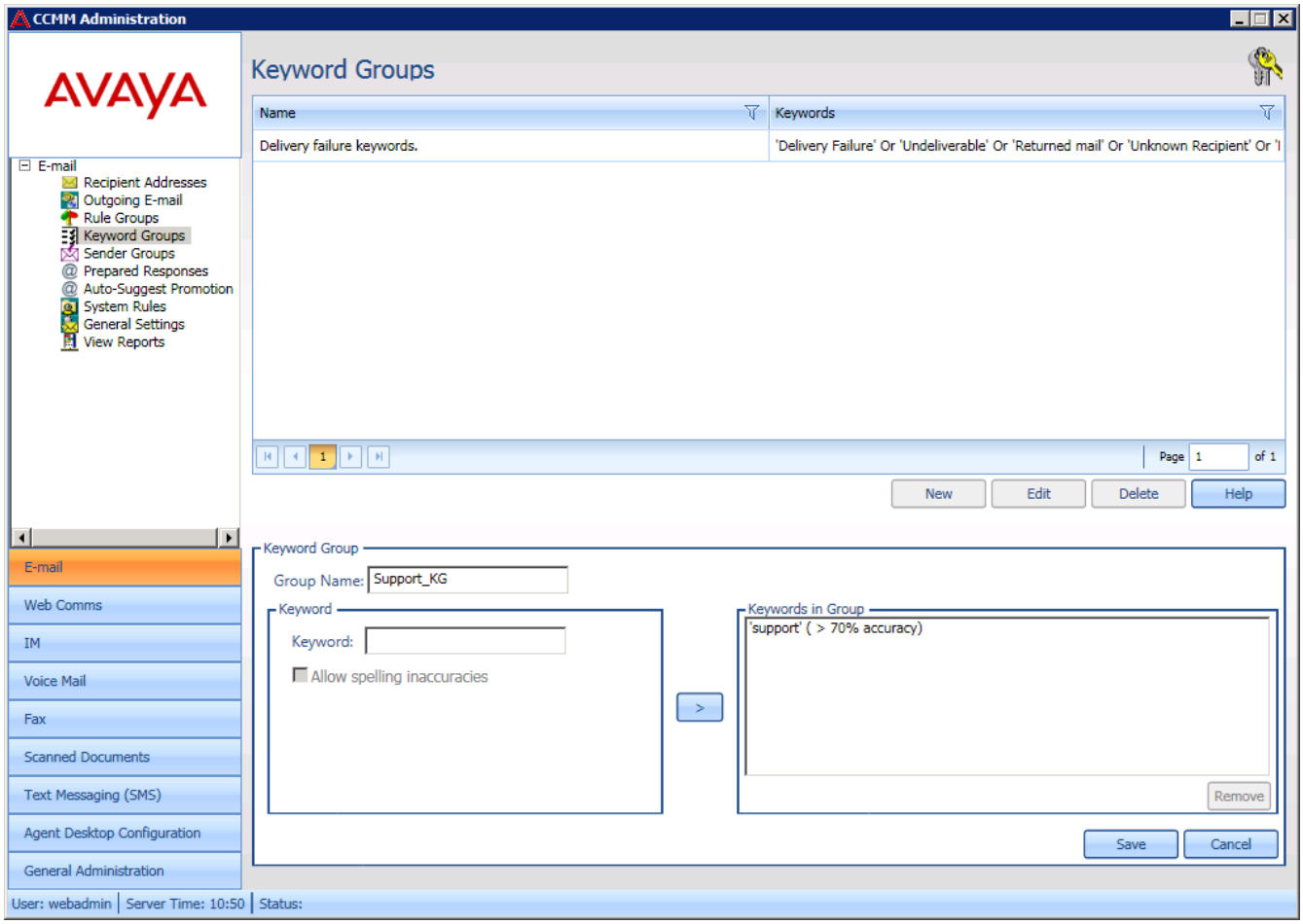
Step	Action
1	In the left column, click **E-mail**.
2	Click **Keyword Groups**.
3	Click **New**.
4	Under **Keyword Group**, in the **Name** box, type **Support_KG**.
5	In the **Keyword** box, type **support**.



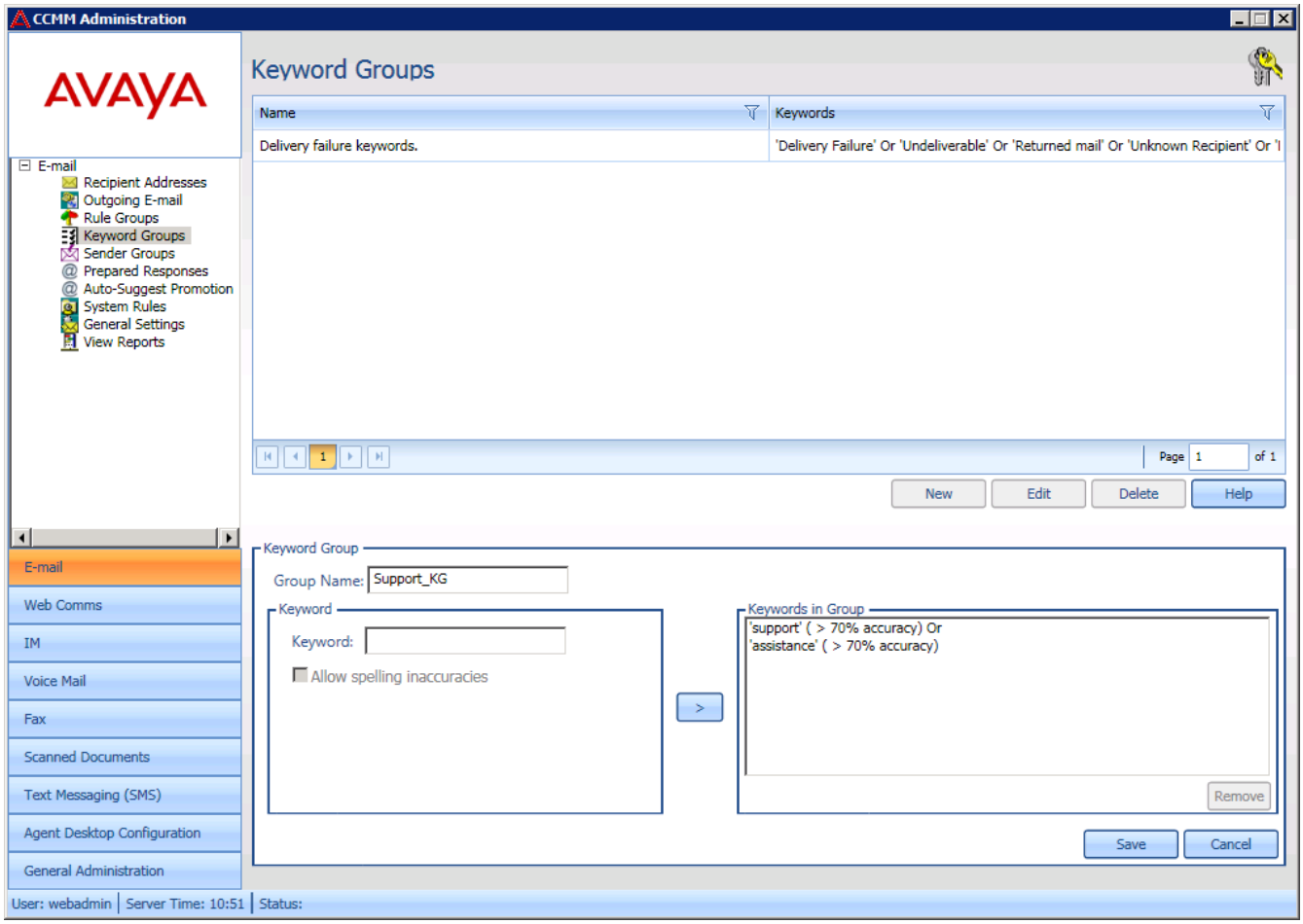
6	To allow misspellings of the word, select the **Allow spelling inaccuracies** check box.
7	Under **Accuracy required**, select **Low (greater than 70% accuracy)**



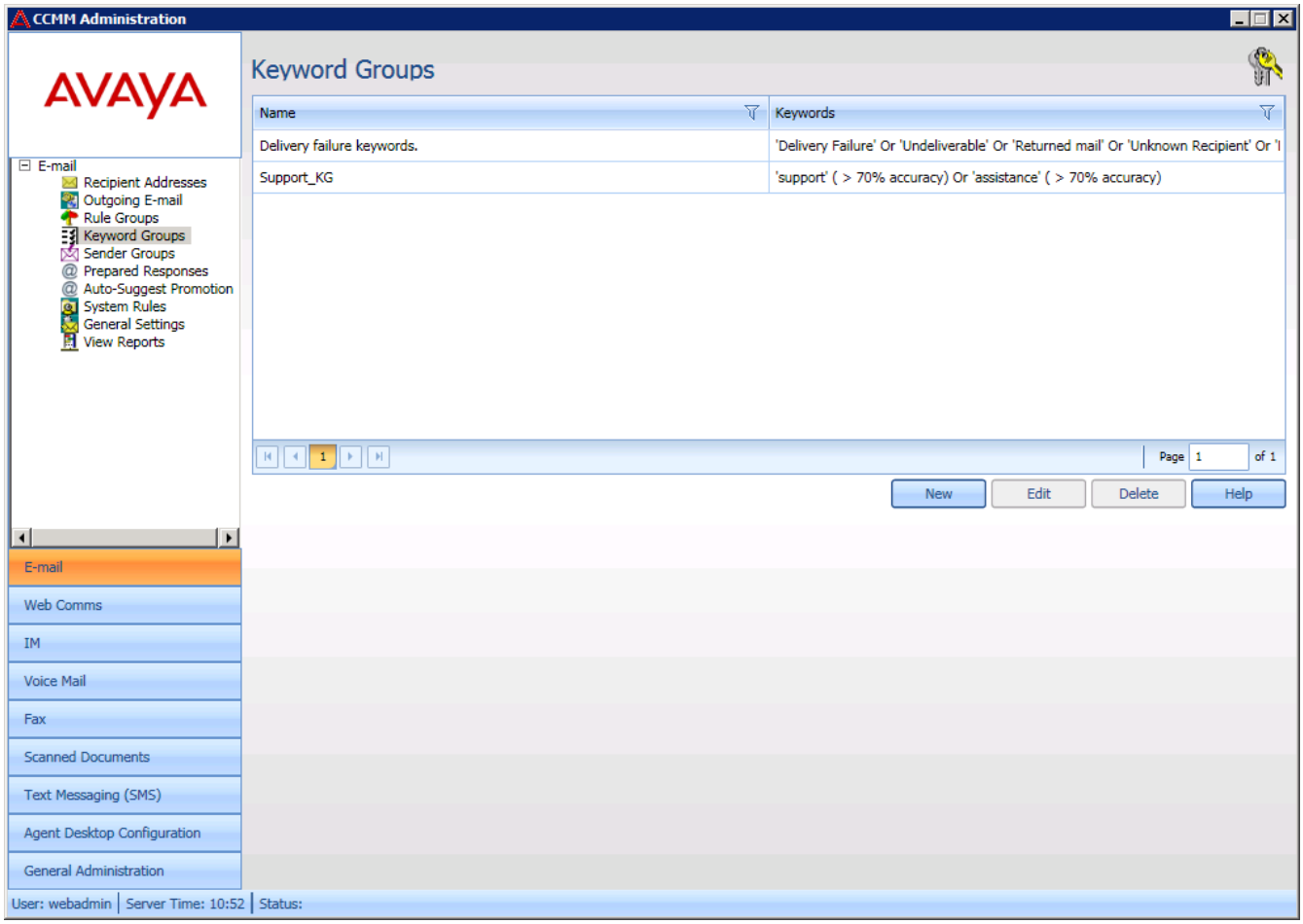
8 Click the right-arrow button > .



9 Repeat step 5 to step 8 to add another keyword, **assistance** to the list.



10 Click **Save**.



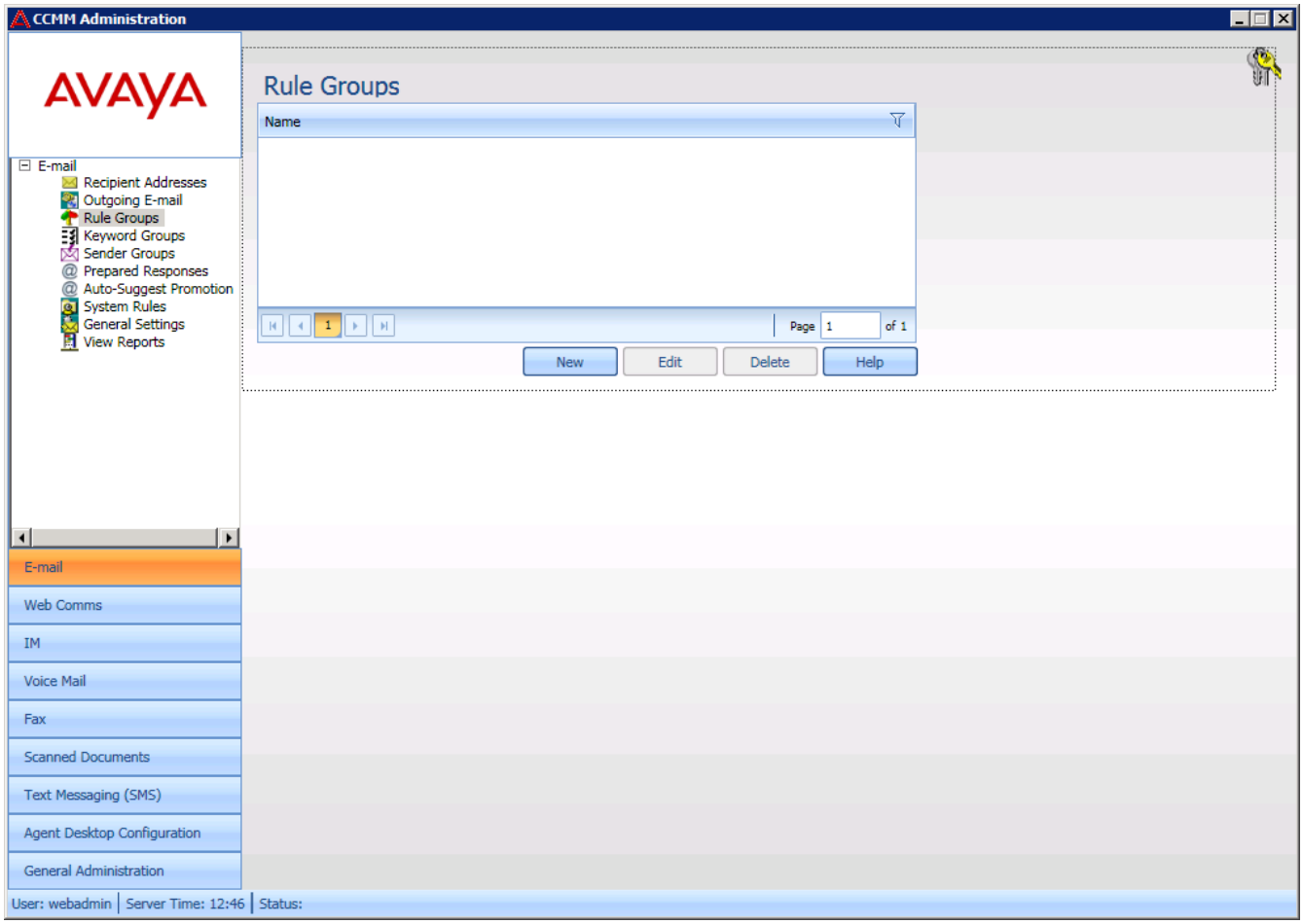
--End--

Creating a Rule Group and a Rule

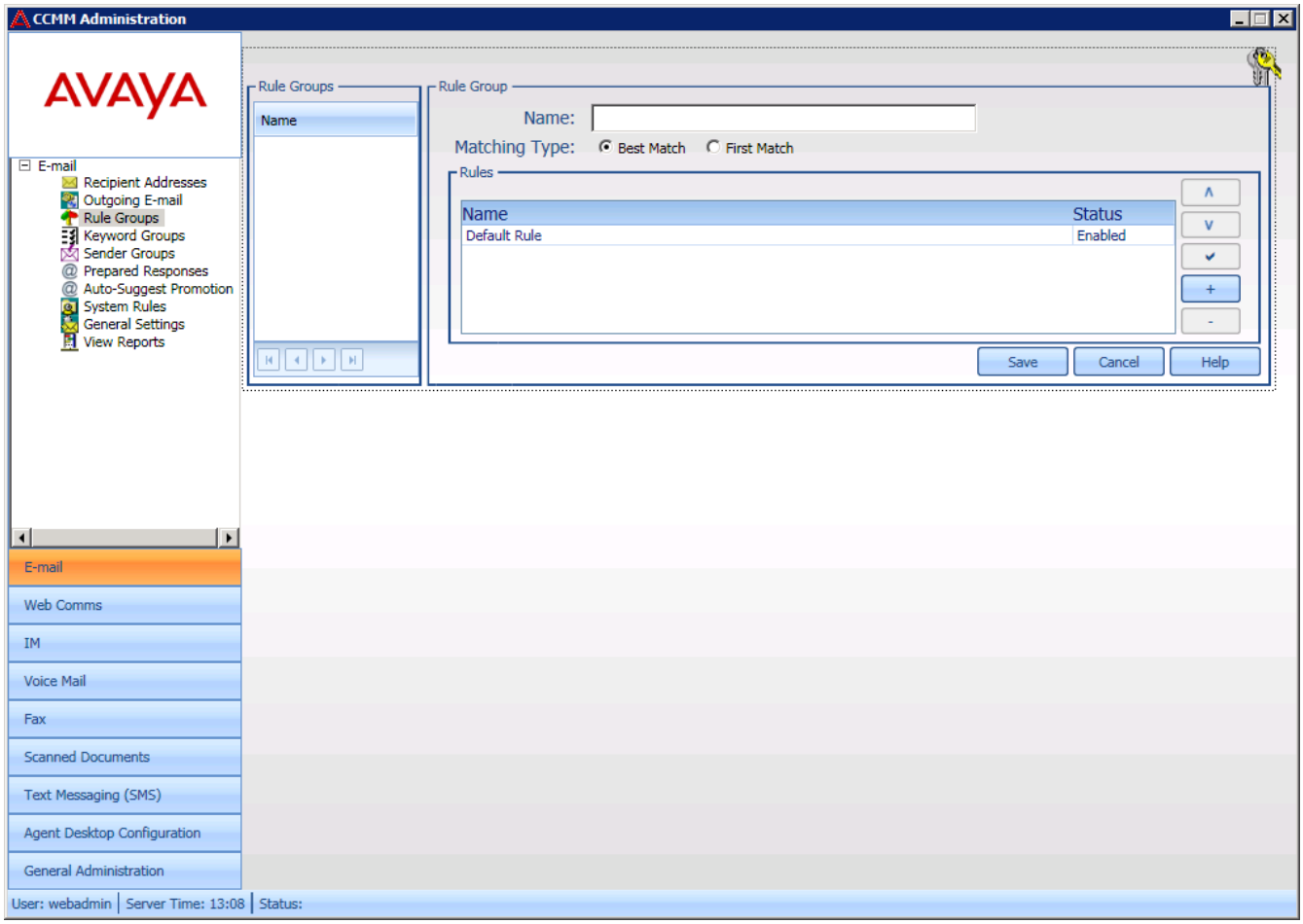
Create a rule group containing one rule to route e-mail contacts to a skillset. In this example, the rule specifies a specific word which, when found in the e-mail message, Contact Center uses to route the e-mail contact.

Procedure steps

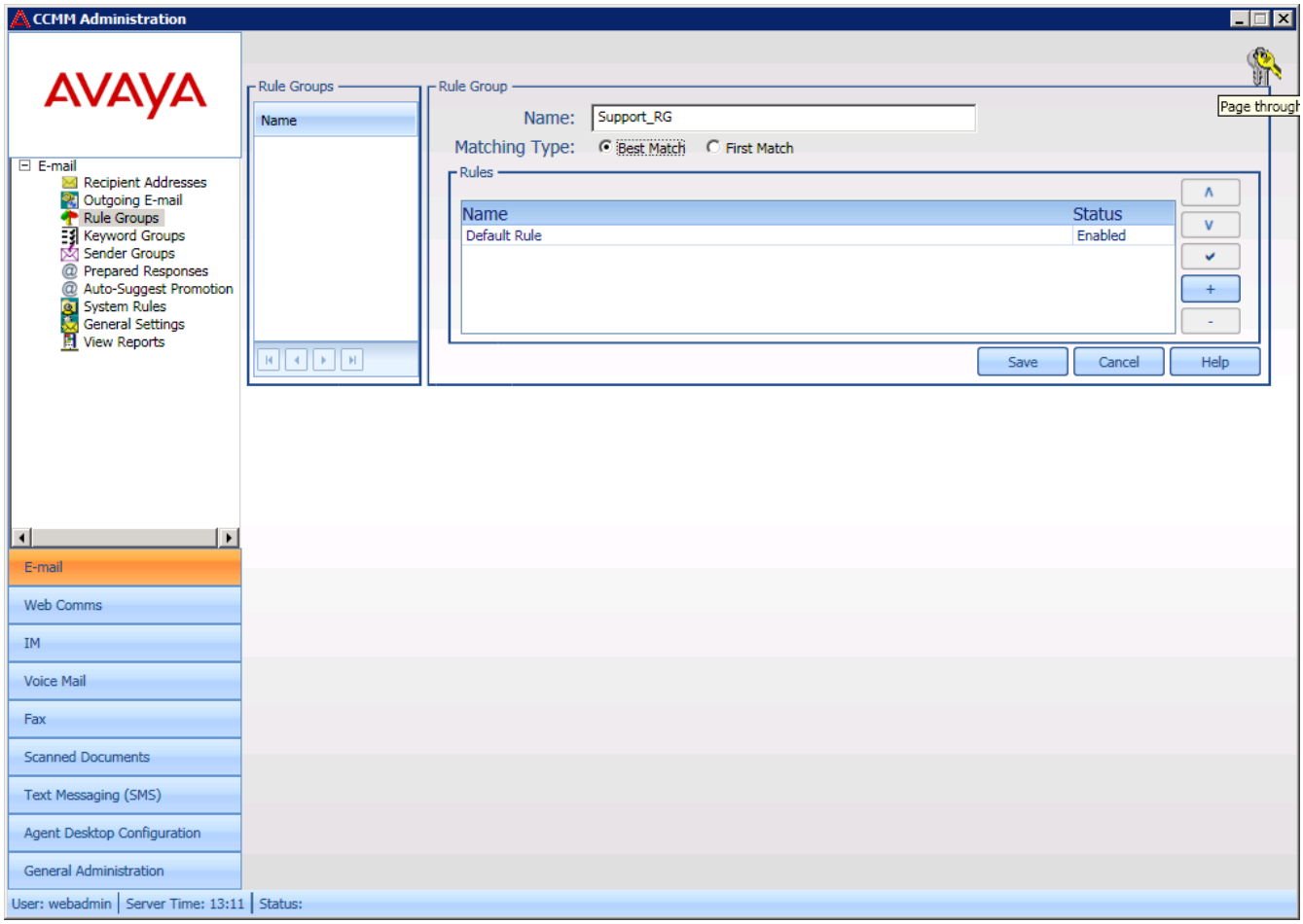
Step	Action
1	In the left column, click **Rule Groups**.



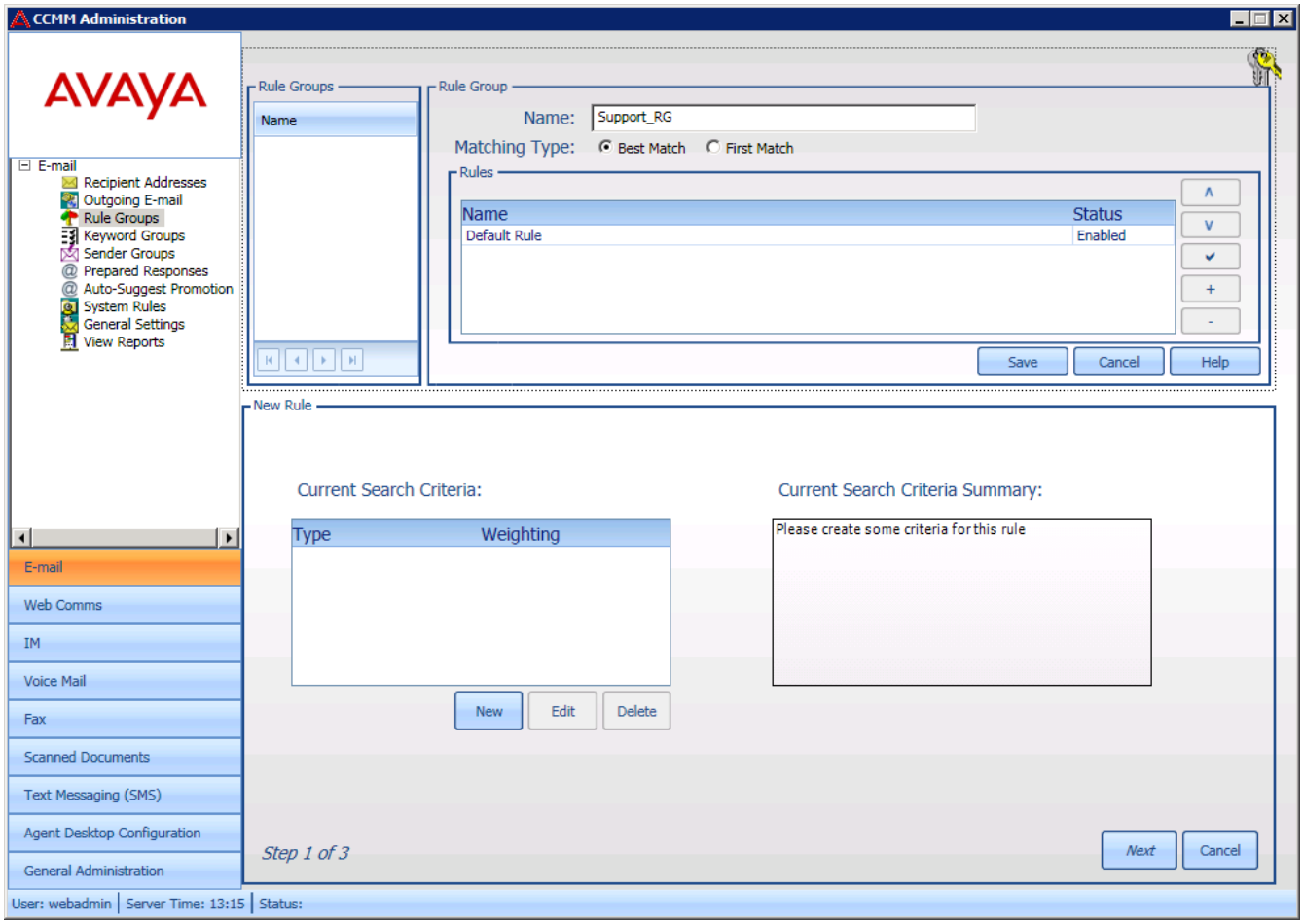
2 Under **Rule Groups**, click **New**



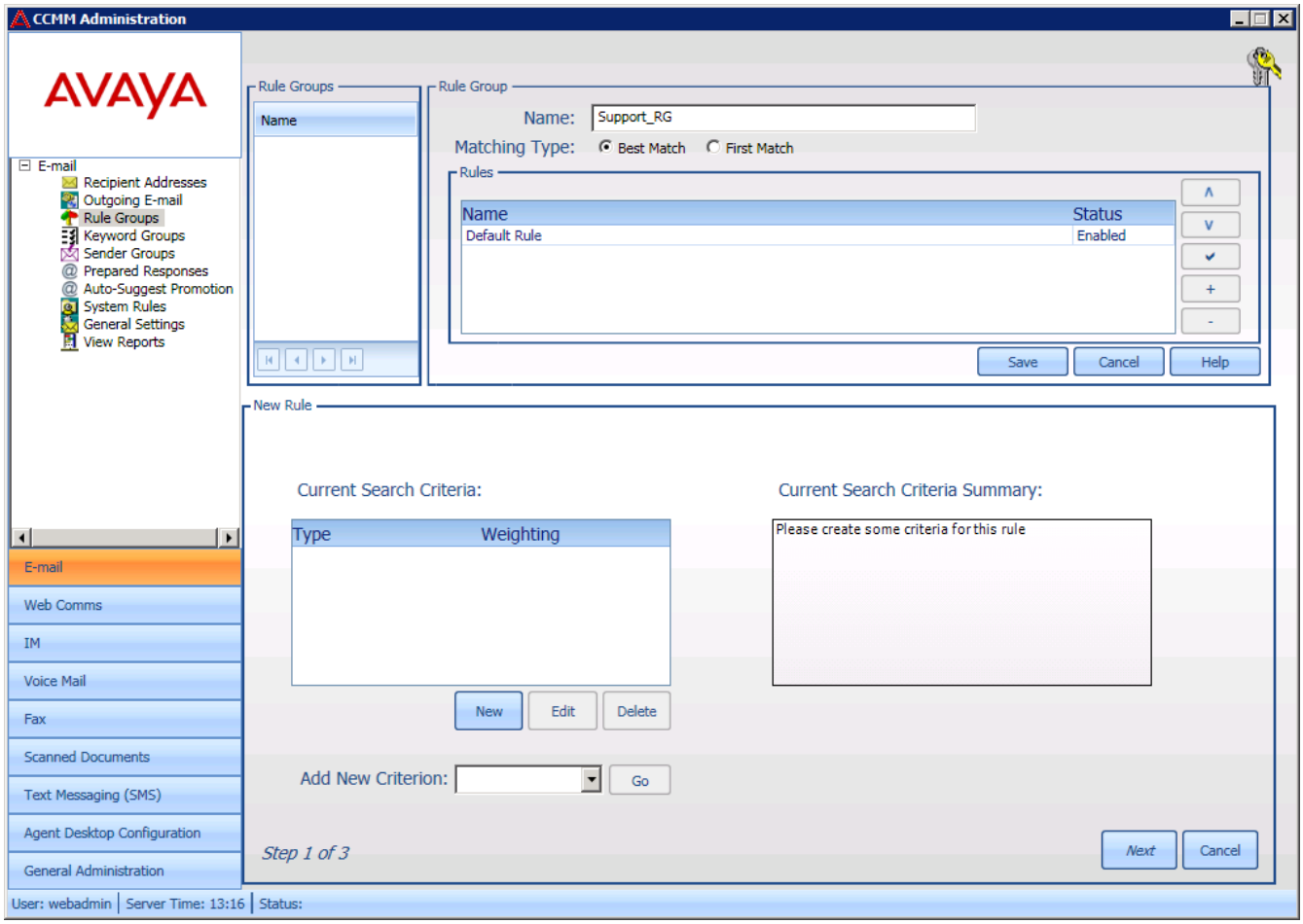
3 In the **Name** box, type a name for the rule group, for example **Support_RG**.



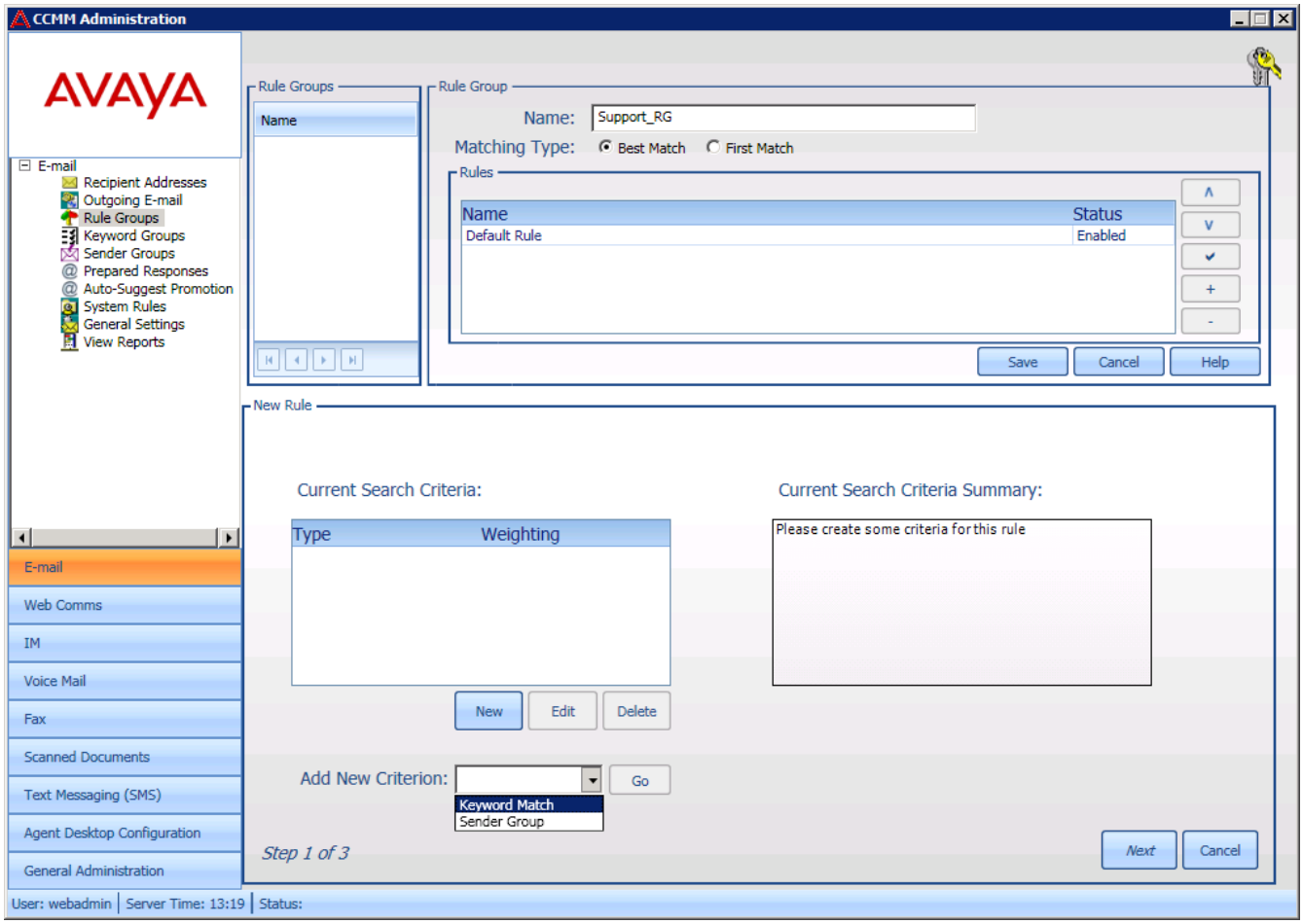
4 Under **Rules**, click the plus button [+].



5 Under **New Rule**, in the **Current Search Criteria** area, click **New**.



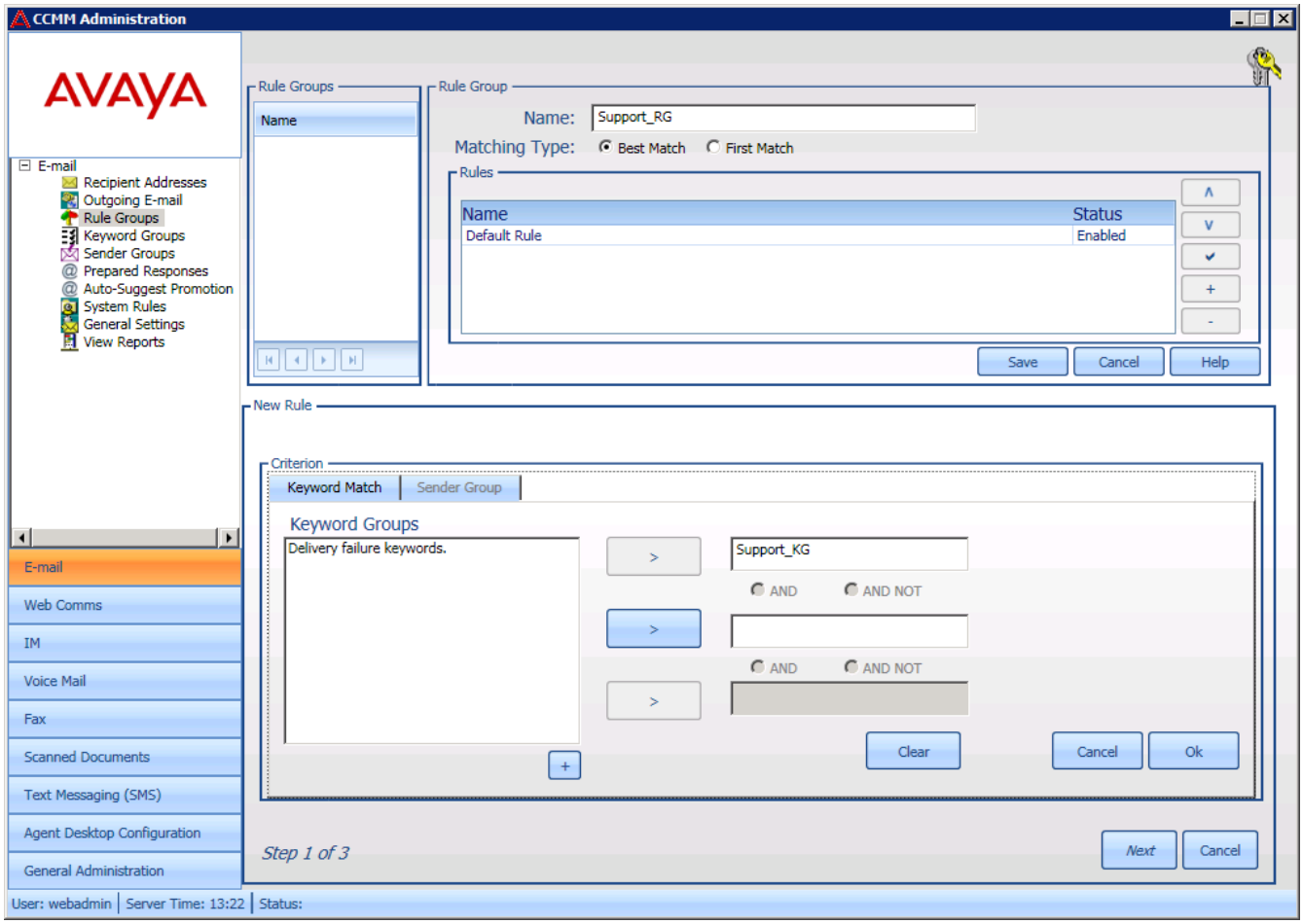
6 From the **Add new Criterion** list, select **Keyword Match**.



7 Click **Go**.

8 On the **Keyword Match** tab, from the **Keyword Groups** list, select the keyword group you just created, for example **Support_KG**.

9 Click the right-arrow button [>].



10 Click **OK**

11 Click **Next**.

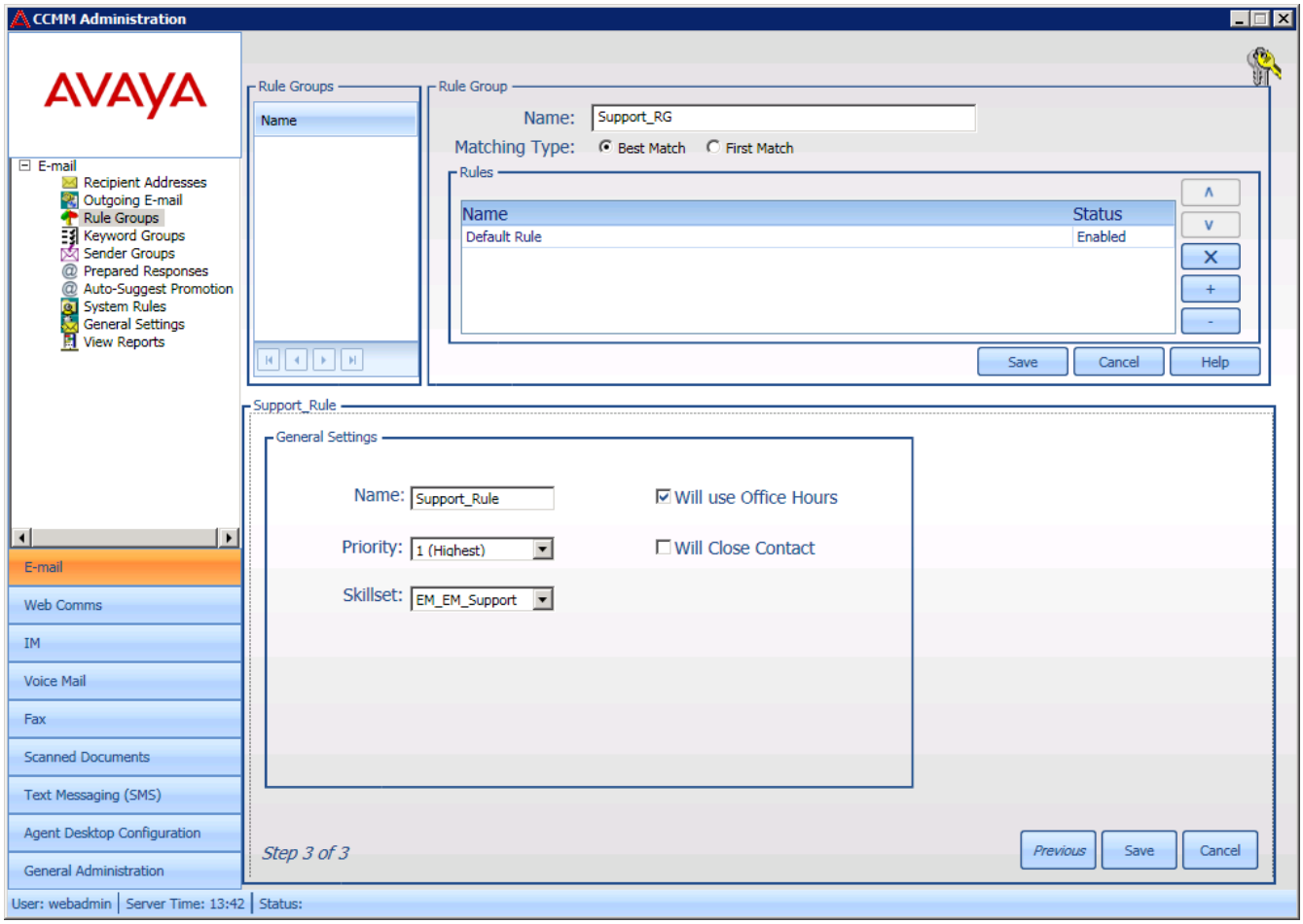
12 Click **Next**.

13 Under **General Settings**, in the **Name** box, type a name for the rule, for example **Support_Rule**.

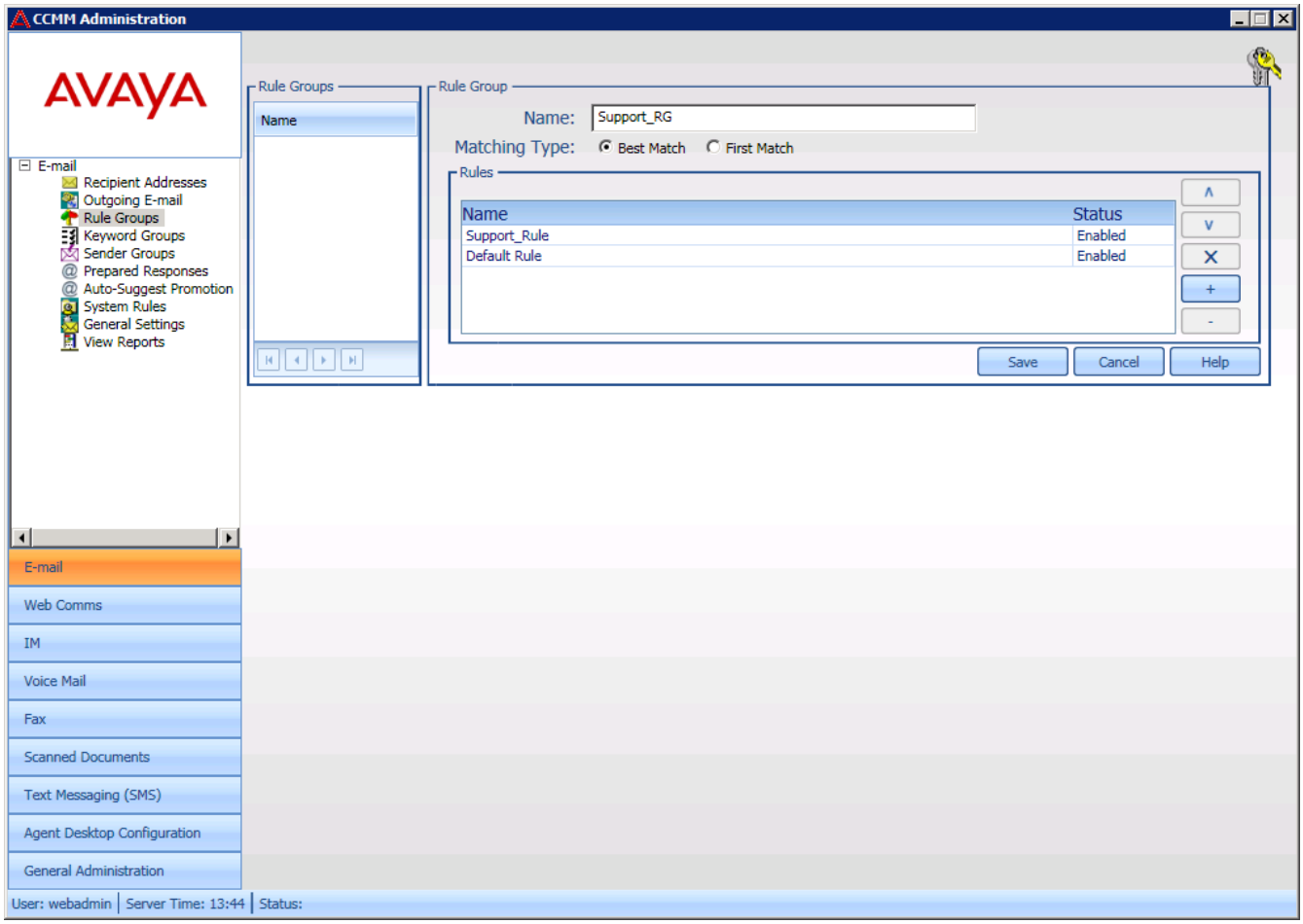
14 From the **Priority** list, select **1 (Highest)**.

15 From the **Skillset** list, select the skillset to which you want Contact Center to route e-mail messages matching this rule, for example **EM_EM_Support**.

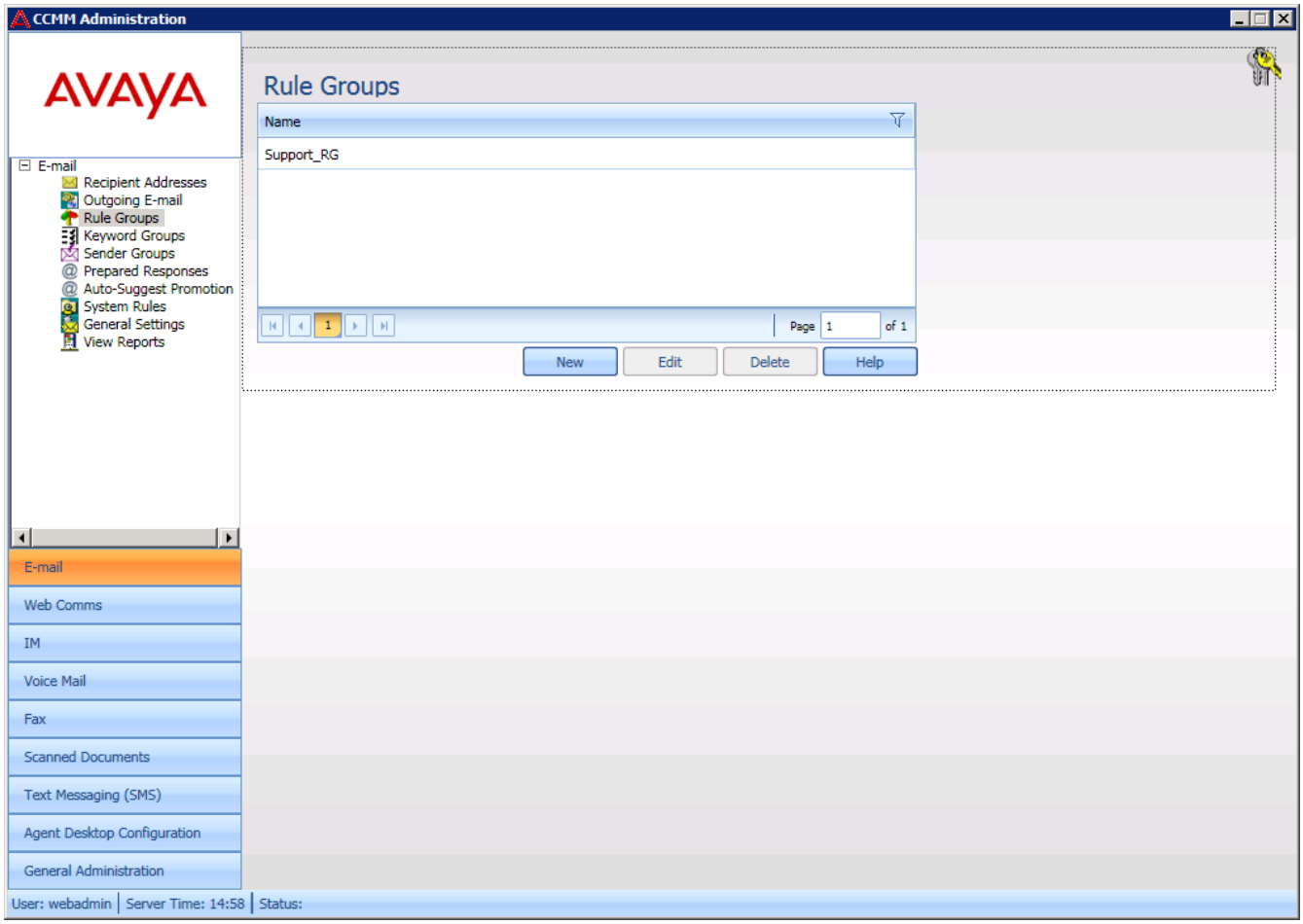
16 Select the **Will use Office Hours** checkbox.



17 Click **Save**.



18 Under **Rule Group**, click **Save**.



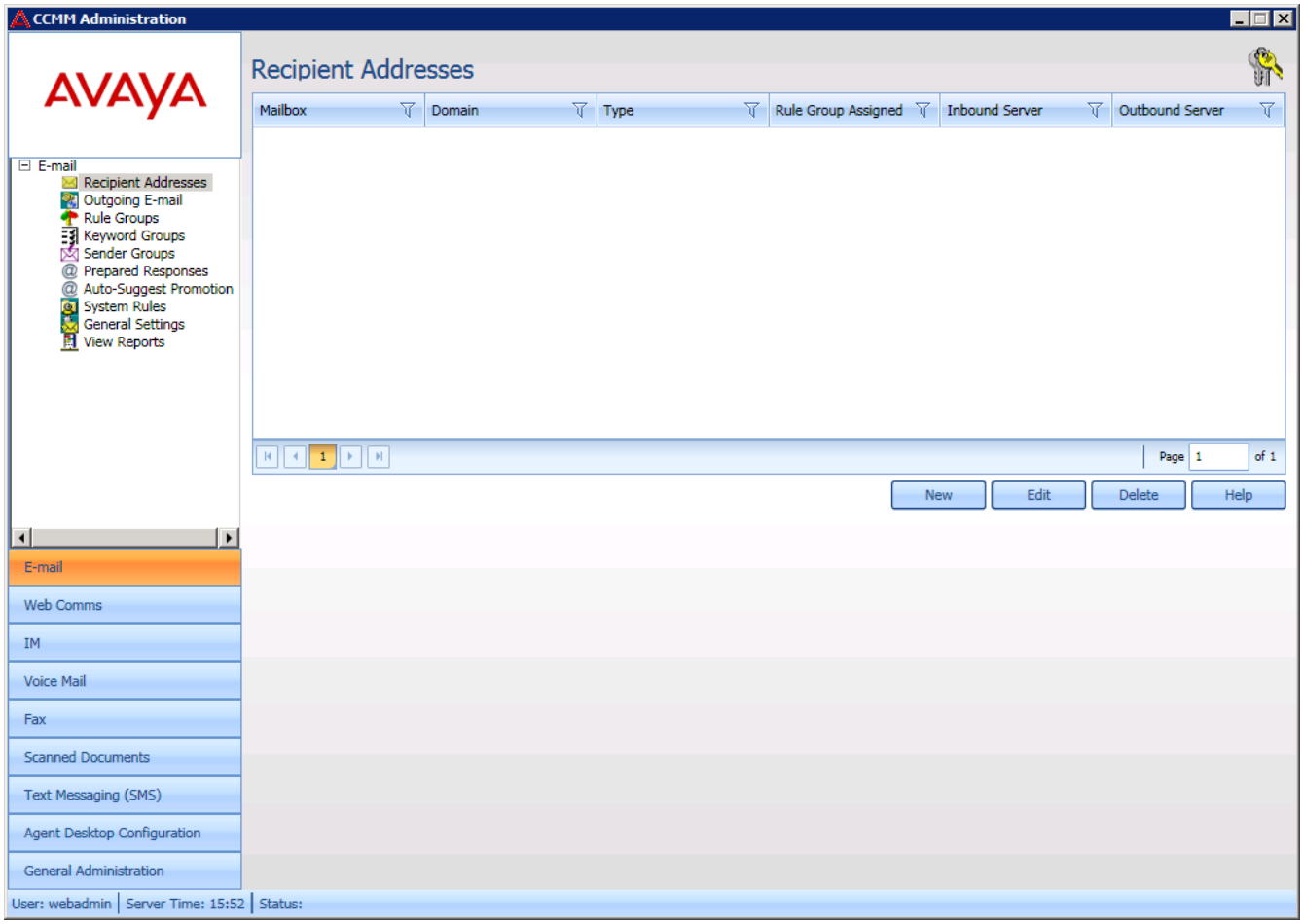
--End--

Configuring the Inbound e-mail recipient address

Configure a recipient mailbox that the Contact Center can scan to retrieve e-mail messages and process them into e-mail contacts.

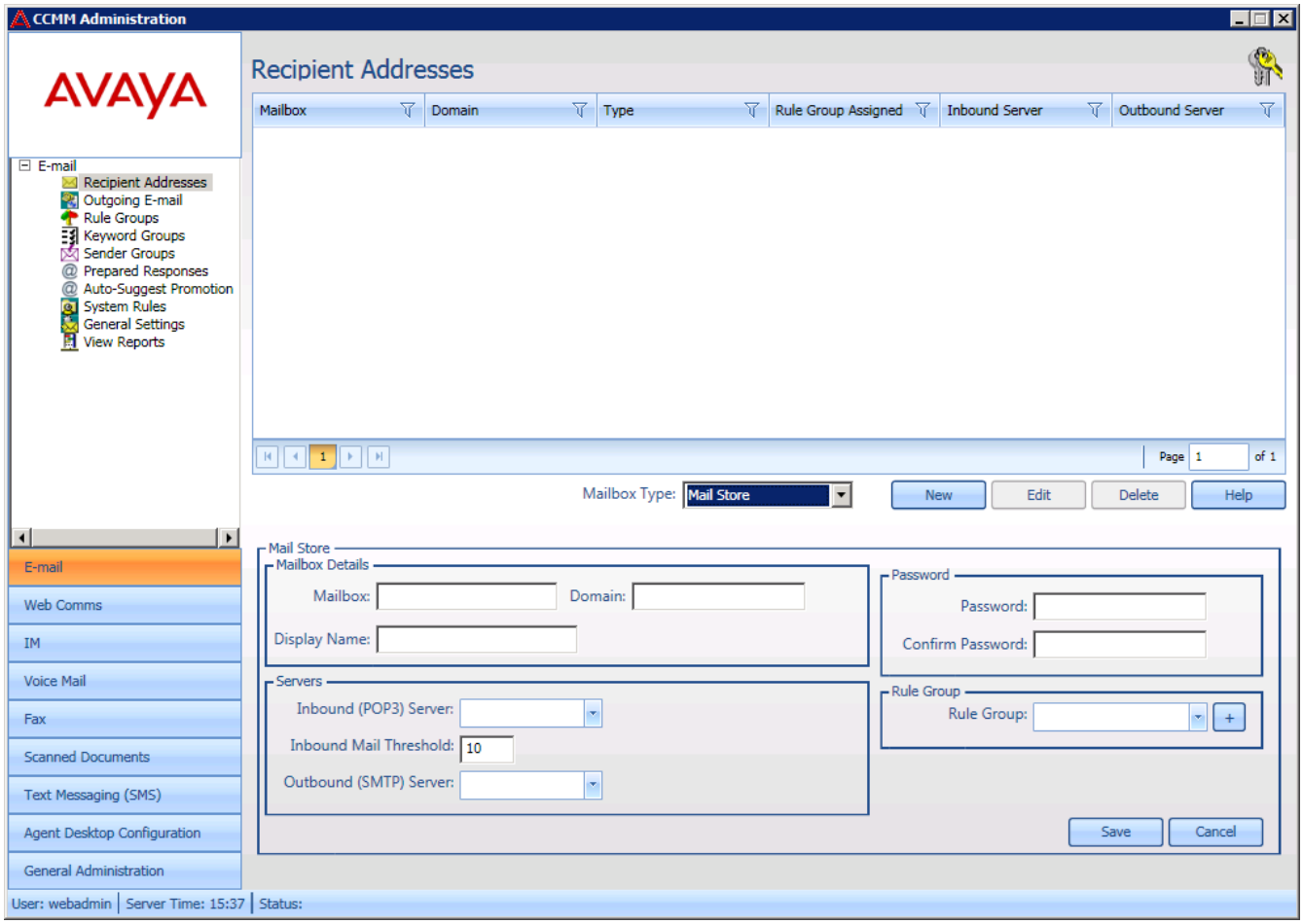
Procedure steps

Step	Action
1	In the left column, select **Email**.
2	Click **Recipient Addresses**.



3 Click **New**.

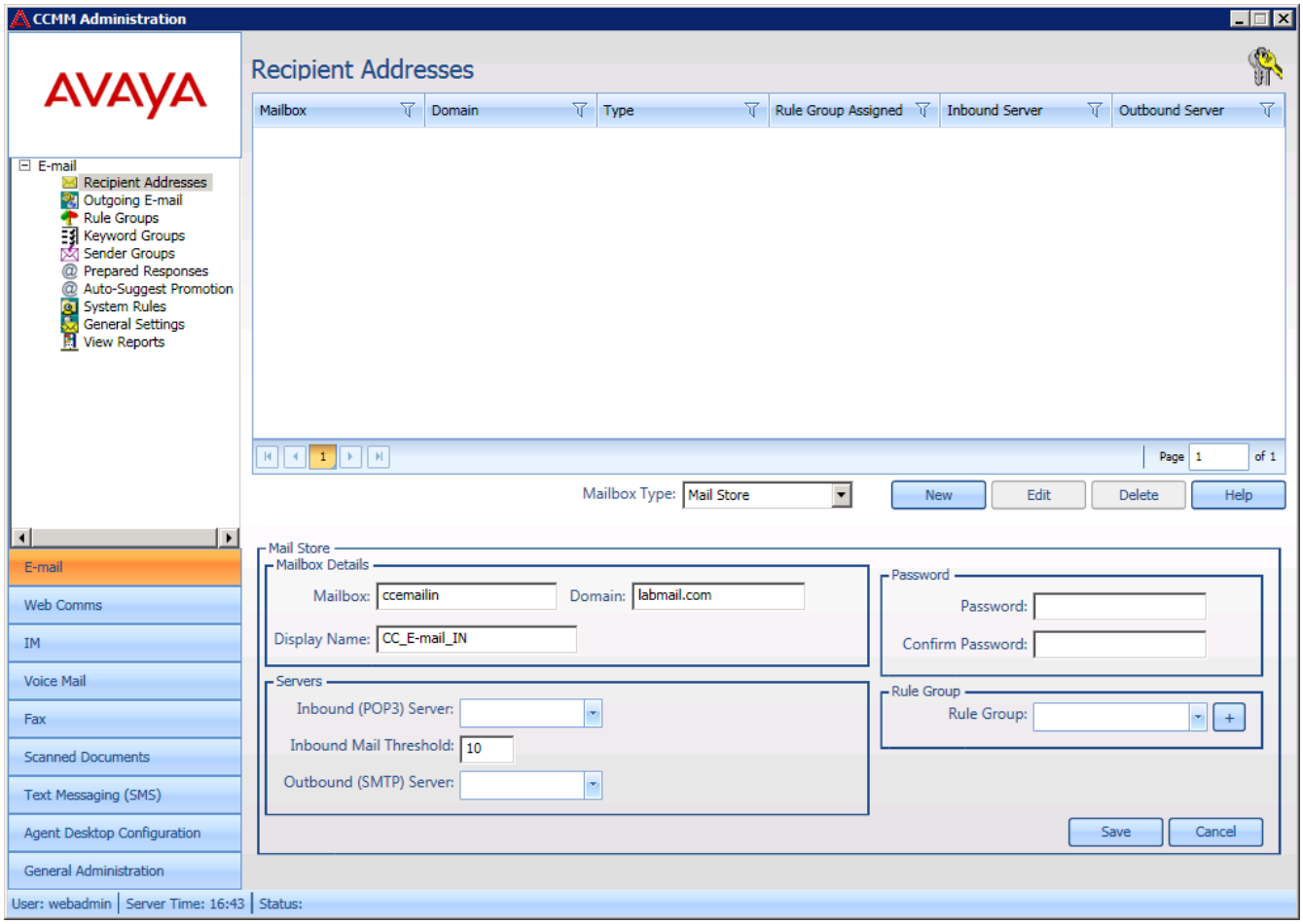
4 From the **Mailbox Type** list, select **Mail Store**.



5 In the **Mailbox:** box, type the recipient mailbox name, for example **ccemailin**.

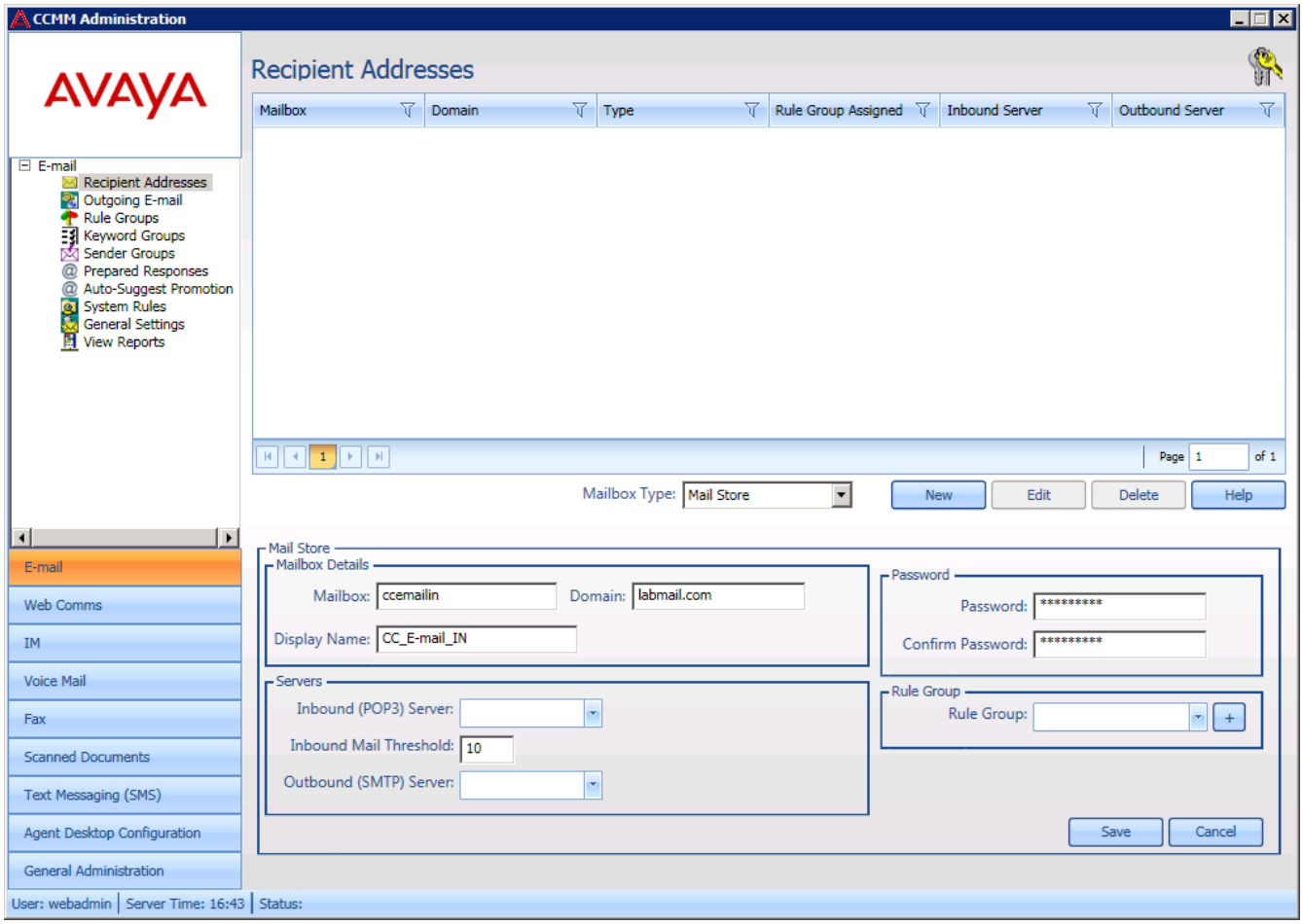
6 In the **Domain:** box, type the recipient mailbox name, for example **labmail.com**.

7 In the **Display Name:** box, type the Display name for this recipient mailbox, for example **CC_e-mail_IN**.



8 In the **Password:** box, type the recipient mailbox password, for example **Passw0rd1**.

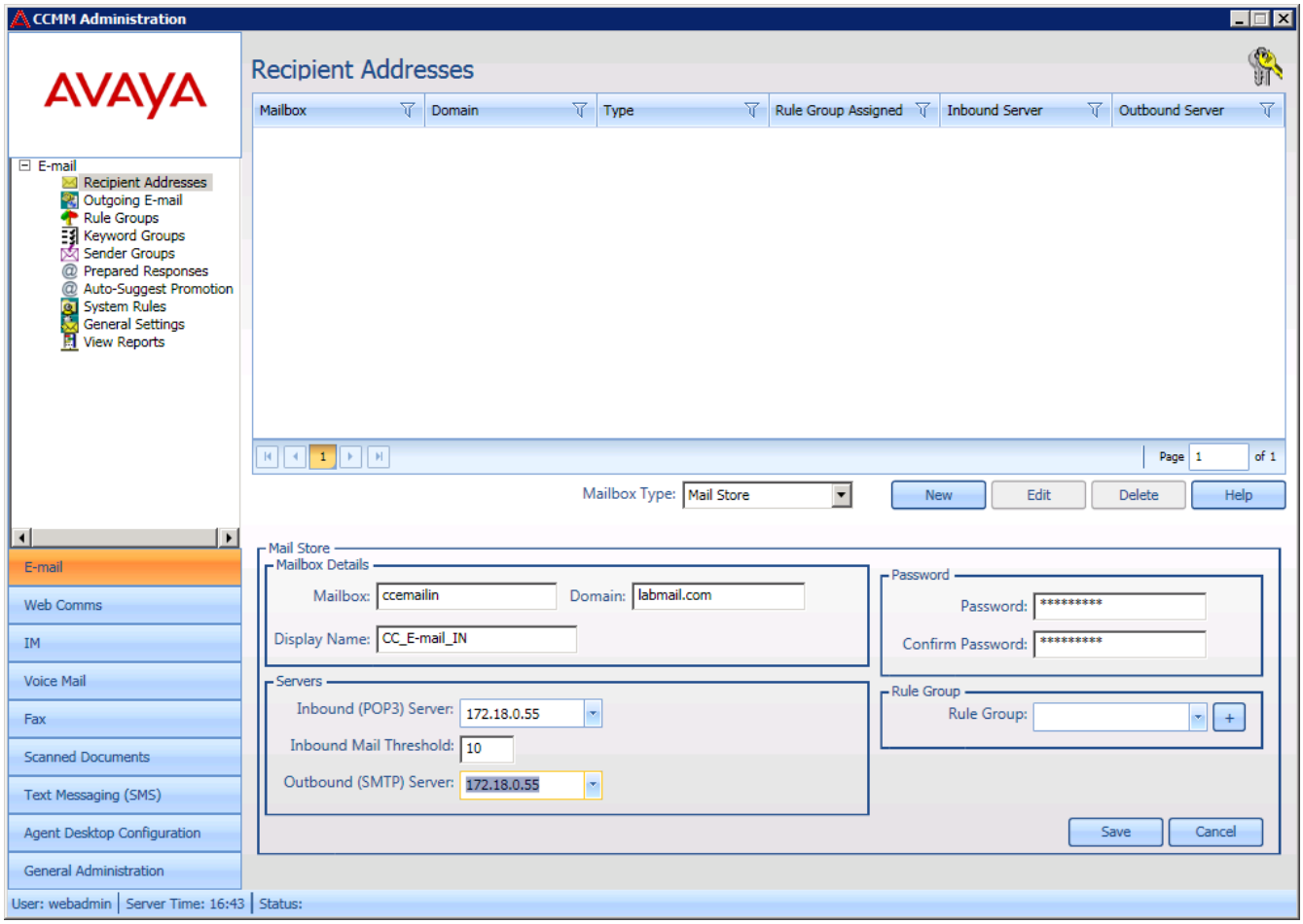
9 In the **Confirm Password:** box, type the recipient mailbox password again.



10 From the **Inbound (POP3) Server:** list, select the e-mail server on which the mailbox is configured, for example **172.18.0.55**.

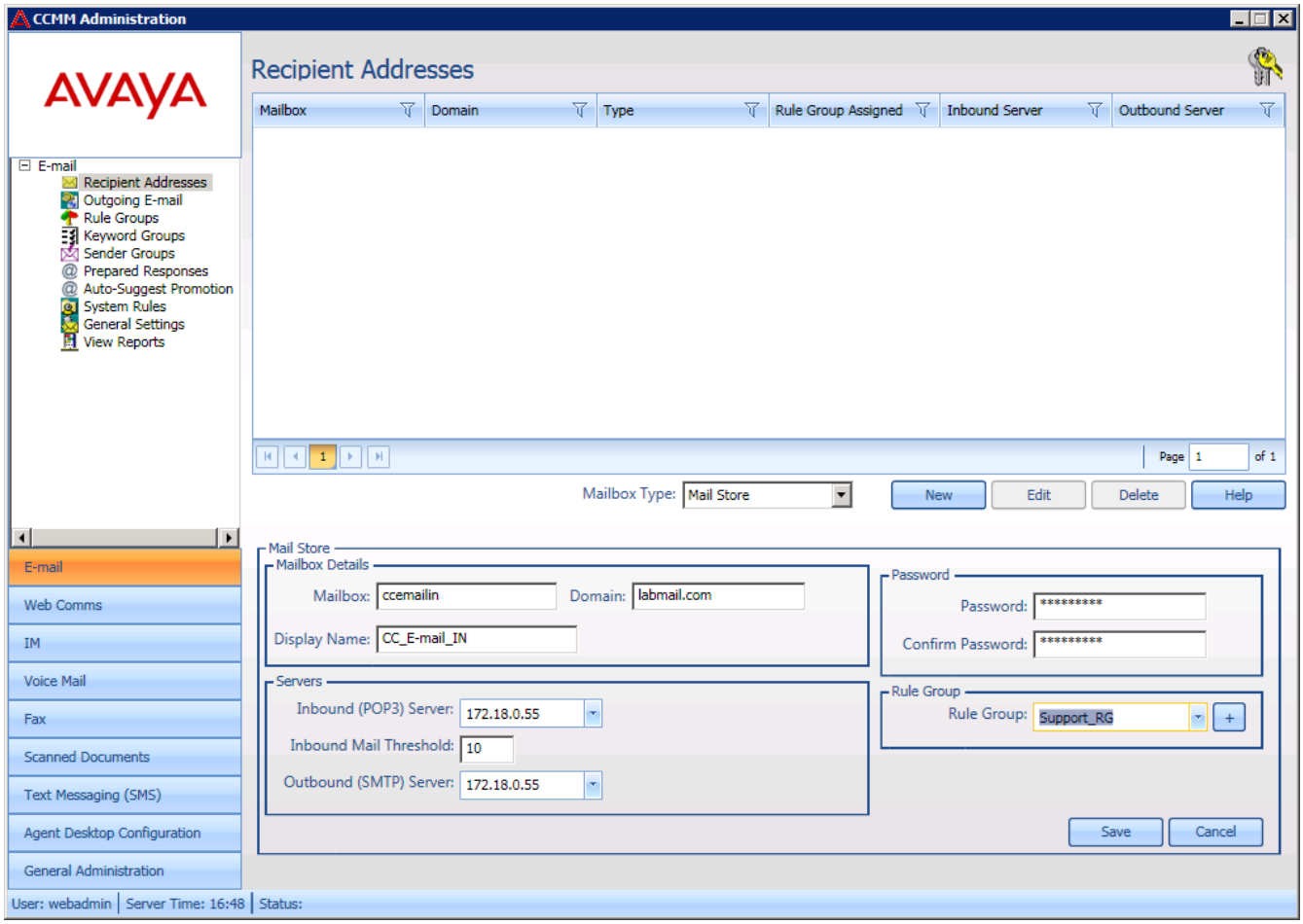
11 In the **Inbound Mail Threshold:** box, type the number of e-mail messages you want Contact Center to retrieve to the database each time it scans the mailbox, for example **100**.

12 From the **Outbound (SMTP) Server:** list, select the e-mail server on which the mailbox is configured, for example **172.18.0.55**.

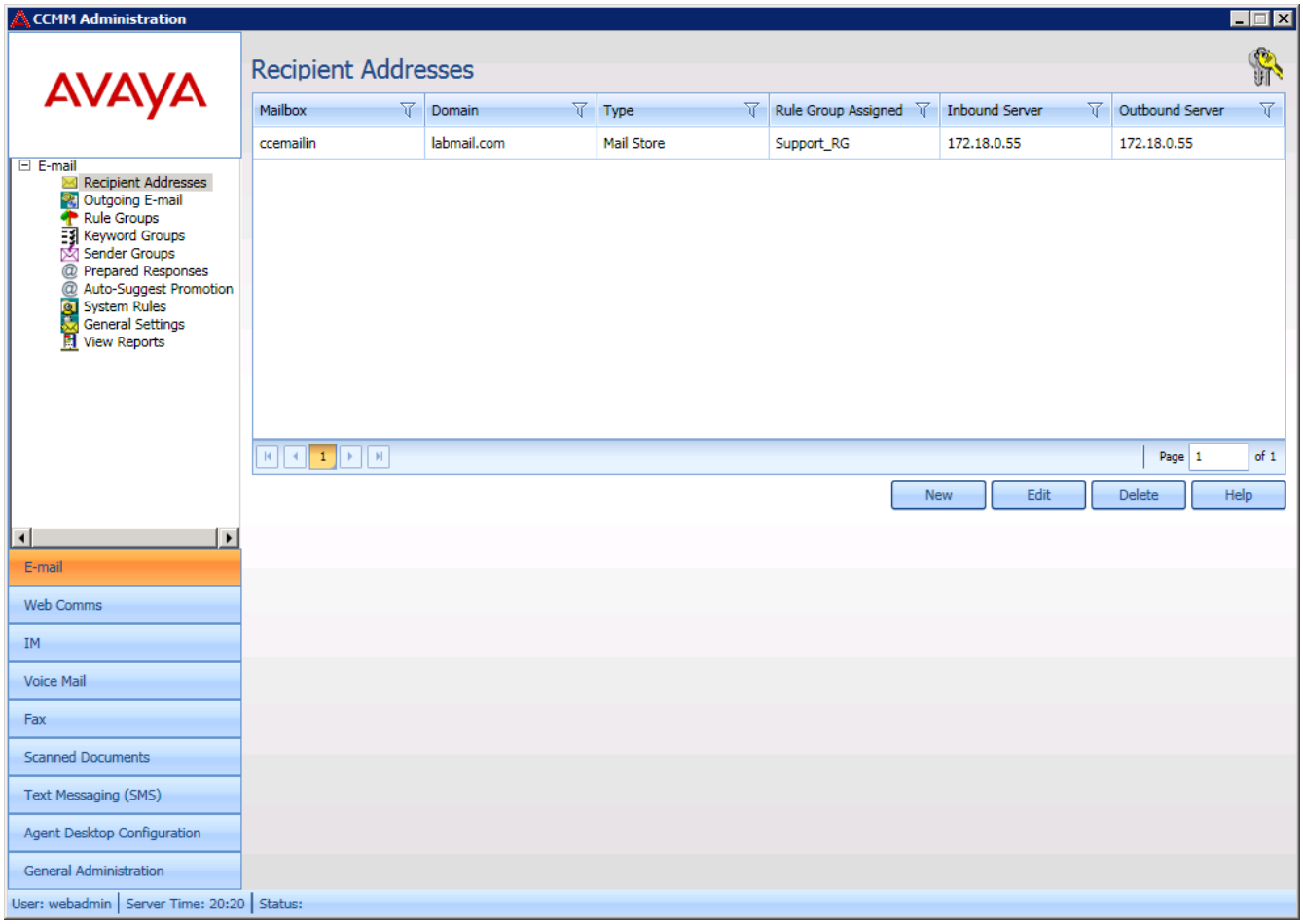


13 From the **Rule Group:** list, select the rule group that contains the rules that Contact Center applies to e-mail messages in this mailbox, for example **Support_RG**.

Applying a rule group to the mailbox allows Contact Center to use the criteria of the rules in the rule group to make routing decisions on the e-mail messages. In this example Contact Center matches e-mail messages containing the word "support" to the Support_Rule, which routes those e-mail contacts to the skillset EM_EM_Support.



14 Click **Save**.



--End--

Configuring the Outbound e-mail recipient address

Configure a recipient mailbox that Contact Center can use to send outbound e-mail message, whether replies composed by agents, or auto-responses configured for e-mail rules.

Procedure steps

Step	Action
1	In the left column, select **Email**.
2	Click **Recipient Addresses**.
3	Click **New**.

4 From the **Mailbox Type** list, select **Mail Store**.

5 In the **Mailbox:** box, type the outbound mailbox name, for example **ccemailout**.

6 In the **Domain:** box, type the recipient mailbox name, for example **labmail.com**.

7 In the **Display Name:** box, type the Display name for this recipient mailbox, for example **CC_e-mail_OUT**.

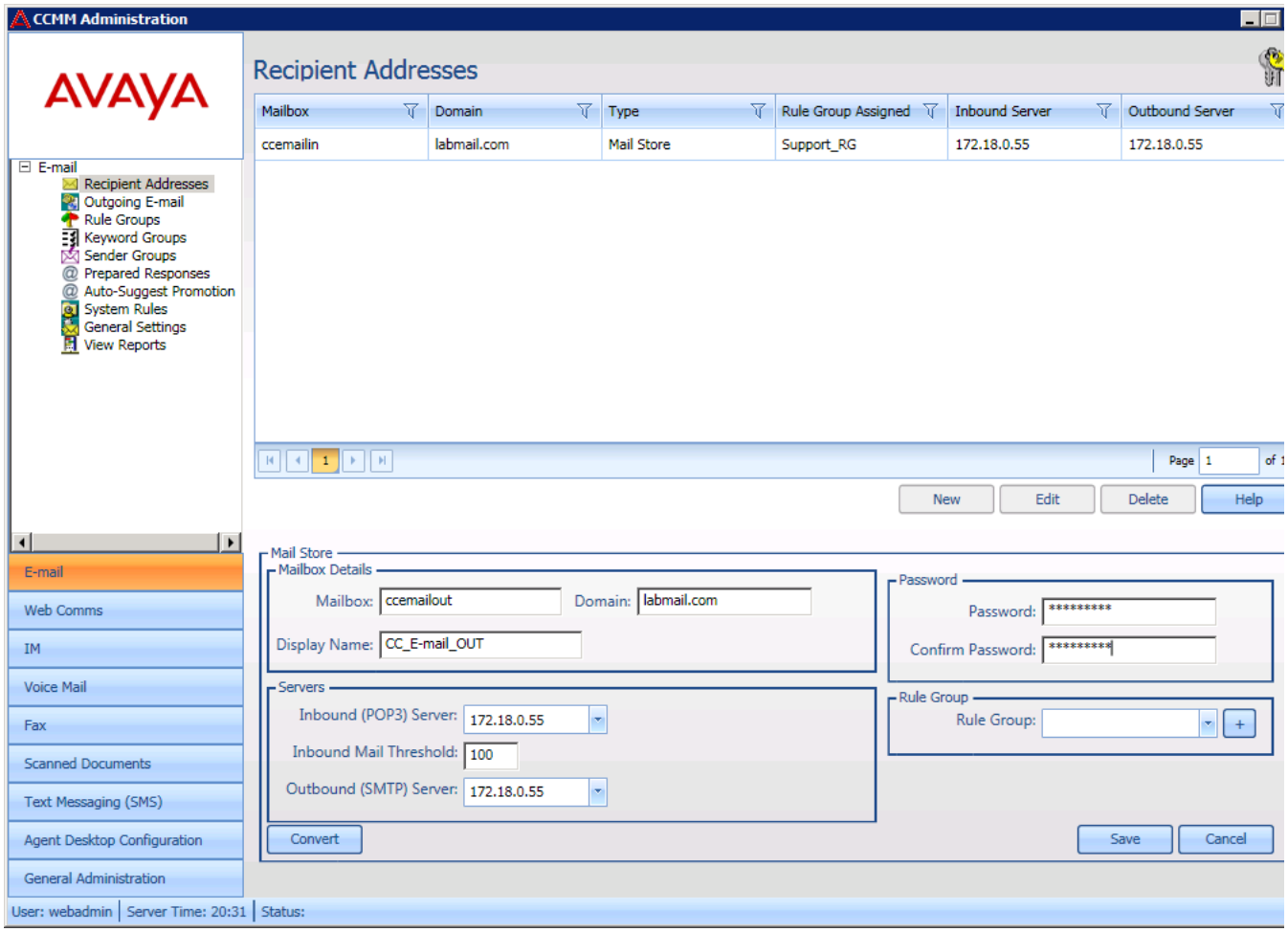
8 In the **Password:** box, type the outbound mailbox password, for example **Passw0rd2**.

9 In the **Confirm Password:** box, type the outbound mailbox password again.

10 From the **Inbound (POP3) Server:** list, select the e-mail server on which the mailbox is configured, for example **172.18.0.55**.

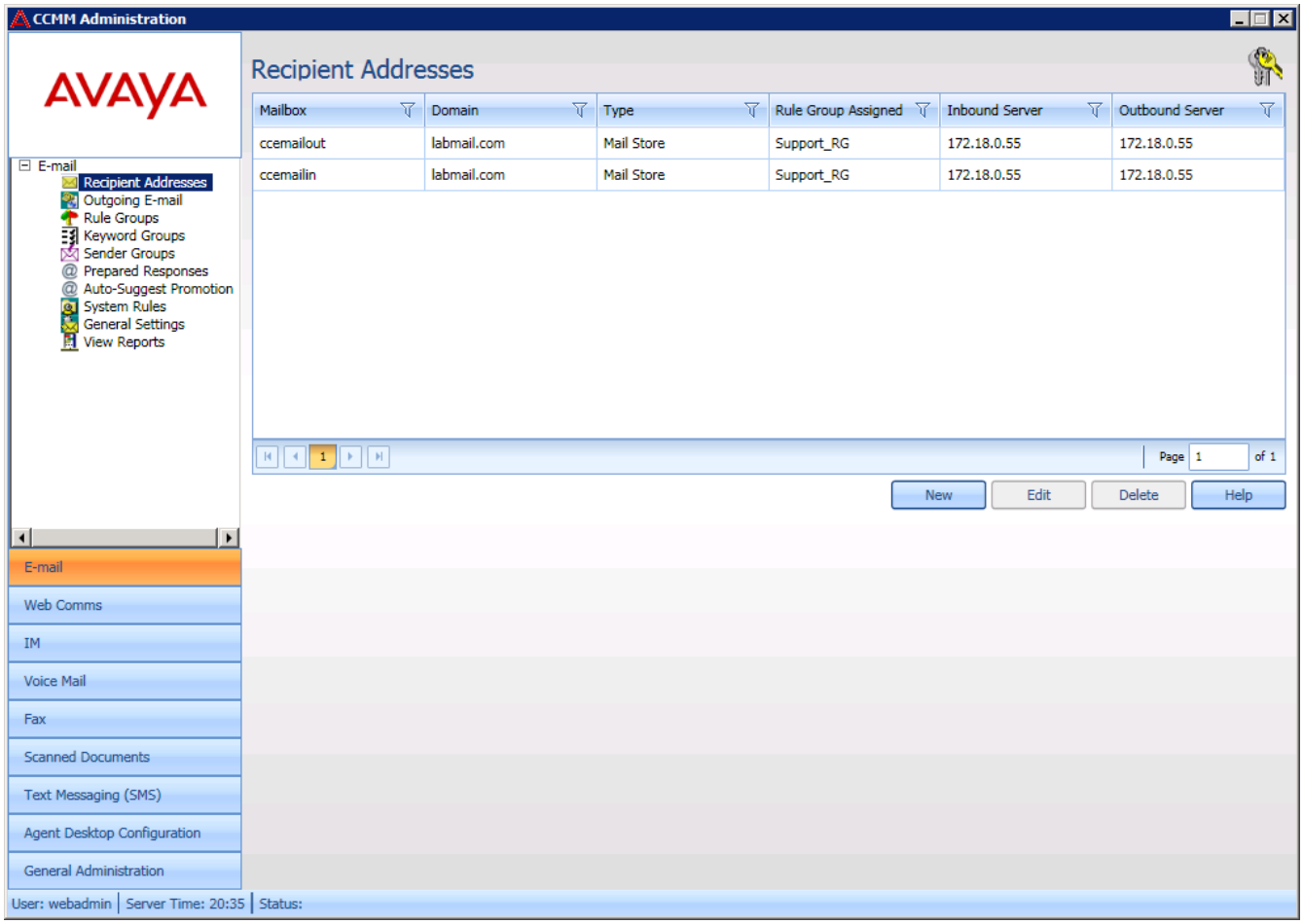
11 In the **Inbound Mail Threshold:** box, type the number of e-mail messages you want Contact Center to retrieve to the database each time it scans the mailbox, for example **100**.

12 From the **Outbound (SMTP) Server:** list, select the e-mail server on which the mailbox is configured, for example **172.18.0.55**.



13 From the **Rule Group:** list, select a rule group, for example **Support_RG**. Contact Center applies this rule group to e-mail messages coming back in to the outbox, for example when a customer replies to an e-mail that an agent sent to them.

14 Click **Save**.



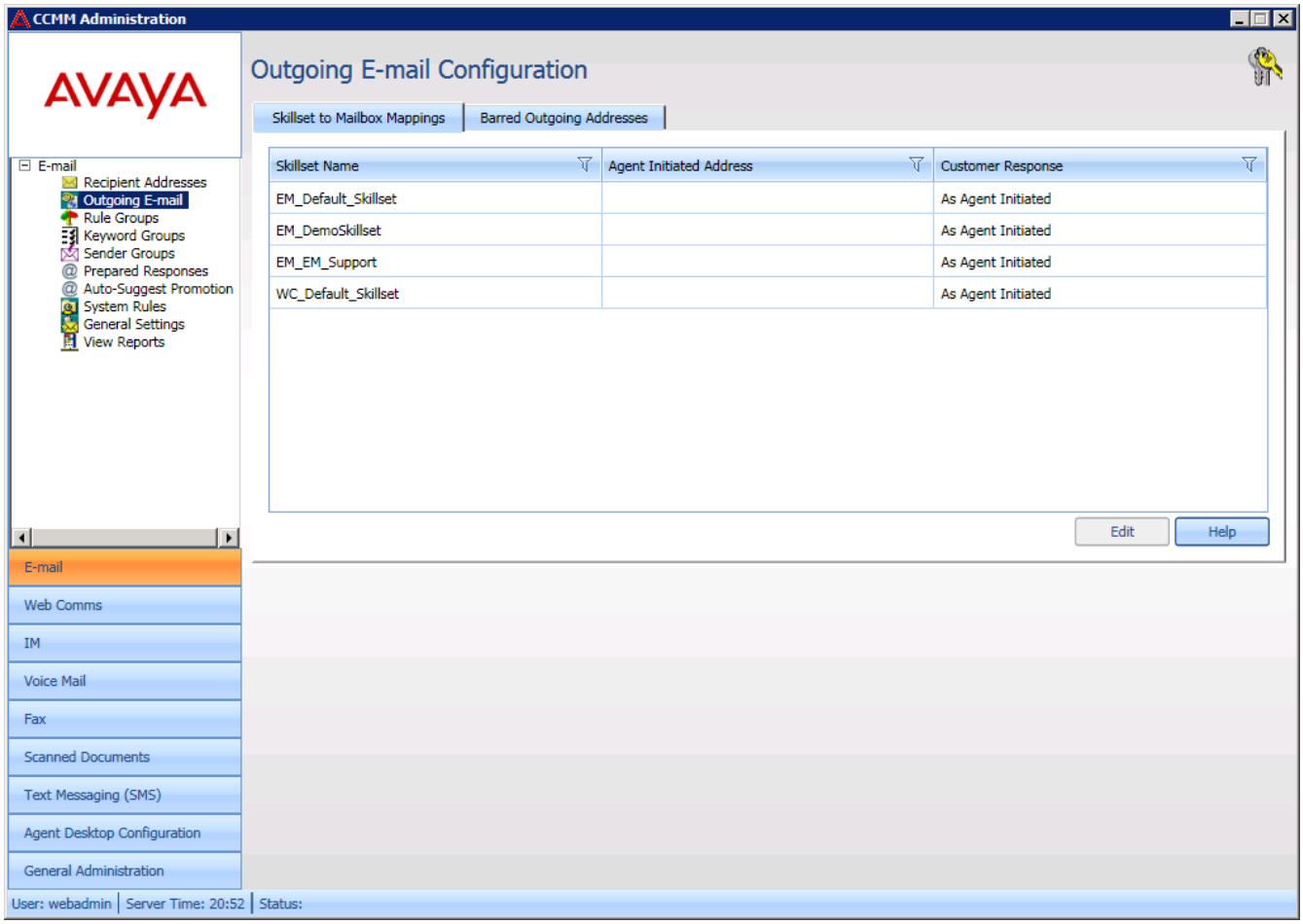
--End--

Configuring the outbound e-mail settings

Configure outbound mailboxes for each Multimedia skillset. Add an outbox to the default skillsets to prevent errors appearing on the Multimedia dashboard.

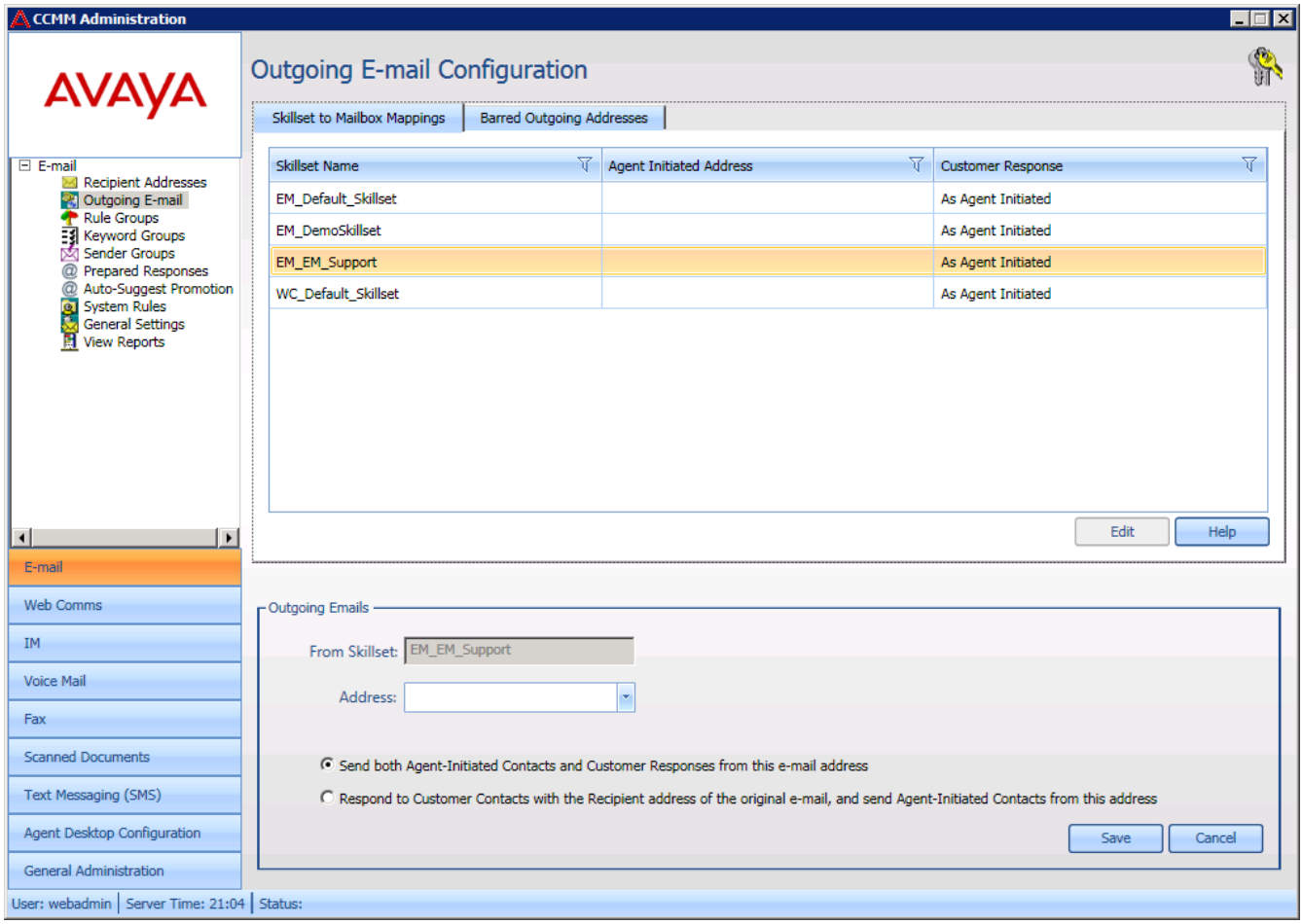
Procedure steps

Step	Action
1	In the left column, under **E-mail**, click **Outgoing E-mail**.

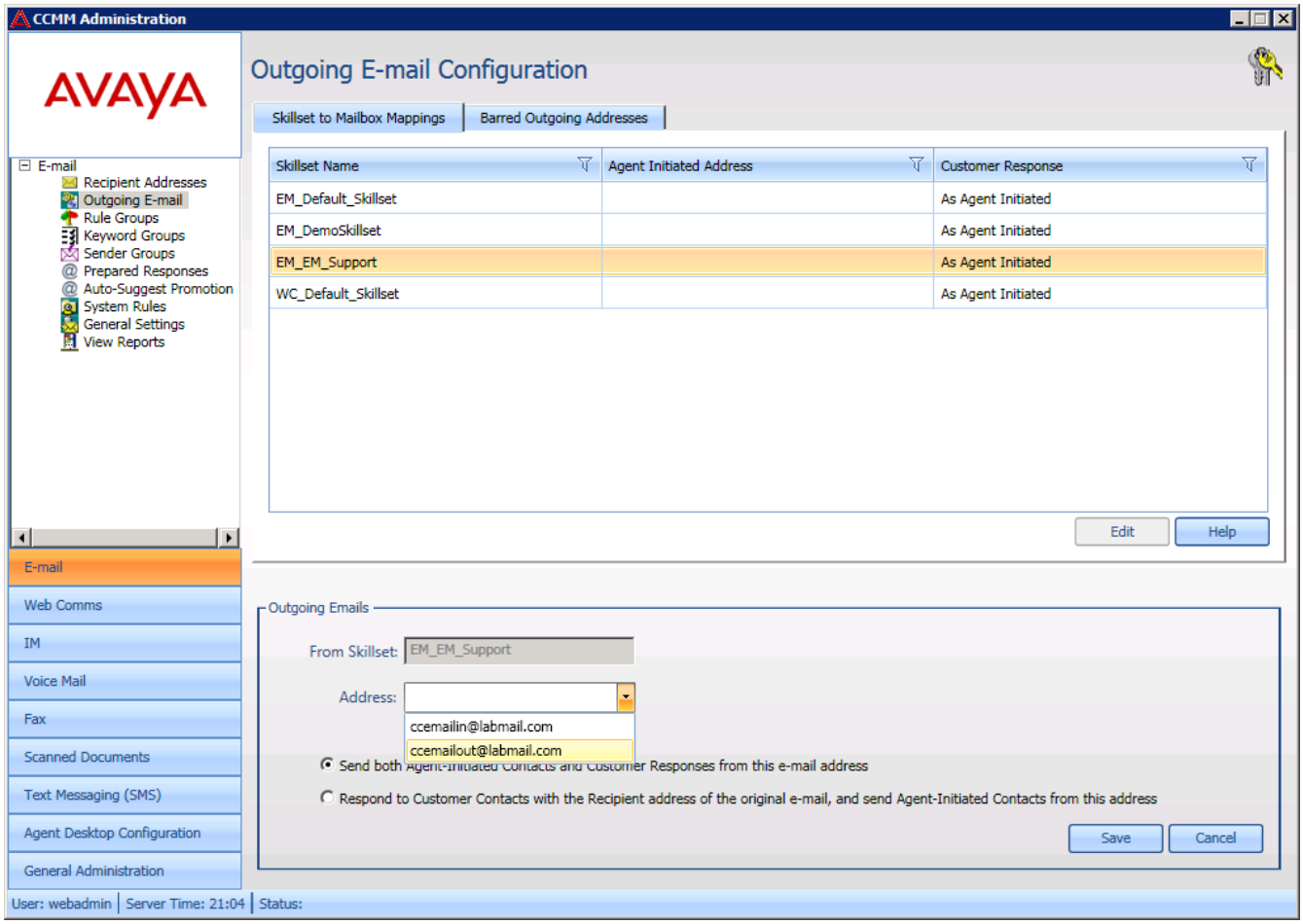


2 On the **Skillset to Mailbox Mappings**, tab, select the skillset you created recently, for example **EM_EM_Support**.

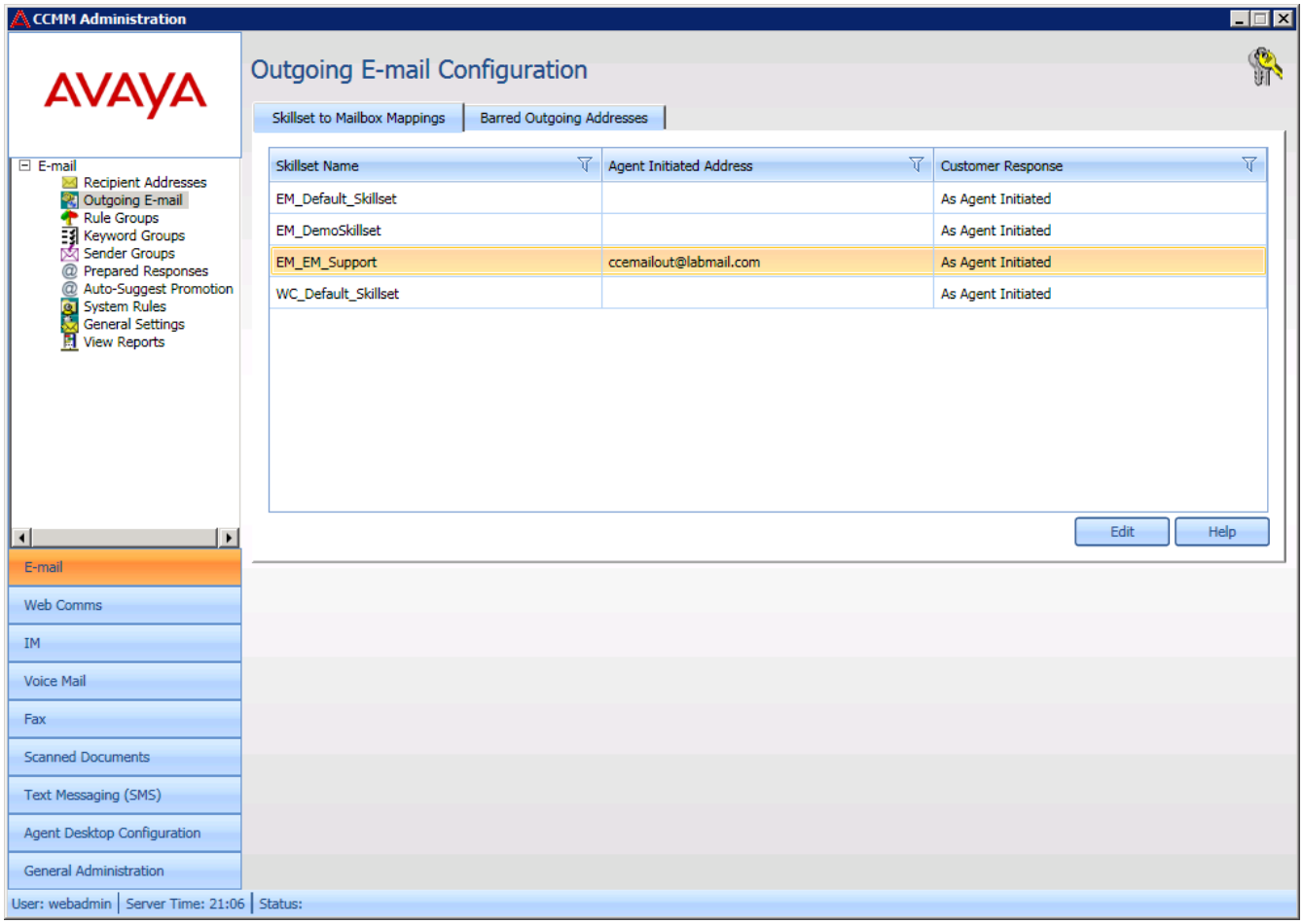
3 Click **Edit**.



4 Under **Outgoing Emails**, from the **Address** list, select a mailbox that you configured for outgoing e-mail messages, for example **ccemailout@labmail.com**.


CCMM Administration
AVAYA
Outgoing E-mail Configuration
Skillset to Mailbox Mappings
Barred Outgoing Addresses
E-mail
Recipient Addresses
Outgoing E-mail
Rule Groups
Keyword Groups
Sender Groups
Prepared Responses
Auto-Suggest Promotion
System Rules
General Settings
View Reports
Skillset Name
Agent Initiated Address
Customer Response
EM_Default_Skillset
As Agent Initiated
EM_DemoSkillset
As Agent Initiated
EM_EM_Support
As Agent Initiated
WC_Default_Skillset
As Agent Initiated
Edit
Help
E-mail
Web Comms
IM
Voice Mail
Fax
Scanned Documents
Text Messaging (SMS)
Agent Desktop Configuration
General Administration
Outgoing Emails
From Skillset:
EM_EM_Support
Address:
ccemailin@labmail.com
ccemailout@labmail.com
Send both Agent-Initiated Contacts and Customer Responses from this e-mail address
Respond to Customer Contacts with the Recipient address of the original e-mail, and send Agent-Initiated Contacts from this address
Save
Cancel
User: webadmin
Server Time: 21:04
Status:

5 Click **Save**.



6 Repeat step 2 to step 5 for each of the default skillsets, for example EM_Default_Skillset and WC_Default_Skillset.

--End--

Configuring the e-mail general settings

Configure the following e-mail settings for e-mail messages entering and leaving your designated contact center mailboxes:

- how frequently Contact Center scans the e-mail server for new messages
- the location in which attachments are stored
- the automatic numbering of e-mail messages

Default values are provided for required fields. You can change or accept the default values for the optional settings.

Procedure steps

Step	Action
1	In CCMM Administration, in the left column, click **E-mail**.
2	Click **General Settings**.
3	To configure a mailbox scan interval, under **Mailbox Scan Interval**, in the **Interval:** box, type the time in minutes.
4	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.
5	To include the customer ID or contact ID in a number for the outgoing e-mail message numbering, under **Message Properties**, select the **Customer ID** check box, the **Contact ID** check box, or both.
6	To include the e-mail message body in the keyword search, under **Message Properties**, select the **Include email body in keyword search** check box.
7	Click **Save**.

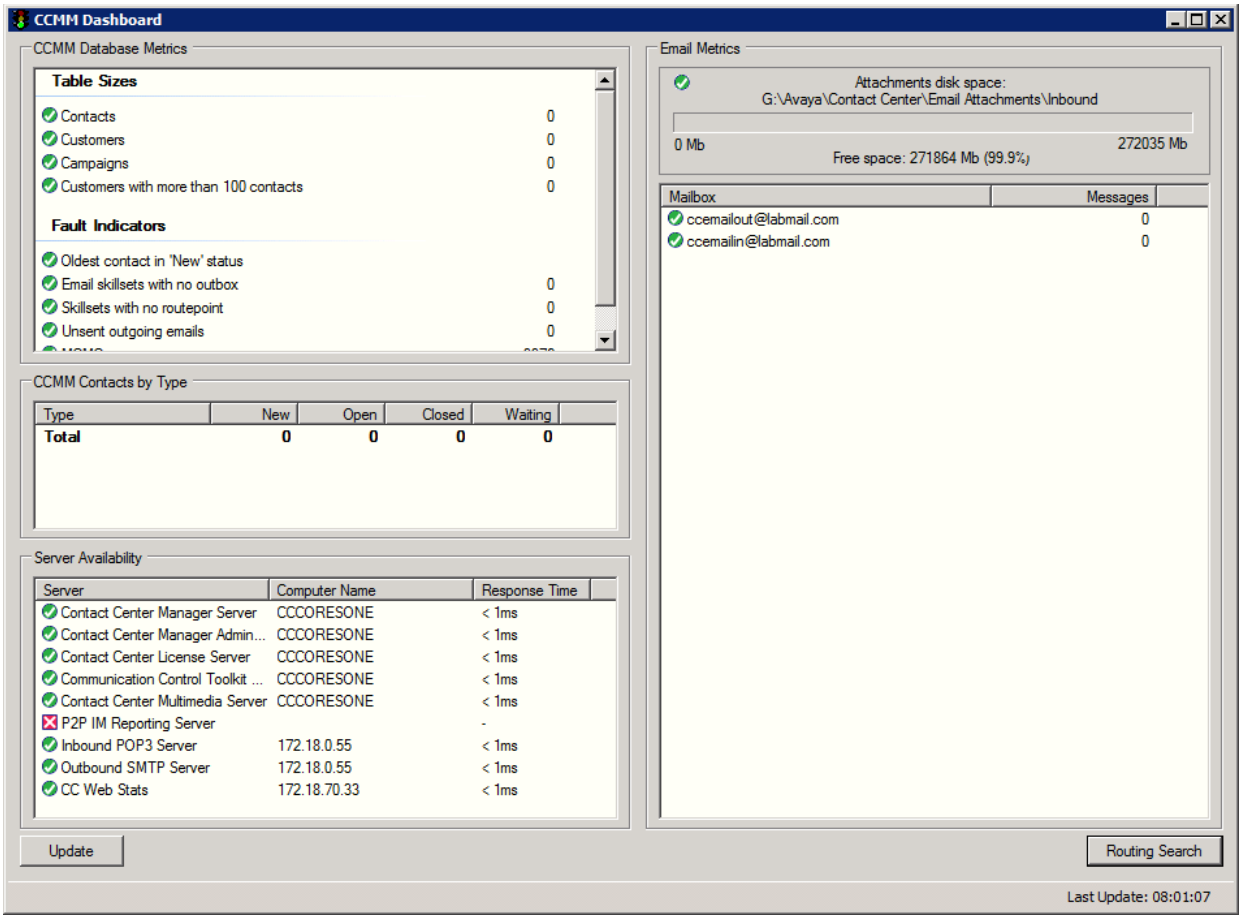
--End--

Checking the status of the Multimedia e-mail configuration

Use the Multimedia dashboard to check the progress and status of the Multimedia e-mail configuration.

Procedure steps

Step	Action
1	Select **Start, All Programs, Avaya, Contact Center, Multimedia server, Multimedia Dashboard**.
2	Review the dashboard information in the **CCMM Database Metrics** box. You see no errors.



3 Review the dashboard information in the **Server availability** box. You see only one error: **P2P IM Reporting Server**.

4 Review the dashboard information in the **Email Metrics** box. You see the outbox and inbox that you configured, with no errors.

--End--

Configuring MIME types to support e-mail attachments

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

Procedure steps

Step **Action**

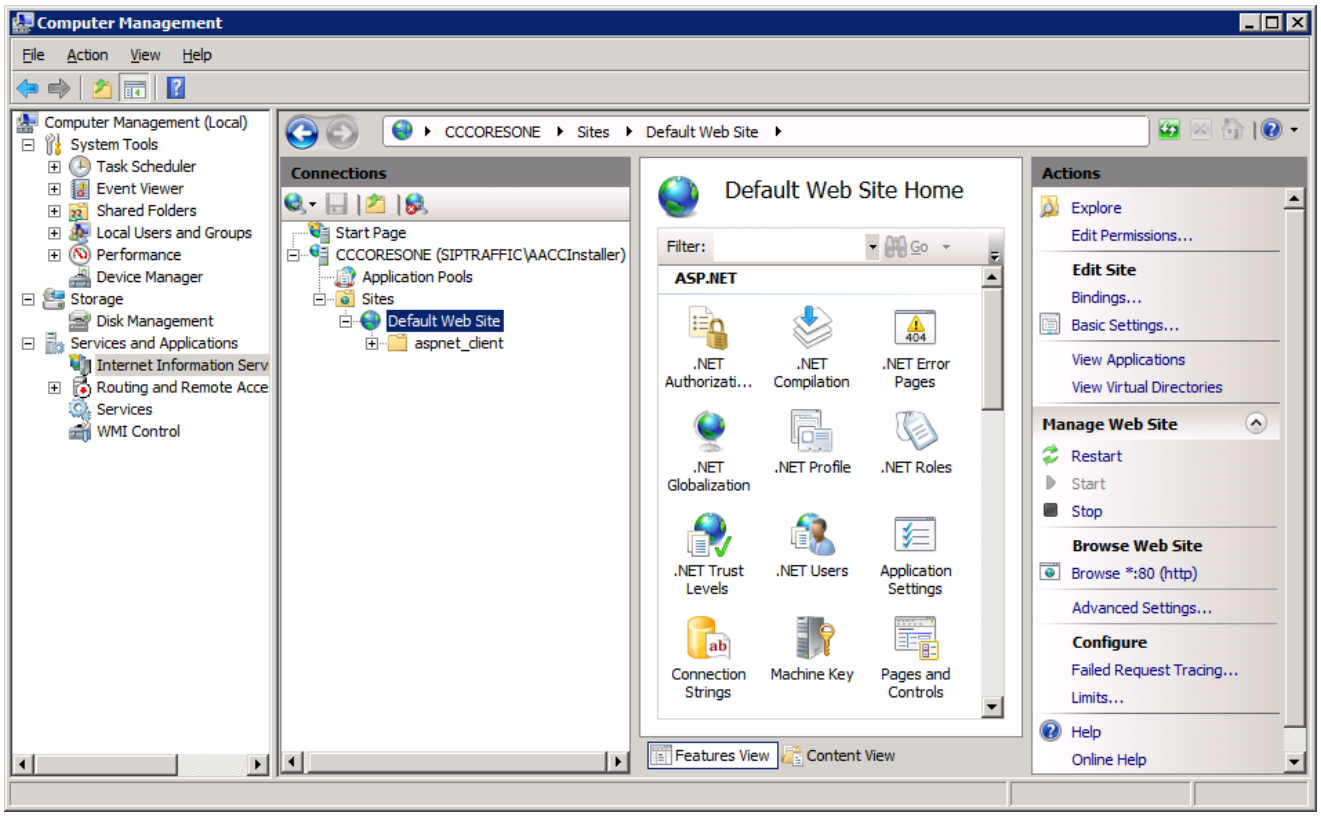
1 Log on to the Contact Center server using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.

2 Click **Start**, **Administrative Tools**, **Computer Management**.

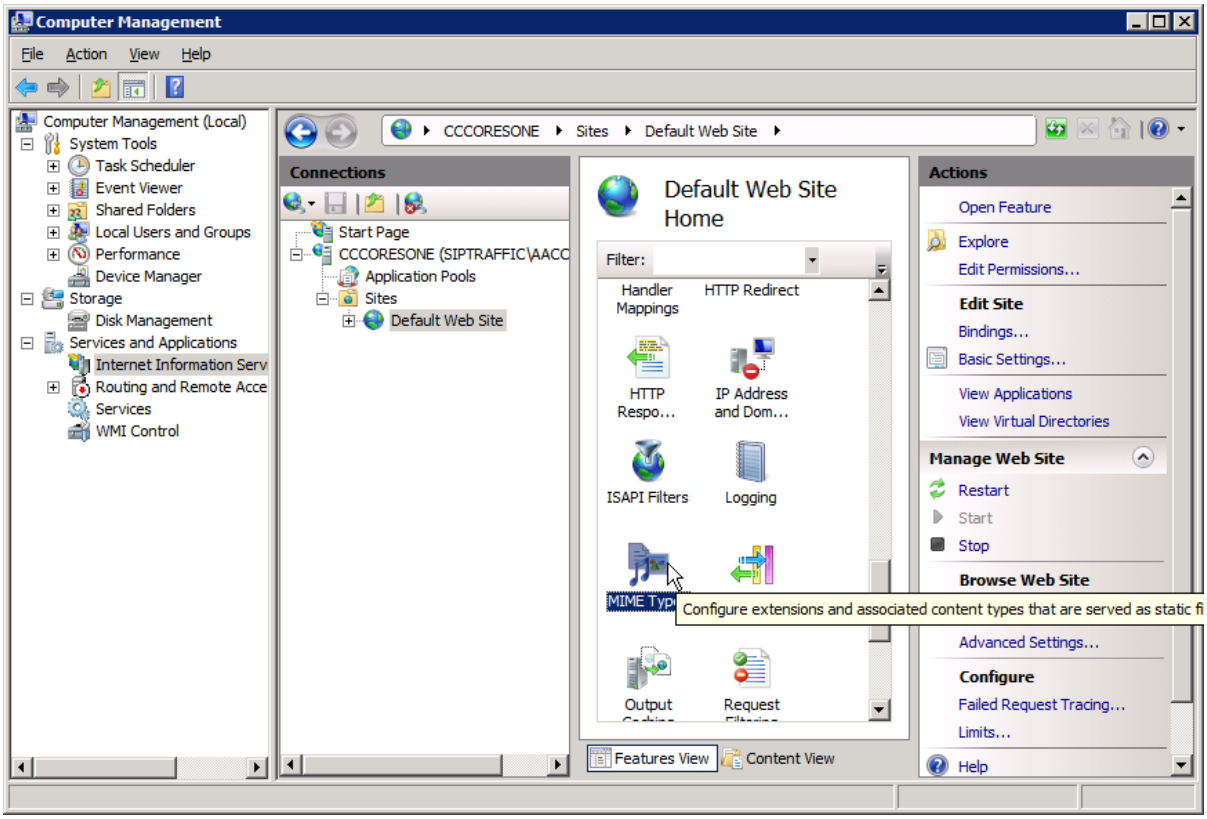
3 In the **Computer Management** dialog box, expand **Services and Applications**, **Internet Information Services (IIS Manager)**.

4 Under **Connections**, expand **CCCORESONE**, **Sites**, **Default Web Site**.

5 Select **Default Web Site**.



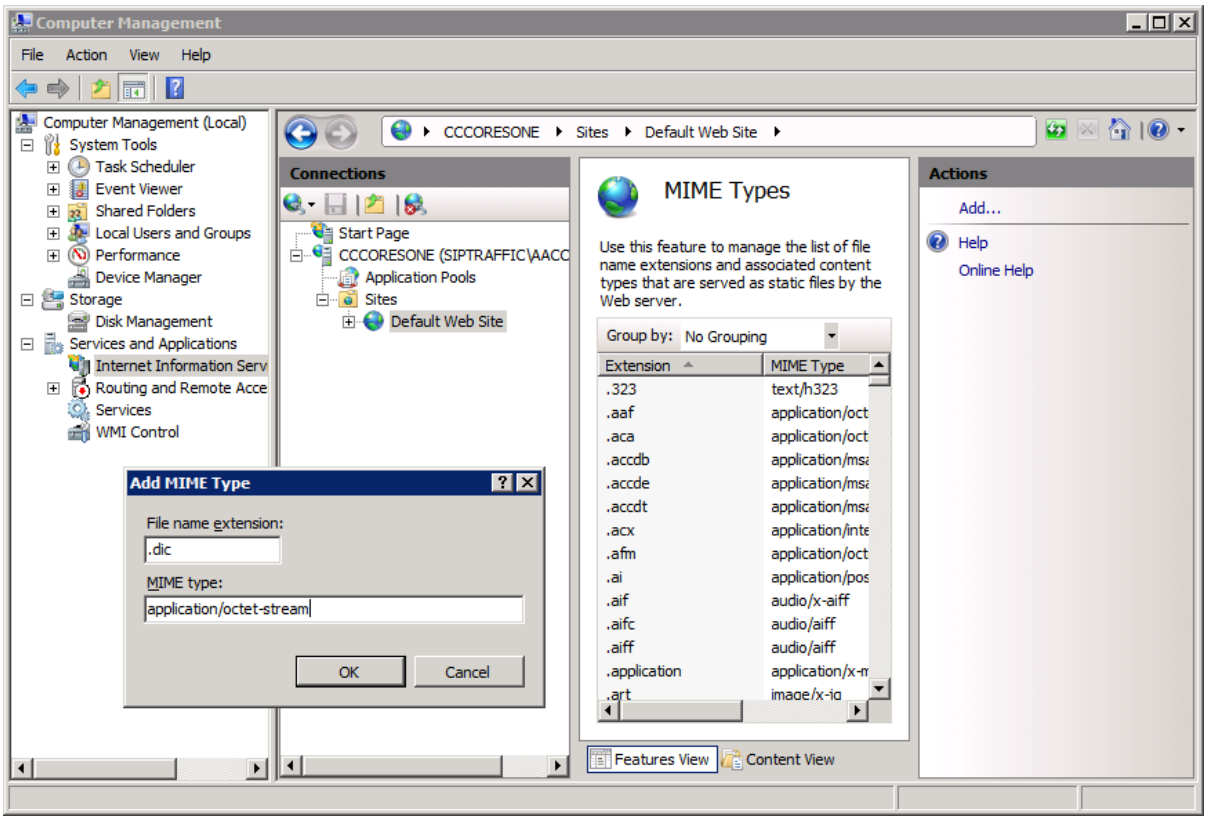
6 In the **Default Web Site Home** pane, under **IIS**, double-click **MIME Types**.



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

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

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

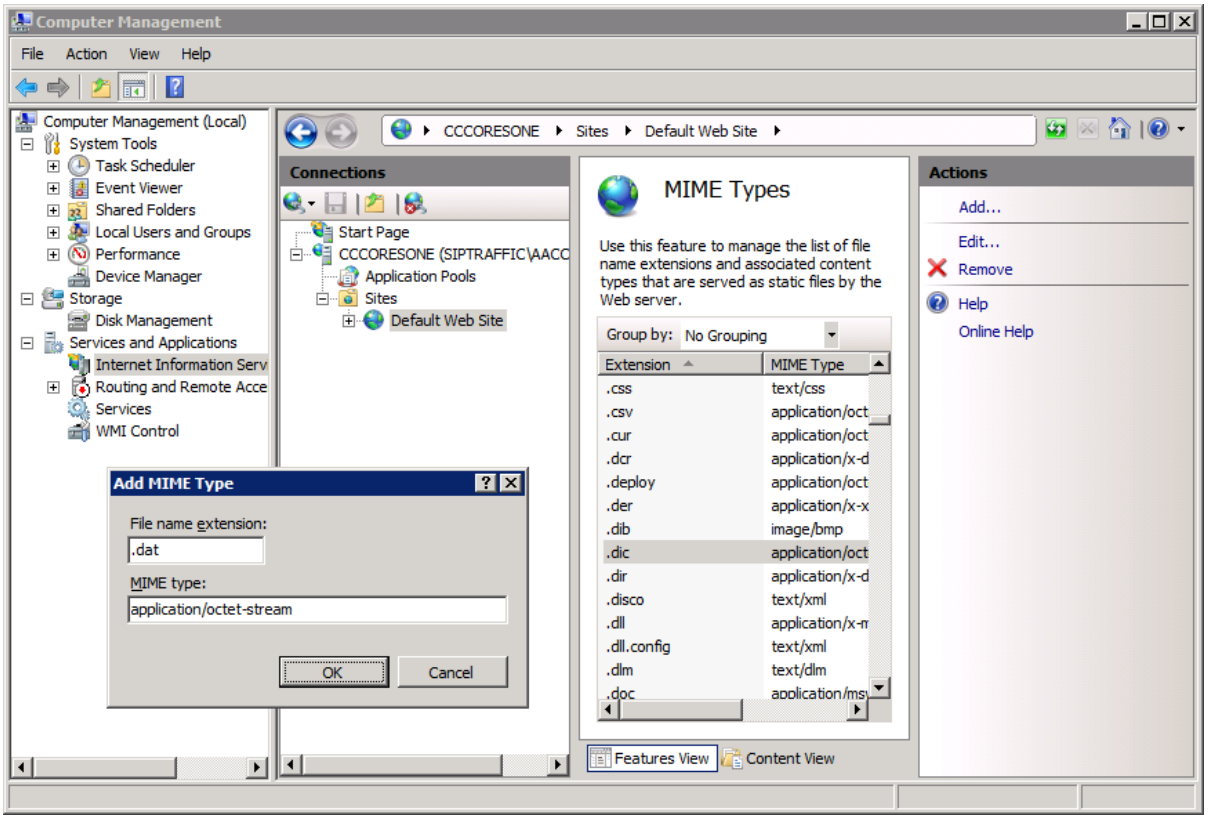


10 Click **OK**.

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**.

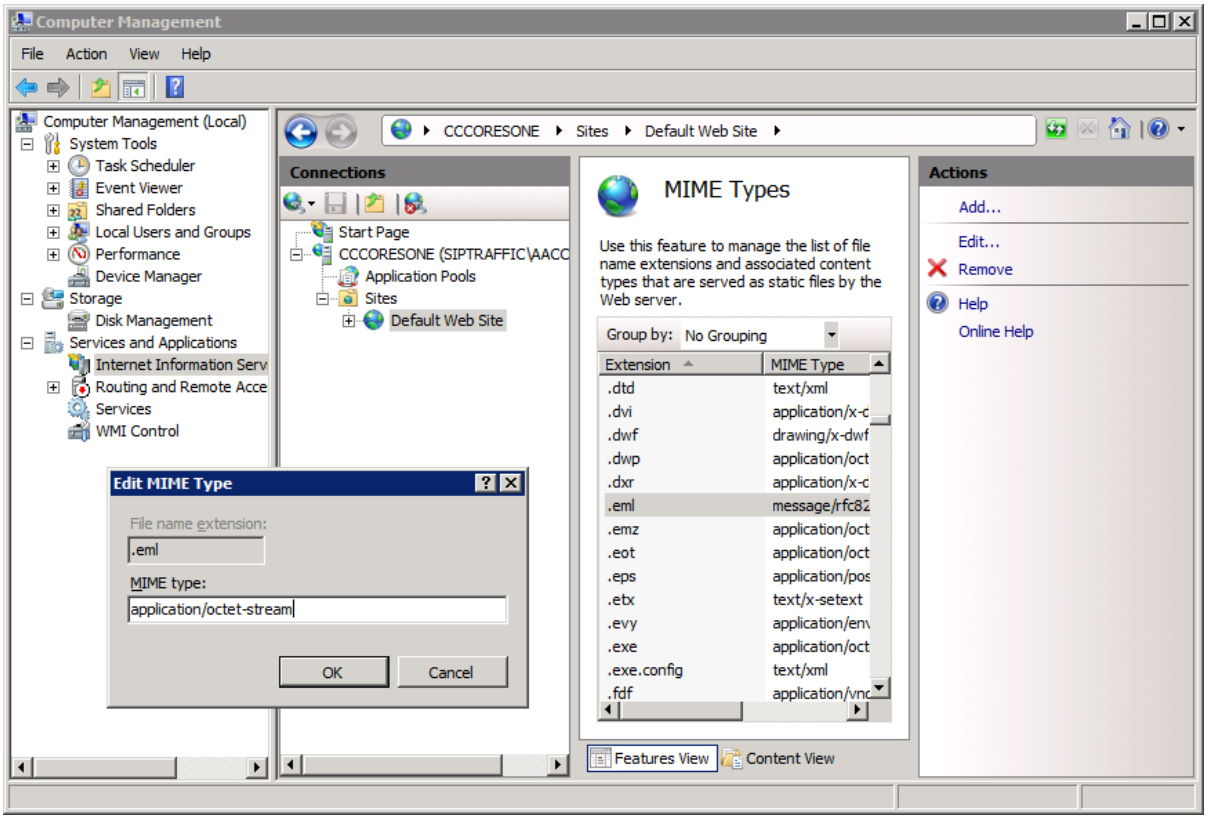


14 Click **OK**.

15 In the MIME Types list, find the **.eml** extension.

16 Right-click the **.eml** extension, and select **Edit**.

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



18 Click **OK**.

19 Close the **Computer Management** window.

--End--

Preparing the Windows Domain for the Call Center Elite Integration with Contact Center

This chapter describes the procedures required to prepare the Windows domain for Call Center Elite integration with Contact Center.

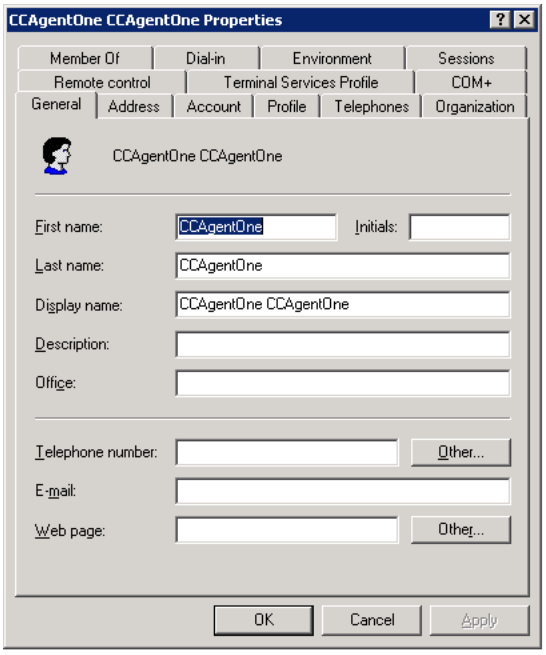
Creating Domain users and groups for agents

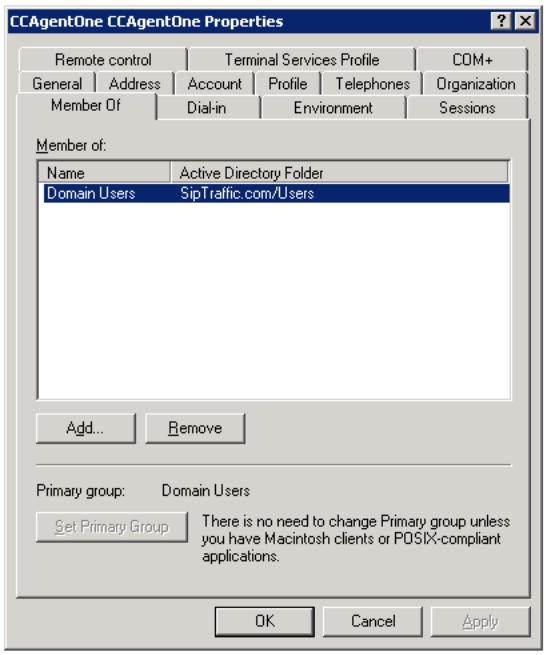
Create domain users for the Call Center Elite agents (if they do not already exist). Add the agents' desktops to the domain, then add the desktops to a Windows domain organizational unit (OU). Agents need a domain account to log onto a desktop computer to use Agent Desktop. Keeping all the contact center desktops in a single group allows management of policies for them.

Attention: You must have administration rights on the domain to complete these procedures. Ask the domain administrator to create or modify the user accounts, computer or server accounts, and organizational unit as required.

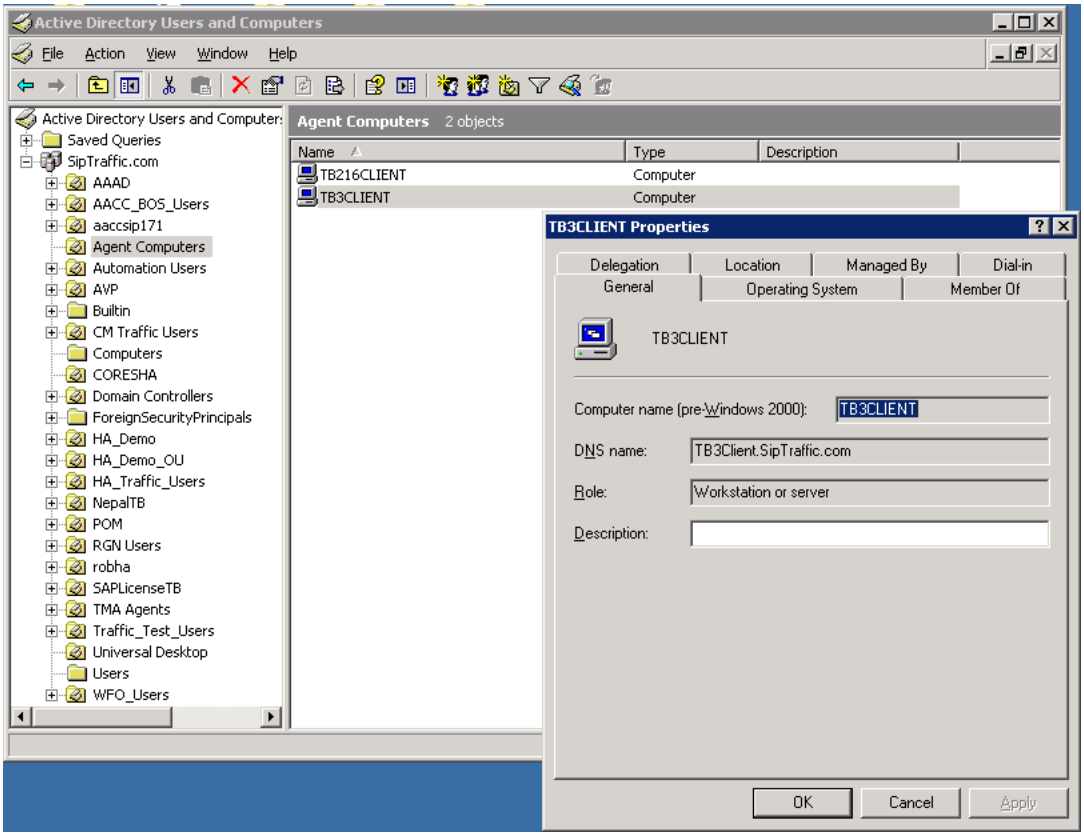
Procedure steps

Step	Action
1	For any agents that do not have a domain account, create an account.

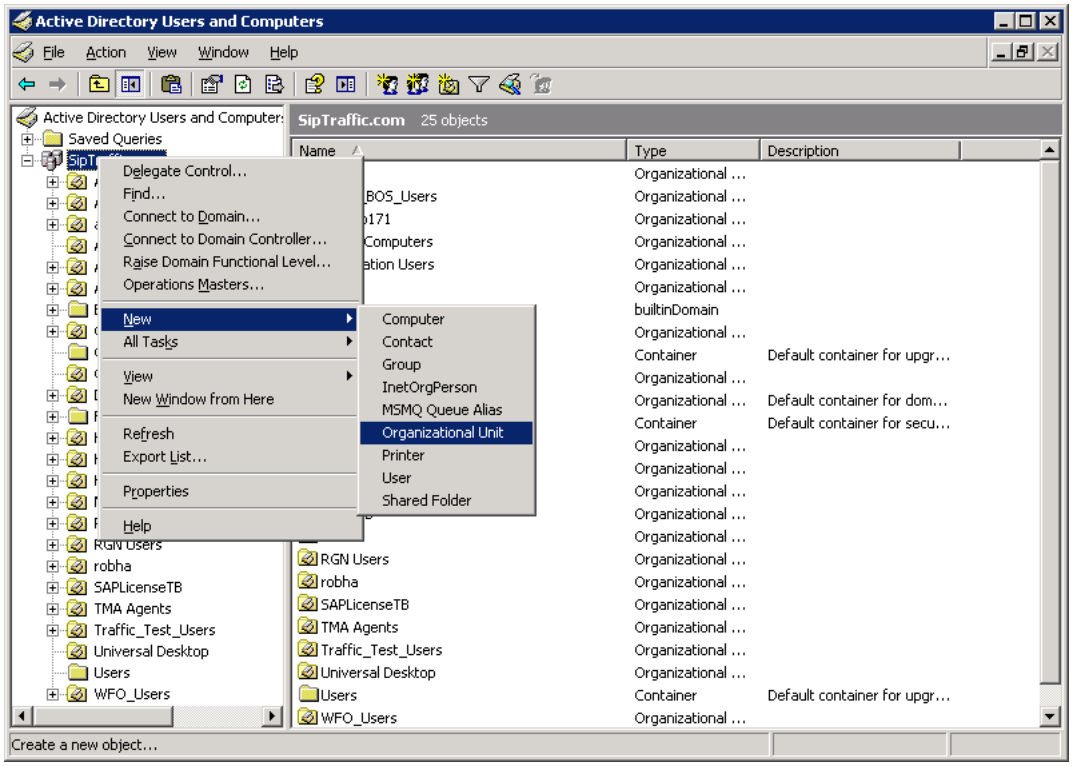


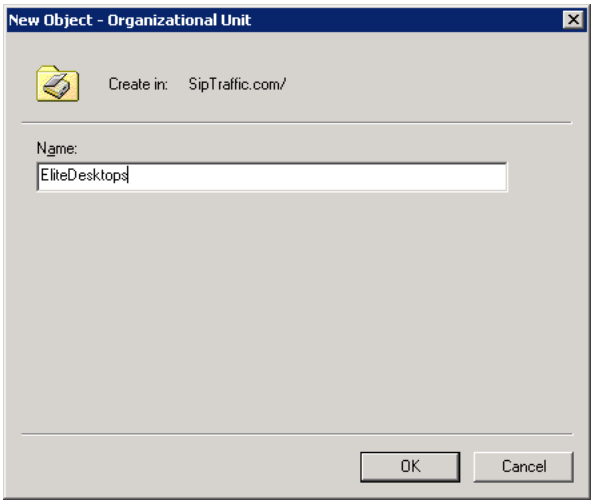


2 Ensure that all the agents' desktop computers are members of the domain. If any are not, add them to the domain.

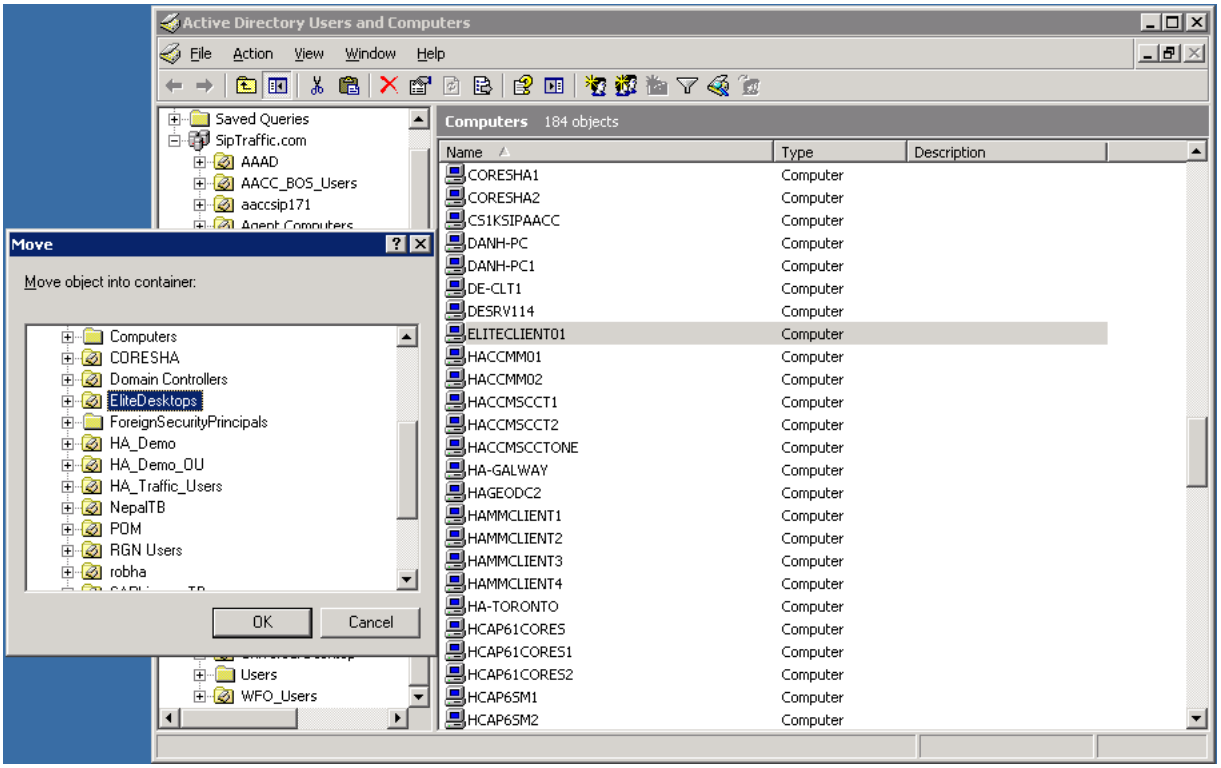


3 On the domain controller server, create a Windows organization unit (OU) to contain all the desktop computers for the agents using Agent Desktop. For example, in the siptraffic.com domain, create an OU called EliteDesktops.





4 Add all the agents' desktops to the OU.



--End--

Assigning a group policy for embedded softphone settings

Assign the Group Policy administrative template, which has specific settings for Agent Desktop, to your Windows domain controller. You need to copy the administrative template file from the CCMM server to the Windows domain controller.

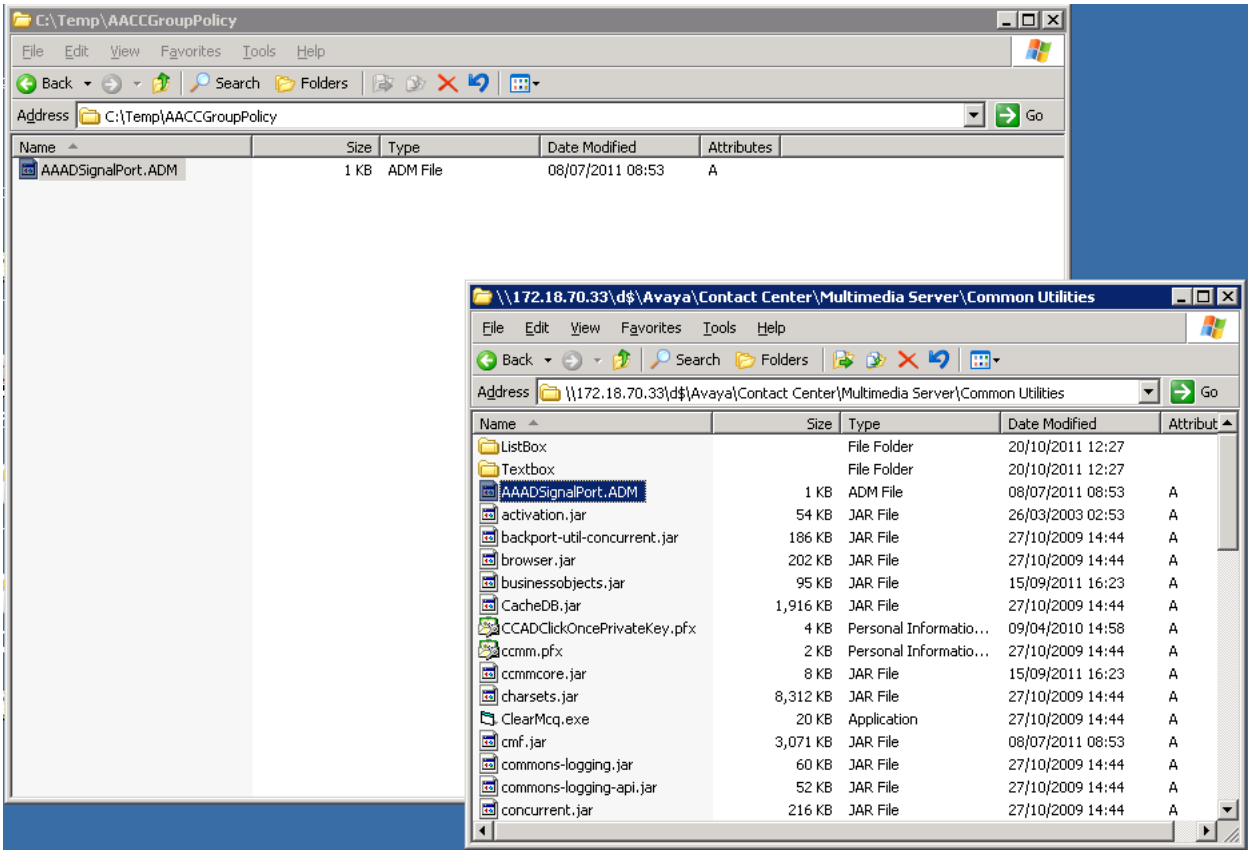
Attention: If you do not have administration rights on the domain, you cannot carry out these procedures. Ask the domain administrator to carry out this procedure if required.

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.

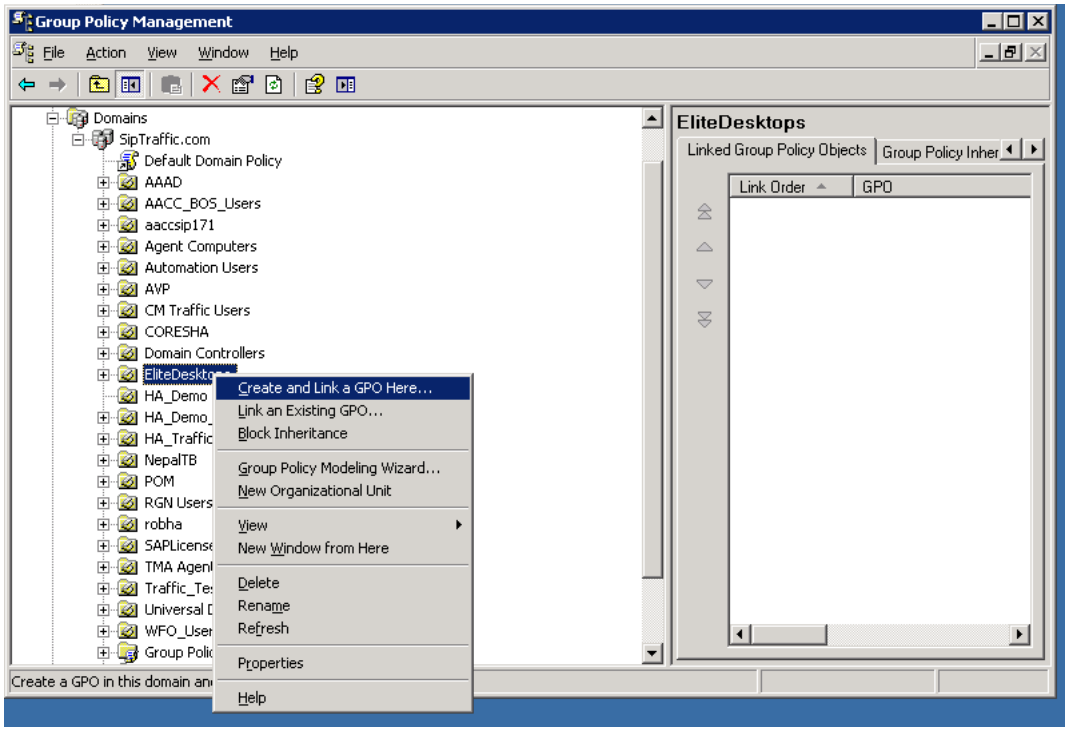
Attention: This procedure requires a reboot of all the desktop computers for the agents using Agent Desktop.

Procedure steps

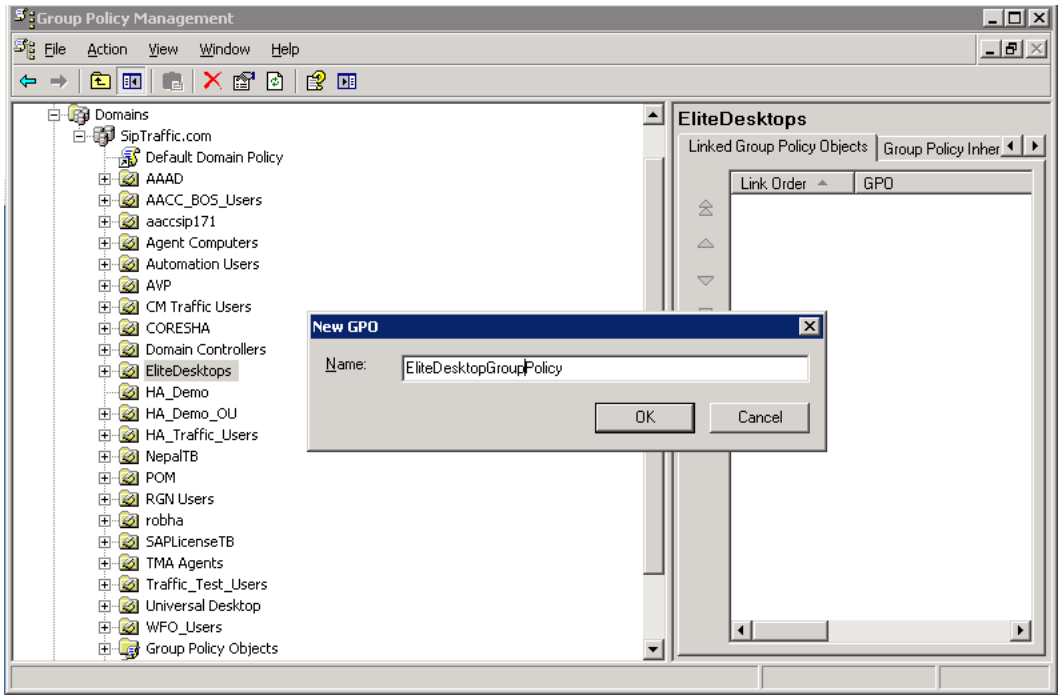
Step	Action
1	Copy the **AAADSignalPort.ADM** file from the D:\Avaya\Contact Center\Multimedia Server\Common Utilities folder on the Contact Center server to a folder on the domain controller, for example **C:\Temp\AACCGroupPolicy**.



2	On the Windows domain controller, choose **Start, Administrative Tools, Group Policy Management**.
3	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.
4	Select **Create and Link a GPO Here...**.



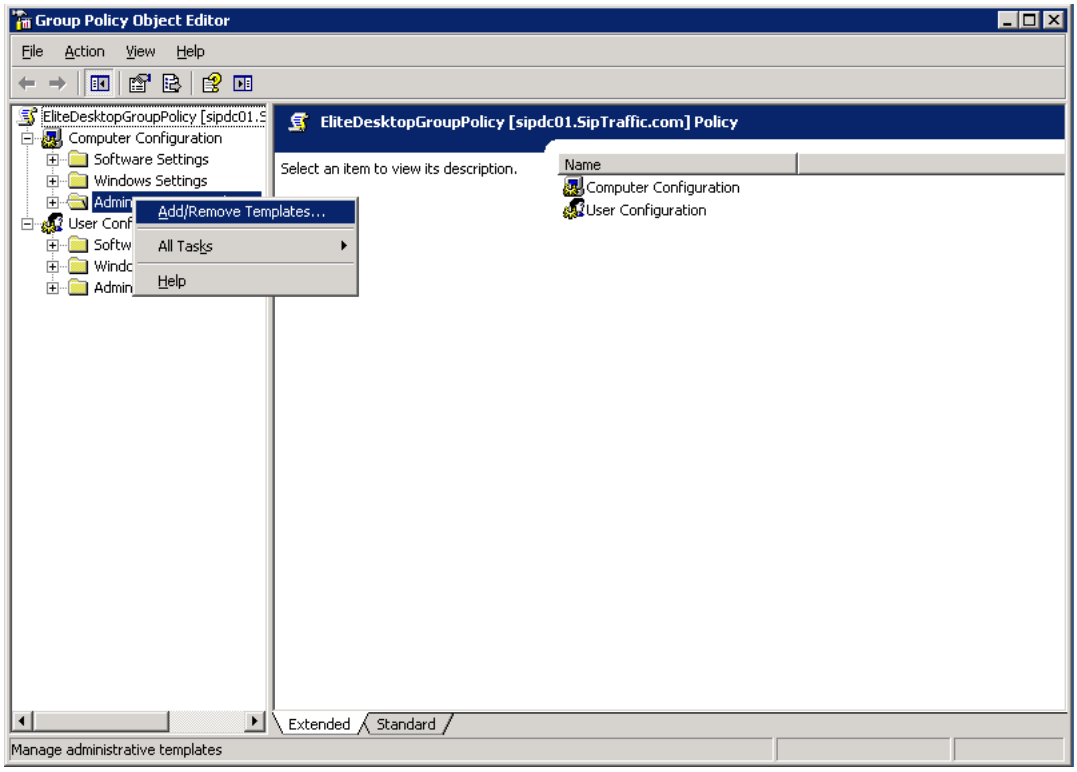
5 In the **Name** box, type a name for the new GPO, for example **EliteDesktopGroupPolicy**.



6 Click **OK**.

7 Right-click the GPO you created, for example **EliteDesktopGroupPolicy**.

8 Select **Edit...**.

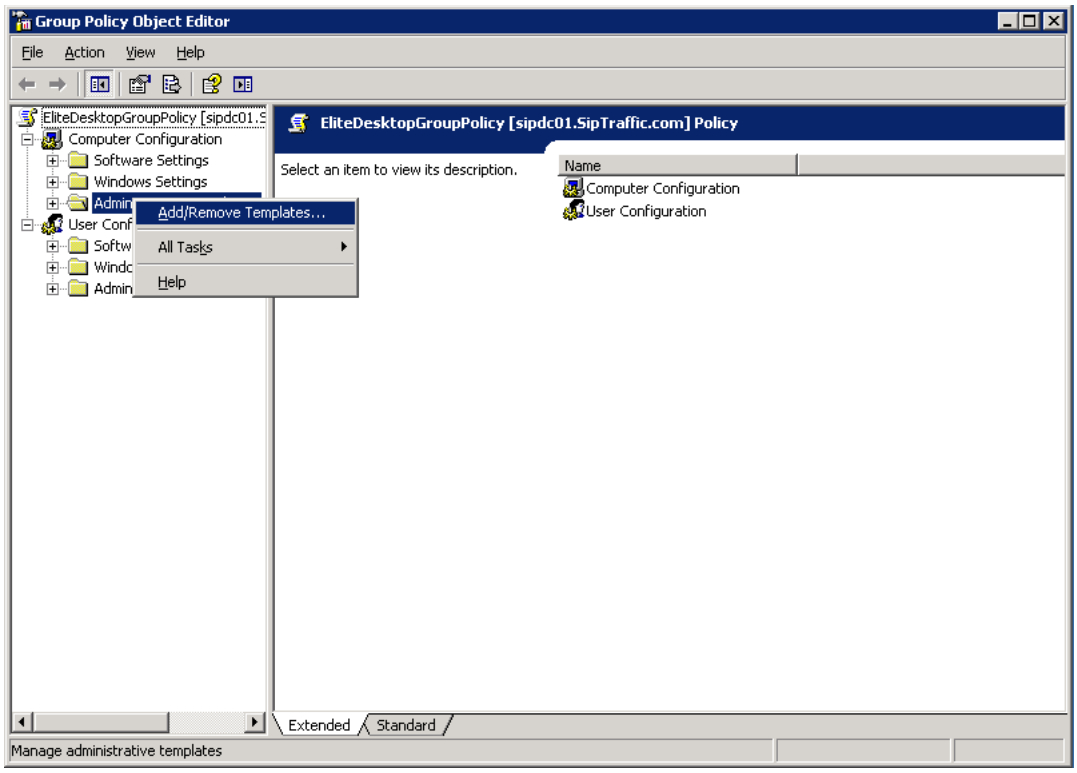


*Windows displays the **Group Policy Object Editor** dialog.*

9 Expand **Computer Configuration**.

10 Under **Computer Configuration**, right-click **Administrative Templates**.

11 Select **Add/Remove Templates...**.

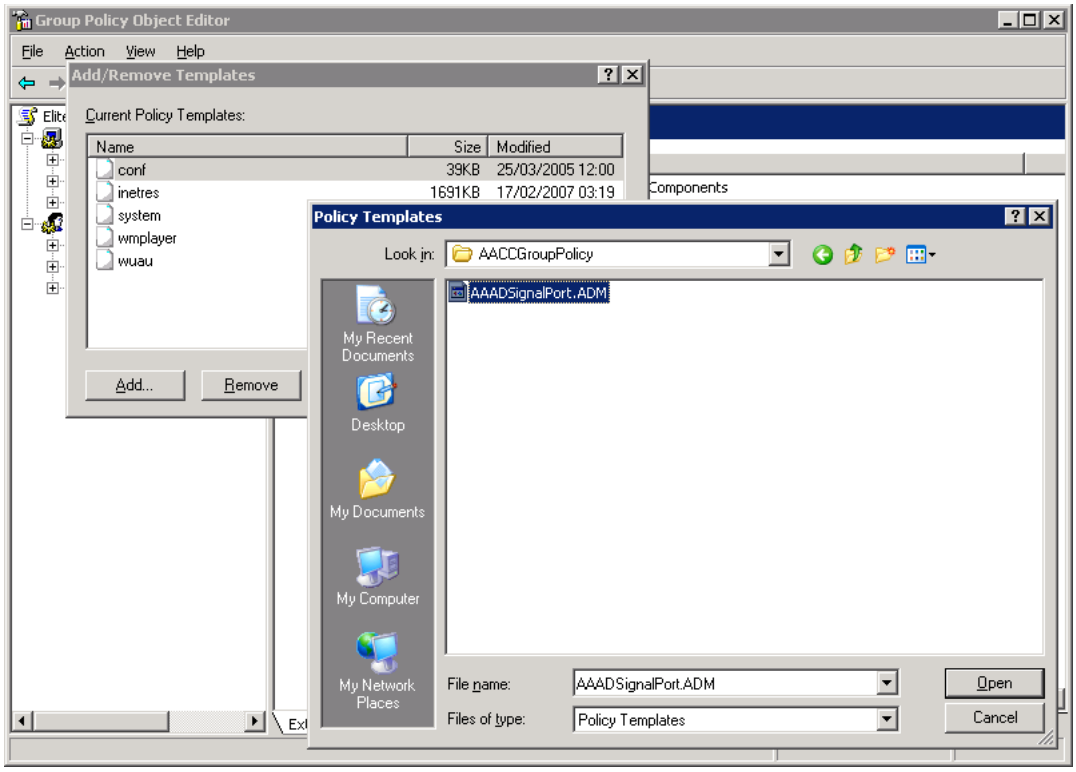


*Windows displays the **Add/Remove Templates** dialog.*

12 Click **Add**.

*Windows displays the **Policy Templates** dialog.*

13 Browse to the location where you copied AAADSignalPort.ADM and select the file.

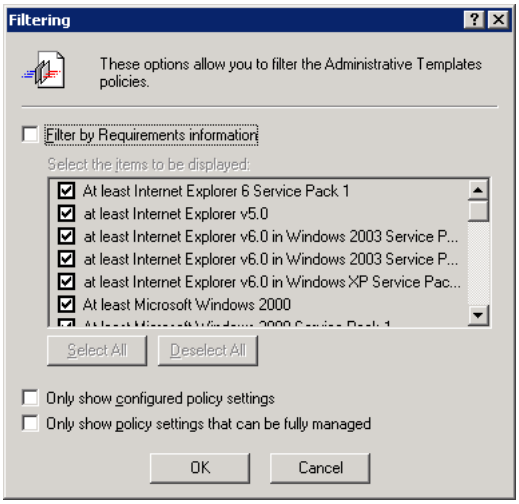


14 Click **Open**.

15 On the **Add/Remove Templates** click **Close**.

16 From the **View** menu, select **Filtering**.

17 Clear **Only show policy settings that can be fully managed**.



18 Click **OK**.

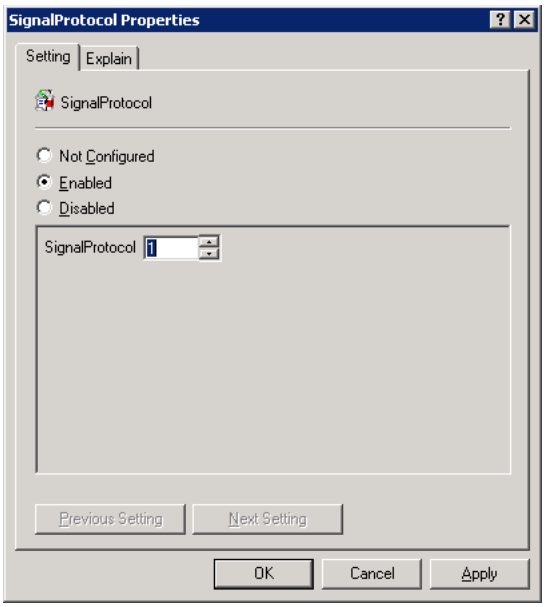
19 Under **Administrative Templates** select the policy template you added, for example **SOFTWARE\Avaya\Avaya one-X Agent\Settings**.

20 In the right-hand pane, right-click the **SignalProtocol** setting, and select **Properties**.

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**.

25 Ensure all agents restart their desktop computers before accessing the Agent Desktop application for the first time.

--End--

Configuring Contact Center to Integrate with Call Center Elite

To integrate Contact Center with Call Center Elite, you need to create agent templates and agent profiles.

Avaya Aura® Agent Desktop supports voice contacts from Call Center Elite. Contact Center agent profiles support the Call Center Elite agents' voice configurations. Agent profiles are dependent on generic agent templates.

The default template contains basic settings for all agents. All agent templates inherit properties from the default template.

Assigning a template to an agent creates that particular agent's profile. You can customize profiles based on individual agent requirements (for example, Elite Login ID and Password).

Templates inherit properties from their parent templates. Inheritance in templates follows a tree structure. Agent Desktop supports up to five levels of inheritance from the default template.

Before creating the template in Contact Center ensure that the Call Center Elite agents and stations exist and are fully operational. Make a note of the agent and station settings so that you can correctly create the templates and profiles in Contact Center.

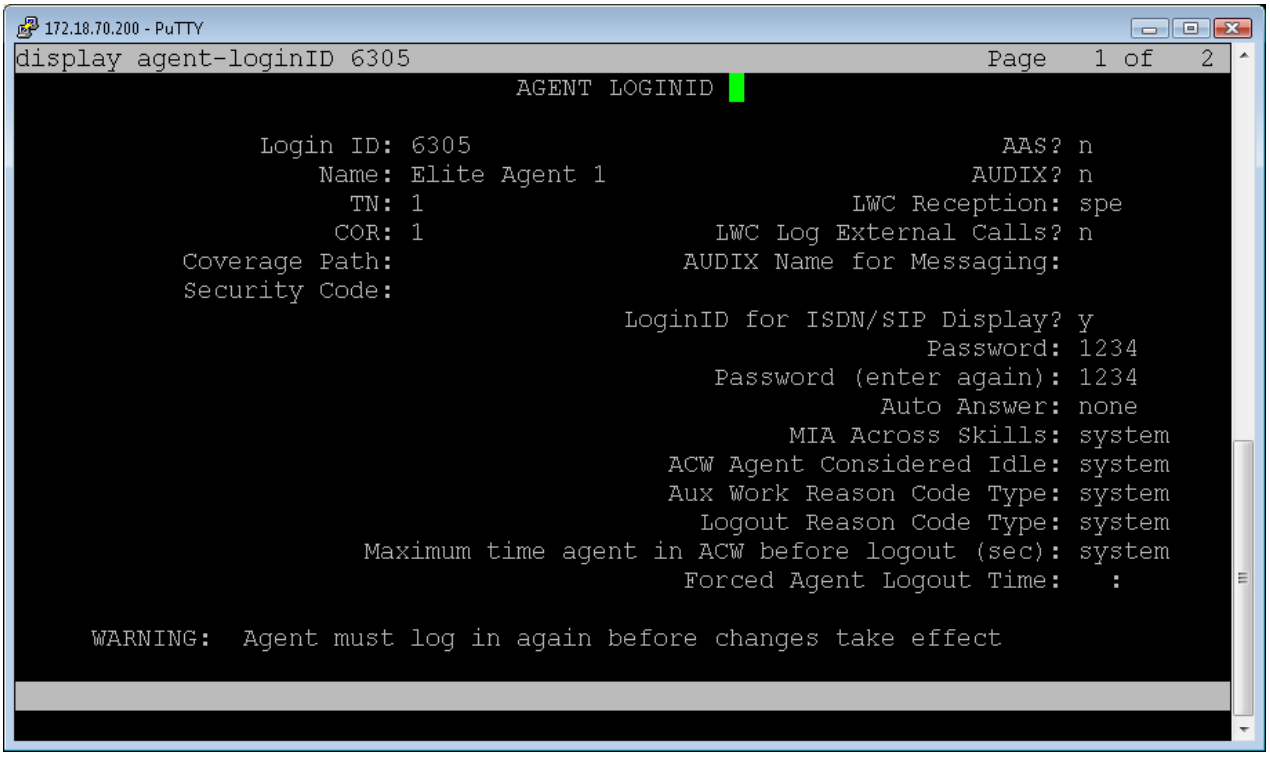
Checking the Elite agent and station settings

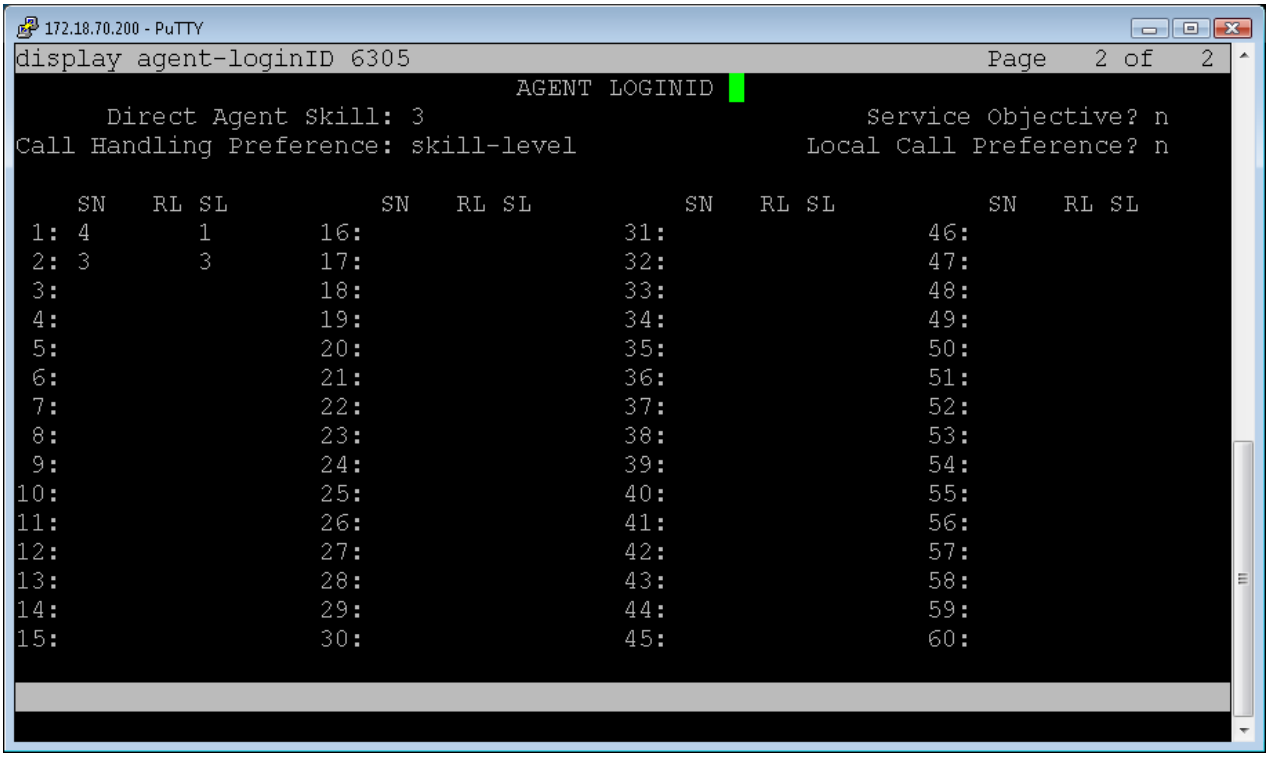
Check that each agent that is to use the Contact Center Multimedia Complement exists and is configured on Call Center Elite. Record information about the agent and their station to ensure you can set up the Contact Center agent templates correctly.

Prerequisites

Procedure steps

Step	Action
1	Access the Call Center Elite administrative tool.
2	Verify the agent exists by checking the agent record.



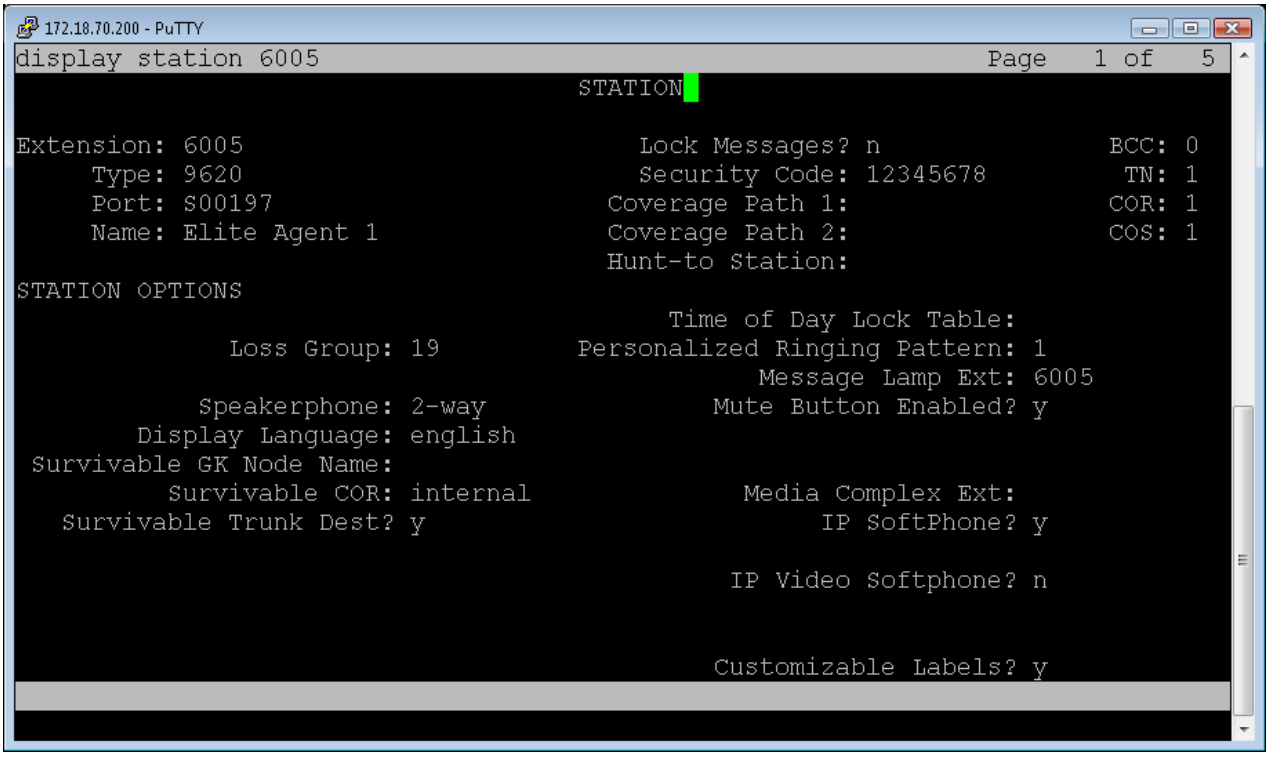


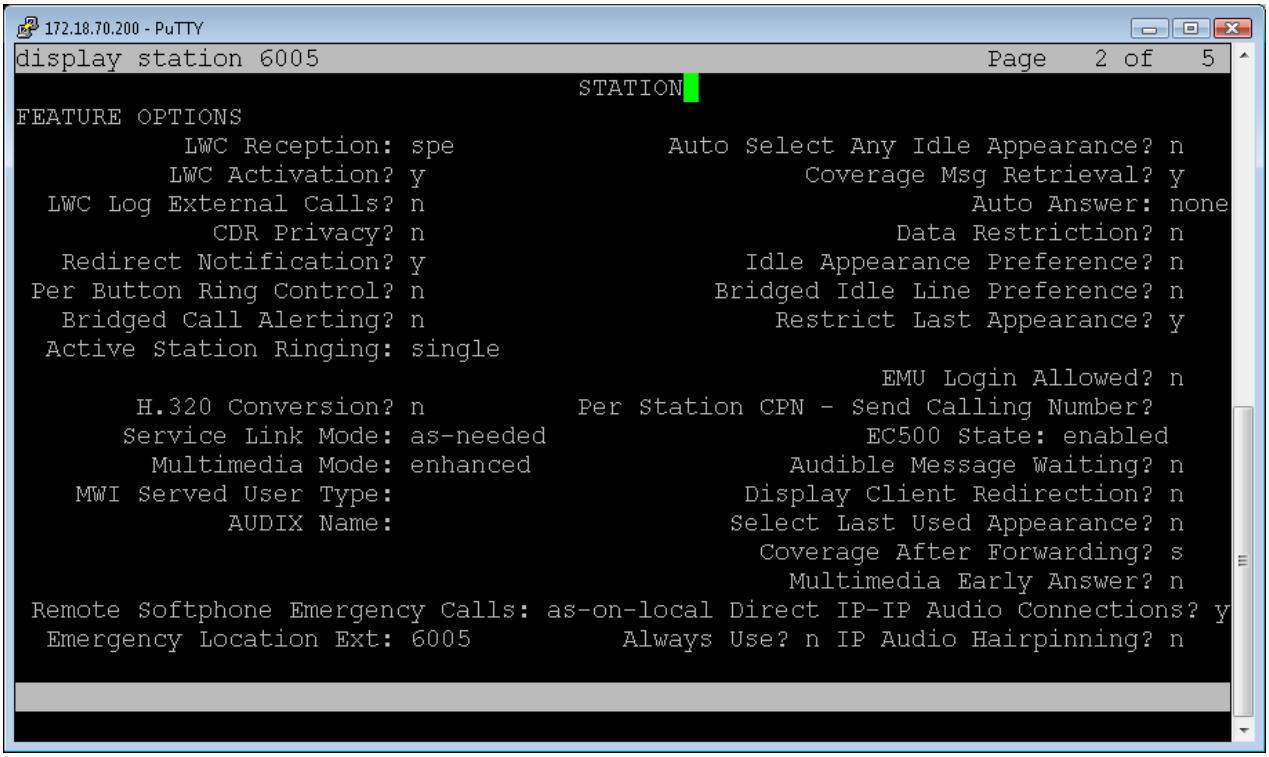
3 Make a record of the agent's **Login ID** and **Password**, for example **6305** and **1234**.

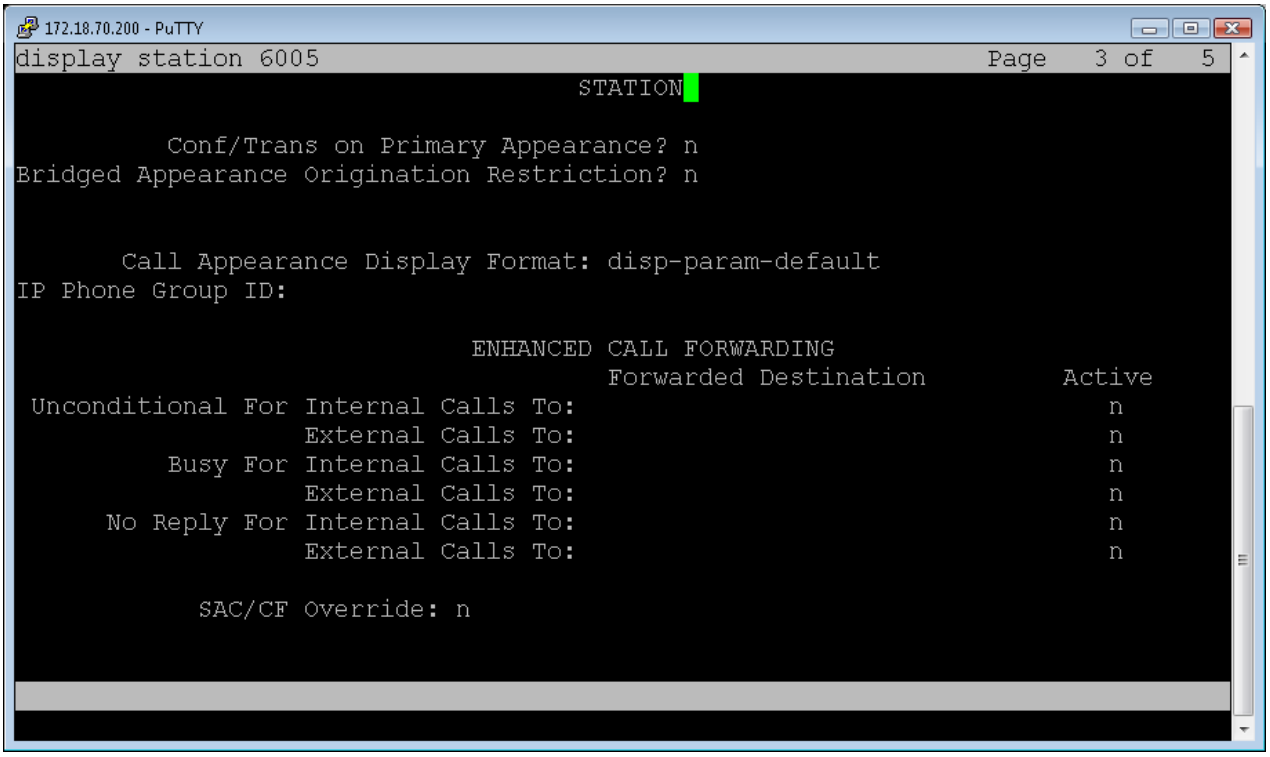
4 Note any other agent setting that is relevant to the way the agent handles voice contacts, for example **Auto Answer** set to **none**.

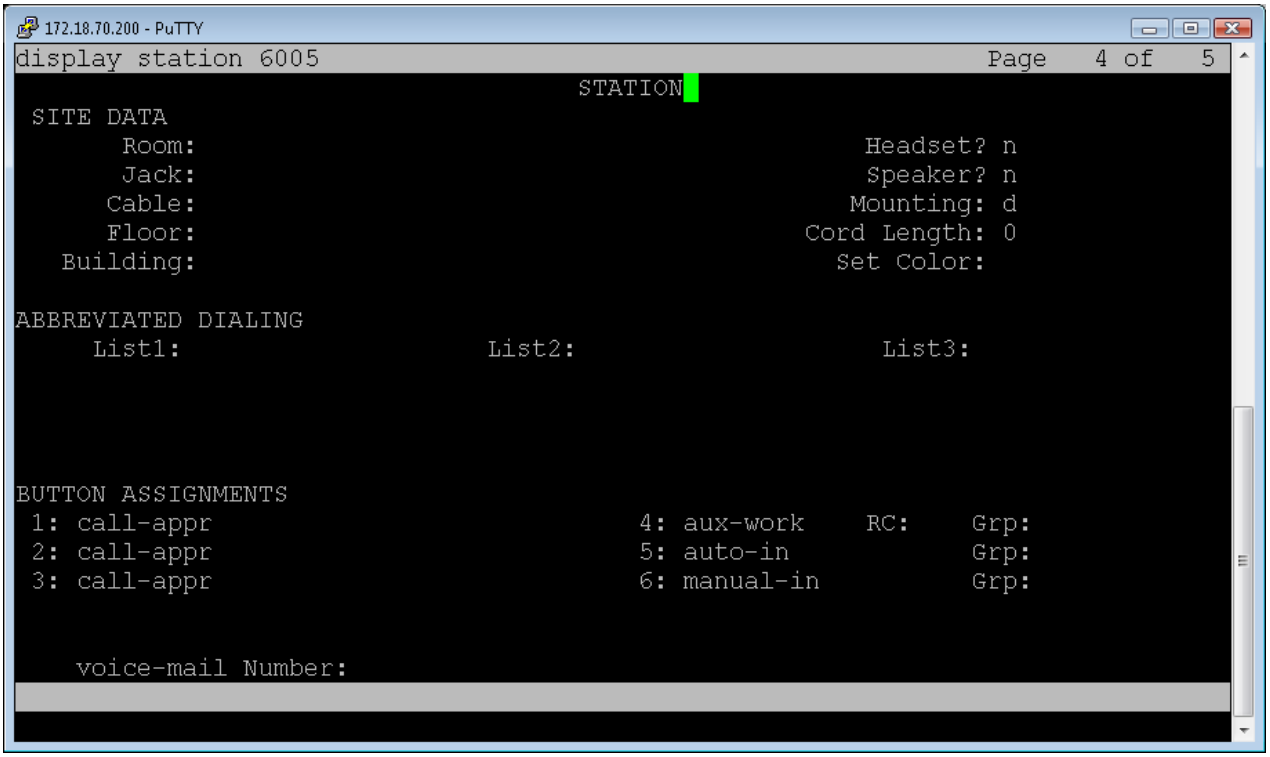
5 Verify the agent's station exists by checking the station record.

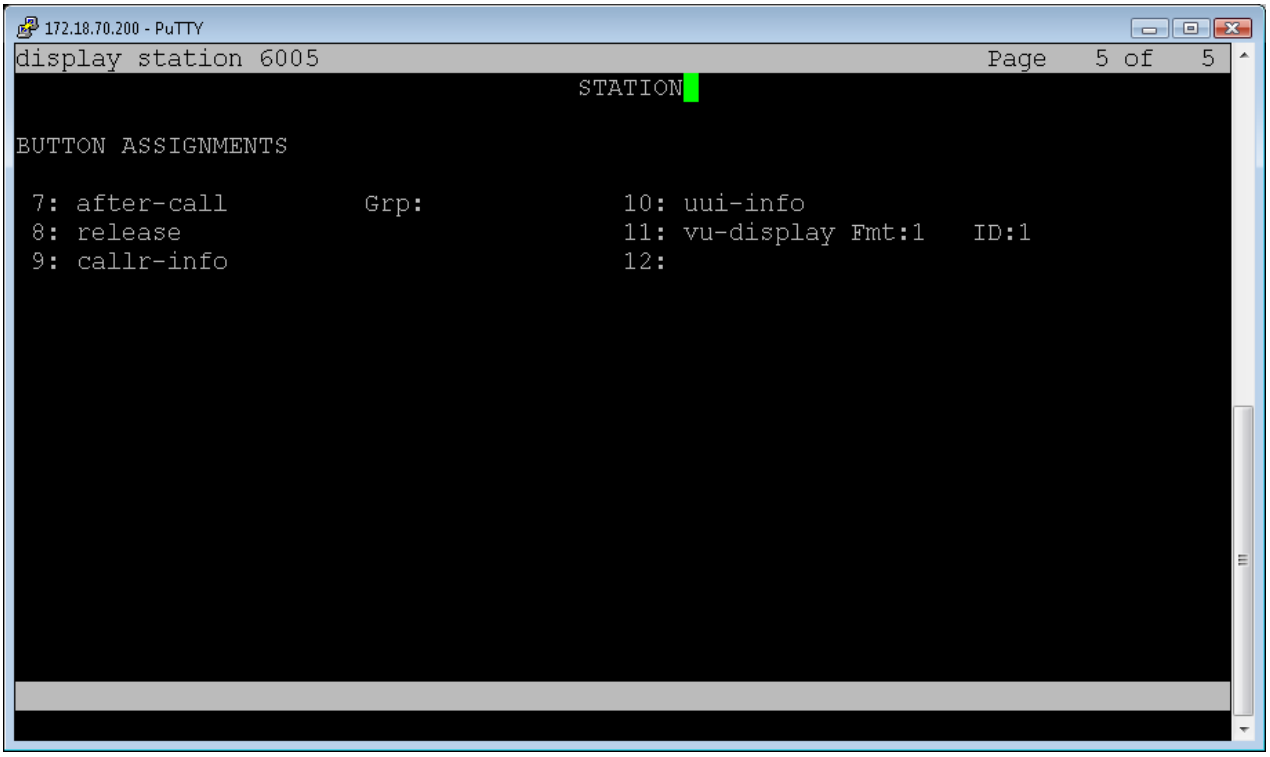
For this example, ensure that the **IP Softphone** prompt is set to **Y** so that the agent can use the Agent Desktop softphone.


172.18.70.200 - PuTTY
display station 6005 Page 1 of 5
STATION
Extension: 6005 Lock Messages? n BCC: 0
Type: 9620 Security Code: 12345678 TN: 1
Port: S00197 Coverage Path 1: COR: 1
Name: Elite Agent 1 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: 6005
Speakerphone: 2-way Mute Button Enabled? y
Display Language: english
Survivable GK Node Name:
Survivable COR: internal Media Complex Ext:
Survivable Trunk Dest? y IP SoftPhone? y
IP Video Softphone? n
Customizable Labels? y


172.18.70.200 - PuTTY
display station 6005 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: 6005 Always Use? n IP Audio Hairpinning? n

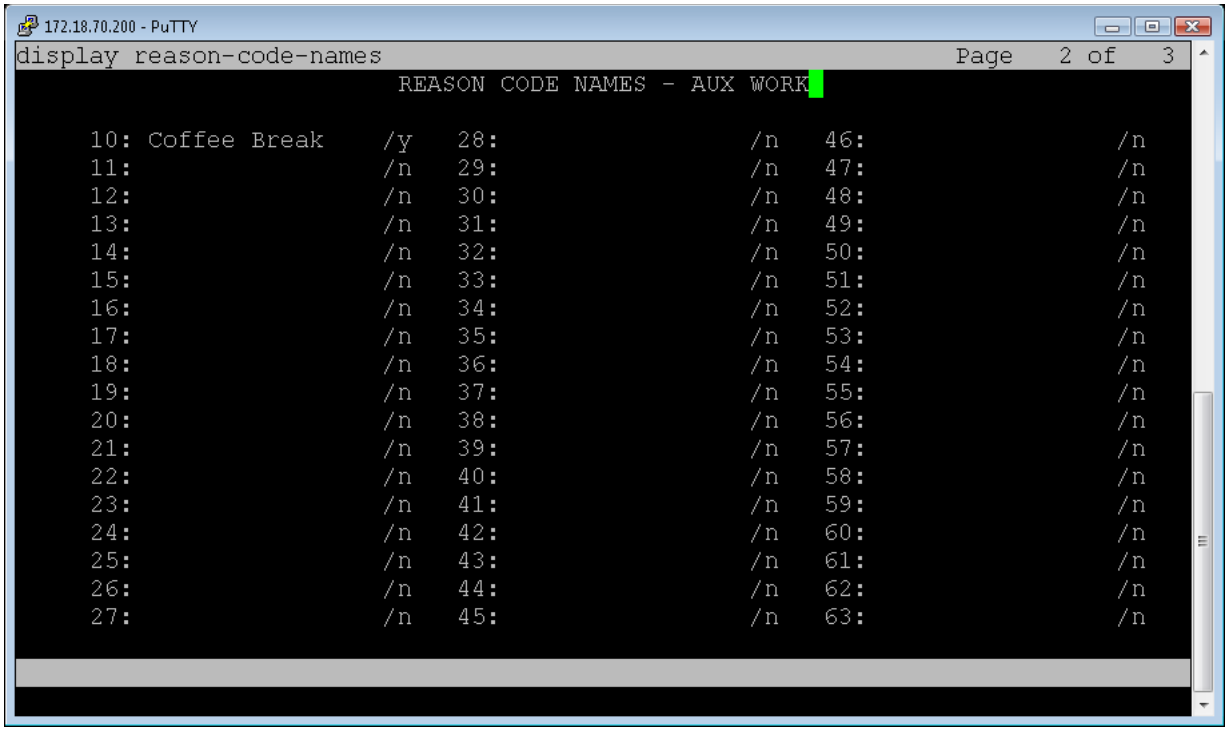

172.18.70.200 - PuTTY
display station 6005 Page 3 of 5
STATION
Conf/Trans on Primary Appearance? n
Bridged Appearance Origination Restriction? n
Call Appearance Display Format: disp-param-default
IP Phone Group ID:
ENHANCED CALL FORWARDING
Forwarded Destination Active
Unconditional For Internal Calls To: n
External Calls To: n
Busy For Internal Calls To: n
External Calls To: n
No Reply For Internal Calls To: n
External Calls To: n
SAC/CF Override: n


172.18.70.200 - PuTTY
display station 6005 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 4: aux-work RC: Grp:
2: call-appr 5: auto-in Grp:
3: call-appr 6: manual-in Grp:
voice-mail Number:



6 From the station record the button assignments, which you must match in the Contact Center agent profile: in this example the relevant buttons are **aux-work**, **auto-in**, **manual-in**, **after-call**, **release**.

7 Record the reason codes normally used by the agents who are to use Agent Desktop. You can associate these codes with Contact Center activity codes in the Contact Center default agent template.



8 Verify that the agent and station are fully operational in the Elite environment by logging on the agent, placing a test call center voice call to their station, and checking the operation of reason codes.

--End--

Configuring the default template with Reason Codes

Create reason codes mappings on the default template, to make them available to the agent on Agent Desktop. This allows the agent to enter reason codes for both Contact Center and Call Center Elite by making a single menu selection on Agent Desktop.

Procedure steps

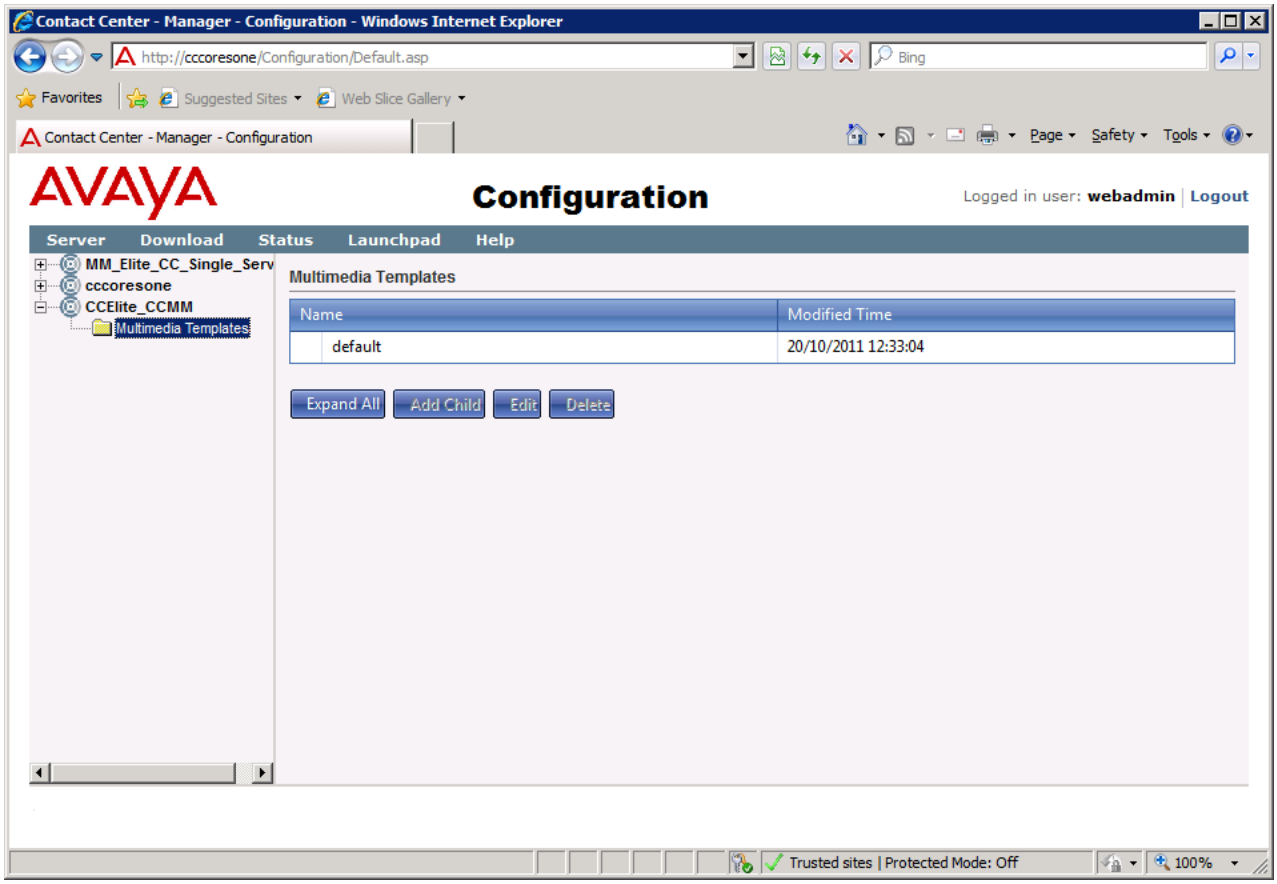
Step	Action
1	On the Contact Center server, start Internet Explorer.
2	In the **Address** box, type the CCMA URL in the format http://<Server name>, for example **http://CCCORESONE**.
3	Press **Enter**.
4	In the main logon window, in the **User ID** box, type **webadmin**.

5 In the **Password** box, type the password, for example **nimdabew**.

6 On the **Launchpad**, select **Configuration**.

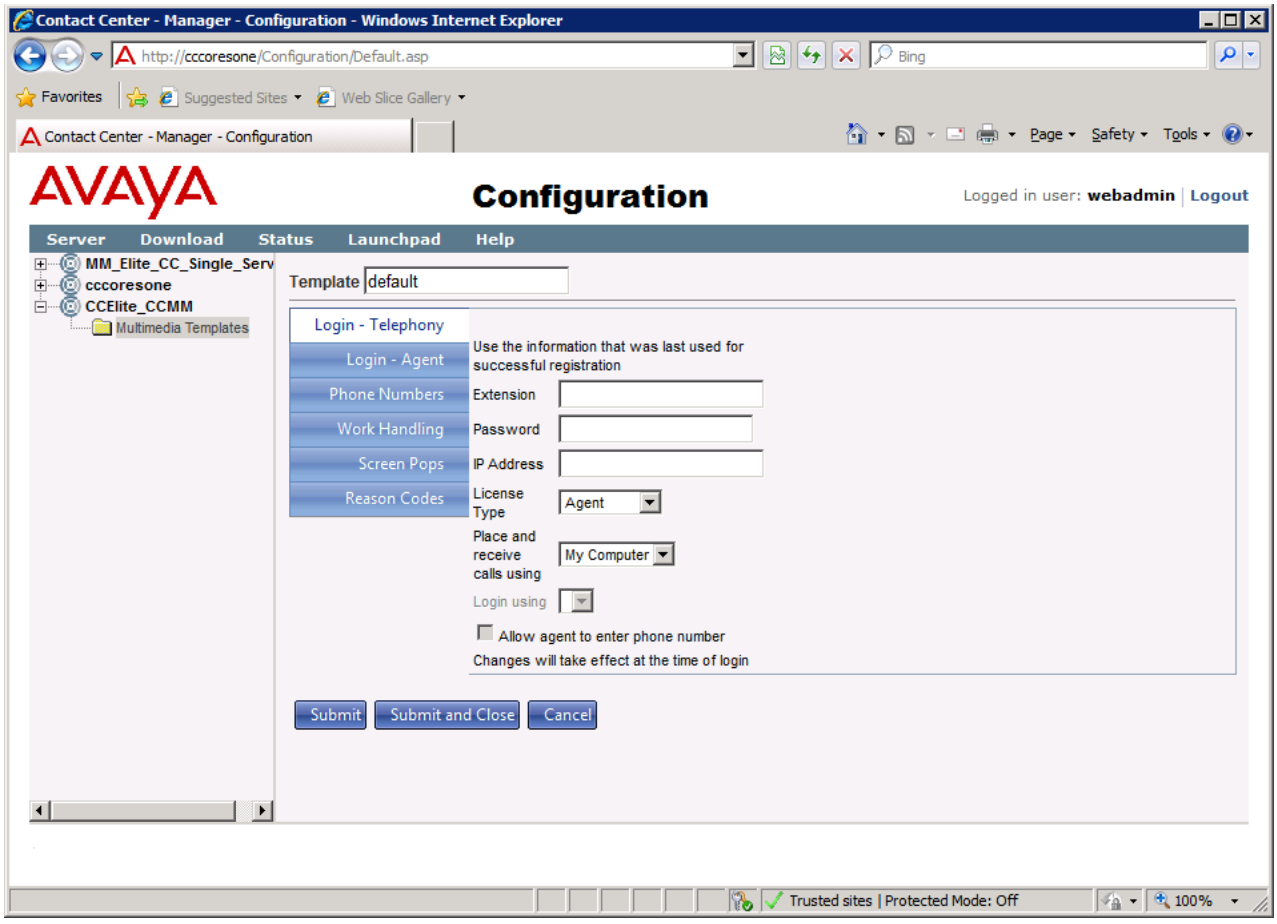
7 From the **Server** menu, expand the CCMM server, for example **CCElite_CCMM**.

8 In the left pane, select **Multimedia Templates**.

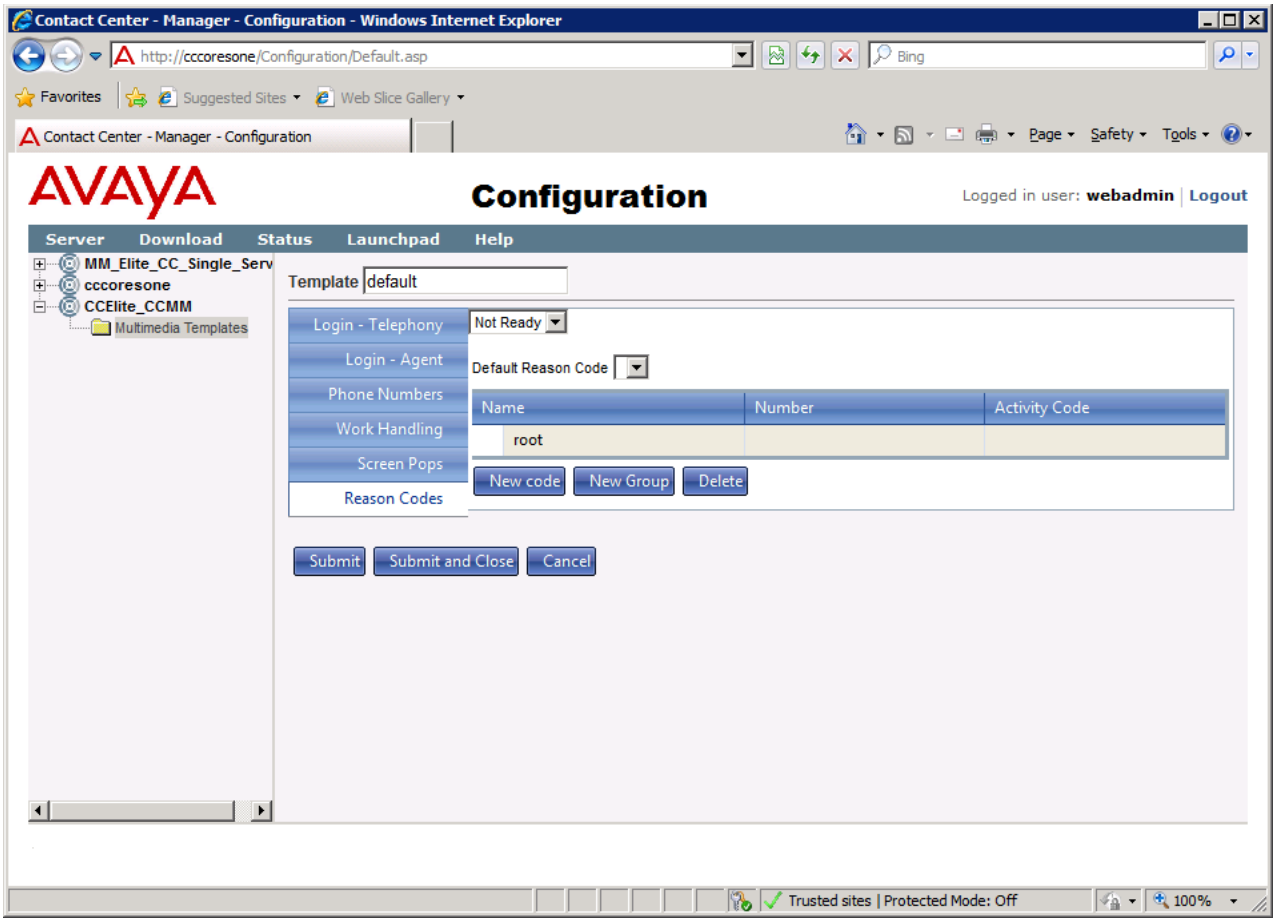


9 In the right pane, select the default template.

10 Click **Edit**.



11 Click **Reason Codes**.



12 Click **New code**.

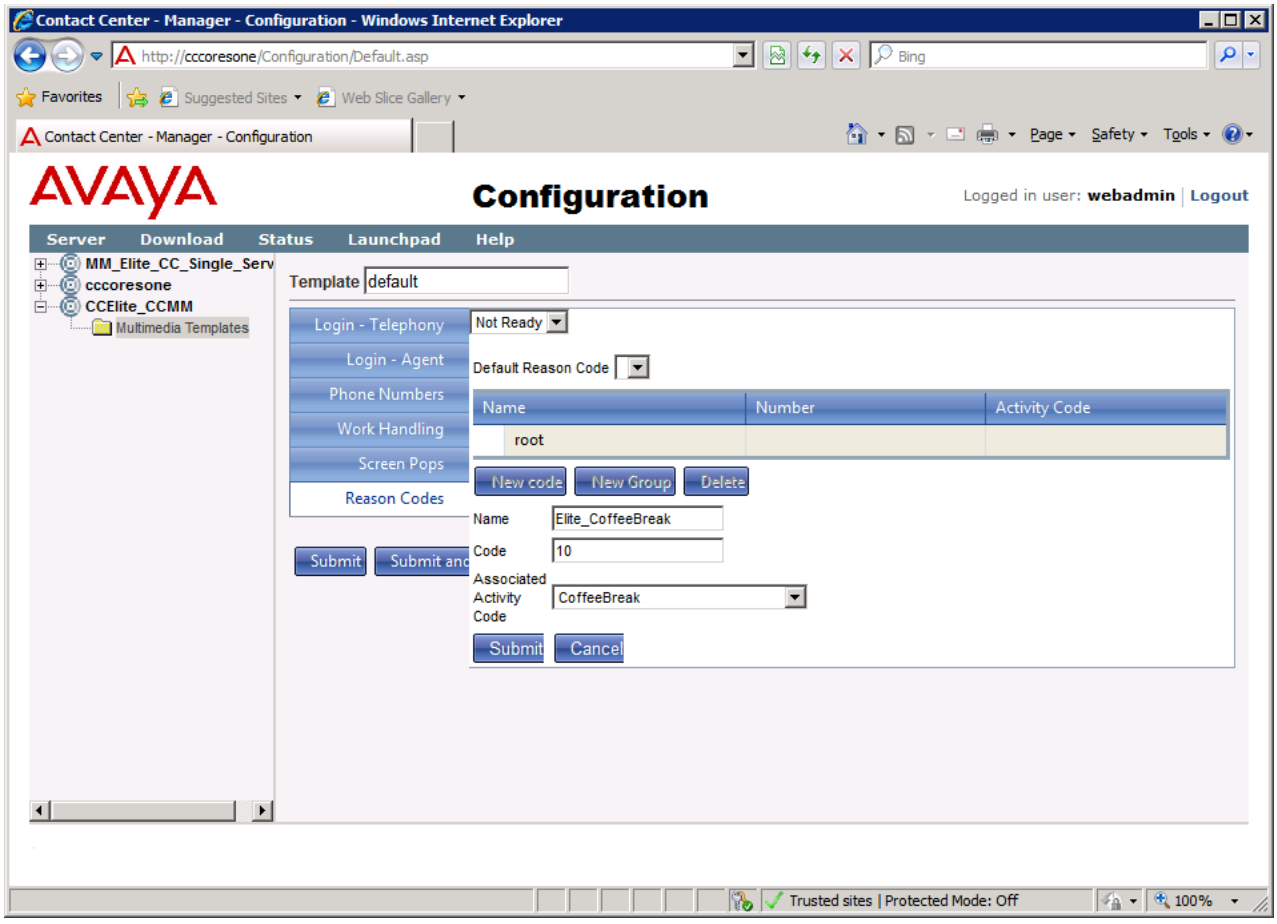
13 In the **Name** box, type a name for the Elite reason code as you want it to appear on Agent Desktop, for example **Elite_CoffeeBreak**.

14 In the **Code** box, type the Elite Aux Work code that you are mapping to a Contact Center reason code, for example **10**.

15 From the **Associated Activity Code** list, select the Contact Center reason code that you are associating with the Elite reason code, for example **CoffeeBreak**.

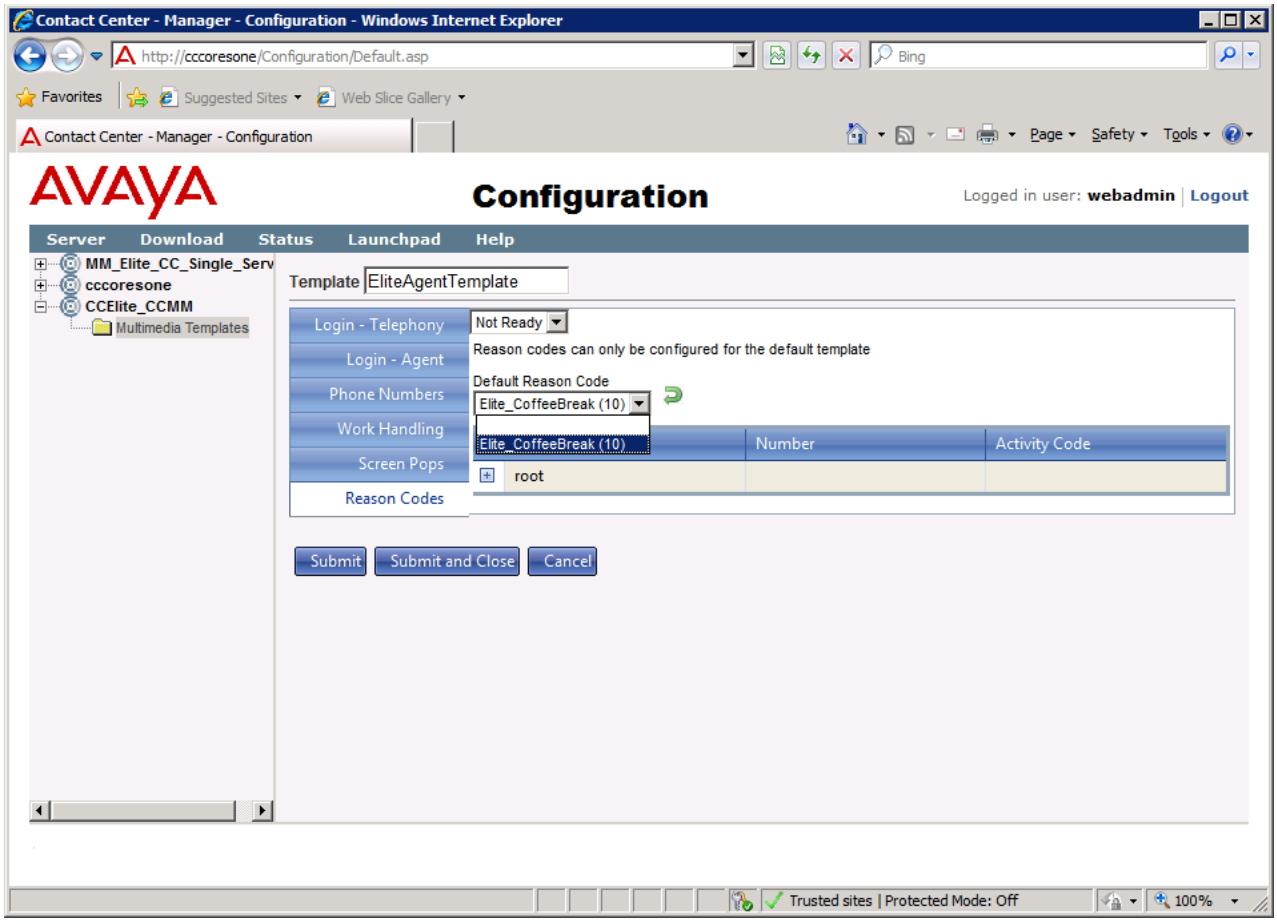
16 Click **Submit**.

When an agent wants to select a reason code for both Contact Center and Call Center Elite they can select this Reason code mapping, and each system receives the appropriate reason code and Aux Work code respectively.



17 Repeat step 12 to step 16 for each Call Center Elite Aux Work reason code and matching Contact Center activity code you want to map.

18 From the **Default Reason Code** list, select a default code, for example **Elite_CoffeeBreak**.



19 Click **Submit and Close**.

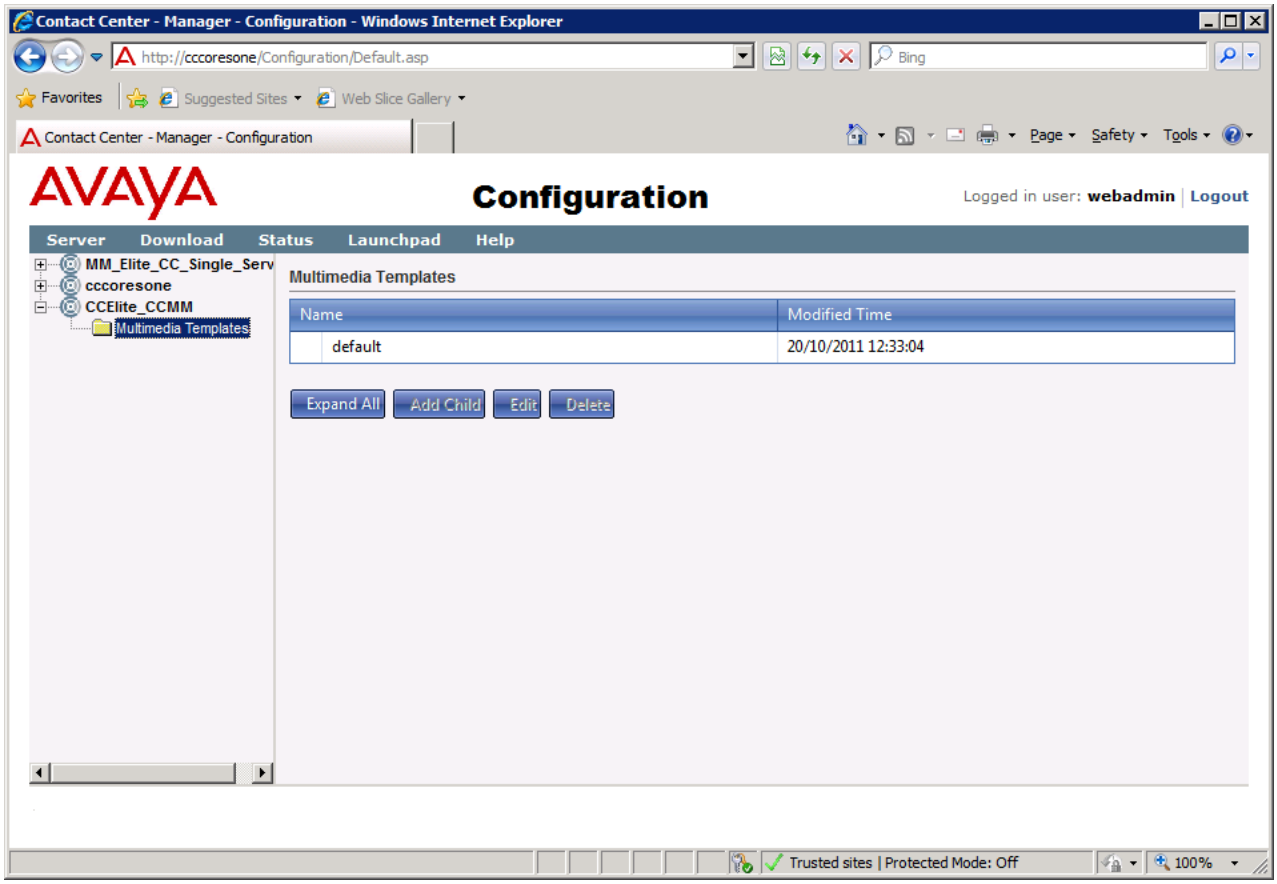
--End--

Adding an agent template

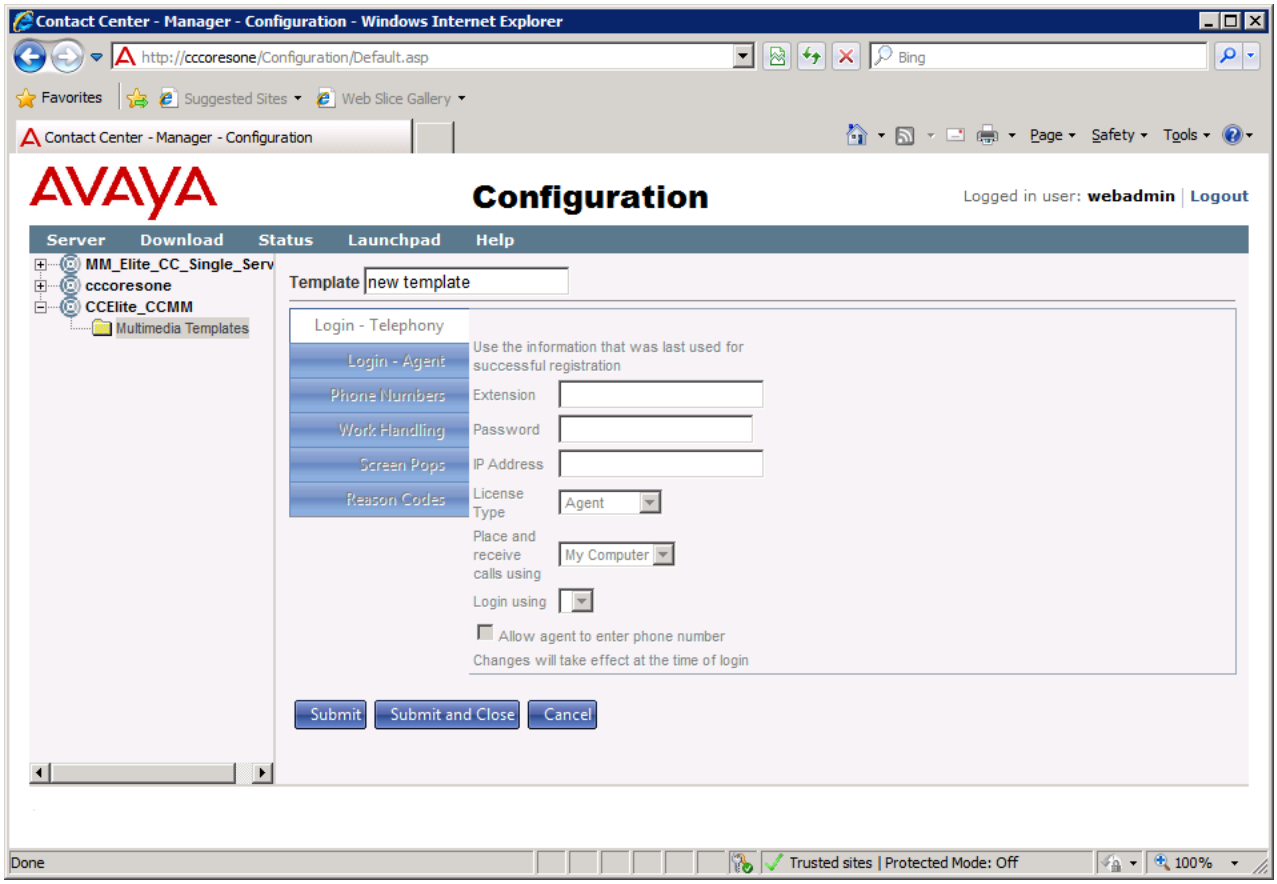
Add an agent template to allow Agent Desktop to implement the correct Call Center Elite agent and station settings when an Elite agent logs on.

Procedure steps

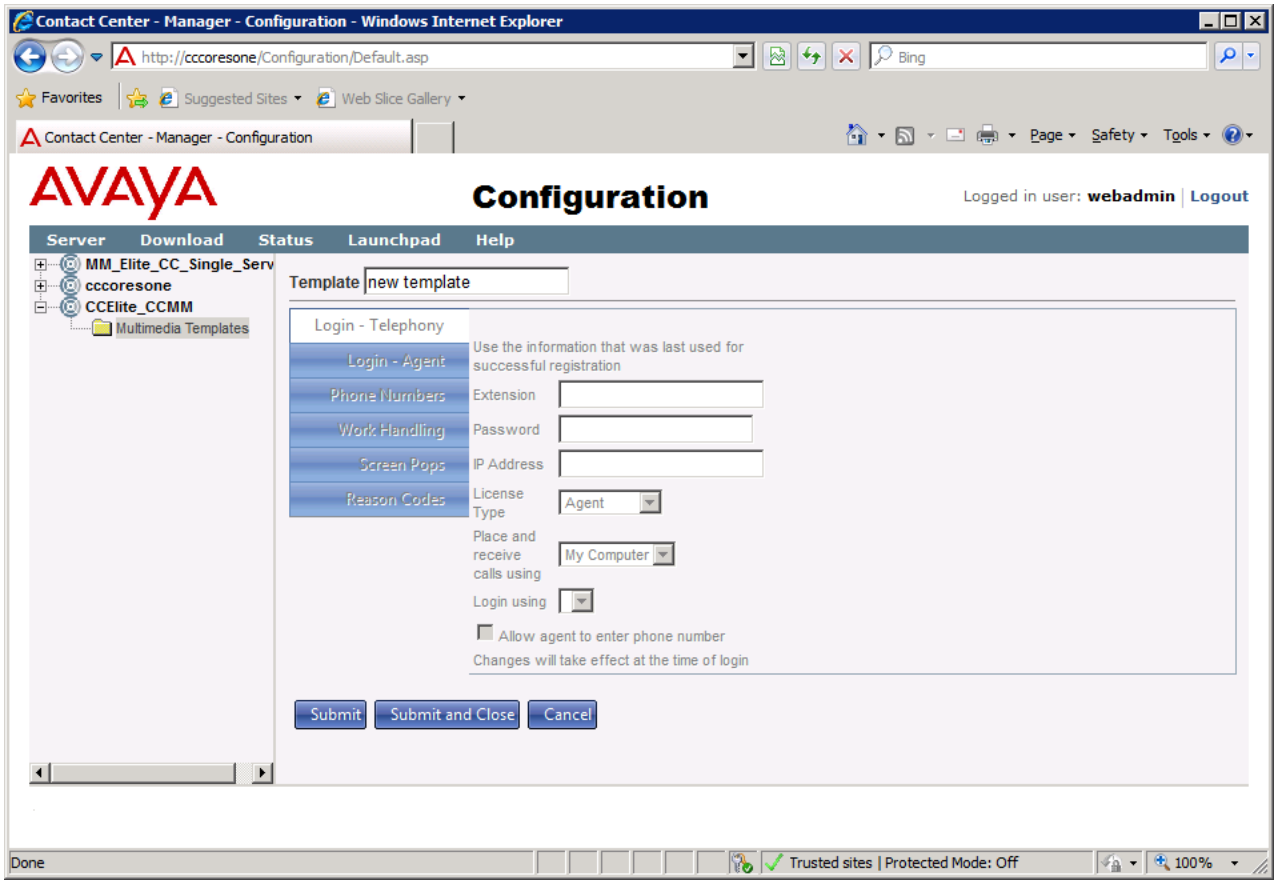
Step	Action
1	From the **Server** menu, expand the CCMM server, for example **CCElite_CCMM**.
2	In the left pane, select **Multimedia Templates**.
3	In the right pane, select the default template.



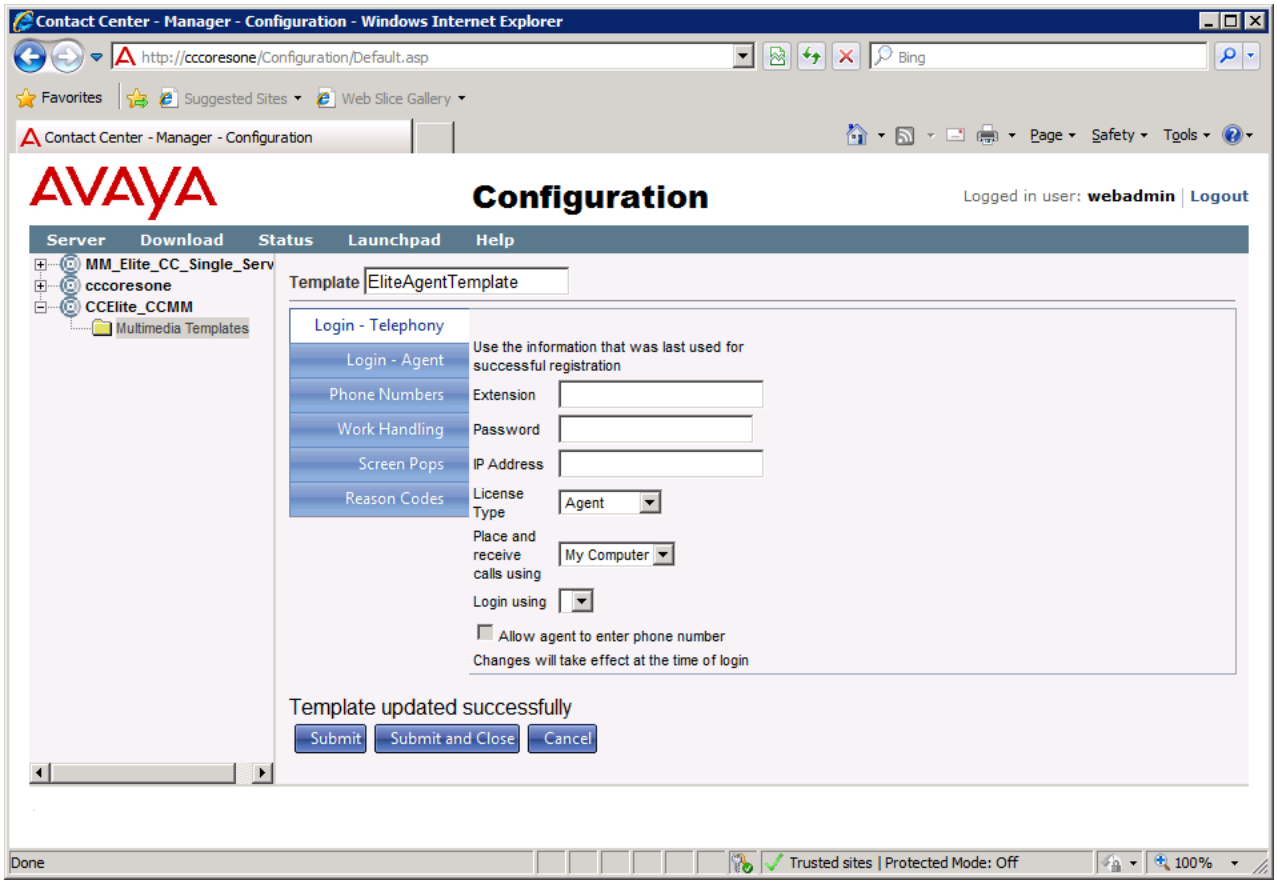
4 Click the **Add Child** button.



5 In the **Template** box, type a descriptive name for the new template, for example **EliteAgentTemplate**.



6 Click **Submit** to enable the default properties and unlock the template settings.

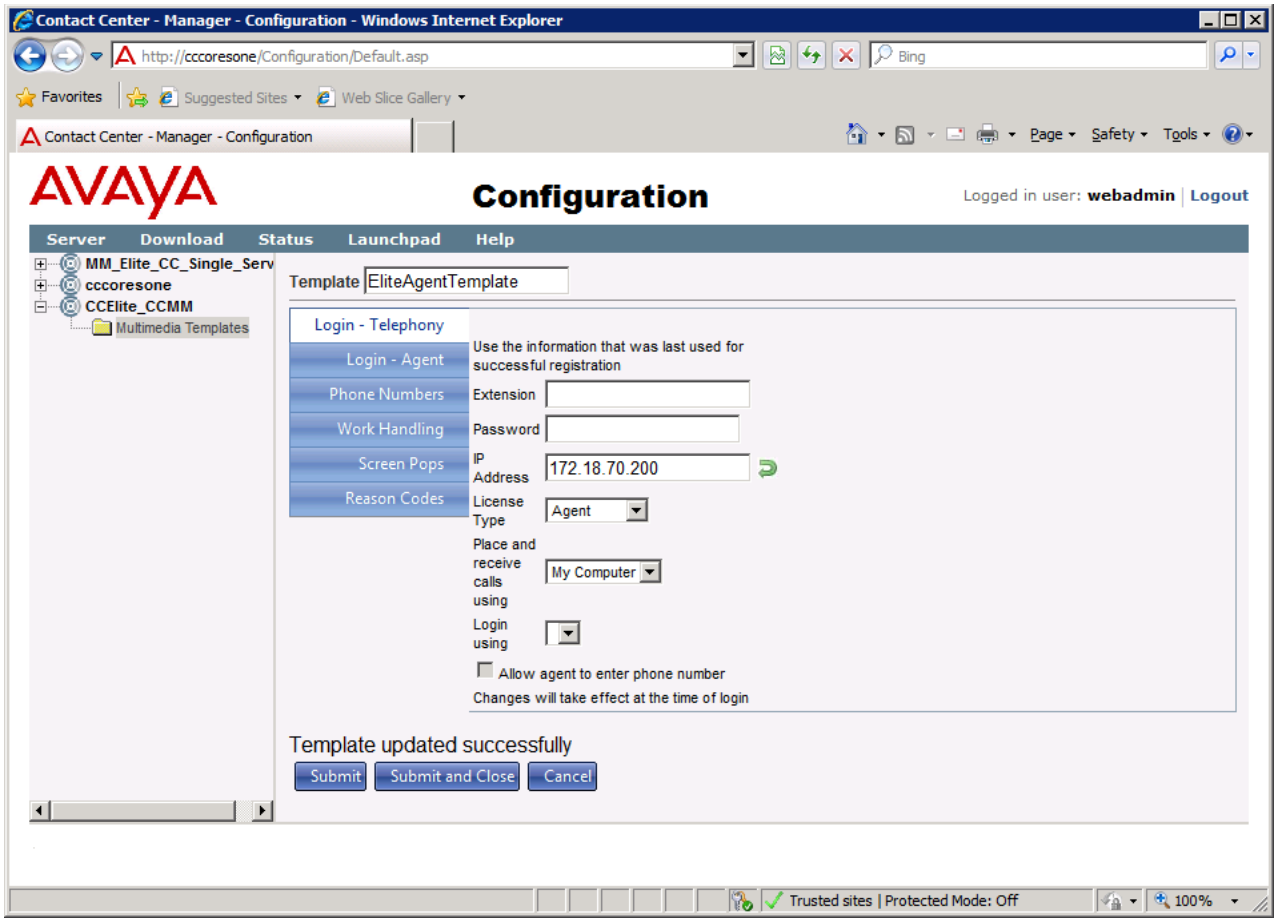


7 In the **IP Address** box, type the IP address of the Communication Manager on which Call Center Elite is installed, for example **172.18.70.200**.

8 From the **License Type** list, select the license type for this template, for example **Agent**.

9 From the **IP Address** list, select **My Computer**. This means that agents using this template by default use the softphone on Agent Desktop to receive calls from Elite.

10 Click **Submit**.

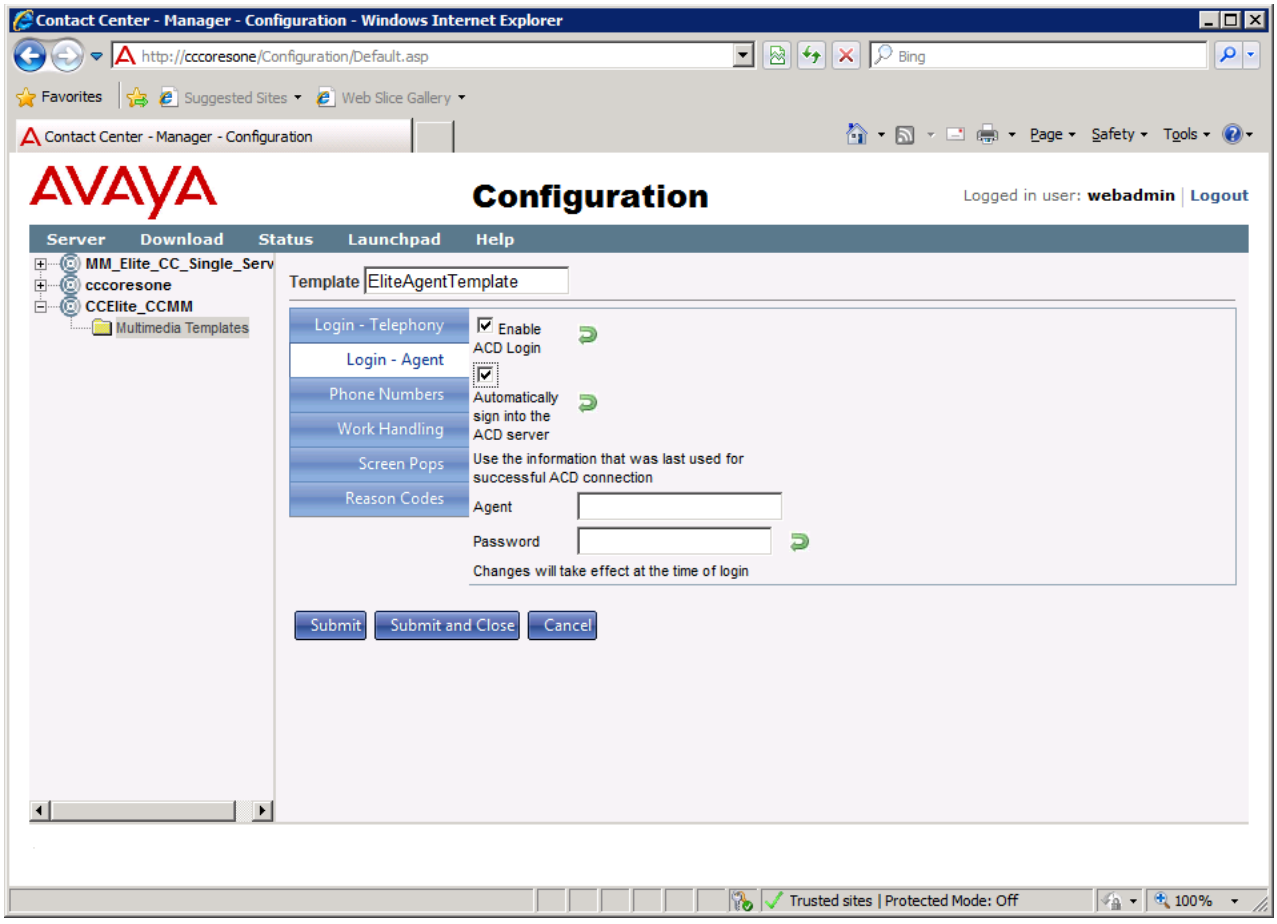


11 Click **Login - Agent**.

12 Select **Enable ACD Login**.

13 Select **Automatically sign into the ACD server**.

14 Click **Submit**.



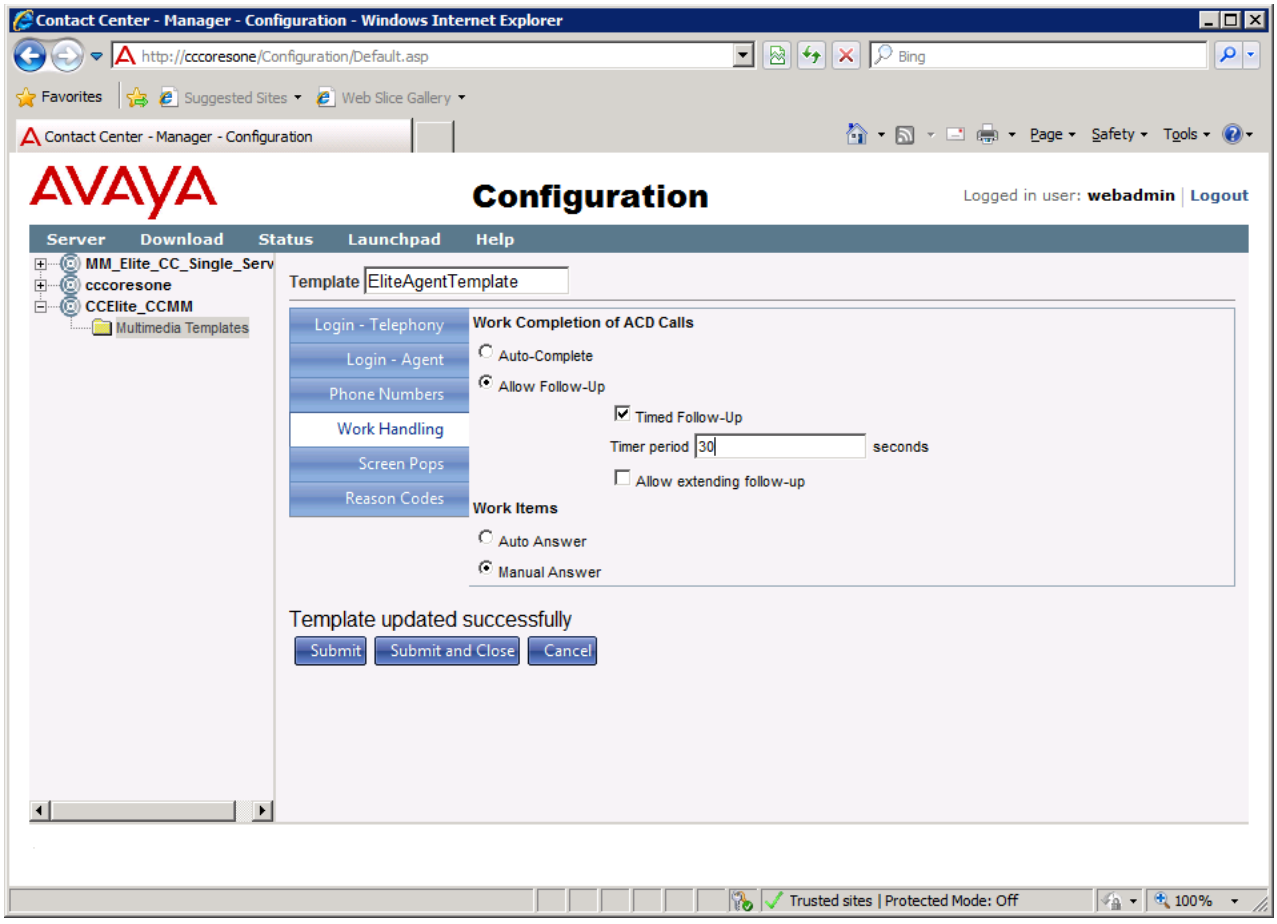
15 Click **Work Handling**.

16 Select **Allow Follow-up**. This allows an agent time to complete follow up actions after a caller has disconnected. (Setting this makes the Elite voice call handling consistent with the example Contact Center Call Presentation Class.

17 Select **Timed Follow up**.

18 In the **Timer Period** box, type the number of seconds to allow the agent complete follow up activities, for example 30 seconds to match the example Contact Center Call Presentation Class.

19 Click **Submit**.



20 Click **Submit and Close**.

--End--

Supervisor and Agent Configuration

Add a supervisor so that you can add agents to Contact Center. When you open Contact Center Management from the CCMA launchpad, the Contact Center Management window opens in Supervisors view. You can use this view to:

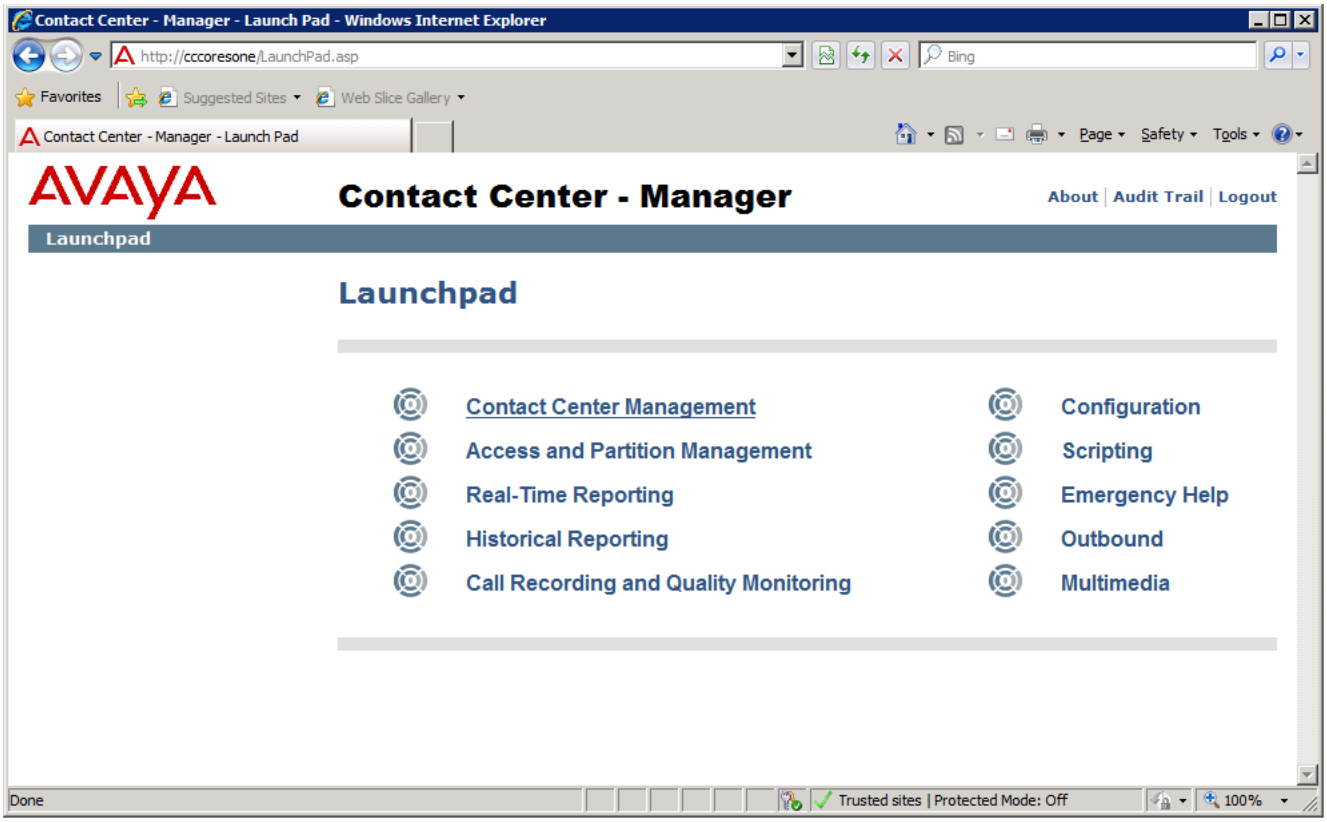
- quickly view the configured supervisors on each server in the system tree
- list the agents assigned to each supervisor
- immediately assign agents to supervisors (ad hoc assignments)
- quickly add many new supervisors by importing a comma-separated values (CSV) file

Adding a supervisor

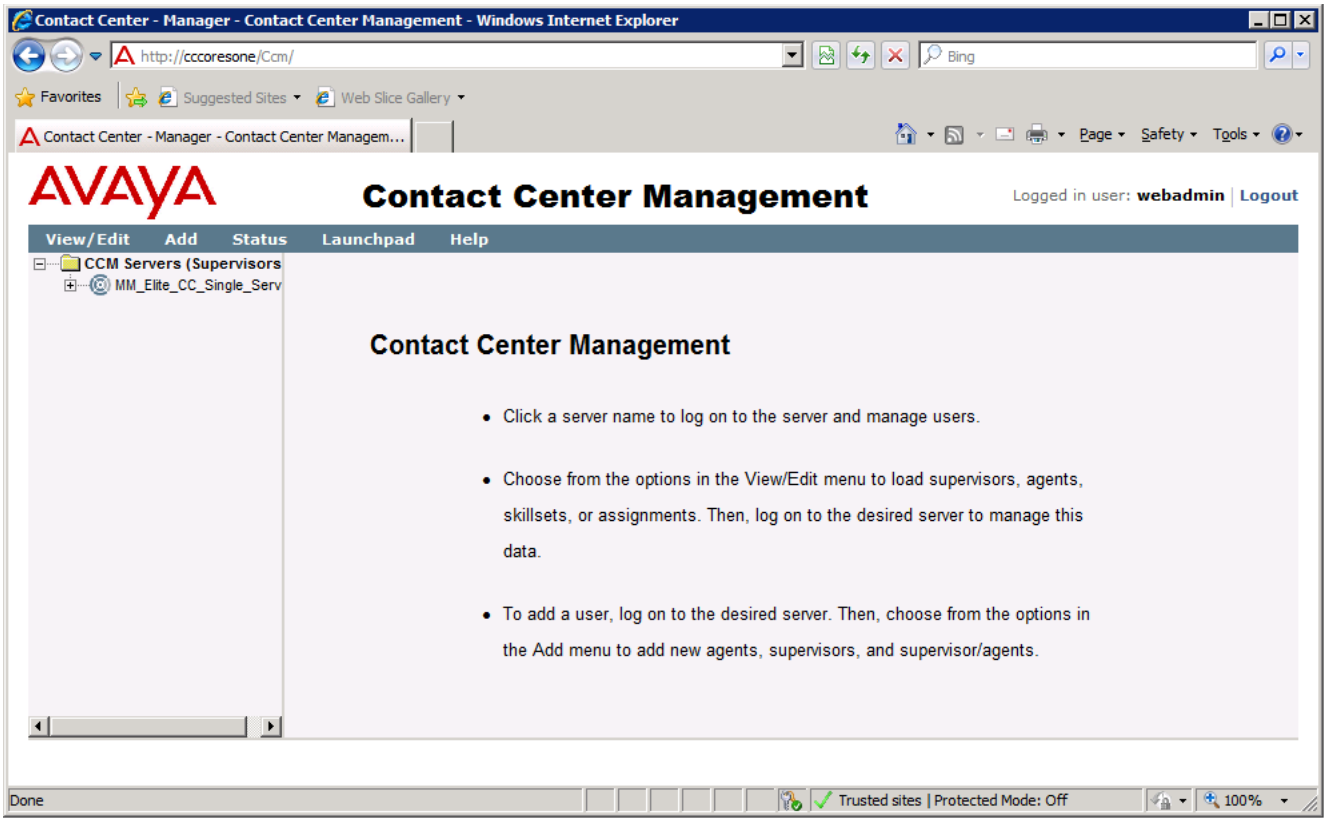
Complete this procedure to add a supervisor in Contact Center Management.

Procedure steps

Step	Action
1	On the Contact Center server, start Internet Explorer.
2	In the **Address** box, type the CCMA URL in the format http://<Server name>, for example **http://CCCORESONE**.
3	Press **Enter**.
4	In the main logon window, in the **User ID** box, type **webadmin**.
5	In the **Password** box, type the password, for example **nimdabew**.

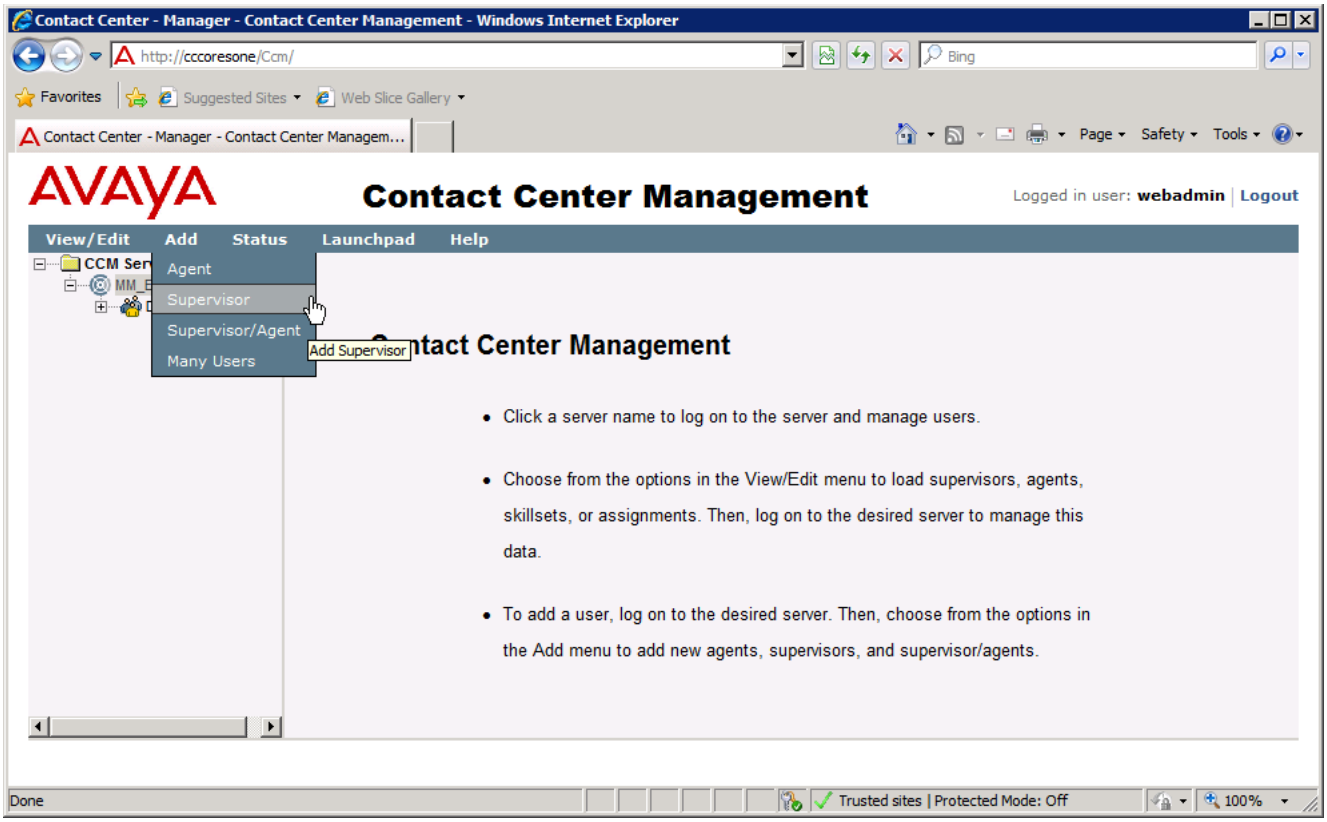


6 On the Launchpad, select **Contact Center Management**.



7 In the left pane, select the Contact Center Manager Server to which you want to add the supervisor, for example **MM_Elite_CC_Single_Server**.

8 From the **Add** menu, select **Supervisor**.



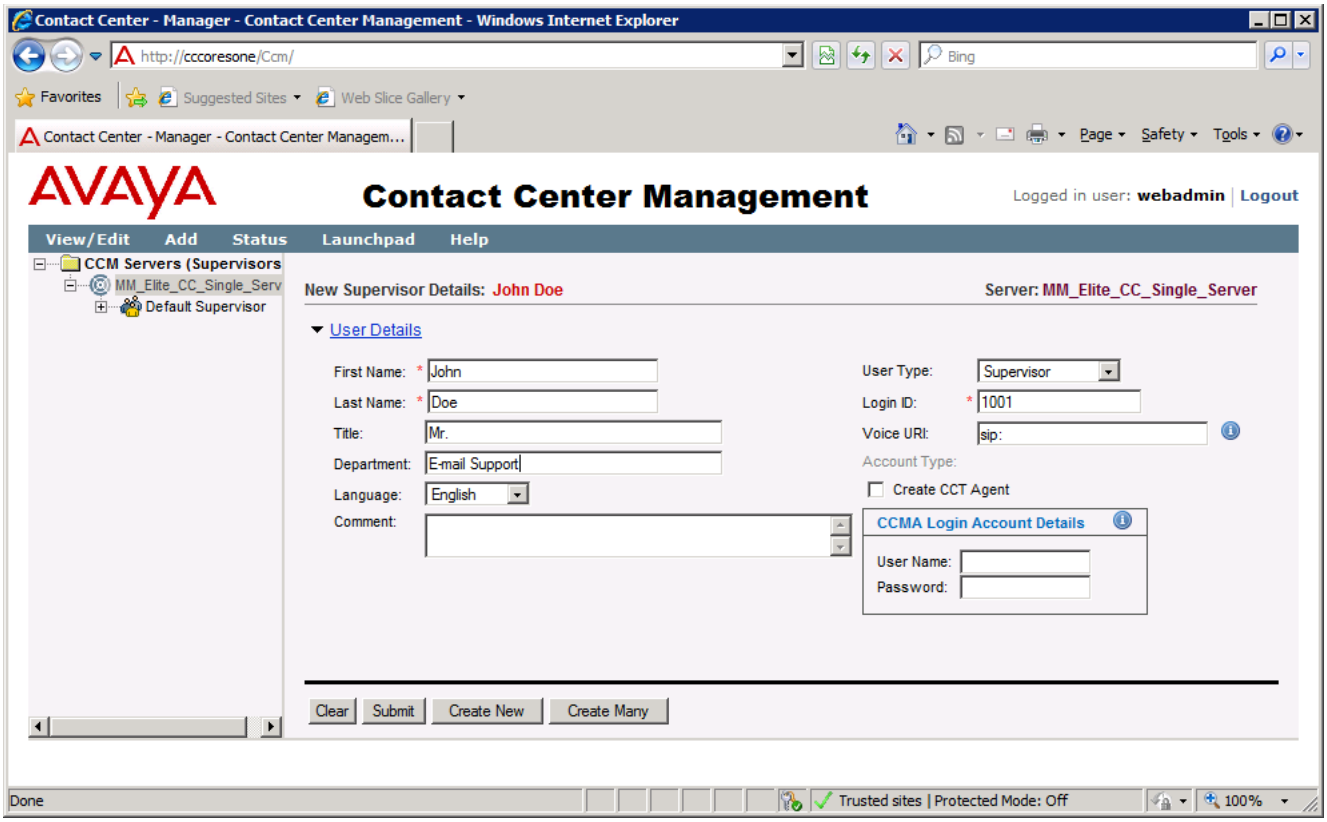
9 In the right pane, in the **First Name** box, type the supervisor's first name, for example **John**.

10 In the **Last Name** box, type the supervisor's last name, for example **Doe**.

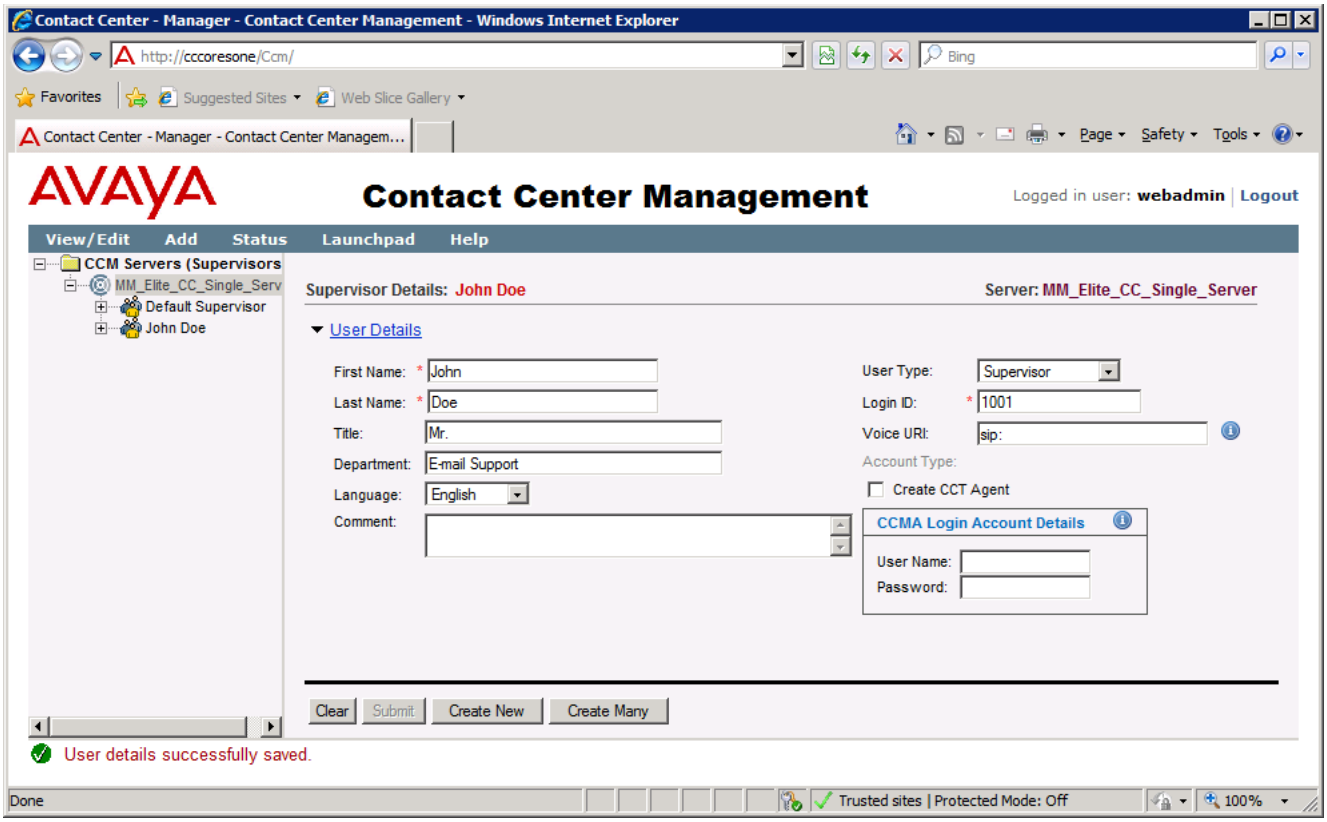
11 In the **Title** box, type the supervisor's title, for example **Mr.**.

12 In the **Department** box, type the supervisor's department, for example **E-mail Support**.

13 In the **Login ID** box, type a login ID for the supervisor, for example **1001**. For supervisors in a Multimedia Complement solution, this value is arbitrary, but it must be unique within this Contact Center. (Supervisors do not log on to stations or the Agent Desktop.)



14 Click **Submit** to save the new supervisor profile.



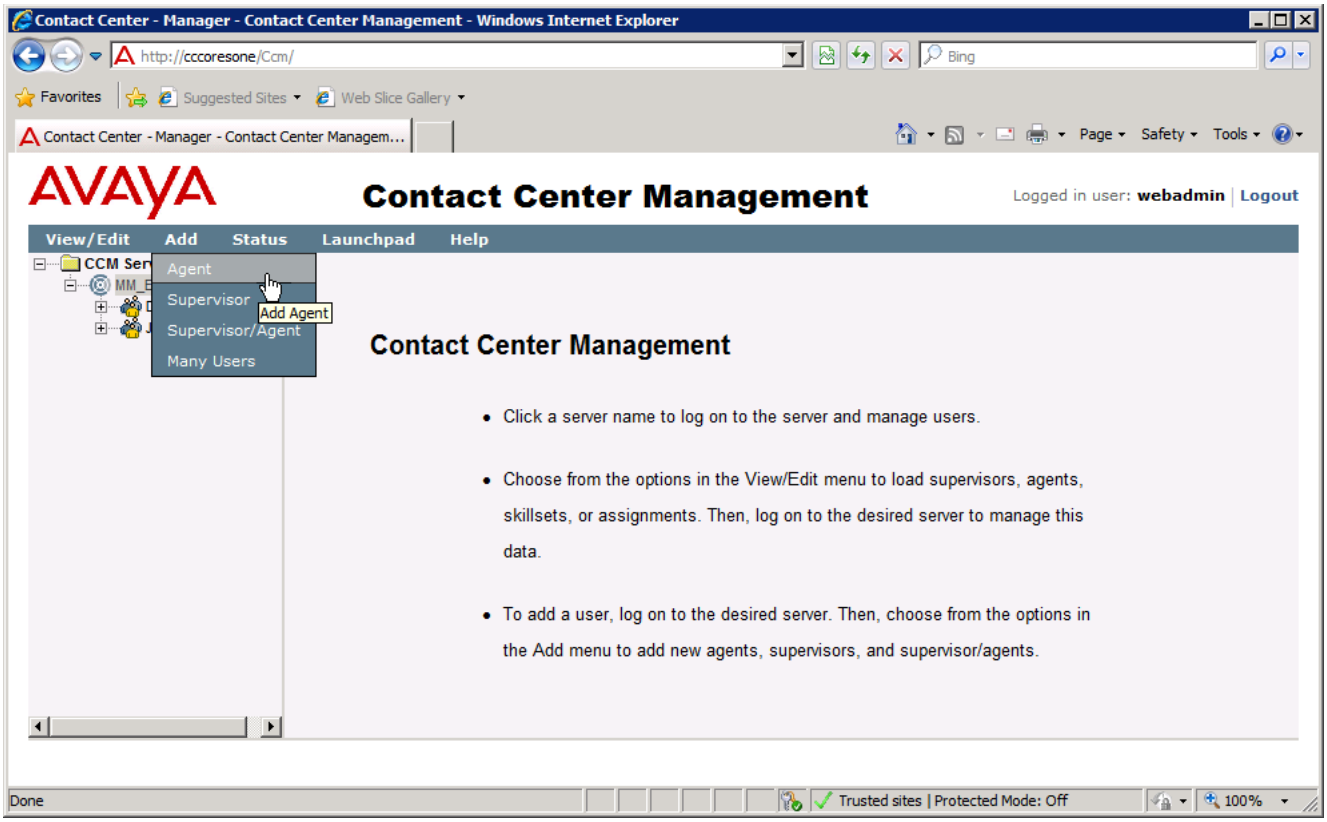
--End--

Adding an agent

Complete this procedure to add an agent in Contact Center Management.

Procedure steps

Step	Action
1	From the **Add** menu, select **Agent**.



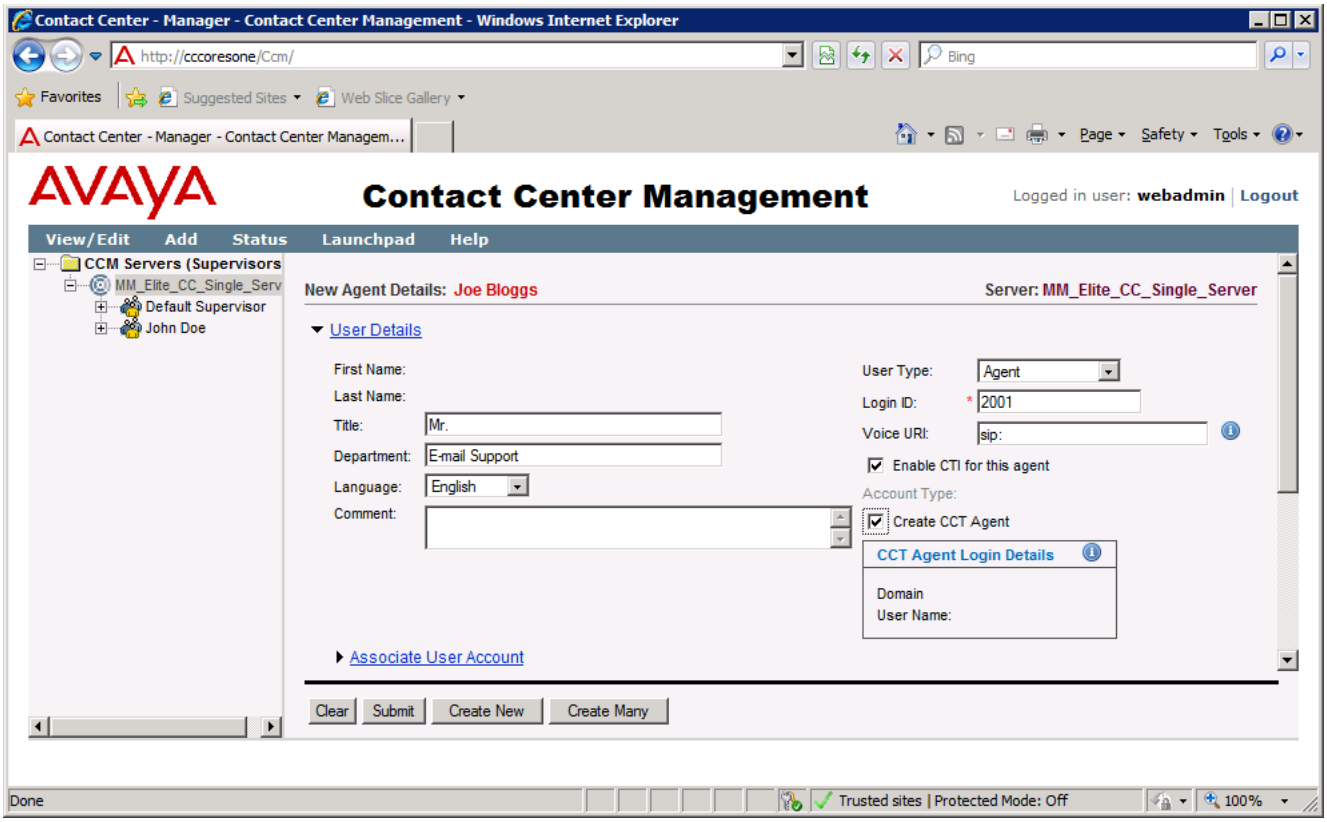
2 In the **Title** box, type the agent's title, for example **Mr.**.

3 In the **Department** box, type the agent's department, for example **E-mail Support**.

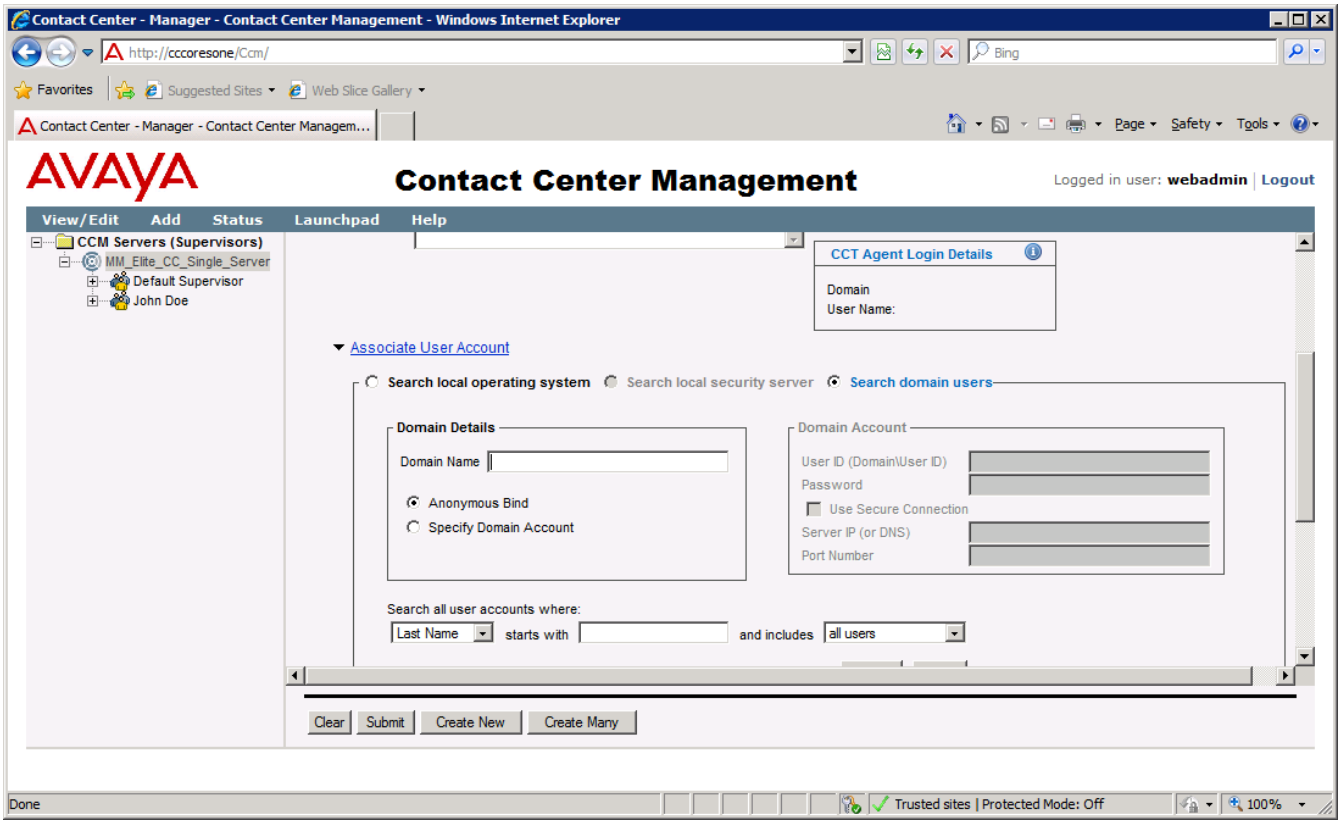
4 In the **Login ID** box, type a login ID for the agent, for example **2001**. For agents in a Multimedia Complement solution, this value is arbitrary, but it must be unique within this Contact Center.

5 Select **Enable CTI for this agent**.

6 Select **Create CCT Agent**.



7 Click **Associate User Account**.



8 Under **Associate User Account**, select **Search domain users**.

9 In the **Domain Name** box, type the domain for the agent's domain user account, for example **siptraffic.com**.

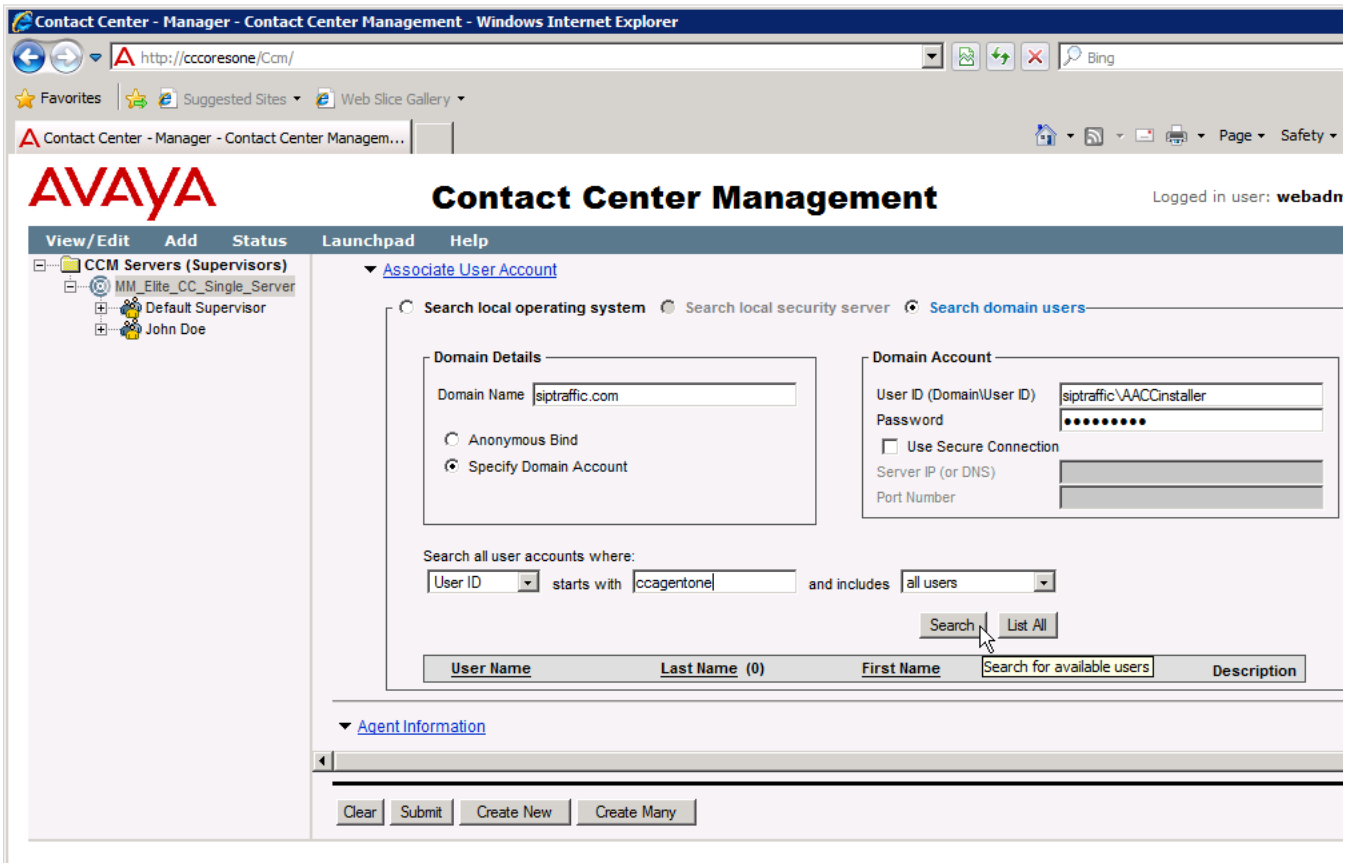
10 Select **Specify domain account**.

11 In the **User ID (Domain\User ID)** box, type the Avaya Aura® CC installer domain user account, in the form domain\user ID, for example **siptraffic\AACCInstaller**.

12 In the **Password** box, type the Avaya Aura® CC installer domain user password, for example **AACCpass1**.

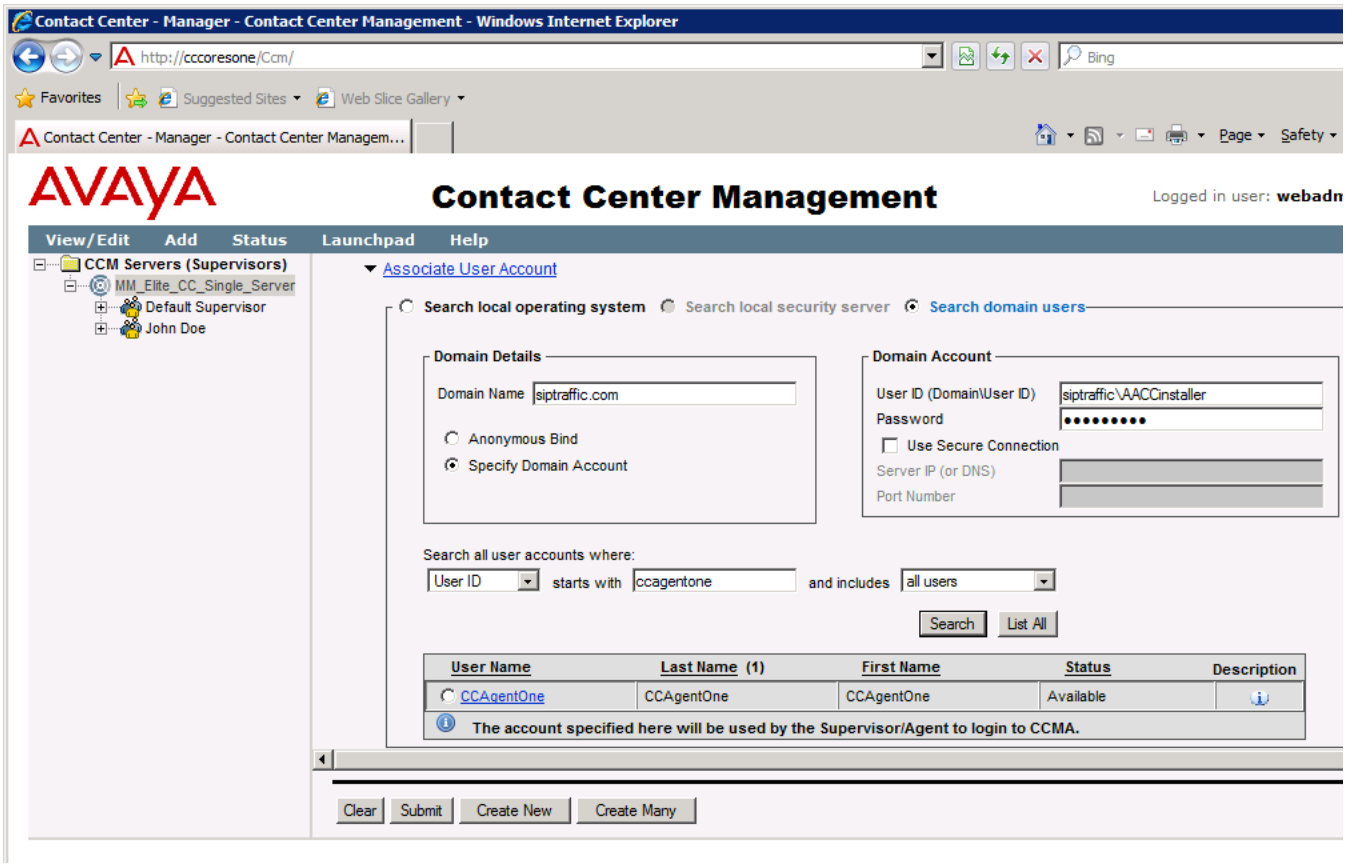
13 Under **Search all user accounts where**, from the list, select a criterion to search on, for example **User ID**.

14 In the **starts with** box, type the start or all of the domain user account criterion, for example **ccagentone**.

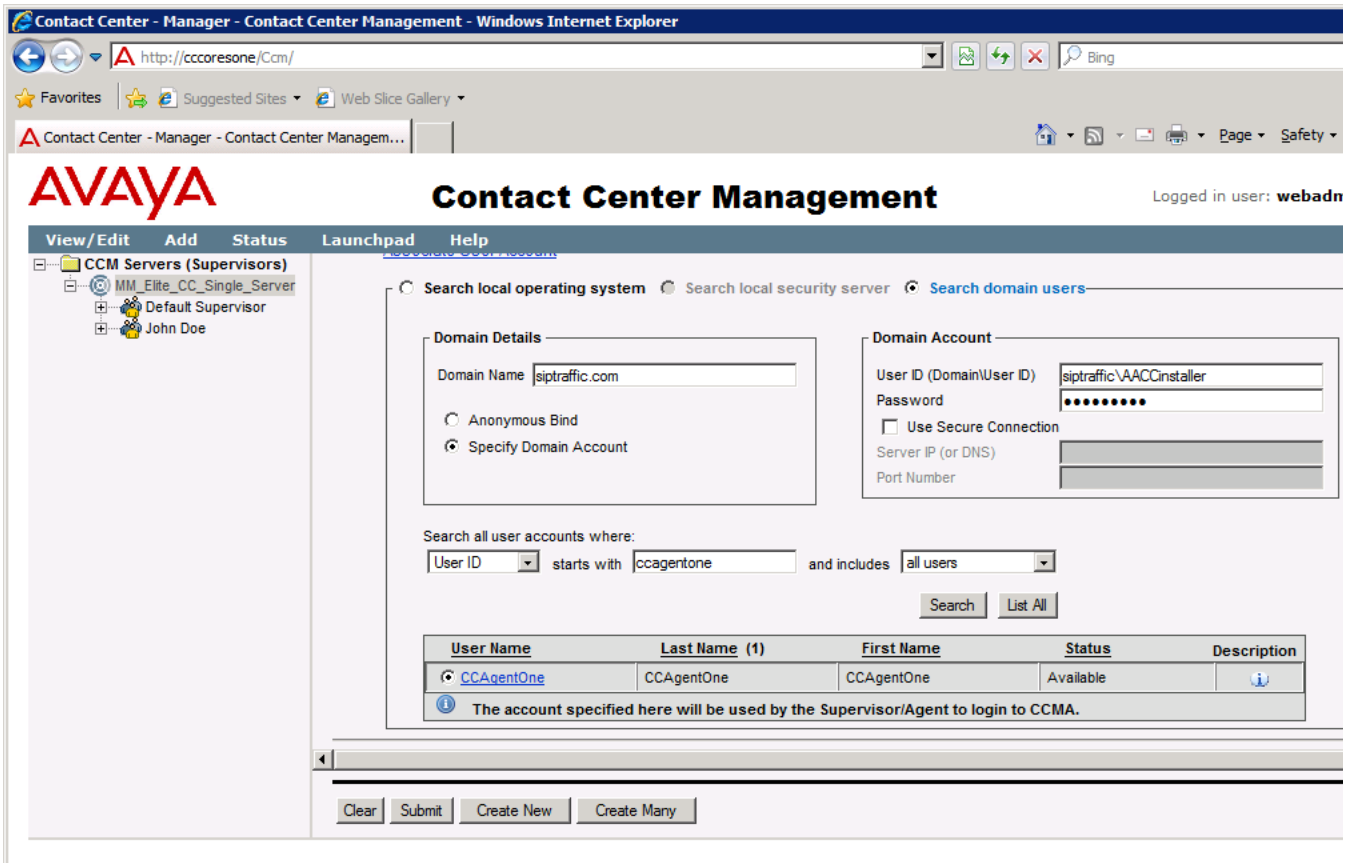


15 Click **Search**.

Contact Center retrieves the list of agents matching the search criteria from the domain.



16 Select the domain user for this agent, for example **CCAgentOne**.

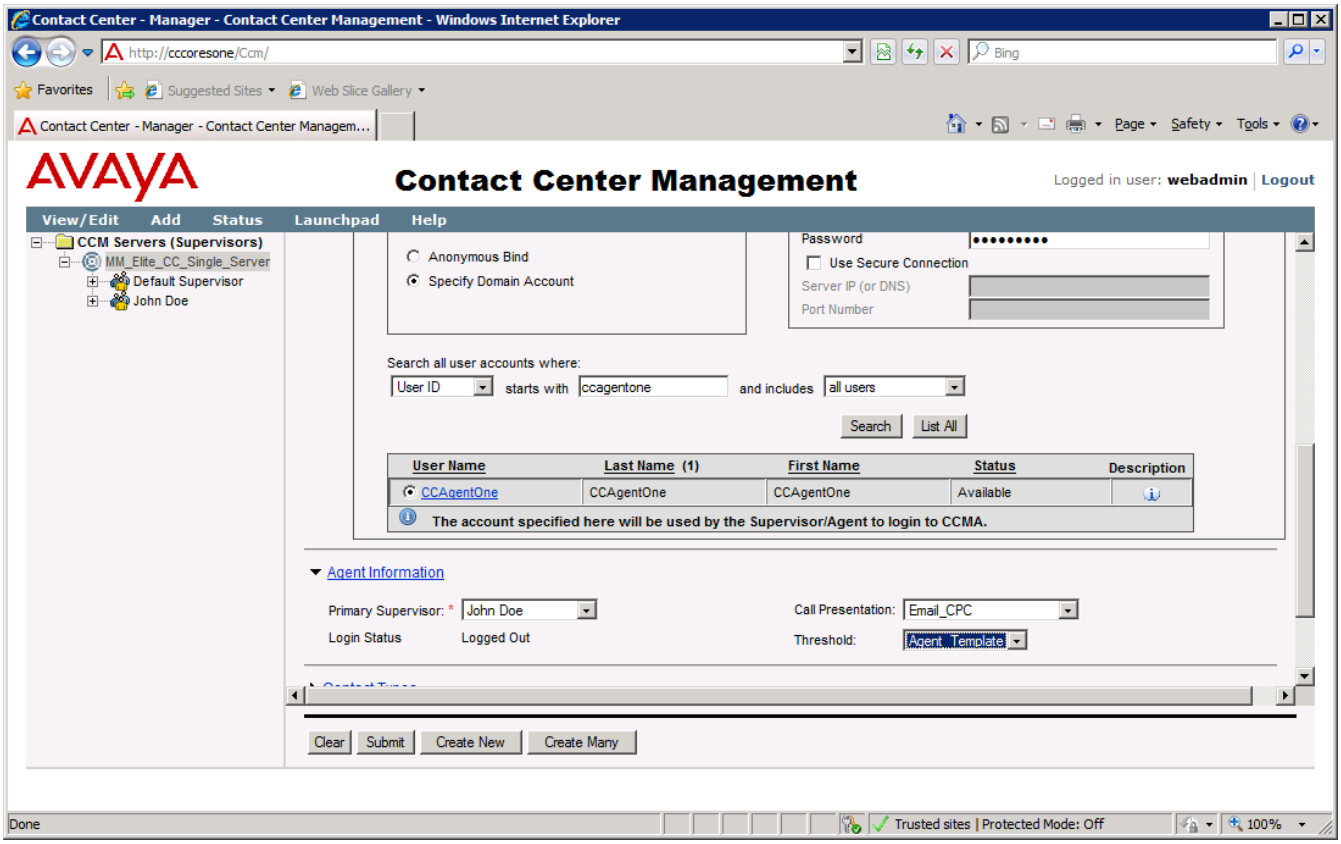


17 Click **Agent Information**.

18 From the **Primary Supervisor** list, select the supervisor for this agent, for example **John Doe**.

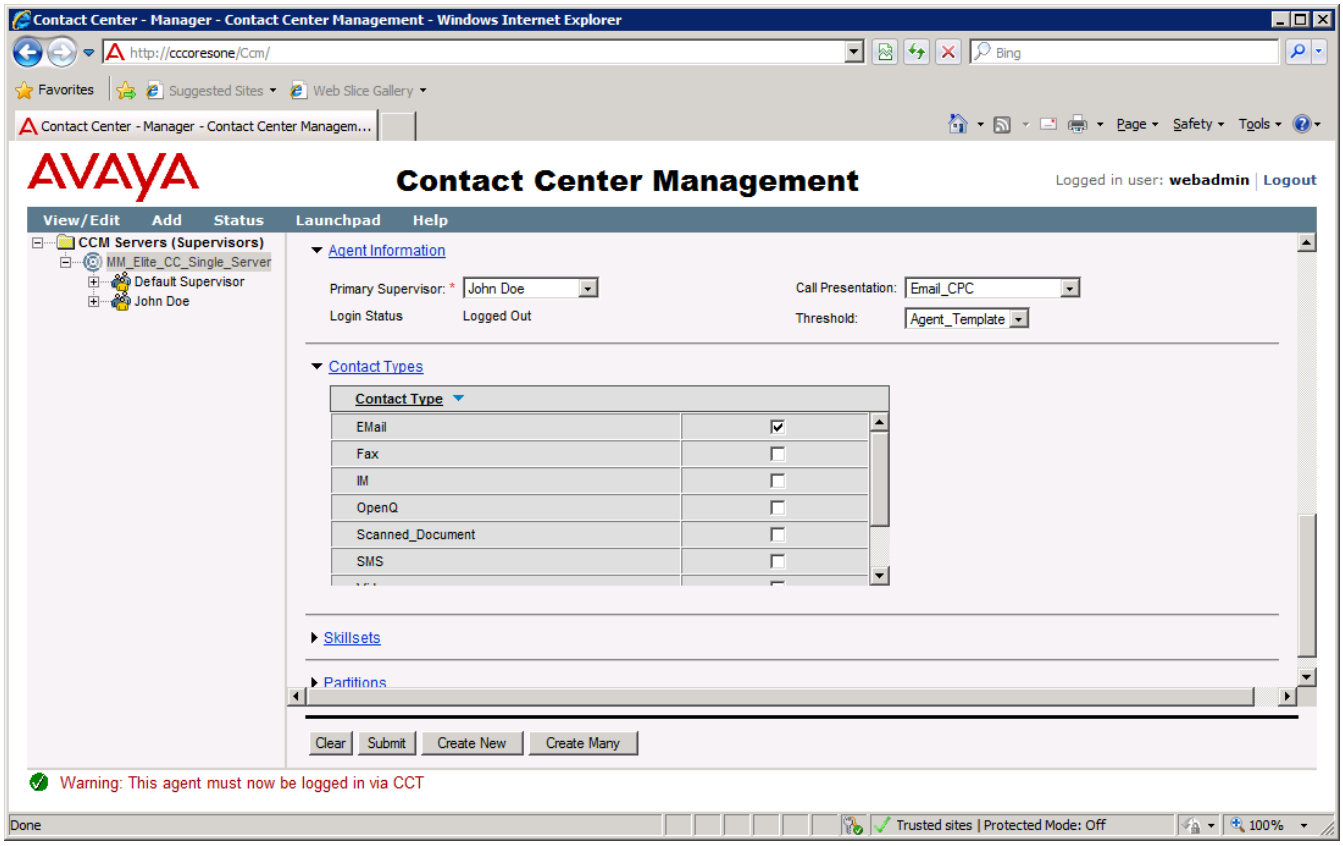
19 From the **Call Presentation Class** list, select a call presentation class for this user, for example **Email_CPC**.

20 Accept the default **Threshold**.



21 Click **Contact Types**.

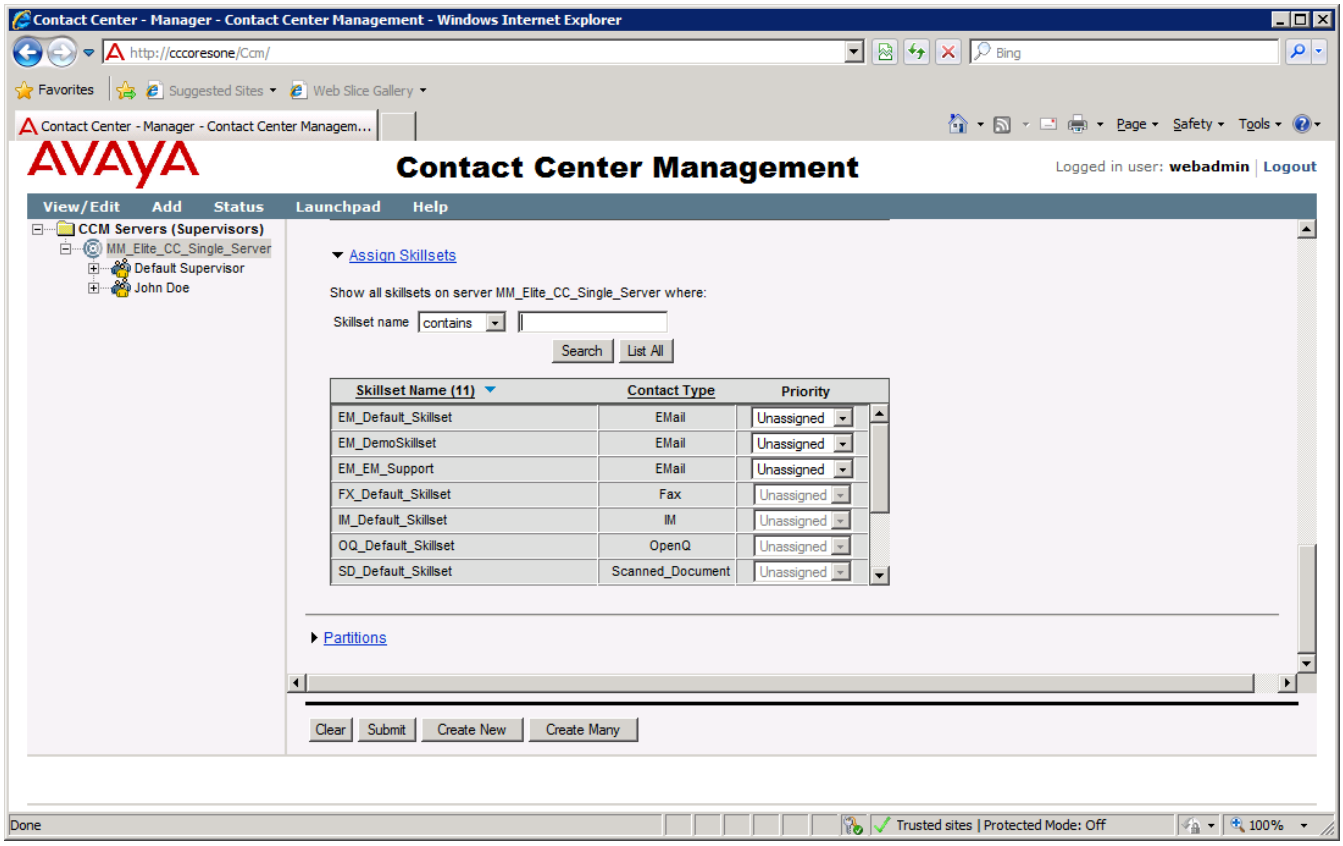
22 Select **EMail**.



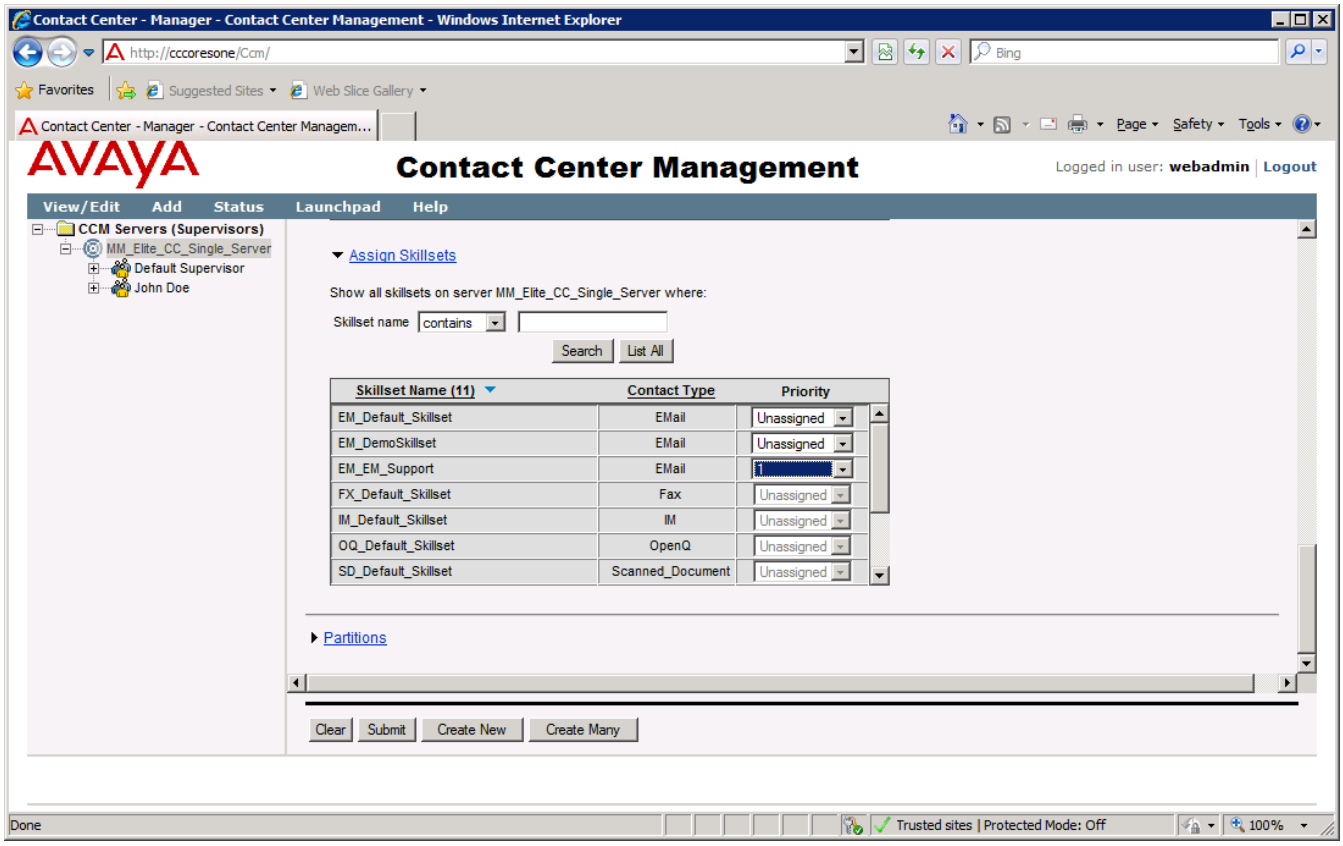
23 Click **Skillsets**.

24 Click **Assign Skillsets**.

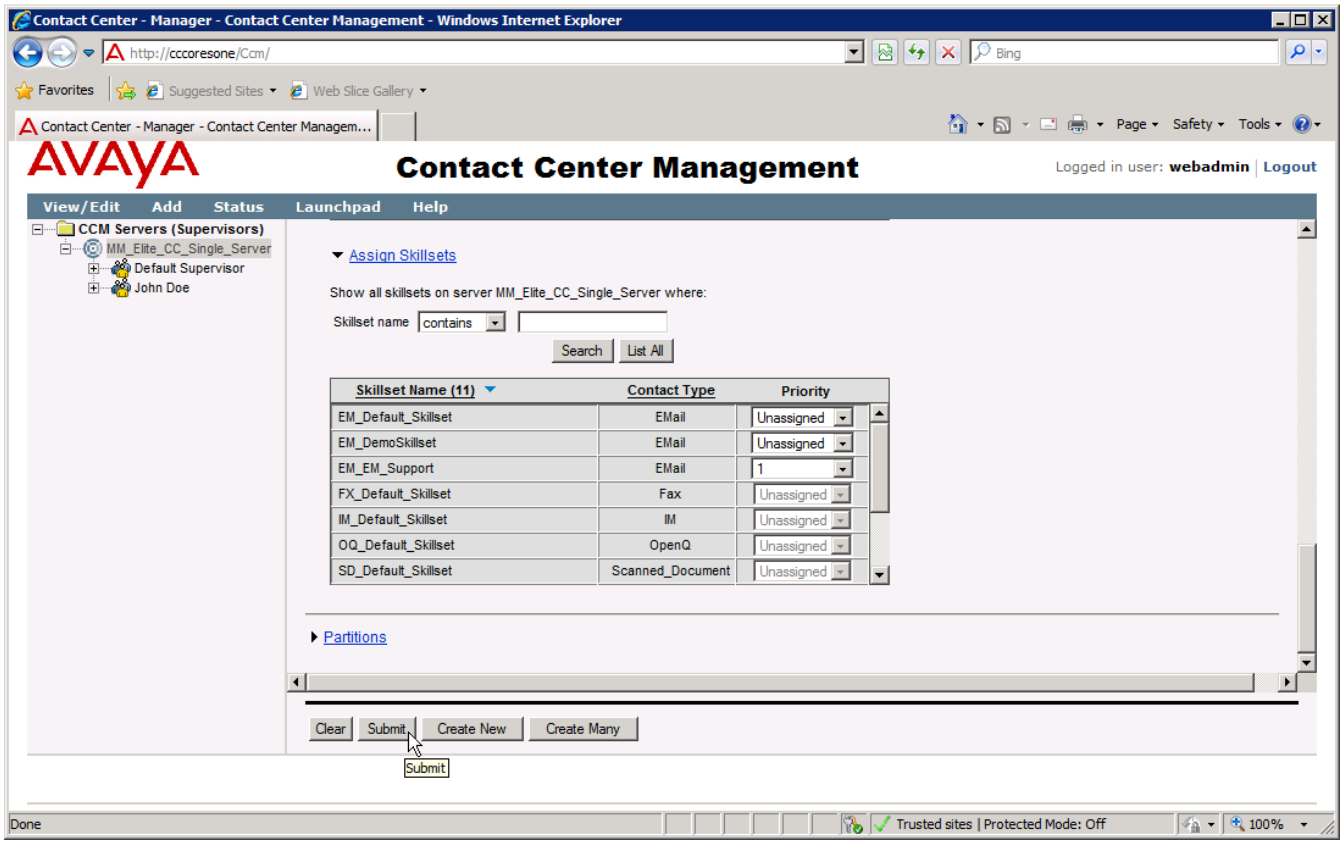
25 Click **List All**.



26 For an E-mail skillset, from the **Priority** list, select the priority of this skillset for the agent, to assign this agent to that skillset. For example for **EM_EM_Support**, select **1**.



27 Click **Submit** to save your changes.



--End--

Adding an agent profile

Assigning a template to an agent creates that agent's profile. You can customize agent profiles based on individual agent requirements, and the changes made to a profile are specific to an agent.

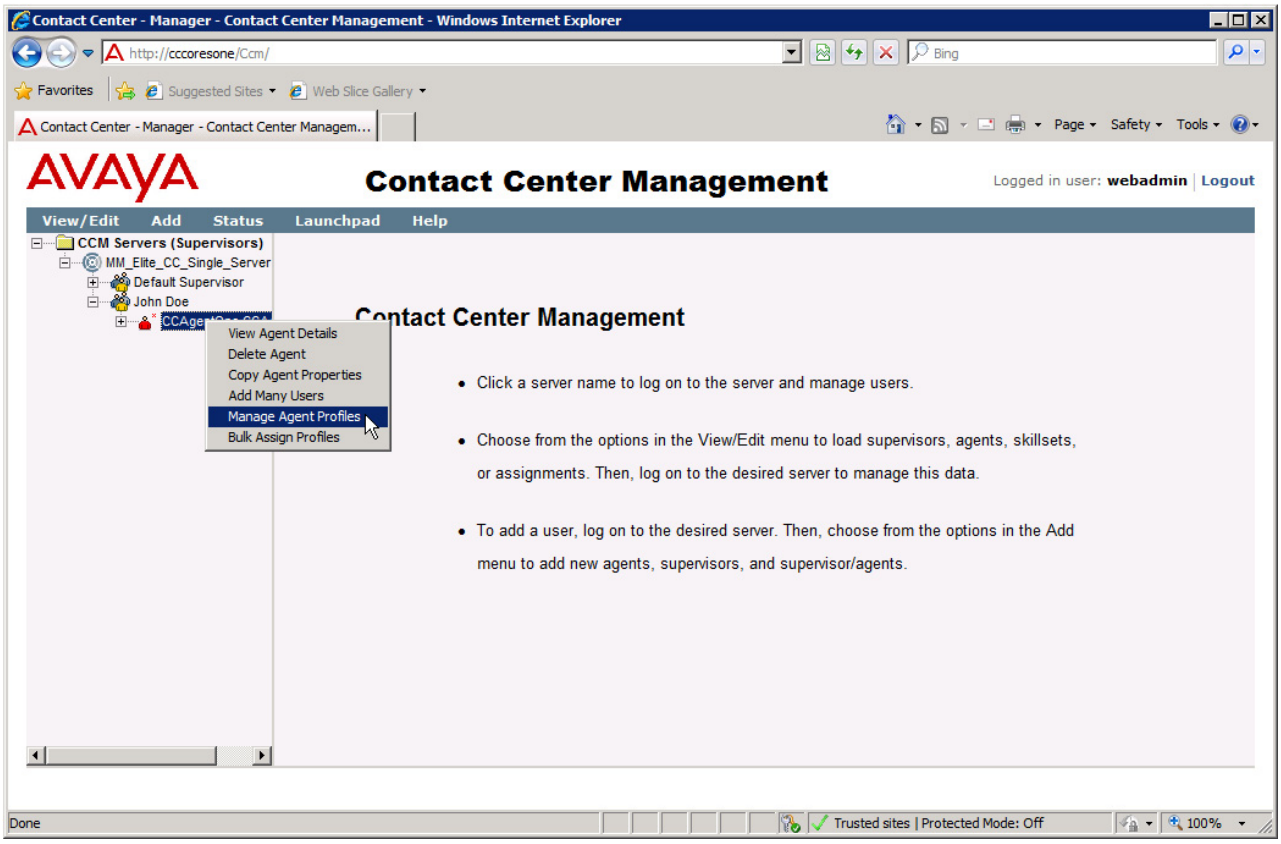
You can assign multiple profiles to agents and then select a preferred profile for an agent. By default the agent logs on to the Agent Desktop using the preferred profile, although they can select a different profile when they log on.

Procedure steps

Step	Action
1	In the left pane, expand the Contact Center Manager Server server that contains the agent to whom you want to assign the profile, for example **MM_Elite_CC_Single_Server**.

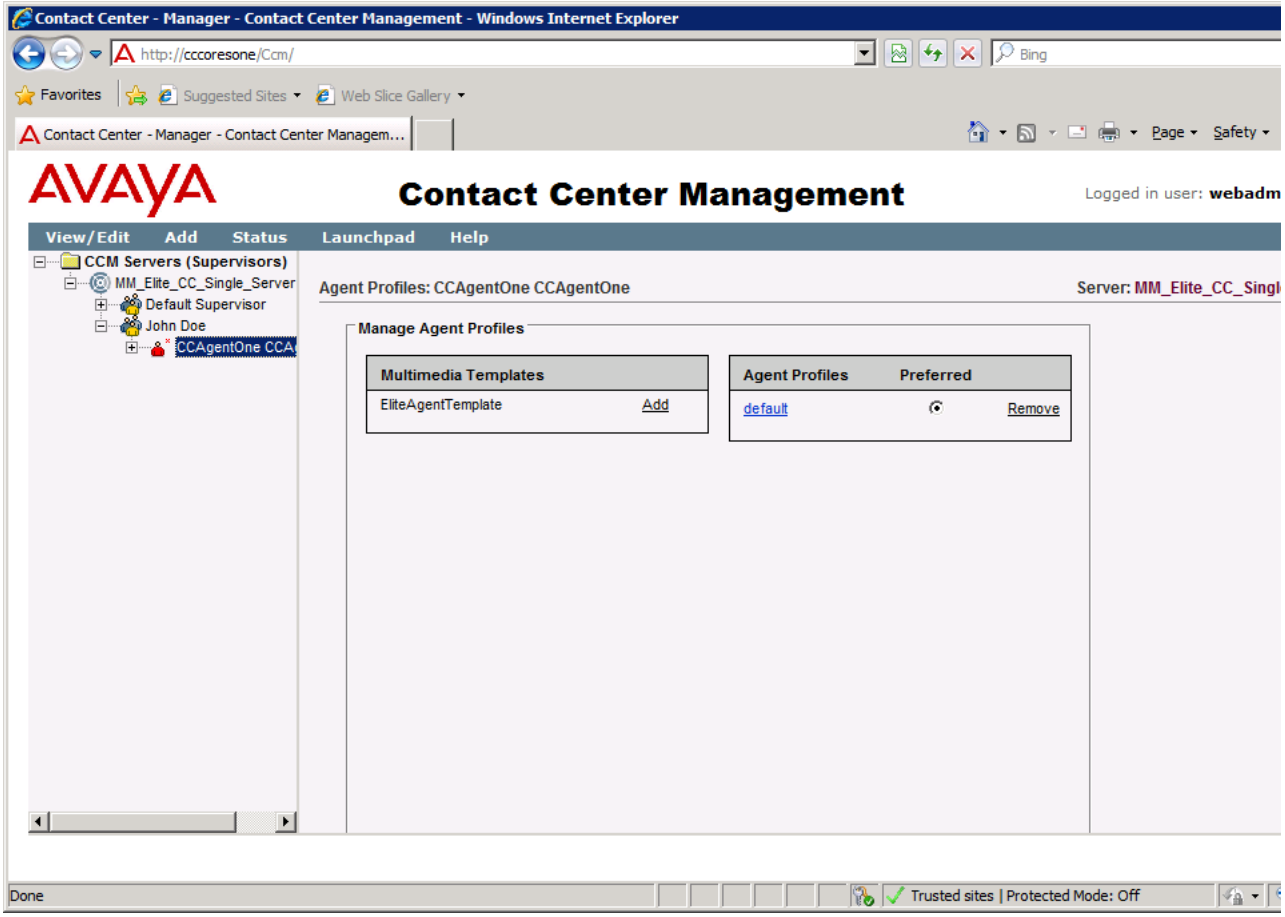
2 In the left pane, right-click the agent and select **Manage Agent Profiles**.

The Agent Profiles page appears in the right pane.

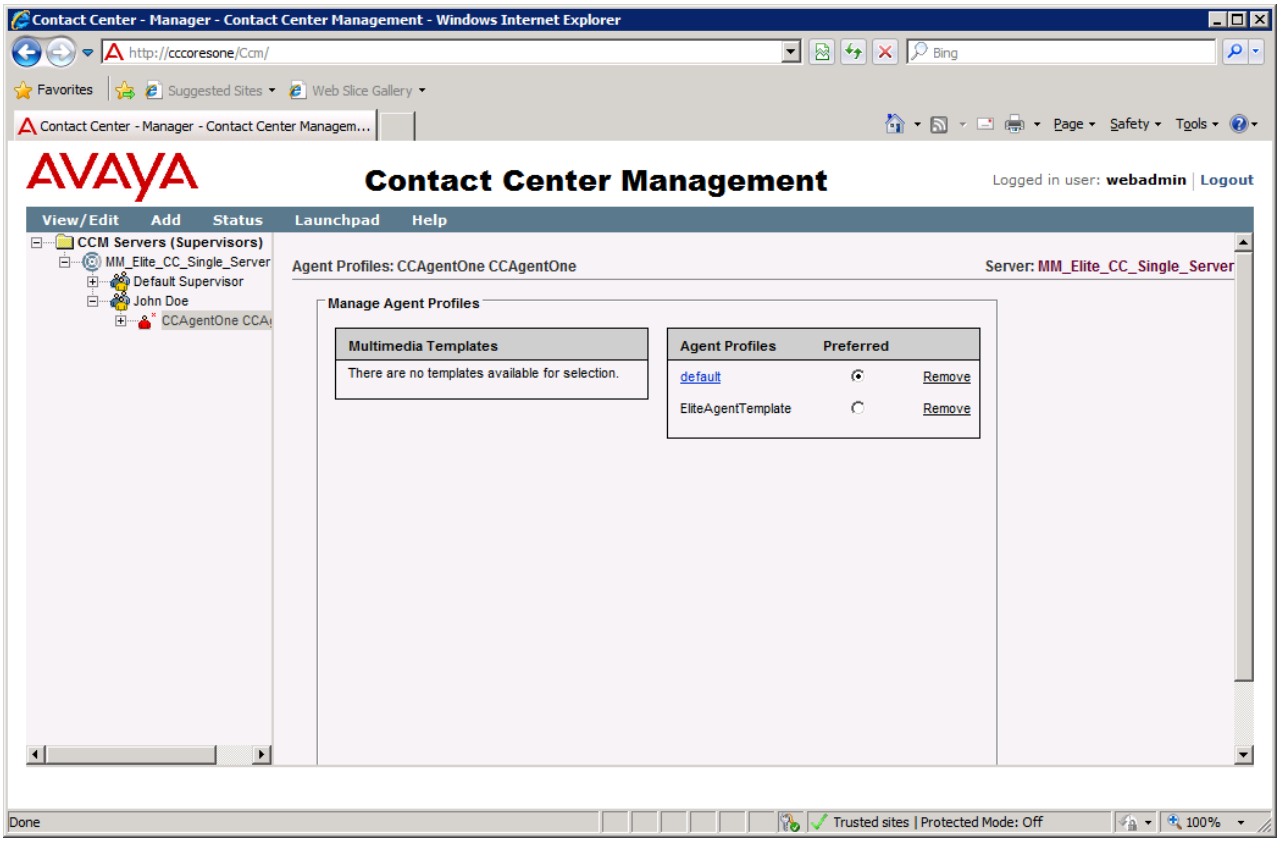


3 Under **Multimedia Templates**, beside the profile that you want to assign to the agent, for example **EliteAgentTemplate**,

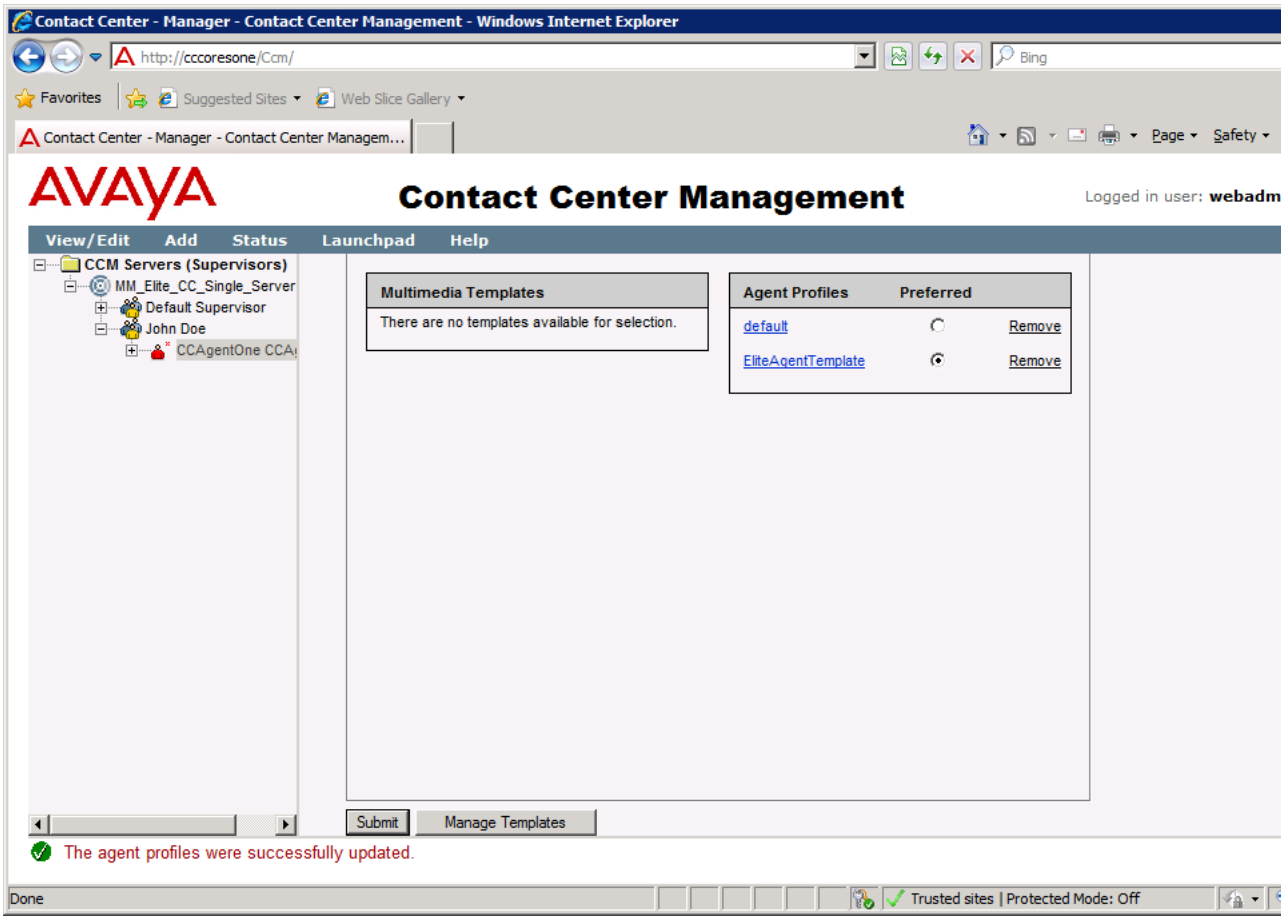
4 Click the **Add** link.



5 Click **Submit**.



6 Under **Agent Profiles**, choose the **Preferred** profile, for example **EliteAgentTemplate**. The agent uses this profile when logging on to the Agent Desktop.



7 Under **Agent Profiles**, click the link for the new agent profile, for example **EliteAgentTemplate**.

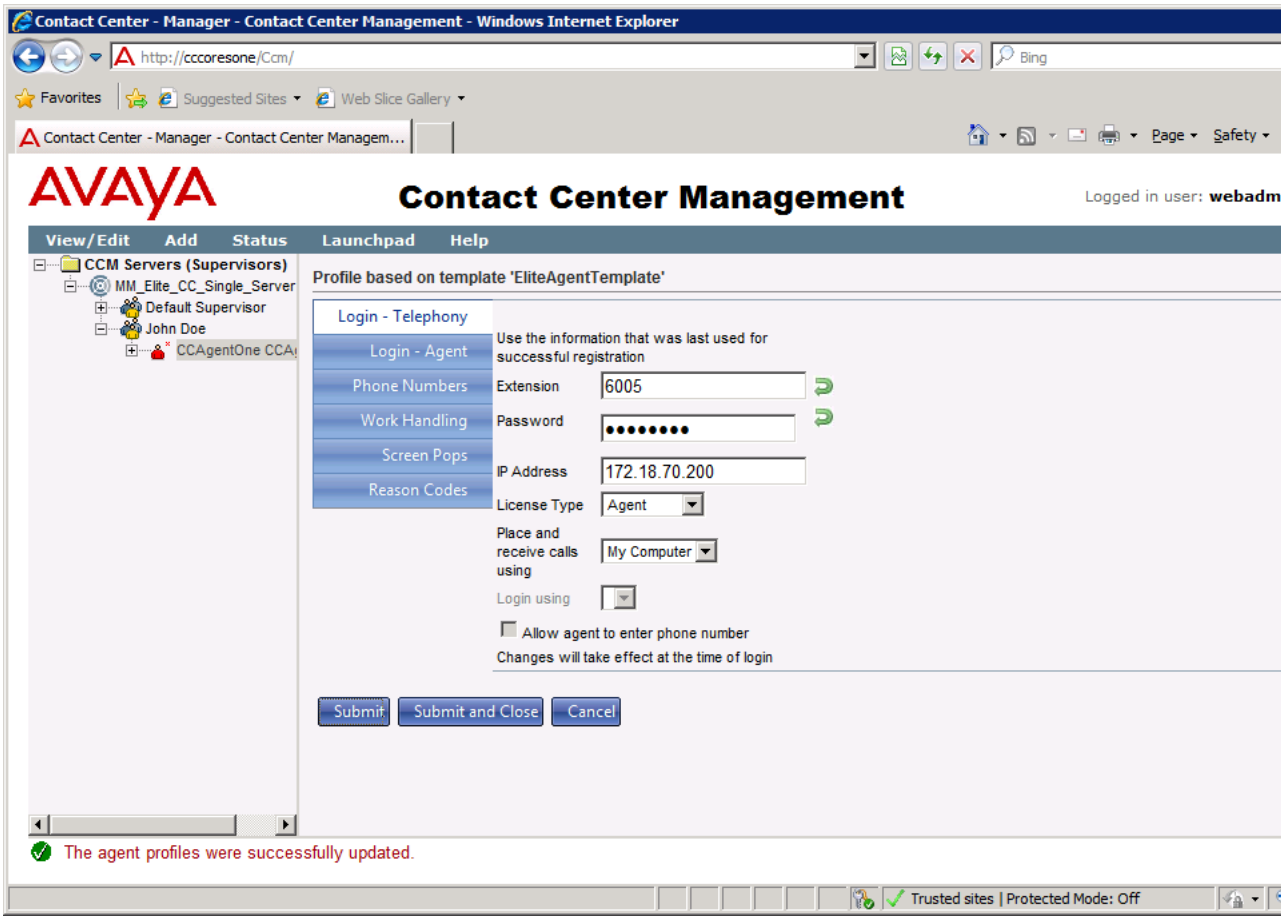
8 In the **Extension** box, type the Communication Manager station extension that this agent uses for their voice calls, for example **6005**.

9 In the **Password** box, type the password for the Communication Manager extension that this agent uses for their voice calls, for example **12345678**.

10 Verify that the Communication Manager IP address is correct in the **IP address** box, for example **172.18.70.200**

11 Verify that the **License Type** selection is **Agent**.

12 Click **Submit**.

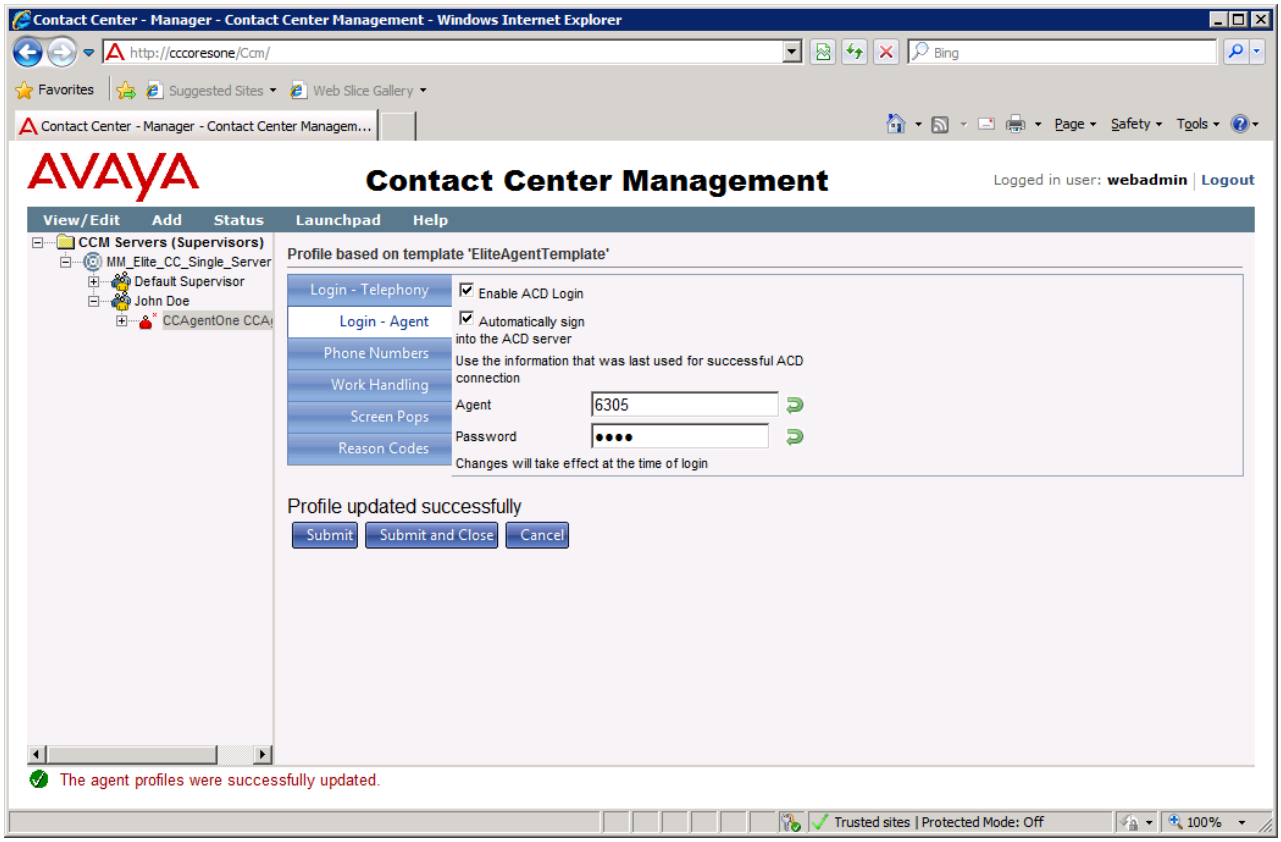


13 Click **Login - Agent**

14 In the **Agent** box, type the Call Center Elite log on ID for this agent, for example **6305**.

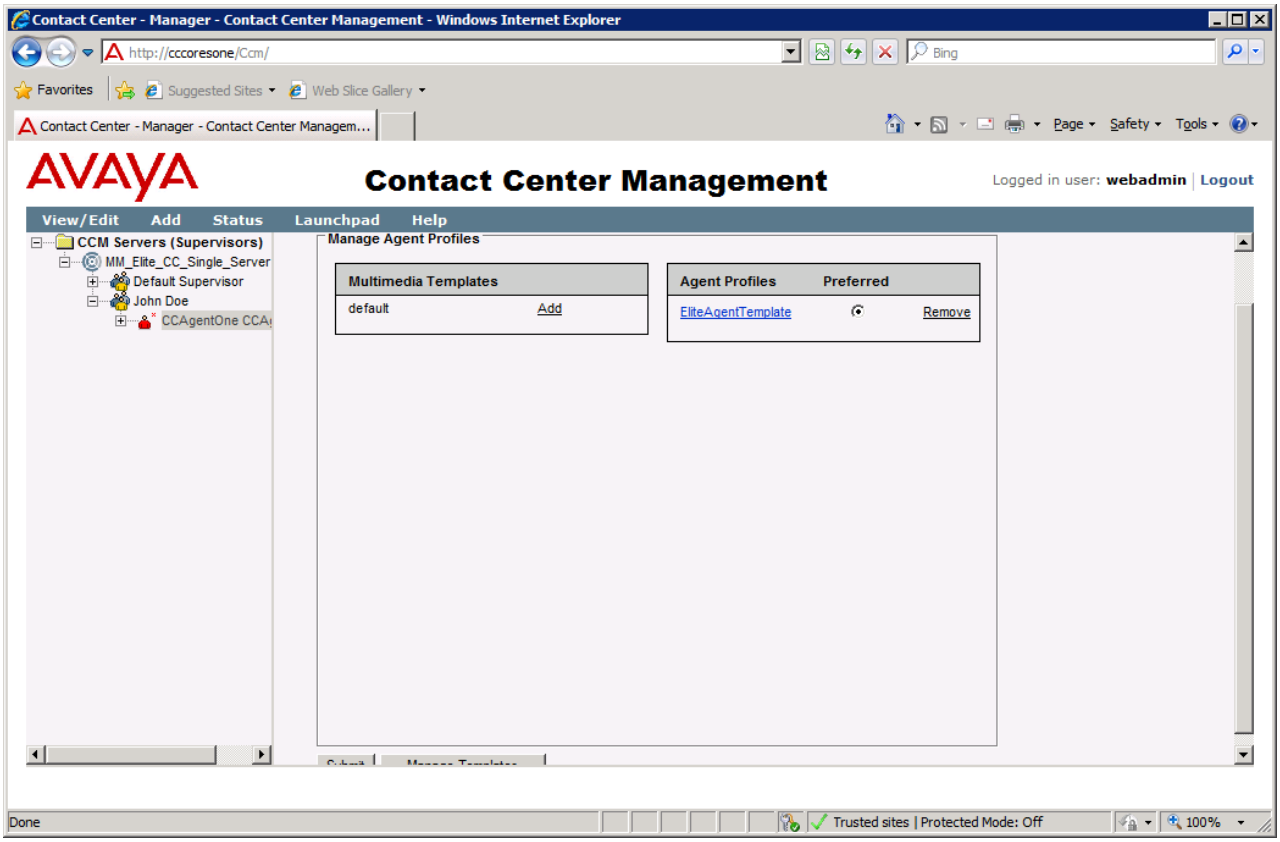
15 In the **Password** box, the Call Center Elite log on ID for this agent, for example **1234**.

16 Click **Submit**.



17 Click **Submit and Close**.

18 Under **Agent Profiles**, beside the **default** profile, click the **Remove** link. This removes the default profile from the agent, so they cannot use it when logging on to Agent Desktop.



19 Click **Submit**.

--End--

Client Installation Section

Agent Desktop client software installation

This chapter describes how to install the Agent Desktop client software on a client computer in your contact center. Agent Desktop enables agents to handle contacts of all media types enabled in your contact center, from the start to the end of a contact.

Attention: If you plan to implement High Availability (HA) with a standby Contact Center server, install the minimum number of Agent Desktop clients required to test the solution. When you configure HA, client computers already installed require a reinstall of Agent Desktop to reference the managed IP address of the HA solution.

You install the Agent Desktop client application on a client computer by accessing an install program at a Web location on the Contact Center server.

Prerequisites for Agent Desktop client software installation

- 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 or later.

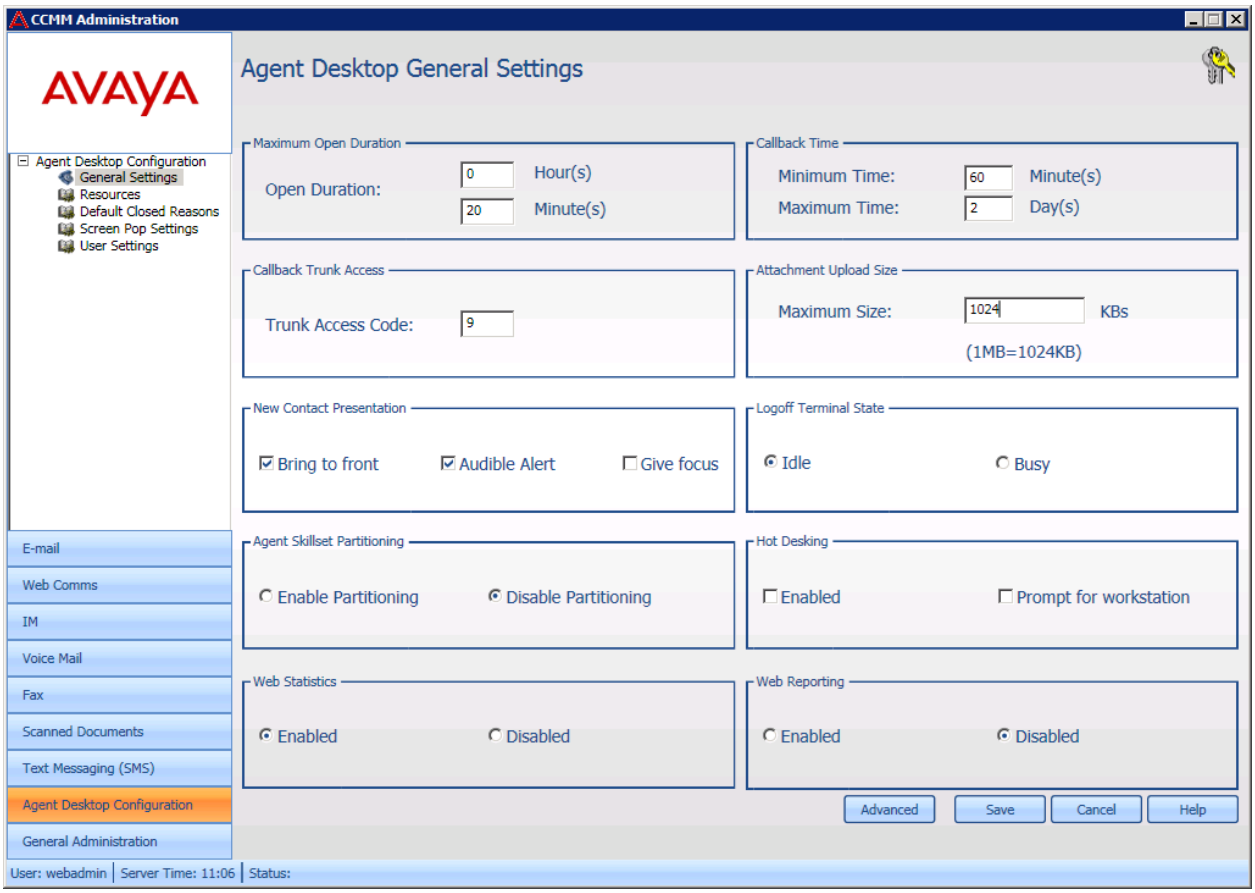
Modifying the agent settings in CCMM Administration client

Review the global Agent Desktop settings in CCMM Administration client, and change any settings required to customize your contact center. It is critical to set the switch type in the Advanced Settings to ensure that agents can log on to Call Center Elite when they launch Agent Desktop.

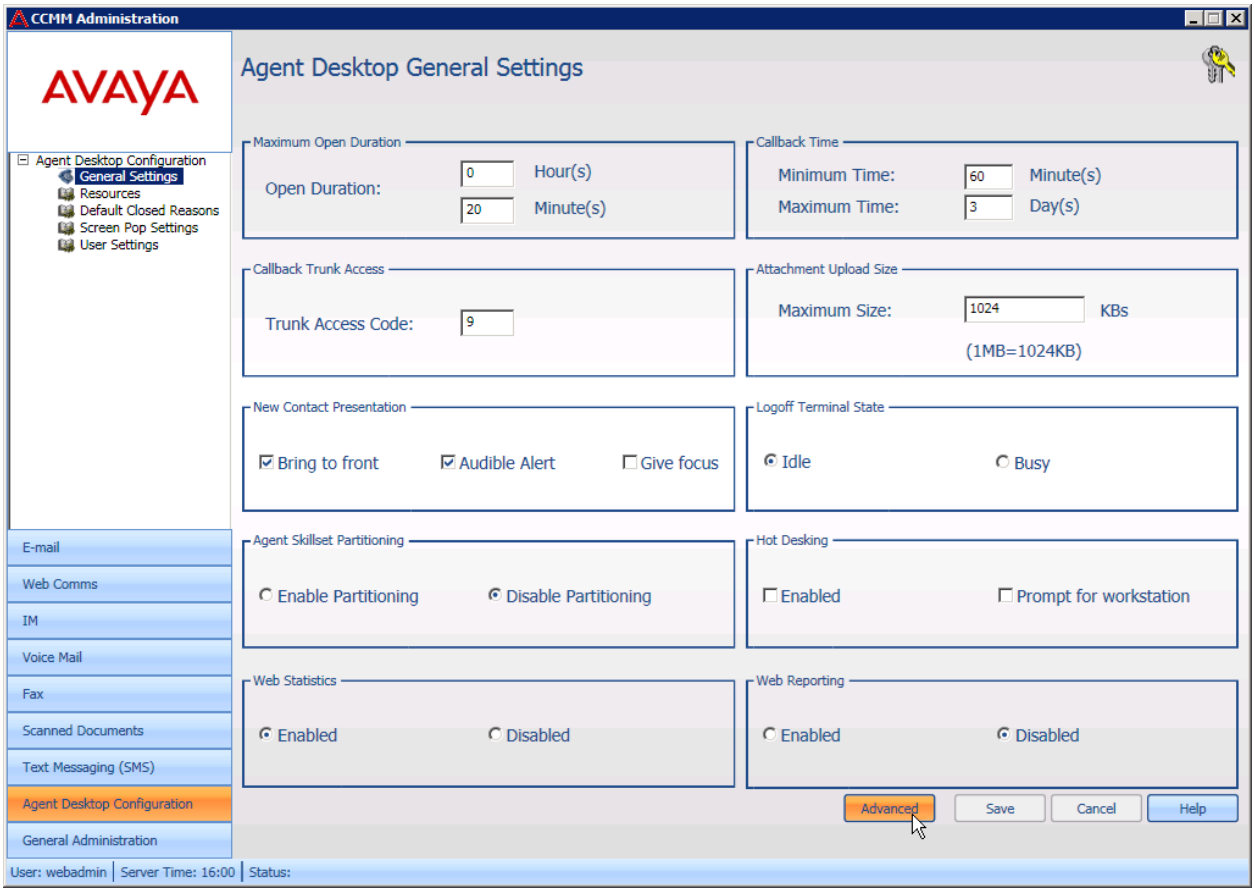
Procedure steps

Step	Action
1	On the CCMA Launchpad, click **Multimedia**.
2	In the left column, select the CCMM server on which you want to configure skillsets, for example **CCElite_CCMM**.
3	In the right pane, click **Launch Multimedia Client**.
4	On any pop-up dialogs that appear, click **Run**.
5	In the left pane, select **Agent Desktop Configuration**.

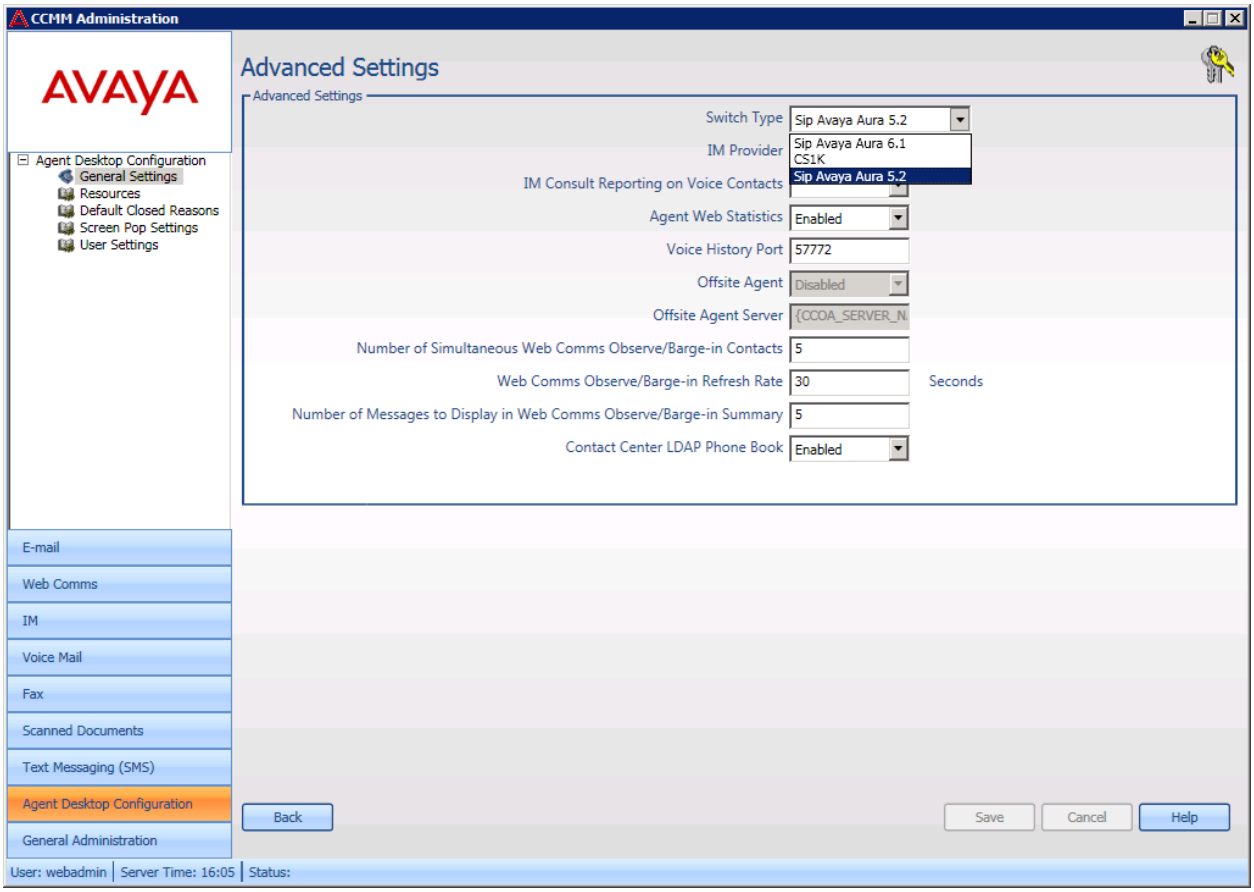
6 Modify the agent desktop settings to match the requirements for your contact center. For example:
– Change the **Callback Time:Maximum Time** to **2** to set the maximum number of days the system waits before re-offering a Pending contact to the agent.
– Change the **Attachment Upload Size:Maximum Size** to **1024** to allow agents to send attachments up to 1 Mb in size in their e-mail responses.



7 Click **Advanced**.

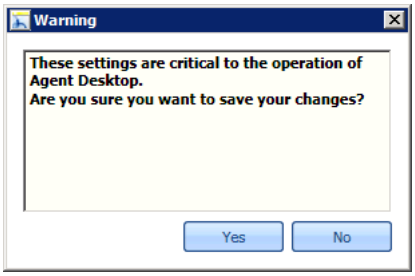


8 On the **Advanced Settings** window, from the **Switch Type** list, select the release of the Communication Manager PABX that hosts Call Center Elite, for example **Sip Avaya Aura 5.2**.

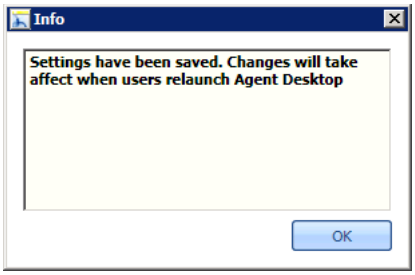


9 Click **Save**.

10 On the **Warning** message box, click **Yes**.



11 On the **Info** message box, click **OK**.



12 On the **Agent Desktop General Settings** window, click **Save**.

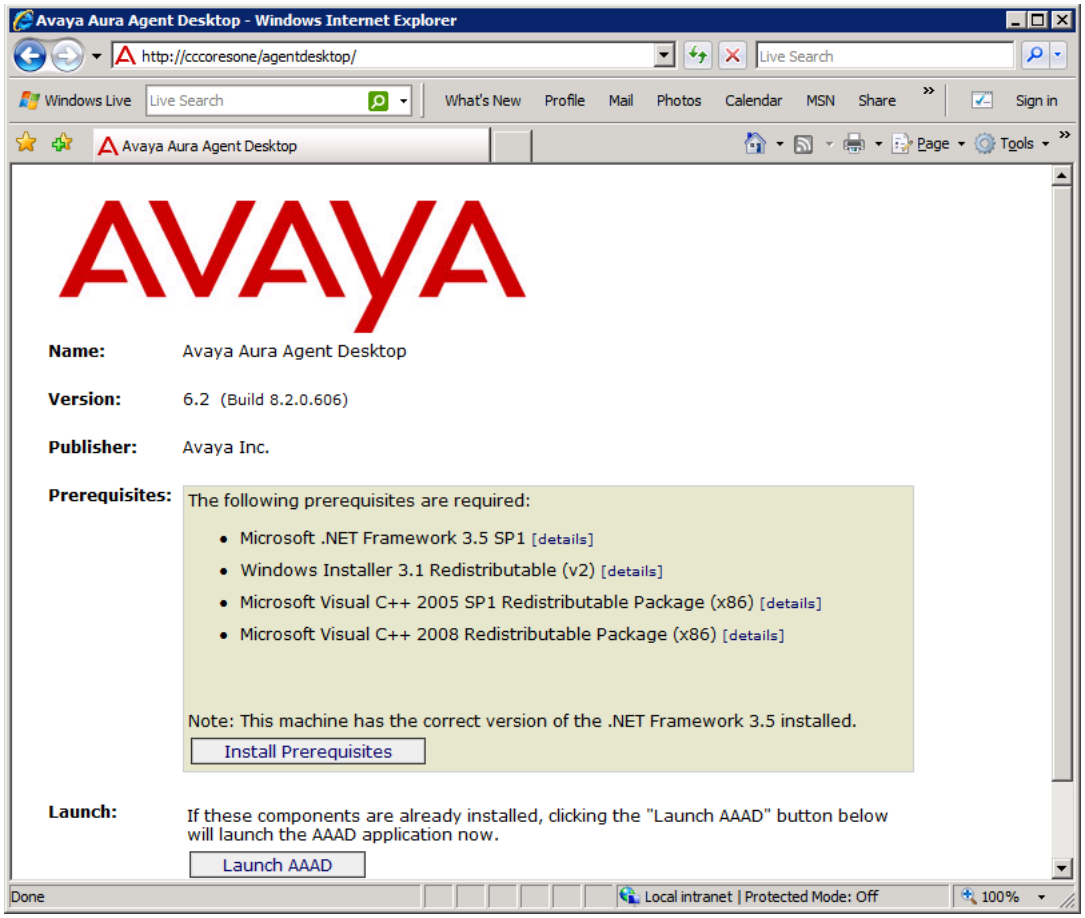
--End--

Installing the Agent Desktop client software

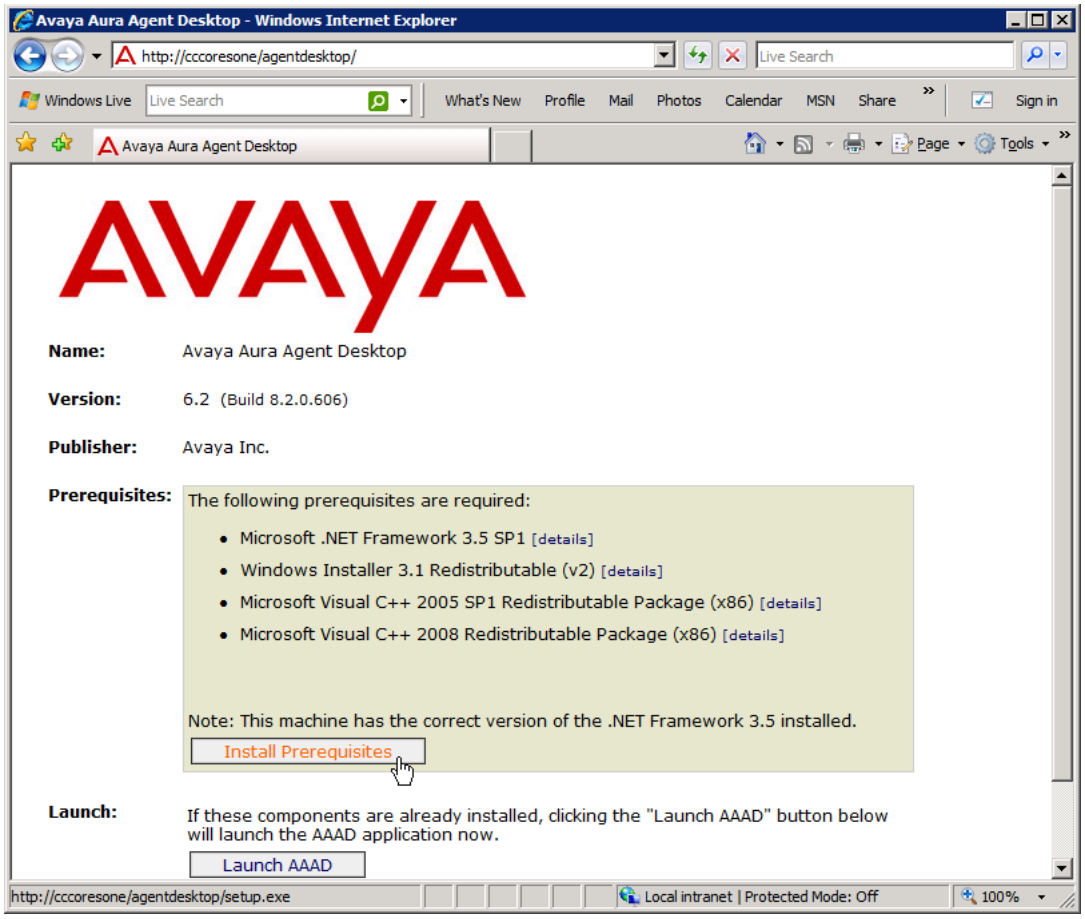
Install the Agent Desktop client software on a client computer to which an agent logs on to handle contacts using the multimedia toolbar and softphone.

Procedure steps

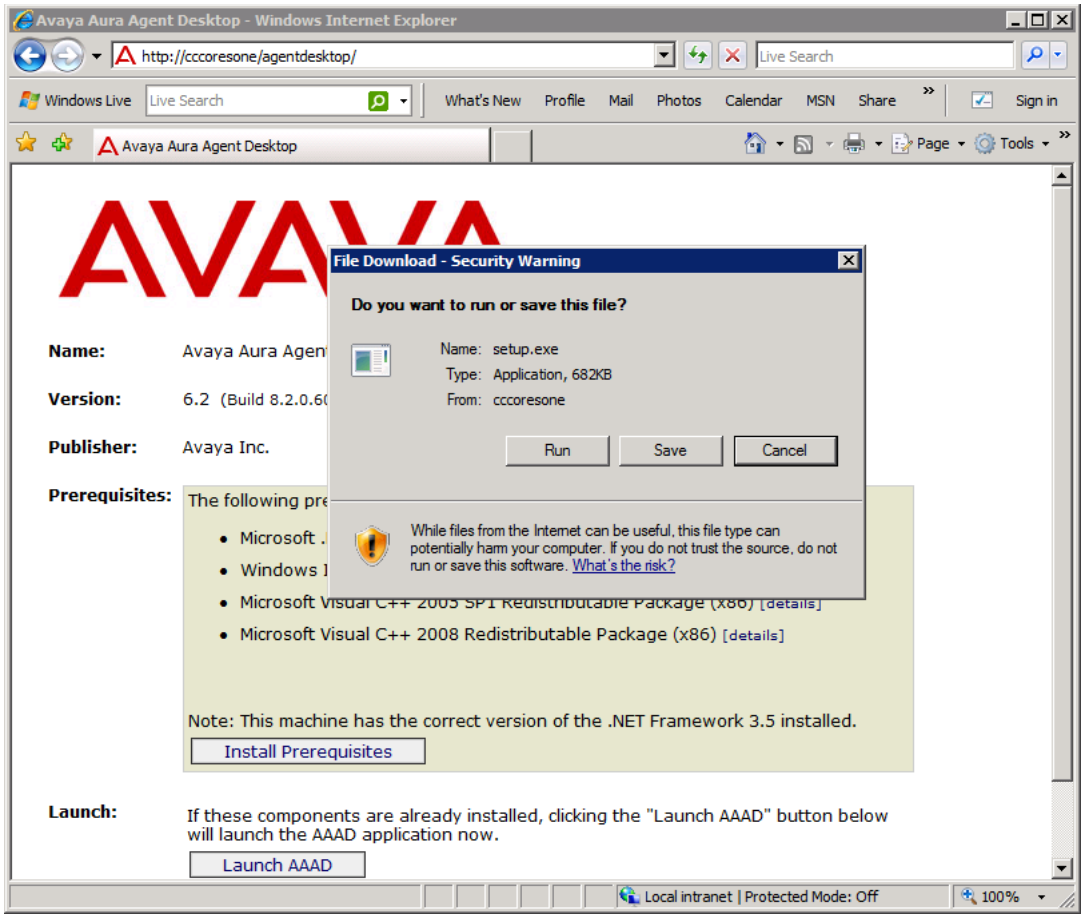
Step	Action
1	Log on to the desktop computer using the agent's domain username and password, for example **CCAgentOne**, **AG1_pass~2**.
2	On the client computer, start Internet Explorer.
3	In Internet Explorer, in the **Address** box, type the link to the installer on the Multimedia server in the form **http://<servername>/agentdesktop**, for example **http://cccoresone/agentdesktop**, and press **Enter**.



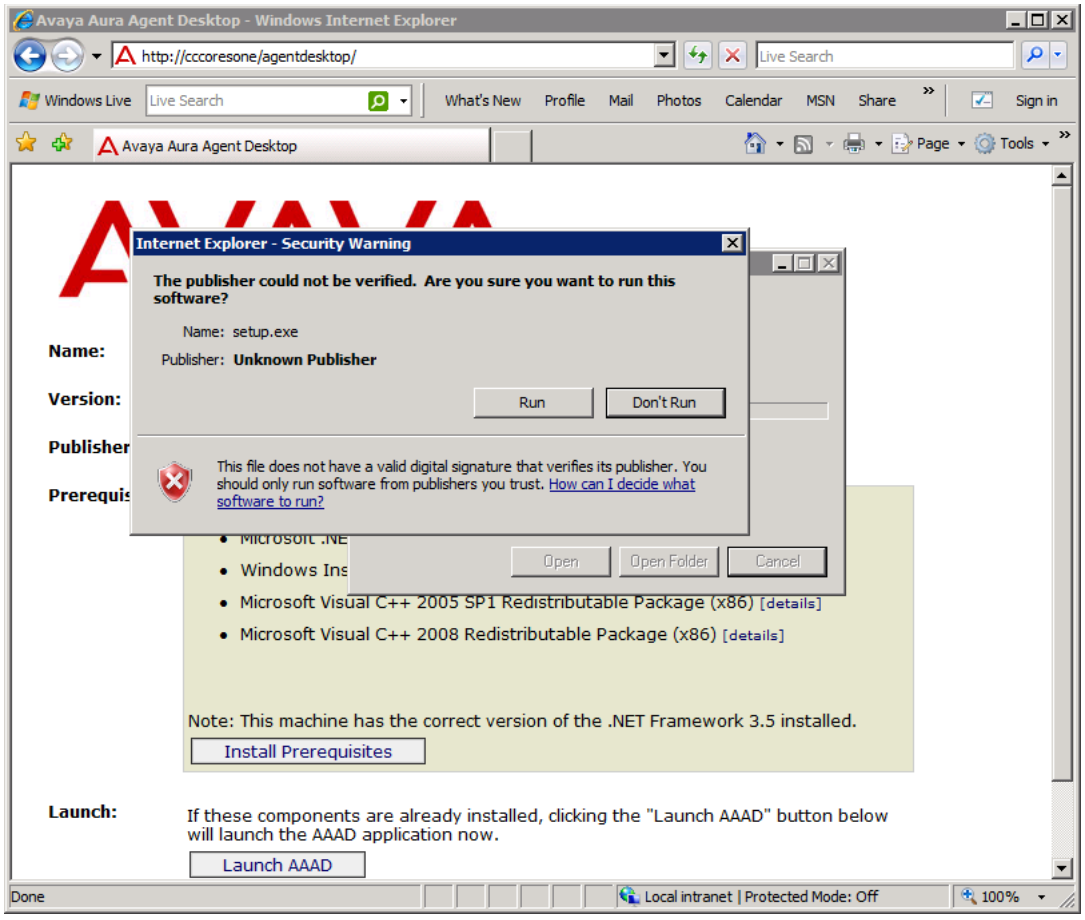
4 On the Agent Desktop page, click **Install Prerequisites**.



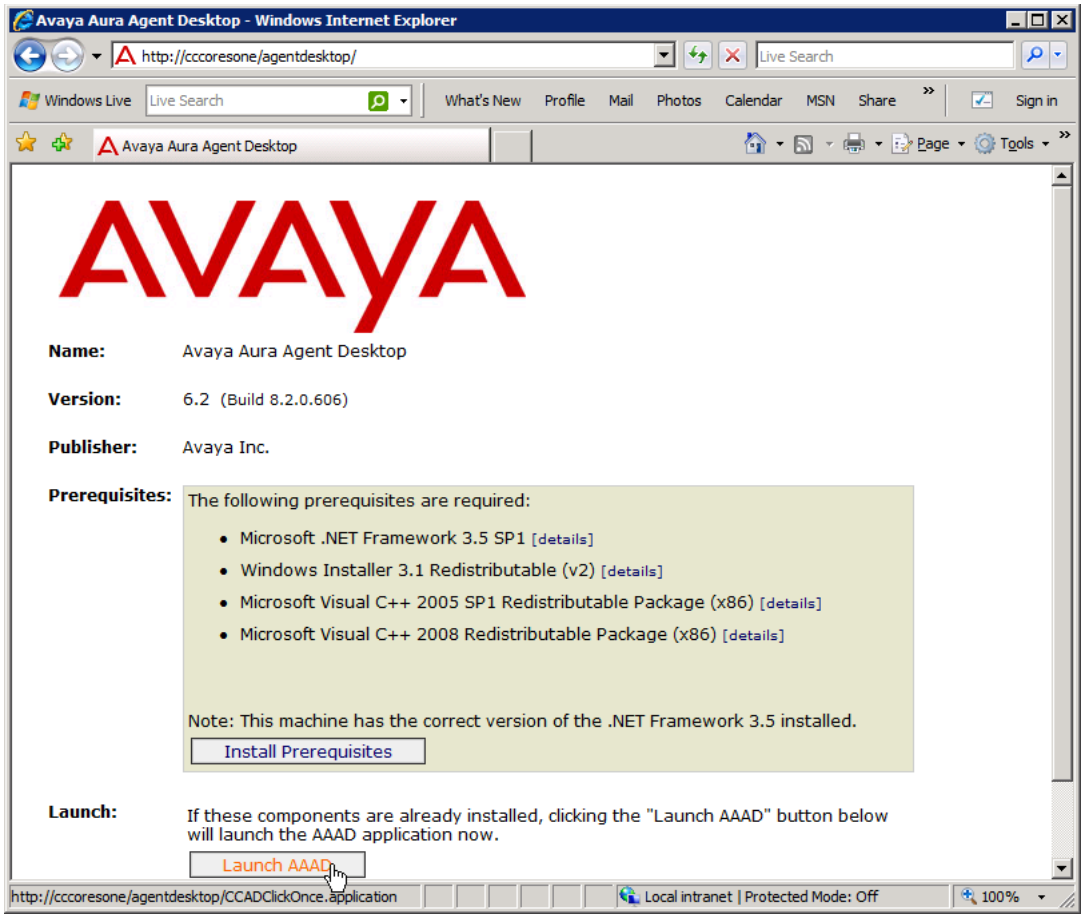
5 On the **File Download - Security Warning** dialog, select **Run**.



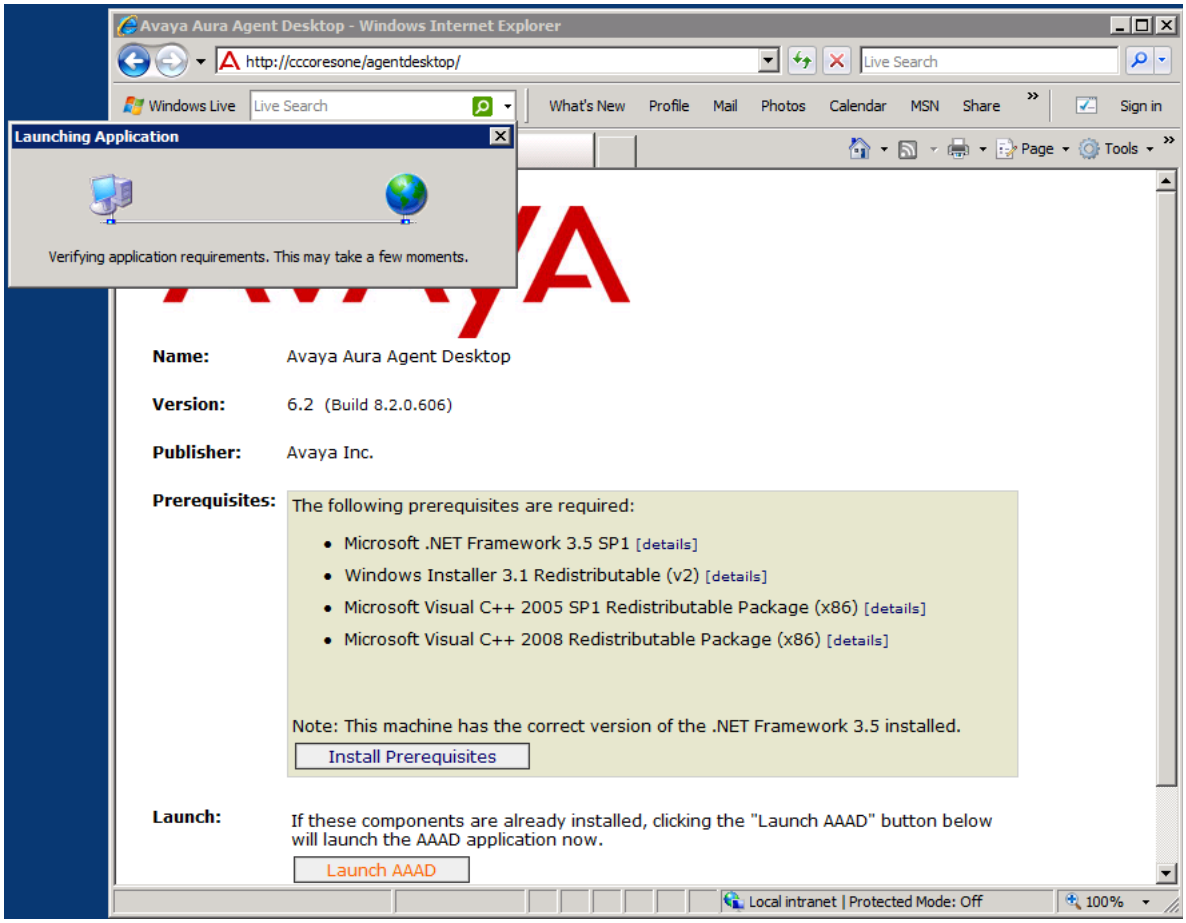
6 On the **Internet Explorer - Security Warning** dialog, select **Run**.



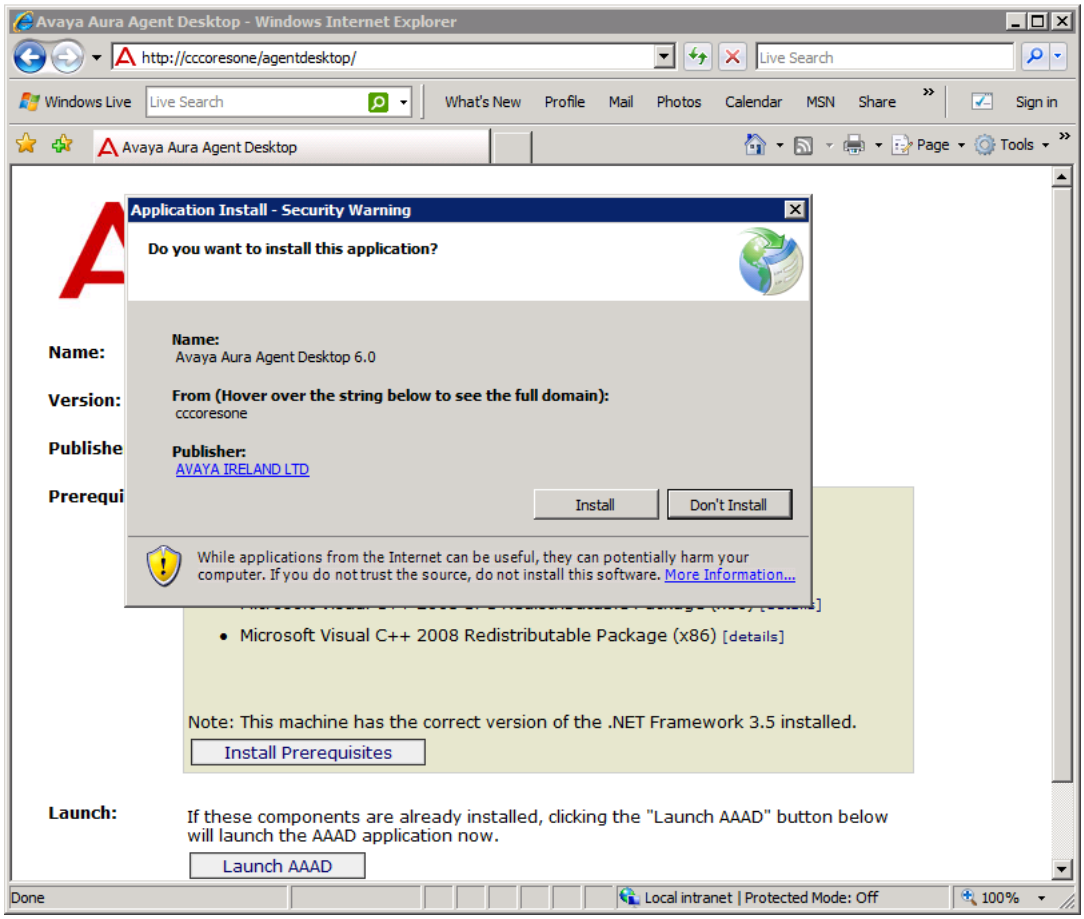
7 When the prerequisites install completes, on the **Avaya Aura Agent Desktop** web page, select **Launch AAAD**.



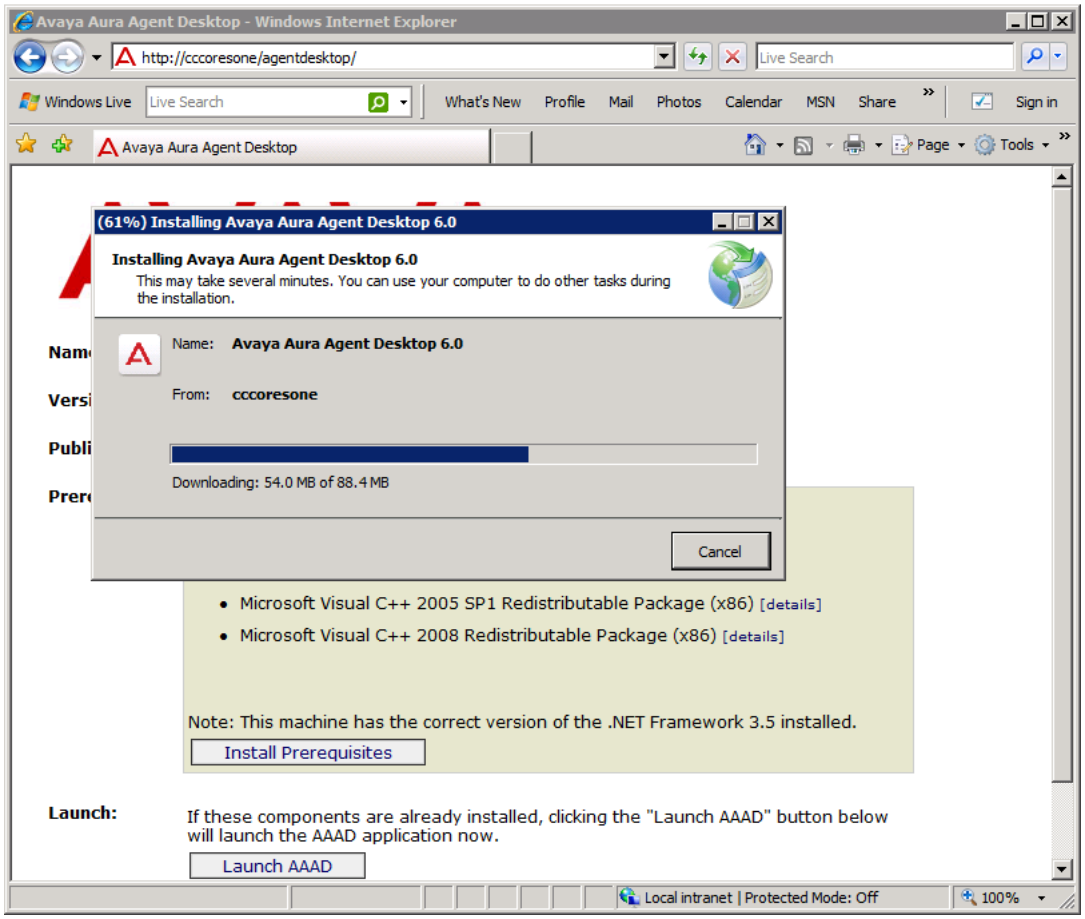
The installer displays the Launching Application dialog while it checks the application prerequisites.



8 On the **Application Install - Security Warning** dialog, select **Install**.



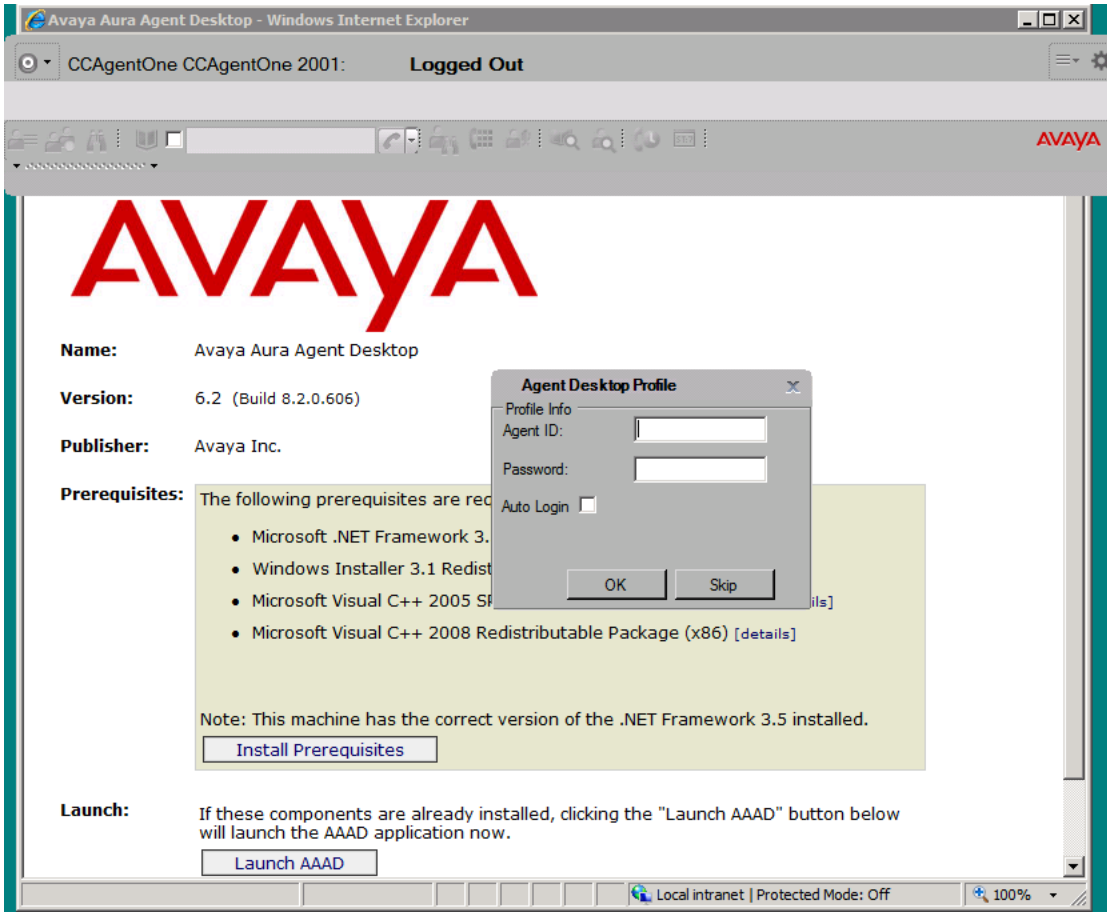
The installer displays a dialog showing the progress of the client installation.



When the installation is complete, Agent Desktop initializes and starts.



9 In the **Agent Desktop Profile** dialog, enter the CCMM login ID and password for the agent, for example **2001**, **2001**.

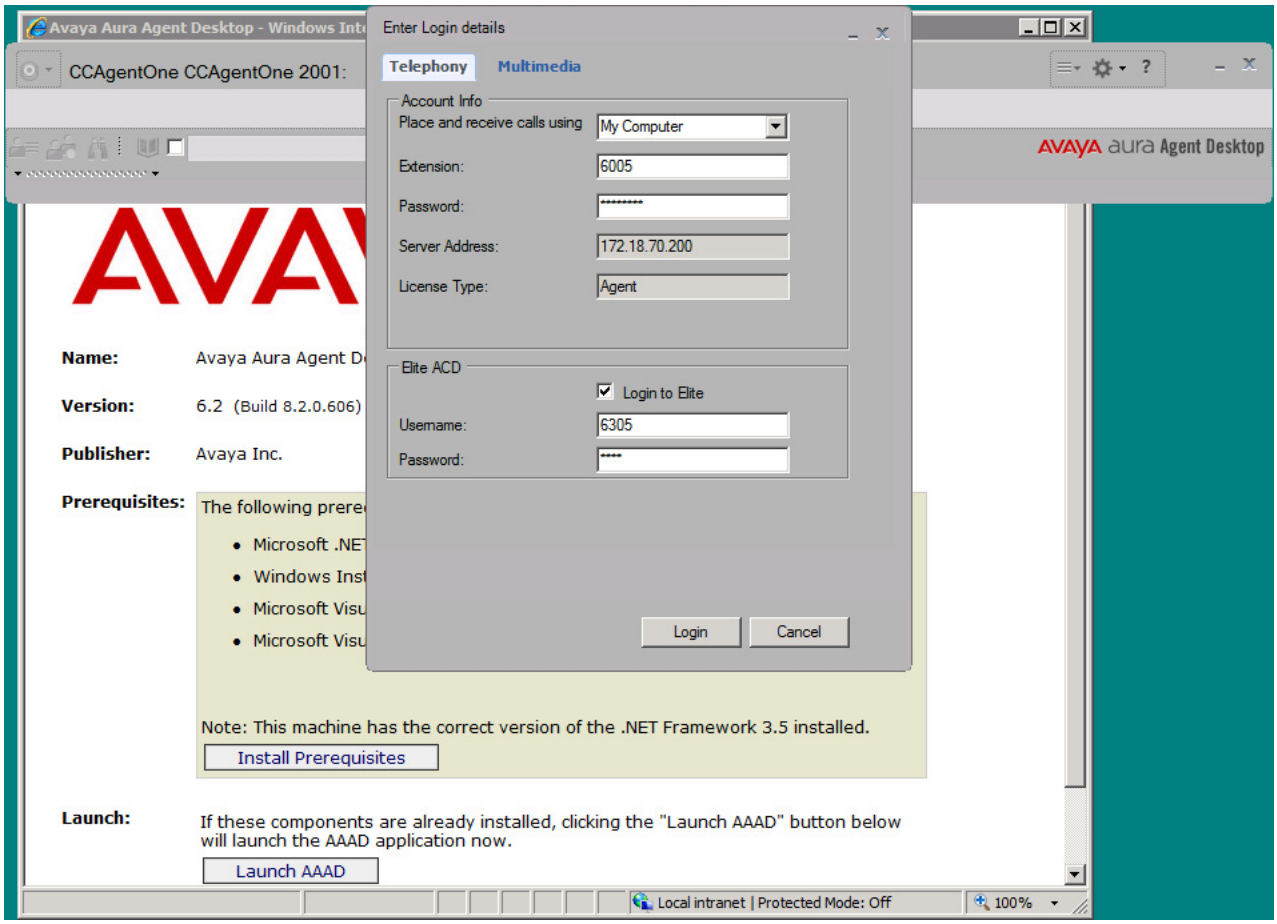


10 Click **OK**.

11 On the Agent Desktop Telephony Toolbar, from the **Status** list, select **Login**.

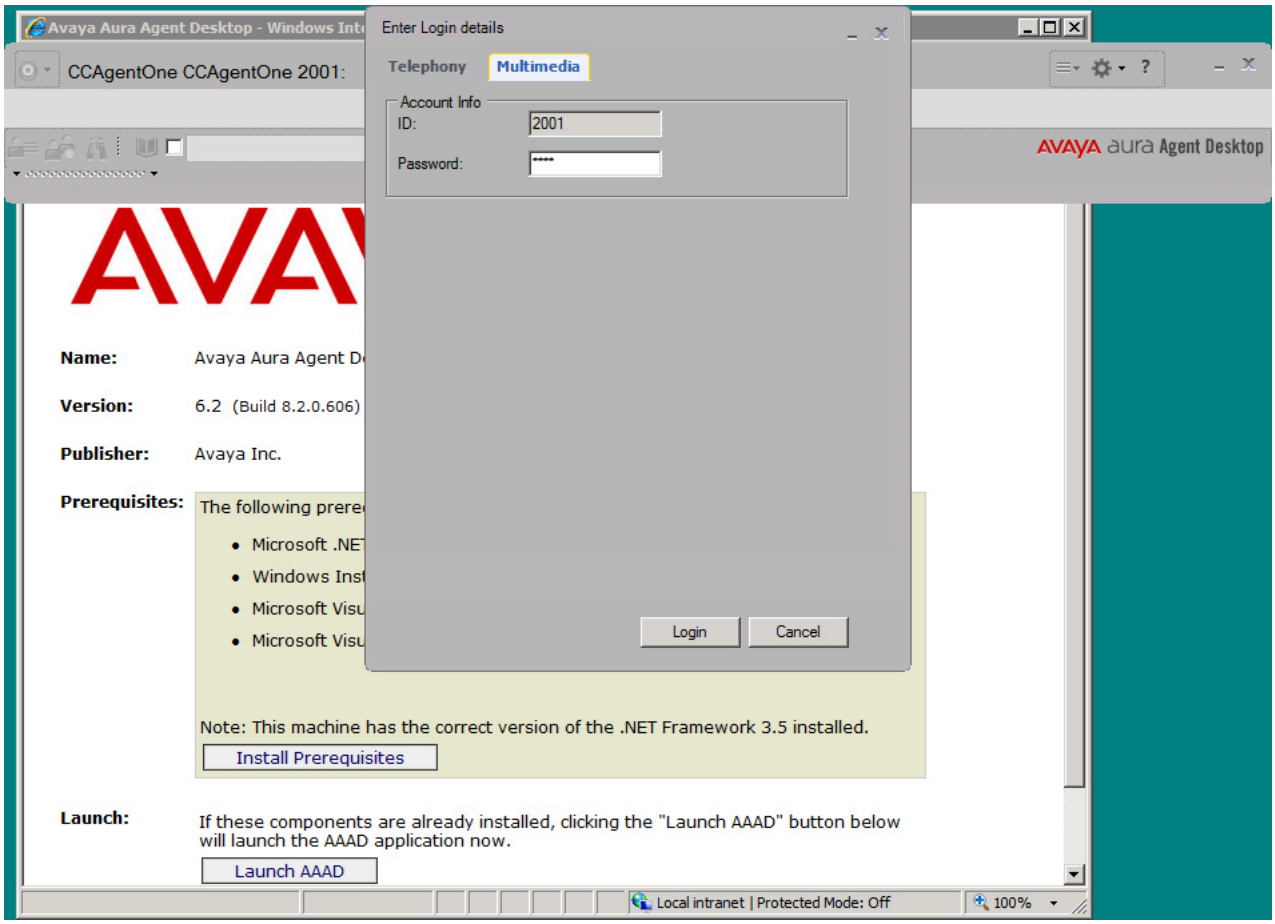


*Agent Desktop displays the **Enter Login details** dialog, pre-populated with the settings from the agent's default profile.*



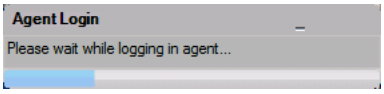
12 Click **Multimedia**.

13 On the **Multimedia** tab, in the **Password** box, type the Contact Center password for this agent, for example **2001**.



14 Click **Login**.

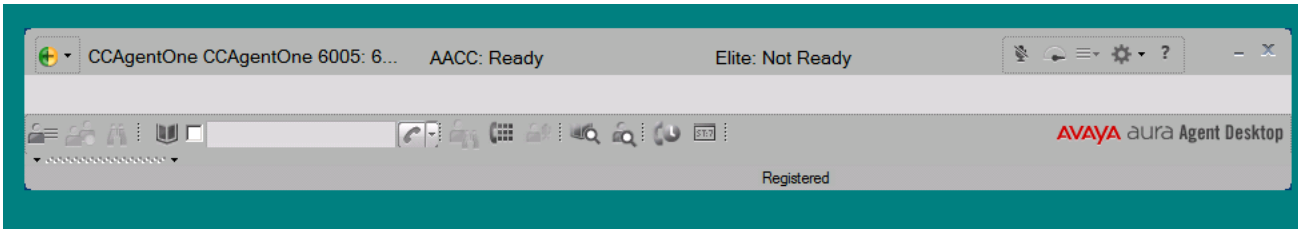
*Agent Desktop displays the **Agent Login** progress window.*



15 On the Agent Desktop Telephony Toolbar, from the **Status** list, select **Go Ready, Multimedia**.



Agent Desktop sets the agent's Avaya Aura® CC status to Ready.



16 On the Agent Desktop Telephony Toolbar, from the **Status** list, select **Go Ready, Voice**.



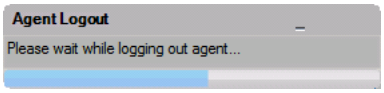
Agent Desktop sets the agent's Elite status to Ready.



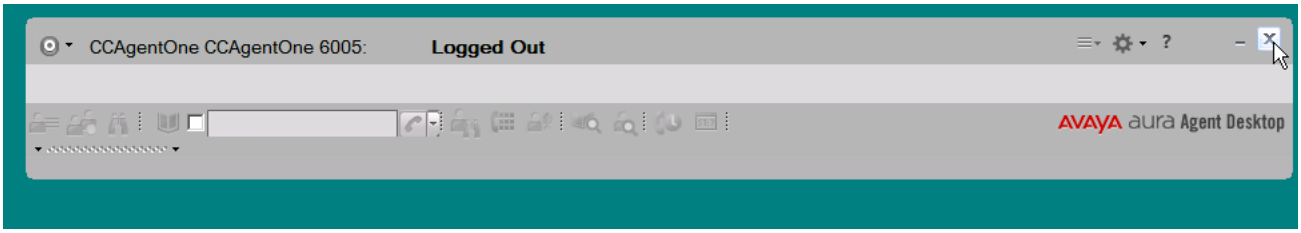
17 On the Agent Desktop Telephony Toolbar, from the **Status** list, select **Logout**.



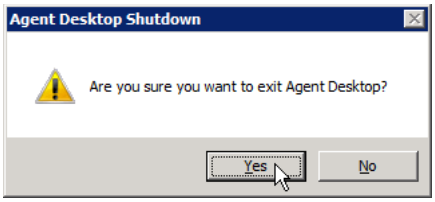
*Agent Desktop displays the **Agent Logout** progress window.*



18 On the Agent Desktop Telephony Toolbar, on the Top Bar, click **Close**.



19 On the Agent Desktop Shutdown dialog, click **Yes**.



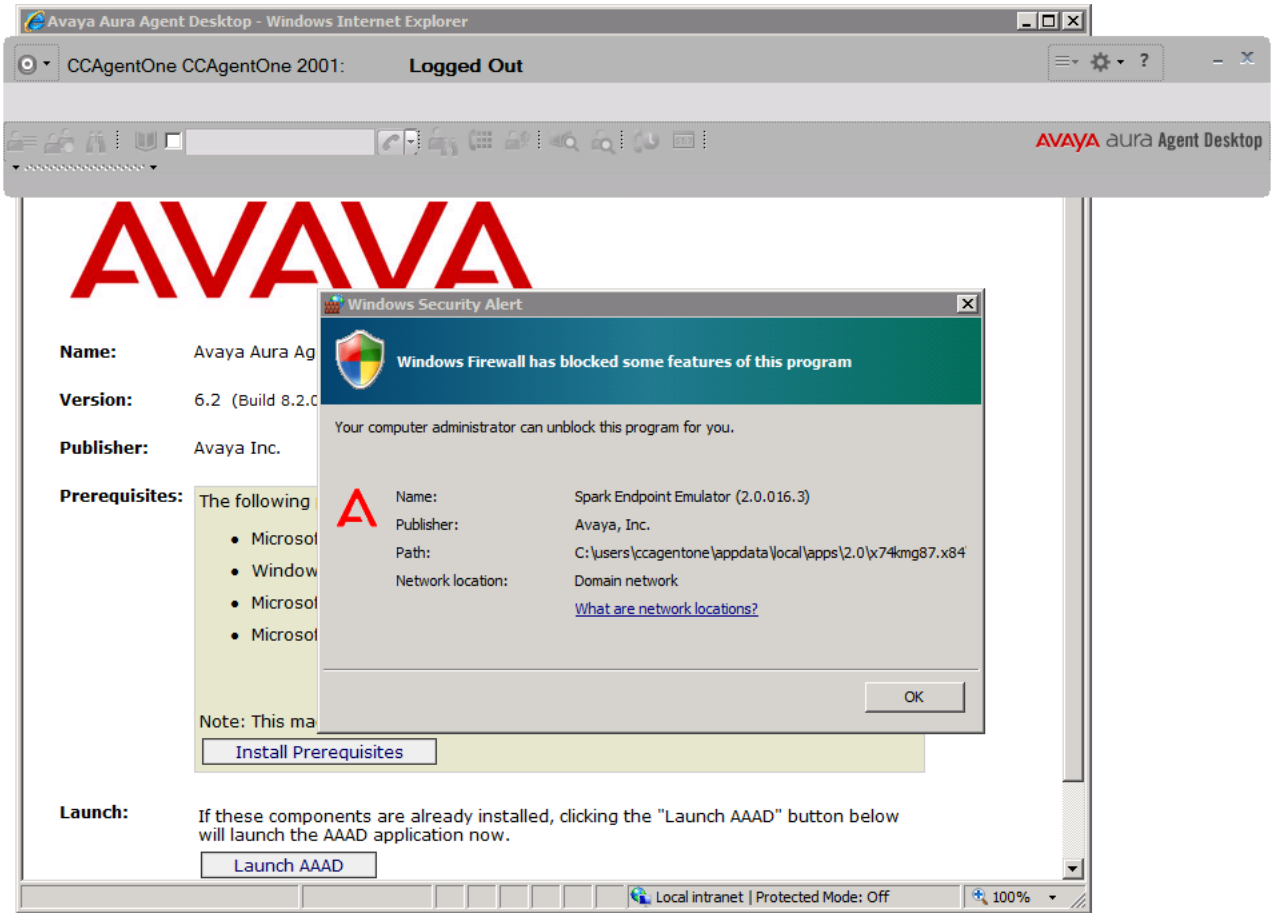
--End--

Agent Desktop installation troubleshooting

Troubleshoot warnings or errors that you can encounter while installing Agent Desktop.

Troubleshooting a Windows Security Alert when you install Agent Desktop

Troubleshoot if Windows displays a Windows Security Alert at the end of the Agent Desktop installation.



This warning can appear during the Agent Desktop install, depending on the security settings on the desktop computer.

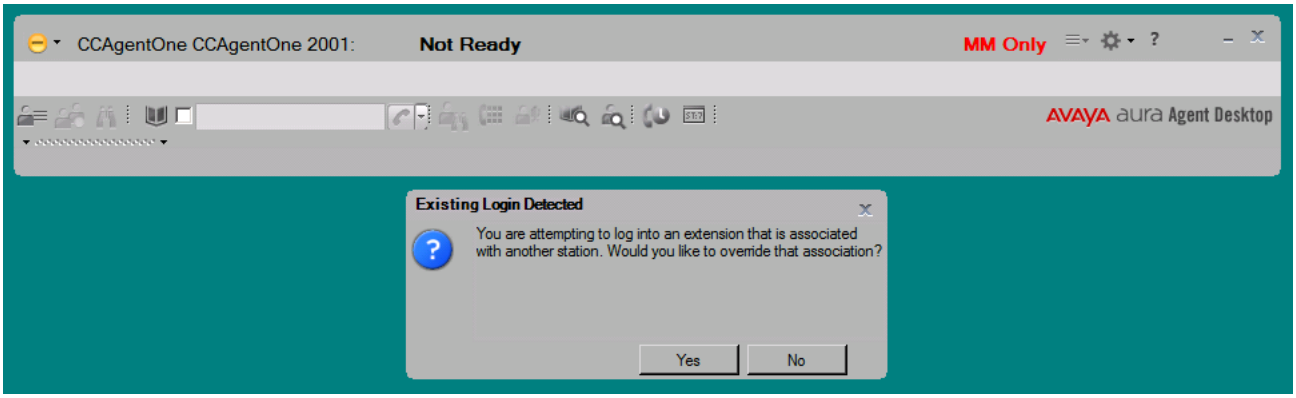
Procedure steps

Step	Action
1	Click **OK**.
	The install continues normally.

--End--

Troubleshooting an Existing Login Detected warning

Troubleshoot when you log on to Agent Desktop and receive a warning "Existing Login Detected".



This error occurs only when you select My Computer on the Enter Login Details dialog. It means that the extension you selected to use for the Agent Desktop softphone is already logged on to another station or computer.

Procedure steps

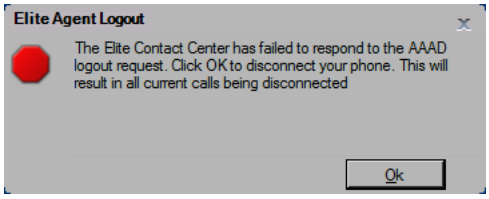
Step	Action
1	Click **Yes** to override the extension that is already logged on. This forces the other extension to log off. **OR**
2	Click **No**.
3	On the Agent Desktop Telephony Toolbar, from the **Status** list, select **Login**.
4	In the **Extension** box, type a different extension to use for the Agent Desktop softphone on this computer.
5	In the **Password** box, type the password for the extension.

6	Click **Login**.

--End--

Troubleshooting an Elite Agent Logout error

This error occurs when your Elite configuration requires an Aux Work code at log off, but you did not set an activity code on Agent Desktop before logging off.



Procedure steps

Step	Action
1	Click **OK** to continue logging off Agent Desktop.

--End--

Testing contacts using Agent Desktop

This chapter describes how to test voice and e-mail message contacts in Agent Desktop to ensure you have completed all the configuration correctly.

Attention: The procedures in this chapter use the example values outlined in earlier chapters in this book. If you used different values, substitute your own values for the example values.

To carry out the procedures in this chapter, you need ready access to the following components of the system:

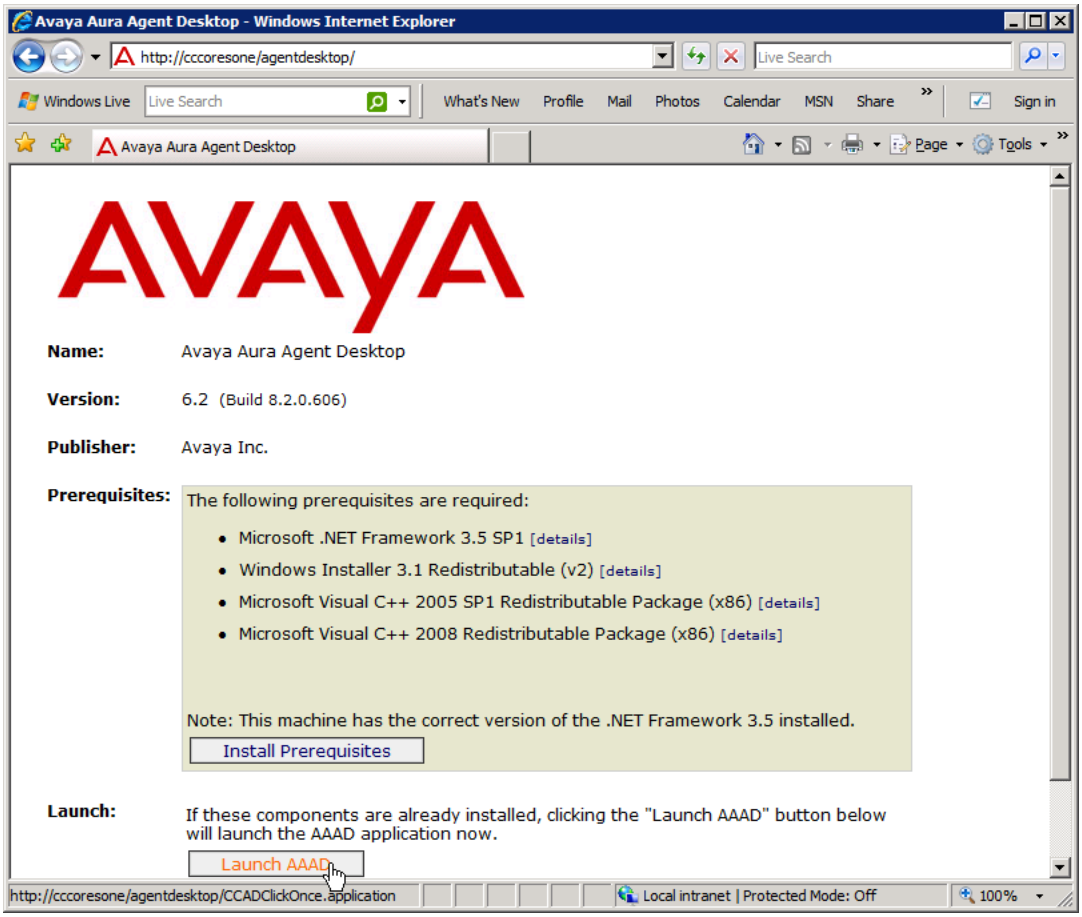
- the Contact Center server
- the Agent Desktop client
- a client from which you can send e-mail messages to the Contact Center mailboxes
- a station (telephone) on the CM from which you can call the Call Center Elite numbers

Logging on to Agent Desktop

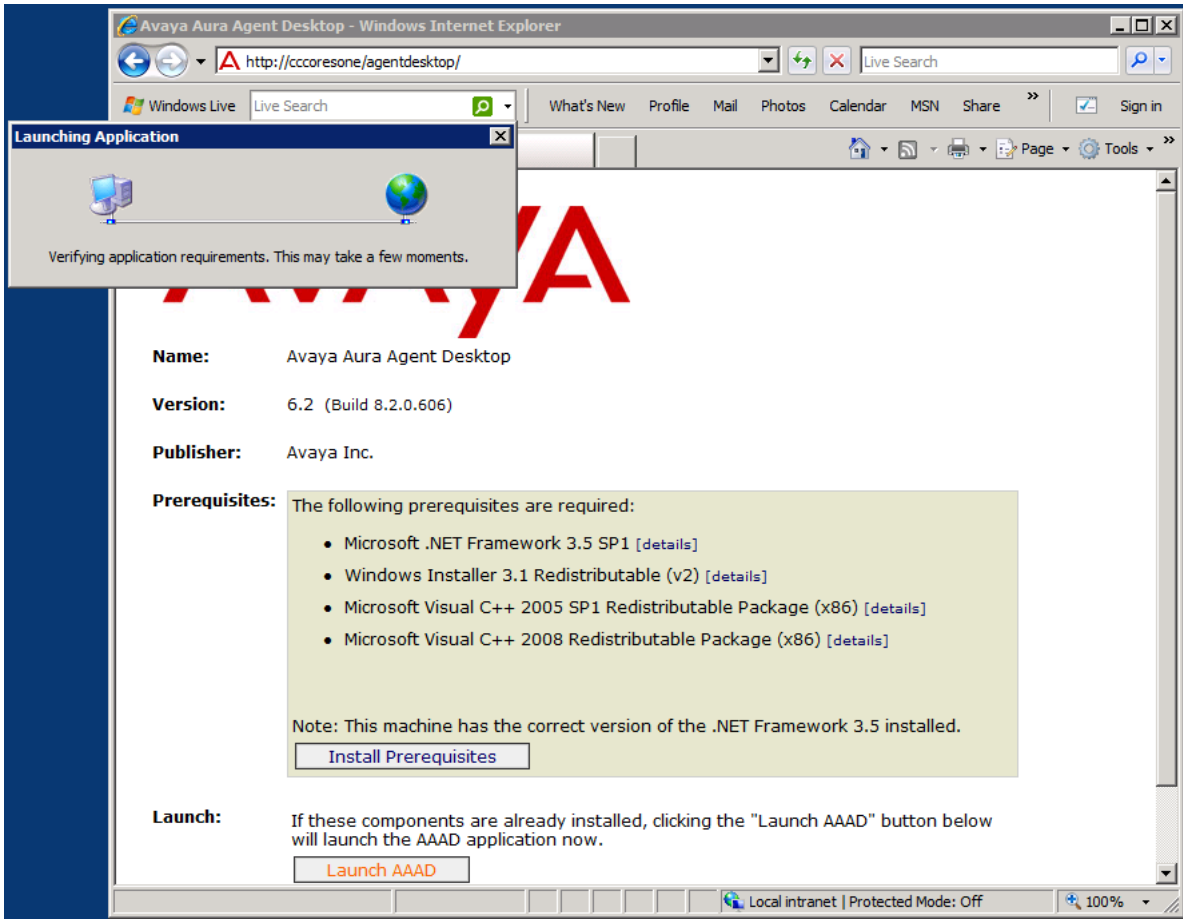
Log on to Agent Desktop on a client computer to test that Contact Center has the correct configuration to accept contacts and route them to agents.

Procedure steps

Step	Action
1	Log on to the desktop computer using the agent's domain username and password, **CCAgentOne**, **AG1_pass~2**.
2	Start Internet Explorer.
3	In Internet Explorer, in the **Address** box, type the URL of the Agent Desktop installer in the format http://<server name>/agent desktop, for example **http://cccoresone/agentdesktop**, and press **Enter**.
4	On the **Avaya Aura Agent Desktop** web page, select **Launch AAAD**.

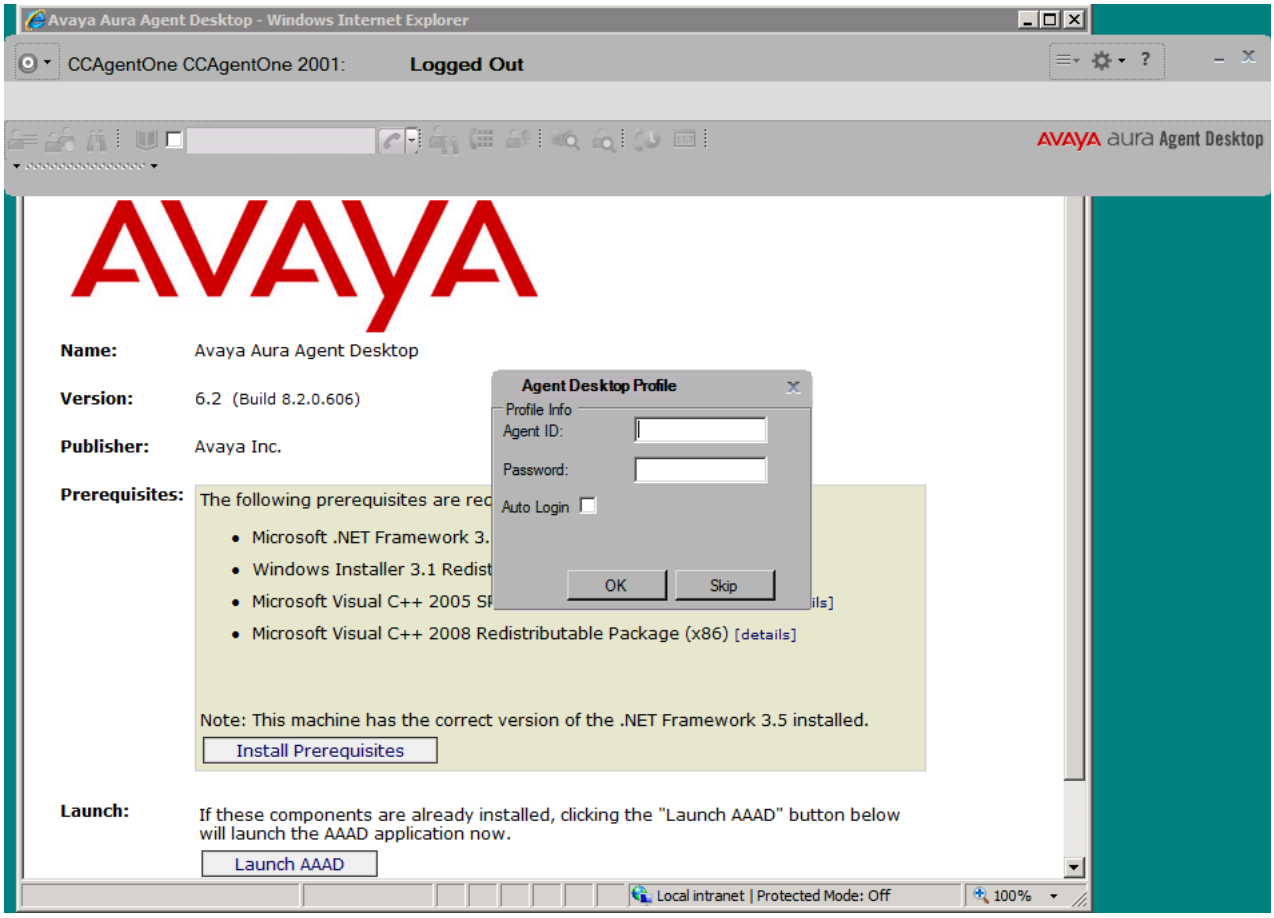


The installer displays the Launching Application dialog while it checks the application prerequisites.



5 In the **Agent Desktop Profile** dialog, in the **Agent ID** field type the agent's Contact Center ID, for example **2001**.

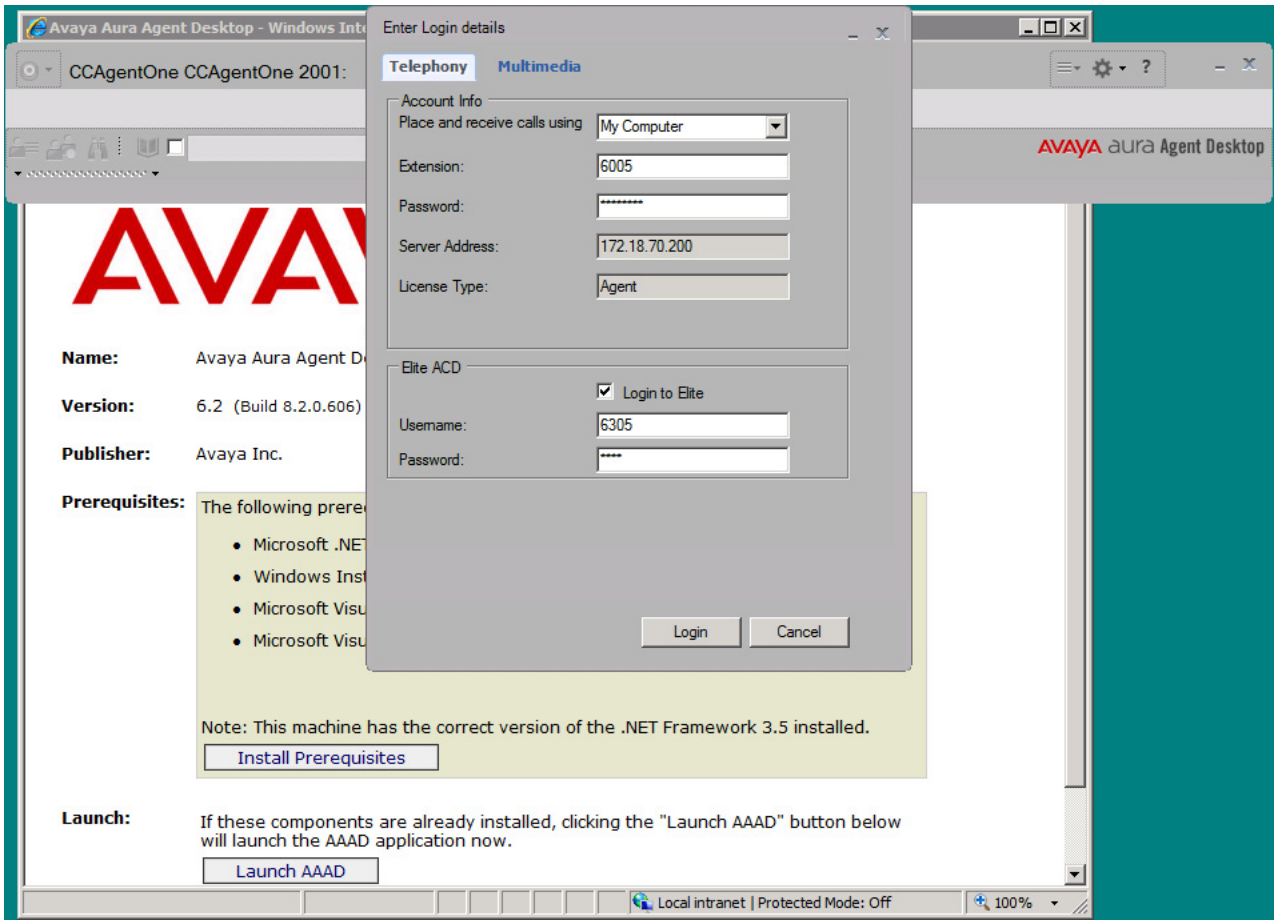
6 In the **Password** field type the agent's Contact Center password, for example **2001**.



7 Click **OK**.

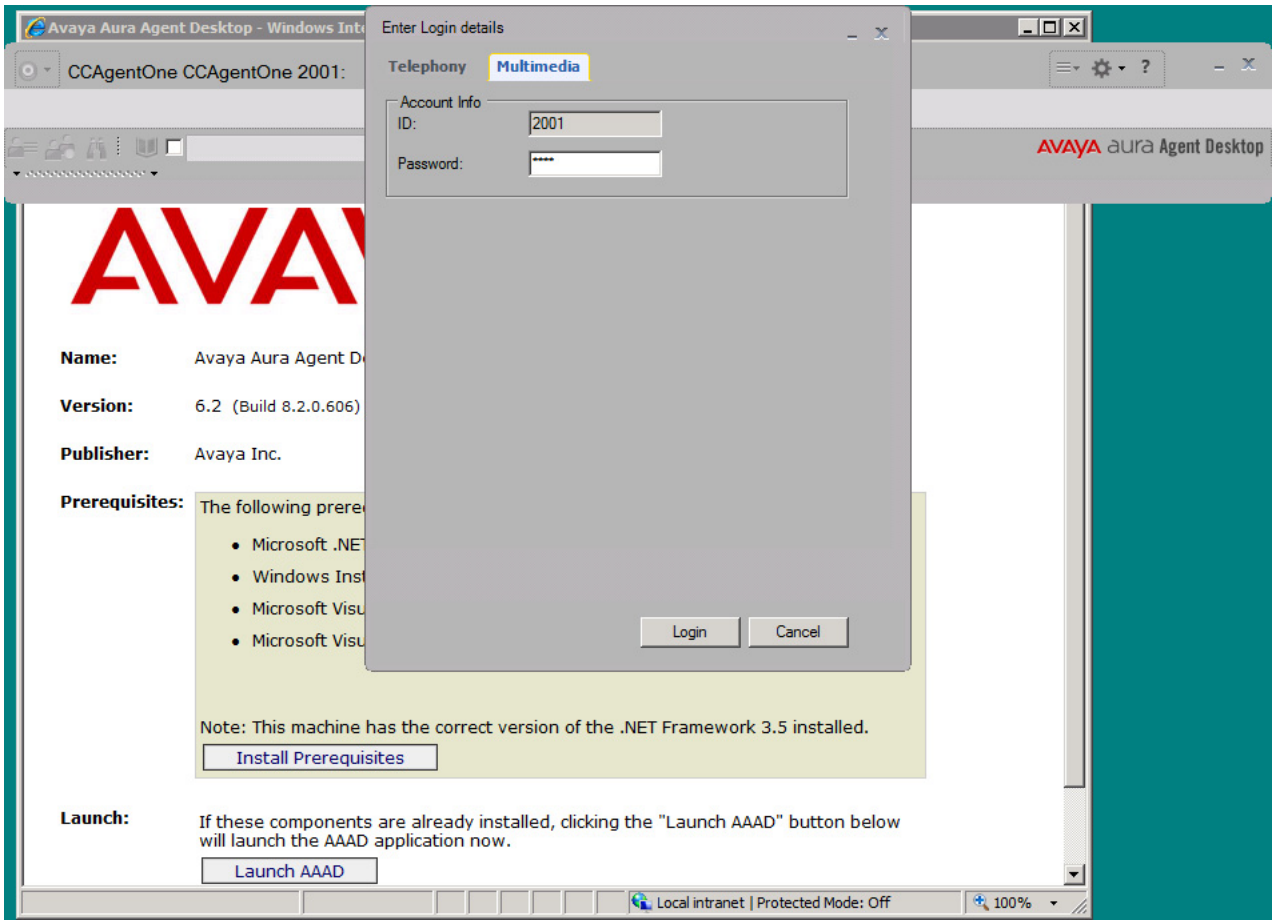
8 On the Agent Desktop Telephony Toolbar, from the **Status** list, select **Login**.





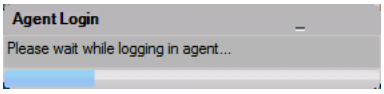
9 Click **Multimedia**.

10 On the **Multimedia** tab, in the **Password** box, type **2001**.



11 Click **Login**.

*Agent Desktop displays the **Agent Login** progress window.*



12 Ensure the agent is **Not Ready**.

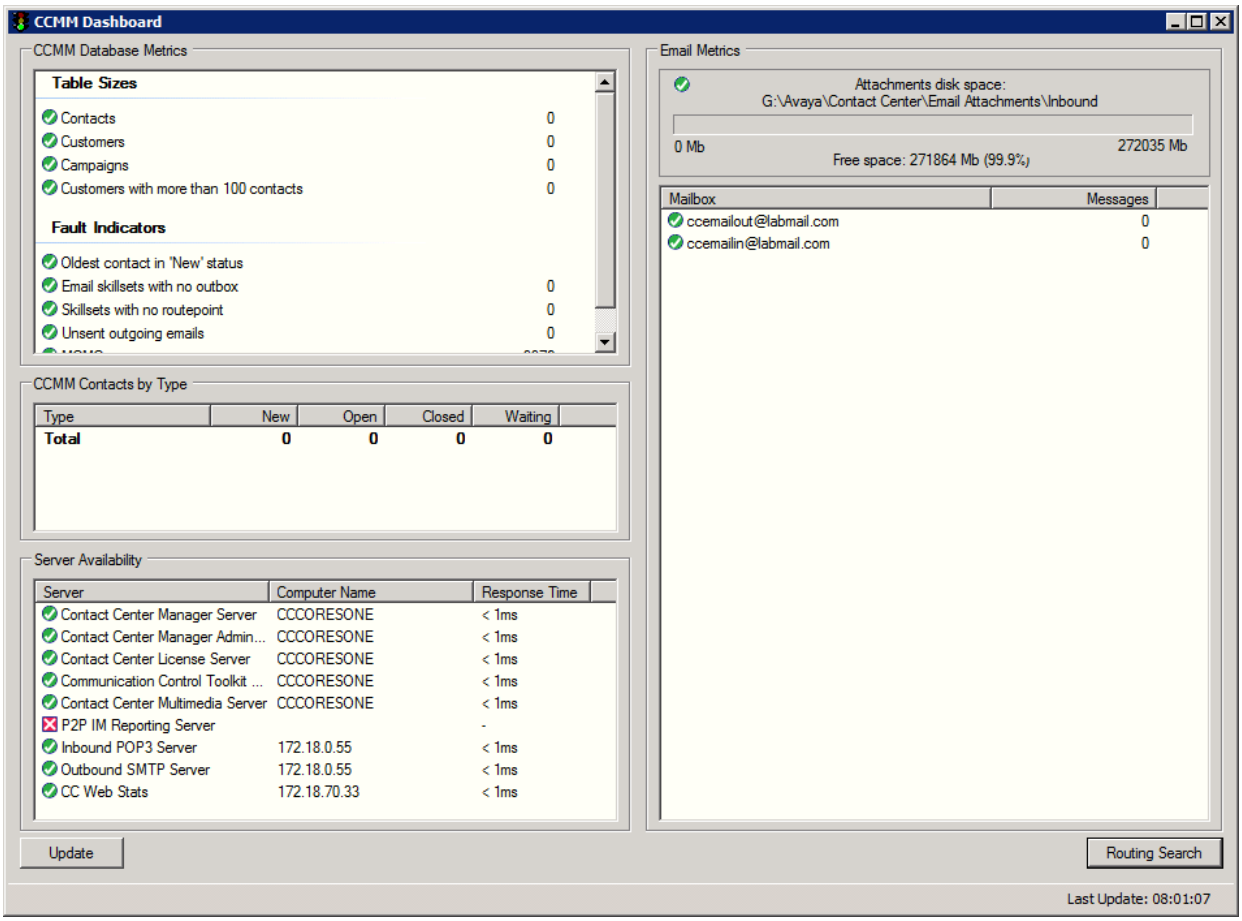
--End--

Opening the Multimedia Dashboard

Open the Multimedia dashboard to check the progress of e-mail contacts through the contact center.

Procedure steps

Step	Action
1	Log on to the Contact Center server CCcoresOne using the contact center administration account AACCinstaller.
2	Select **Start, All Programs, Avaya, Contact Center, Multimedia server, Multimedia Dashboard**.
3	Review the dashboard information in the **CCMM Database Metrics** box. You see no errors.



4	Keep the dashboard open so that you can refer to it in the following procedures.

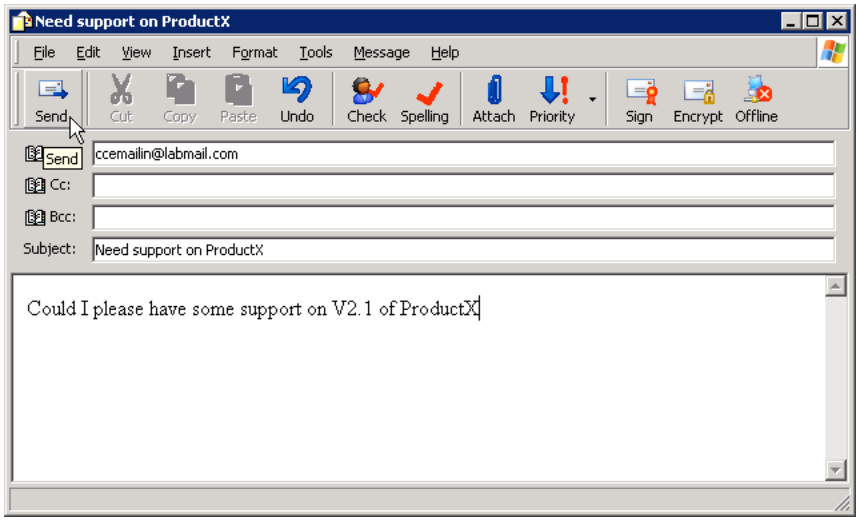
--End--

Sending a test e-mail to the Contact Center e-mail inbox

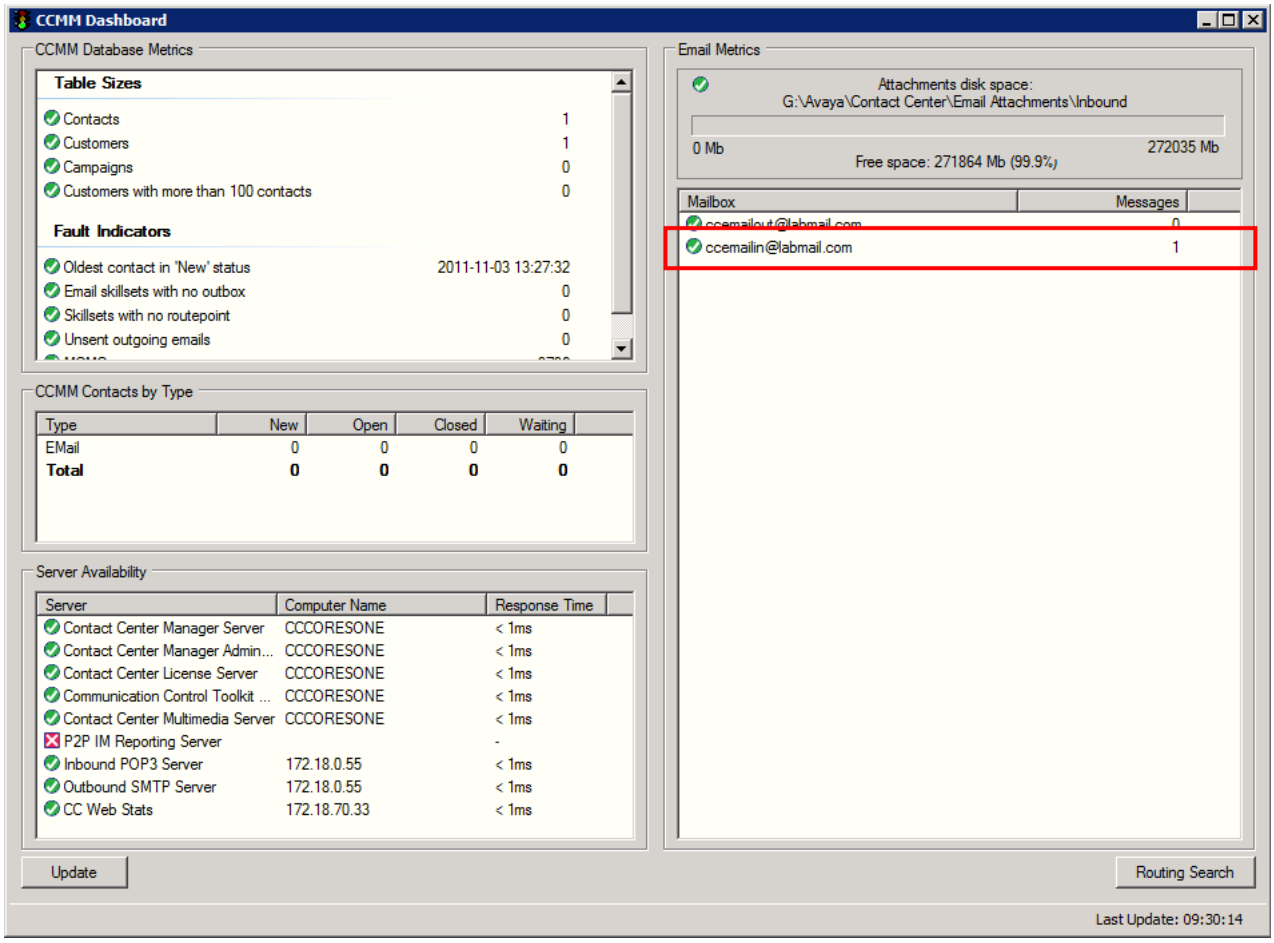
Send a test e-mail to the Contact Center e-mail inbox to verify the e-mail contact configuration and operation. Review the Multimedia dashboard to check that the e-mail message arrives at the inbox and that Contact Center processes it to create a contact.

Procedure steps

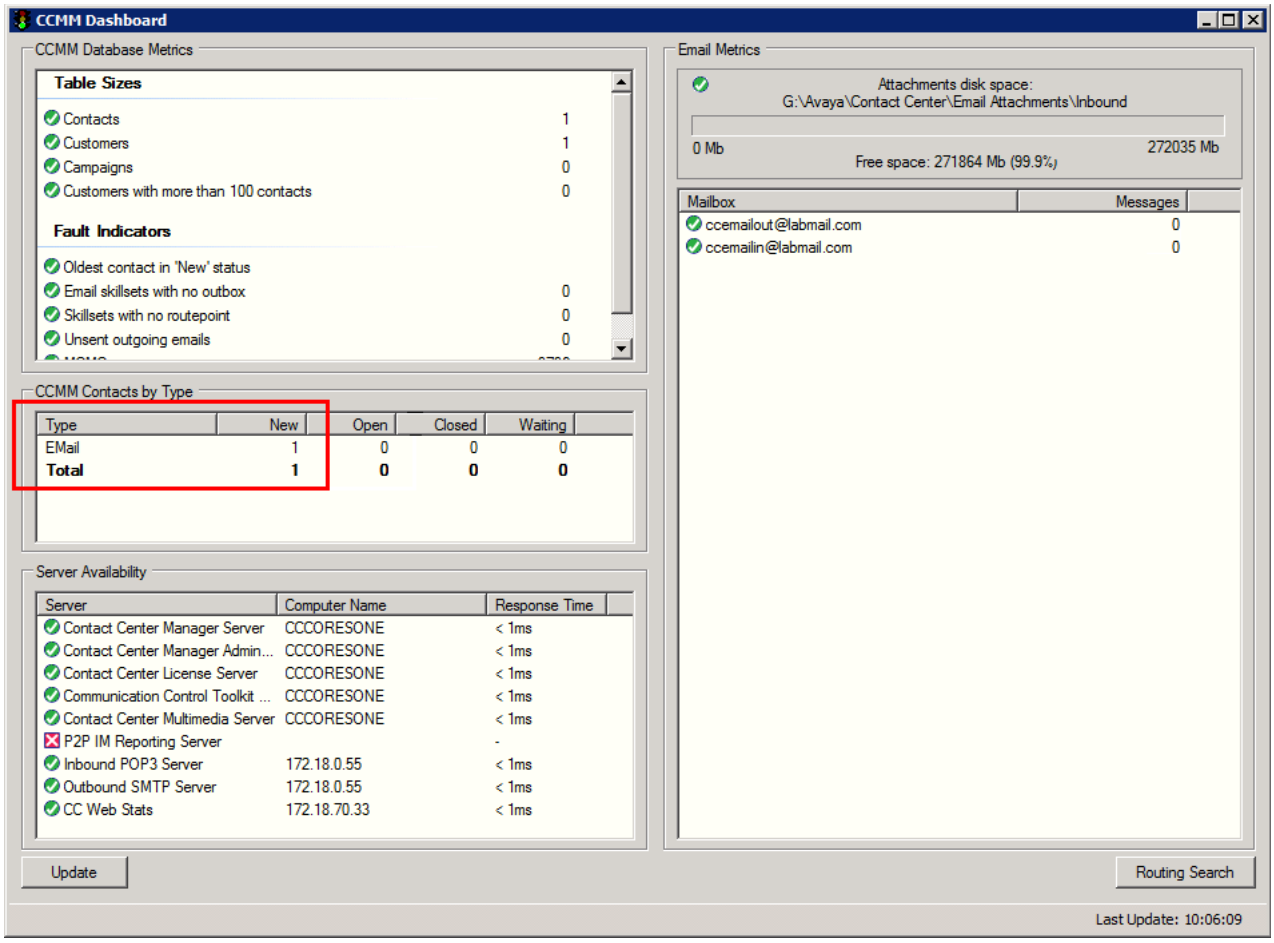
Step	Action
1	Using an e-mail client, create a new e-mail message.
2	In the **To** box, type **ccemailin@labmail.com**.
3	In the **Subject** box, type **Need support on ProductX**.
4	In the e-mail body, type **Could I please have support on V2.1 of ProductX**.



5	Click **Send**.
6	Check the Multimedia Dashboard. Under **E-mail Metrics** you see a single e-mail for the **ccemailin@labmail.com**.



7 Keep refreshing the Multimedia Dashboard by pressing F5. When the CCMM e-mail handler picks up the e-mail from the ccemailin mailbox, under CCMM Contact by type the **New** field in the **EMail** row changes to 1.



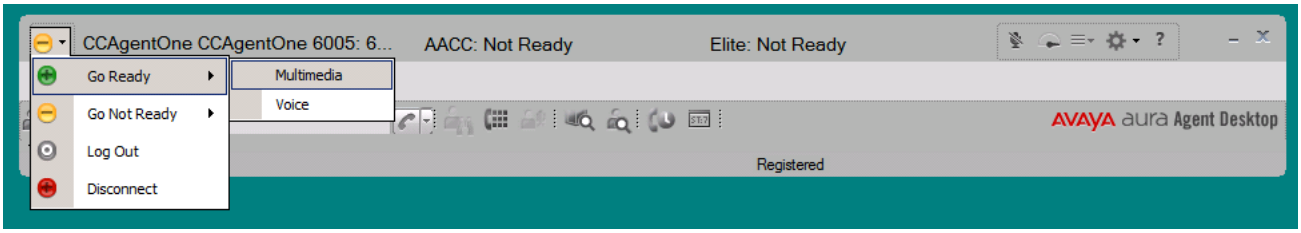
--End--

Making the agent Ready and accepting the e-mail contact

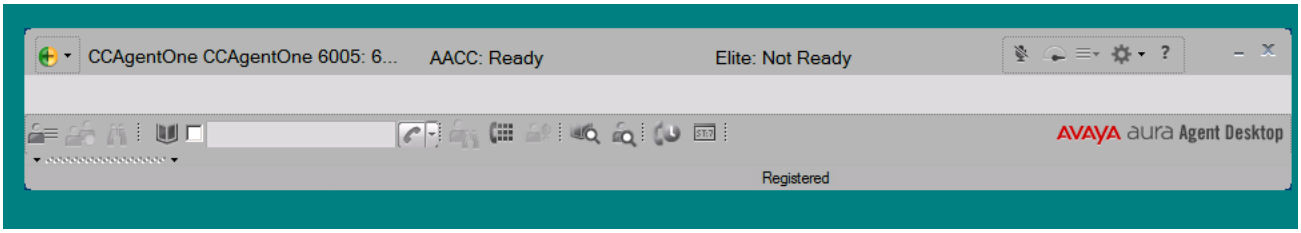
Make the agent ready and accept the e-mail contact that Contact Center offers to the agent.

Procedure steps

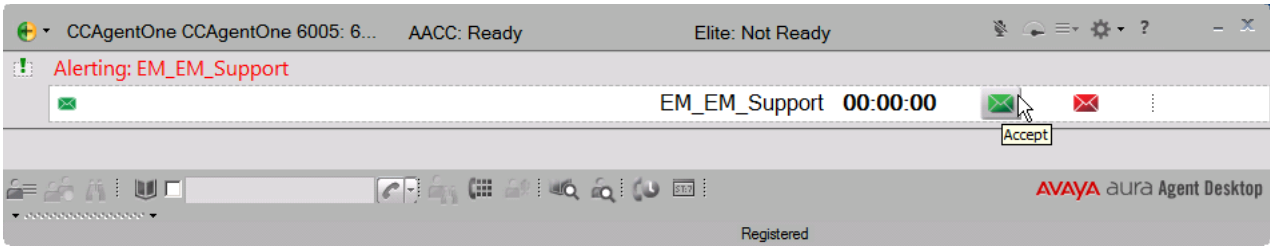
Step	Action
1	On the Agent Desktop Telephony Toolbar, from the **Status** list, select **Go Ready, Multimedia**.



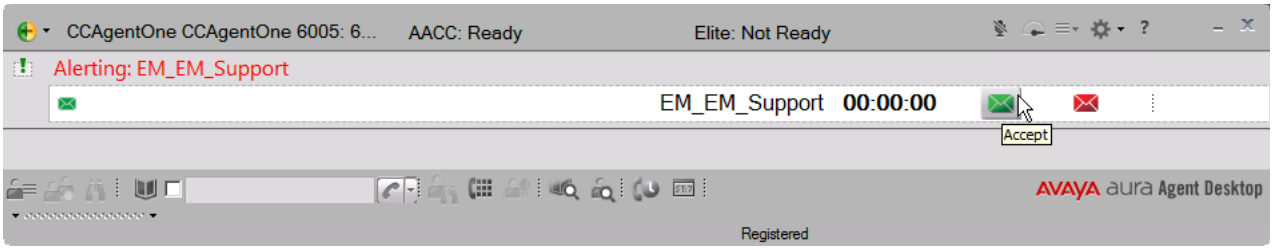
Agent Desktop sets the agent's Avaya Aura® CC status to Ready.



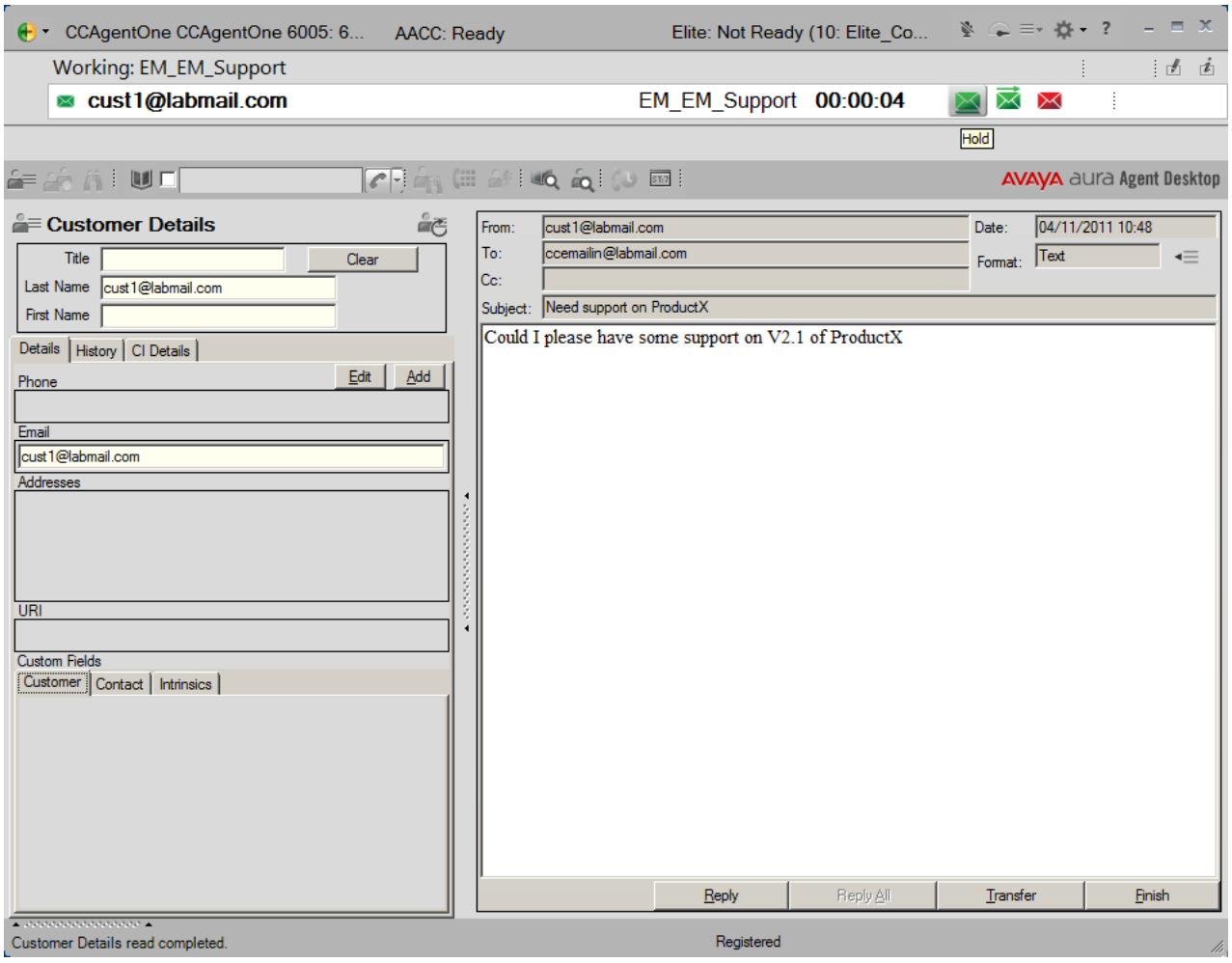
Contact Center routes the e-mail contact to this agent and the Agent Desktop alerts the agent.



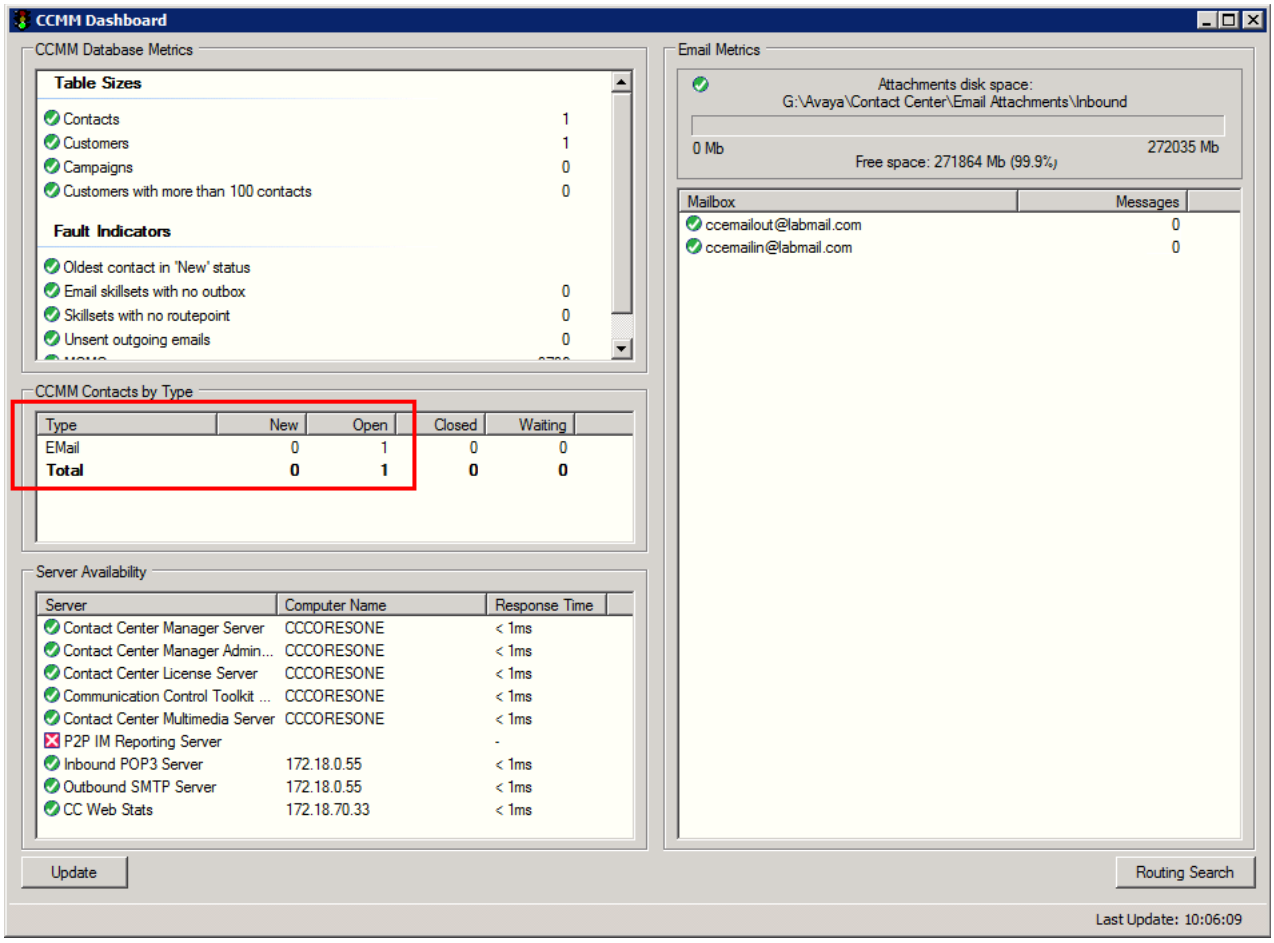
2 Click **Accept**.



Agent Desktop displays the contact details.



3 Check the Multimedia Dashboard. Under **CCMM Contacts by Type** you see one open e-mail contact.



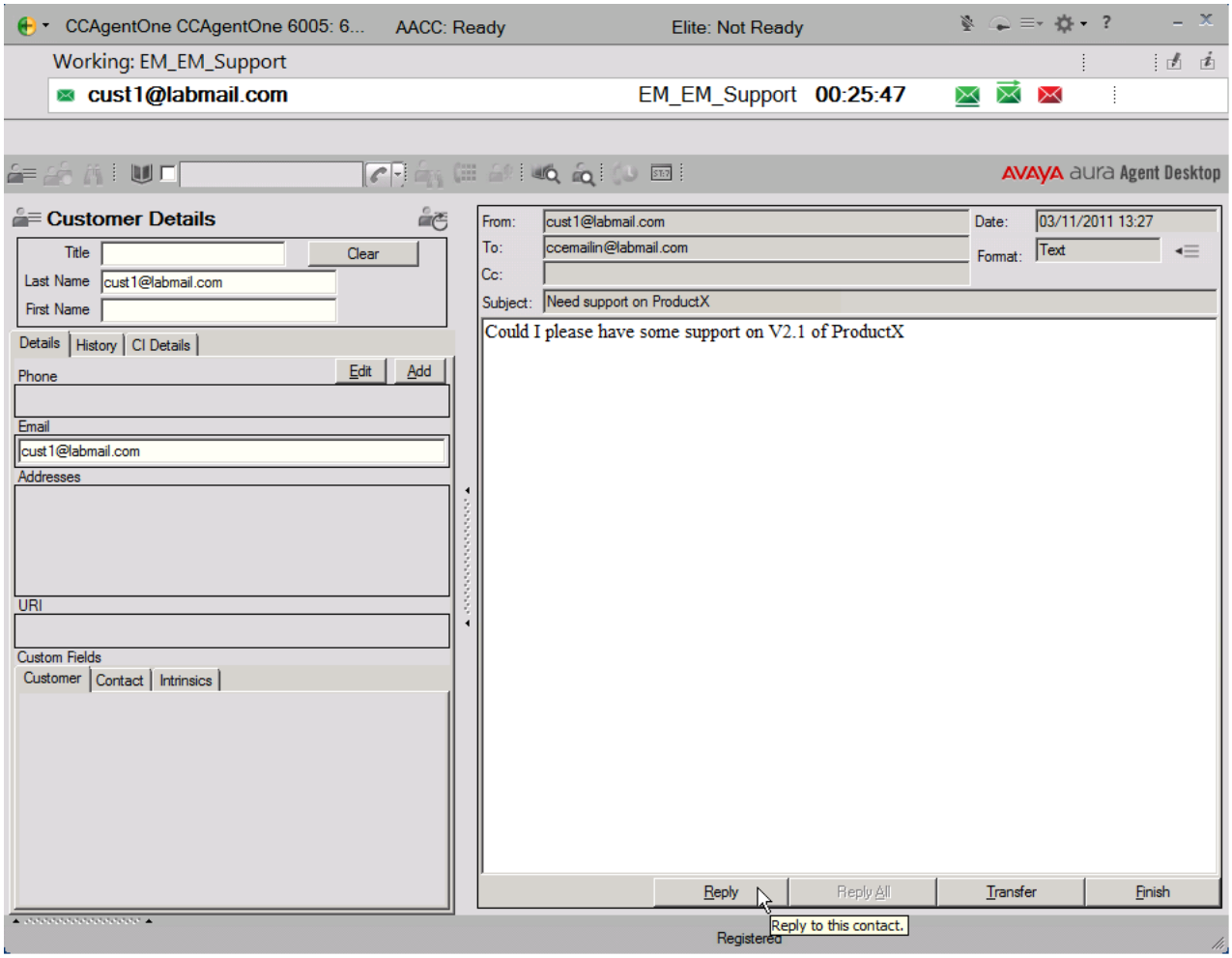
--End--

Replying to and closing the e-mail contact

Send a reply to the e-mail contact and close it, and ensure the reply gets to the mailbox that you used to send the test e-mail.

Procedure steps

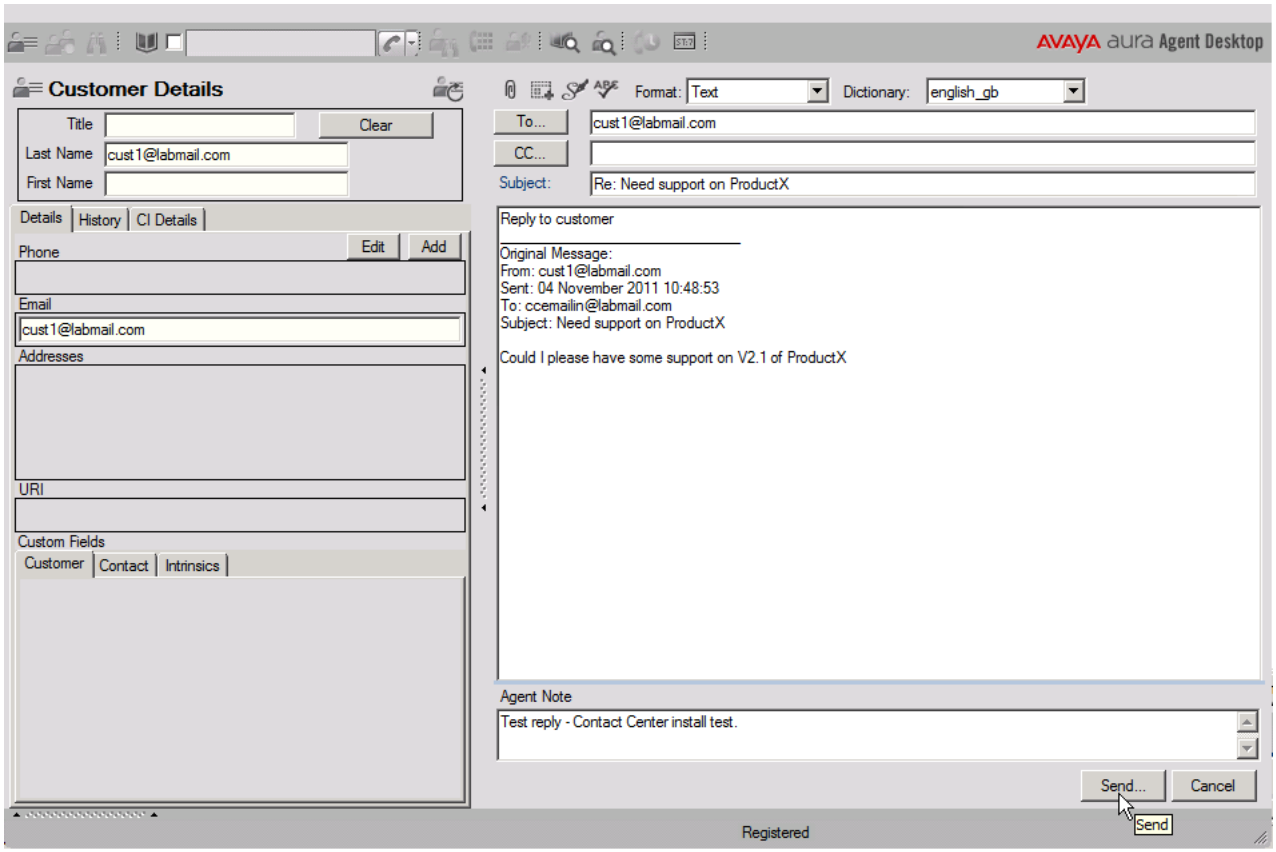
Step	Action
1	On the e-mail contact screen, click **Reply**.



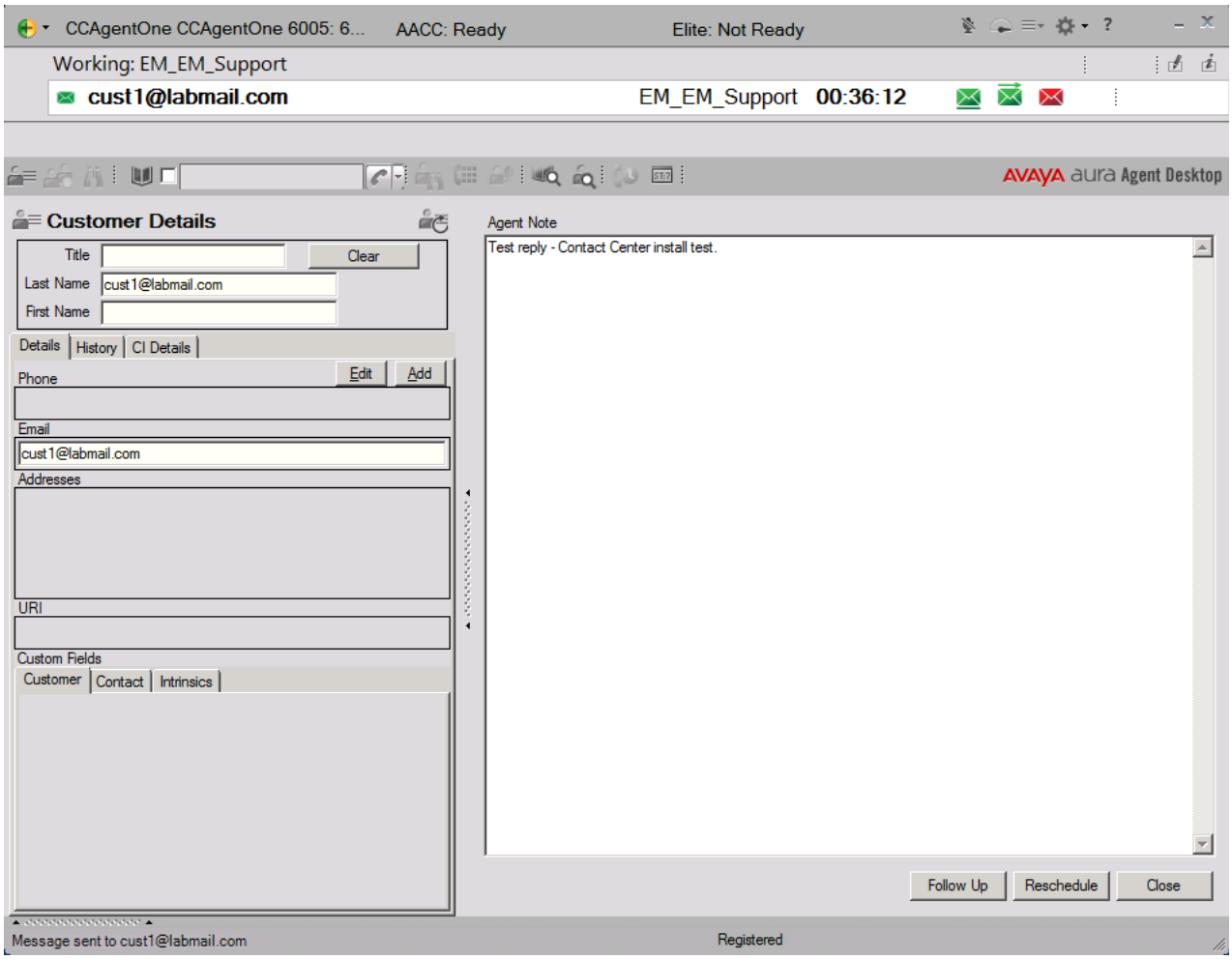
2 In the e-mail body box, type **Reply to customer**.

3 In the **Agent Note** box, type **Test reply - Contact Center install test.**

4 Click **Send**.

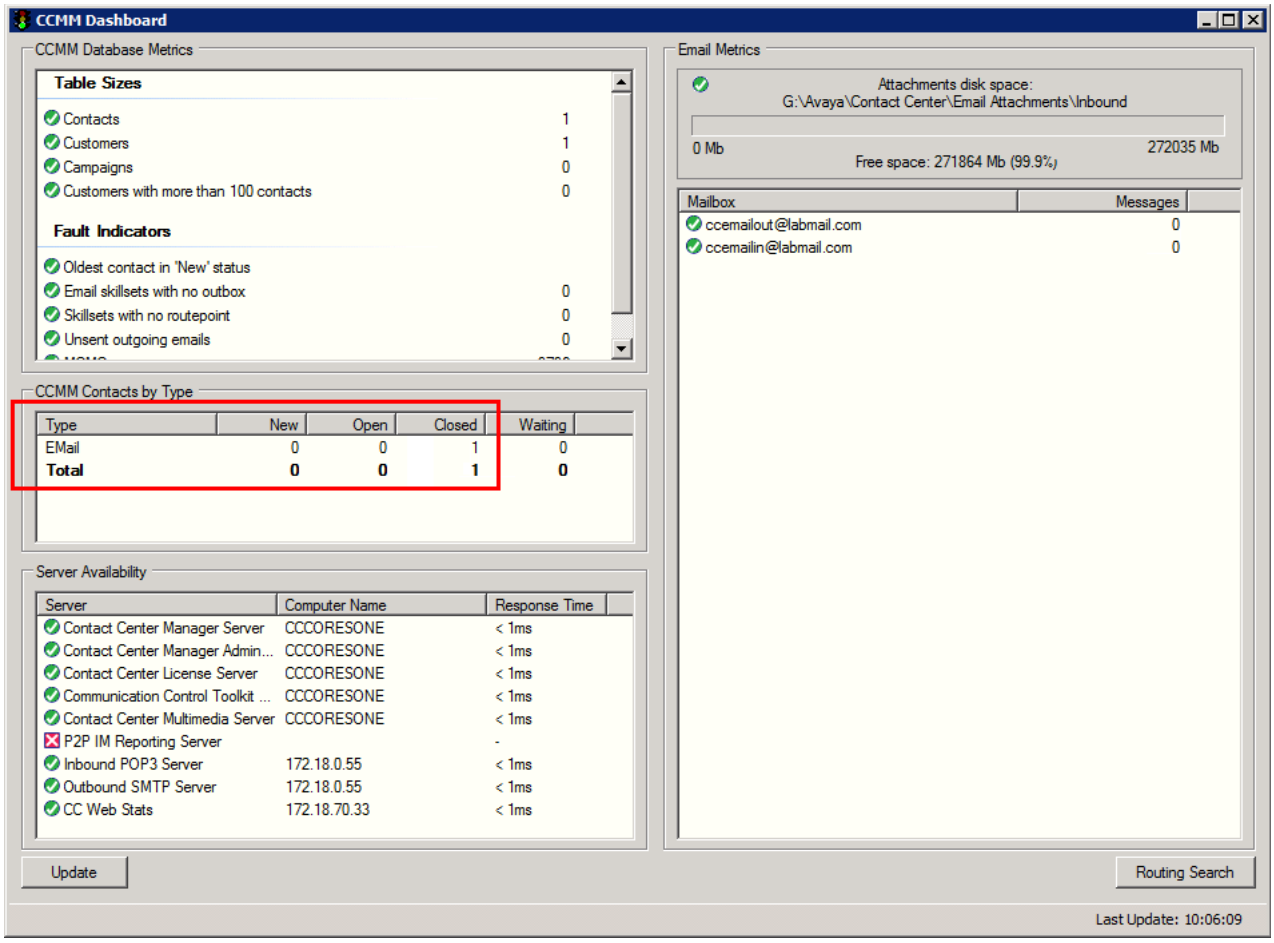


Agent Desktop displays the contact details.



5 Click **Close**.

6 Check the Multimedia Dashboard. Under **CCMM Contacts by Type** you see one closed e-mail contact.



7 On the Agent Desktop Telephony Toolbar, from the **Status** list, select **Go Not Ready, Multimedia**.

--End--

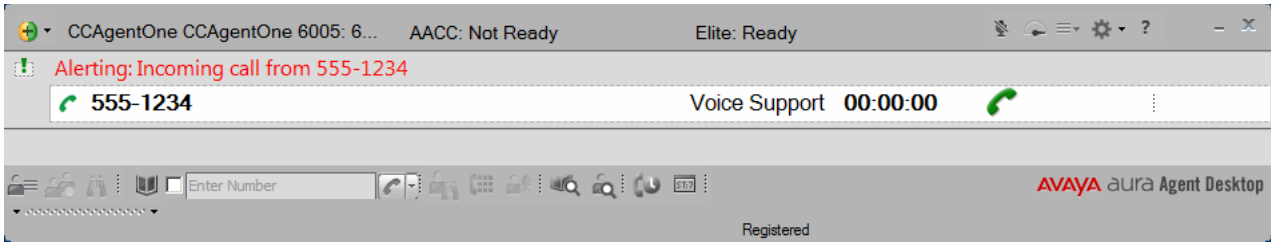
Testing a Call Center Elite voice call by answering it on Agent Desktop

Make a voice call to the agent's Call Center Elite VDN and answer it on Agent Desktop.

Procedure steps

Step	Action
1	From a station on the CM, make a call to a VDN to which the agent is assigned.
2	On the Agent Desktop Telephony Toolbar, from the **Status** list, select **Go Ready, Voice**.

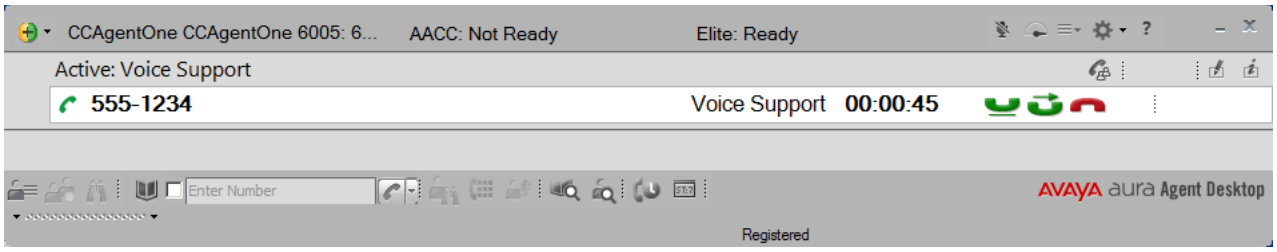
Call Center Elite routes the call to the agent and Agent Desktop shows an alerting status.



3 On the voice contact, click **Accept**.



Agent Desktop answers the call.



--End--

Accepting a Multimedia Contact while on the voice call

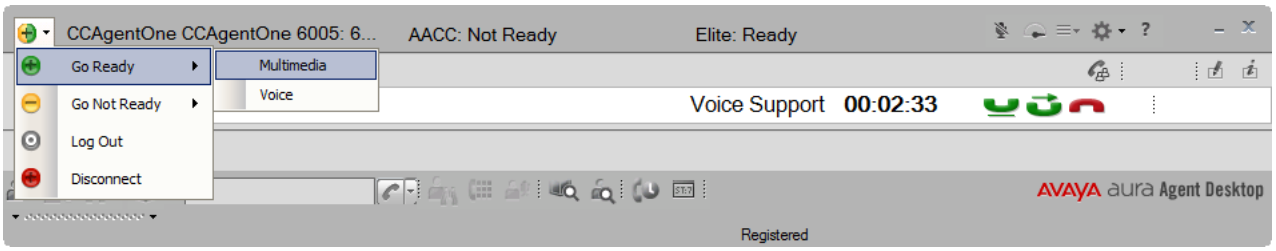
Go ready on Avaya Aura® CC Multimedia and accept an e-mail contact while the voice call is still active on Agent Desktop.

Procedure steps

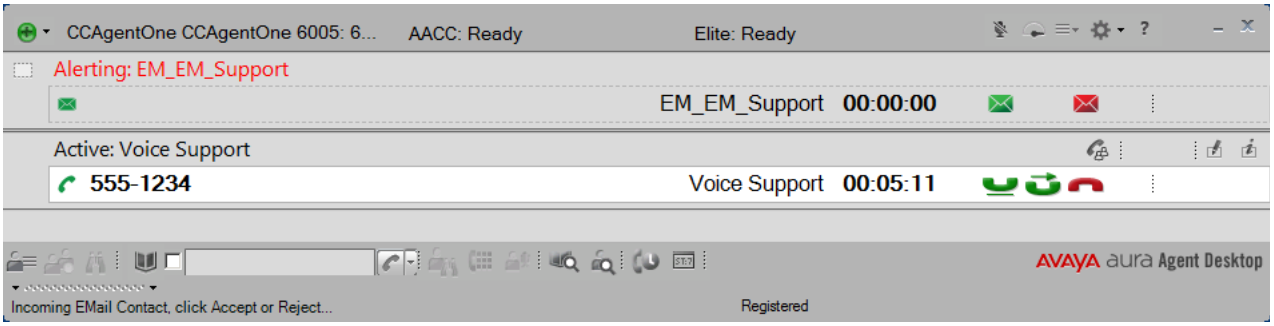
Step	Action
1	Using an e-mail client, create a new e-mail message.
2	In the **To** box, type **ccemailin@labmail.com**.
3	In the **Subject** box, type **Need support on ProductX**.

4 In the e-mail body, type **Could I please have support on V2.1 of ProductX**.

5 On the Agent Desktop Telephony Toolbar, from the **Status** list, select **Go Ready, Multimedia**.

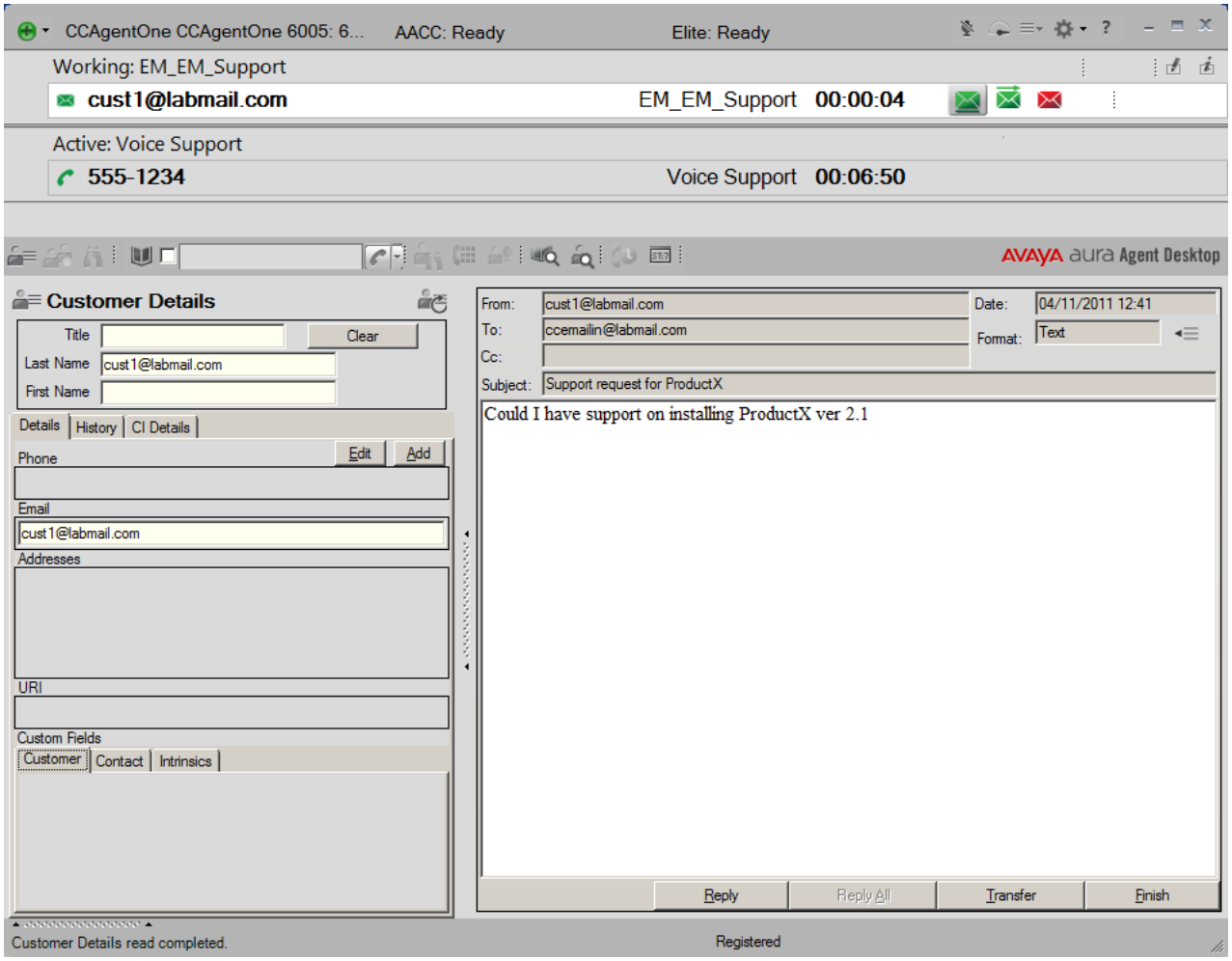


Agent Desktop sets the agent's Avaya Aura® CC status to Ready. Contact Center routes the e-mail contact to this agent and the Agent Desktop alerts the agent.



6 Click **Accept**.

Agent Desktop displays the e-mail contact details.



7 Hang up the voice contact.

8 Reply to and close the e-mail contact.

--End--

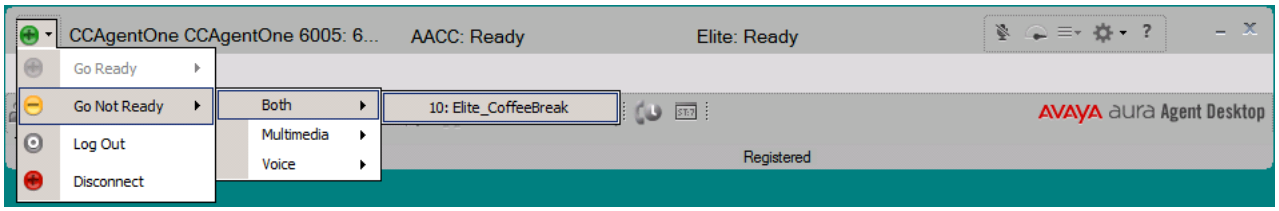
Making the agent not ready

Make the agent not ready on both voice and multimedia to show that the activity code mapping is correct.

Procedure steps

Step	Action

1 On the Agent Desktop Telephony Toolbar, from the **Status** list, select **Go Not Ready, Both, 10:Elite_CoffeeBreak**.



The agent status changes to Not Ready for both Avaya Aura® CC and Elite.

2 In the Top Bar, review the activity codes. Agent Desktop displays the native Elite and Contact Center codes that map to the code selected.



3 If you want to see the full description of the Elite Aux Work code or the Contact Center activity code, place the mouse over the code and Agent Desktop displays a tooltip with the complete description.



--End--

High Availability Section

High Availability pre-install configuration

This chapter describes the initial configuration you carry out to prepare a CCMM Complement solution for implementing High Availability. This includes configuring the windows accounts used by Contact Center Manager Administration (CCMA) replication in your Avaya Aura® Contact Center solution. It also describes how to update the Contact Center license file for High Availability.

Perform the procedures in this chapter on the Active Avaya Aura® Contact Center co-resident server.

Adding High Availability to a CCMM Complement solution

The following topics outline how you add another server to the CCMM Complement solution to implement High Availability.

Overview of the components in the example solution with High Availability

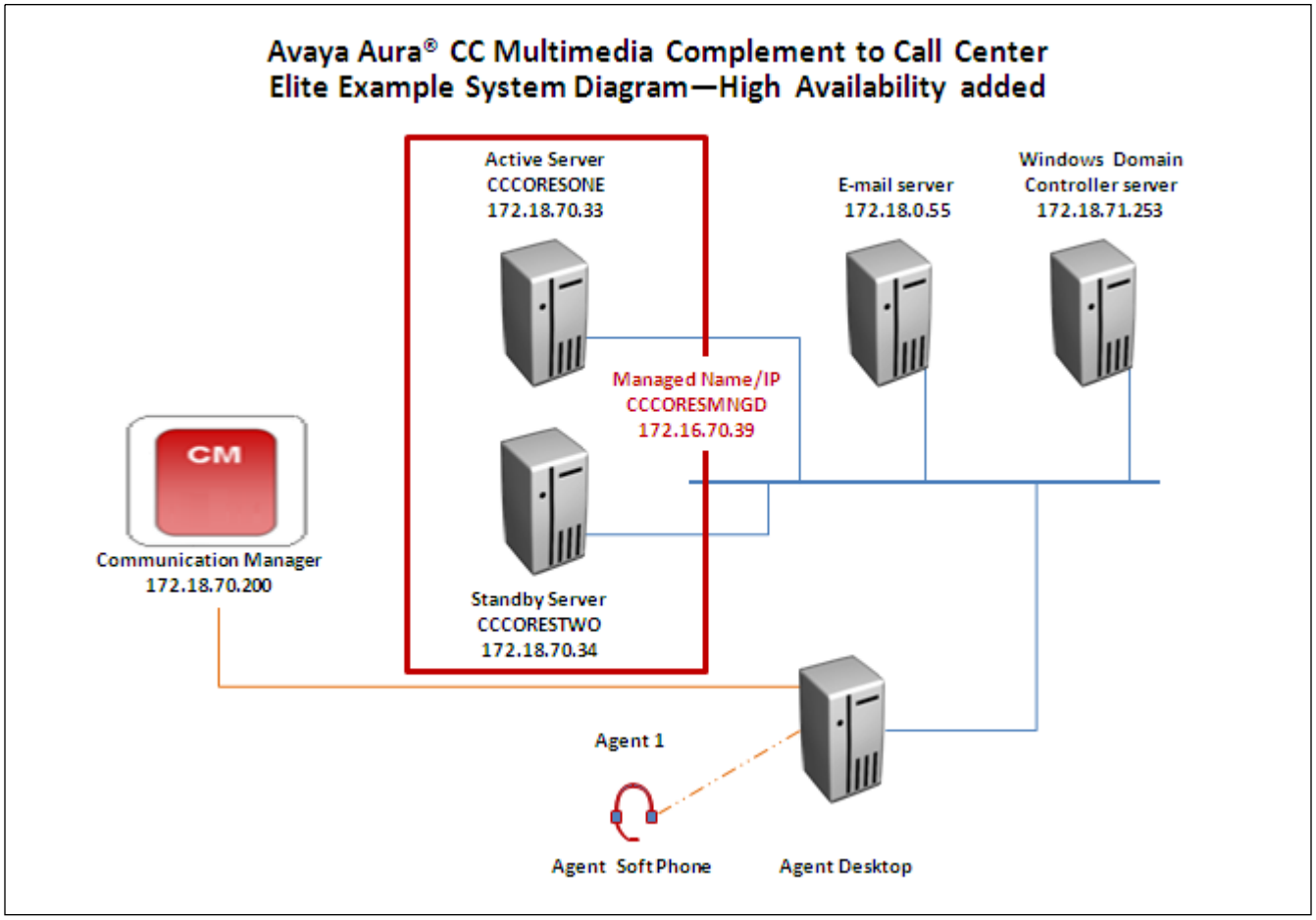
To add HA to the example solution described in this Deployment Guide, you require an additional server.

Implementing a Standby server gives resiliency for the Contact Center server. The Standby Contact Center server monitors and shadows the Active Contact Center server but does not process contacts. If the Active server fails, the Standby server recognizes the failure. It initiates a switchover, changes to active mode, and starts processing multimedia contacts. In a Warm HA solution, when the Standby server initiates a switchover, all agents must log off Agent Desktop, and log back in again. Contact Center re-queues all in-progress Multimedia contacts so that they become available to agents when they log back in.

This guide uses the term Active server for the original server, and Standby server for the additional server. When a server is processing contacts it is in active mode, and when it is monitoring and shadowing, it is in standby mode. Thus, after a switchover, the Standby server is in active mode.

When the Active server failure is corrected, the Active server can start in standby mode and monitor and shadow the Standby server.

Contact Center Multimedia Complement with HA system diagram



Contact Center configuration with High Availability

High Availability requires an additional Contact Center server, CCCORESTWO, configured to exactly match the original Contact Center server. The Standby Server has the same applications as the Active server, as follows:

- Contact Center Manager Server
- Contact Center Manager Administration
- Communication Control Toolkit
- Contact Center Multimedia
- Contact Center License Manager
- Orchestration Designer
- Contact Center Manager Server Utility

High Availability also requires an additional IP address and virtual computer name, termed the Managed IP address and the Managed Name. In this example the Managed IP address is 172.18.70.39, and the Managed Name is CCCORESMNGD. All applications connecting to a High Availability Contact Center connect using the Managed IP address or the Managed Name. The server that is in active mode communicates with all other network hosts using the Managed IP address and Managed Name.

Example server details	
Active server name	CCCORESONE
Active server IP Address	172.18.70.33
Standby server name	CCCORESTWO
Standby server IP Address	172.18.70.34
Managed server name	CCCORESMNGD
Managed IP Address	172.18.70.39

You complete the initial configuration of the Standby server using the server's unique name and IP address, CCCORESTWO and 172.18.70.34 respectively. You configure the Managed IP address and the Managed Name when you commission HA.

Call Center Elite configuration with High Availability

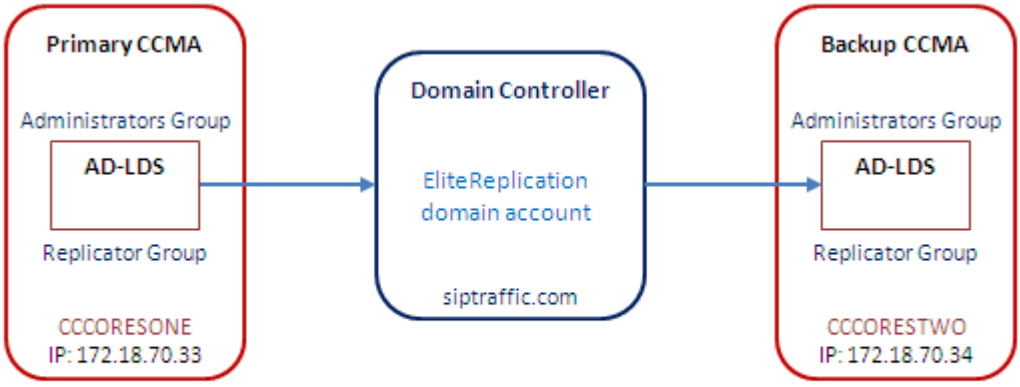
The Contact Center HA configuration does not affect the Call Center Elite configuration. The scope of the Contact Center HA feature includes only the Contact Center servers.

CCMA Replication

The addition of a replication or standby CCMA server provides Contact Center Manager Administration (CCMA) redundancy. 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, using AD-LDS replication to maintain a copy of the primary CCMA configuration data. If the active CCMA fails, the standby CCMA has all Contact Center configuration 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\EliteReplication for CCMA replication



The siptraffic\EliteReplication domain user account is a member of the Administrators Group and the Replicator Group on both Contact Center servers. AD-LDS uses this account to replicate CCMA data.

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

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 replicates 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 server. 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.

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

Attention: If the primary CCMA server has a failure that requires a complete rebuild of the server, because the database contains the schema and settings of a primary server, you must have a backup created from the primary server. You cannot use a backup from a secondary CCMA server to rebuild a primary server. Ensure you permanently keep a backup of the primary CCMA server to allow for this situation.

Domain environments

When both CCMA servers are in domain, 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\EliteReplication.
- Assign this domain user account to the local Administrators and local Replicator groups on both CCMA servers.

If the active server is co-resident with Contact Center Manager Server (CCMS) and Communication Control Toolkit (CCT), you must install CCMS, CCT, and CCMA on the standby server. All applications must be on the same patch level.

Licensing for High Availability

In a High Availability solution, both the Active and the Standby servers have License Manager and also have a local copy of the Contact Center license file. If you want to add High Availability to a Multimedia Complement for Call Center Elite, you must get an updated license file.

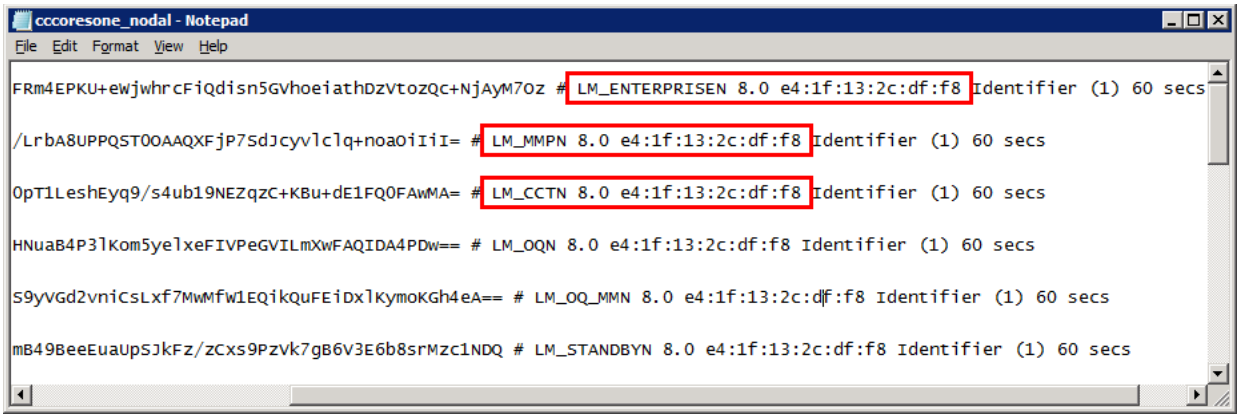
HA is a licensed feature. In addition, a license file for a HA solutions contains both the MAC address of the Active server and the MAC address of the Standby server. When you order the updated license file, you must:

- request the HA feature

- supply the MAC address of the Standby server

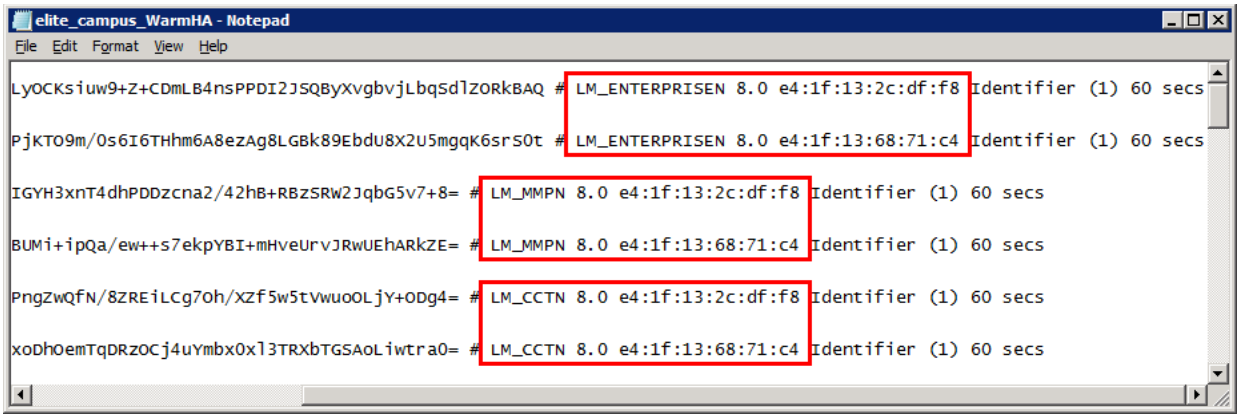
In a license file for a non-HA Contact Center solution, there is a single line for each license key, containing the MAC address of the Contact Center server.

Example of a license file for a non-HA Contact Center solution



In a license file for a HA Contact Center solution, there are two lines for each license key, one containing the MAC address of the Active server, and one containing the MAC address of the Standby server.

Example of a license file for a HA Contact Center solution



Before installing the Standby server, replace the existing license file on the Active server with the updated license file.

Adding the domain AD-LDS replication account to the Active server administrators and replicator group

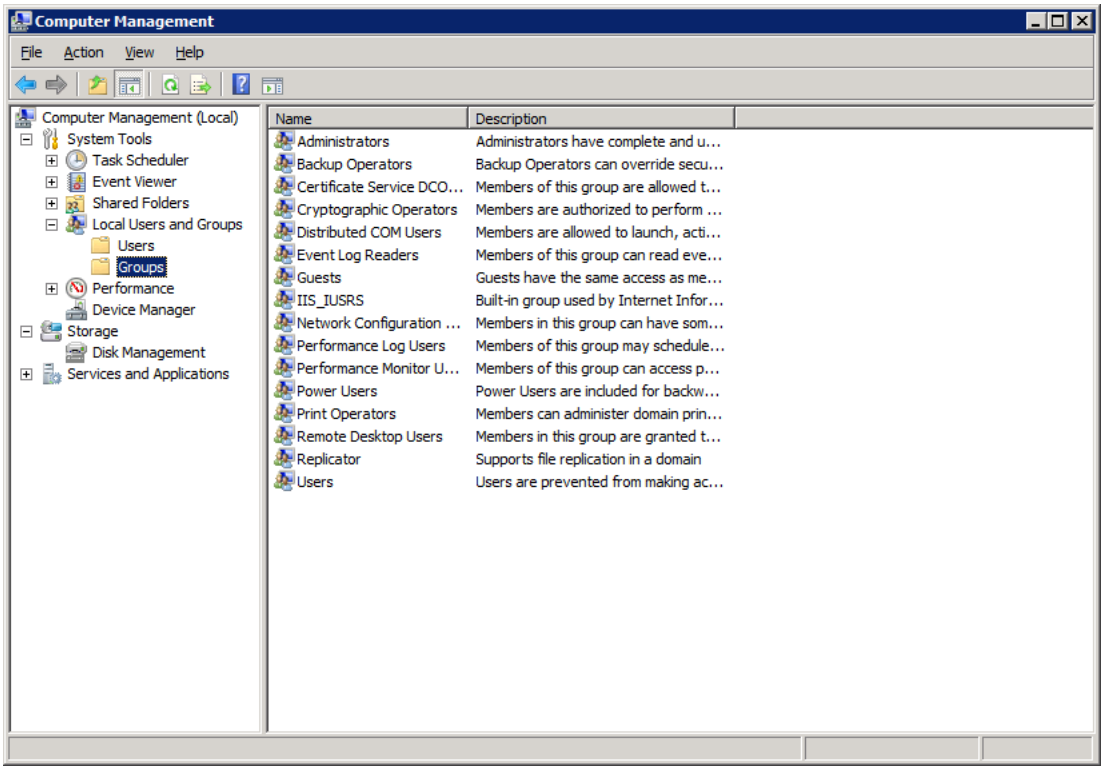
Add the AD-LDS replication account to the local Administrators and replicator group on the Active CCMA server.

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.

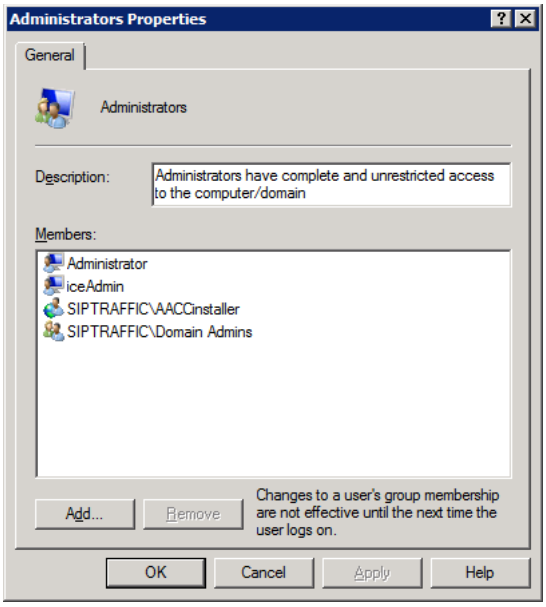
For this procedure, the name of the AD-LDS replication account is siptraffic\EliteReplication. You can choose another name for the account.

Procedure steps

Step	Action
1	Log on to the Active server (for example, **CCCORESONE**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Click **Start**, **Administrative Tools**, **Computer Management**.
3	In the **Computer Management** window, expand **Local Users and Groups**.
4	Click the **Groups** folder.

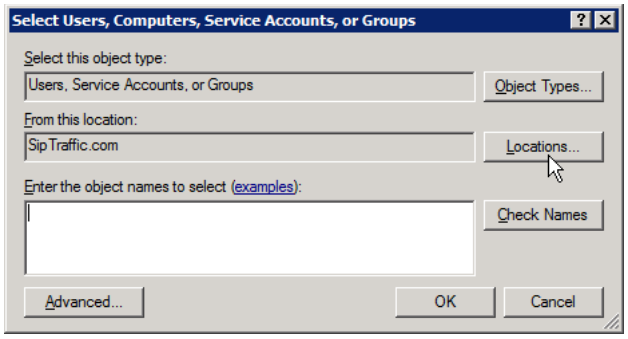


5	Double-click on the **Administrators** group.

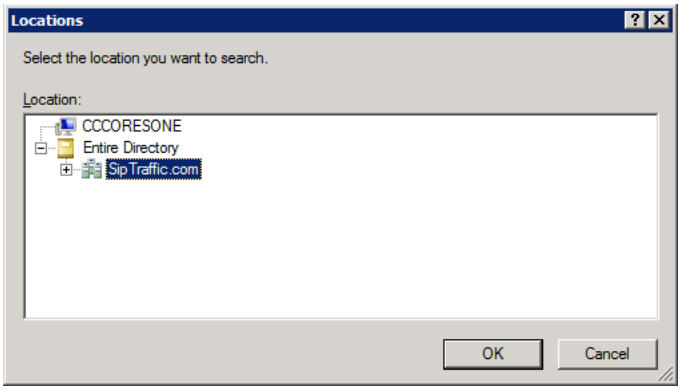


6 On the **Administrators Properties** window, click **Add**.

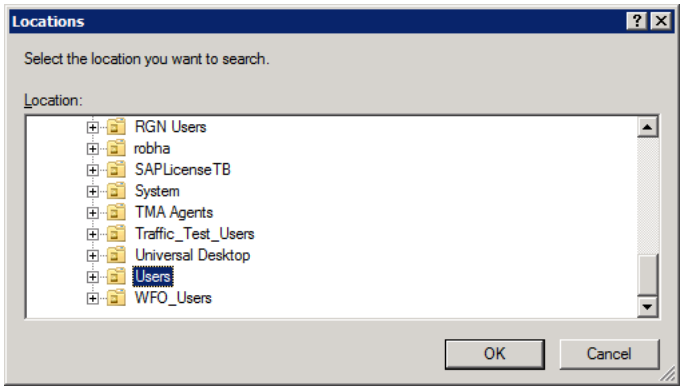
7 On the **Select Users**, **Computers**, **Service Accounts**, **or Groups** window, **click Locations**.



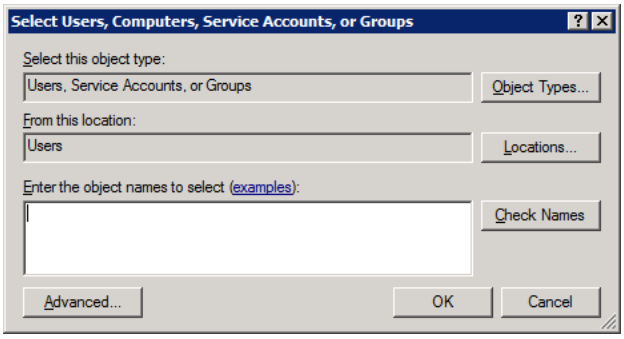
8 On the **Locations** dialog, select the domain for CCMA to use for replication, for example **siptraffic.com**.



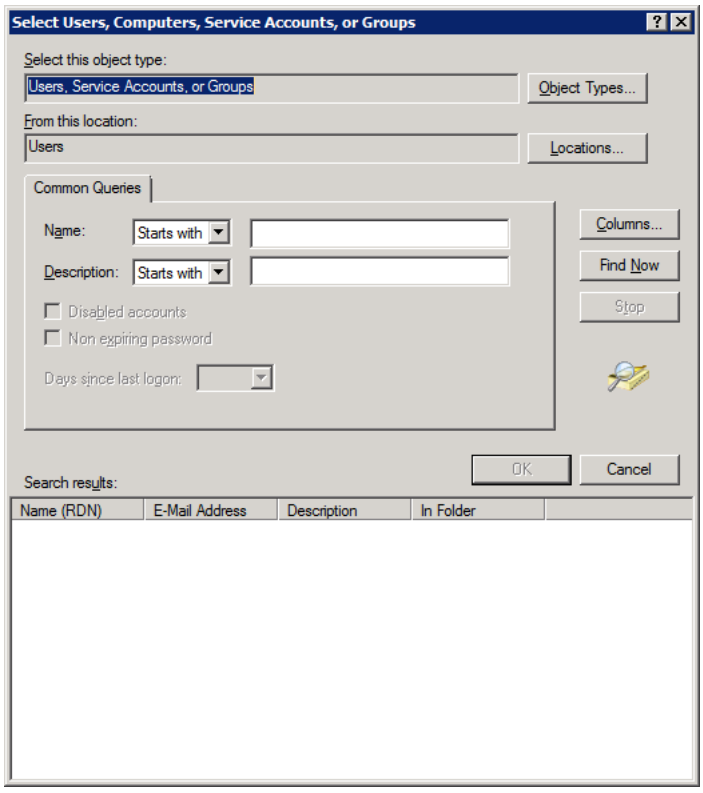
9 Expand the domain folder, scroll down and select **Users**.



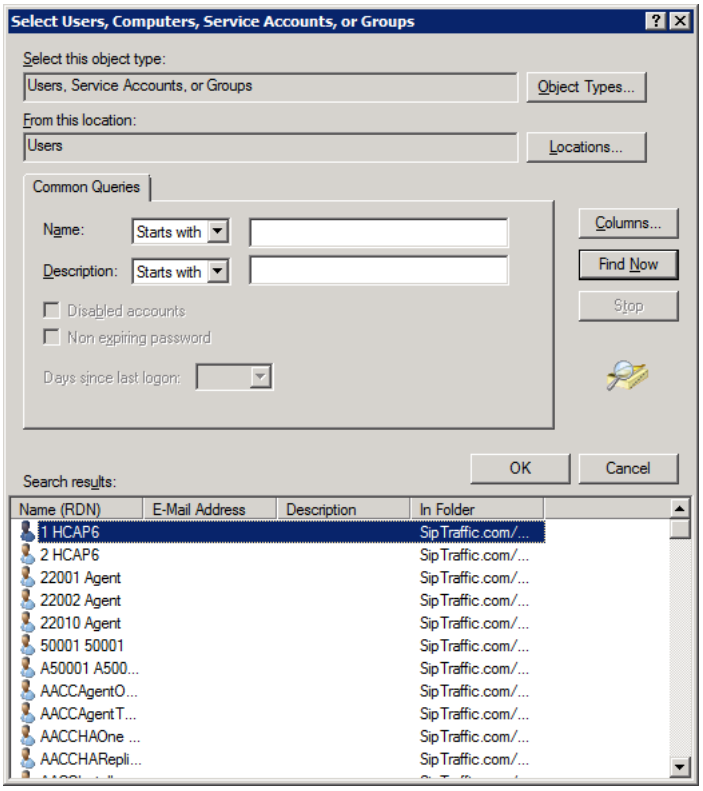
10 Click **OK**.



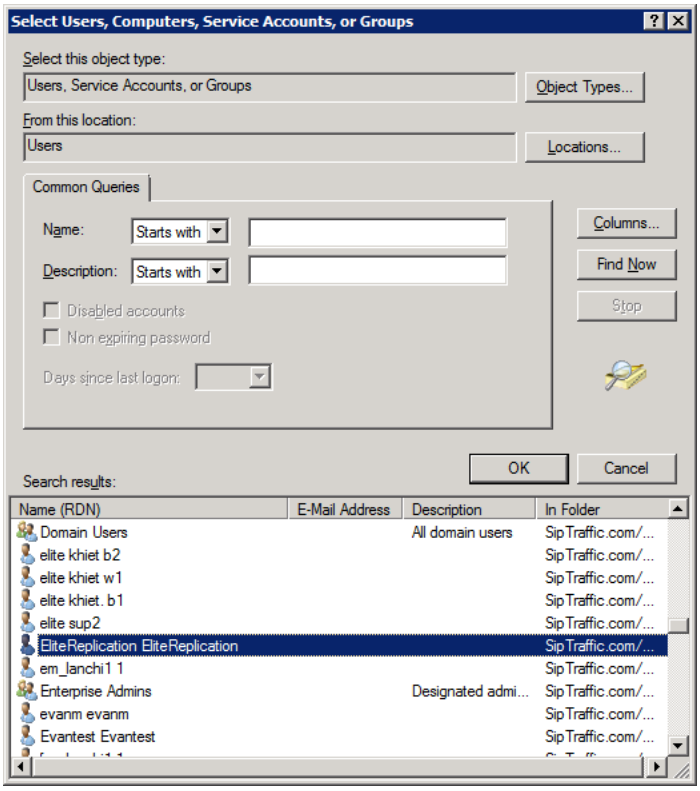
11 Click **Advanced**.



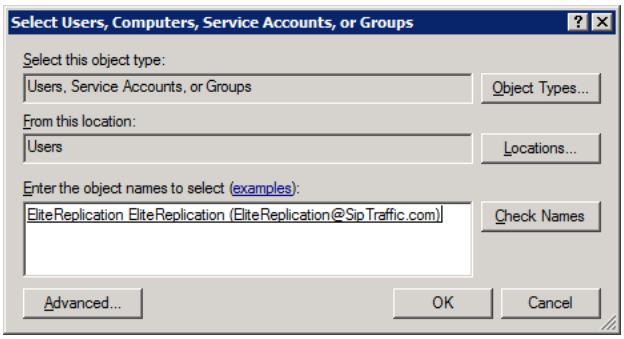
12 Click **Find Now**, to display domain users.



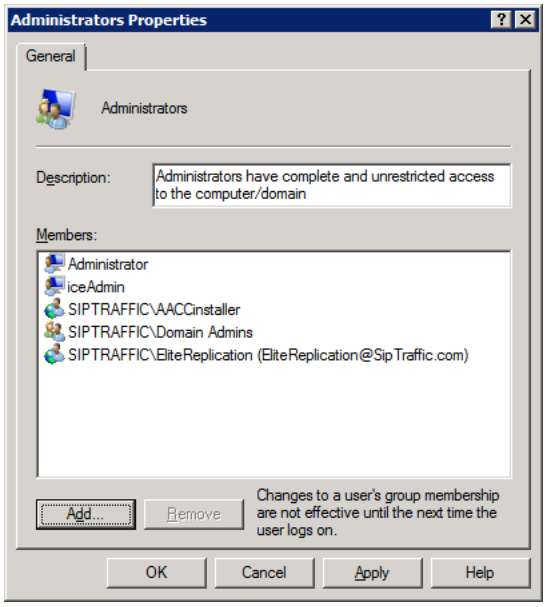
13 From the list of domain users select the CCMA replication domain user account, for example **siptraffic\EliteReplication**.



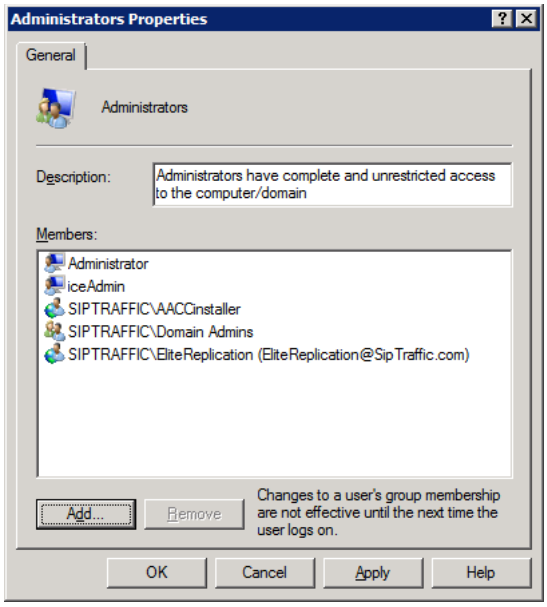
14 Click **OK**.



15 Click **OK**.

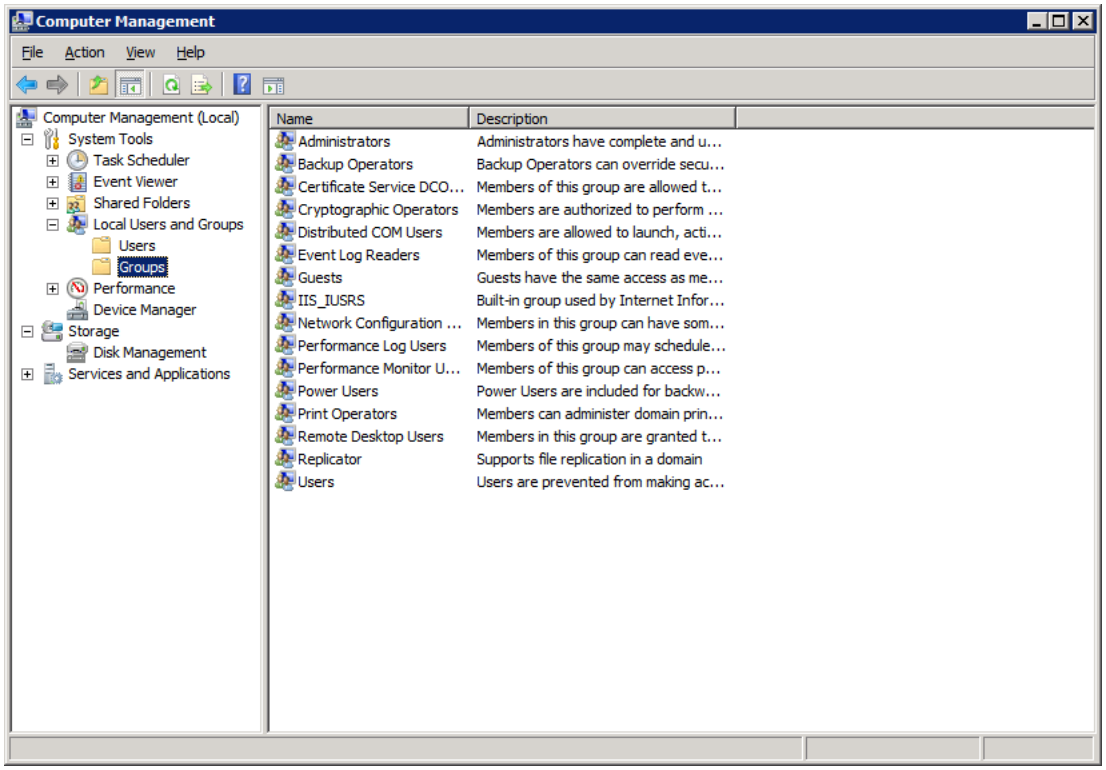


16 Click **Apply**.



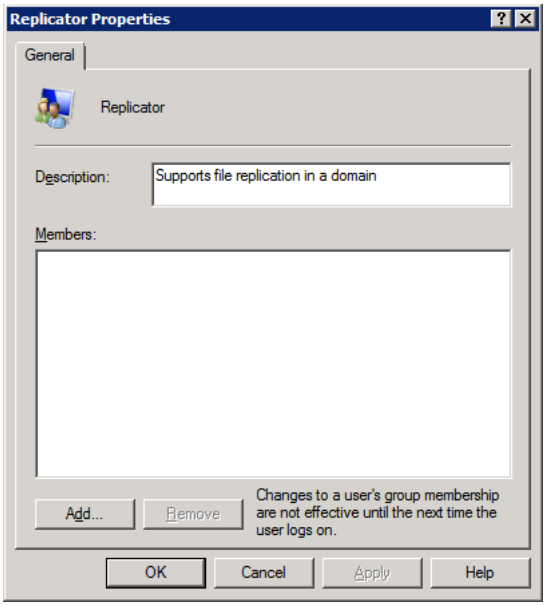
17 Click **OK**.

18 Click the **Groups** folder.

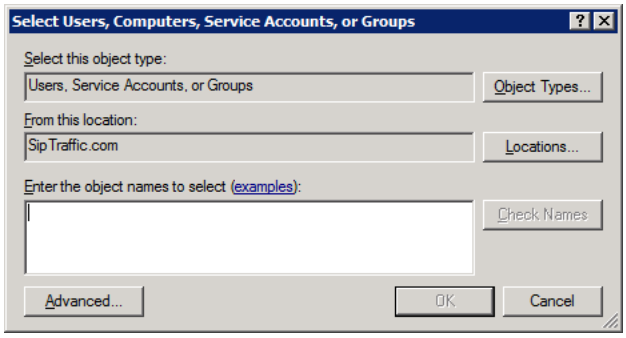


19 Double-click on the **Replicator** group.

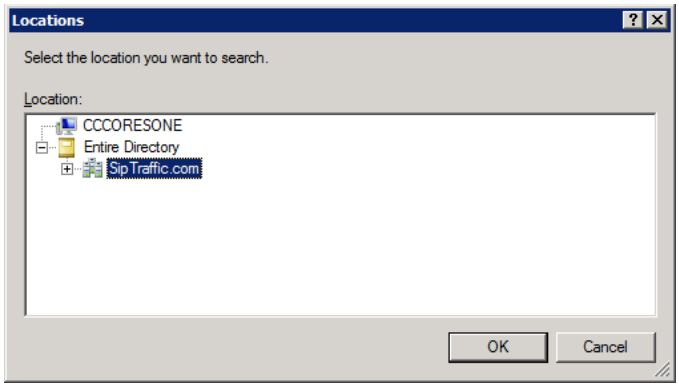
20 Click **Add**.



21 Click **Locations**.

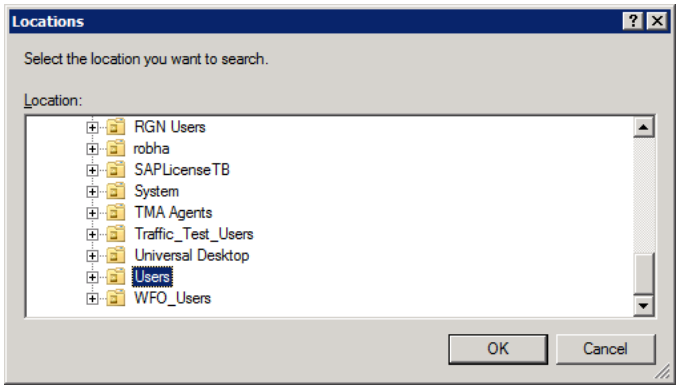


22 On the **Locations** dialog, select the domain to be used by CCMA replication. For example, select **siptraffic.com**.

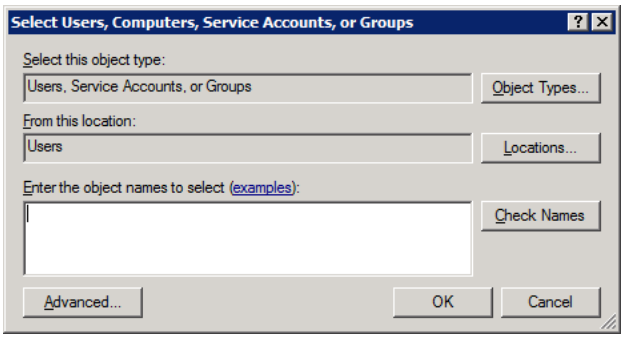


23 Expand the domain folder to display domain users.

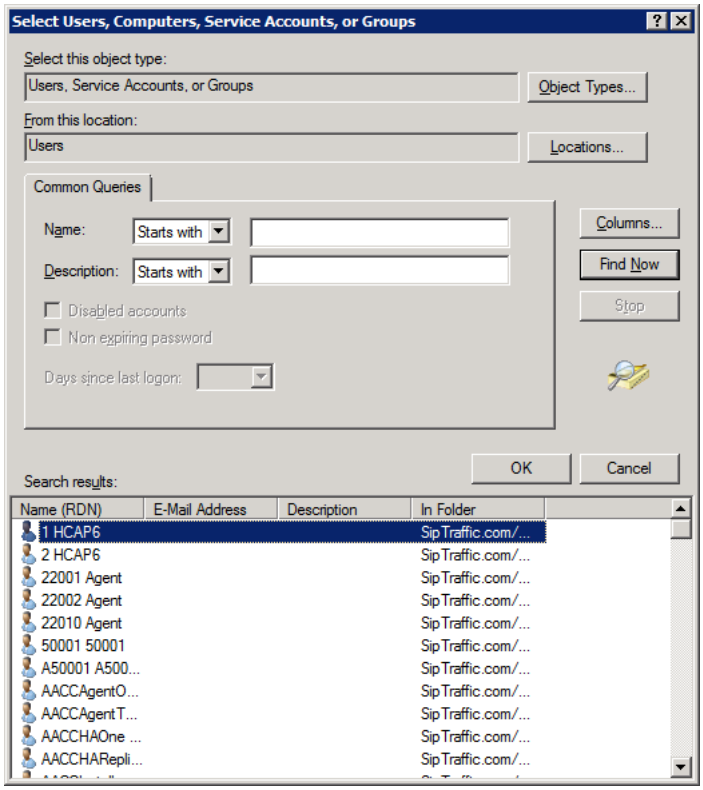
24 Click **Users**.



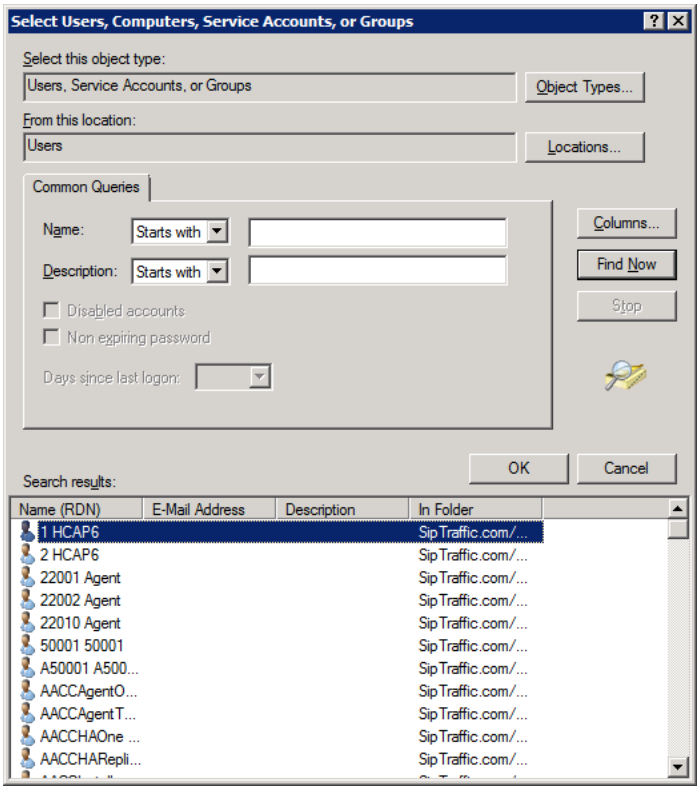
25 Click **OK**.



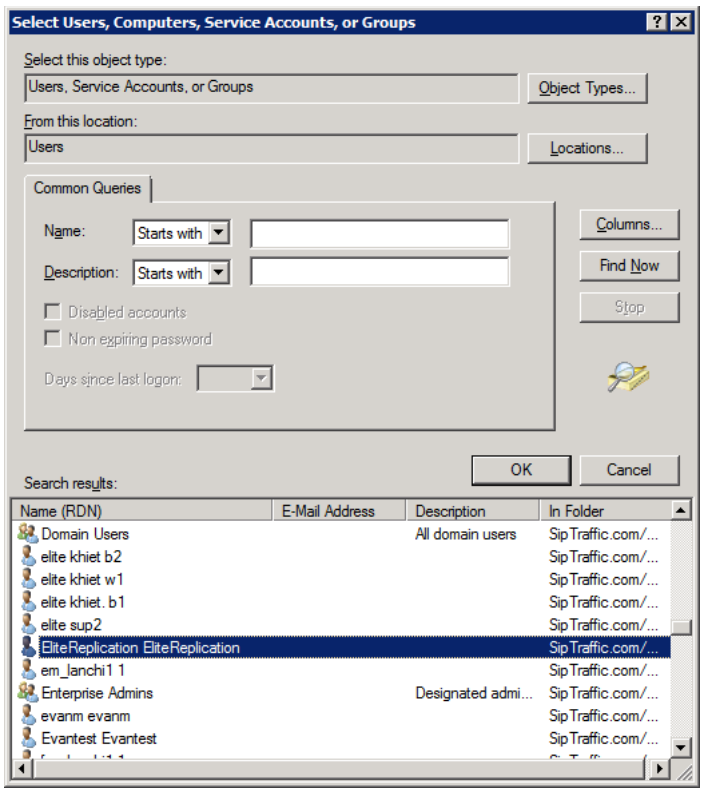
26 Click **Advanced**.



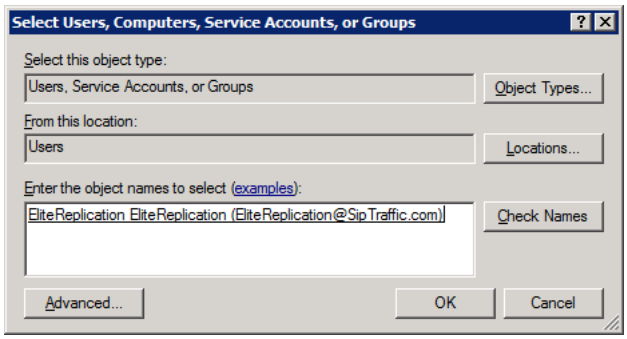
27 Click **Find Now**, to display domain users.



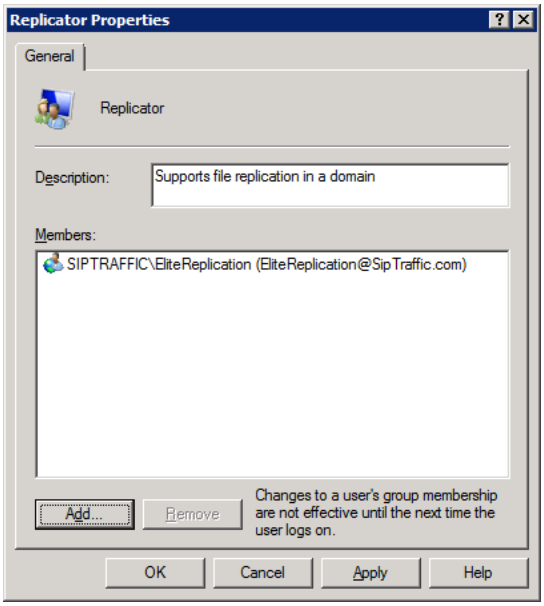
28 From the list of users select the CCMA replication domain user account, for example **siptraffic\EliteReplication**.



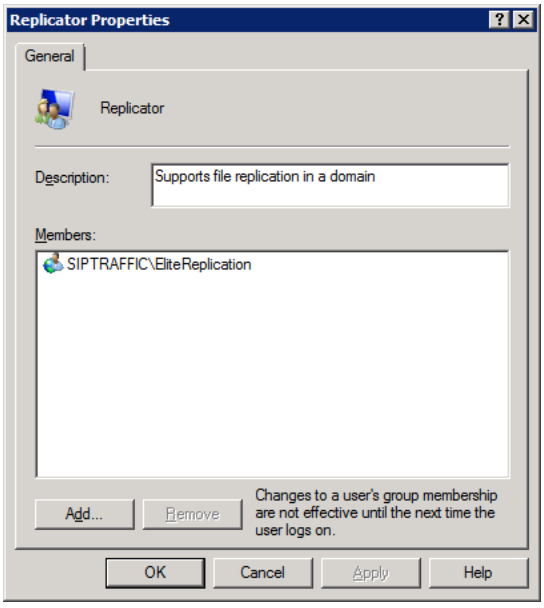
29 Click **OK**.



30 Click **OK**.



31 Click **Apply**.



32 Click **OK**.

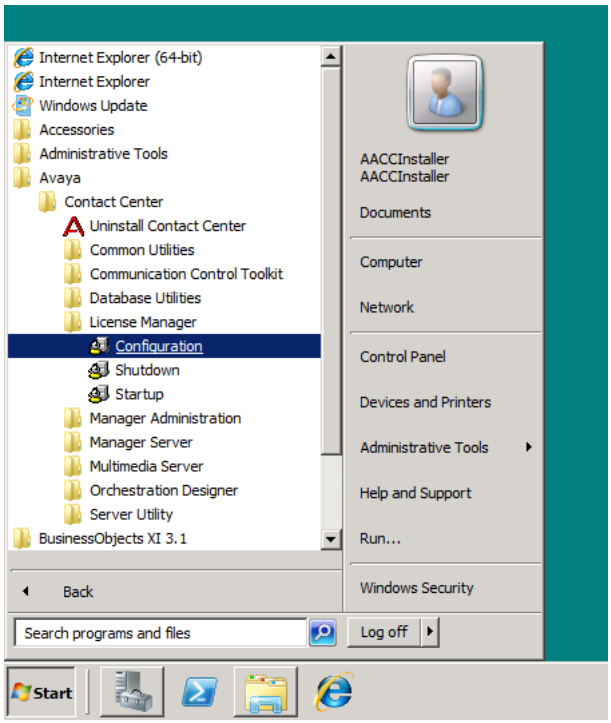
--End--

Updating the license file on the Active server

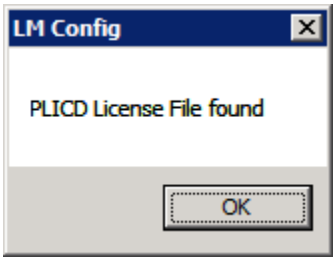
Apply the updated license file to support the HA feature. The license file must have entries for both the Active and Standby servers.

Procedure steps

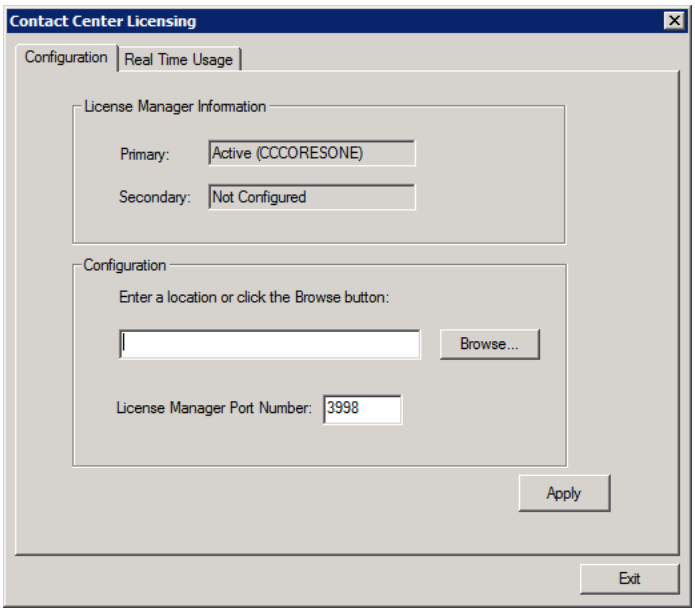
Step	Action
1	Log on to the Active server (for example, **CCCORESONE**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Click **Start, All Programs, Avaya, Contact Center, License Manager, Configuration**.



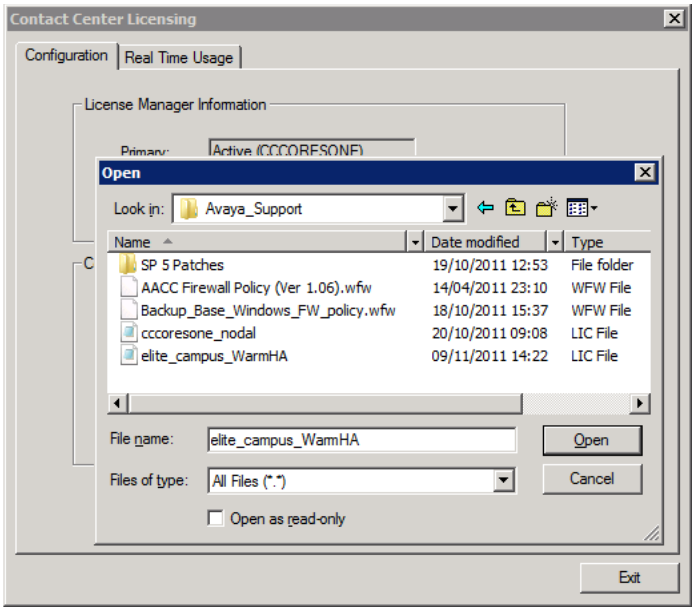
3	On the LM Config page, click **OK**.



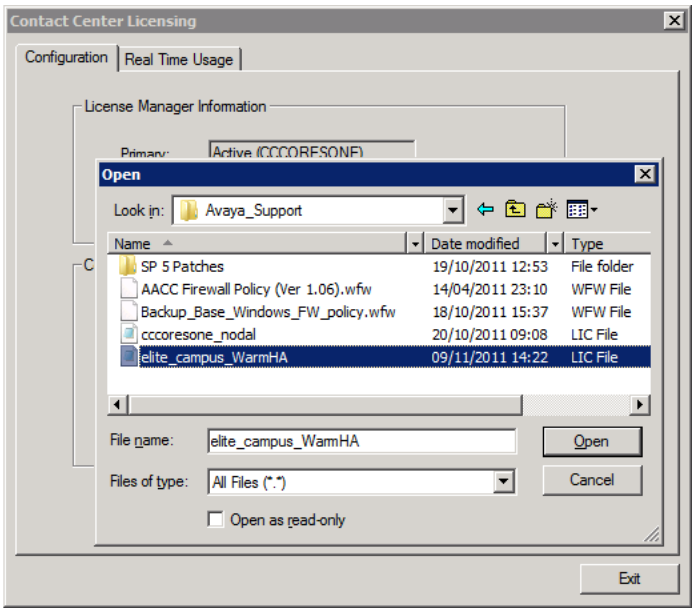
4	On the Configuration page, click **Browse**.



5 Navigate the file system to the location where you downloaded the new license file, for example **C:\Avaya_Support**.

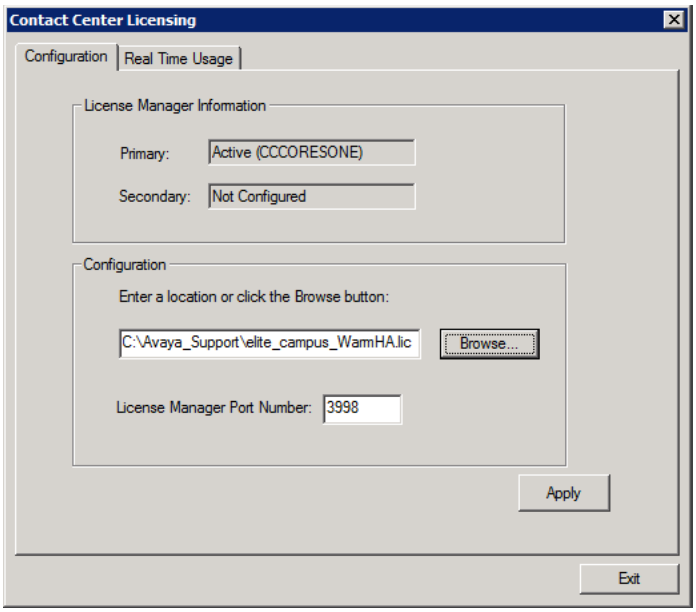


6 Select the new license file, for example **elite_campus_WarmHA.lic**.

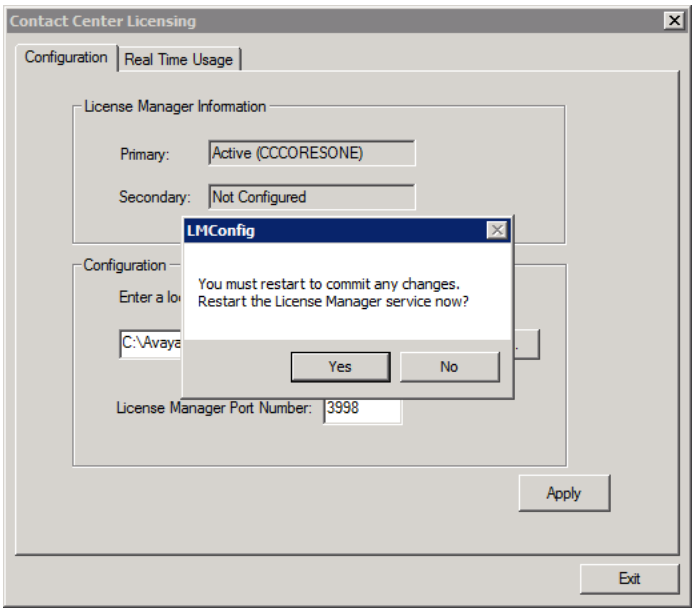


7 Click **Open**.

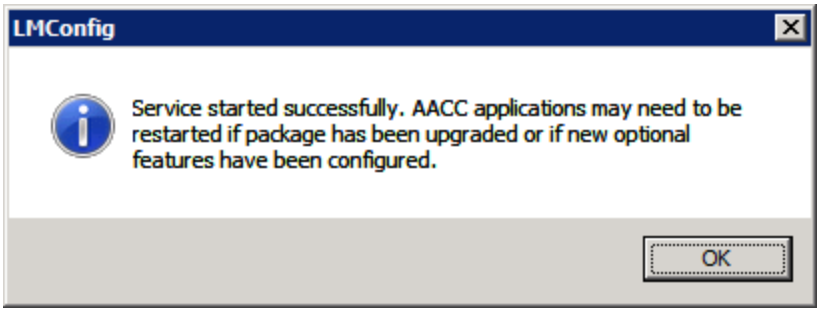
8 Click **Apply**.



9 Click **Yes** to restart the Contact Center License Manager server.



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



11 Click **Exit**.

12 Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Common Utilities**, **System Control and Monitor Utility**.

13 On the Contact Center tab, click **Shut down Contact Center**, and wait until all the components have stopped.

14 Click **Start Contact Center**.

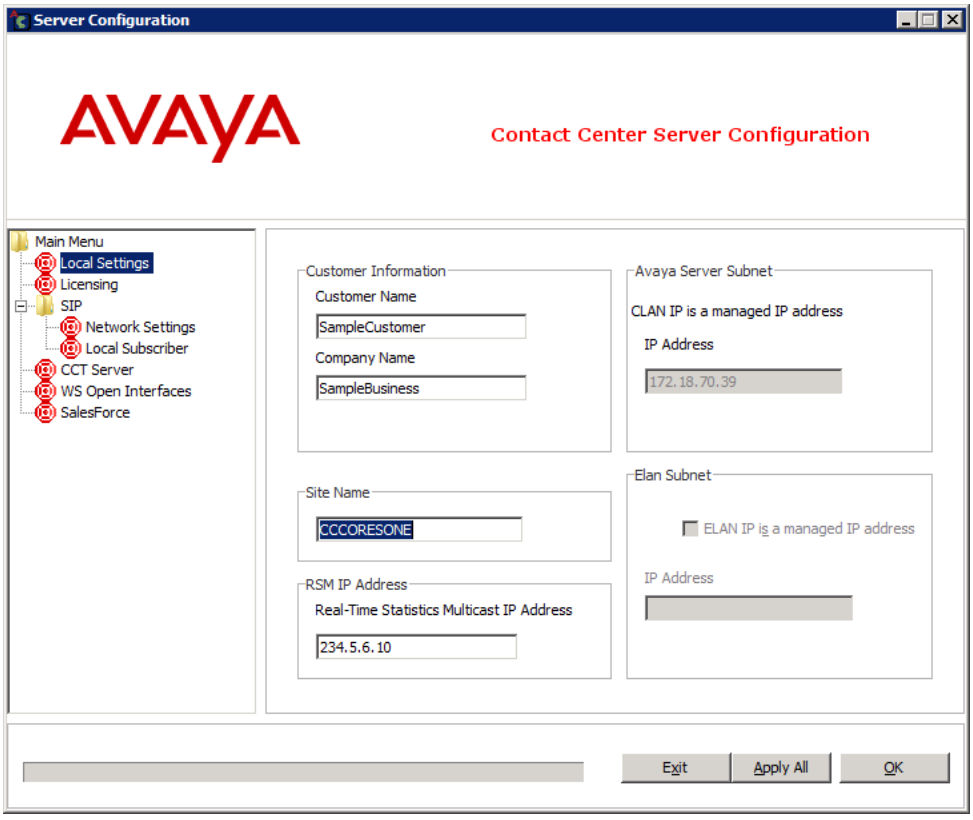
15 Click **Close**.

--End--

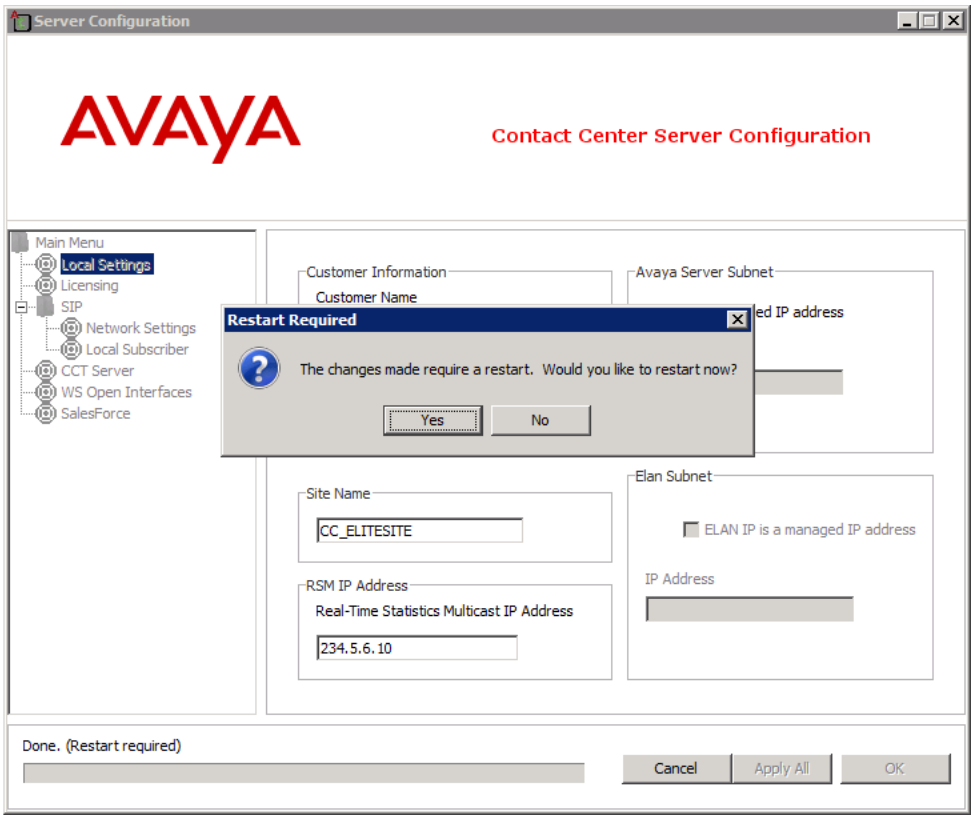
Updating the site name on the Active server

Ensure that the site name on the active server is not the same as the server name. The default on a non-HA install is for the site name to be the same as the server name.

Step	Action
1	Log on to the Active server (for example, **CCCORESONE**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Click **Start, All Programs, Avaya, Contact Center, Manager Server, Server Configuration**.
3	On the Server Configuration page, in the left pane, select **Local Settings**.
4	Check whether the site name is the same as the server name, for example **CCCORESONE**.



5	If the site name is the same as the server name, in the Site Name box type a new site name, for example **CC_ELITESITE**.
6	Click **OK**.
7	On the **Updated IP Warning** dialog, click **OK**.
8	On the **Updated IP Warning** dialog, click **Yes** to restart the server.


Server Configuration
AVAYA
Contact Center Server Configuration
Main Menu
Local Settings
Licensing
SIP
Network Settings
Local Subscriber
CCT Server
WS Open Interfaces
SalesForce
Customer Information
Customer Name
Avaya Server Subnet
ed IP address
Restart Required
The changes made require a restart. Would you like to restart now?
Yes
No
Site Name
CC_ELITESITE
Elan Subnet
ELAN IP is a managed IP address
IP Address
RSM IP Address
Real-Time Statistics Multicast IP Address
234.5.6.10
Done. (Restart required)
Cancel
Apply All
OK

--End--

Windows server preparation—Standby server

This chapter provides the common procedures to prepare the Windows server on which you plan to install the Avaya Aura® Contact Center Standby server software. You must perform the procedures in this chapter on the Standby server.

Prerequisites to server preparation

- Ensure the server hardware meets the requirements described in *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).

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.

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.

  Do not upgrade your operating system from a previous release. Remove the drive partitions and reformat the hard drives on the server.
- Configure all servers for RAID as described in *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
- Ensure that you have a DVD for Windows Server 2008 Release 2.
- Install the Network Interface Card in the server.
- Know the IP address 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. This partition must be a minimum of 61440 Mb. You can either change it now or expand it after the installation.

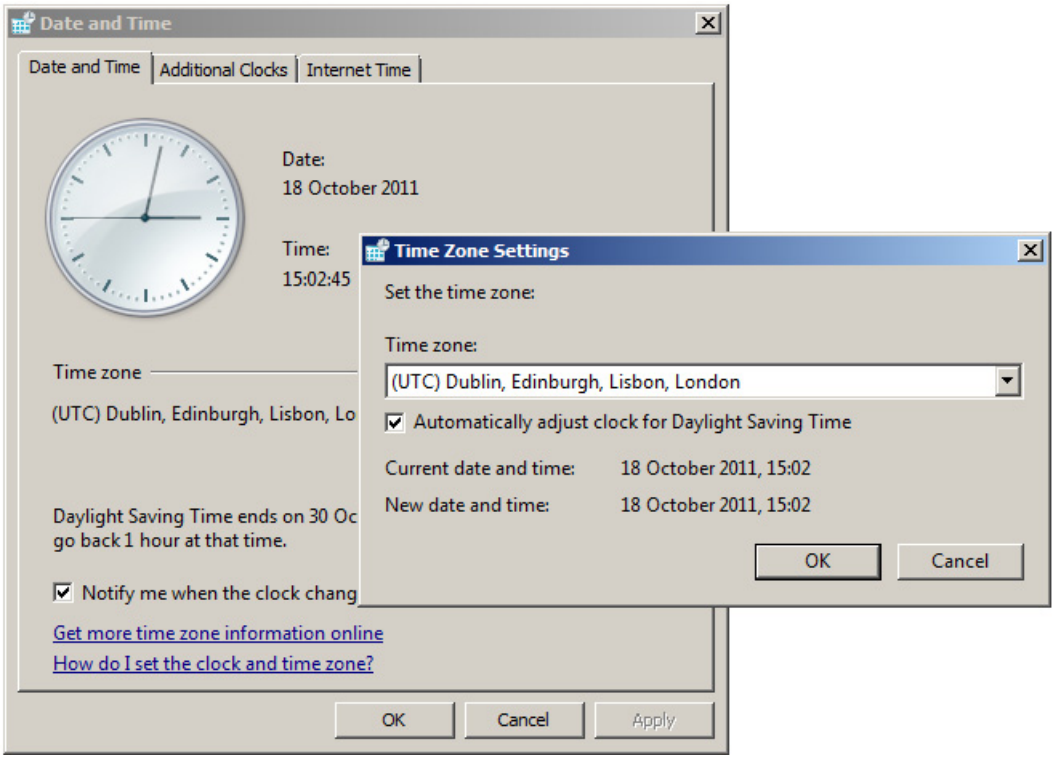
16 Click **Next**.

The install proceeds and automatically restarts the server several times.

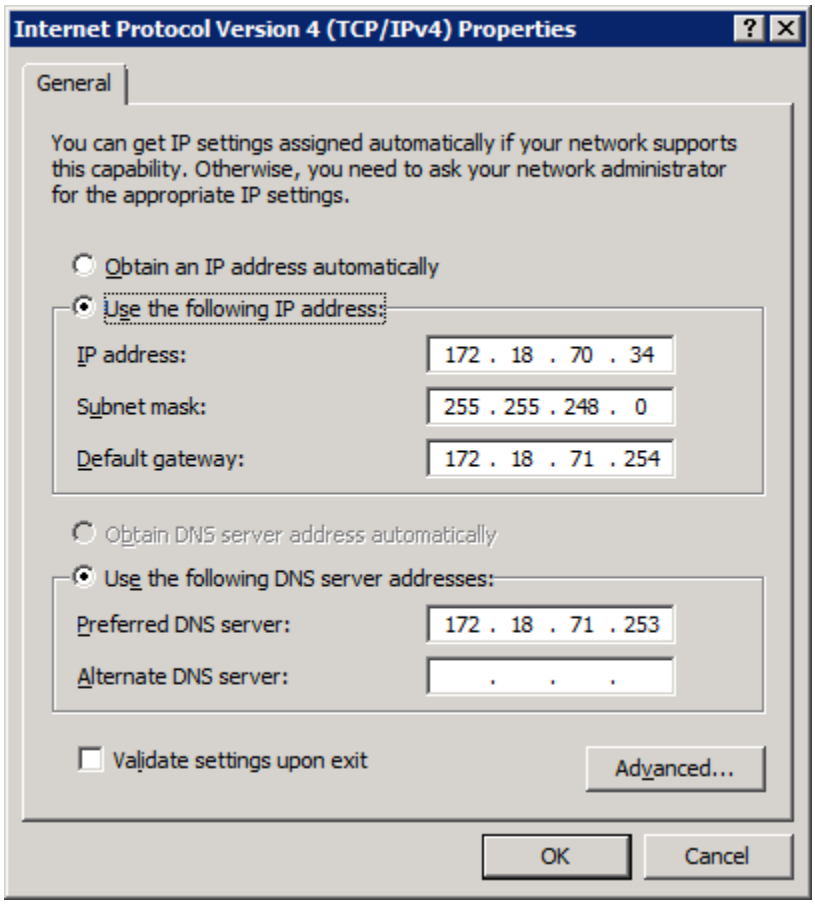
17 After completing the installation, log on to the server as Administrator. Enter and confirm the local Administrator password, for example **MultiMpassw1**.

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

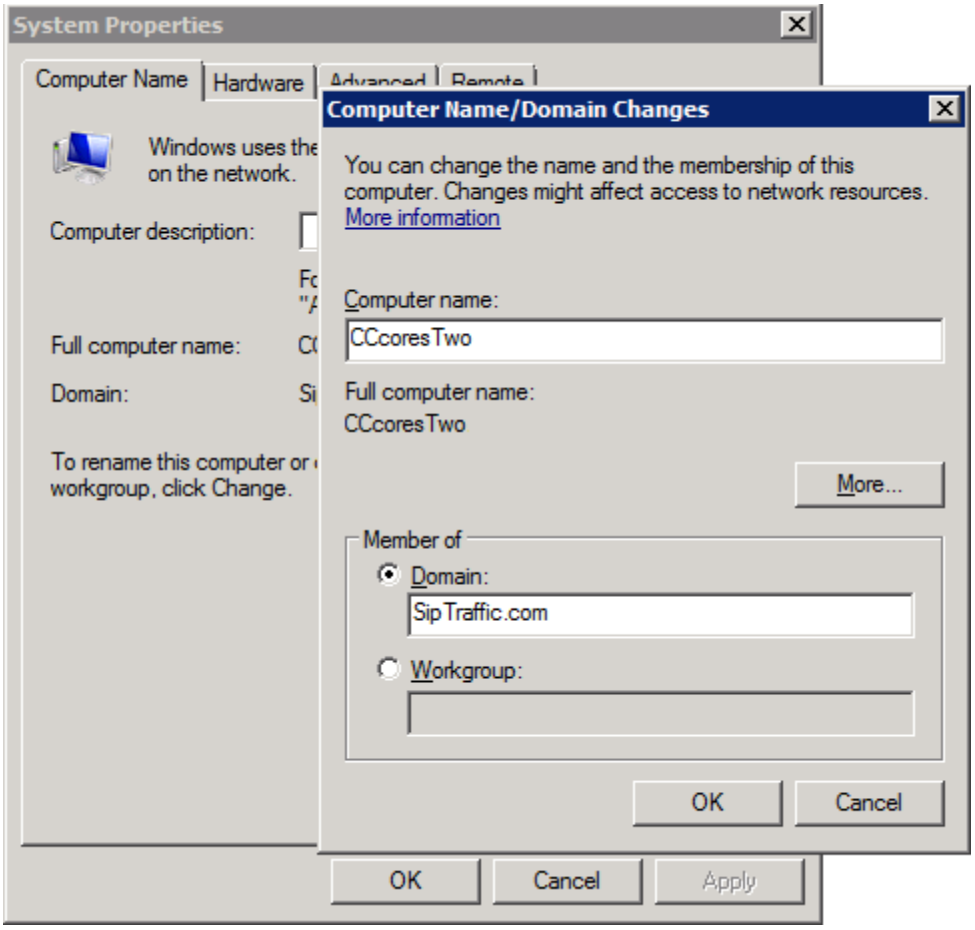
19 Select **Set time zone** and complete the information as required for your system. Ensure you select **Automatically adjust clock for Daylight Saving Time**: CCMM does not support manual DST time changes.



20 Select **Configure Networking** and complete the information for your Network Interface Card (NIC) with the server IP address, subnet mask, default gateway, and DNS server. For example use **172.18.70.34, 255.255.248.0, 172.18.71.253** and **172.18.71.253** respectively for the Standby server.



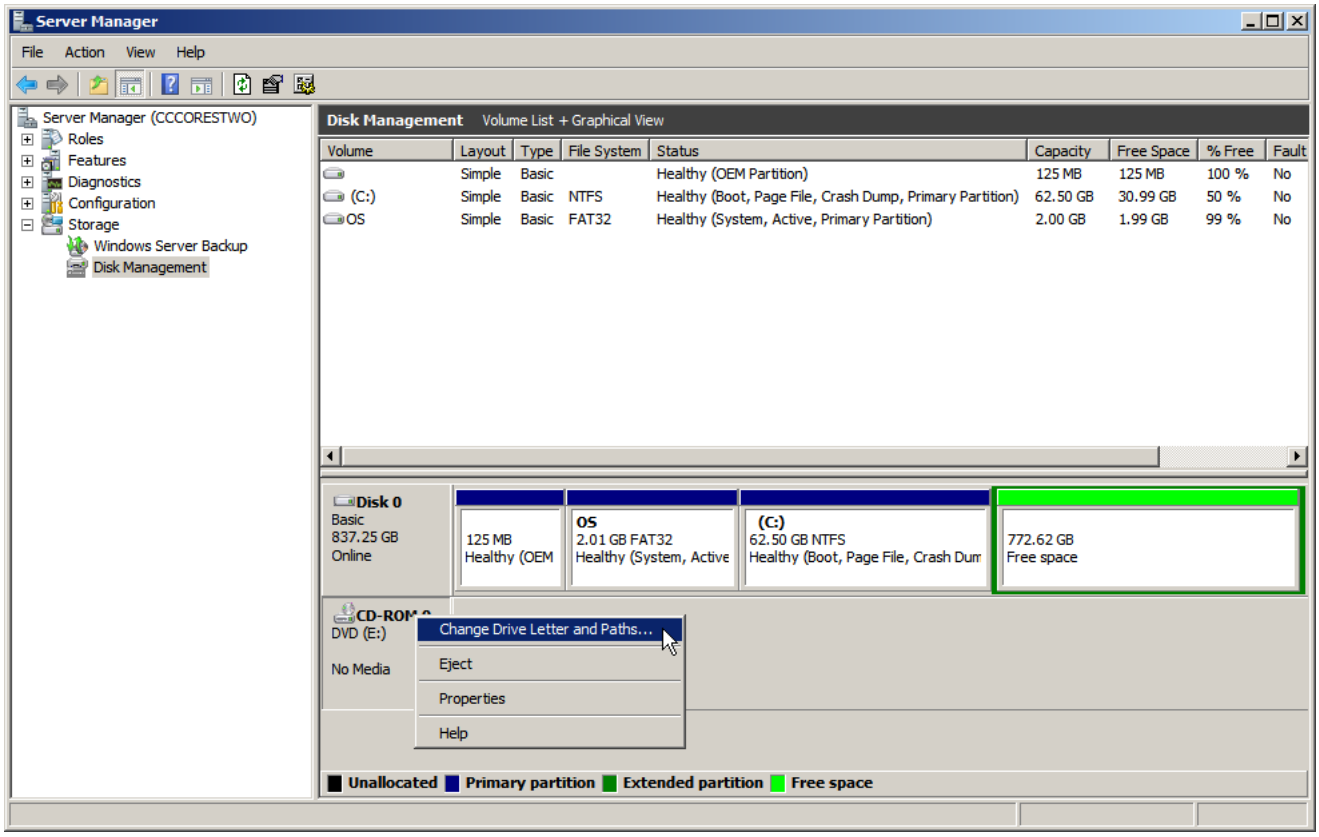
21 Select **Provide computer name and domain** and complete the information for your server name and domain settings. For example, use **CCCORESTWO** for the Standby server, in the domain **SipTraffic.com**.



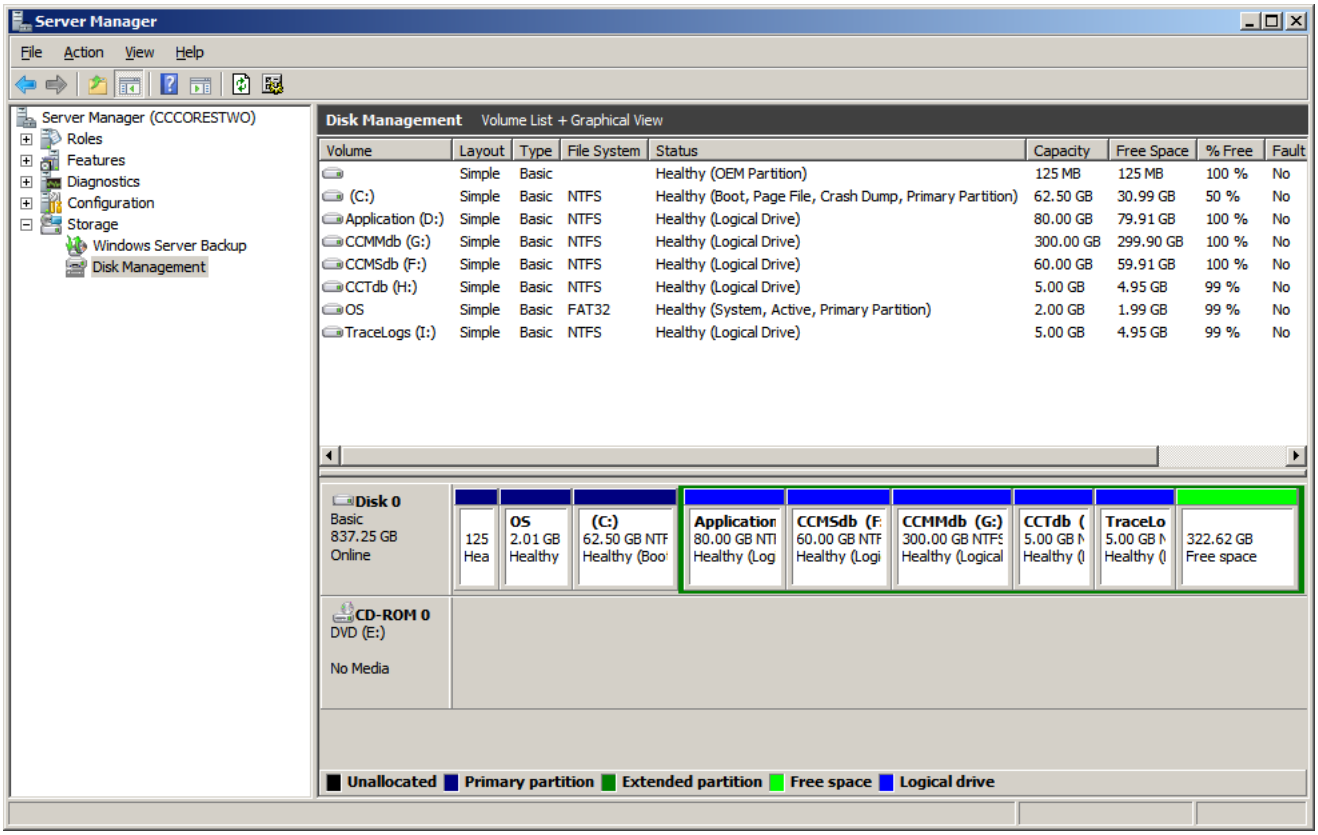
22 Choose **Restart Later** when prompted to restart the computer, and log back in as the local administrator.

23 Configure disk drive C: to be the only primary partition on your hard drive. Ensure that it is at least 60Gb in size; if drive C: is less than 60Gb, expand the volume.

24 Change the DVD drive letter to E:, to ensure that the correct drive letters are free for the drives needed for the Avaya Aura® CC application components.



25 Configure the remaining drives for this server as follows:
— D: 80Gb Application drive
— F: 60Gb CCMS Database drive
— G: 300Gb CCMM Database drive
— H: 5Gb CCT Database drive
— I: 5Gb Trace logs drive



26 Install any drivers specifically required for your hardware configuration.

--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.

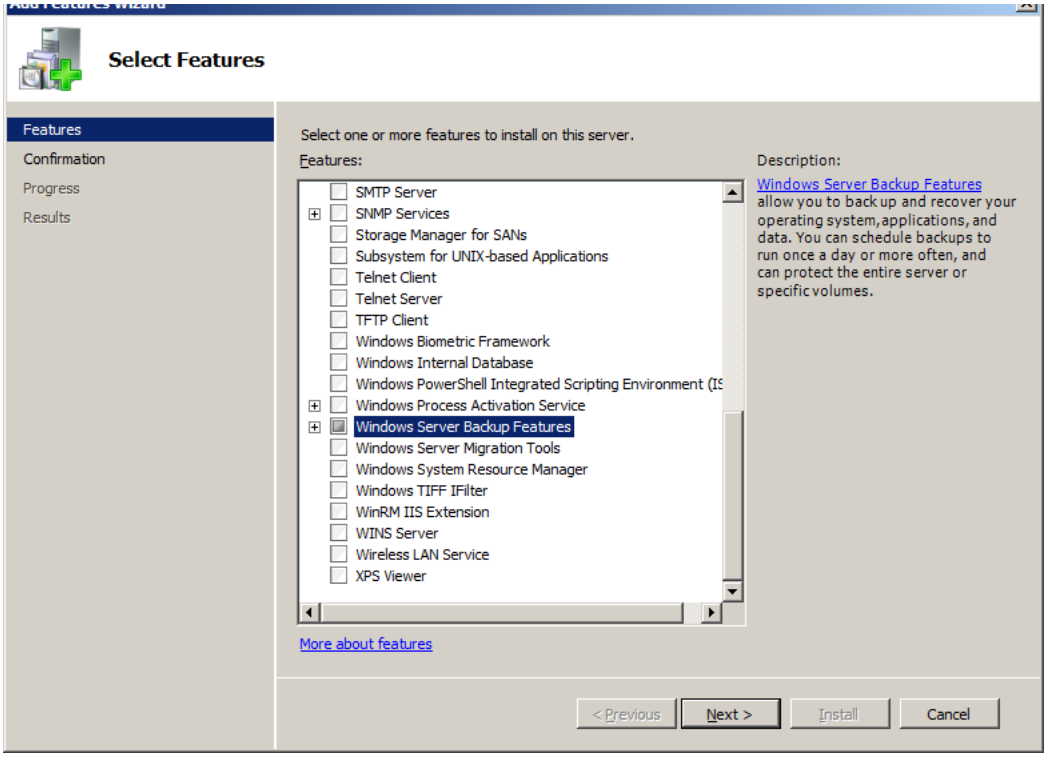
Procedure steps

Step	Action
1	Log on to the Windows Server 2008 server as the local administrator, for example **CCCORESTWO\Administrator**.
2	On the **Initial Configuration Tasks** window, select the **Don't display this screen on startup** check box and click **Close**.
3	Update the emergency repair disk to record the latest configuration data for the server.
4	Choose **Start, Administrative Tools, Server Manager**.

5 In the left pane, click **Features**.

6 Click **Add Features**.

7 Select **Windows Server Backup Features**.



8 Click **Next**.

9 Click **Install**.

10 Click **Close**.

11 Choose **Start, All Programs, Accessories, System Tools, Windows Server Backup**.

12 Follow the on-screen instructions to select what you want to back up.

--End--

Installing the latest operating system service packs

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

Prerequisites

- Access the Avaya Contact Center Service Packs Compatibility and Hotfix Availability list on the support Web site http://www.avaya.com/support.
- Review the recommendations on operating system service updates in *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
- Install the Microsoft .NET Framework 3.5 and Microsoft .NET Framework 3.5 SP1.

Procedure steps

Step	Action
1	Review the Contact Center Service Packs Compatibility and Security Hotfixes Applicability list to determine the most recent supported patches or service packs.
2	Download the appropriate Microsoft Windows Server 2008 patches for the server software installed on this server.
3	Install the most recent Windows Server 2008 service pack that is validated with the server software by following the Microsoft installation instructions.

--End--

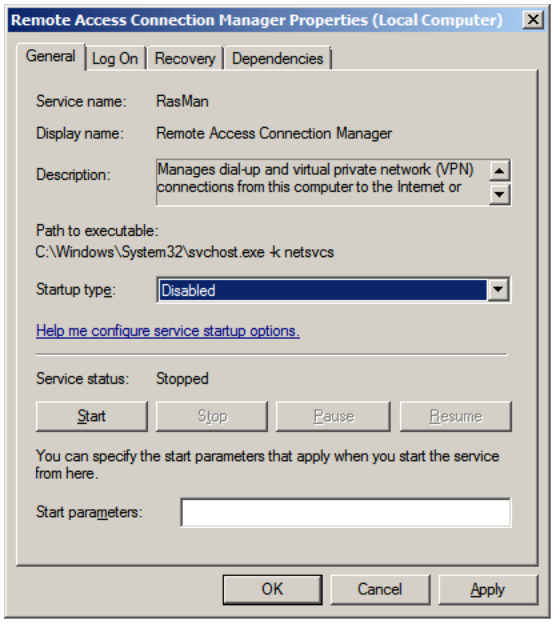
Disabling the Remote Access services

Disable the Remote Access services on the core contact center server, to support Communication Control Toolkit.

Attention: This procedure requires you to 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**.

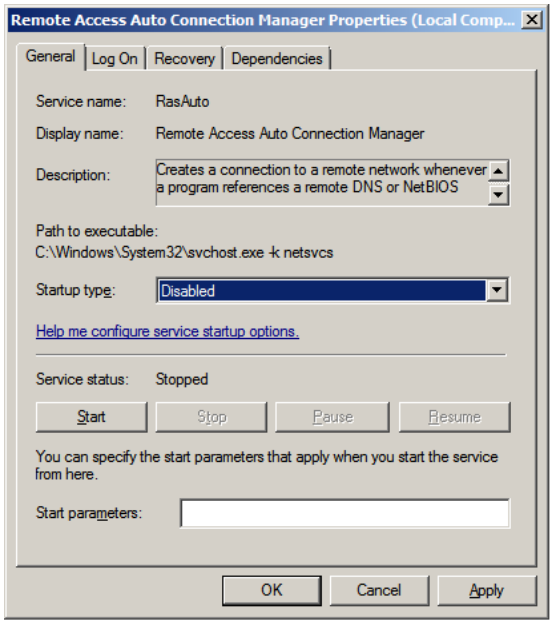


5 Click **OK**.

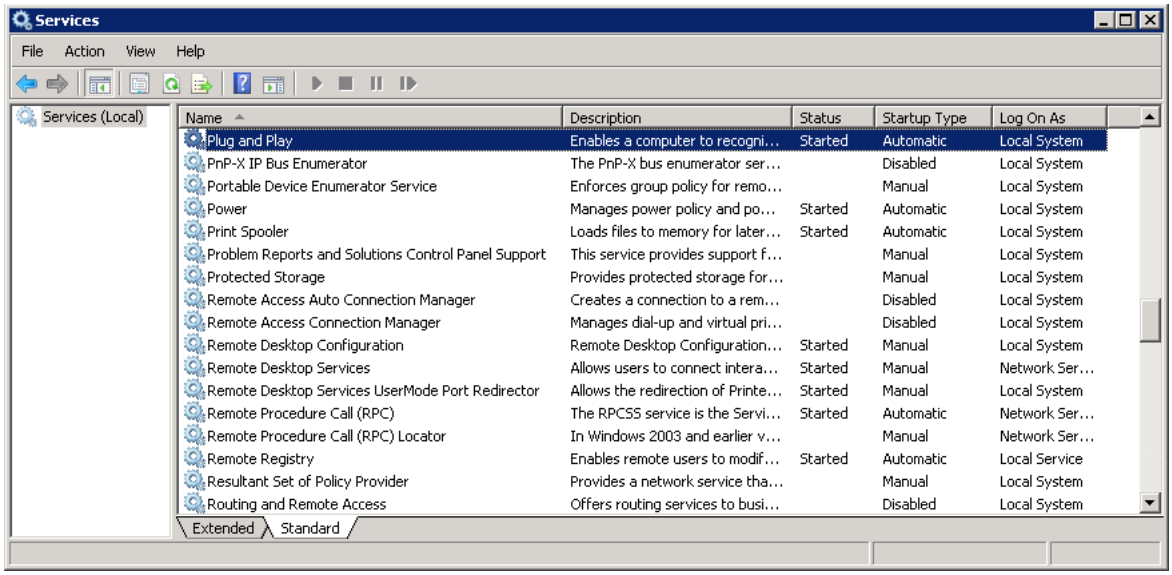
6 In the **Services** window, right-click the **Remote Access Auto Connection Manager** icon.

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.

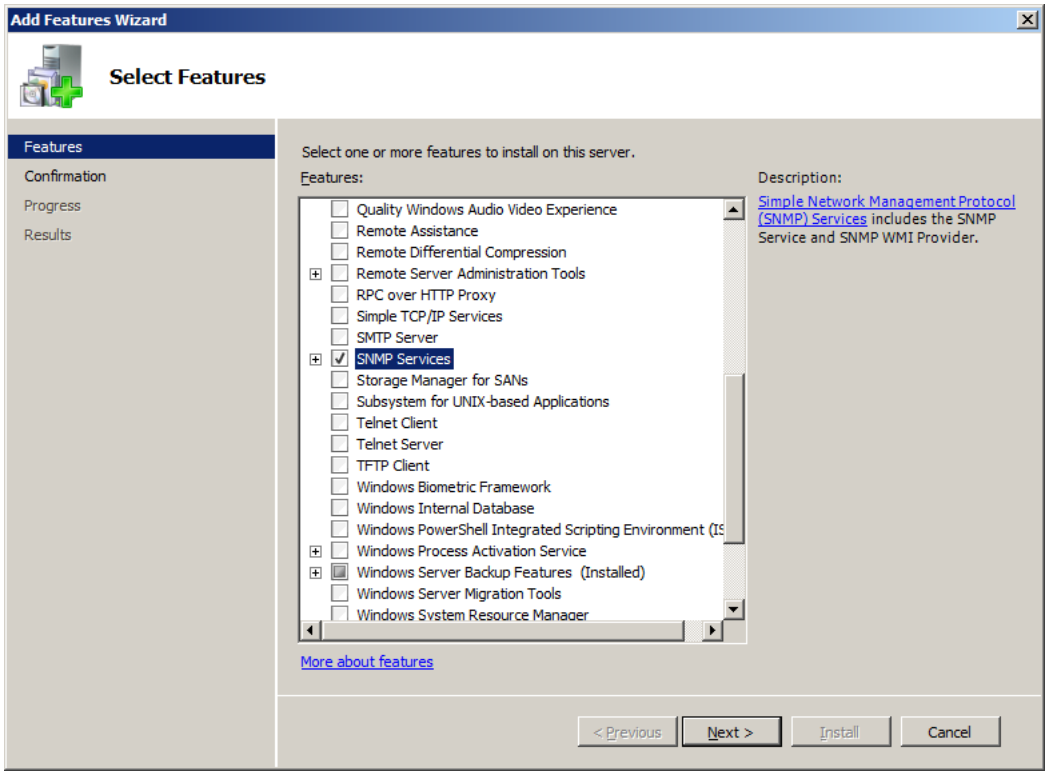
--End--

Configuring SNMP on your server

Configure Simple Network Management Protocol (SNMP) on your server to ensure you have all of the required components of the Internet Protocol for monitoring devices in your network. SNMP helps you manage data that describes the system configuration and errors that may occur between servers.

Procedure steps

Step	Action
1	Log on to the Windows Server 2008 server as the local administrator, for example **CCCORESTWO\Administrator**.
2	Choose **Start**, **Control Panel**, **Programs**.
3	In the **Programs and Features** section, click **Turn Windows features on or off**.
4	In the **Server Manager** window, select **Features** and click **Add Features**.
5	Select **SNMP Services**.



6 Click **Next**.

7 Click **Install**.

8 If prompted, insert the Windows Server 2008 DVD.

9 Click **Close**.

--End--

Configuring the server to use the Contact Center installer account

Add the installer account to the Administrators group on the local server, and configure User Account Control (UAC) to give the account full local administration privileges.

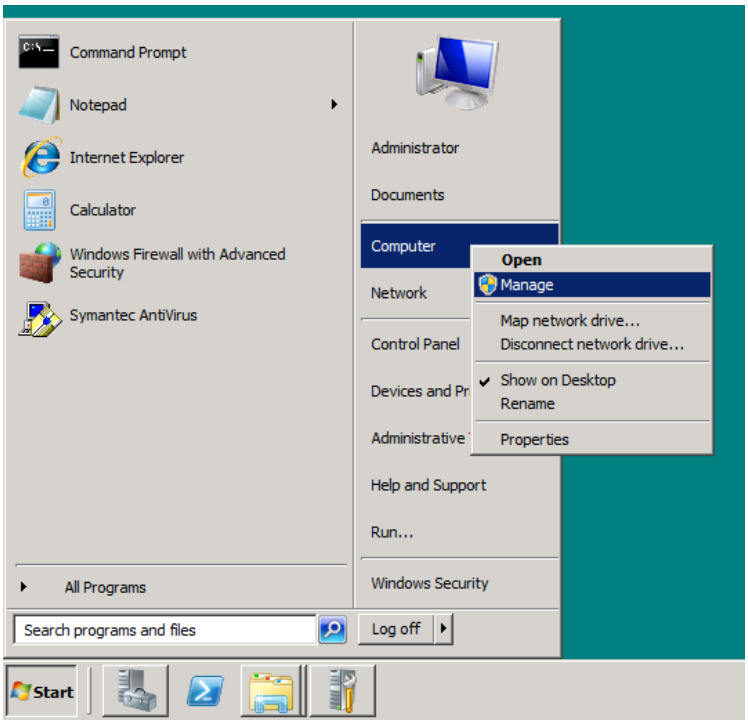
Attention: This procedure requires a restart of the Windows 2008 server.

Procedure steps

Step	Action
1	Log on to the Windows Server 2008 server as the local administrator, for example **CCCORESTWO\Administrator**.

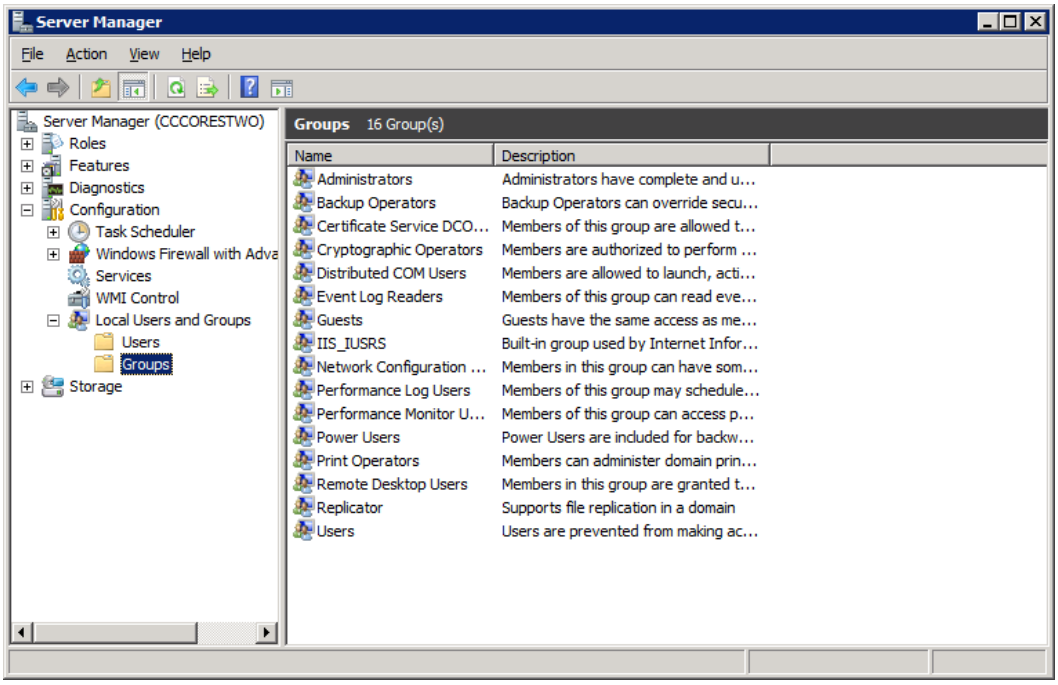
2 Click **Start**.

3 Right-click **Computer** and select **Manage**.



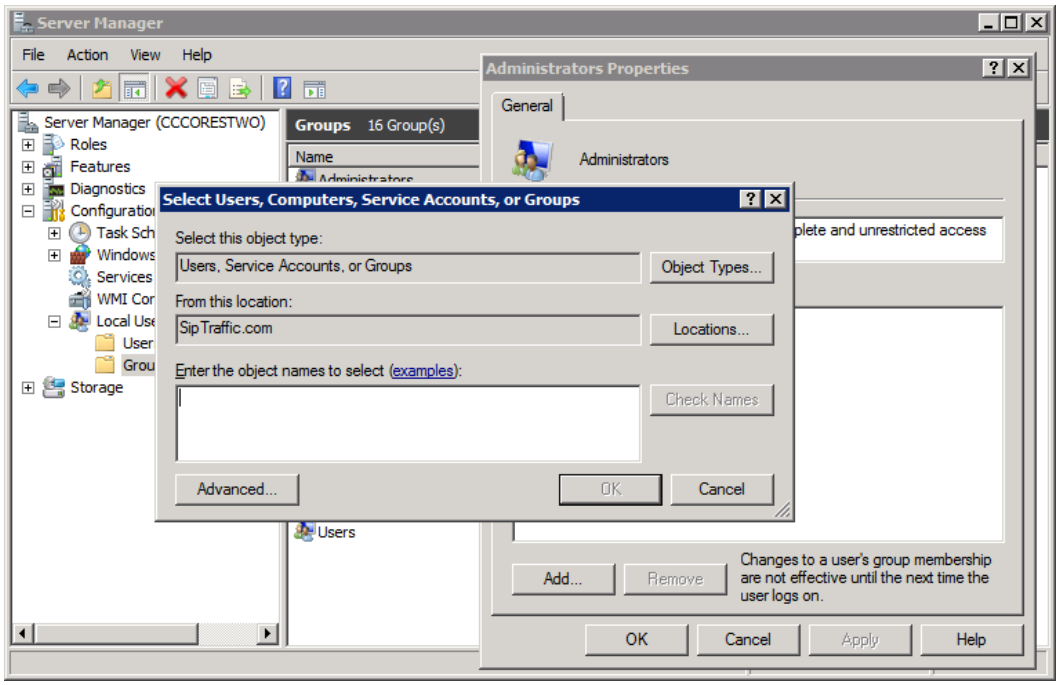
4 In the left pane, expand **Configuration**, **Local Users and Groups**.

5 Select **Groups**.

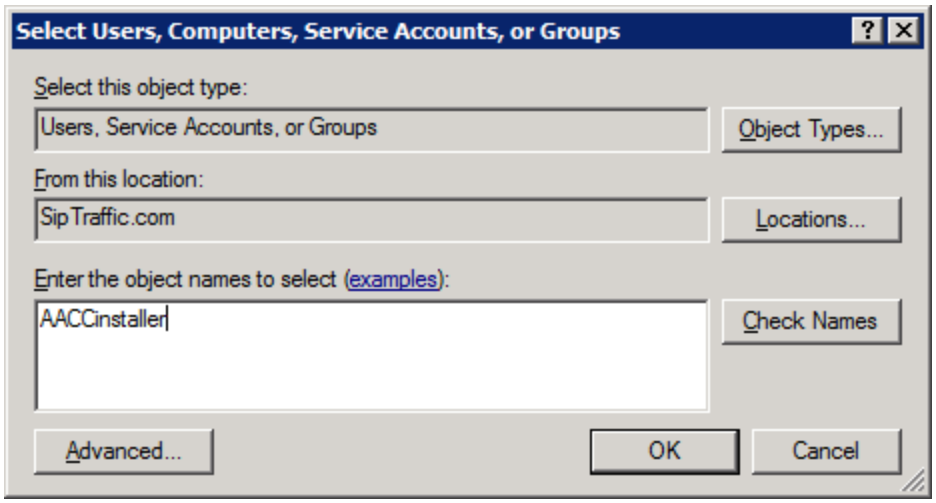


6 In the right pane, double-click **Administrators**.

7 In the **Administrators Properties** Window, click **Add**.



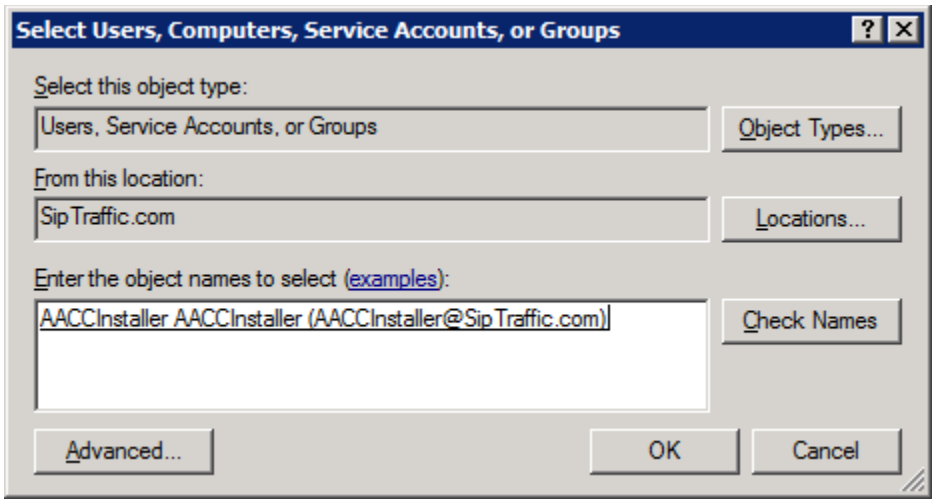
8 On the **Select Users, Computers, Service Accounts, or Groups** window, in the **Enter the object names to select (examples)** box, type the domain account that you created for installing Avaya Aura® CC, for example AACCinstaller.



9 Click **Check Names**.

10 When prompted, enter a domain administrator user name and password.

The system verifies the domain account.

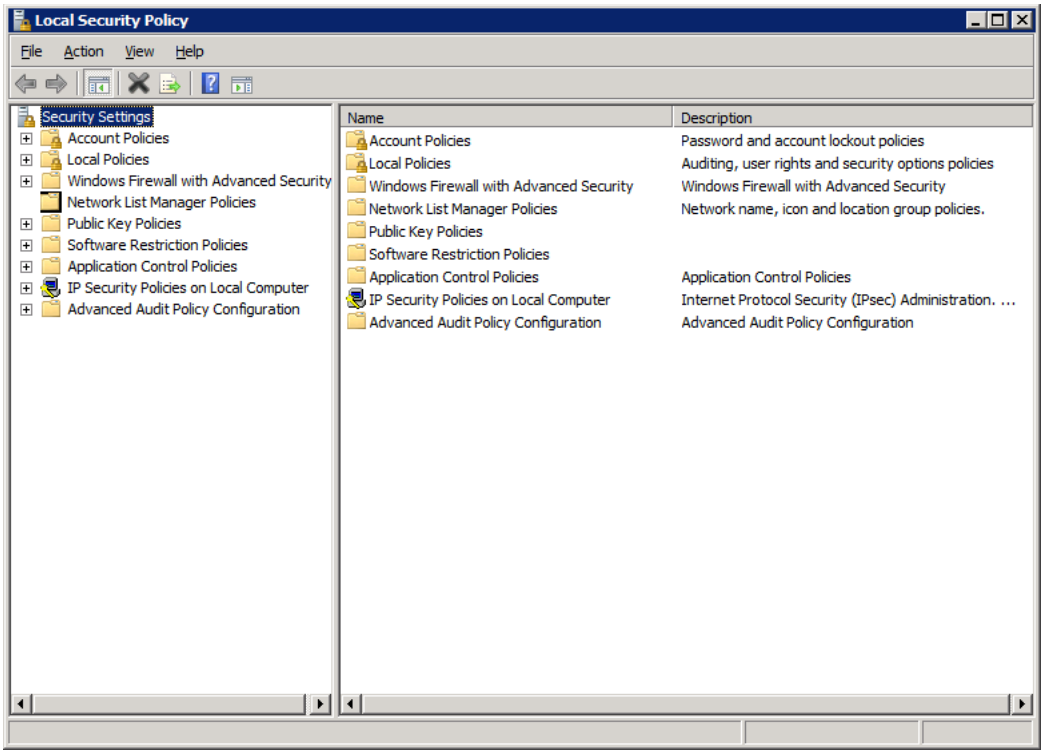


11 Click **OK**.

12 Click **OK**.

13 Exit the Server Manager window.

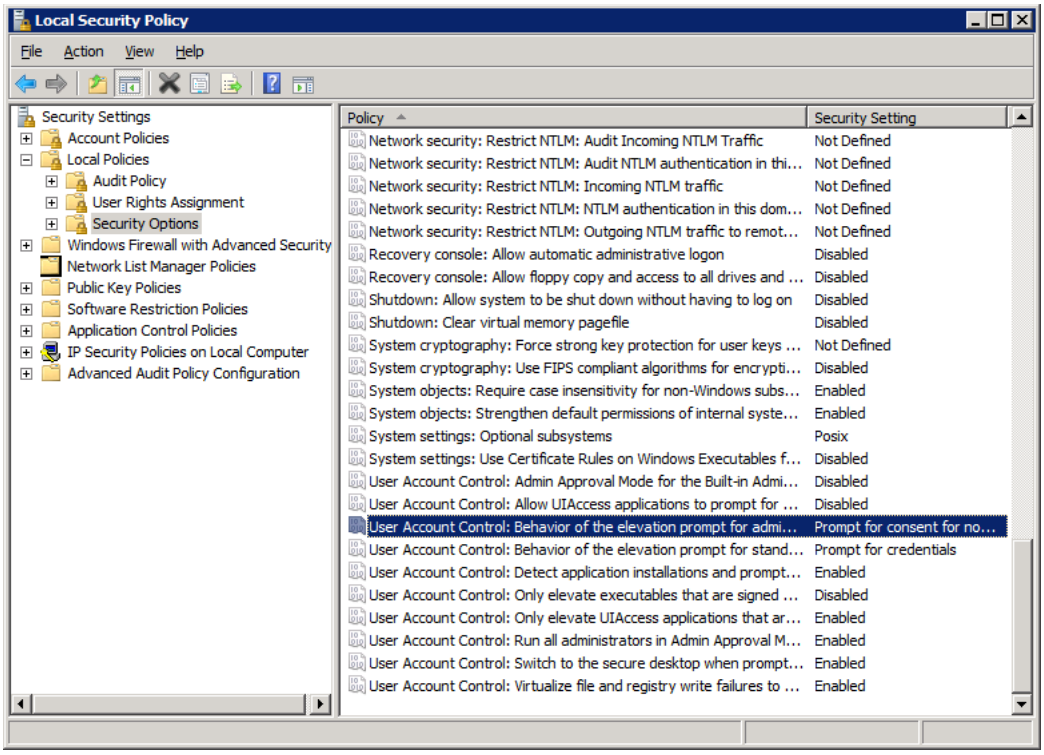
14 Select **Start, Administrative Tools, Local Security Policy**.



15 In the left pane, expand **Local Policies**.

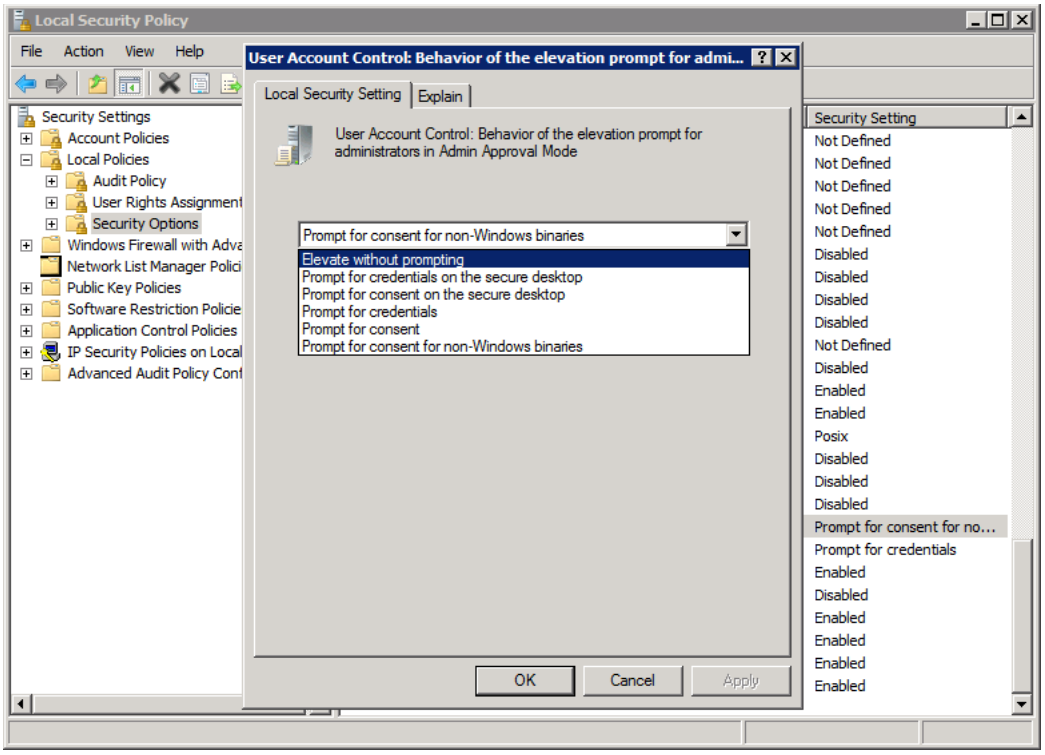
16 Select **Security Options**.

17 In the right pane, scroll down to find **User Account Control: Behavior of the elevation prompt for administrator**.

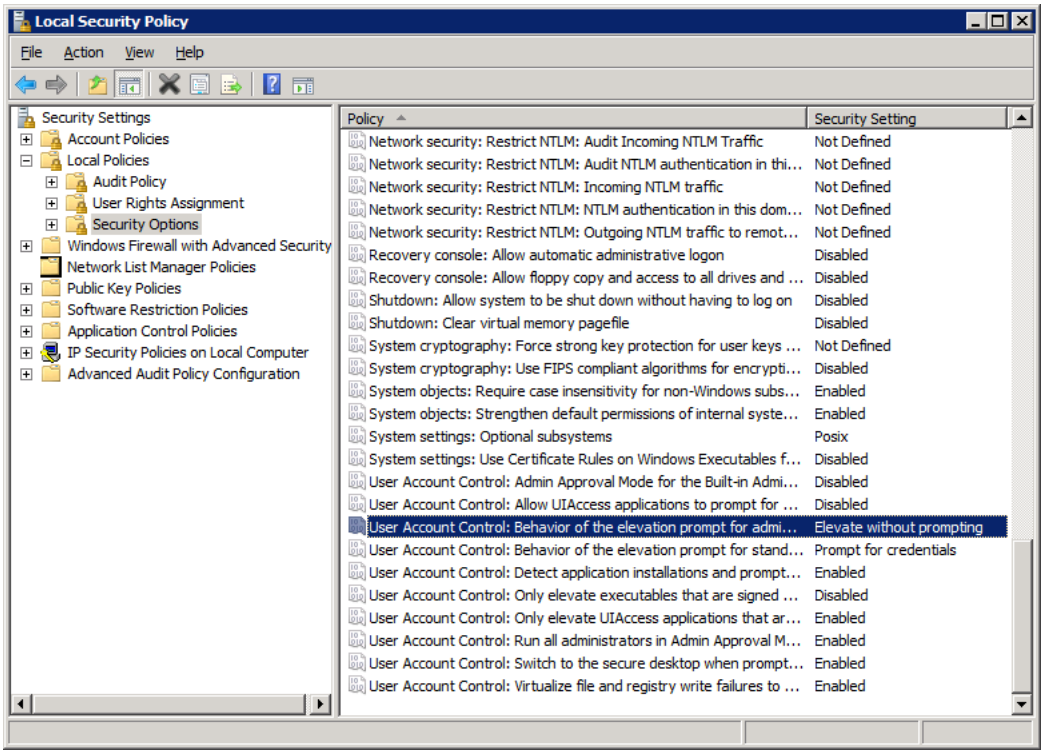


18 Double-click **User Account Control: Behavior of the elevation prompt for administrator**.

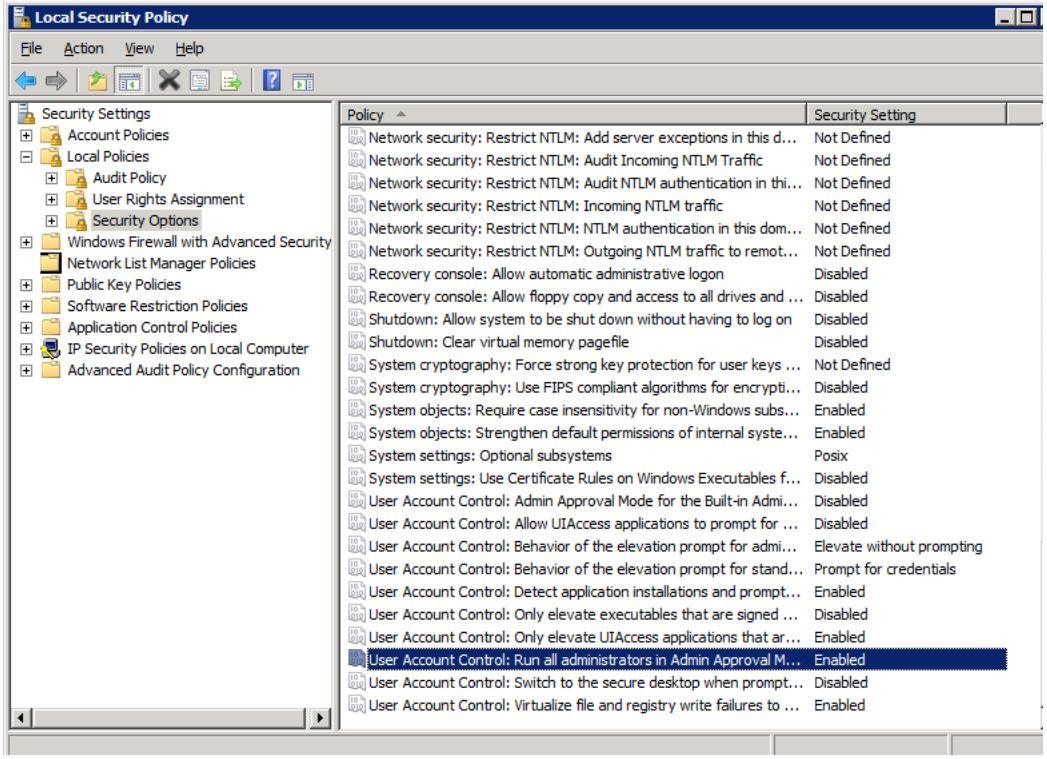
19 On the **Local Security Setting** tab, select **Elevate without prompting**.


Local Security Policy
File Action View Help
User Account Control: Behavior of the elevation prompt for admi...
Local Security Setting
Explain
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode
Prompt for consent for non-Windows binaries
Elevate without prompting
Prompt for credentials on the secure desktop
Prompt for consent on the secure desktop
Prompt for credentials
Prompt for consent
Prompt for consent for non-Windows binaries
OK
Cancel
Apply
Security Setting
Not Defined
Not Defined
Not Defined
Not Defined
Not Defined
Disabled
Disabled
Disabled
Disabled
Not Defined
Disabled
Enabled
Enabled
Posix
Disabled
Disabled
Disabled
Prompt for consent for no...
Prompt for credentials
Enabled
Disabled
Enabled
Enabled
Enabled
Enabled
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Adva
Network List Manager Polici
Public Key Policies
Software Restriction Policie
Application Control Policies
IP Security Policies on Local
Advanced Audit Policy Conf

20 Click **OK**.

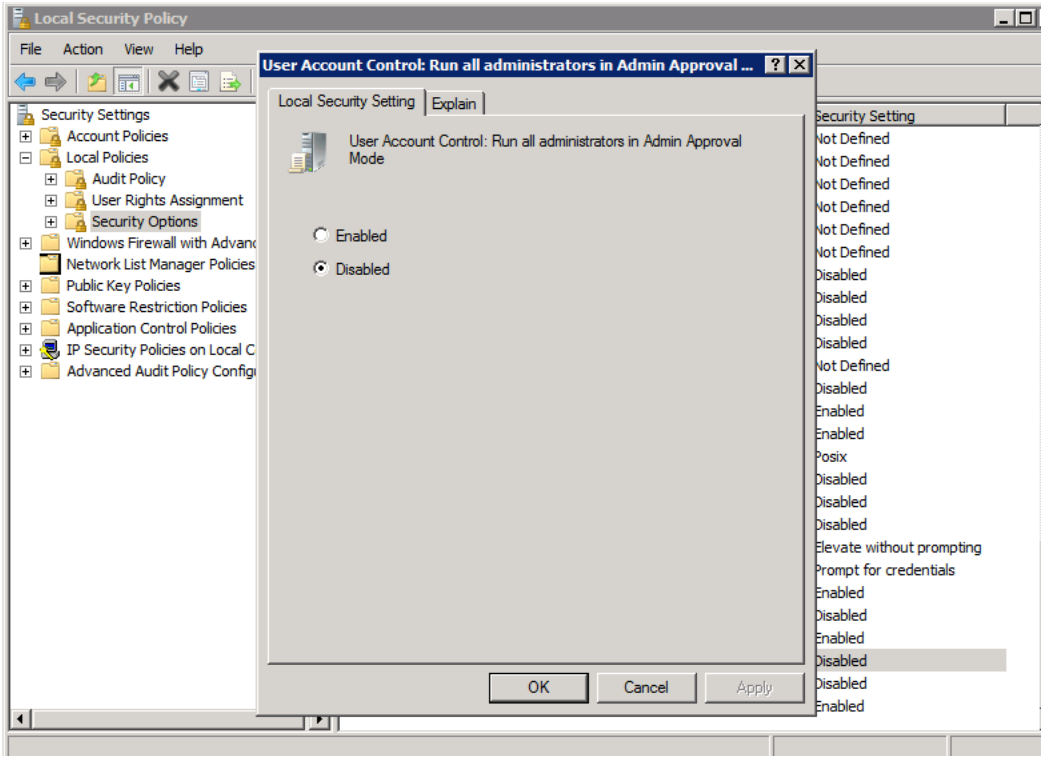

Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Policy
Security Setting
Network security: Restrict NTLM: Audit Incoming NTLM Traffic Not Defined
Network security: Restrict NTLM: Audit NTLM authentication in thi... Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic Not Defined
Network security: Restrict NTLM: NTLM authentication in this dom... Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to remot... Not Defined
Recovery console: Allow automatic administrative logon Disabled
Recovery console: Allow floppy copy and access to all drives and ... Disabled
Shutdown: Allow system to be shut down without having to log on Disabled
Shutdown: Clear virtual memory pagefile Disabled
System cryptography: Force strong key protection for user keys ... Not Defined
System cryptography: Use FIPS compliant algorithms for encrypti... Disabled
System objects: Require case insensitivity for non-Windows subs... Enabled
System objects: Strengthen default permissions of internal syste... Enabled
System settings: Optional subsystems Posix
System settings: Use Certificate Rules on Windows Executables f... Disabled
User Account Control: Admin Approval Mode for the Built-in Admi... Disabled
User Account Control: Allow UIAccess applications to prompt for ... Disabled
User Account Control: Behavior of the elevation prompt for admi... Elevate without prompting
User Account Control: Behavior of the elevation prompt for stand... Prompt for credentials
User Account Control: Detect application installations and prompt... Enabled
User Account Control: Only elevate executables that are signed ... Disabled
User Account Control: Only elevate UIAccess applications that ar... Enabled
User Account Control: Run all administrators in Admin Approval M... Enabled
User Account Control: Switch to the secure desktop when prompt... Enabled
User Account Control: Virtualize file and registry write failures to ... Enabled

21 In the right pane, scroll down to find **User Account Control: Run all administrators in Admin Approval mode**.

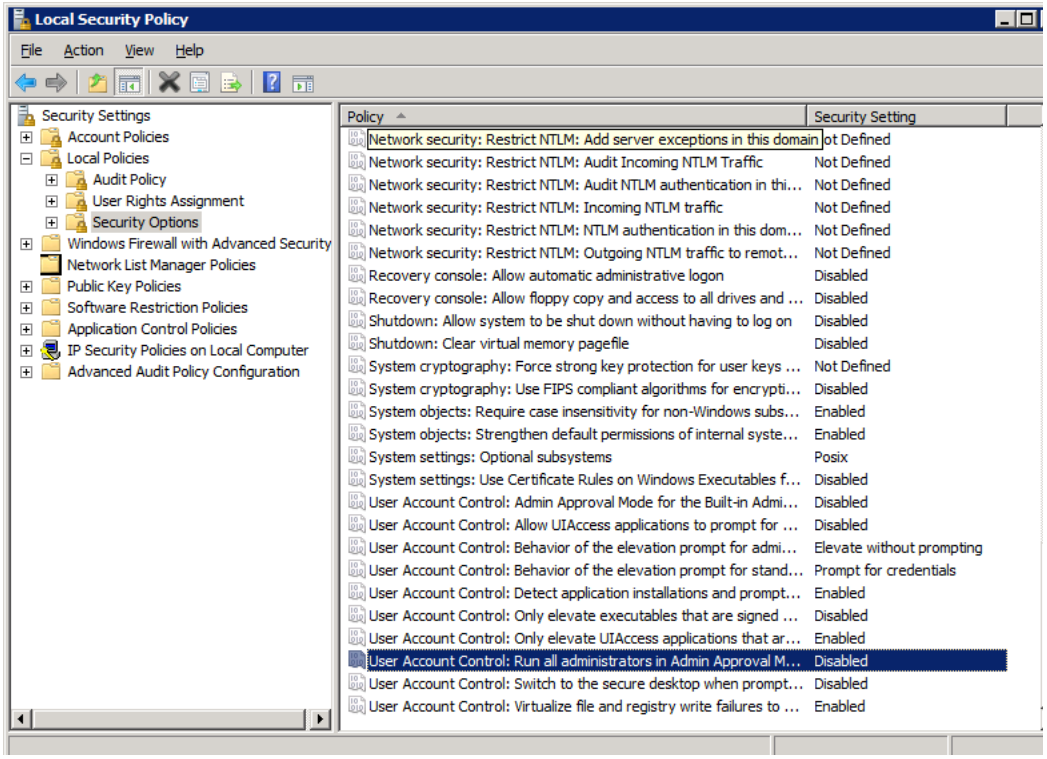


22 Double-click **User Account Control: Run all administrators in Admin Approval mode**.

23 On the **Local Security Setting** tab, select **Disable**.


Local Security Policy
File Action View Help
User Account Control: Run all administrators in Admin Approval ...
Local Security Setting
Explain
User Account Control: Run all administrators in Admin Approval Mode
Enabled
Disabled
OK
Cancel
Apply
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanc
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local C
Advanced Audit Policy Config
Security Setting
Not Defined
Not Defined
Not Defined
Not Defined
Not Defined
Not Defined
Disabled
Disabled
Disabled
Disabled
Not Defined
Disabled
Enabled
Enabled
Posix
Disabled
Disabled
Disabled
Elevate without prompting
Prompt for credentials
Enabled
Disabled
Enabled
Disabled
Disabled
Enabled

24 Click **OK**.


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Policy
Security Setting
Network security: Restrict NTLM: Add server exceptions in this domain
Network security: Restrict NTLM: Audit Incoming NTLM Traffic
Network security: Restrict NTLM: Audit NTLM authentication in thi...
Network security: Restrict NTLM: Incoming NTLM traffic
Network security: Restrict NTLM: NTLM authentication in this dom...
Network security: Restrict NTLM: Outgoing NTLM traffic to remot...
Recovery console: Allow automatic administrative logon
Recovery console: Allow floppy copy and access to all drives and ...
Shutdown: Allow system to be shut down without having to log on
Shutdown: Clear virtual memory pagefile
System cryptography: Force strong key protection for user keys ...
System cryptography: Use FIPS compliant algorithms for encrypti...
System objects: Require case insensitivity for non-Windows subs...
System objects: Strengthen default permissions of internal syste...
System settings: Optional subsystems
System settings: Use Certificate Rules on Windows Executables f...
User Account Control: Admin Approval Mode for the Built-in Admi...
User Account Control: Allow UIAccess applications to prompt for ...
User Account Control: Behavior of the elevation prompt for admi...
User Account Control: Behavior of the elevation prompt for stand...
User Account Control: Detect application installations and prompt...
User Account Control: Only elevate executables that are signed ...
User Account Control: Only elevate UIAccess applications that ar...
User Account Control: Run all administrators in Admin Approval M...
User Account Control: Switch to the secure desktop when prompt...
User Account Control: Virtualize file and registry write failures to ...
Not Defined
Not Defined
Not Defined
Not Defined
Not Defined
Not Defined
Disabled
Disabled
Disabled
Disabled
Not Defined
Disabled
Enabled
Enabled
Posix
Disabled
Disabled
Disabled
Elevate without prompting
Prompt for credentials
Enabled
Disabled
Enabled
Disabled
Disabled
Enabled

25 Select **File, Exit**.

26 Restart the Windows Server 2008 server.

--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 the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Create a folder **Avaya_Support** on the **C:** drive.
3	Download the most recent Contact Center service pack file and save it on the Contact Center server in the **Avaya_Support** folder.
4	Right-click the service pack .zip file and select **Extract All** from the context menu.

--End--

Disabling Internet Protocol version 6

Disable Internet Protocol version 6 (IPv6) to ensure correct operation of the contact center software.

Attention: this procedure requires modification of the Windows Server 2008 registry. This is an advanced administrator function: if you are not qualified to carry out edits to the registry, ask a qualified person to complete this procedure.

Attention: The published steps are extracted from Microsoft article 929852. Check the Microsoft support site to ensure that you use the most up to date procedure.

Step	Action
1	Search the Microsoft support site to locate the instructions to disable IPv6 in the Windows Server 2008 registry.
2	On the Windows server, click **Start**.
3	Type **regedit** in the **Start Search** box, and then click **regedit.exe** in the **Programs** list.
4	In the **User Account Control** dialog box, click **Continue**.

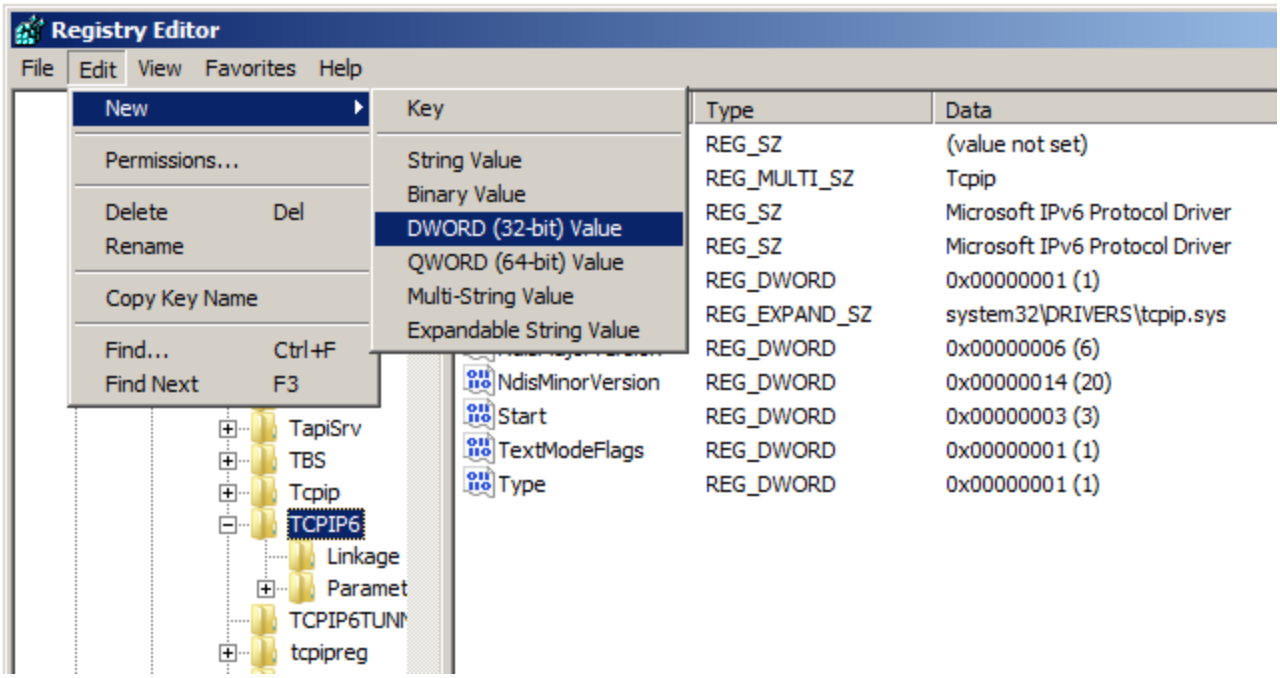
5 In Registry Editor, locate and then click the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP6\Parameters\

6 Double-click **DisabledComponents** to modify the **DisabledComponents** entry.

7 If the **DisabledComponents** entry is unavailable, you must create it by following steps 8 to 9. Otherwise go to step 10.

8 From the **Edit** menu, choose **New**, and select **DWORD (32-bit) Value**.

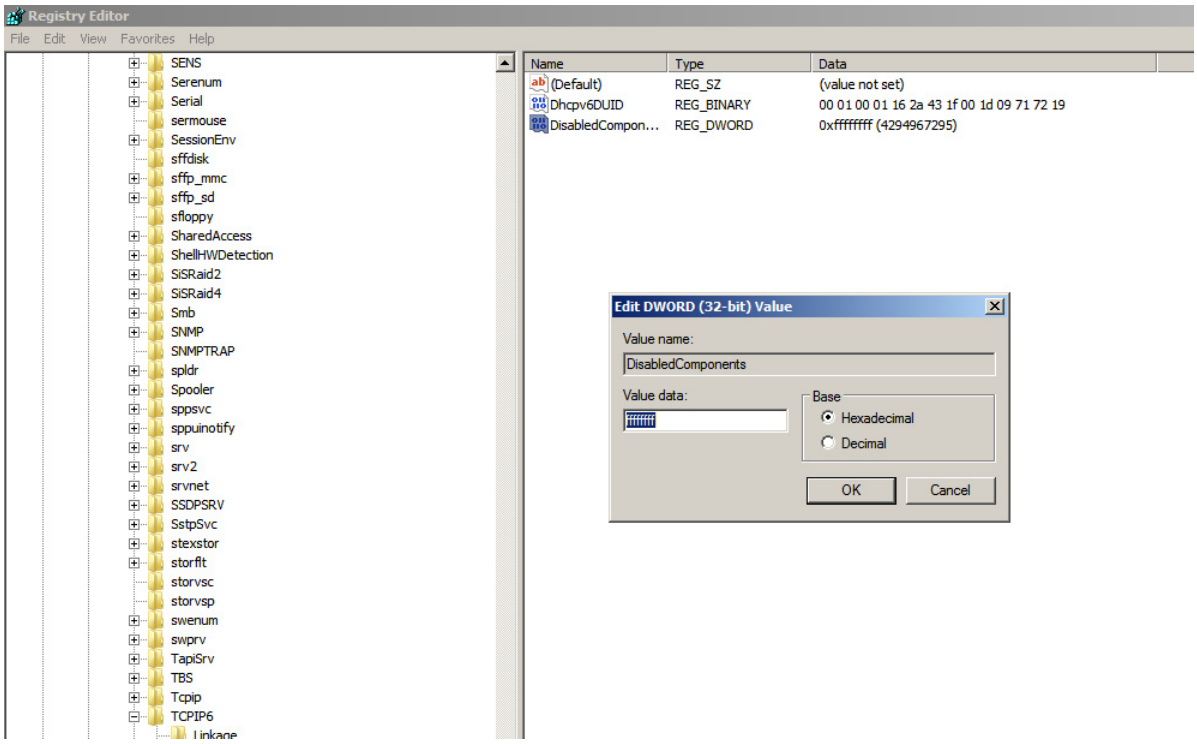


9 Type **DisabledComponents**, and then press **Enter**.

10 Double-click **DisabledComponents**.

11 Select **Hexadecimal**.

12 In the Value data: box Type **ffffffff** to disable all IPv6 components.



13 Click **OK**.

14 Reboot the server, if required.

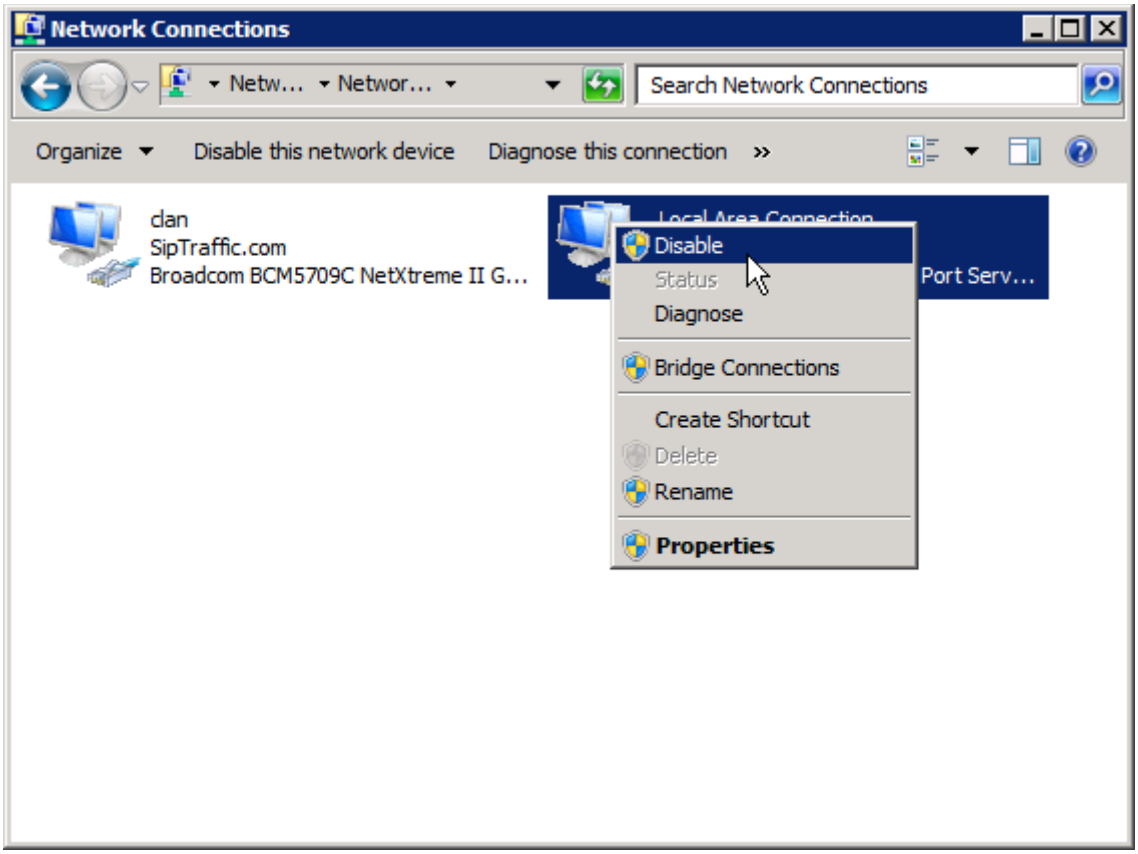
--End--

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 the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Click **Start**, **Control Panel**, **Network and Internet**, **Network and Sharing Center**, **Change Adaptor Settings**.
3	Right-click the unused Network Adaptor, and select **Disable**.



4 Repeat this procedure for all unused Network Adapters.

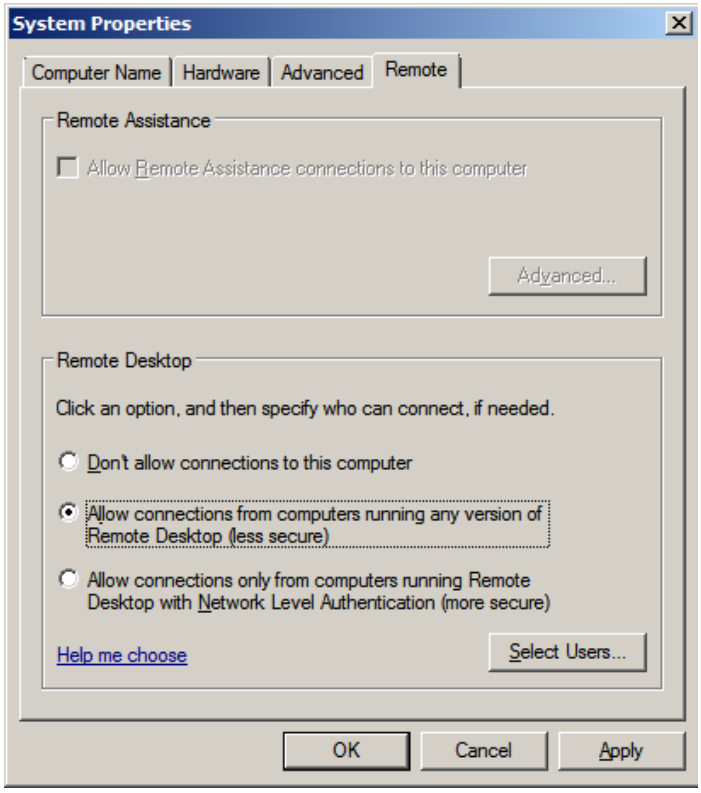
--End--

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	Choose **Start**, **Control Panel**, **System and Security**.
2	In the **System** section, select **Allow remote access**.
3	Click the **Remote** tab.
4	Select **Allow connections from computers running any version of Remote Desktop (less secure)**.



5 On the **Remote Desktop Connection** window, click **OK**.

6 Click **OK**.

--End--

Configuring Data Execution Prevention

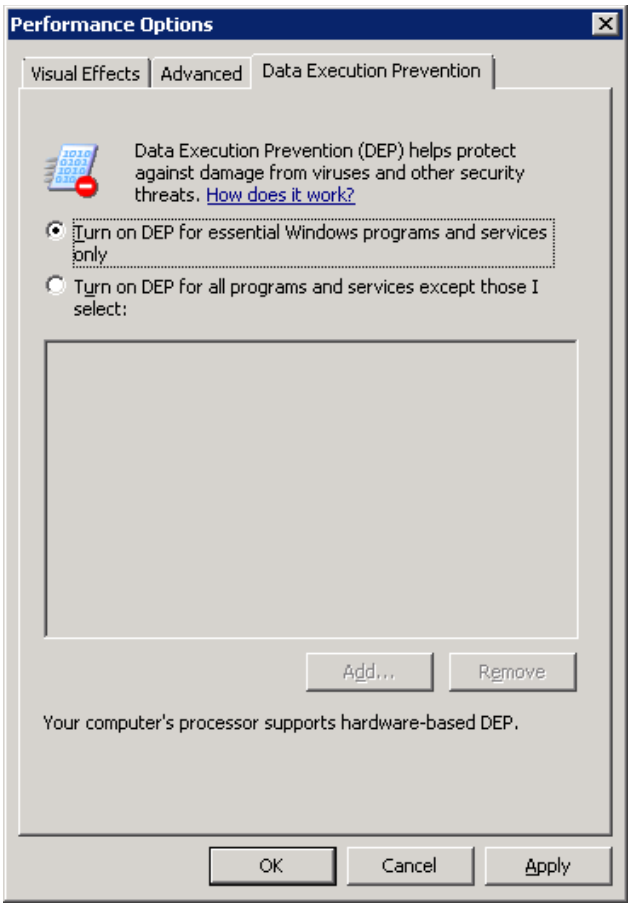
Configure the Data Execution Prevention (DEP) hardware and software to perform additional checks on memory that protect the Contact Center server against malicious code exploitation.

Procedure steps

Step	Action
1	Choose **Start, Control Panel, System and Security**.
2	Click **System**.
3	In the **System** window, click **Advanced system settings**.
4	In the **System Properties** dialog box, click the **Advanced** tab.
5	Under **Performance**, click **Settings**.

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

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



8 Click **OK**.

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

10 If prompted, click **OK** to restart the computer.

--End--

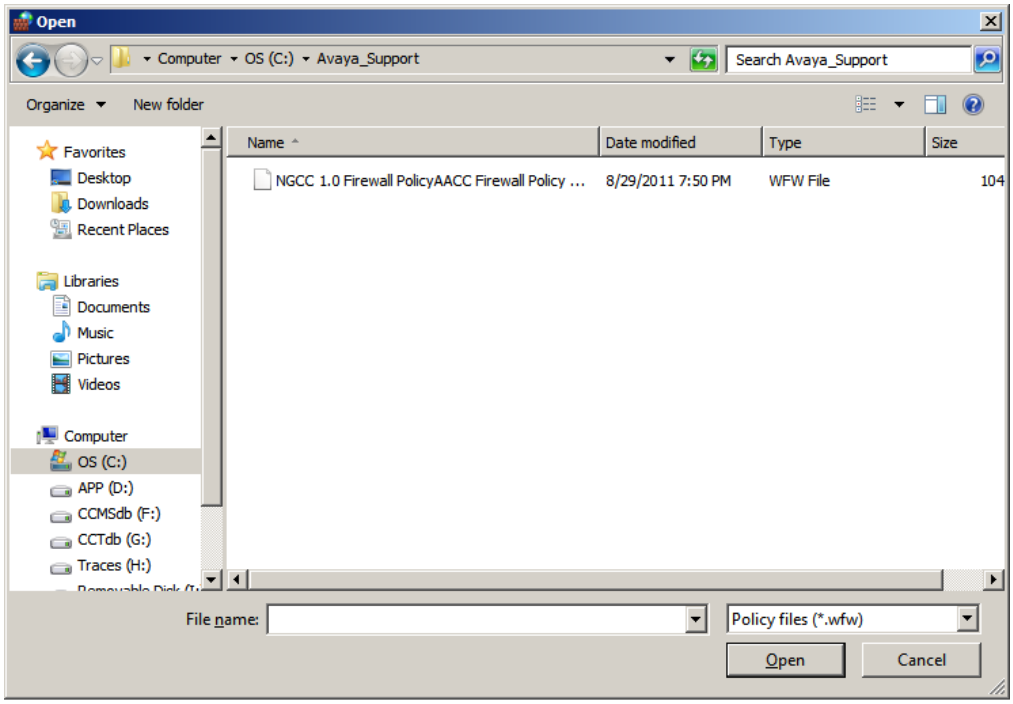
Importing the Contact Center Firewall Security policy

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

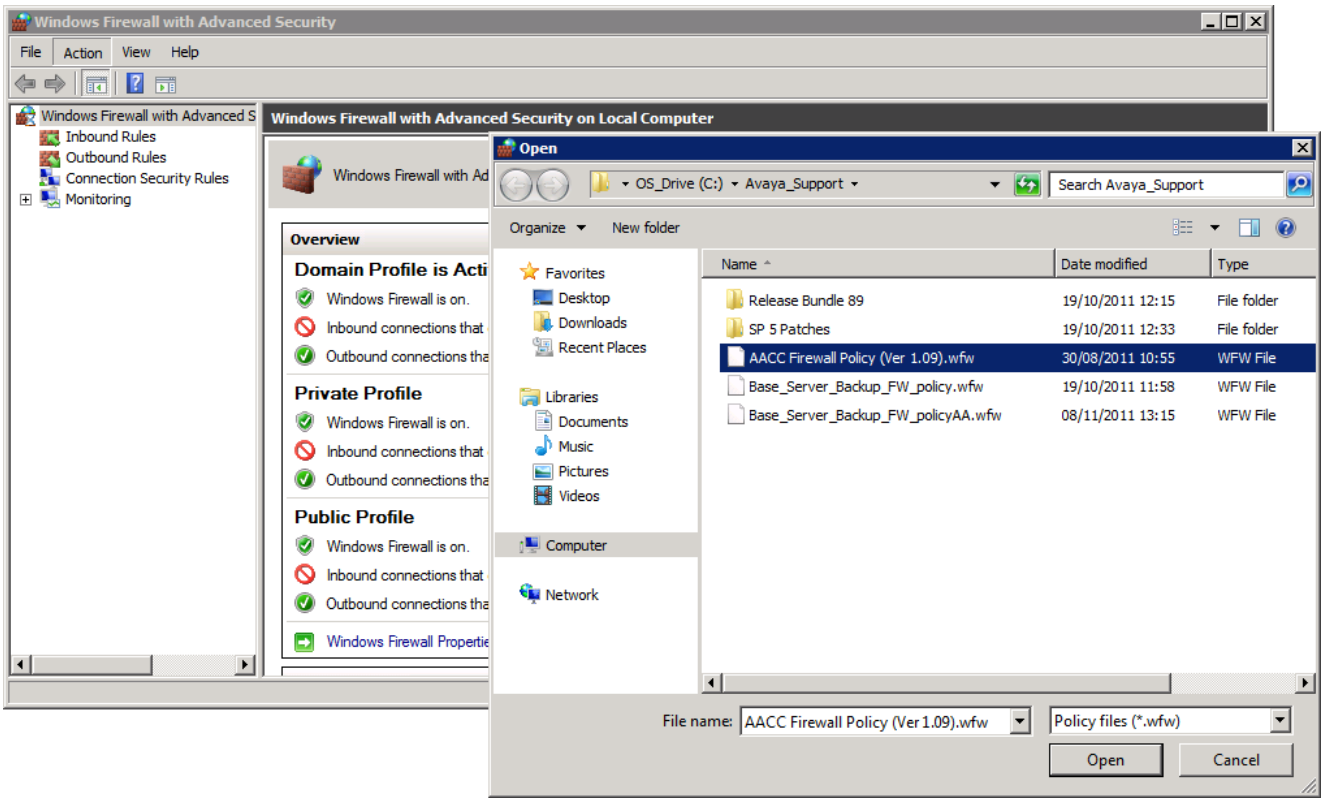
Export and backup your existing firewall security policy before importing the Avaya Aura® Contact Center Firewall Security policy. You can use this backup policy to rollback the Avaya Aura® Contact Center Firewall Security policy.

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 the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
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.
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.



11 Select the Avaya Aura® CC Firewall Policy you downloaded, for example **AACC Firewall Policy (Ver 1.09).wfw**.

12 Click **Open**.

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

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

--End--

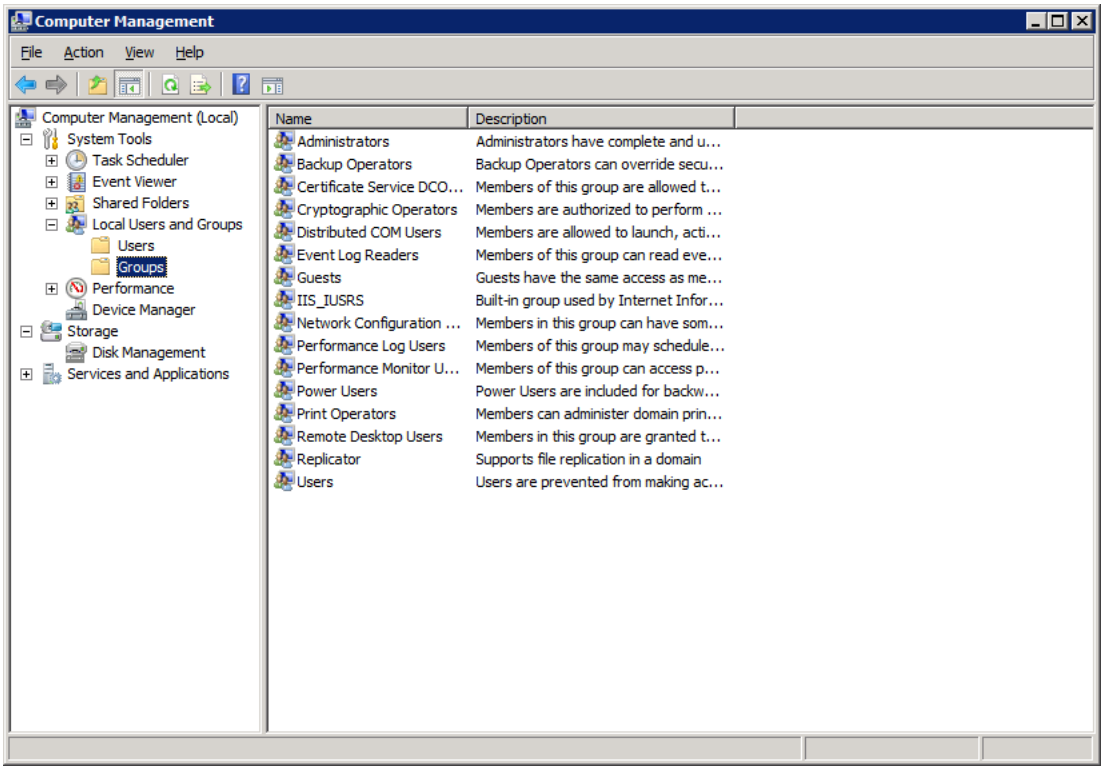
Adding the domain AD-LDS replication account to the Standby server administrators and replicator group

Add the AD-LDS replication account to the local Administrators and replicator group on the Standby CCMA server.

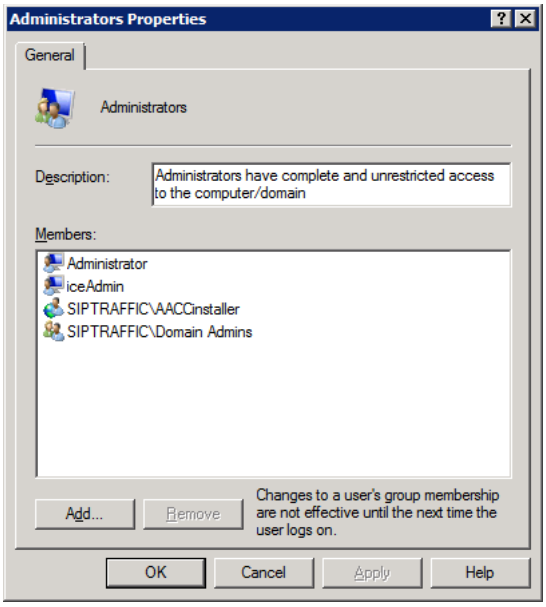
This must be the same account that you added to the Active server. See Adding the domain AD-LDS replication account to the Active server administrators and replicator group (page 319)

Procedure steps

Step	Action
1	Log on to the Standby server (for example, **CCCORESTWO**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Click **Start**, **Administrative Tools**, **Computer Management**.
3	In the **Computer Management** window, expand **Local Users and Groups**.
4	Click the **Groups** folder.

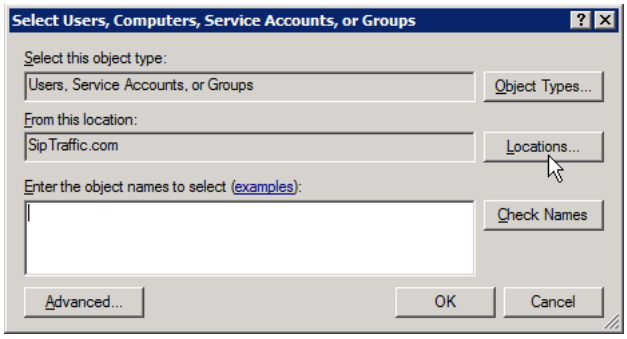


5	Double-click on the **Administrators** group.

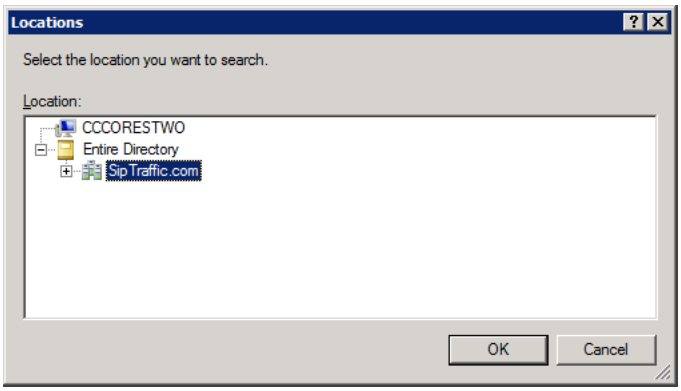


6 On the **Administrators Properties** window, click **Add**.

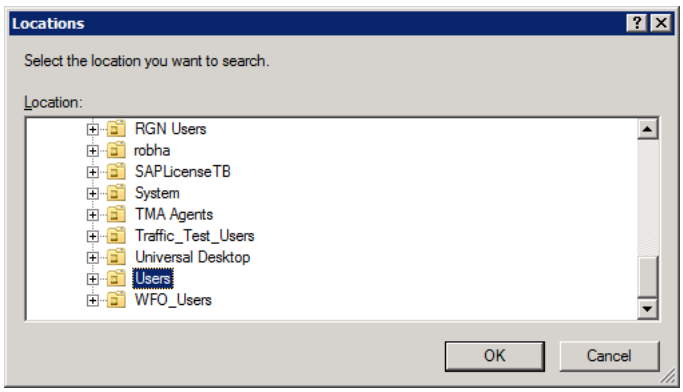
7 On the **Select Users**, **Computers**, **Service Accounts**, **or Groups** window, **click Locations**.



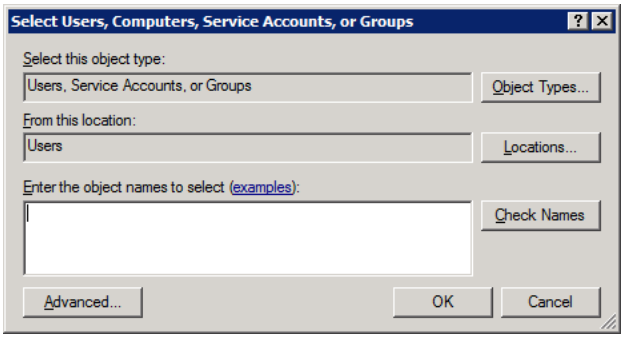
8 On the **Locations** dialog, select the domain for CCMA to use for replication, for example **siptraffic.com**.



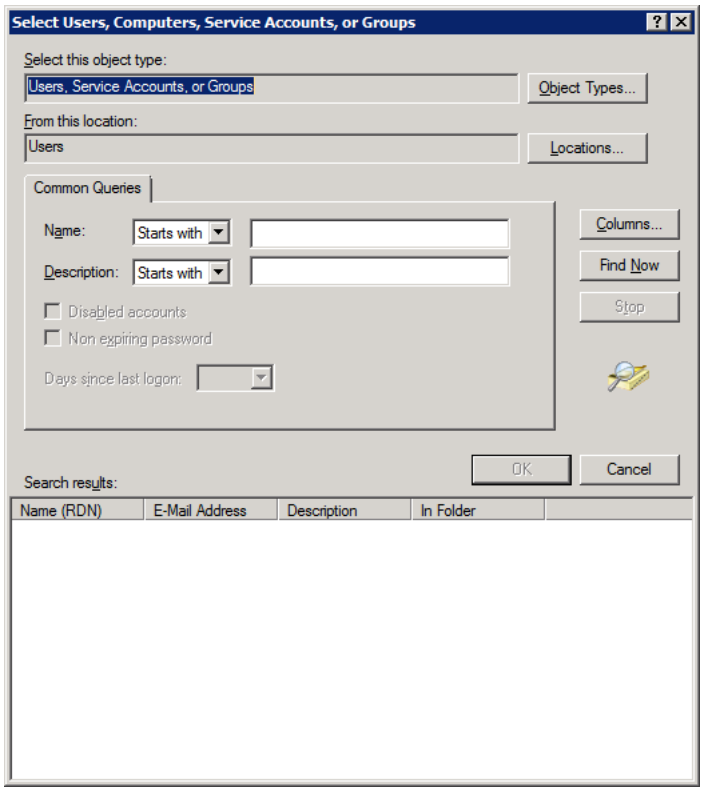
9 Expand the domain folder, scroll down and select **Users**.



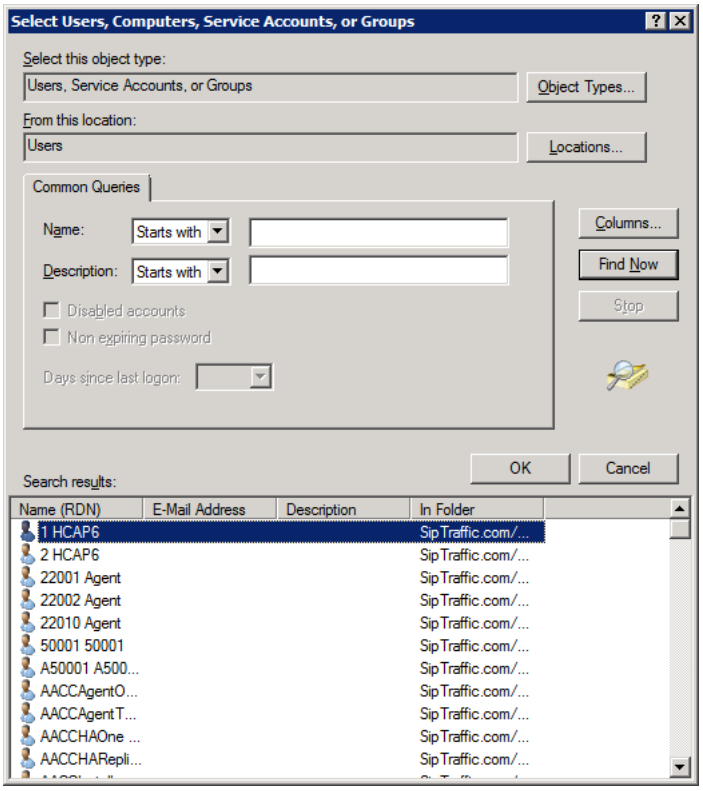
10 Click **OK**.



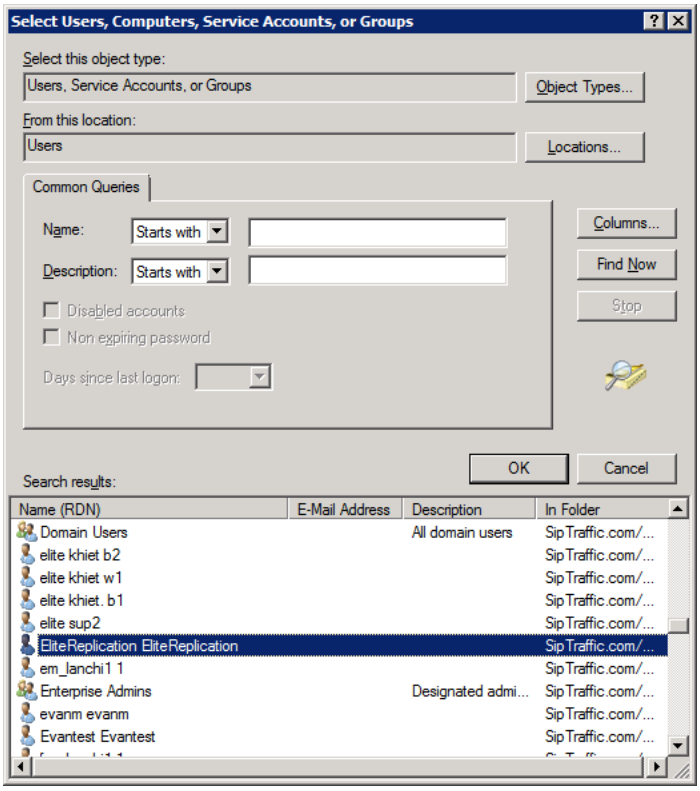
11 Click **Advanced**.



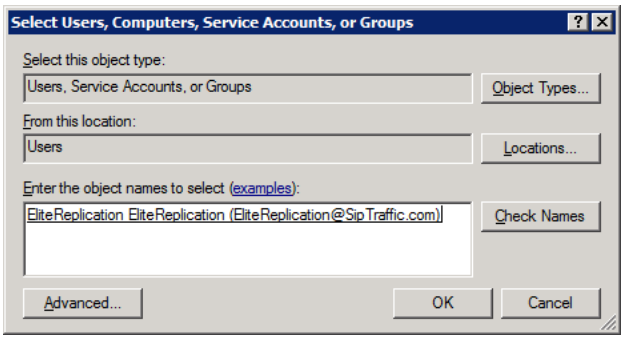
12 Click **Find Now**, to display domain users.



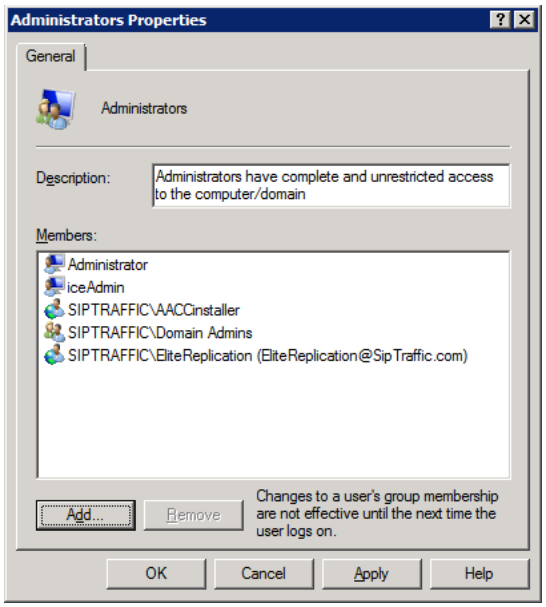
13 From the list of domain users, select the CCMA replication domain user account, for example **EliteReplication**.



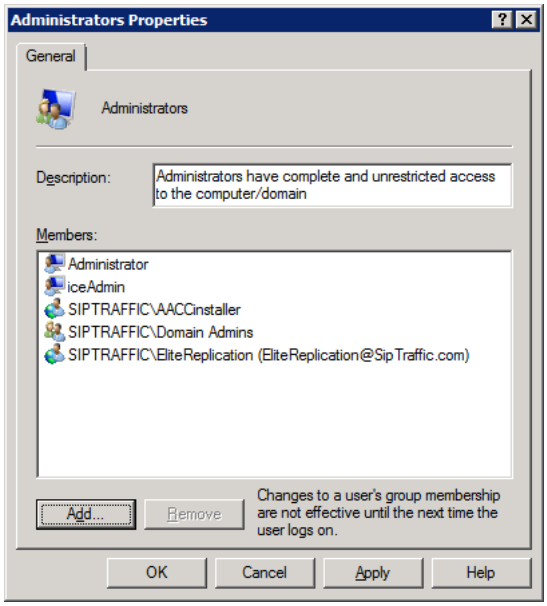
14 Click **OK**.



15 Click **OK**.

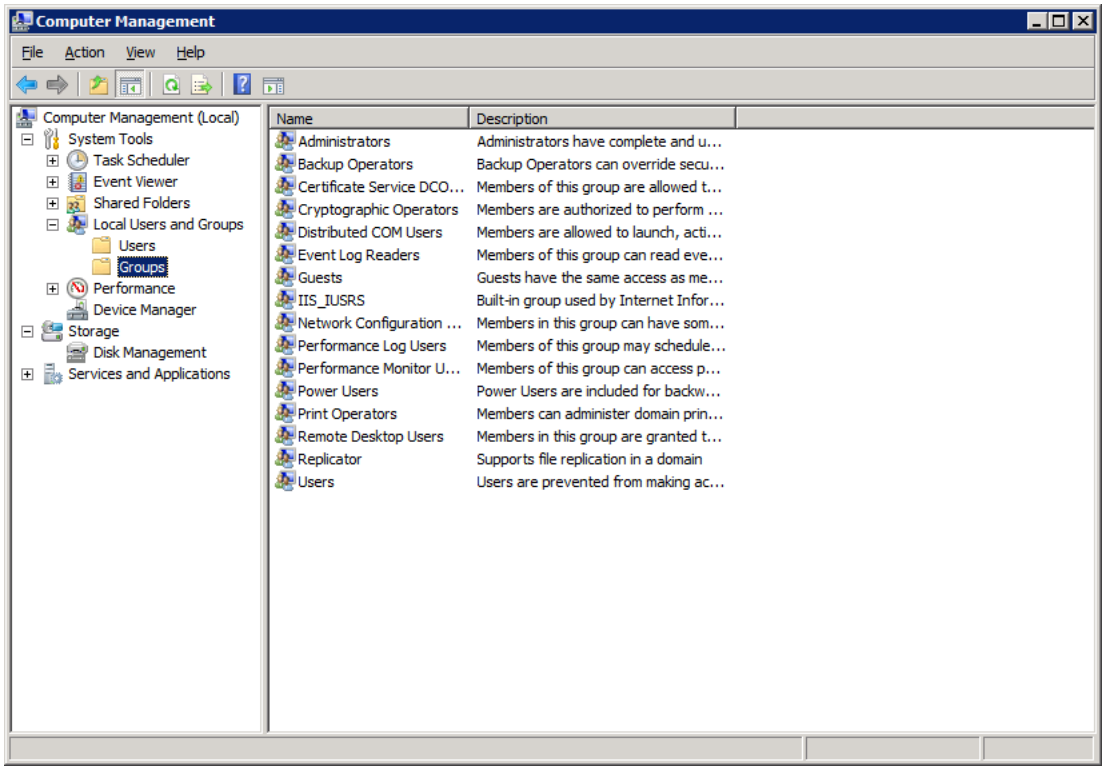


16 Click **Apply**.



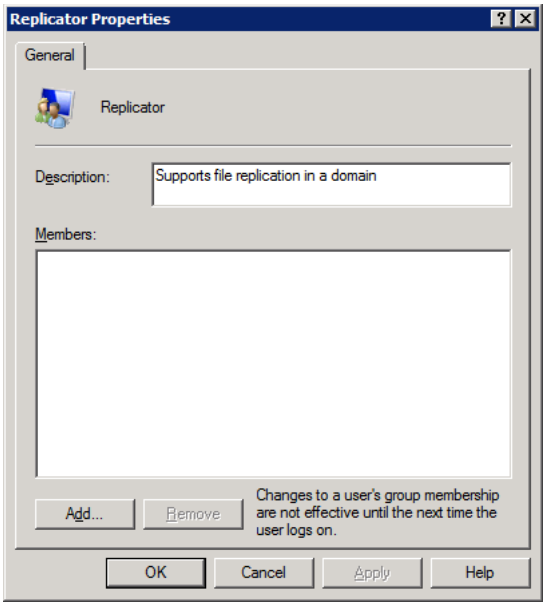
17 Click **OK**.

18 Click the **Groups** folder.

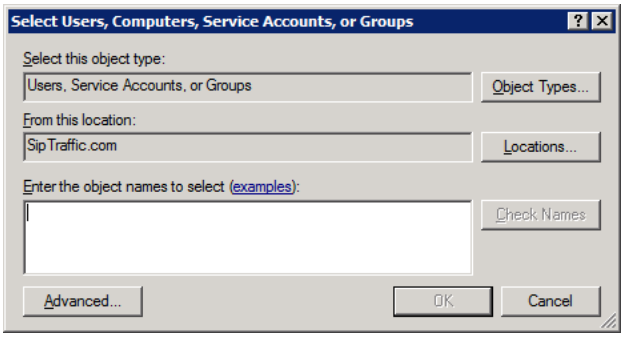


19 Double-click on the **Replicator** group.

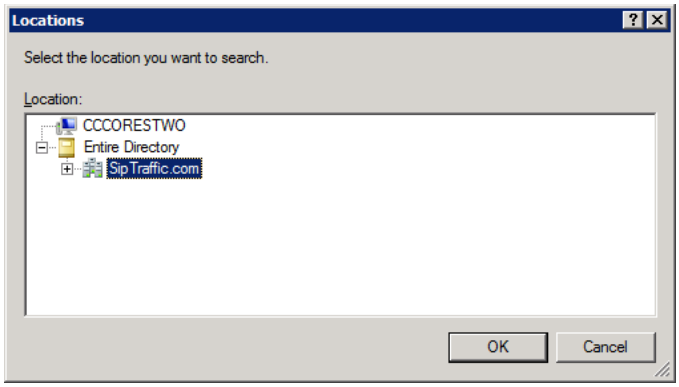
20 Click **Add**.



21 Click **Locations**.

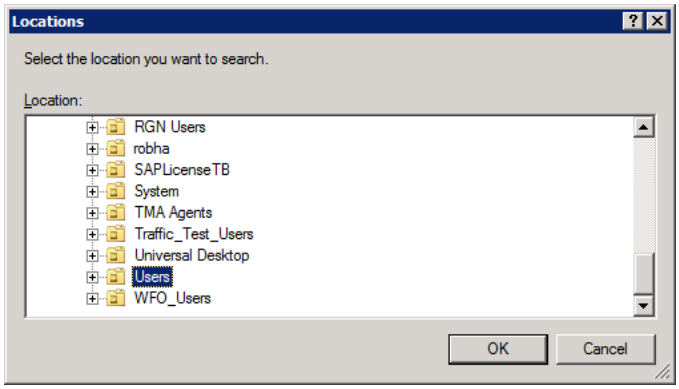


22 On the **Locations** dialog, select the domain to be used by CCMA replication. For example, select siptraffic.com.

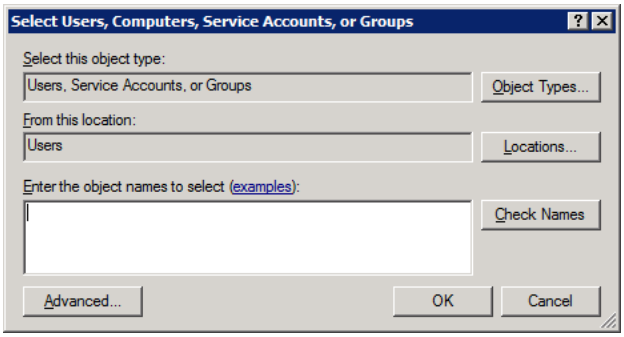


23 Expand the domain folder to display domain users.

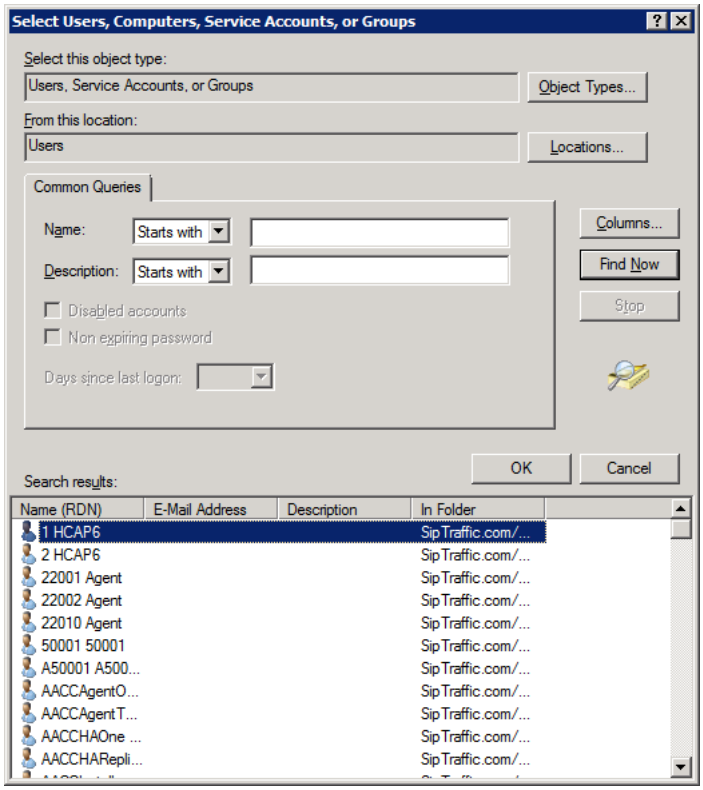
24 Click **Users**.



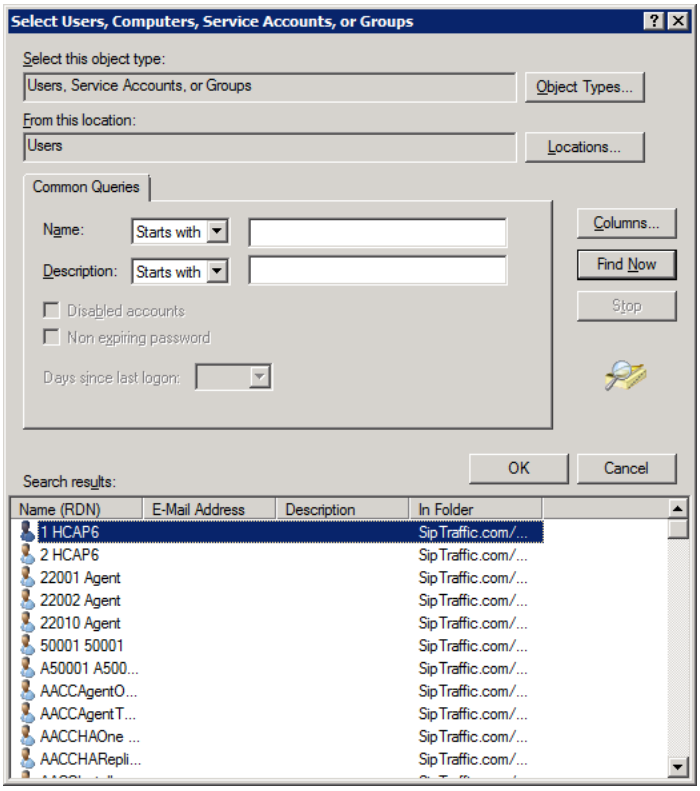
25 Click **OK**.



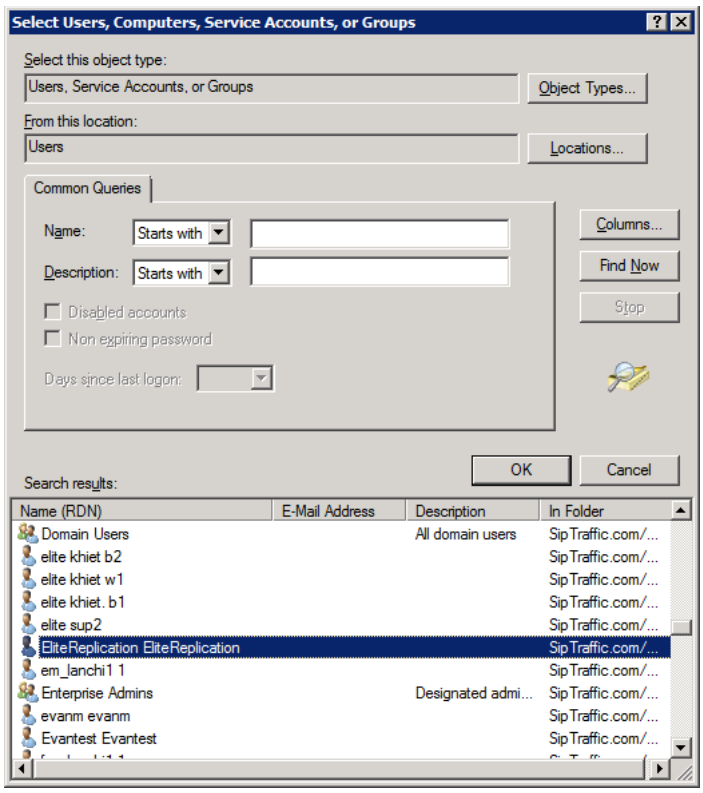
26 Click **Advanced**.



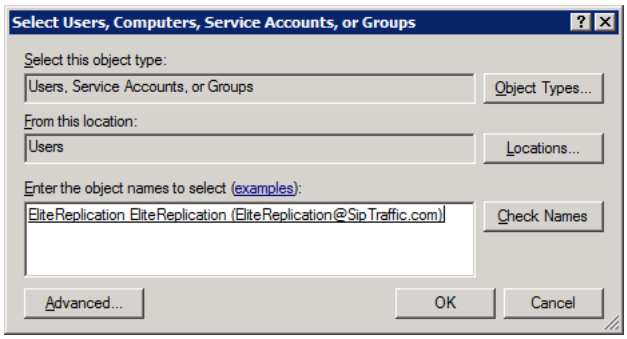
27 Click **Find Now**, to display domain users.



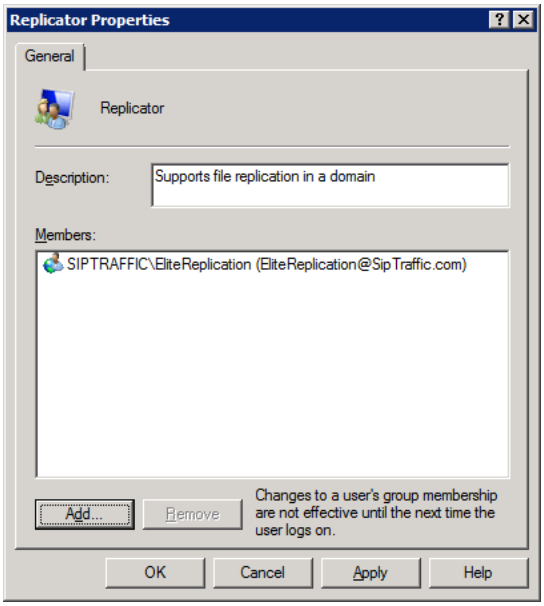
28 From the list of users select the CCMA replication domain user account, for example siptraffic\EliteReplication.



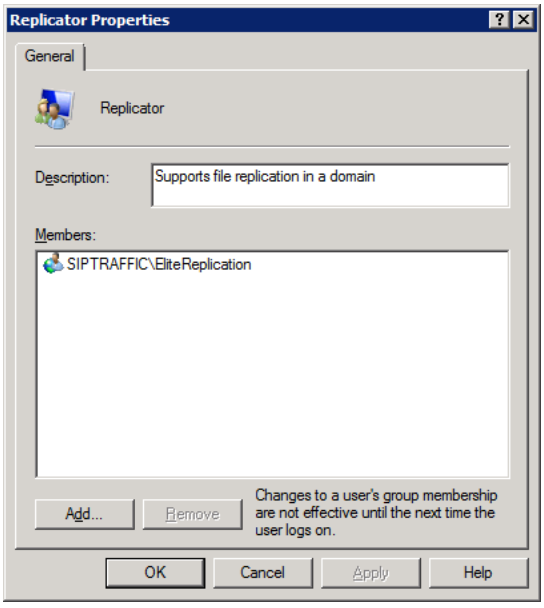
29 Click **OK**.



30 Click **OK**.



31 Click **Apply**.



32 Click **OK**.

--End--

Standby Contact Center server software installation

This chapter provides the steps to install the Avaya Aura® Contact Center server software on the server. This includes the following server software:

- Contact Center Manager Server
- Communication Control Toolkit
- Contact Center Multimedia
- Contact Center Manager Server Utility
- Contact Center License Manager
- Contact Center Manager Administration
- Orchestration Designer

Prerequisites to co-resident server software installation

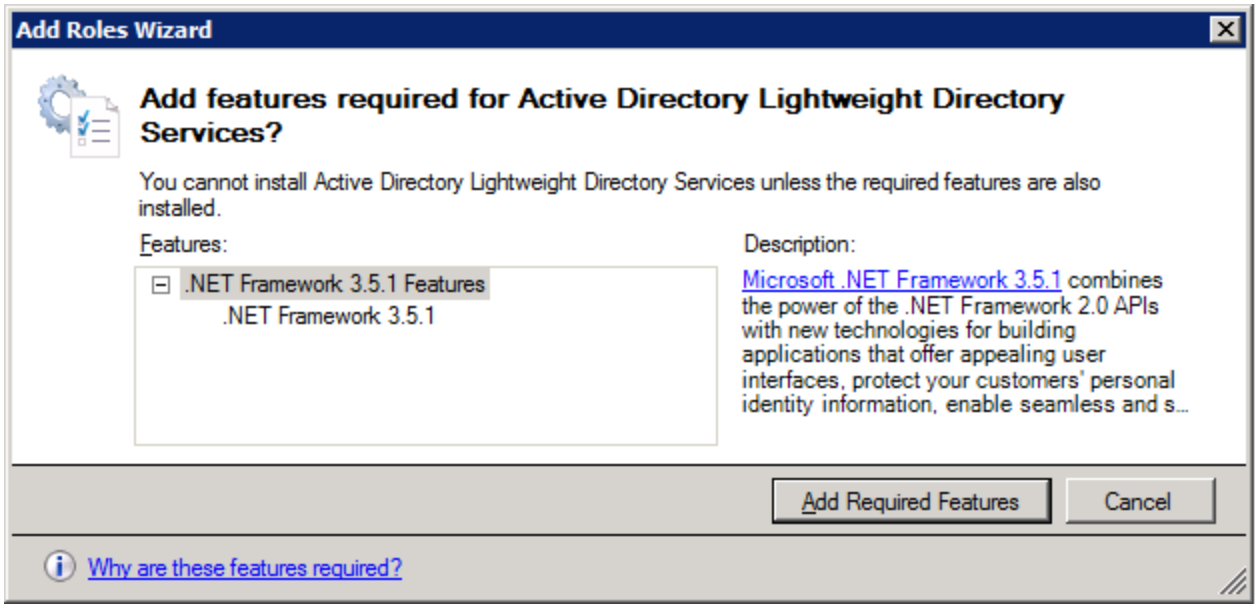
- Ensure that your have your updated Contact Center license file.
- Ensure that you have the Contact Center Release 6.2 DVD.

Installing operating system components for Contact Center Manager Administration

Before installing Contact Center Manager Administration, you must install specific operating system software components such as Internet Information Services to integrate with the components in Contact Center.

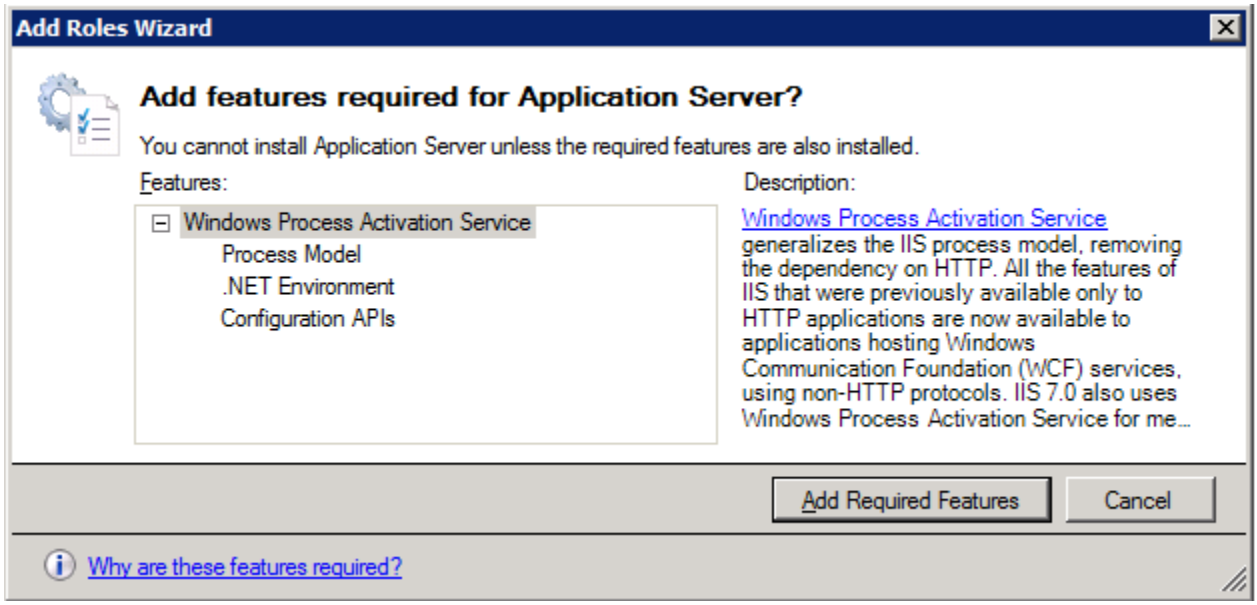
Procedure steps

Step	Action
1	Log on to the Standby server (for example, **CCCORESTWO**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Choose **Start**, **Administrative Tools**, **Server Manager**.
3	In the left-hand column of the **Server Manager**, right-click **Roles** and select **Add Roles**.
4	Review the requirements for the new role, and click **Next**.
5	Under **Server Roles**, select **Active Directory Lightweight Directory Services**.
6	If an **Add Roles Wizard** message box that lists features required by Active Directory Lightweight Directory Services appears, click **Add Required Features**.



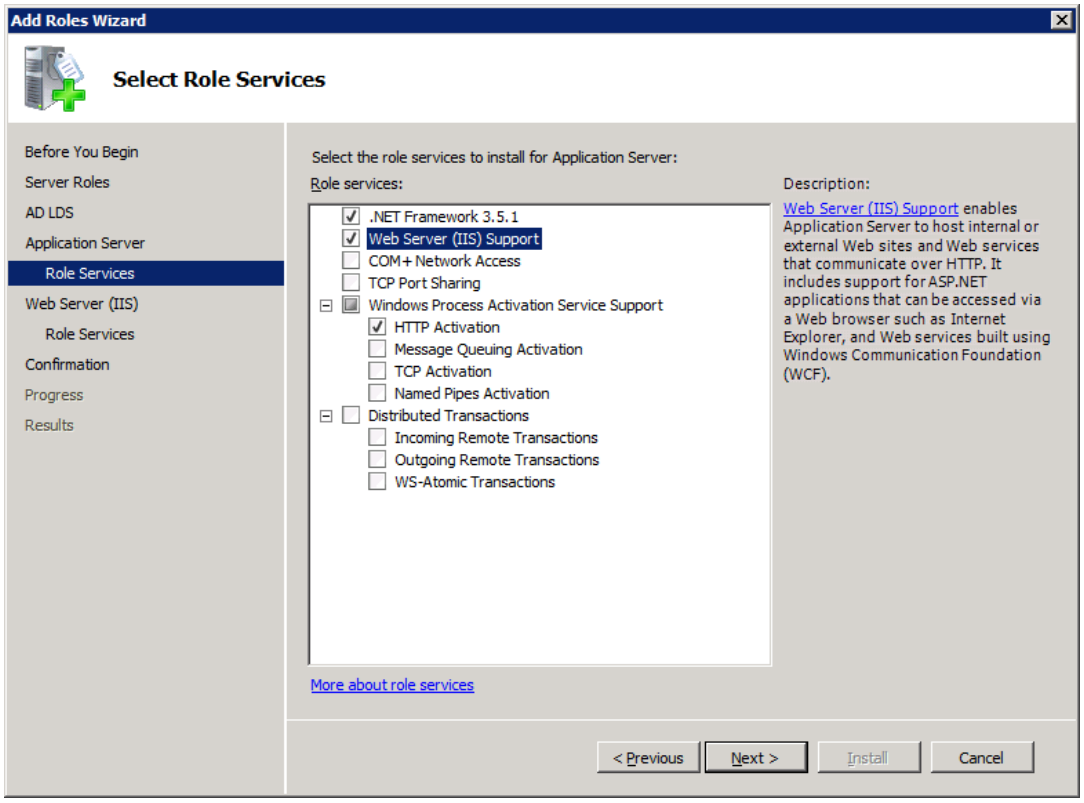
7 Under **Server Roles**, select **Application Server**.

8 If an **Add Roles Wizard** message box that lists features required by Application Server appears, click **Add Required Features**.

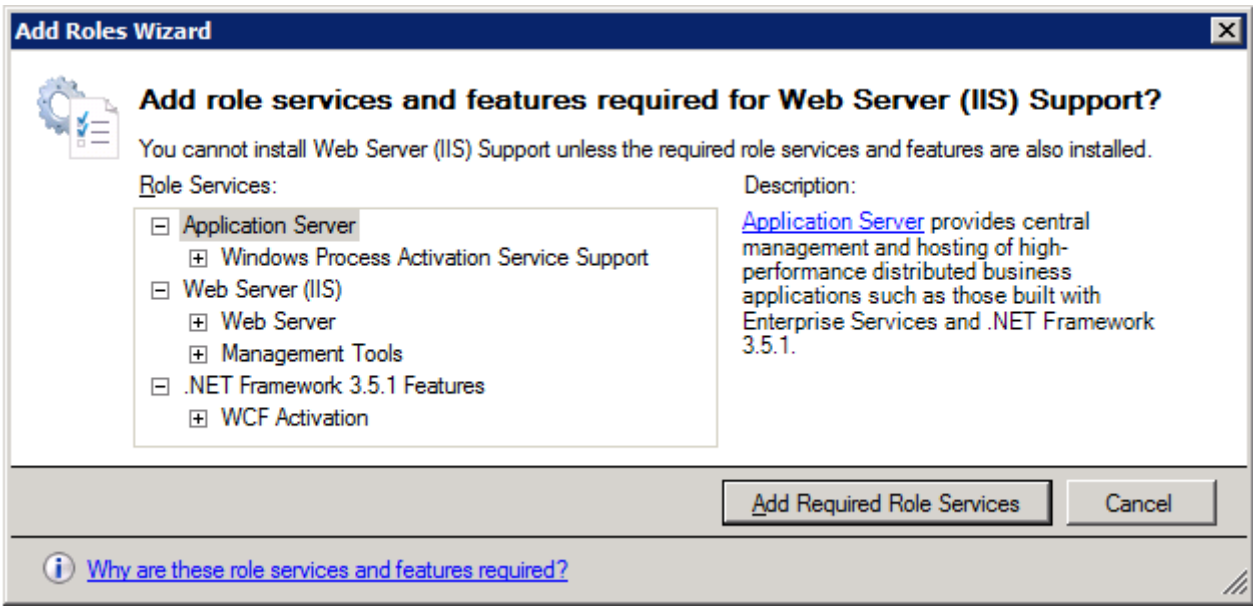


9 In the left pane, under **Application Server**, select **Role Services**.

10 Select **Web Server (IIS) Support**.



11 If an **Add Roles Wizard** message box appears, listing features required by Web Server (IIS) Support, click **Add Required Role Services**.



12 Click **Next**.

13 On the **Introduction to Web Server (IIS)** page, click **Next**.

14 On the **Select Role Services** page, under **Common HTTP Features**, select the following services:

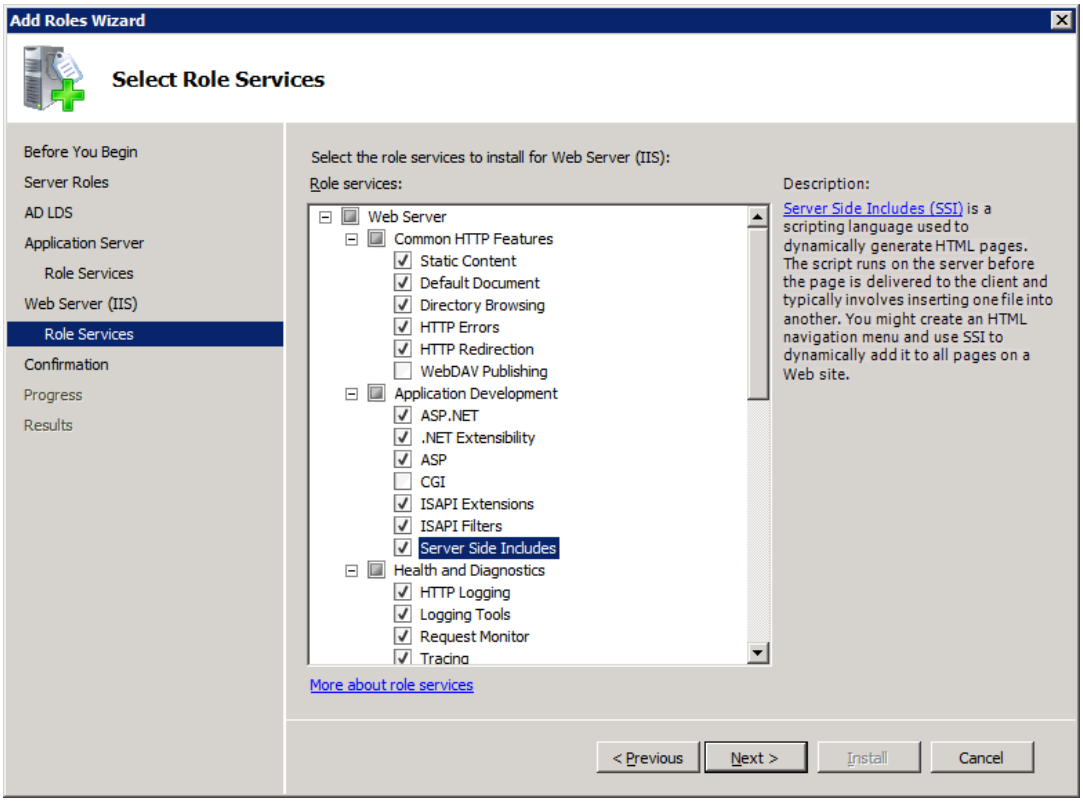
- Static Content
- Default Document
- Directory Browsing
- HTTP Errors
- HTTP Redirection

Attention: Clear the check boxes for all other services.

15 On the **Select Role Services** page, under **Application Development**, select the following services:

- ASP.NET
- .NET Extensibility
- ASP
- ISAPI Extensions
- ISAPI Filters
- Server Side Includes

Attention: Clear the check boxes for all other services.



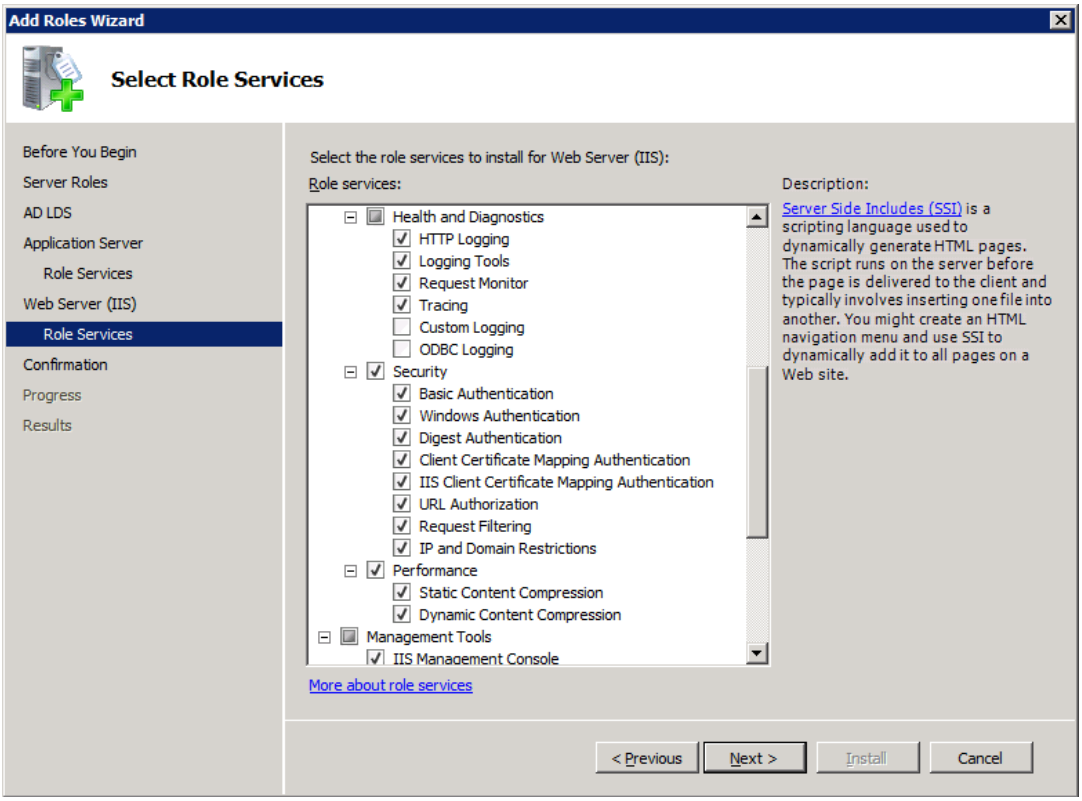
16 On the **Select Role Services** page, under **Health and Diagnosis**, select the following services:

- HTTP Logging
- Logging Tools
- Request Monitor
- Tracing

Attention: Clear the check boxes for all other services.

17 On the **Select Role Services** page, under **Security**, select all services.

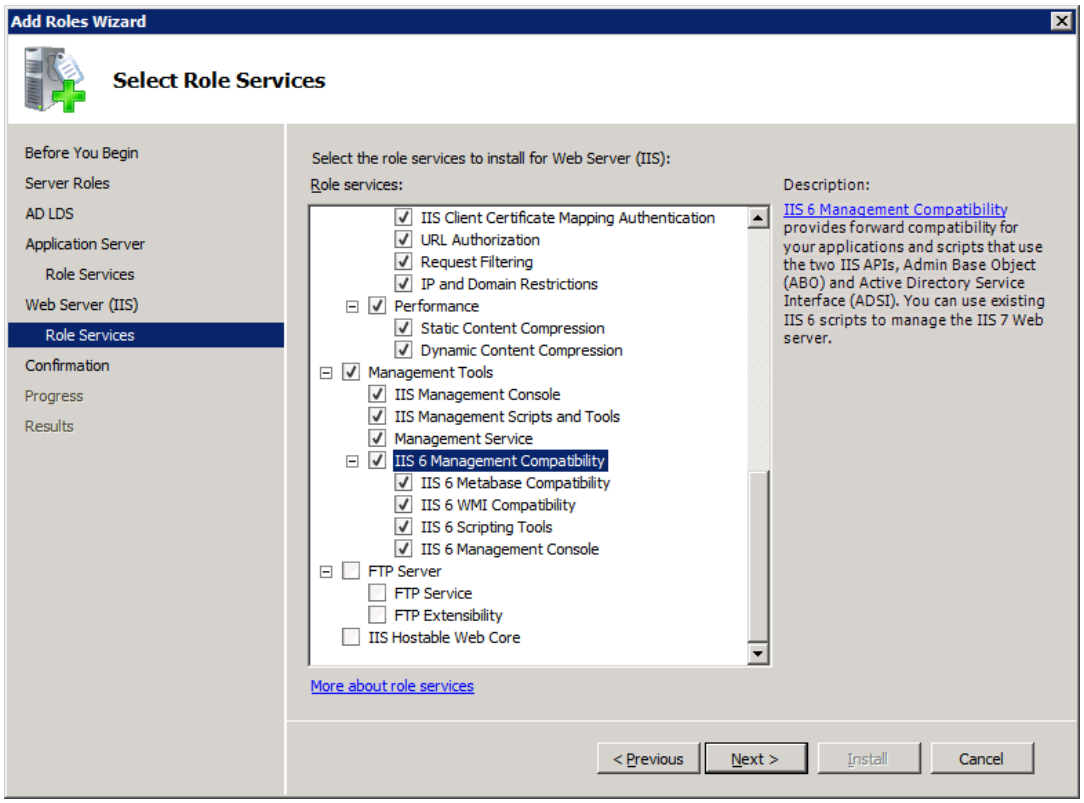
18 On the **Select Role Services** page, under **Performance**, select all services.



19 On the **Select Role Services** page, under **Management Tools**, select the following services:

- IIS Management Console
- IIS Management Scripts and Tools
- Management Service
- All items under IIS 6 Management Compatibility

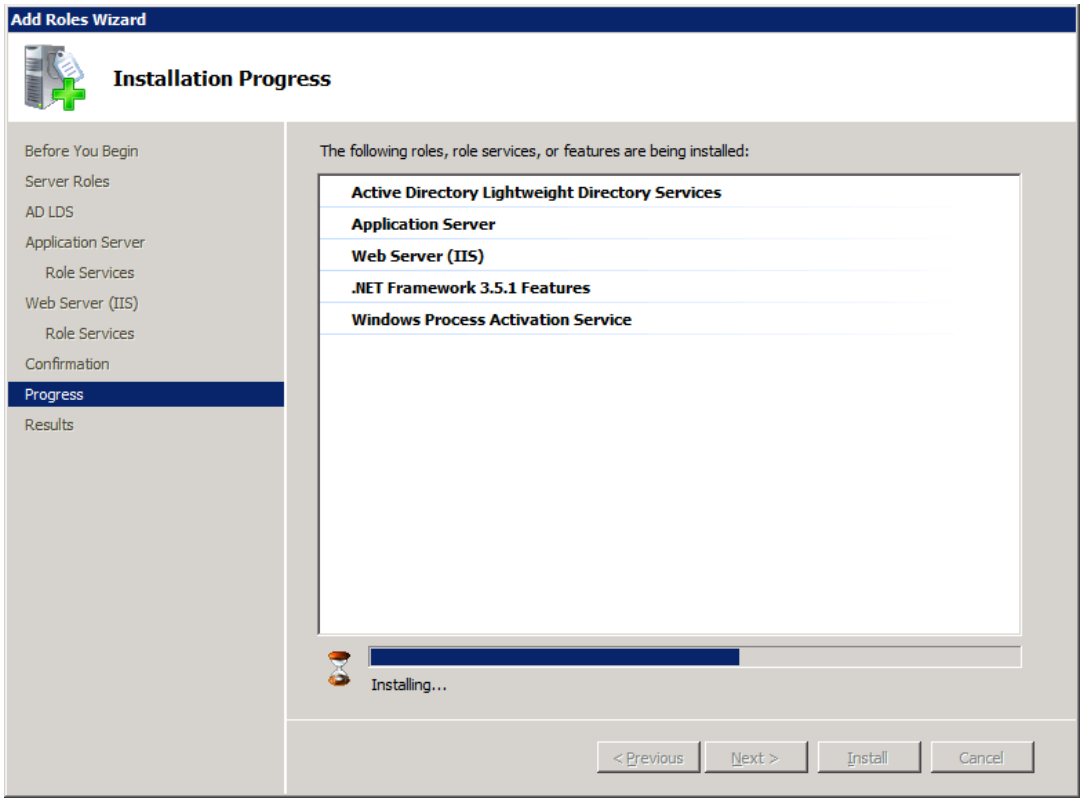
Attention: Clear the check boxes for all other services.



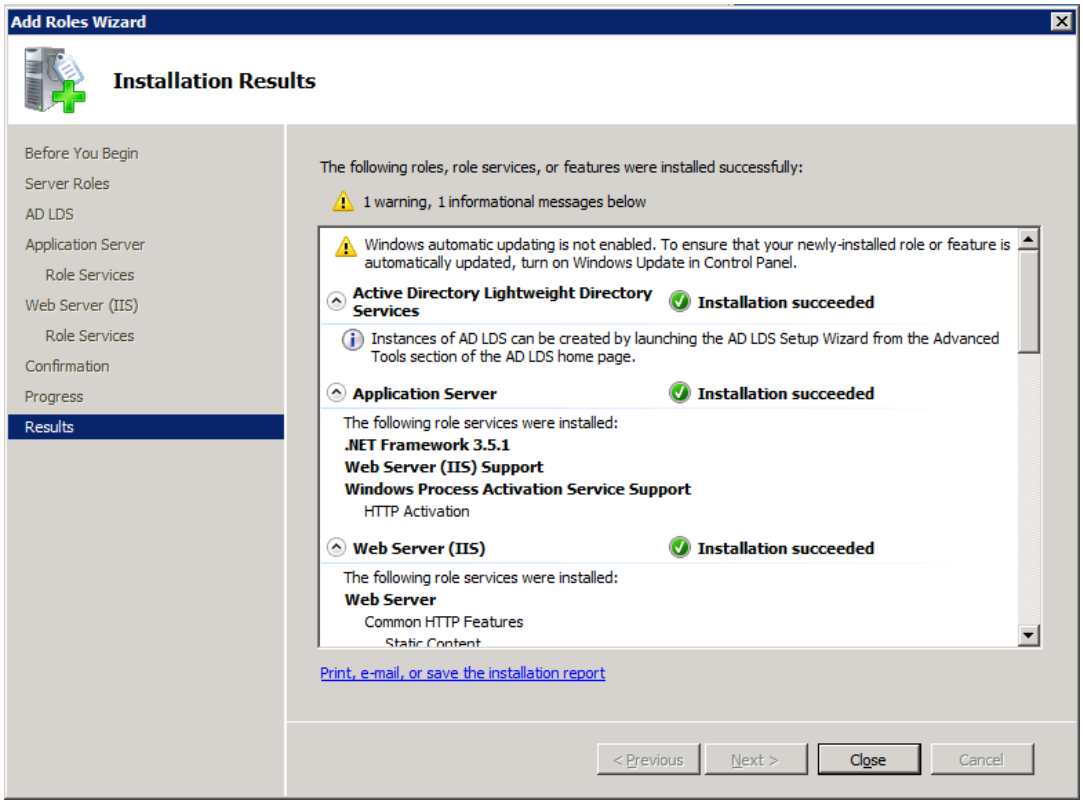
20 Click **Next**.

21 Review the installation information.

22 Click **Install**.



23 On the **Installation Results** page, click **Close**.



24 Restart the server if required.

--End--

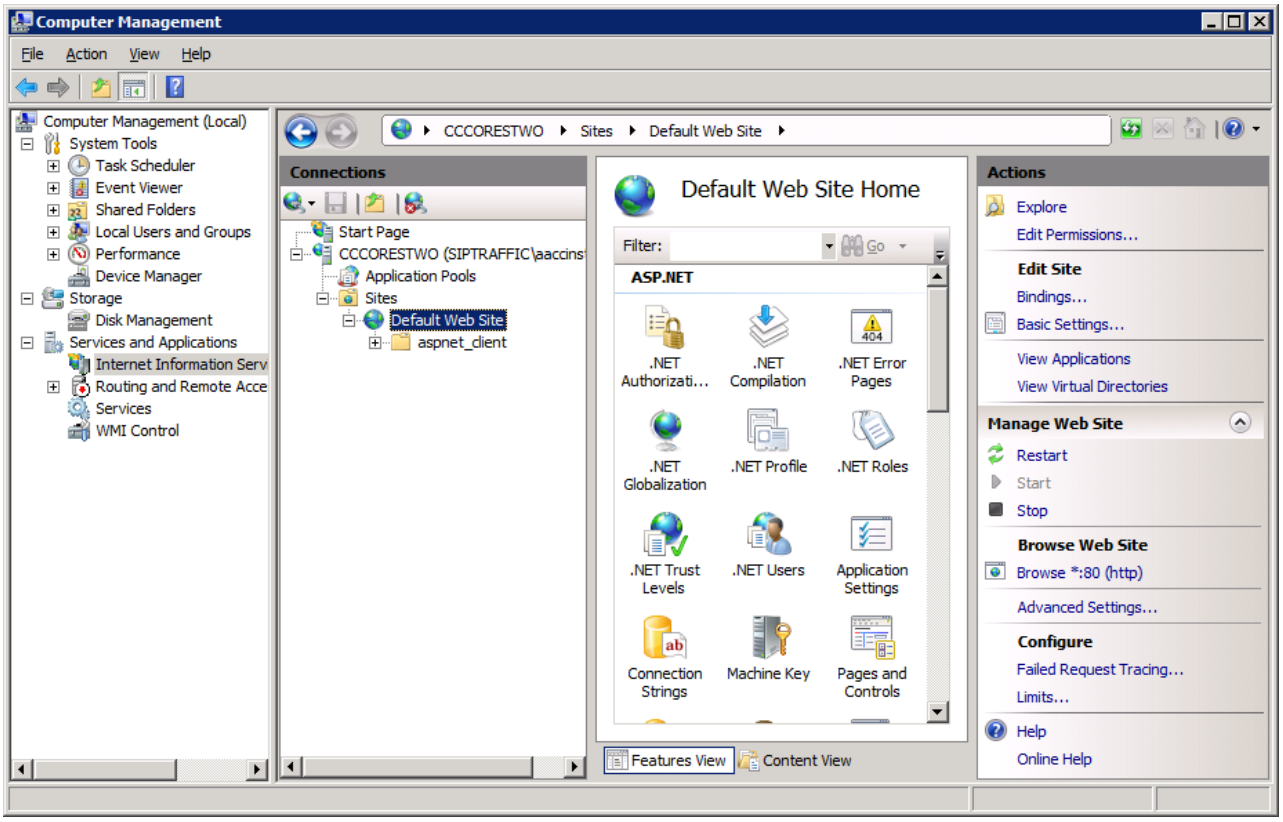
Configuring MIME types to support Microsoft updates

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

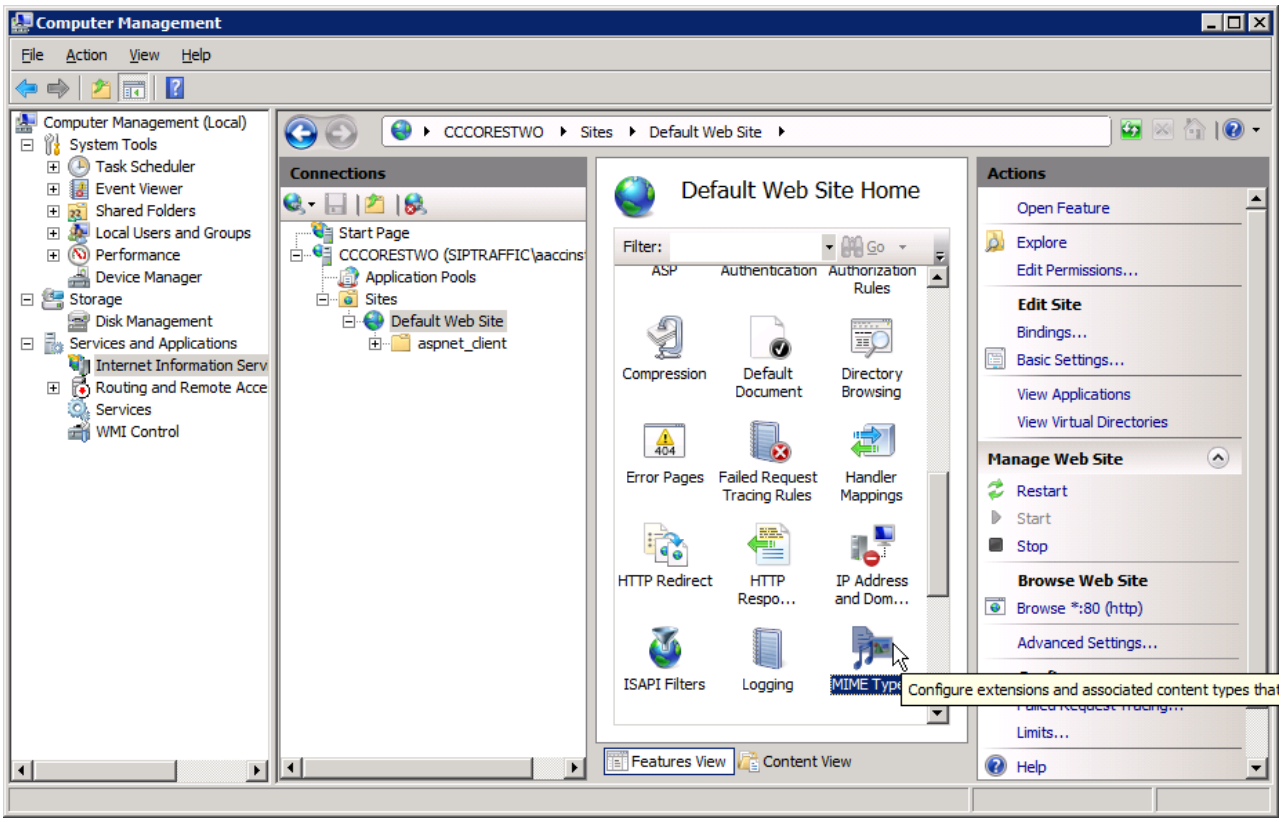
Procedure steps

Step	Action
1	Log on to the Standby server (for example, **CCCORESTWO**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
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 the default web site, for example **CCCORESTWO**, **Sites**, **Default Web Site**.

5 Select **Default Web Site**.



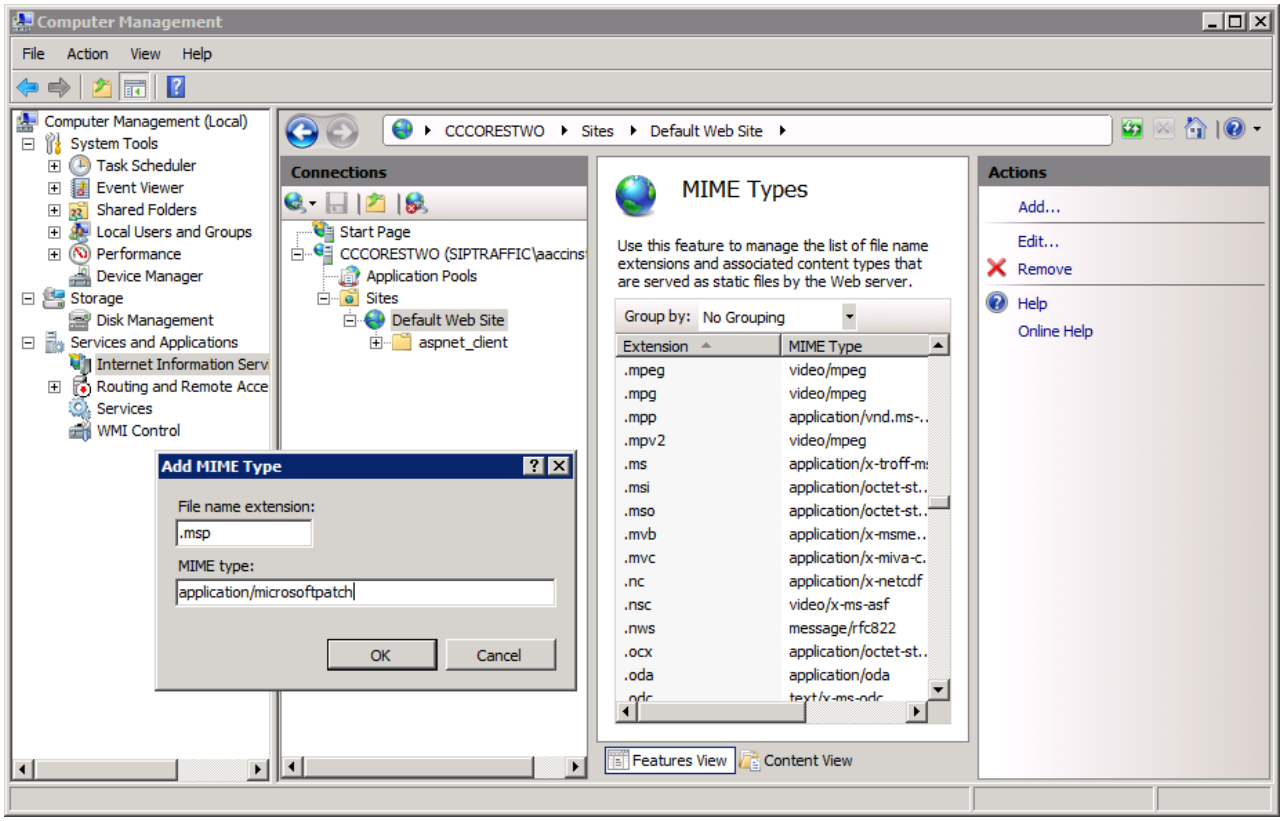
6 In the **Default Web Site Home** pane, under **IIS**, double-click **MIME Types**.



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**.

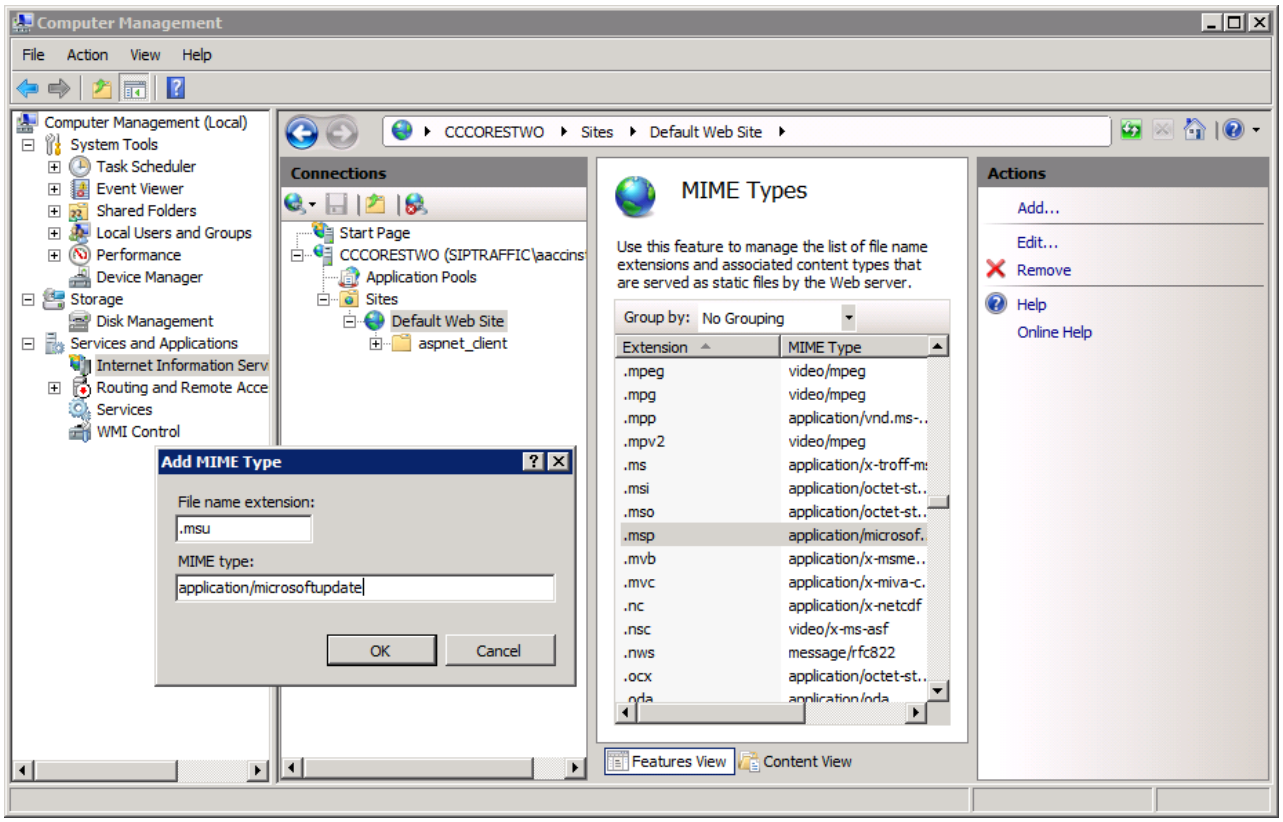


10 Click **OK**.

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**.

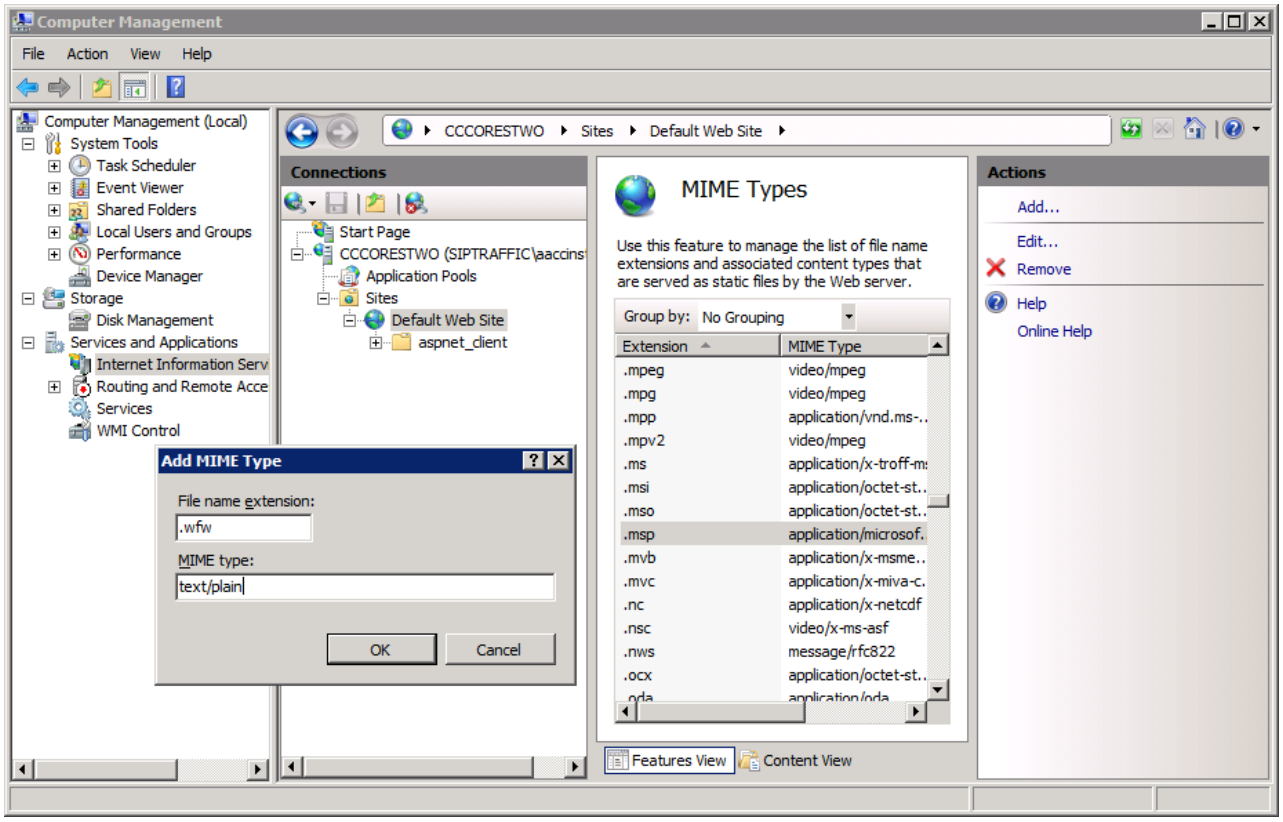


14 Click **OK**.

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.

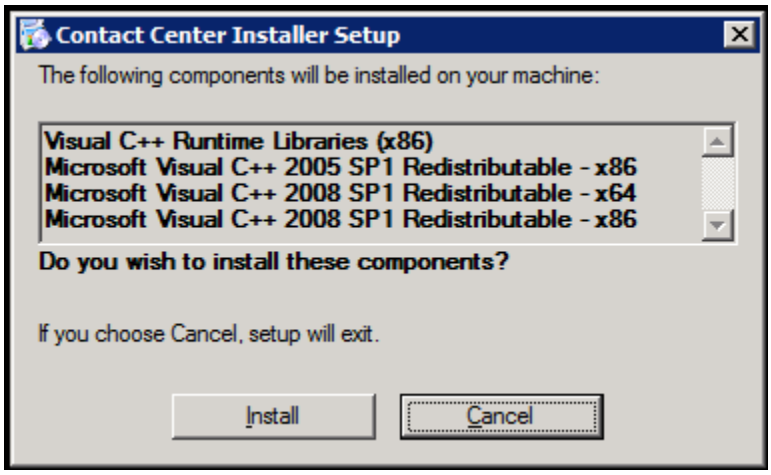
--End--

Installing the Contact Center server software on the Standby server

Install the Contact Center software and enable your contact center to route contacts.

Procedure steps

Step	Action
1	Log on to the Standby server (for example, **CCCORESTWO**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
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.

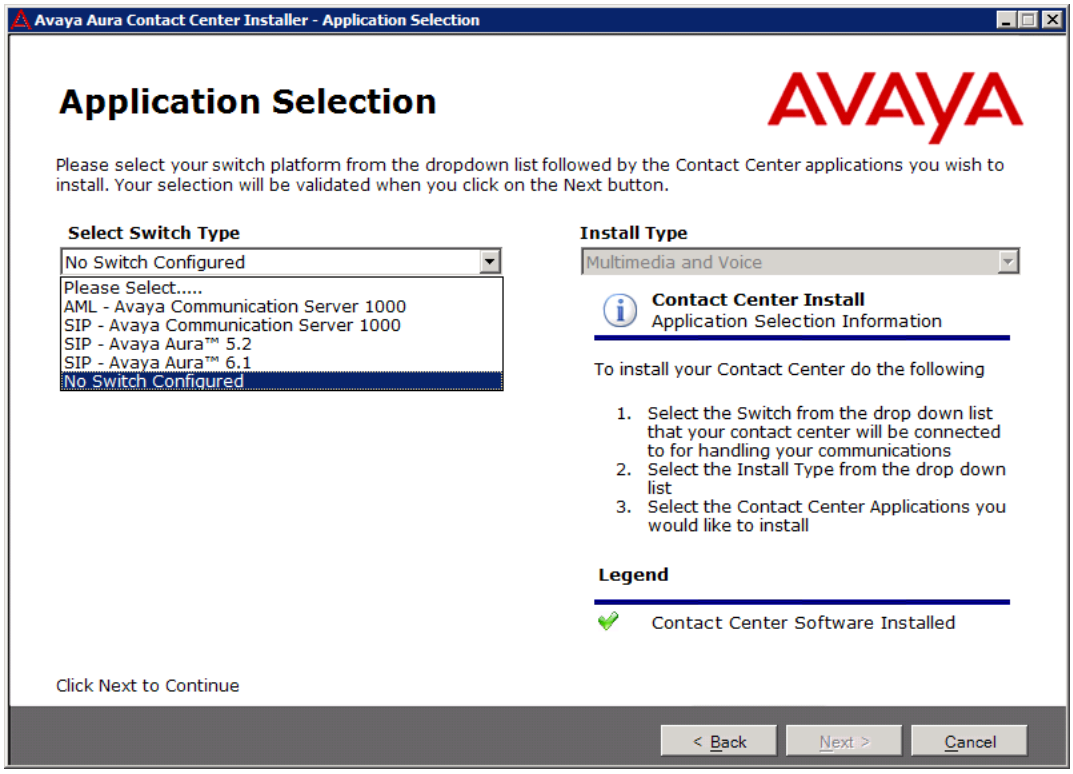
5 On the **Welcome** window, click **Next**.

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 **Application Selection** window, from the **Select Switch Type** list, select **No Switch Configured**.



10 Under **Contact Center Manager Server (CCMS)**, select **Nodal Server**.

In addition to installing Contact Center Manager Server, this selection installs the Open Queue Open Interface, the Open Networking Open Interface, and Multiplicity, which you can license and configure at a later time.

11 Under **Communication Control Toolkit (CCT)**, select **Contact Center Feature Set**.

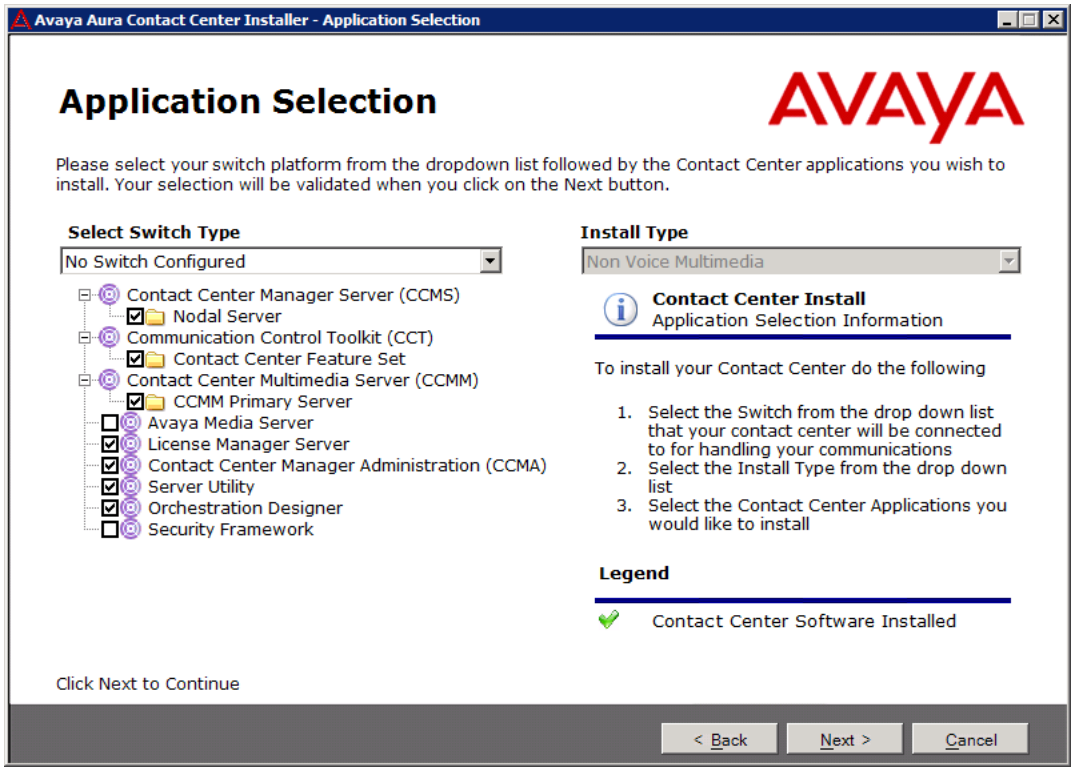
12 Under **Contact Center Multimedia Server (CCMM)**, select **CCMM Primary Server**.

13 Select **License Manager Server**.

14 Select **Contact Center Manager Administration (CCMA)**.

15 Select **Server Utility**.

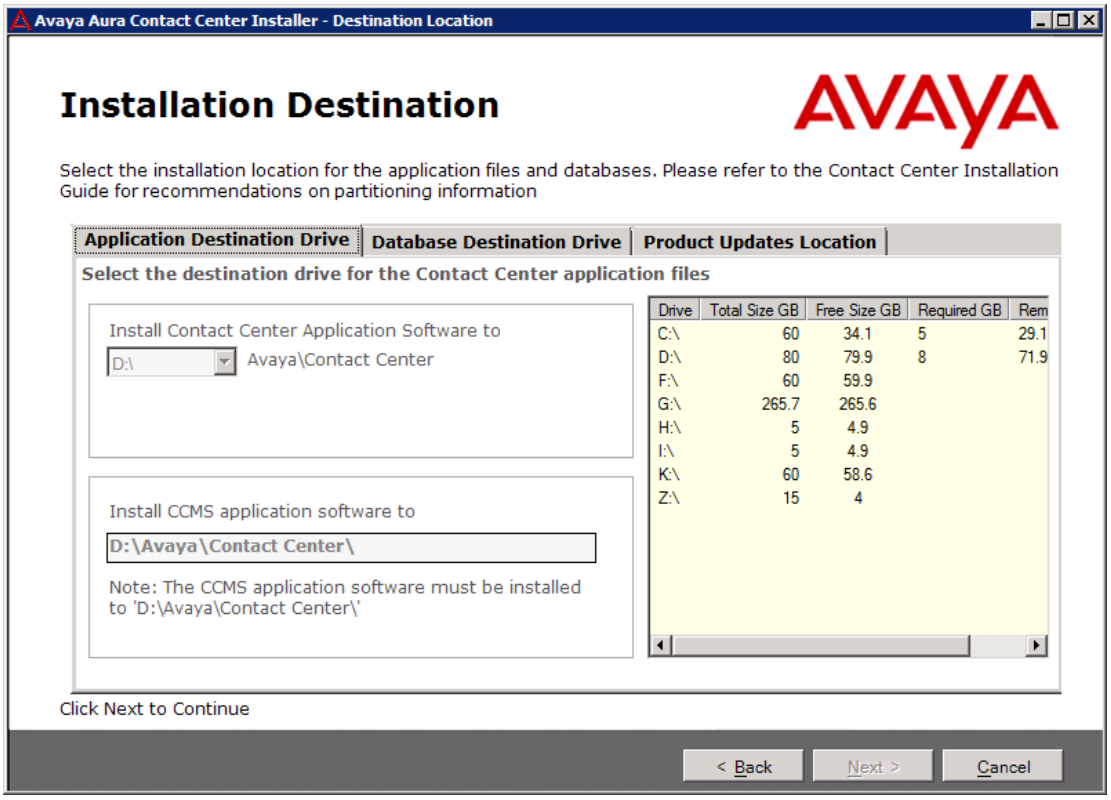
16 Select **Orchestration Designer**.



17 Click **Next**.

18 On the **Product Data Upgrade** window, click **Next**.

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

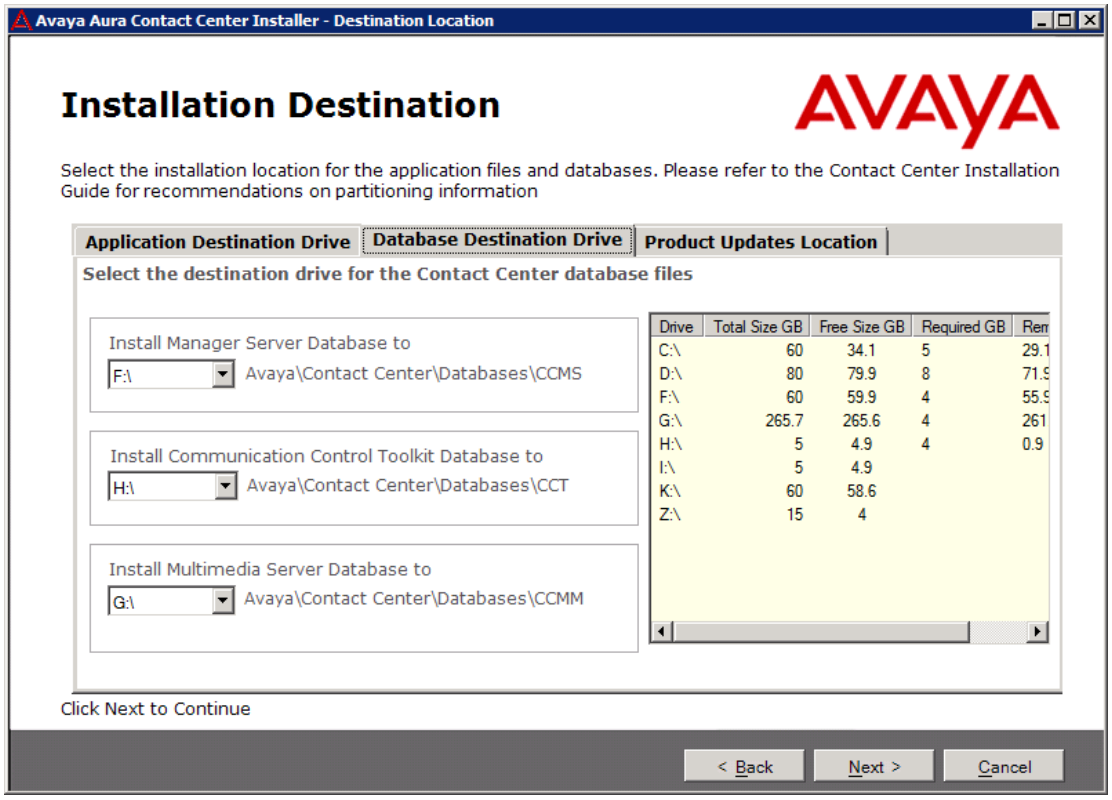


20 Select the **Database Destination Drive** tab.

21 From the **Install Manager Server Database to** list, select **F:**.

22 From the **Install Communication Control Toolkit Database to** list, select **H:**.

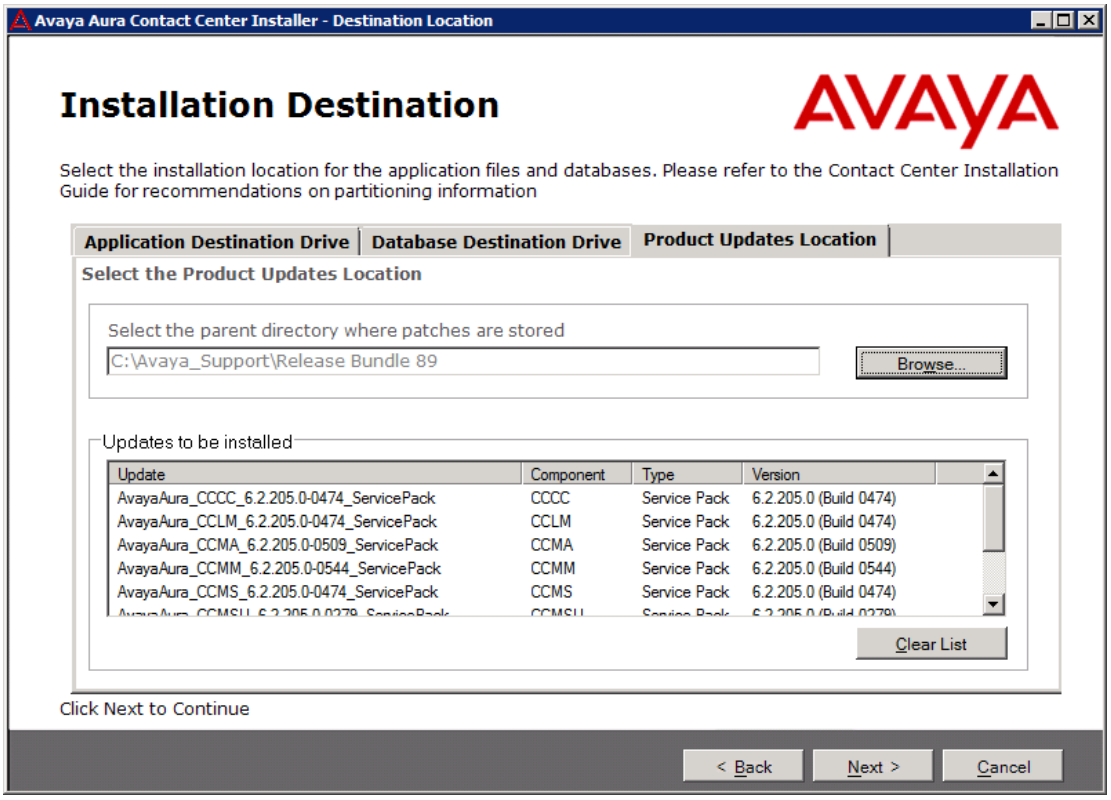
23 From the **Install Multimedia Server Database to** list, select **G:**.



24 Select the **Product Updates Location** tab.

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

26 Select the support directory you created, for example **C:\Avaya_Support**.

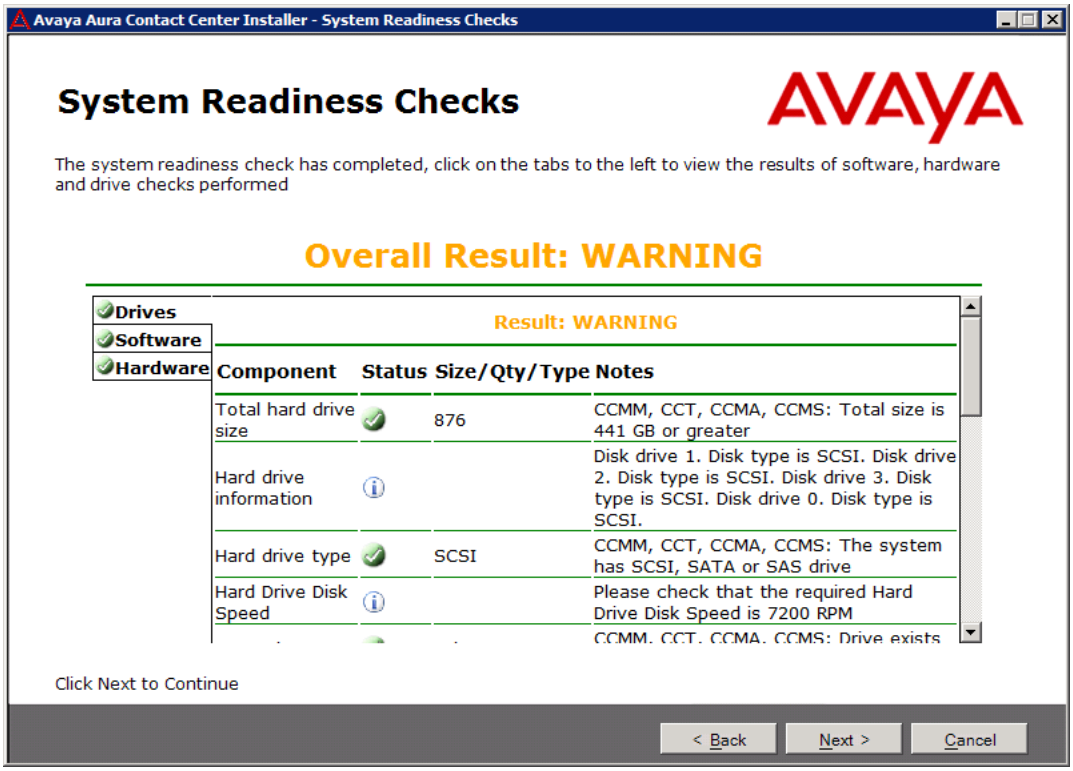


27 Click **Next**.

The System Readiness Check runs on the server.

28 If you have followed the previous instructions in this guide, and the server hardware meets the specifications in the *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210) 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.



29 Click **Next**.

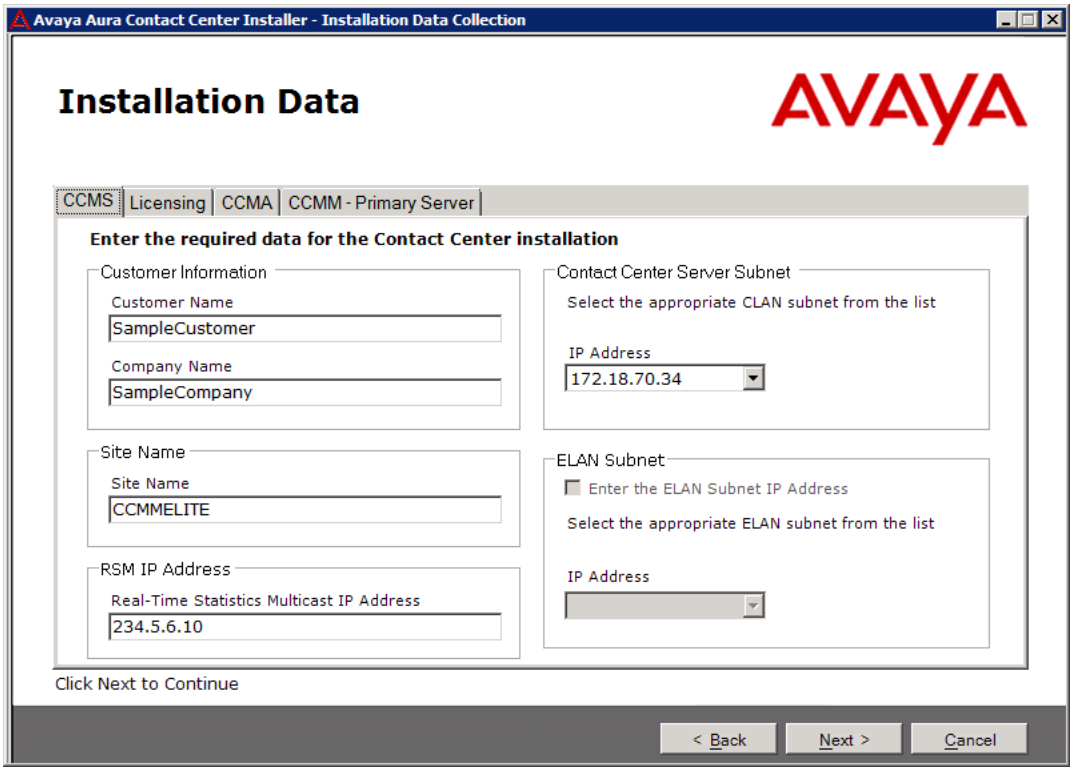
30 On the **Installation Data** window, select the **CCMS** tab. Complete the fields as follows:

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

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

Site Name — Type the name of site, for example **CC_ELITESITE**. The site name of the Standby server must match the site name of the Active server. Do not enter the Active server computer name or the Standby server computer name here.

Contact Center Server Subnet IP Address — Select the Standby server IP address, for example **172.18.70.34**.



31 Select the **Licensing** tab.

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

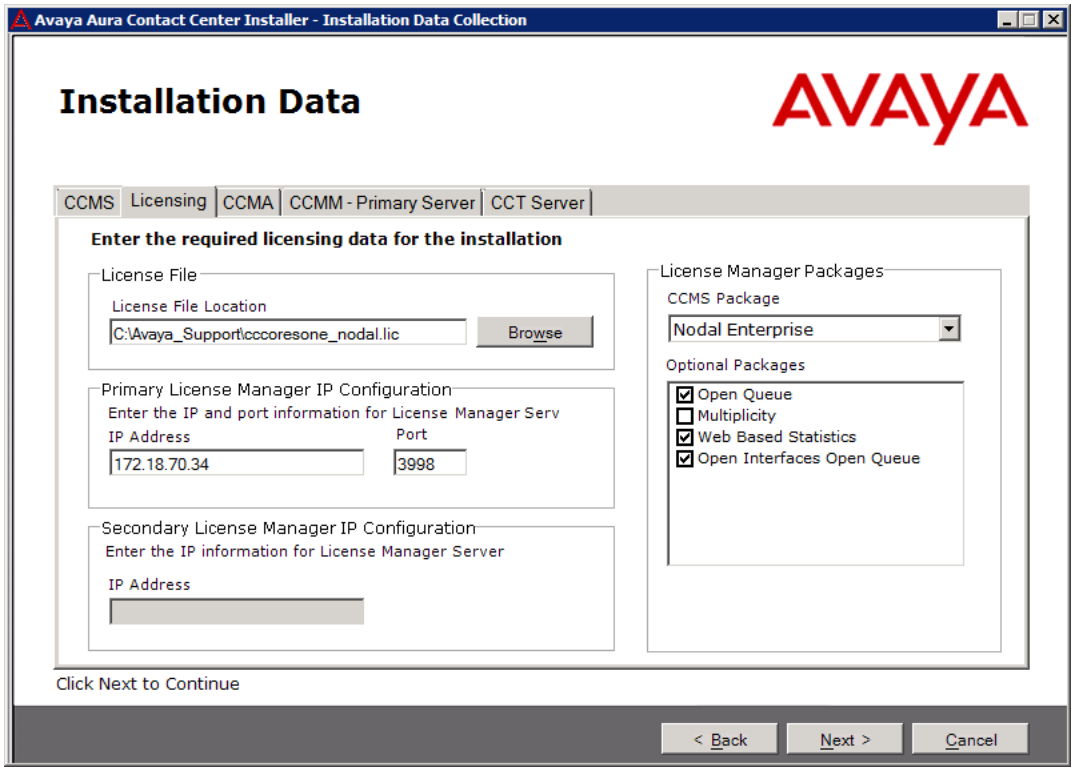
License File Location — Use the **Browse** button to find and select the license file that you downloaded to the Standby server.

IP Address — The IP address of the license server, in this case the co-resident server itself, for example **172.18.70.34**.

Port — Accept the default port, **3998**.

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

Optional Packages — Select **Open Queue**, **Web Based Statistics**, and **Open Interfaces Open Queue**.



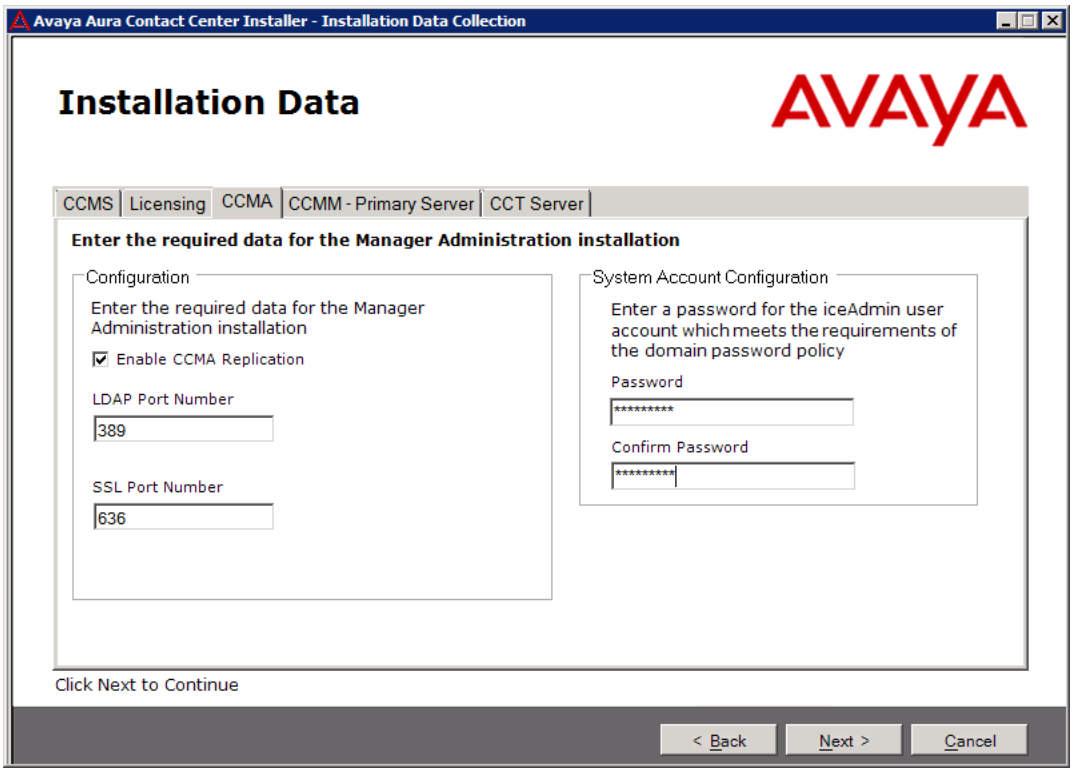
33 Select the **CCMA** tab.

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

System Account Configuration - Password — Type the password for the CCMA System Account (iceAdmin), for example **ICEpassw1**.
Attention! The password must conform to your domain password policy.

System Account Configuration - Confirm Password — Type the password for the CCMA System Account (iceAdmin), for example **ICEpassw1**.

Configuration - Enable CCMA Replication — Select the **Enable CCMA Replication** check box.



35 On the **Contact Center Installer** message box, click **Yes**.

36 Select the **CCMM - Primary Server** tab.

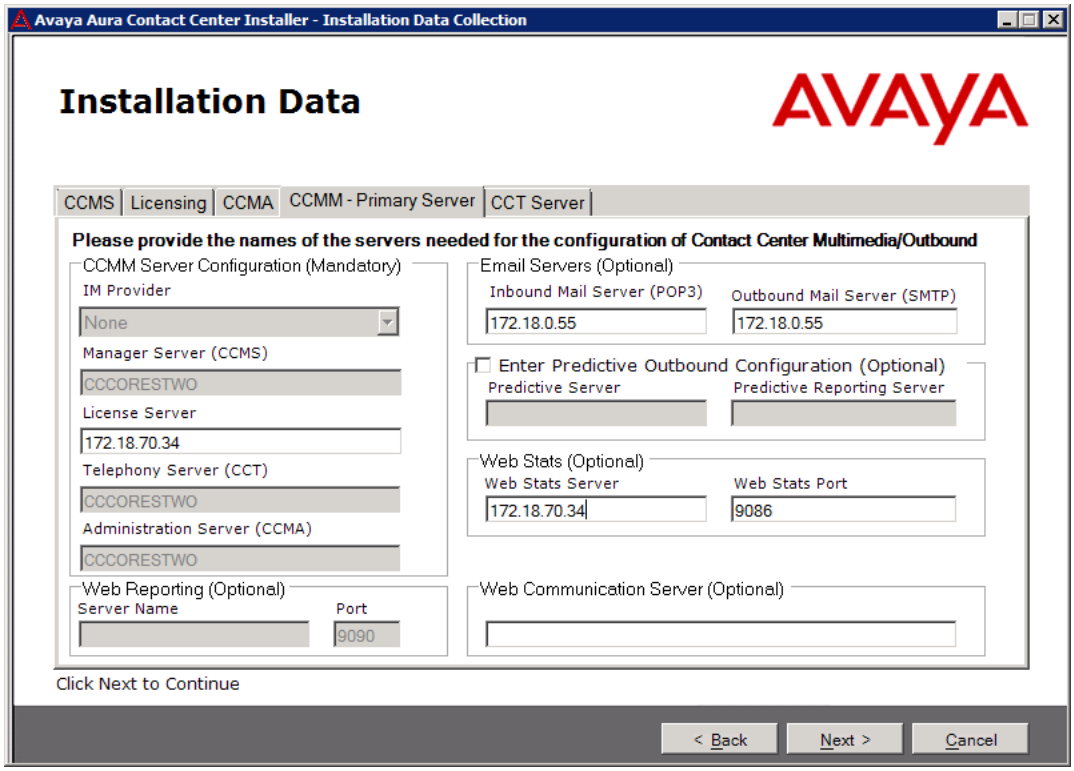
37 Complete the **CCMM - Primary Server** tab fields as follows:

License Server — Type the IP address of the License server, for example **172.18.70.34**.

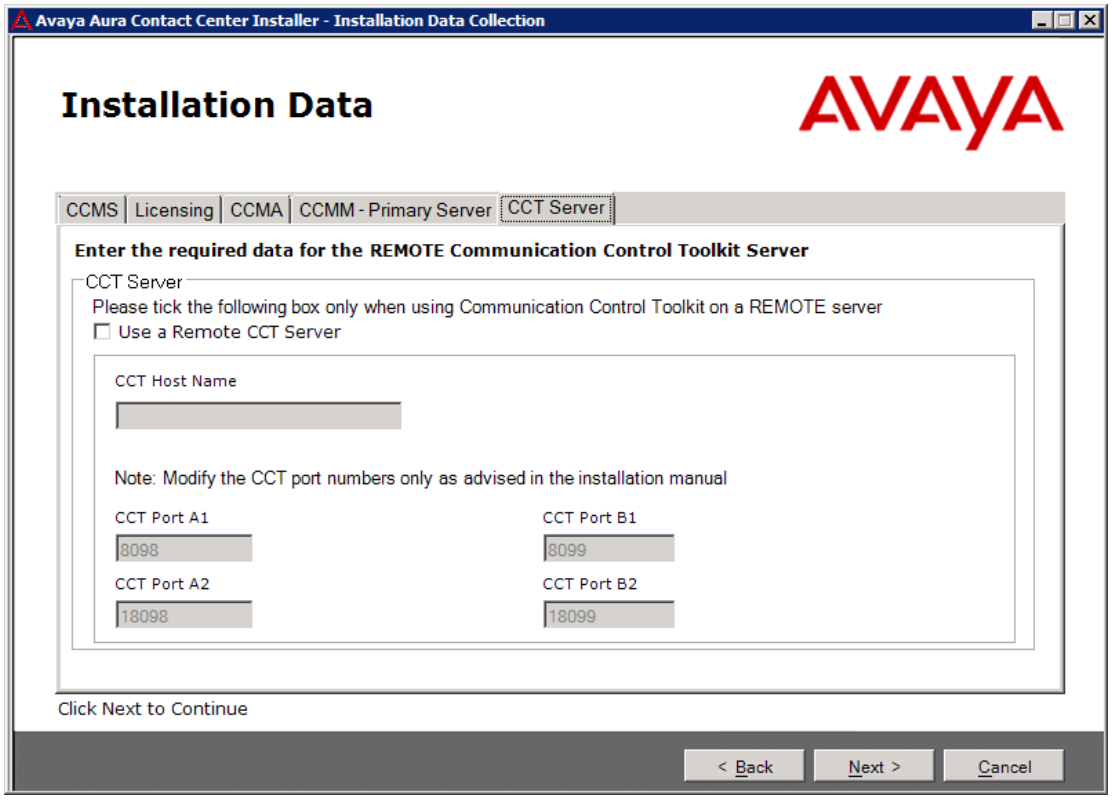
Inbound mail server (POP3) — Type the IP address of the e-mail server, for example **172.18.0.55**.

Outbound mail server (SMTP) — Type the IP address of the e-mail server, for example **172.18.0.55**.

Web Stats Server (Optional) — Type the IP address of the web statistics server, for example **172.18.70.34**.

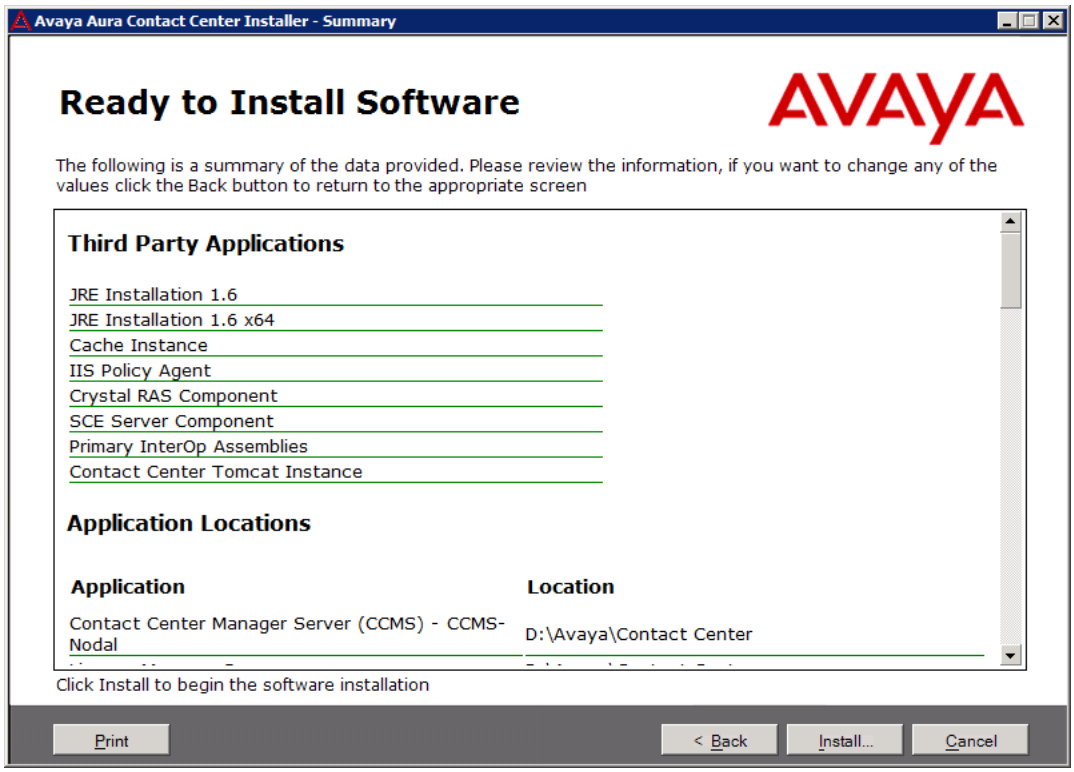


38 On the **Installation Data** window, in the **CCT Server** tab, you do not complete any configuration:



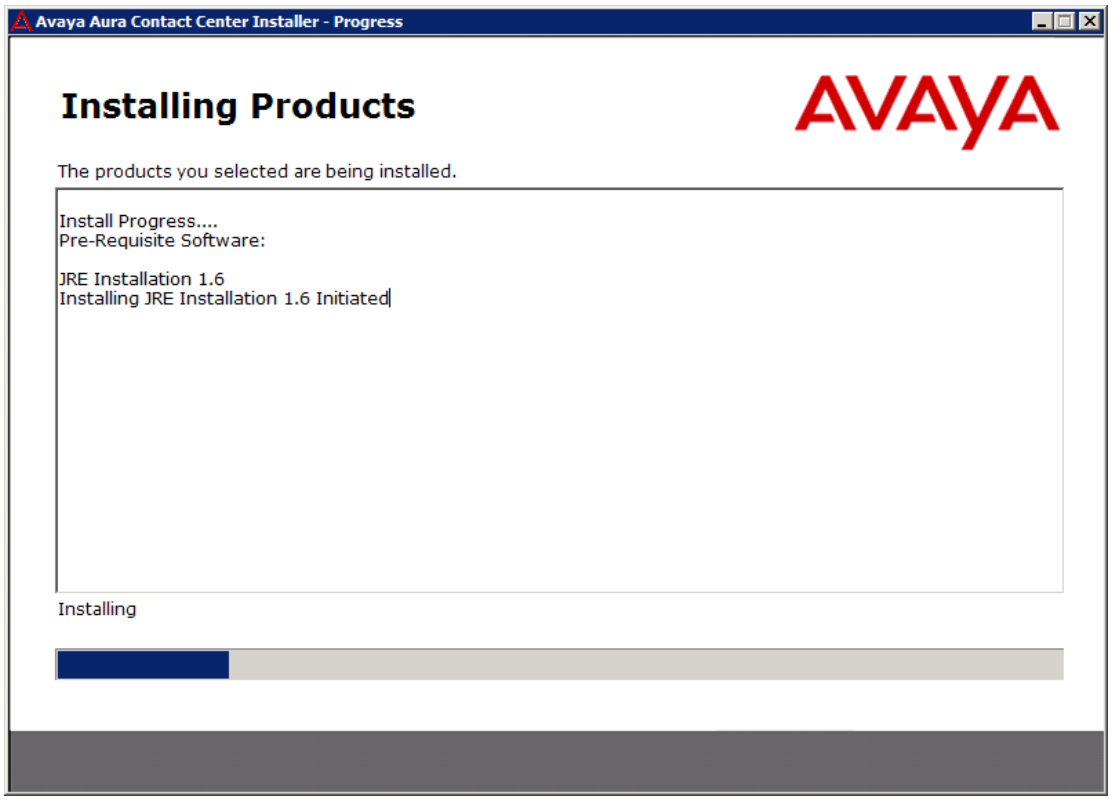
39 Click **Next**.

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



41 Click **Install**.

The system displays the Installing Products window, which updates you on the progress of the install.

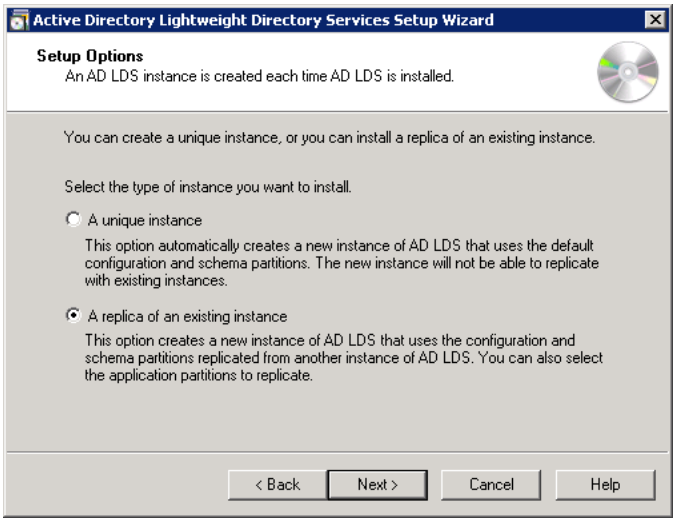


The install continues for some time until the AD-LDS setup wizard appears.

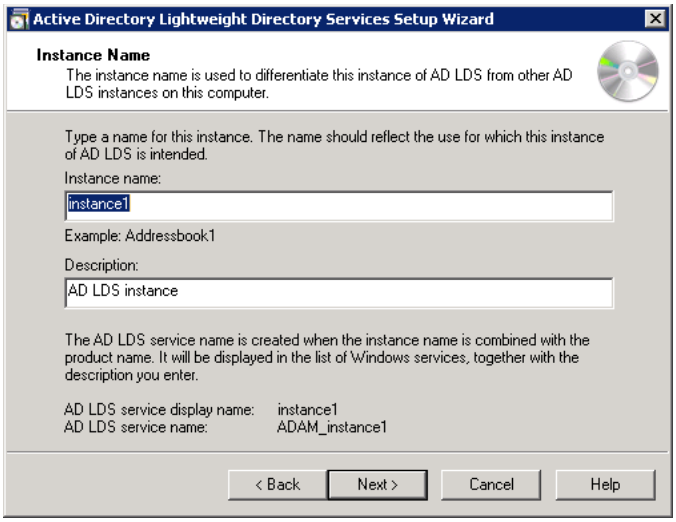


42 Click **Next**.

43 In the **Setup Options** dialog box, select **A replica of an existing instance**.



44 Click **Next**.



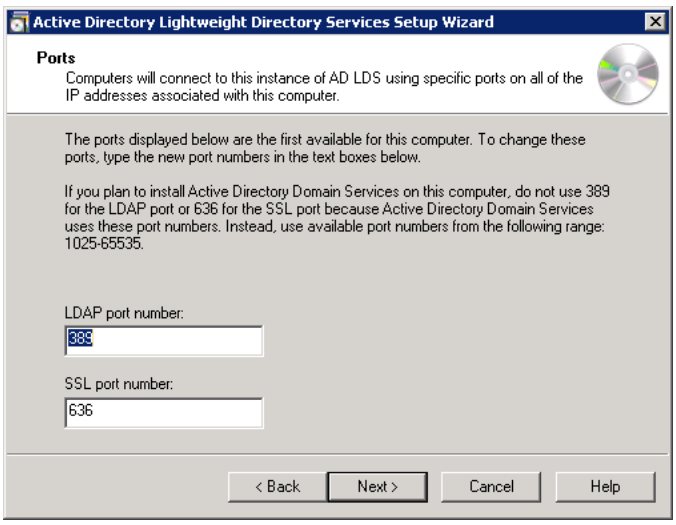
45 On the **Instance Name** dialog box, in the **Instance name** box, type the AD-LDS instance name, **SymposiumWC**.



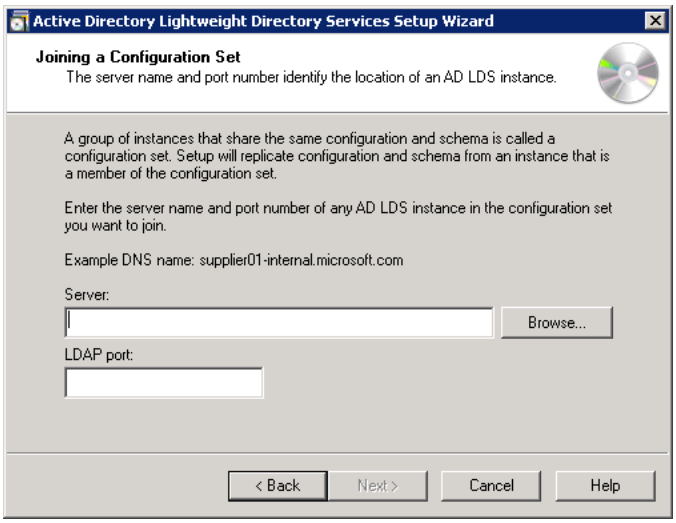
46 In the **Description** box, type **SymposiumWC**.

47 Click **Next**.

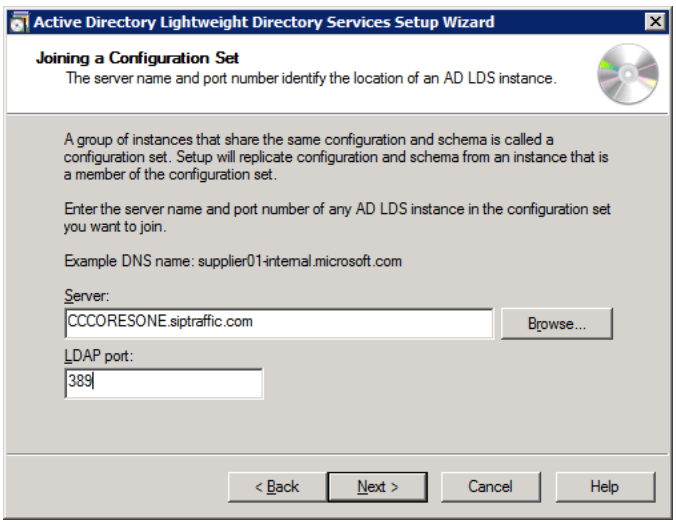
48 On the **Ports** dialog box, accept the default values in the LDAP port number and SSL port number boxes.



49 Click **Next**.

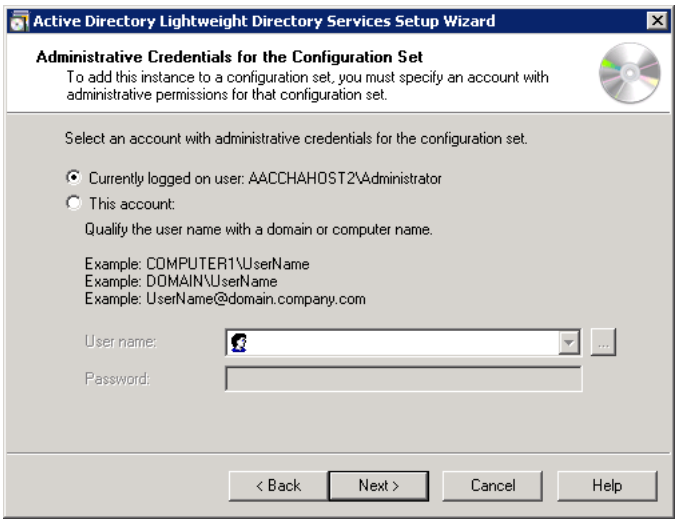


50 On the **Joining a Configuration Set** dialog box, in the **Server** box, type the FQDN name of the primary Contact Center Manager Administration server to replicate. For example type **CCCORESONE.siptraffic.com**.



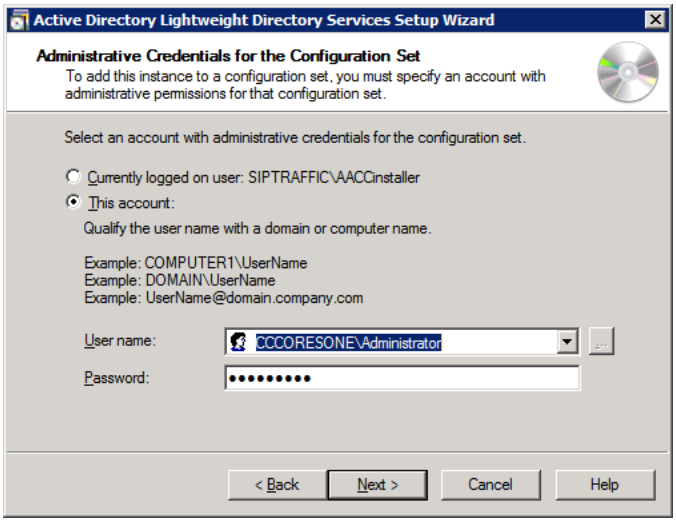
51 On the **Joining a Configuration Set** window, in the **LDAP Port** box, type the port number on the AD-LDS instance on the primary CCMA. The default is port number **389**.

52 Click **Next**.



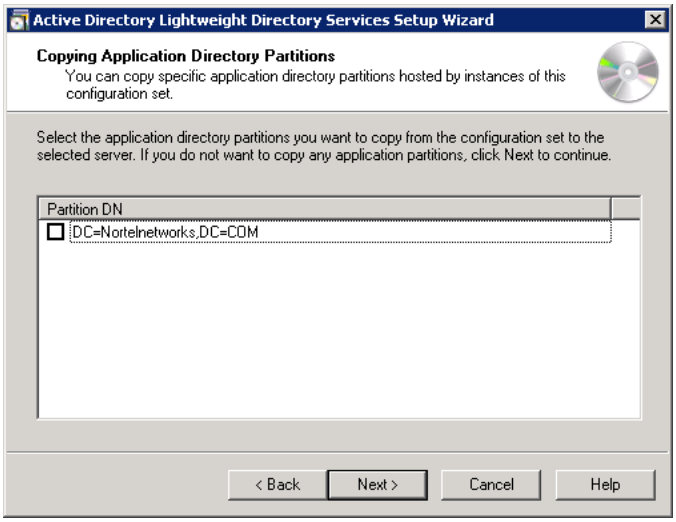
53 On the **Administrative Credentials for the Configuration Set** window, select **This account**.

54 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 **CCCORESONE\Administrator**.

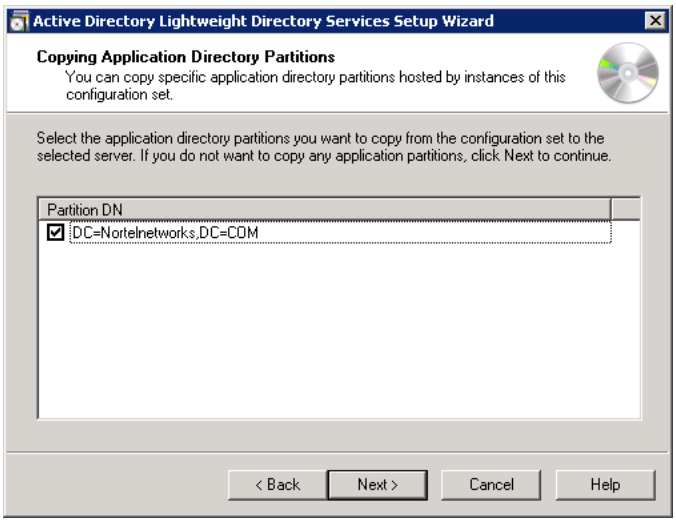


55 In the **Password** box, type the password for this user account, for example **MultiMpassw1**.

56 Click **Next**.

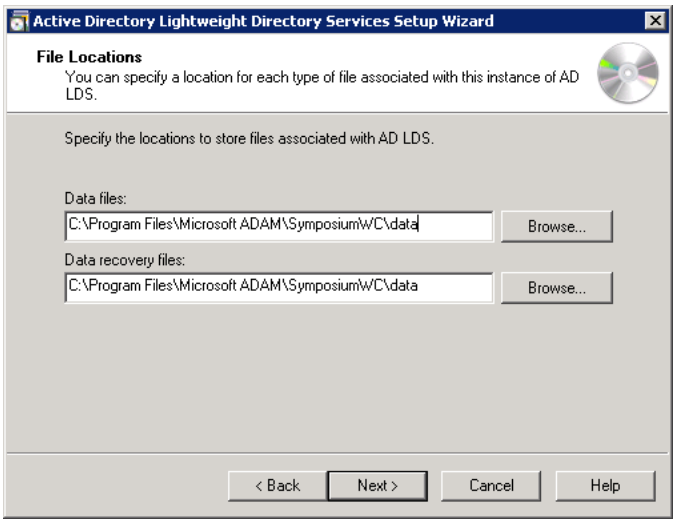


57 In the **Copying Application Directory Partitions** dialog box, in the Partition DN list, select the partition **DC=Nortelnetworks,DC=COM**.



58 Select **Next**.

59 In the **File Location** dialog box, accept the default values.

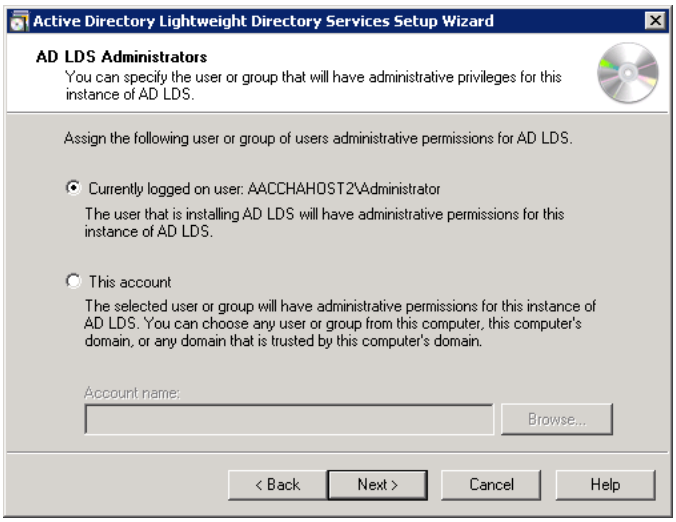


60 Click **Next**.



61 In the **Service Account Selection** dialog box, select **Network service account**.

62 Click **Next**.

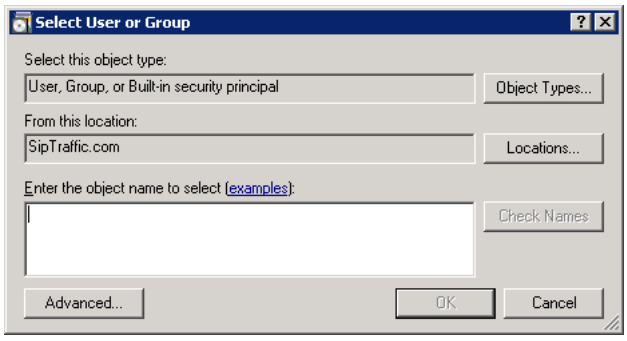


63 In the **AD LDS Administrators** dialog box, select **This account**.



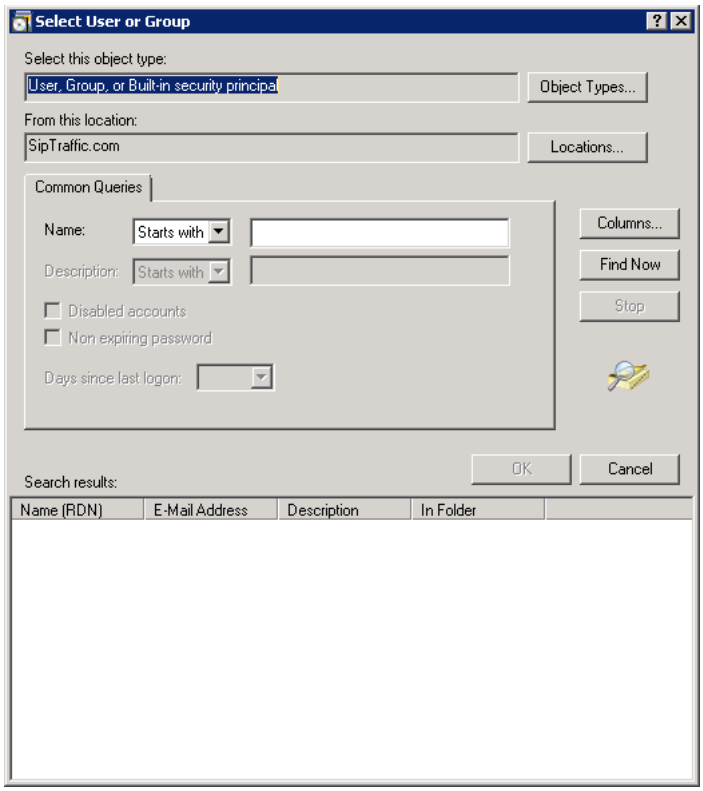
64 Select **Browse** to locate the CCMA AD-LDS replication account.

The Select User or Group dialog box appears. Note that the location is the local domain.

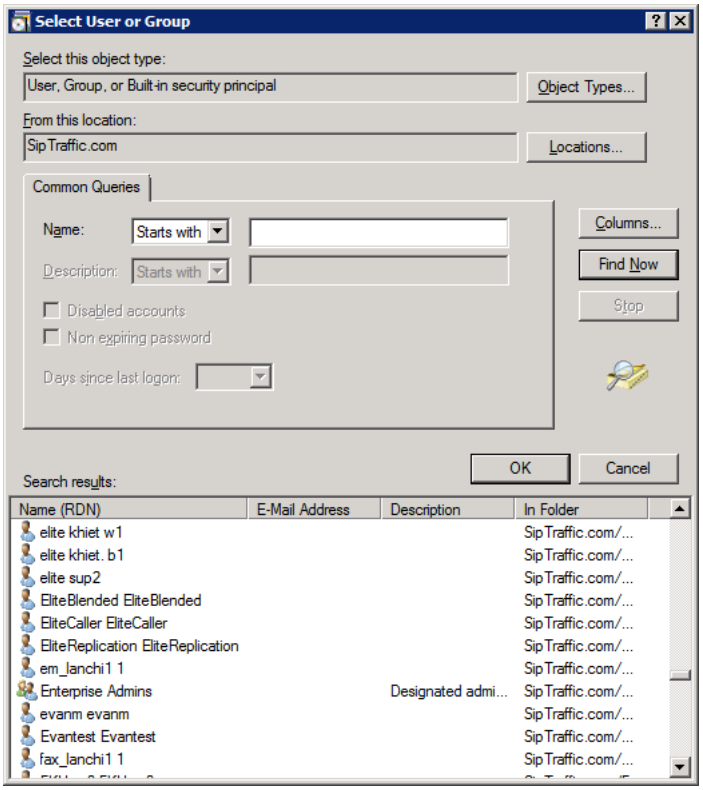


65 In the **Select User or Group** dialog box, click **Advanced**.

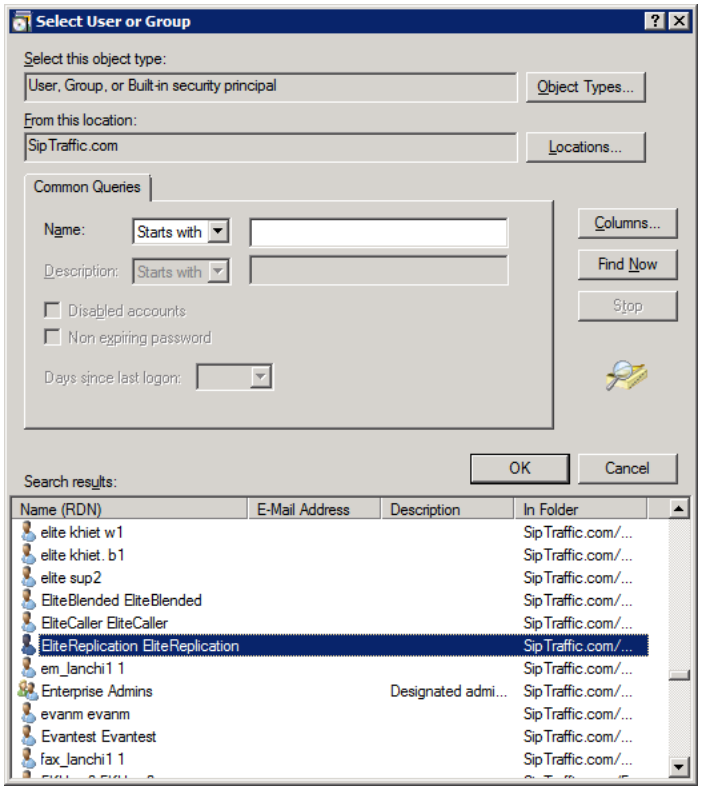
The advanced Select User or Group dialog box appears.



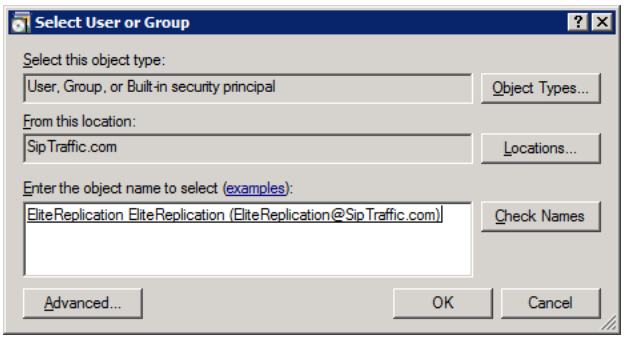
66 In the advanced **Select User or Group** dialog box, click **Find Now**.



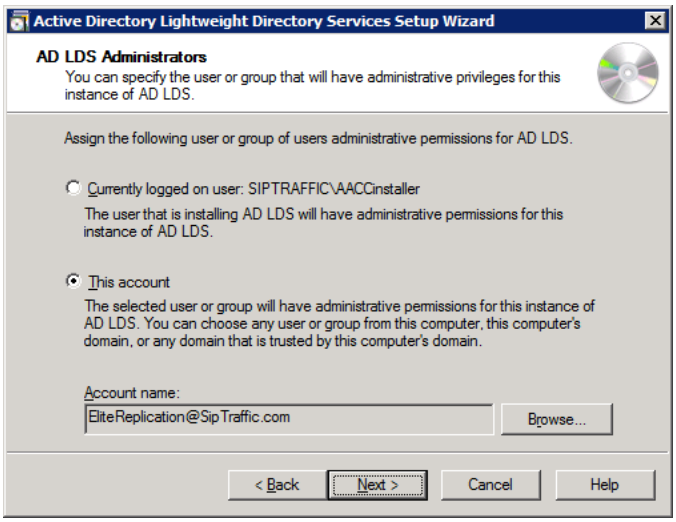
67 From the **Search results** list, select the CCMA replication account, for example **EliteReplication**.



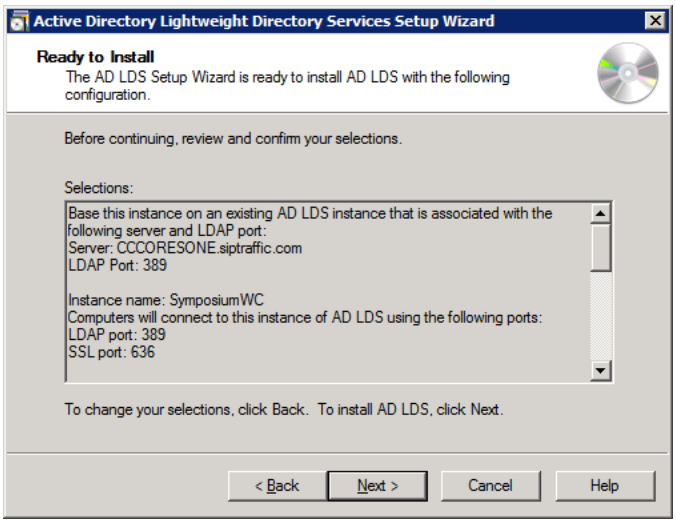
68 In the advanced **Select User or Group** dialog box, click **OK**.



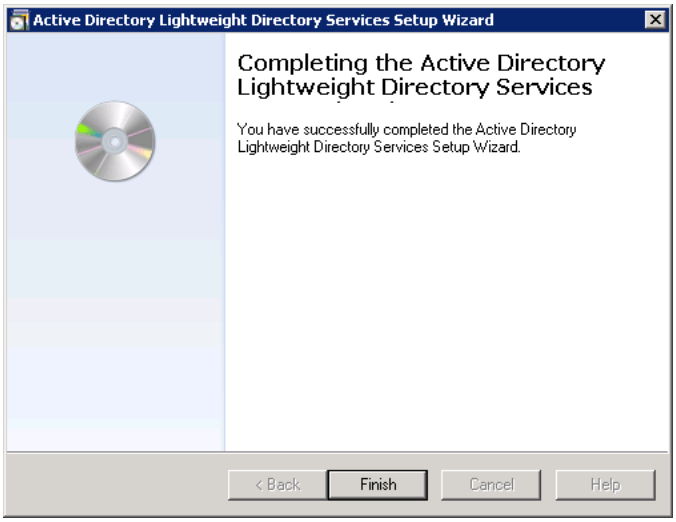
69 In the **Select User or Group** dialog box, click **OK**.



70 Click **Next**.



71 Confirm the installation components, and click **Next**.



72 Click **Finish**.

The Avaya Aura® Contact Center standby server installation continues.

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

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

75 After the server restarts, disable Java Runtime Environment (JRE) updates. See Disabling Java Runtime Environment updates on the co-resident server (page 420).

Attention: Updating to an unsupported version of JRE can cause the contact center to cease operation and may require the reinstallation of the contact center server.

--End--

Disabling Java Runtime Environment updates on the co-resident server

Contact Center supports only specific versions of Java Runtime Environment (JRE). The Contact Center installer installs a supported JRE version, and Contact Center service packs install any required JRE updates. It is important that you disable JRE automatic updating in the Windows Control Panel on all contact center servers.

Attention: Updating to an unsupported version of JRE can cause the contact center to cease operation and may require the complete reinstallation of the contact center server.

Procedure steps

Step	Action

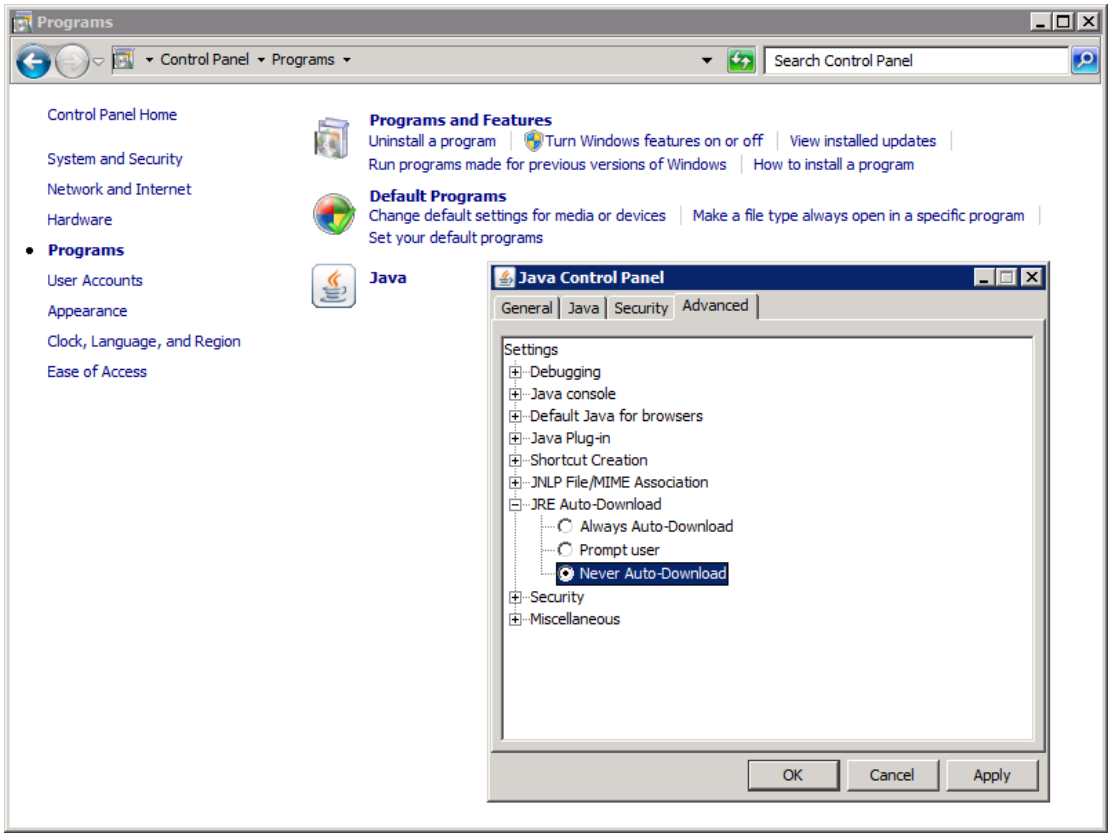
1 Log on to the Standby server (for example, **CCCORESTWO**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.

2 Choose **Start**, **Control Panel**, **Programs**, **Java**.

3 On the **Java Control Panel**, select the **Advanced** tab.

4 Expand **JRE Auto-Download**.

5 Select **Never Auto-Download**.



6 Click **OK**.

--End--

Standby Server Post-install Commissioning

This chapter contains the procedures you must perform on the Standby Contact Center after installing the Contact Center applications.

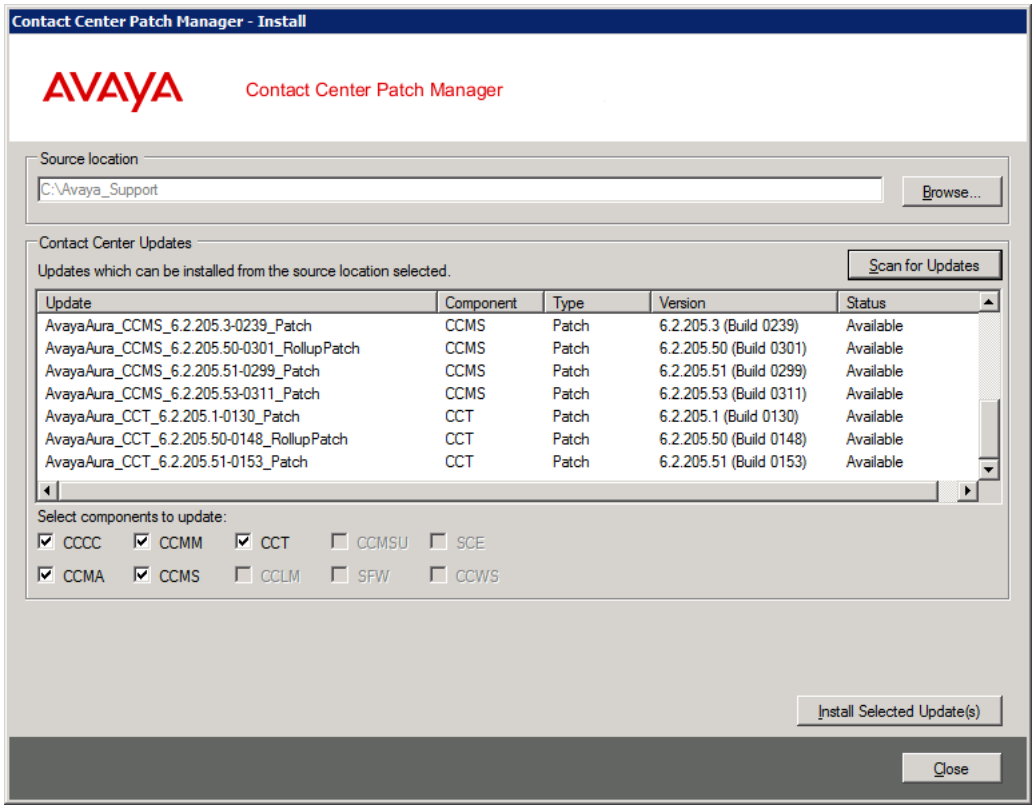
Applying Post-installation Patches

This is a general procedure for applying Contact Center patches after the initial installation. The Contact Center installer allows application only of service packs as part of the install.

Attention: You must carefully review the README files for each patch you download. The precise steps for installation vary from patch to patch. For example, most patches require you to shut down Contact Center before application, but some do not. There can also be dependencies on the order of installation of patches.

Procedure steps

Step	Action
1	Browse www.avaya.com/support to find the latest patches for Contact Center.
2	Download the patches to the Contact Center server support folder, for example **C:\ Avaya_Support**.
3	Carefully review the patch README file(s) to determine installation pre-conditions and the order (if any) in which to apply them.
4	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Common Utilities**, **System Control and Monitor Utility**.
5	If required for the patches you are installing, click **Shut down Contact Center**.
6	Exit the **System Control and Monitor Utility**.
7	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Common Utilities**, **Contact Center Patch Manager**.
8	Select **Actions, Install**.
9	Click **Browse** and browse to the **C:\Avaya_Support**.
10	Click **Scan for Updates**. *The system scans the Avaya_Support folder and subfolders for patches, and displays available patches in the **Contact Center Updates** box.*



11 Verify that the list contains only the patches you intend to install.

12 Click **Install Selected Update(s)**.

13 On the **Contact Center Patch Manager - Install** message box, click **Yes**.

14 When the patch installs complete, click **Close**.

--End--

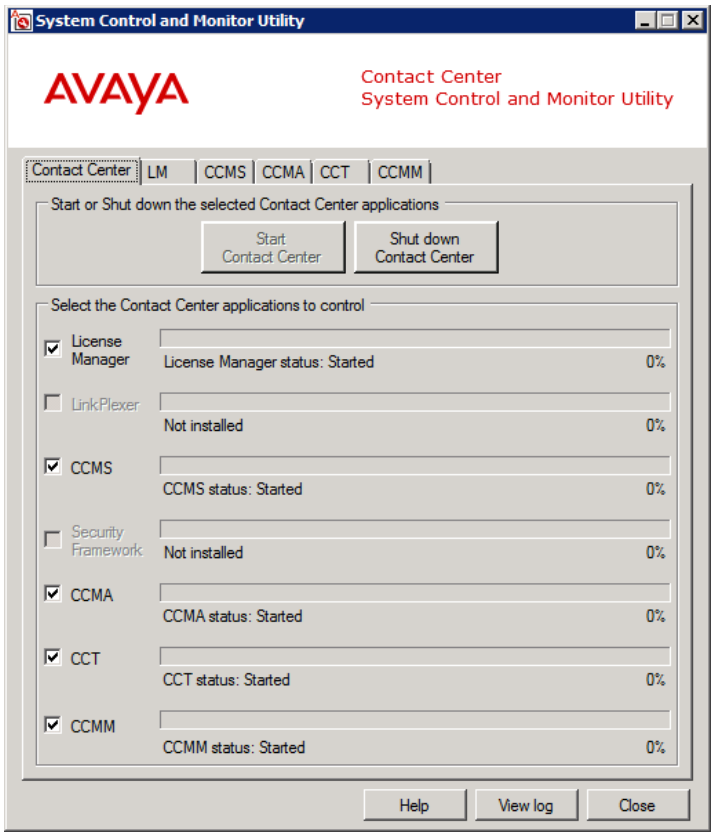
Confirming that the Contact Center services start

Confirm that all appropriate Contact Center Manager Server services start on the Contact Center Manager Server.

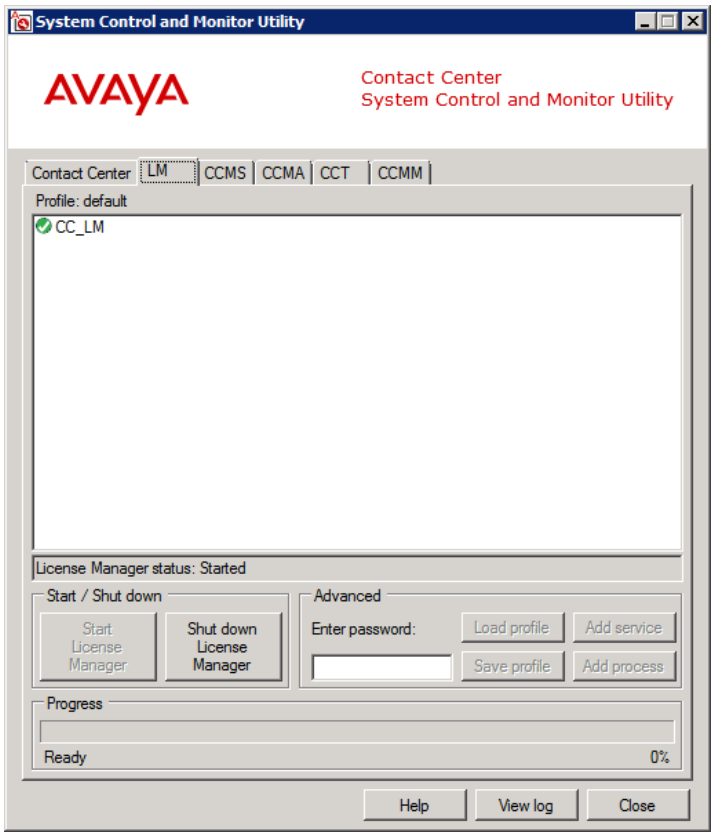
Use the System Control and Monitor Utility to start and stop all applications in Contact Center including the license manager. The System Control and Monitor Utility can also start, stop, or monitor the services in Contact Center Manager Server.

Procedure steps

Step	Action
1	Log on to the Standby server (for example, **CCCORESTWO**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Common Utilities**, **System Control and Monitor Utility**.
3	Click the **Contact Center** tab.
4	Check that the following applications show a status of **Started**: License Manager CCMS CCMA CCT CCMM

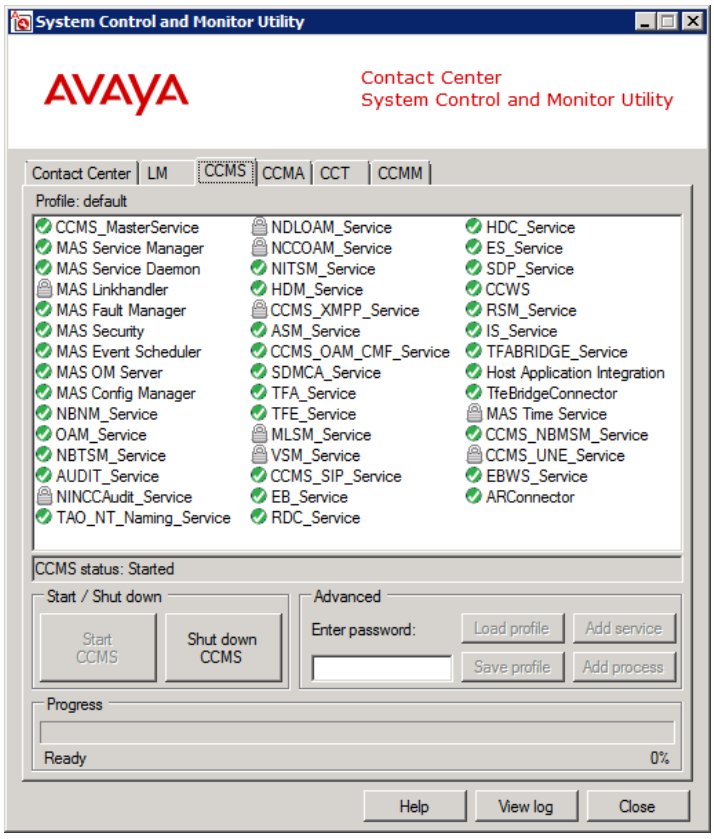


5	Click the **LM** tab.
6	Ensure that the **CC_LM** service in the **Profile** box has a green circle next to it.



7 Click the **CCMS** tab.

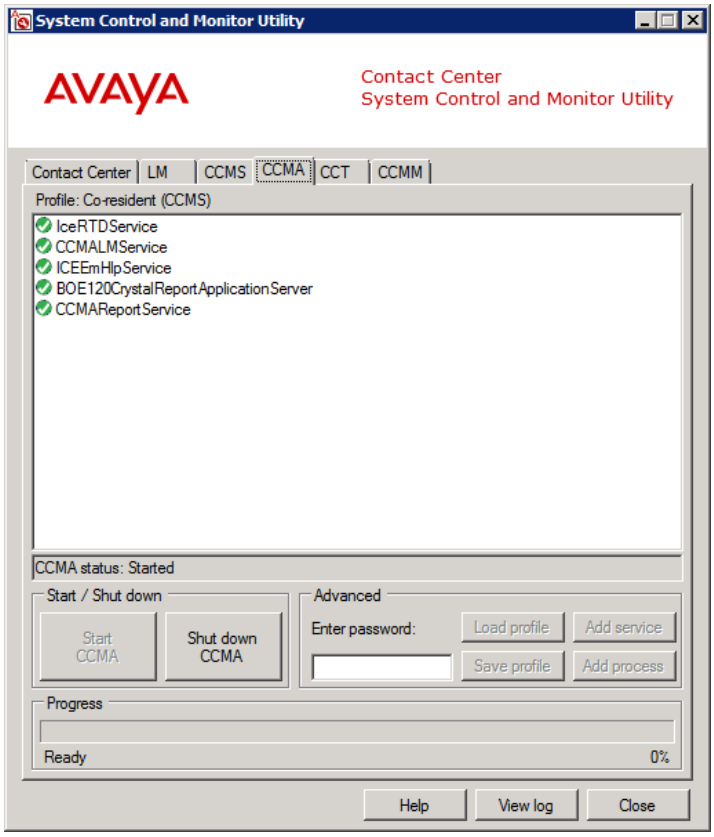
8 Ensure that all licensed services in the **Profile** box have a green circle next to them. (Unlicensed services show a lock icon; these do not require any action.)



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

10 Select the **CCMA** tab.

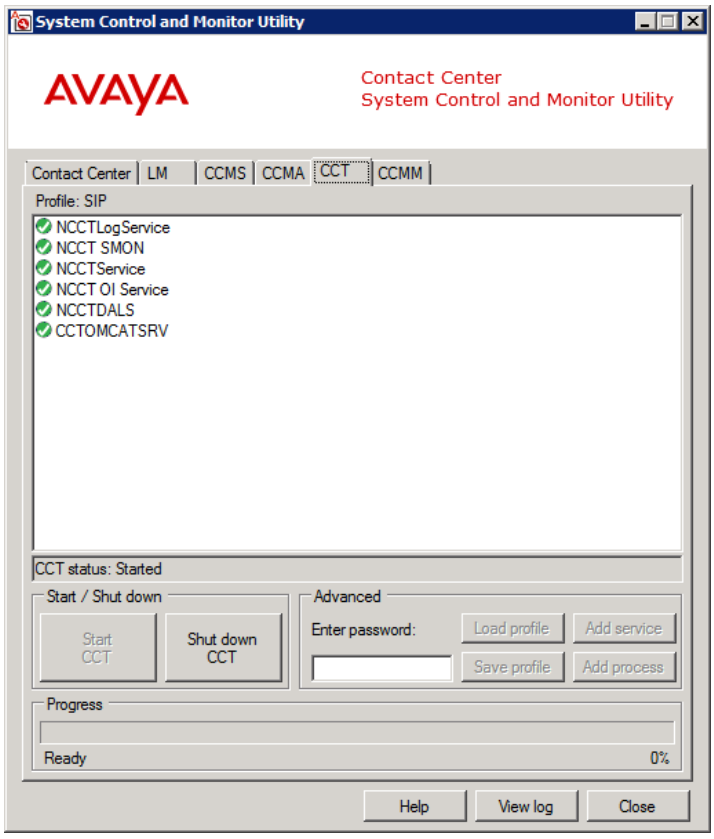
11 Ensure that all licensed services in the **Profile** box have a green circle next to them.



12 If some of the services are not started, click **Start CCMA**.

13 Select the **CCT** tab.

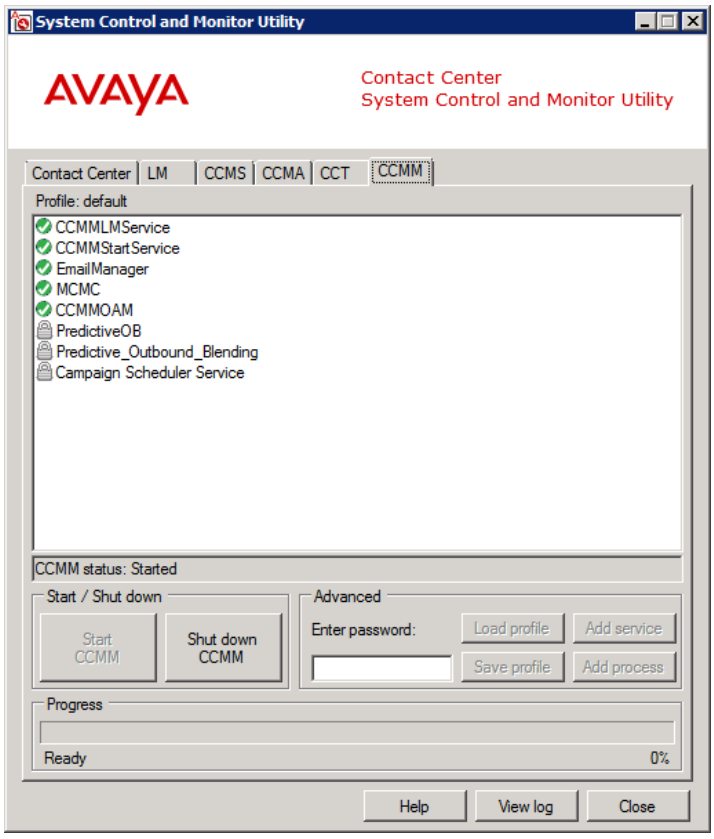
14 Ensure that all licensed services in the **Profile** box have a green circle next to them.



15 If some of the services are not started, click **Start CCT**.

16 Select the **CCMM** tab.

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



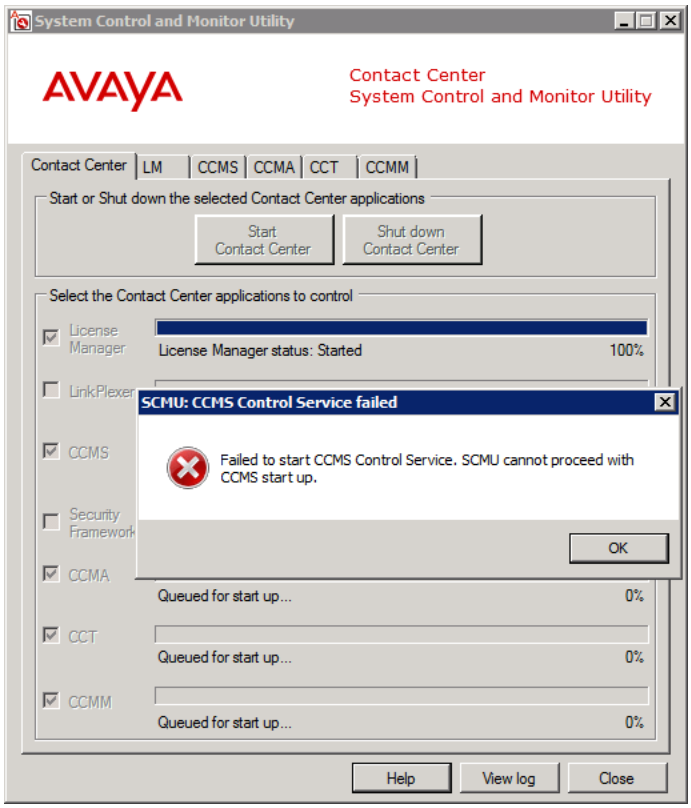
18 If some of the services are not started, click **Start CCMM**.

19 Click **Close**.

--End--

Troubleshooting if the LM and CCMS services do not start on the Standby server

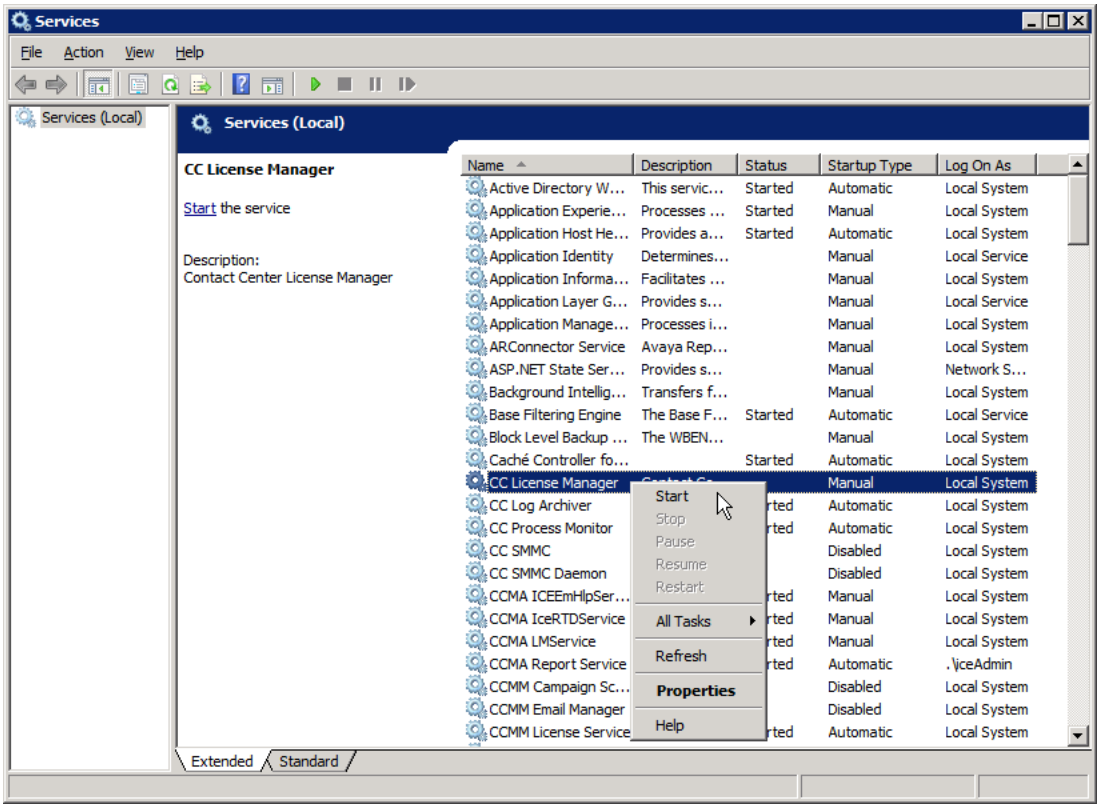
In some situations, the LM and CCMS services do not start the first time after the Standby server install. When you access the System Control and Monitor Utility, the Contact Center and LM tabs show all services as stopped. If you try stopping and restarting the contact center, you see an error message similar to the following example:



If this occurs, start the License Manager server manually and let it run for at least 60 second: then start Contact Center using the System Control and Monitor Utility.

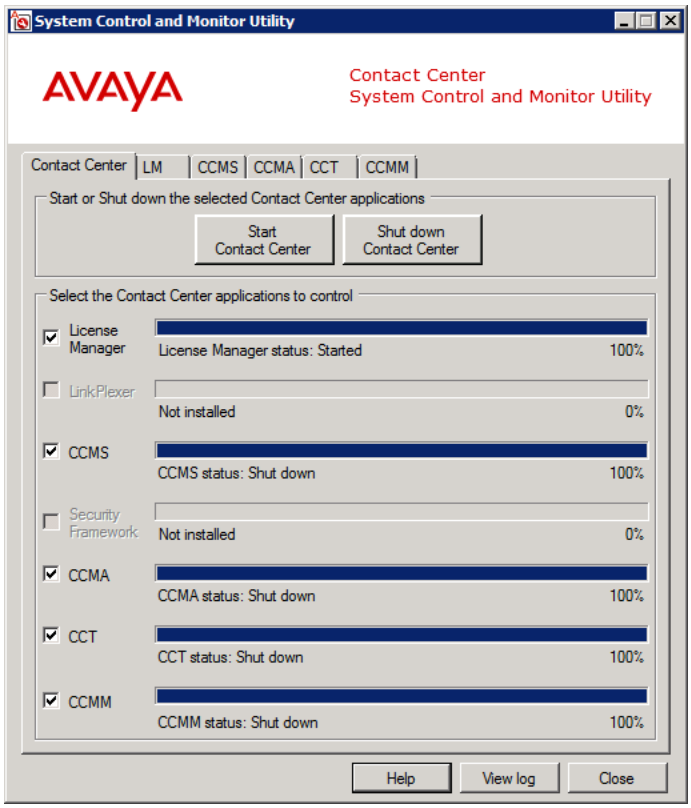
Procedure steps

Step	Action
1	Ensure you are logged on to the Standby server using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Common Utilities**, **System Control and Monitor Utility**.
3	Click the **Contact Center** tab.
4	Click **Shut down Contact Center**, and wait until all the components have stopped.
5	Select **Start**, **Administrative Tools**, **Services**.
6	In the **Services (local)** pane, scroll down to find the **CC License Manager** service.



7 Right-click the **CC License Manager** service, and select **Start**.

8 When the **CC License Manager** starts, wait 60 seconds and then open the System Control and Monitor Utility.



9 Click **Start Contact Center**.

The remaining Contact Center components start.

10 Click **Close**.

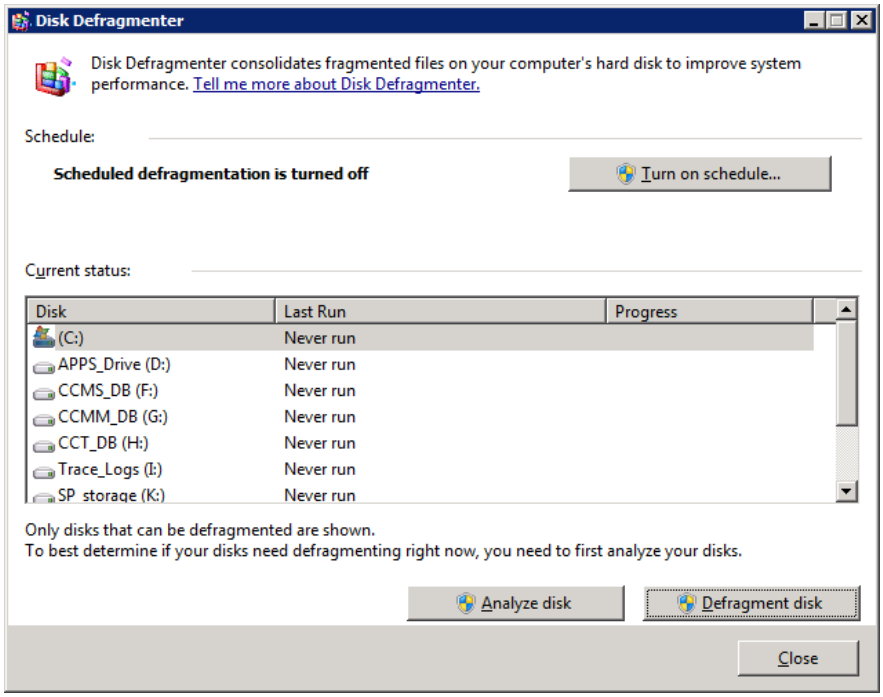
--End--

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)**.

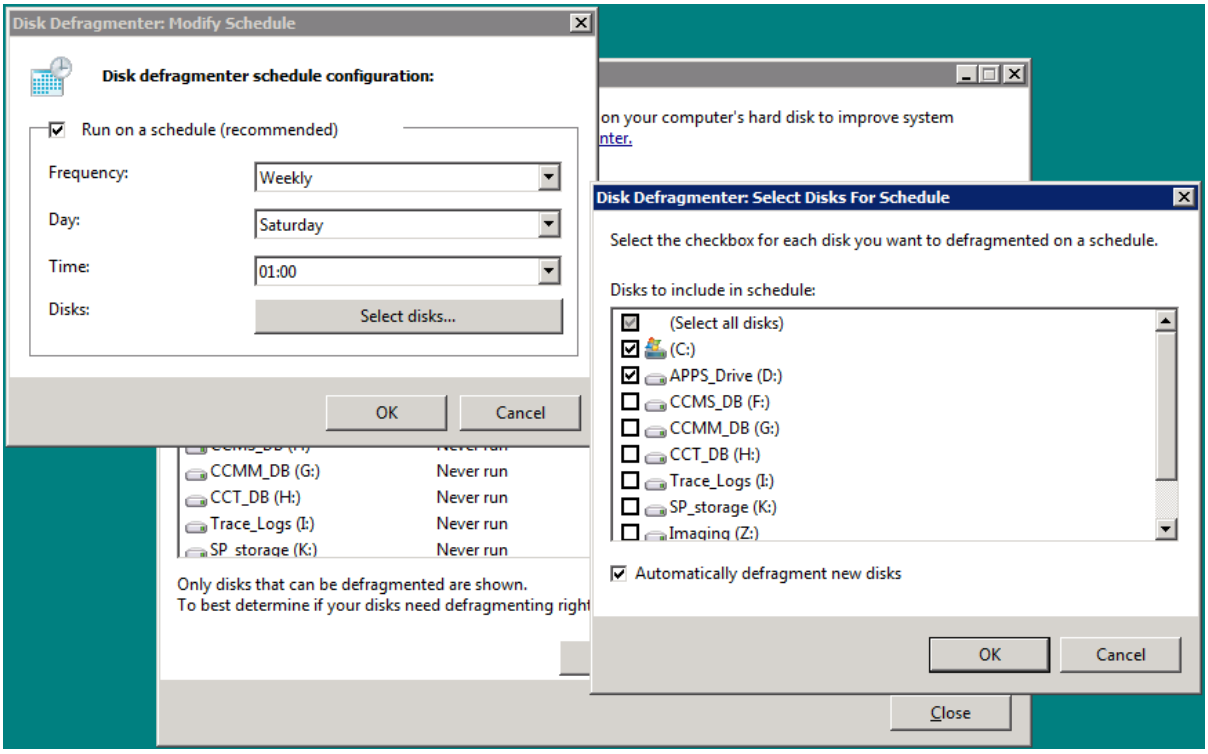
7 Under **Frequency**, select **Weekly**.

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**.

--End--

Configuring the Multicast controller

Configure the Multicast controller to use the IP Multicast delivery method to send Real Time Reporting data. Multicast is a network addressing method for delivering information to a group of destinations in a one-to-many distribution.

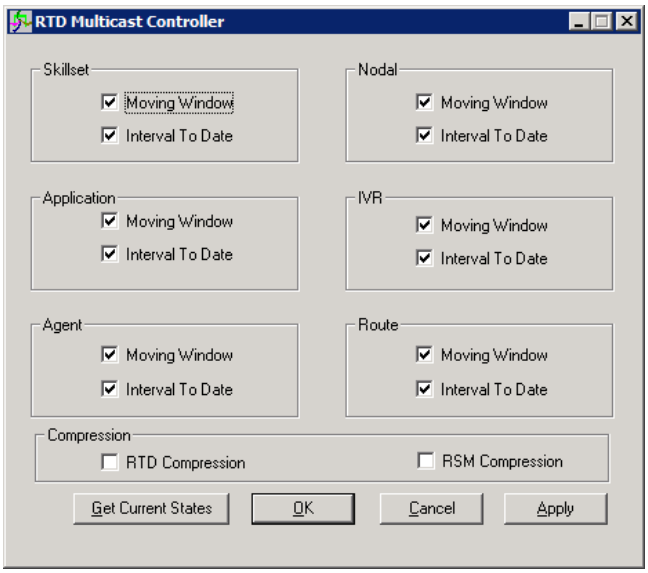
Attention: The Multicast controller settings on the Standby server must exactly match the Multicast controller settings on the Active server.

If you plan to use the unicast delivery method, you do not need to configure CCMS, and you can skip this procedure. For Unicast delivery, only one user can log on at a time and you must ensure that you disconnect all terminal services sessions.

For more information about multicast and unicast, see *Avaya Aura® Contact Center Fundamentals* (NN44400-110).

Procedure steps

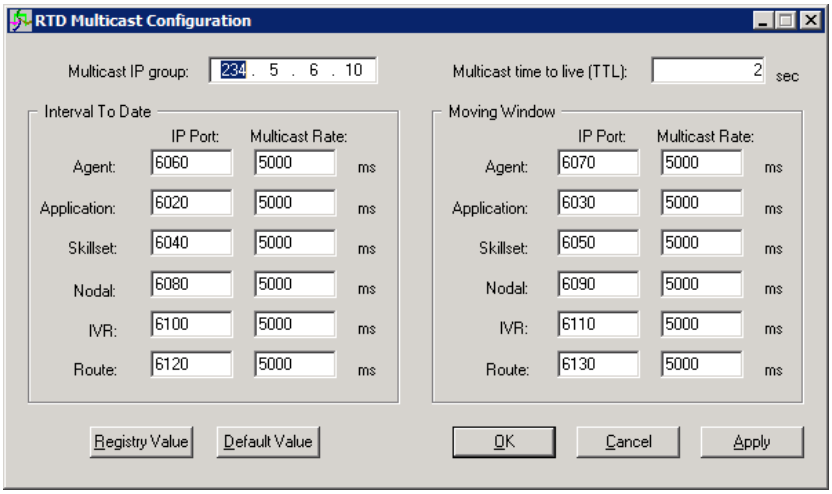
Step	Action
1	Log on to the Standby server (for example, **CCCORESTWO**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Manager Server**, **Multicast Stream Control**.
3	In the **RTD Multicast Controller** dialog box, select the check boxes for the Real Time data to enable.



4	Click **OK**.
5	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Manager Server**, **Multicast Address and Port Configuration**.
6	In the **RTD Multicast Configuration** dialog box, in the **Multicast IP group** box, type the multicast IP address Contact Center Manager Server uses to transmit the RTD, for example **234.5.6.10**. This is the same address as the Contact Center Manager Administration server receiving IP multicast address.
7	In the **Multicast Time To Live (TTL)** box, accept the default setting for the number of network hops packets can transition. **OR** Type a new value that matches your network topology.

Attention: Do not change the ports.

8 For the **Interval to Date IP Port** and **Multicast Rate**, and the **Moving Window IP Port** and **Multicast Rate** boxes, accept the default values.

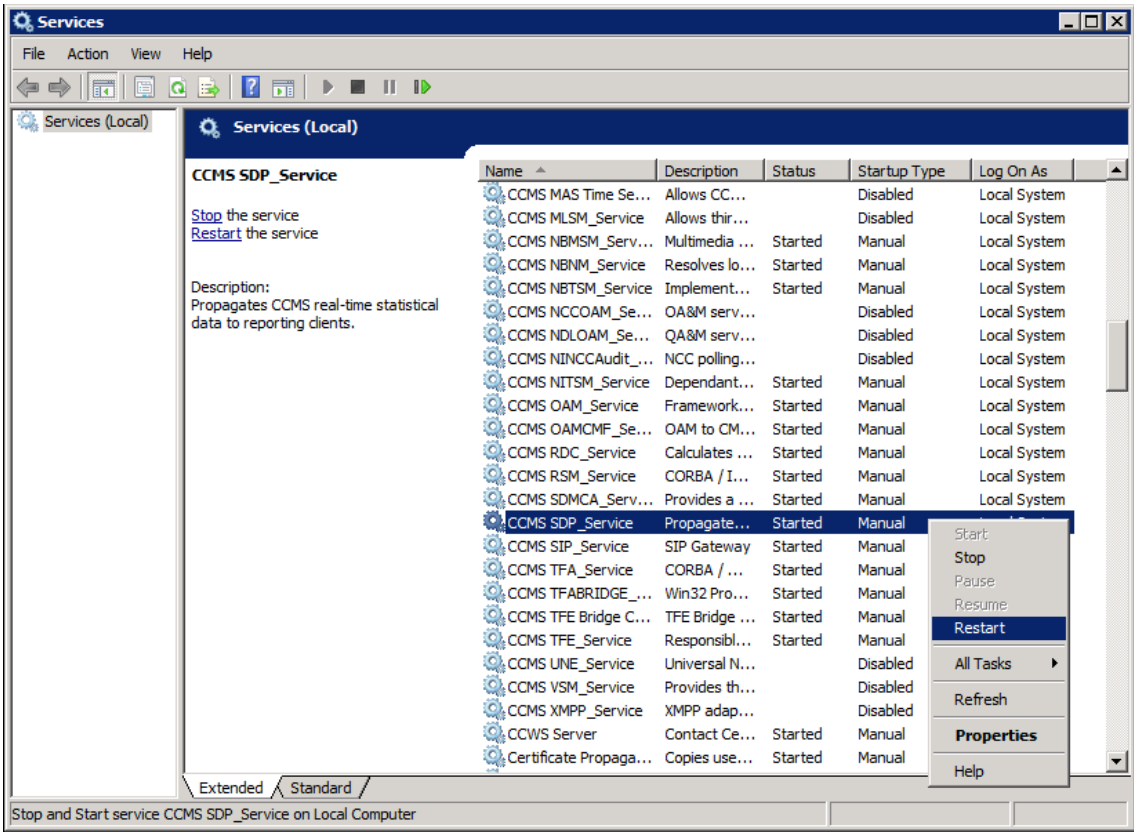


9 Click **OK**.

10 Click **Start**, **All Programs**, **Administrative Tools**, **Services**.

11 Scroll down to **CCMS SDP_Service**.

12 Right-click the **CCMS SDP_Service** and select **Restart**.



13 On the **Restart Other Services** dialog, click **Yes**.

--End--

Configuring Real-Time Reporting

Configure Real-Time Reporting if you plan to use multicast-based data transmission. You must configure the IP multicast addresses for the Contact Center Manager Server to receive Multicast data and for the Contact Center Manager Administration server sending IP multicast data.

If you configure a replicating server, you must select multicast for the transmission options under the Real-time Reporting Configuration.

Attention: The Real-Time Reporting settings on the Standby server must exactly match the Real-Time Reporting settings on the Active server.

Prerequisites

- Ensure that the IP multicast addresses that you select for Real-time Statistics Multicast (RSM) sending and receiving are in the 224.0.1.0 to 239.255.255.255 range. Check with your network administrator for acceptable IP multicast addresses for your network.
- Ensure that the Contact Center Manager Administration server sending and receiving IP multicast addresses differ.

Procedure steps

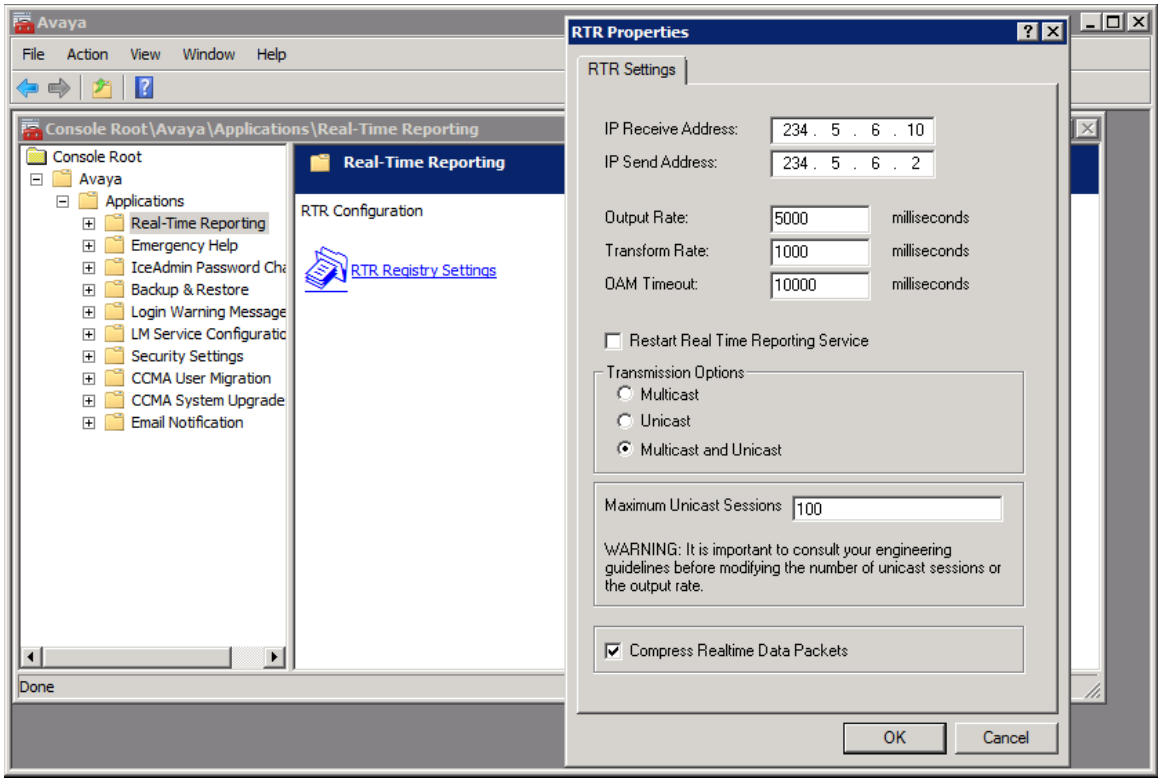
Step	Action
1	Log on to the Standby server (for example, **CCCORESTWO**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Click **Start, All Programs, Avaya, Contact Center, Manager Administration, Configuration**.
3	In the **Avaya Applications Configuration** window, in the left pane, navigate to **Avaya, Applications, Real-Time Reporting**.
4	In the right pane, click the **RTR Registry Settings** icon.
5	In the **RTR Properties** dialog box, in the **IP Receive Address** box, type the Contact Center Manager Administration server receiving IP multicast address, for example 234.5.6.10.
6	In the **IP Send Address** box, type the Contact Center Manager Administration server sending IP multicast address, for example **234.5.6.2**.
7	For the **Output Rate** box and the **Transform Rate** box, accept the default values (5000 and 1000).

Attention: You can adjust the default values; however, reducing the Output Rate value and the Transform Rate value increases the workload on the Contact Center Manager Administration server.

8	For the **OAM Timeout** box, accept the default value (10 000).
9	Select the **Compress Realtime Data Packets** check box.

Attention: If you clear this check box, you disable real-time data packet compression.

10	In the **Transmission Options** area, select one of the following options: • If your network supports multicast traffic, select **Multicast**. Avaya recommends this option. • To support both transmission types, select **Multicast and Unicast**.



11 If you select the **Multicast** option, proceed to step 14.

12 In the **Maximum Unicast Sessions** box, type the maximum number of simultaneous unicast sessions that you want the server to allow.

13 Select the **Restart Real Time Reporting Service** check box.

14 Click **OK**.

The Restart ICERtdService status window appears while the service is restarting, and closes after the service successfully restarts.

15 Close all windows to complete the procedure.

--End--

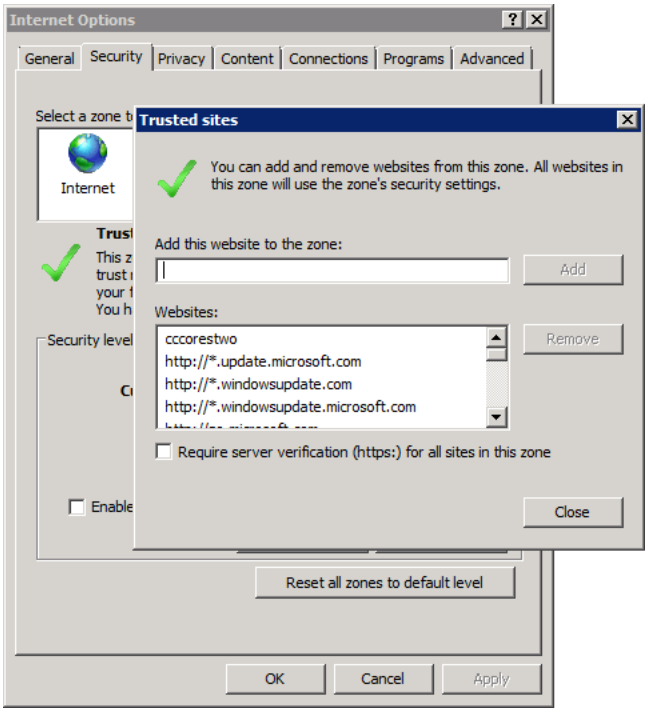
Configuring Internet Explorer on the Contact Center server

Configure Internet Explorer on the Contact Center server to access Contact Center Manager Administration for the first time.

Install Microsoft Internet Explorer 7.0 or later (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 Standby 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: • **Download signed ActiveX controls** • **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**. (Applies to Internet Explorer 7.0 and later.)
11	Click **OK**.
12	If you 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) of the Standby Contact Center server, for example **cccorestwo**.



17 Click **Add**.

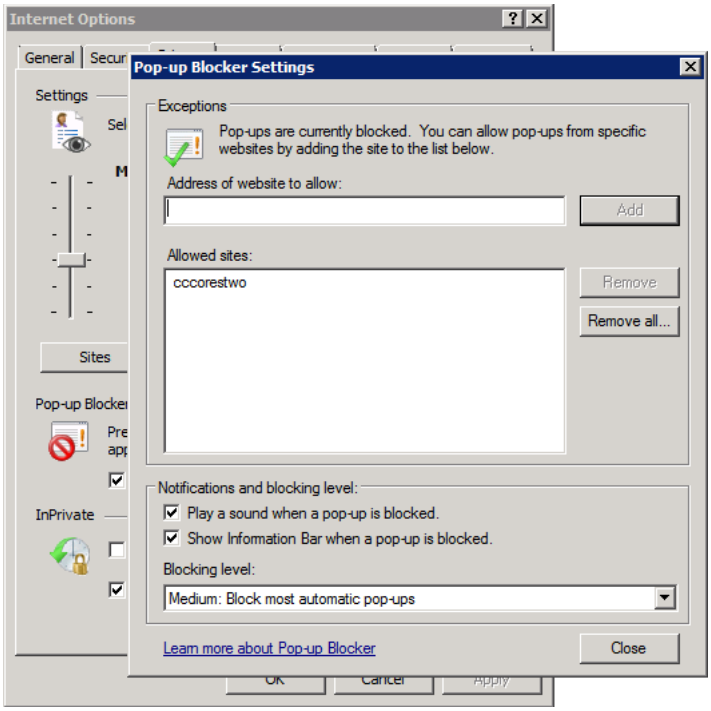
18 Click **Close** to return to the **Internet Options** dialog box.

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://cccorestwo**.



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.

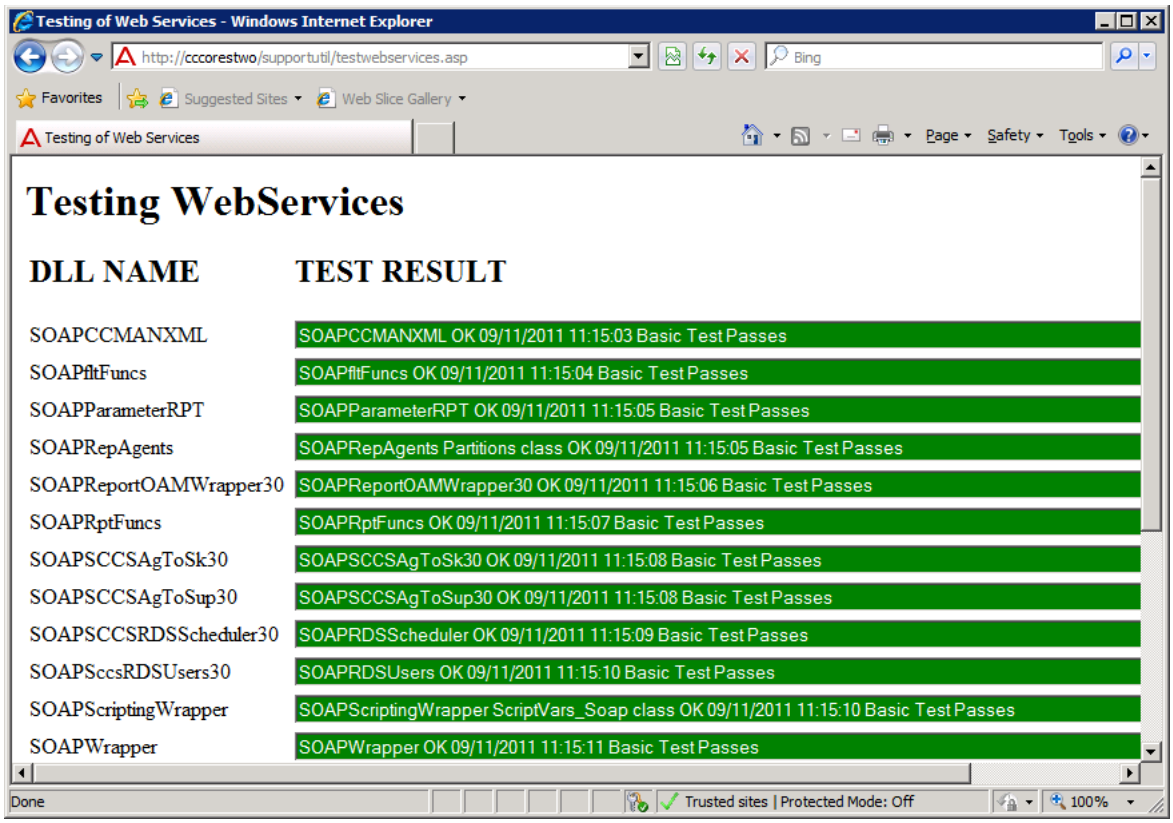
Procedure steps

Step	Action
1	On the Standby server, start Internet Explorer.

2 Enter the following URL in the format http://<server name>supportutil/testwebservices.asp, for example **http://cccorestwo/supportutil/testwebservices.asp**.

3 Wait for the page to refresh.

The web services that appear in green are running correctly.



--End--

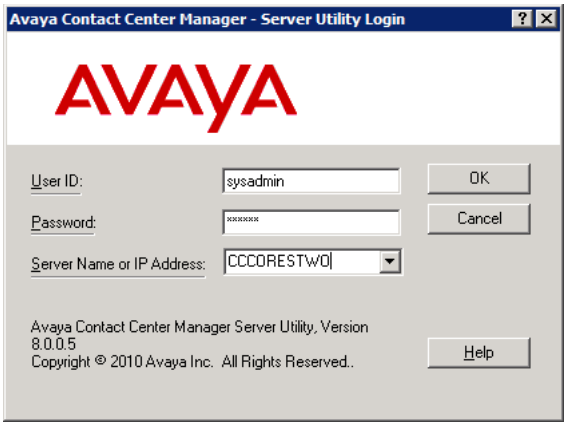
Changing the default sysadmin password

Change the sysadmin password from the default value. It is important to do this before logging on to CCMA for the first time and creating the CCMS server record in CCMA.

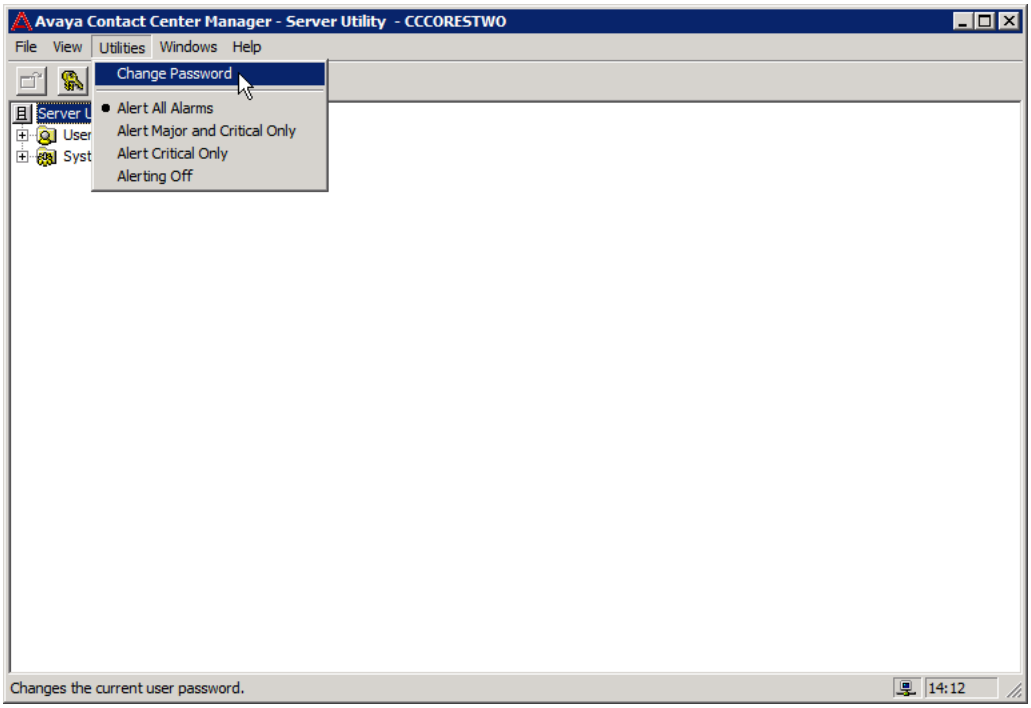
Attention: Ensure you keep a record of the sysadmin password. If you lose or forget this password, you are not able to carry out many important maintenance functions. There is no recovery mechanism for a lost sysdamin password–ultimately a lost sysadmin password requires a complete re-install of Contact Center.

Procedure steps

Step	Action
1	Log on to the Standby server (for example, **CCCORESTWO**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Select **Start, All Programs, Avaya, Contact Center, Server Utility, Server Utility**.
3	In the **User ID** box, type the system administrator user name **sysadmin**.
4	In the **Password** box, type the default system administrator password **avaya1**.



5	Click **OK**.
6	Close the **Alarm Monitor** window.
7	Choose **Utilities, Change Password**.



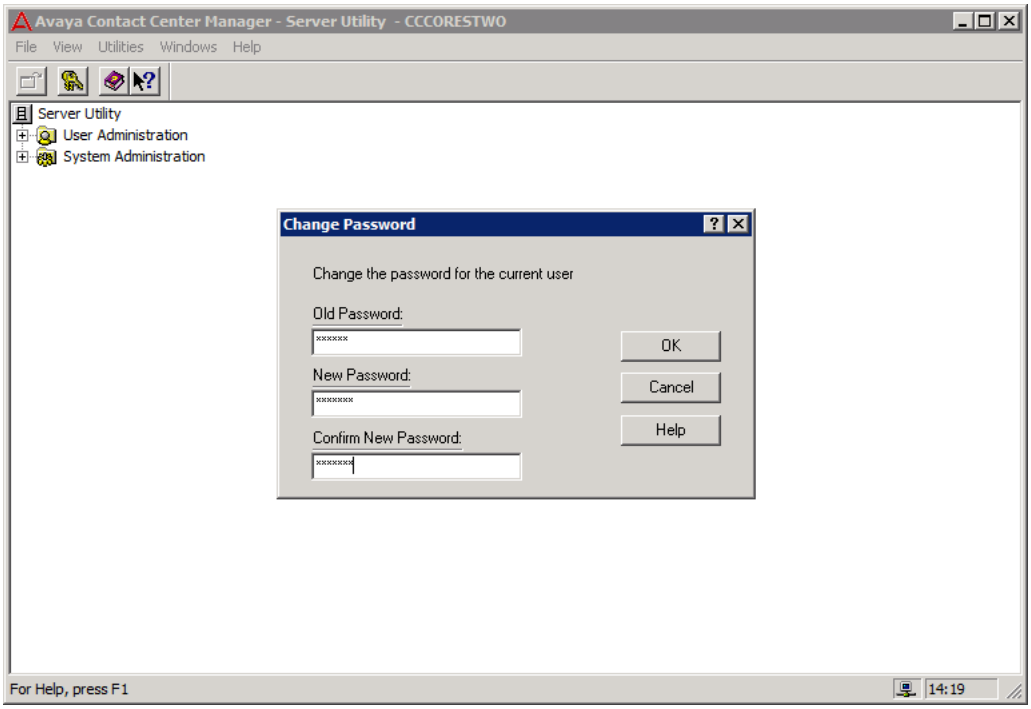
8 In the **Change Password** dialog box, in the **User name** box, type **sysadmin**.

9 In the **Old Password** box, type **avaya1**.

10 In the **New Password** box, type a new password, for example **sample1**.

11 In the **Confirm New Password** box, type the new password again.

Attention: Ensure you keep a record of the changed sysadmin password. If you lose or forget the new sysadmin password, you cannot perform many important maintenance tasks. There is no recovery from losing the sysdamin password: it requires a complete re-install of Contact Center.



12 Click **OK**.

13 Exit Server Utility.

--End--

Providing local users with the Log on as a service right

Provide local users with the 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

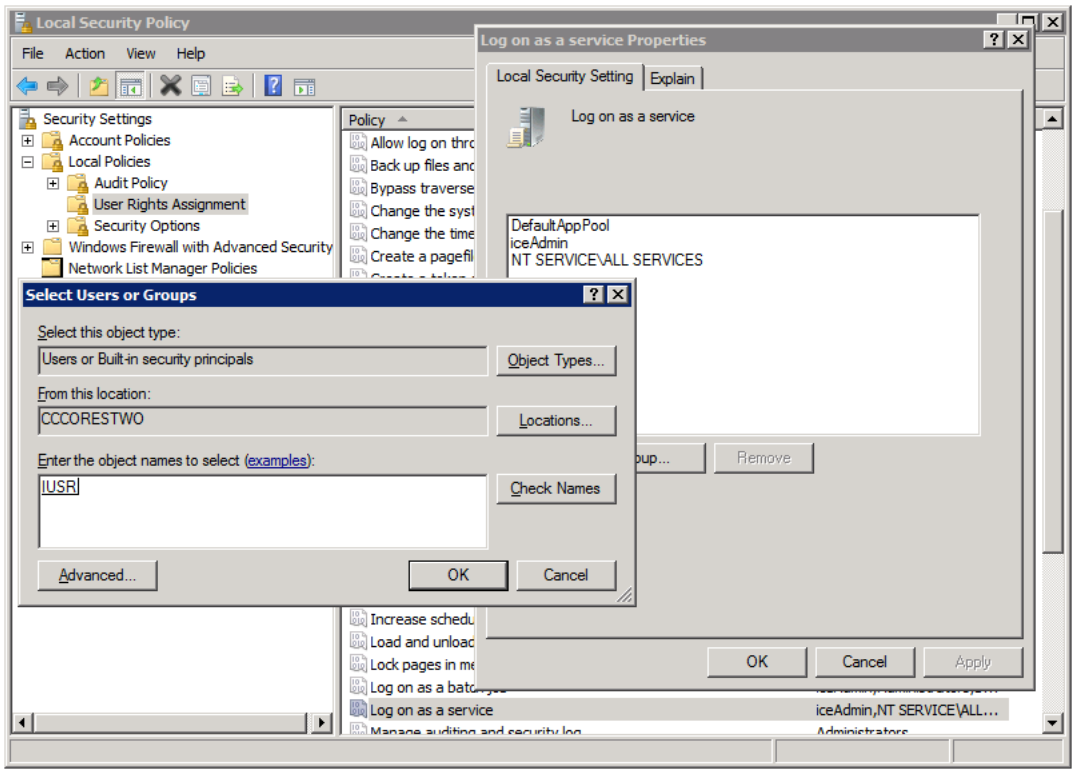
Step	Action
1	Click **Start**, **Administrative Tools**, **Local Security Policy**.
2	In the left pane, under **Security Settings**, expand **Local Policies**.
3	In the left pane, click **User Rights Assignment**.
4	In the right pane, double-click **Log on as a service**.
5	Click **Add User or Group**.
6	Click **Locations**.

7 In the **Locations** dialog box, select the Contact Center Multimedia 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 On the **Log on as a service Properties** dialog, click **OK**.

13 Close the **Local Security Settings** window.

--End--

Verifying the Multimedia database installation

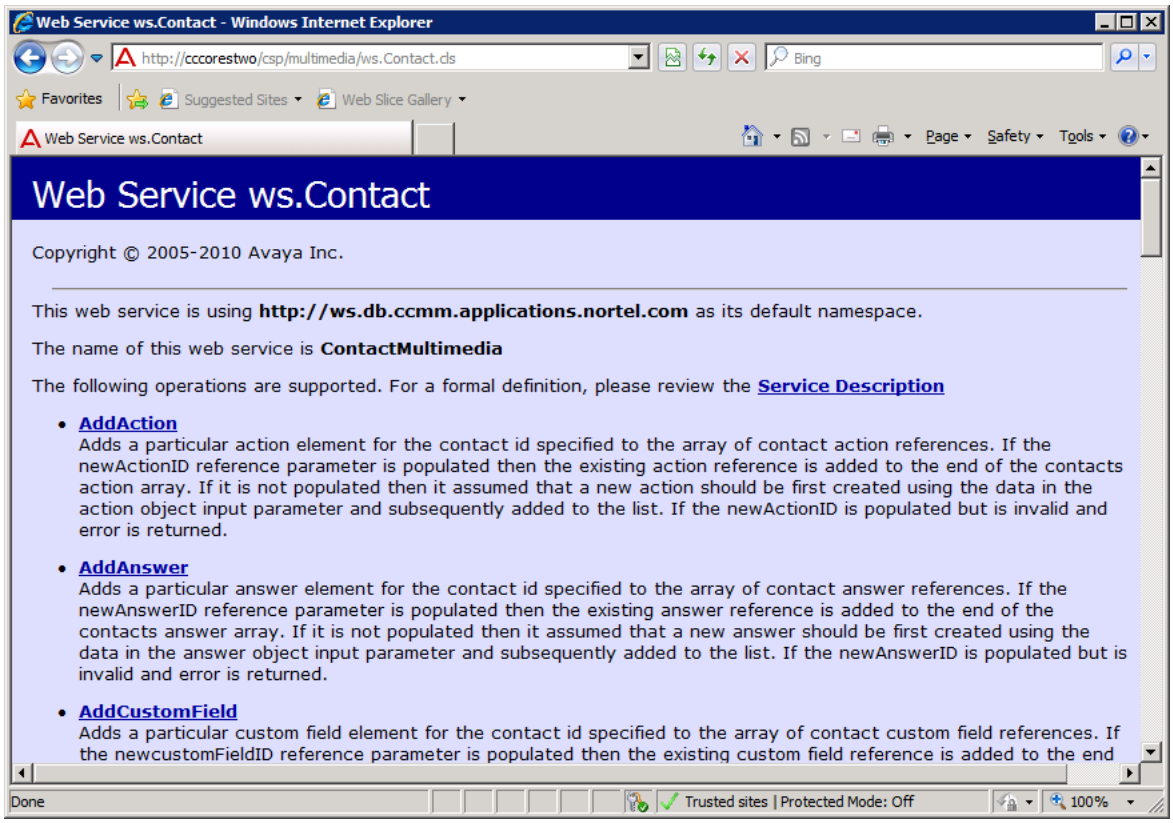
Verify that the Multimedia database is installed and configured correctly.

Procedure steps

Step **Action**

1 On the Contact Center Multimedia server, open Internet Explorer.

2 Browse to **http://cccorestwo/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

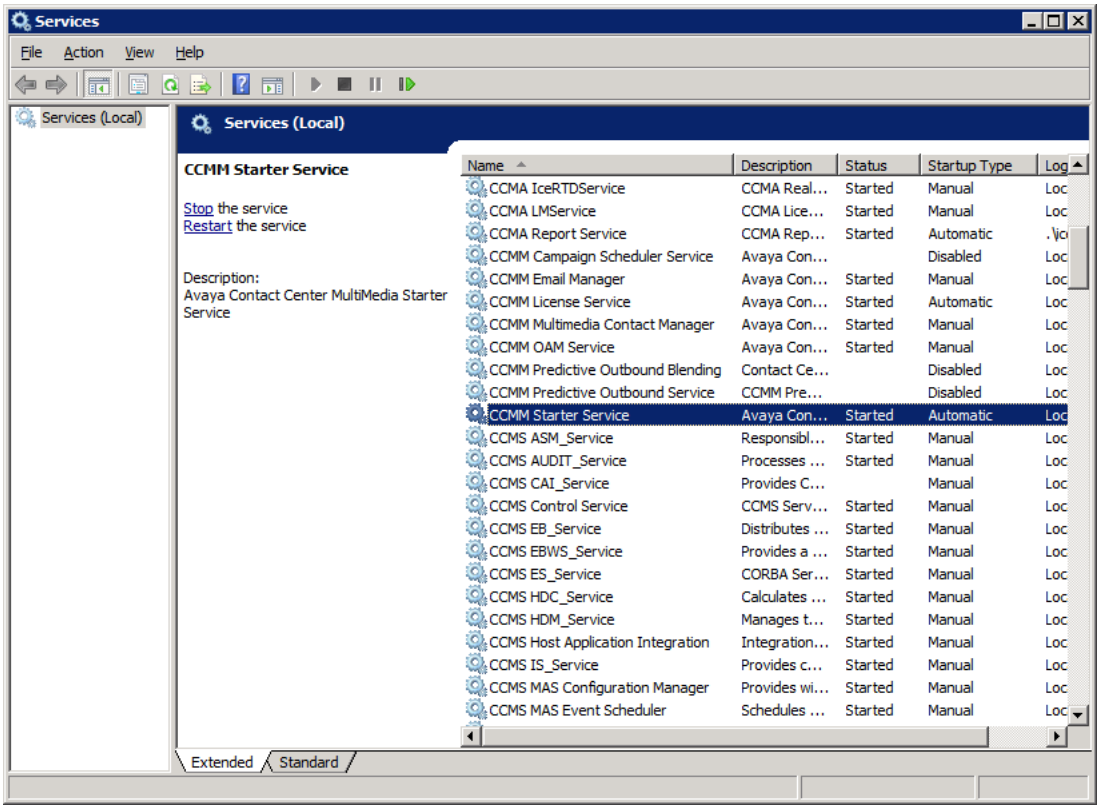
Verify that the Contact Center Multimedia services have the correct configuration to start automatically, to ensure that contacts are routed immediately after a server restart.

Procedure steps

Step	Action
1	On the Contact Center server, click **Start**, **Administrative Tools**, **Services**.
2	Next to **CCMM License Service**, verify that the status is **Started** and the startup type is **Automatic**.

3 Next to **CCMM Starter Service**, verify that the status is **Started** and the startup type is **Automatic**.

If either service does not have a startup type of **Automatic**, right-click the service and modify the properties to correct this.



4 Verify that the following services have a Status of **Started**:

- CCMM Multimedia Contact Manager
- CCMM OAM service
- CCMM Email Manager

5 If any service did not start, in the **Services** window, right-click the service name, and click **Start**.

6 Exit the **Services** window.

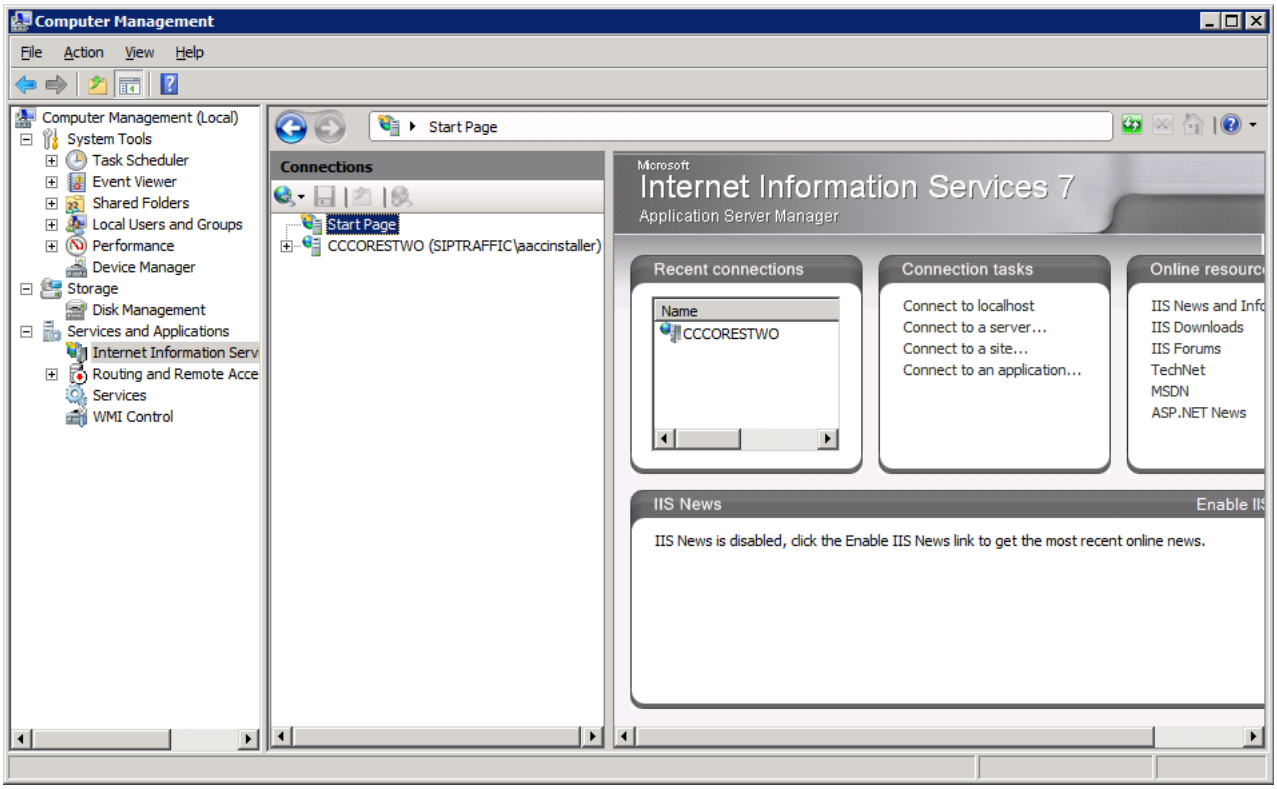
--End--

Configuring MIME types to support e-mail attachments

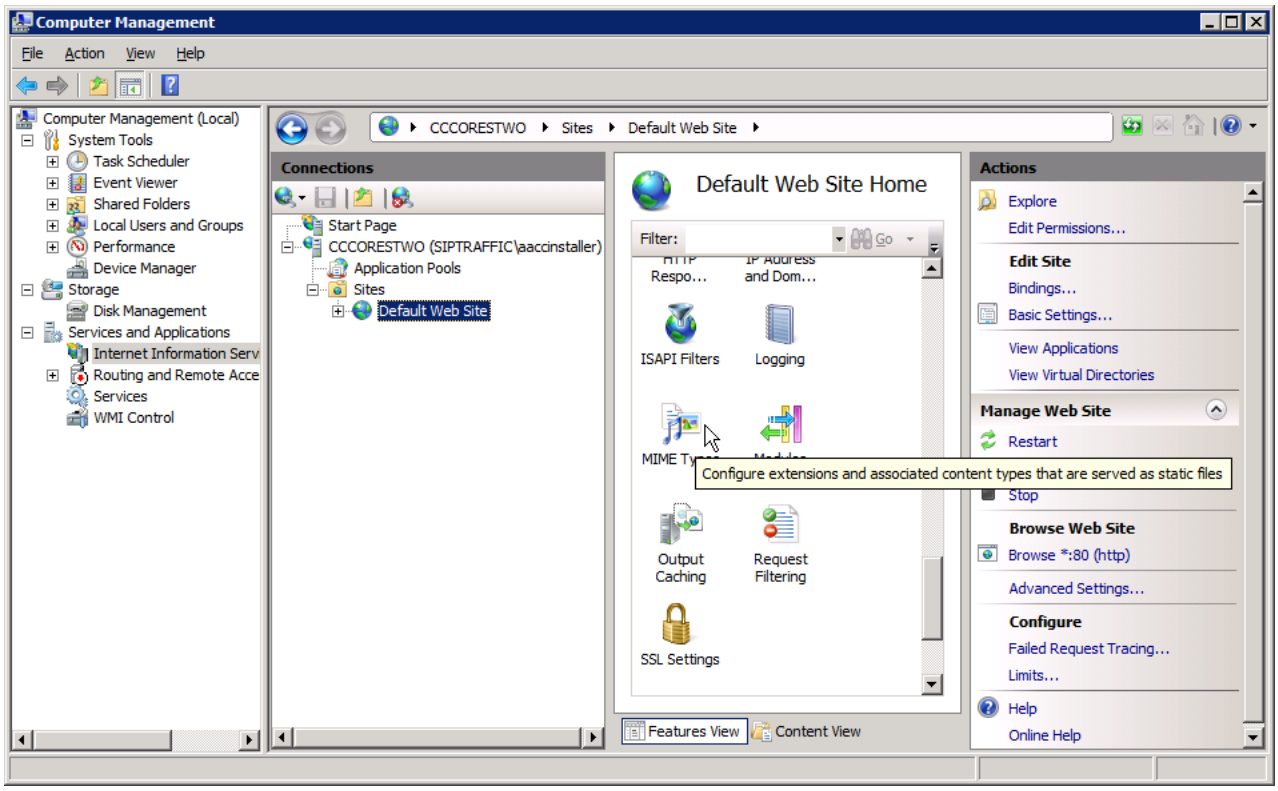
Configure the Multipurpose Internet Mail Extension (MIME) types to ensure that agents can access e-mail message attachments.

Procedure steps

Step	Action
1	Log on to the Standby server (for example, **CCCORESTWO**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
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 **CCCORESTWO**, **Sites**, **Default Web Site**.
5	Select **Default Web Site**.



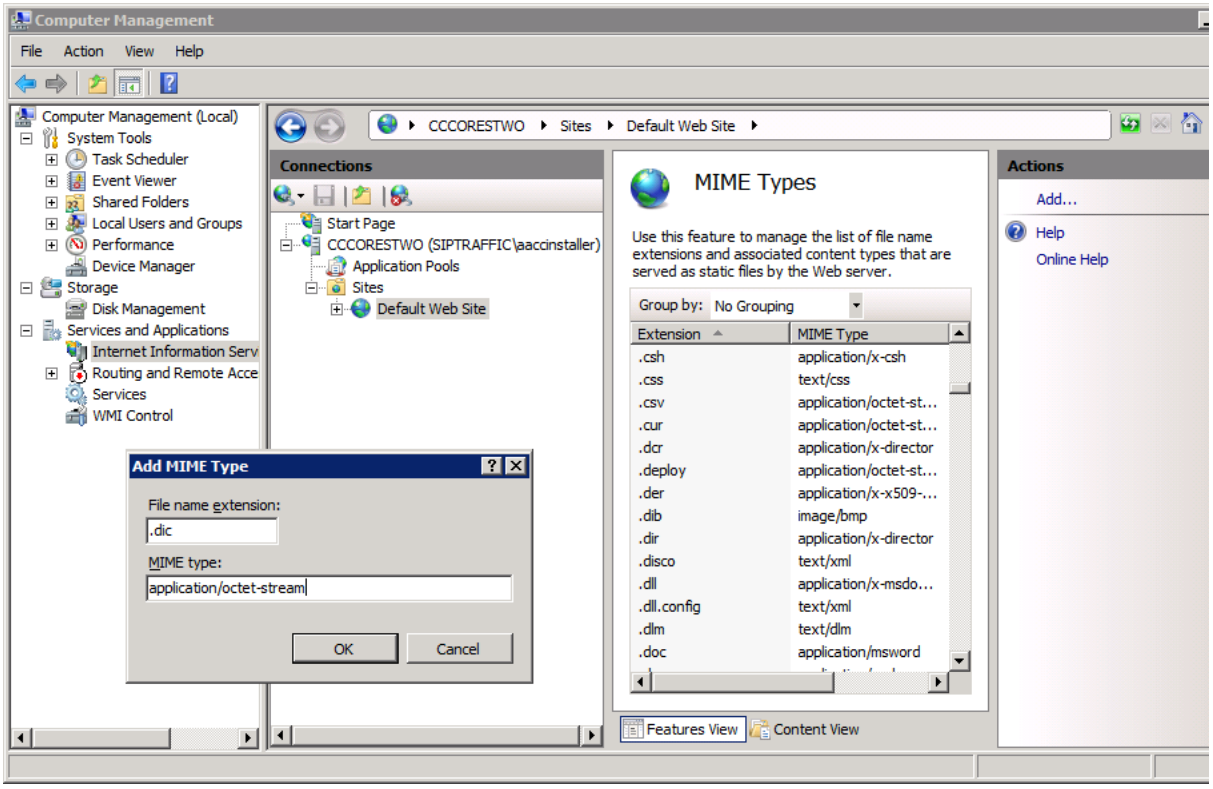
6	In the **Default Web Site Home** pane, under **IIS**, double-click **MIME Types**.



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

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

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

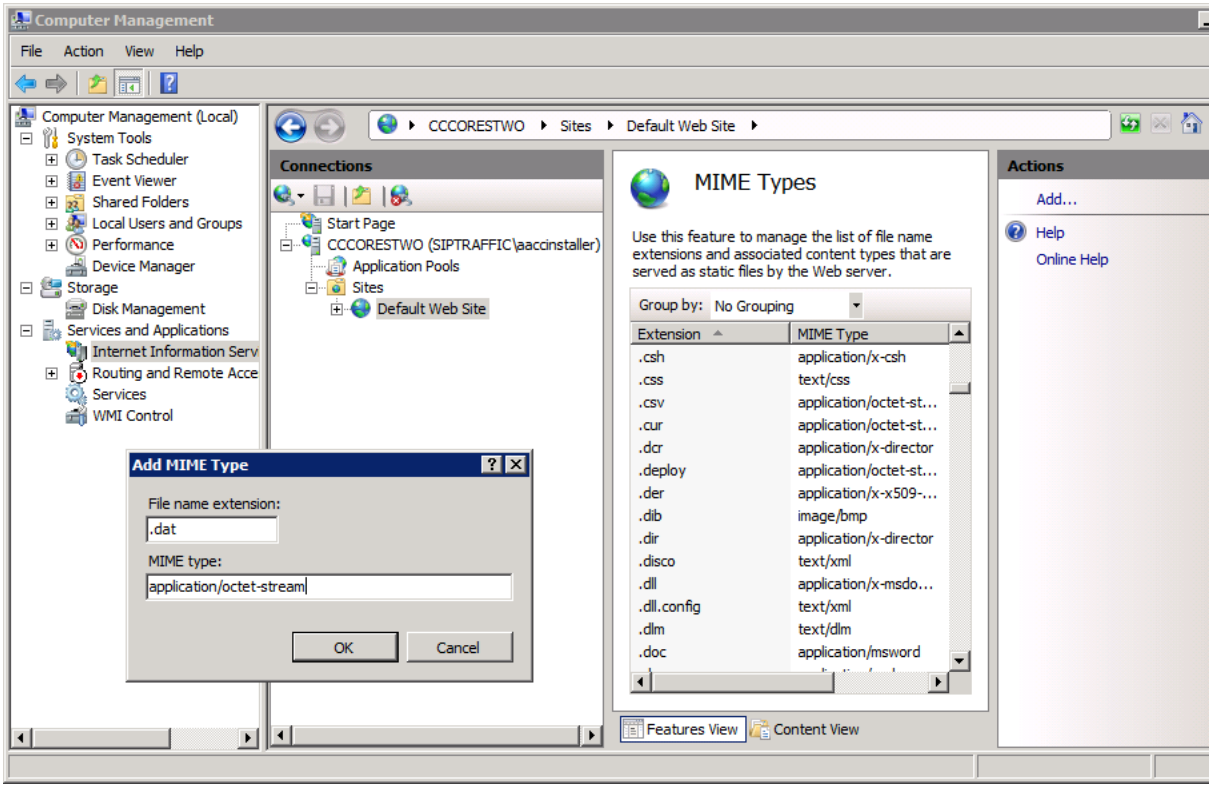


10 Click **OK**.

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**.

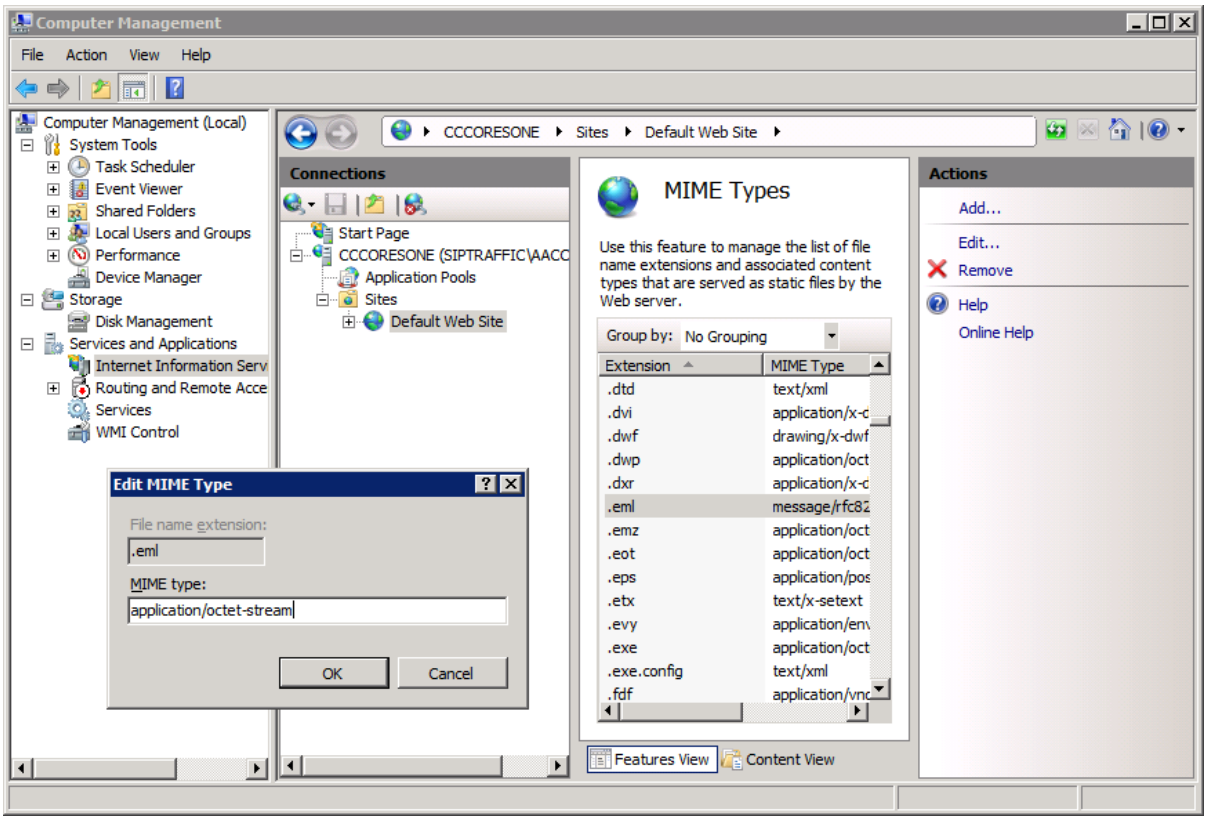


14 Click **OK**.

15 In the MIME Types list, find the **.eml** extension.

16 Right-click the **.eml** extension, and select **Edit**.

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



18 Click **OK**.

19 Close the **Computer Management** window.

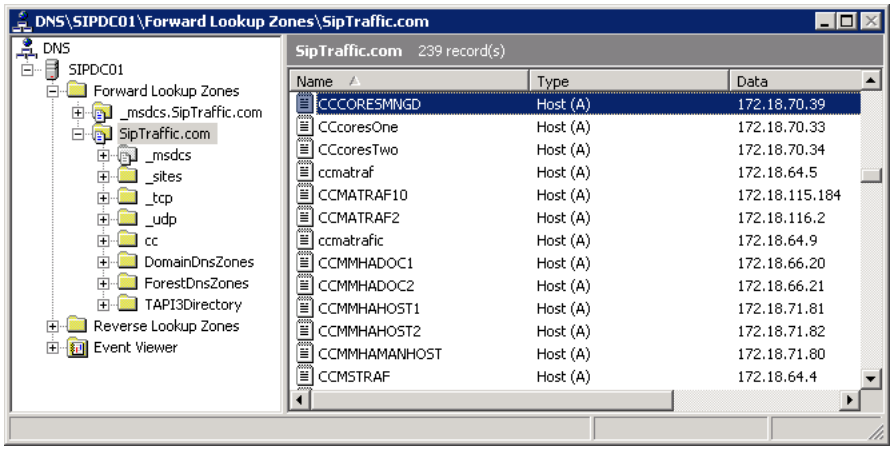
--End--

High Availability server commissioning

This section describes how to configure High Availability (HA) resiliency for a pair of co-resident Contact Center servers installed as a Multimedia Complement to Call Center Elite.

Example server details	
Active server name	CCCORESONE
Active server IP Address	172.18.70.33
Standby server name	CCCORESTWO
Standby server IP Address	172.18.70.34
Managed server name	CCCORESMNGD
Managed IP Address	172.18.70.39

A typical High Availability campus solution with a pair of co-resident 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.



High Availability campus overview

In a Multimedia Complement HA configuration, one Contact Center server is the active server and one is the standby server. The active 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 standby mode, recognizes the failure and starts processing contacts. After the switchover, High Availability is disabled on the original active server.

The Active and Standby servers are part of the same Avaya Aura® Contact Center and they must be in the same IP subnet for High Availability resiliency to work.

The Standby server must be configured to be 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. The shadowing process automatically copies any Active server configuration changes to the Standby server, so that the Standby server can take over processing from the Active server when necessary.

In a co-resident High Availability solution, a failure of a Contact Center service, hardware, network, or database can initiate a switchover but only in the following situations:

- The Active server is in active mode.
- The Active server is running: all the critical services are monitored and running.
- The Standby server has Enable Switchover on.
- The Active and Standby servers can communicate with a trusted server.
- The Active server database and Standby server database are synchronized, and the Standby server database is shadowing the Active server database.

If an Administrator uses the Windows Service Control Manager (SCM) to stop a monitored service on an Active server, a switchover occurs. If an 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 an Administrator stops it, the Standby server stops all services and the contact center solution is no longer resilient.

High Availability Utility

Configure High Availability resiliency using the High Availability (HA) Utility in Database Utilities. Use the High Availability Utility to configure which server is the Active and which server is the Standby. The HA utility is also where you configure the Managed IP address of the Active server.

The High Availability Utility on an Active Server has the following dialogs on the Configuration tab:

- Server Mode, which allows you to:
  - configure the IP addresses for the Active and Standby servers
  - configure the IP addresses for Trusted servers
  - identify if the server is in active or standby mode
  - enable Switchover
  - configure the switchover time-out; this is the wait time, in case of a network outage, before the server starts an automatic switchover

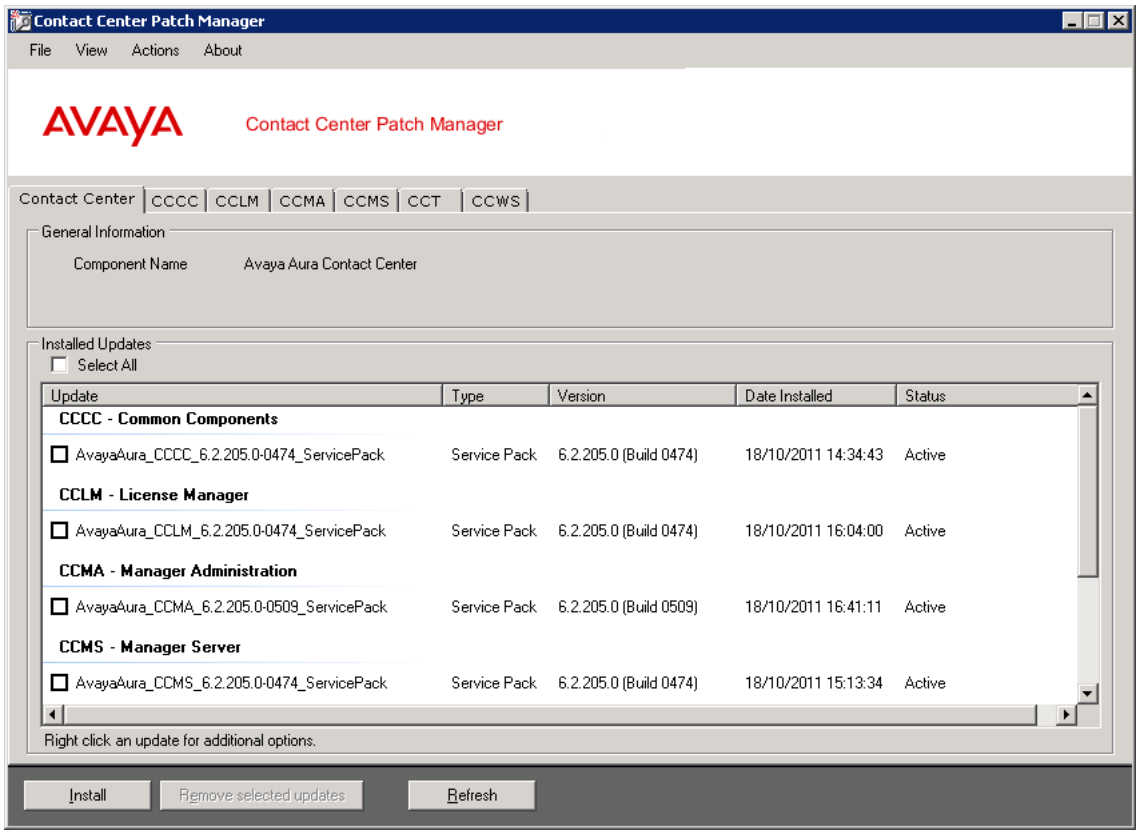
- Notifications, which allows you to:
  - configure an e-mail server for e-mail notifications
  - configure where and how often to send e-mail notifications
  - configure the e-mail character set
- System, which allows you to:
  - display information on the system status
  - verify that database shadowing is running
- CC Applications, which allows you to:
  - review the statuses of the different Contact Center applications
  - stop or start the different Contact Center applications
- CC Applications, which allows you to:
  - configure which Contact Center services High Availability monitors
  - configure the switchover settings for each Contact Center service
- System Control, which allows you to:
  - stop and start shadowing
  - force a manual switchover

Installing the latest Contact Center software patches on the Active server

Install the most recent Contact Center Manager Server software service patches on the Active server to ensure that you have the most current development updates.

Procedure steps

Step	Action
1	Log on to the Active server (for example, **CCCORESONE**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Download the latest Contact Center patches from www.avaya.com/support to the patch directory on the Active server, for example **C:\Avaya_Support**.
3	Right-click each .ZIP file and select **Extract to here...**.
4	Click **Start, All Programs, Avaya, Contact Center, Common Utilities, Contact Center Patch Manager**.



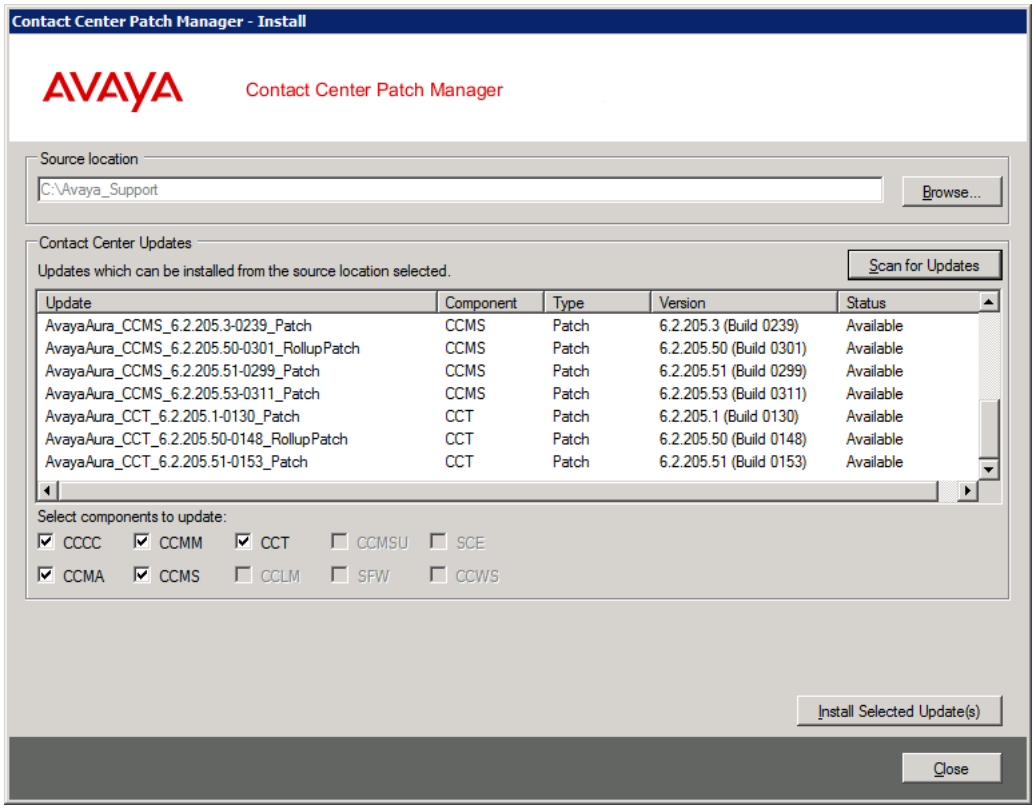
5 Click **Install**.

6 Click **Browse** and navigate to the folder where you have downloaded the patches, for example **C:\Avaya_Support**.

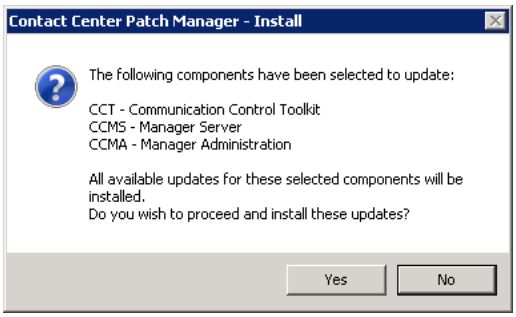
7 Click **Scan for Updates**.

The Contact Center Updates section displays the available patches.

8 Select the patches that you downloaded and extracted.



9 Click **Install Selected Updates**.



10 Click **Yes**.

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

11 Click **Close**.

12 Verify that the newly installed patch appears under **Installed Updates**.

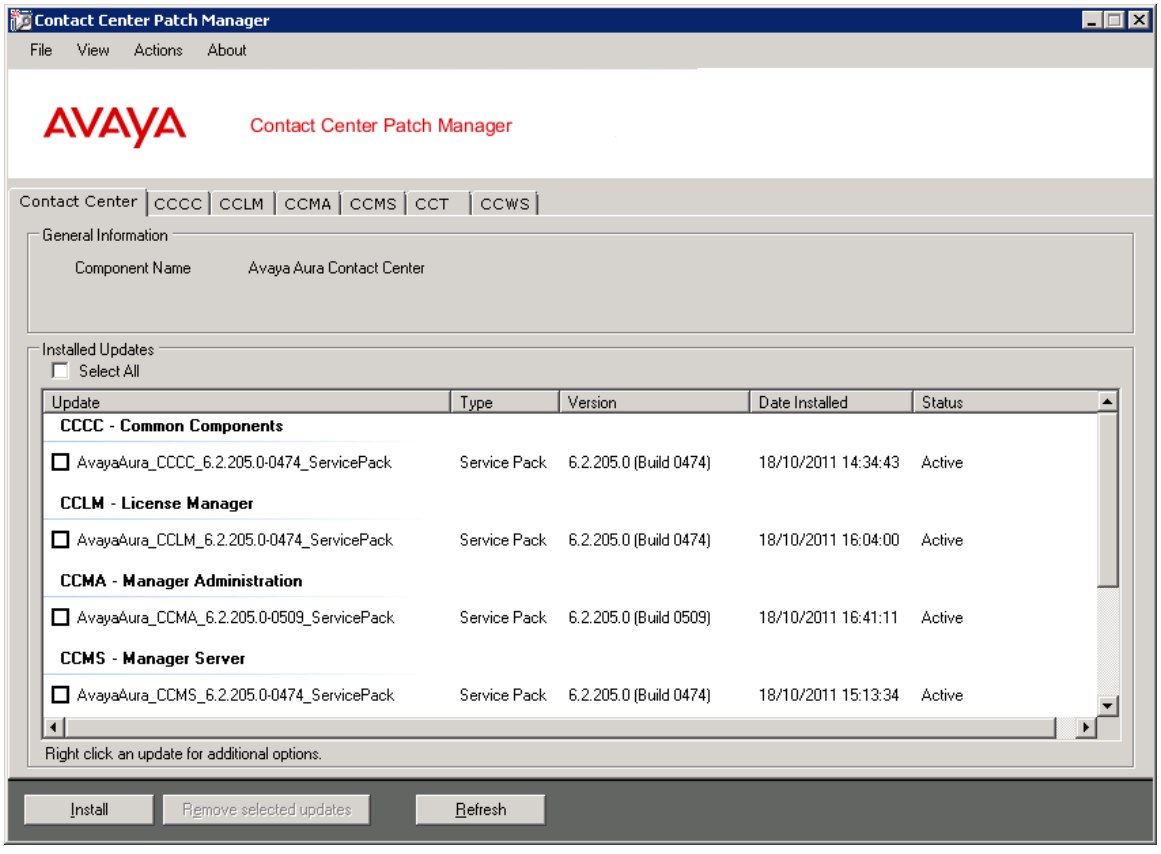
--End--

Installing the latest Contact Center software patches on the Standby server

Install the most recent Contact Center Manager Server software service patches on the Standby server to ensure that you have the most current development updates. Ensure the patches installed on the Standby server exactly match those installed on the Active server.

Procedure steps

Step	Action
1	Log on to the Standby server (for example, **CCCORESTWO**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Download the latest Contact Center patches from support.avaya.com to the patch directory on the Standby server, for example **C:\Avaya_Support**.
3	Right-click each .ZIP file and select **Extract to here...**.
4	Click **Start, All Programs, Avaya, Contact Center, Common Utilities, Contact Center Patch Manager**.

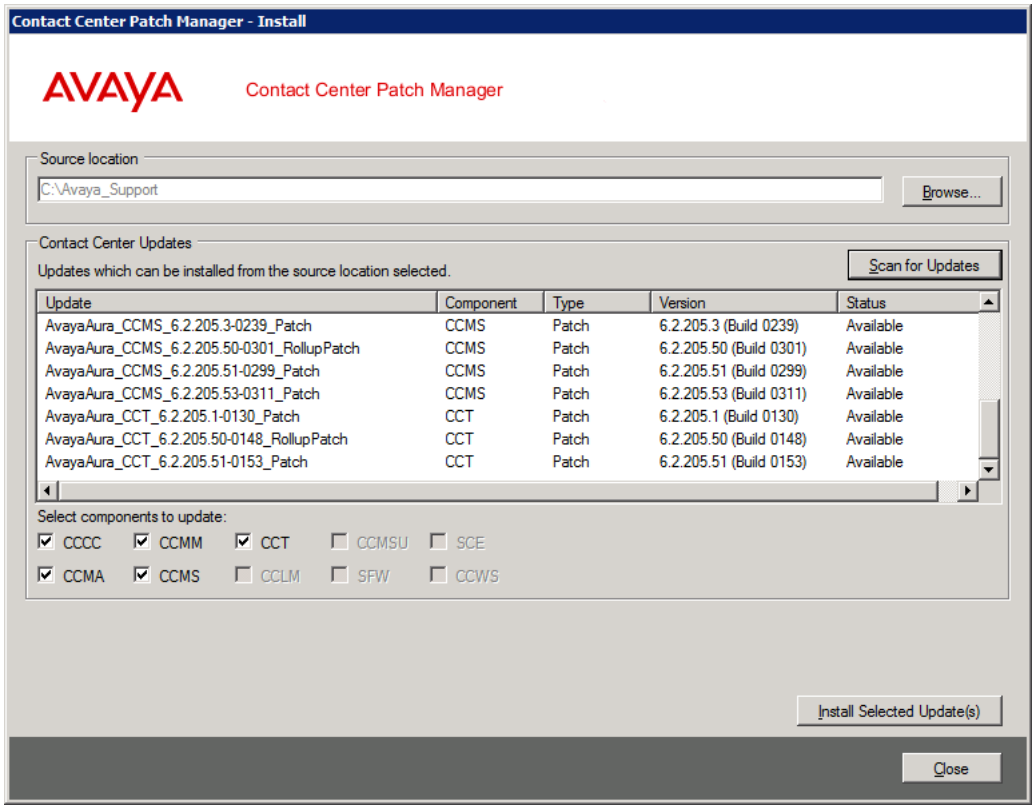


5	Click **Install**.
6	Click **Browse** and navigate to the folder where you have downloaded the patches, for example **C:\Avaya_Support**.

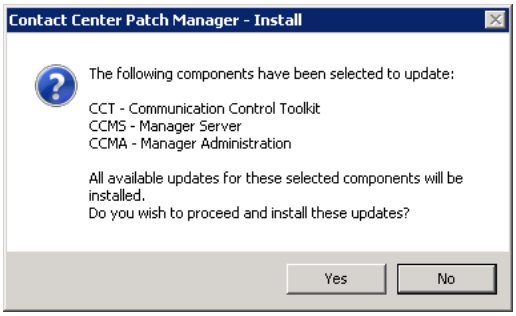
7 Click **Scan for Updates**.

The Contact Center Updates section displays the available patches.

8 Select the patches that you downloaded and extracted.



9 Click **Install Selected Updates**.



10 Click **Yes**.

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

11 Click **Close**.

12 Verify that the newly installed patches appear under **Installed Updates**.

13	Verify that the patches listed under **Installed Updates** exactly match those installed on the Active server.

--End--

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 using the Windows hosts file.

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

A typical High Availability campus solution with a pair of co-resident 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.

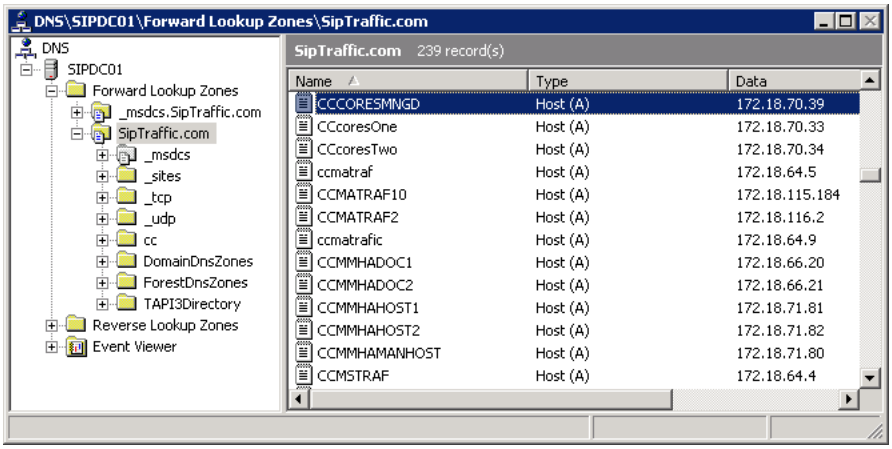
Procedure steps

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 CCCORESONE with an IP address 172.18.70.33; the Standby (secondary) server - hostname CCCORESTWO with an IP address 172.18.70.34;and the Managed name and Managed IP - CCCORESMNGD and 172.18.70.39.

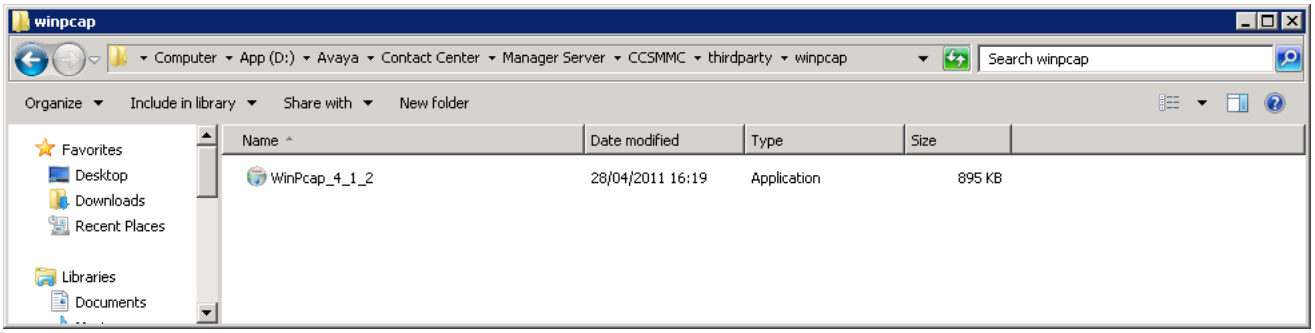


Installing a third-party utility to support High Availability on the Active server

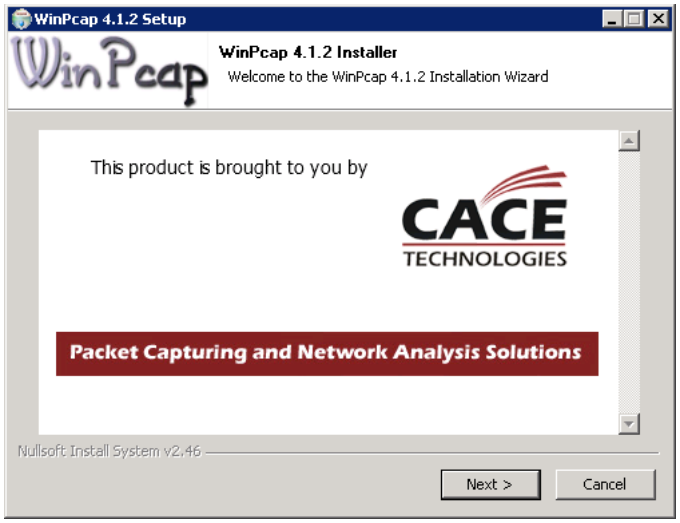
Install a third-party utility required by the Avaya Aura® Contact Center High Availability feature.

Procedure steps

Step	Action
1	Log on to the Active server (for example, **CCCORESONE**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
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**.

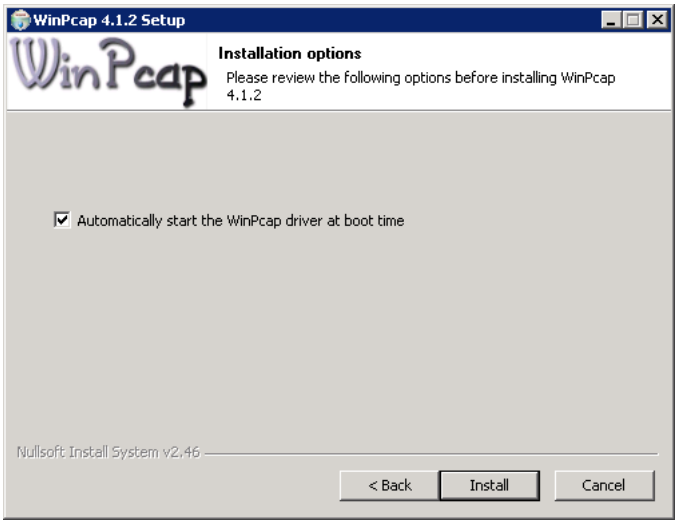


5 On the WinPcap installer **Setup Wizard** dialog, click **Next**.

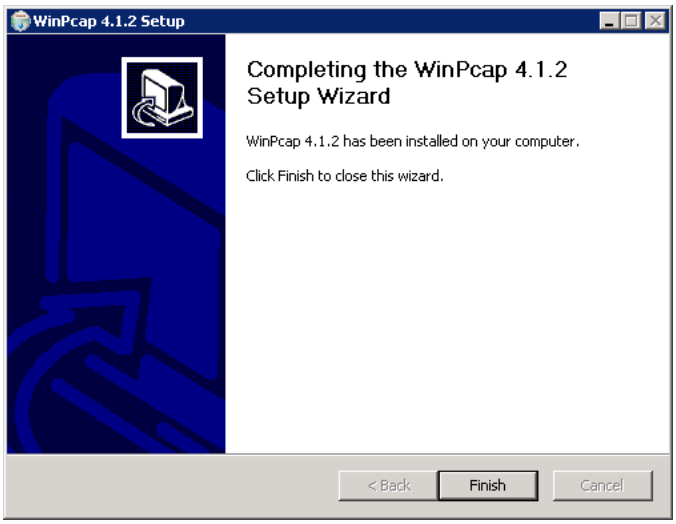


6 On the WinPcap installer **License Agreement** dialog, click **I Agree**.

7 On the WinPcap installer **Installation options** dialog, click **Install**.



8 On the WinPcap installer dialog, click **Finish**.



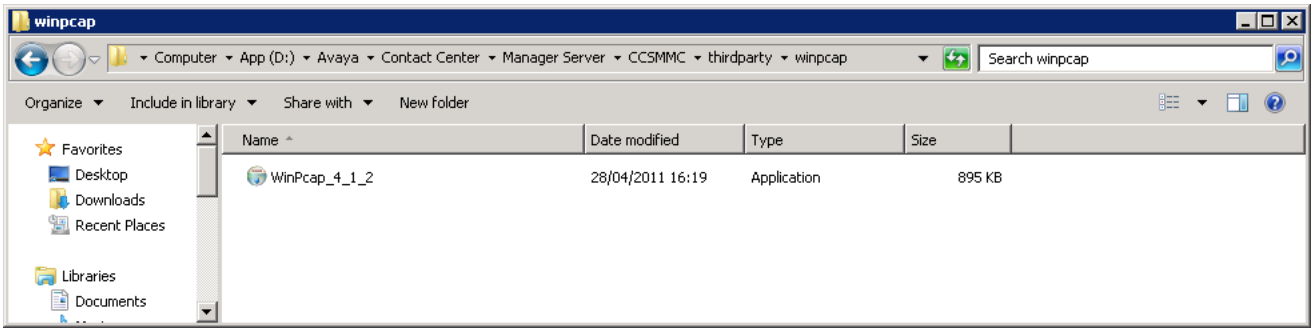
--End--

Installing a third-party utility to support High Availability on the Standby server

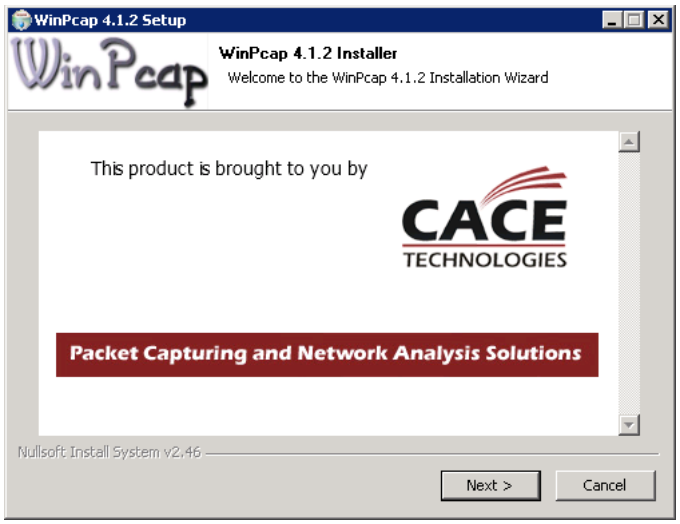
Install a third-party utility required by the Avaya Aura® Contact Center High Availability feature.

Procedure steps

Step	Action
1	Log on to the Standby server (for example, **CCCORESTWO**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Using Windows Explorer, navigate to D:\Avaya\Contact Center\Manager Server\CCSMMC\thirdparty\winpcap.



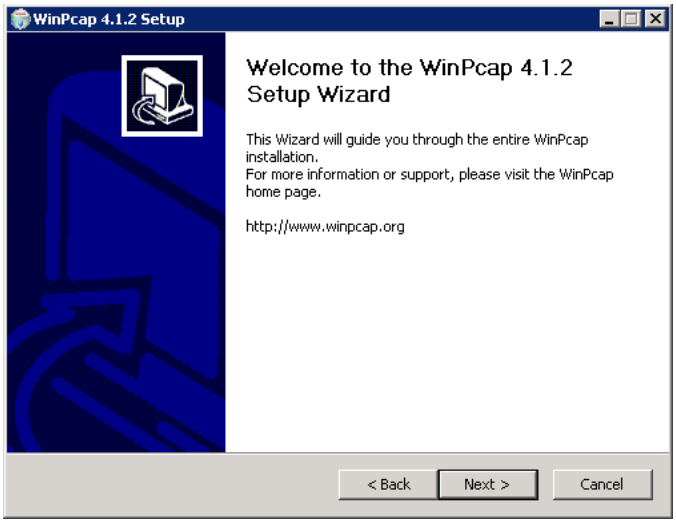
3 Double-click **WinPcap_4_1_2.exe**.



4 On the **WinPcap** installer dialog, click **Next**.

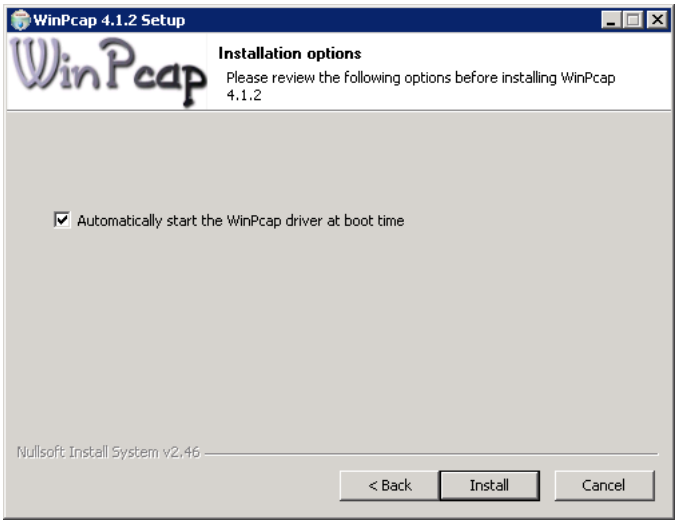


5 On the WinPcap installer **Setup Wizard** dialog, click **Next**.

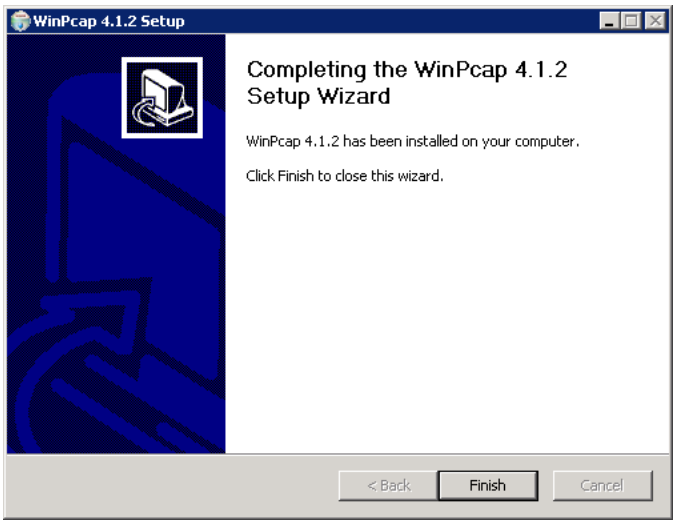


6 On the WinPcap installer **License Agreement** dialog, click **I Agree**.

7 On the WinPcap installer **Installation options** dialog, click **Install**.



8 On the WinPcap installer dialog, click **Finish**.



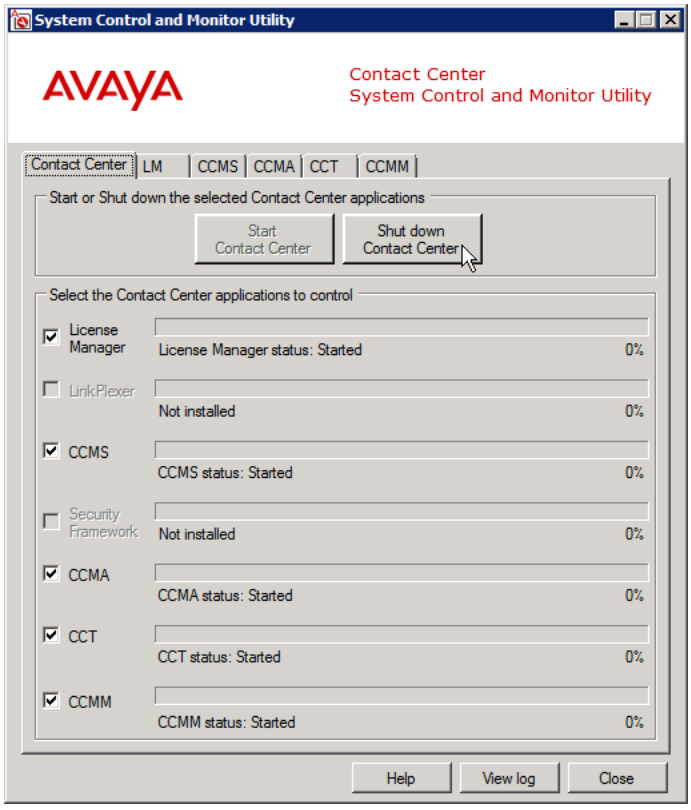
--End--

Verifying services are ready for High Availability on the active server

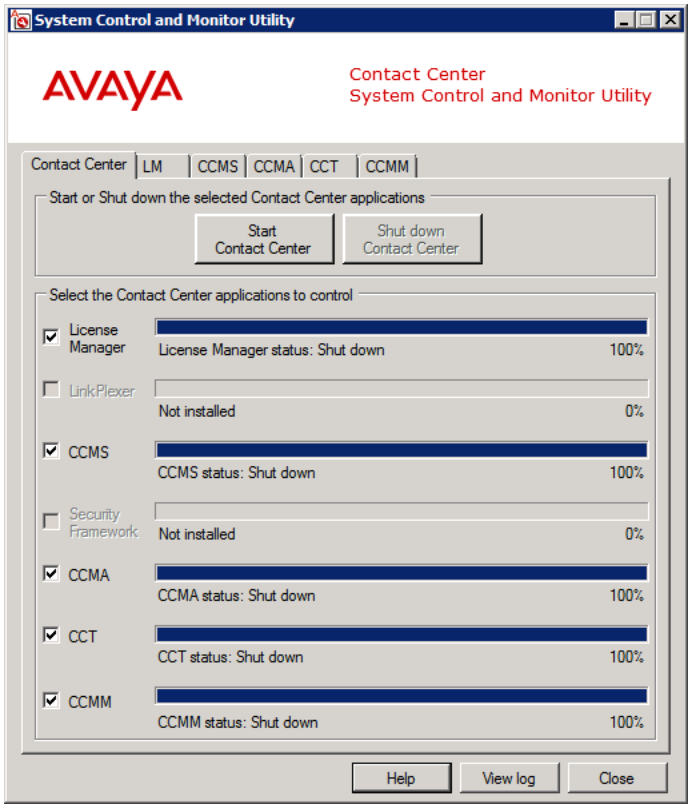
Verify that all Contact Center services stop before you configure High Availability. This ensures that all resources are available to the Active Server when it starts.

Procedure steps

Step	Action
1	Log on to the Active server (for example, **CCCORESONE**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Click **Start, All Programs, Avaya, Contact Center, Common Utilities, System Control and Monitor Utility**.
3	On the **Contact Center** tab, click **Shut down Contact Center**.



4 Wait until all the Contact Center components have stopped.



5 Click **Close**.

--End--

Verifying services are ready for High Availability on the standby server

Verify that all Contact Center services stop before you configure High Availability. This ensures that all resources are available to the Active Server when it starts.

Procedure steps

Step	Action
1	Log on to the Standby server (for example, **CCCORESTWO**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Click **Start, All Programs, Avaya, Contact Center, Common Utilities, System Control and Monitor Utility**.
3	On the **Contact Center** tab, click **Shut down Contact Center**.
4	Wait until all the Contact Center components have stopped.

5 Click **Close**.

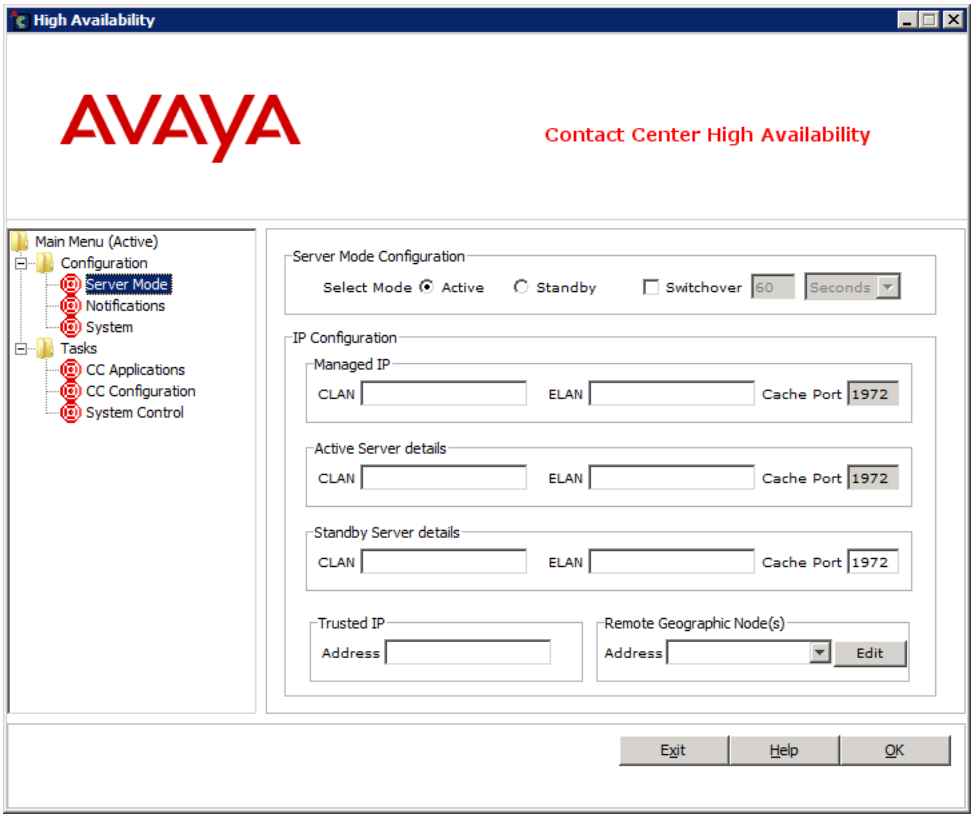
--End--

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 co-resident CCMS and CCT server that normally processes calls.

Procedure steps

Step	Action
1	Log on to the Active server (for example, **CCCORESONE**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Database Utilities**, **High Availability**.
3	Expand **Configuration**.



4 Click **Server Mode**.

5 Under **Server Mode**, select **Active**.

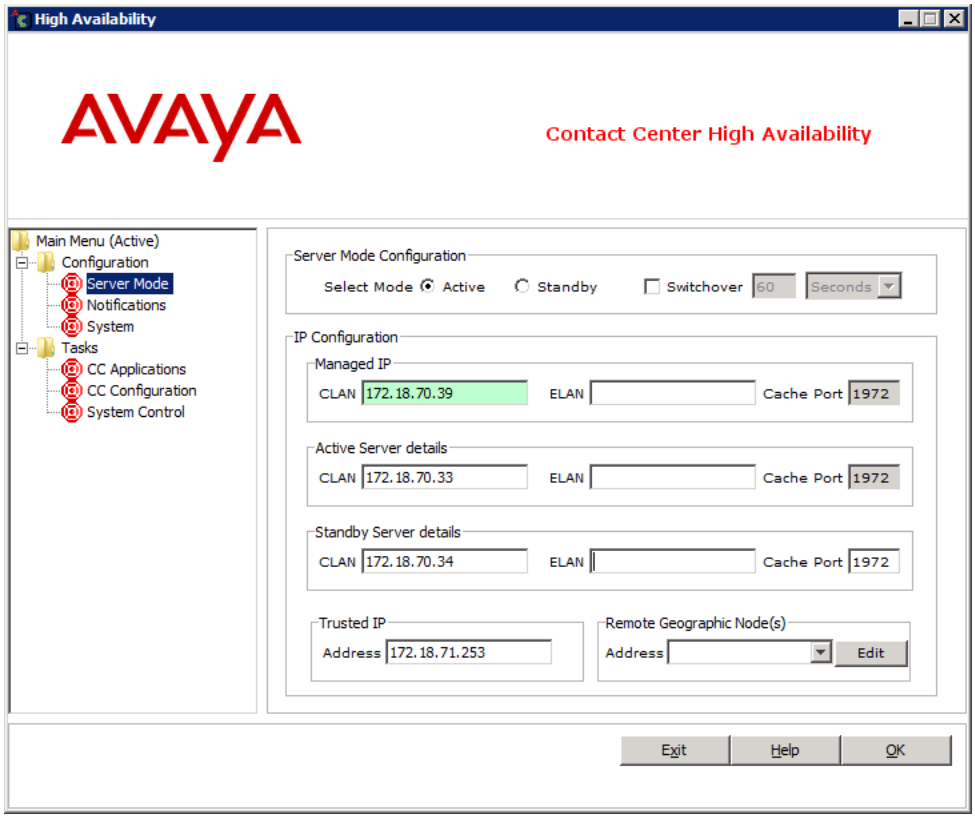
6 Under **IP Configuration**, in the **Managed IP** box, type the managed IP address for the contact center, for example **172.18.70.39**.

7 Under **IP Configuration**, in the **Active CLAN** box, type the IP address for the active server. For example, type **172.18.70.33**.

8 Under **IP Configuration**, in the **Standby CLAN** box, type the IP address for the standby server. For example, type **172.18.70.34**.

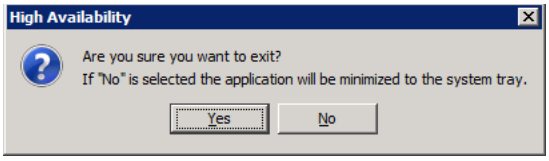
9 Under **IP Configuration**, in the **Trusted IP** box, type the IP address of a trusted server. For example, use the DNS server IP address, **172.18.71.253**.

10 Leave the **Remote Geographic Node (Optional)** box blank.



11 Click **OK**

12 Click **Exit**.



13 Click **Yes**.

--End--

Configuring E-mail notification on the Active Server

If an automatic switchover occurs, the High Availability utility can send e-mail messages to configured users at a defined interval.

The default e-mail notification character set is US_ASCII. The following character sets are also supported:

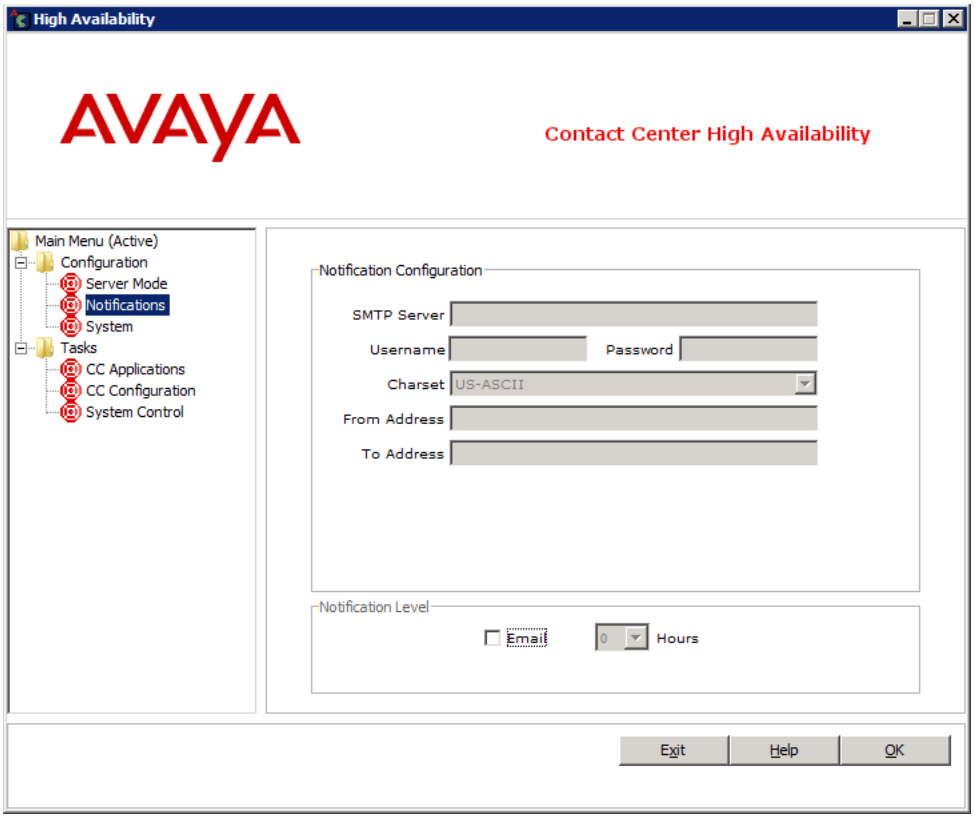
- ISO-8859-1
- UTF-16BE
- UTF-8
- UTF-8
- UTF-16BE
- UTF-16LE
- UTF-16

Prerequisites

- If anonymous users are allowed, a user name and password may not be required. Check with the Administrator of the e-mail server for setup configuration.

Procedure steps

Step	Action
1	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Database Utilities**, **High Availability**.
2	Expand **Configuration**.
3	Double-click **Notification**.



4 Select the **Email** check box.

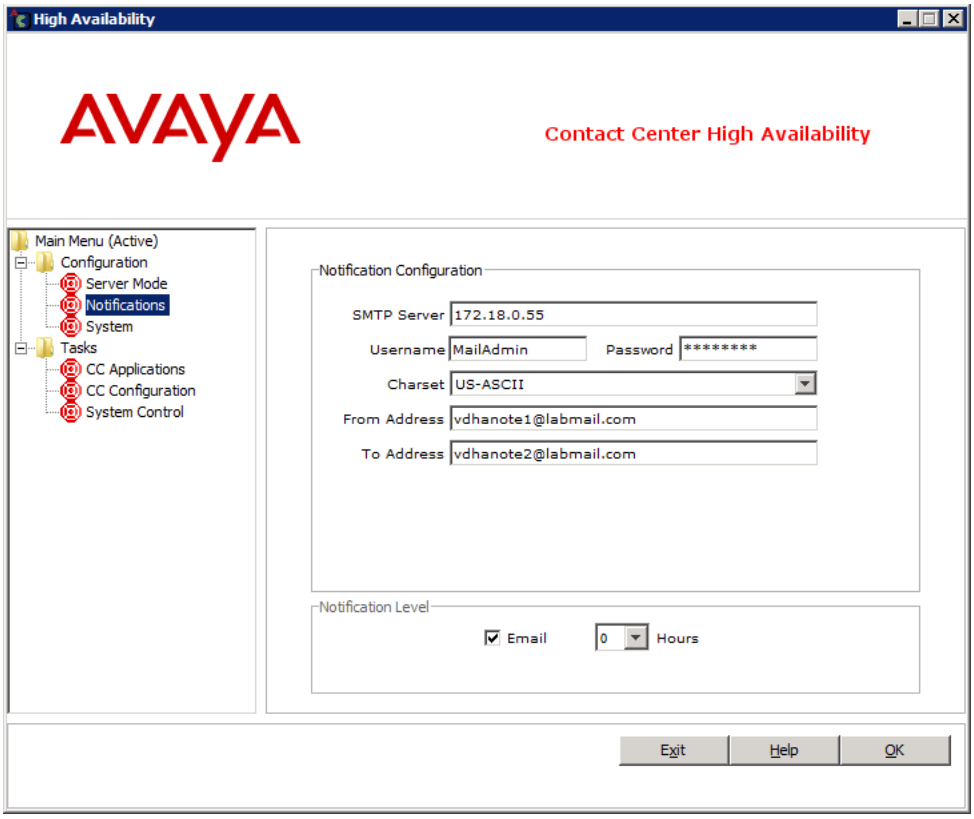
5 Type the **SMTP Server** name or IP address, for example **172.18.0.55**.

6 Type the **Username** of a mailbox where you want to see the HA alerts, for example, **MailAdmin**.

7 Type the **Password**, for example, **MApass~1**.

8 Type the **From Address** e-mail address. For example **vdhanote1@labmail.com**.

9 Type the **To Address** e-mail address.For example **vdhanote2@labmail.com**.



10 Click **OK** to save the data.

--End--

Configuring service monitoring on the Active Server

The High Availability feature monitors a number of critical services on the Active Server. If these critical services stop or fail, they automatically restart in the correct order. If a critical service fails a defined number of times, the Active Server may, if switchover is enabled, shut down and hand over processing to the Standby Server.

Critical services are listed, monitored, restarted, and controlled using the Contact Center Configuration tab on the Tasks tab of the High Availability utility. The Contact Center Configuration tab lists the critical CCMS services and all of the CCT services on the co-resident CCMS and CCT server.

There is no requirement to change the data in this table, the default values are suitable for most solutions.

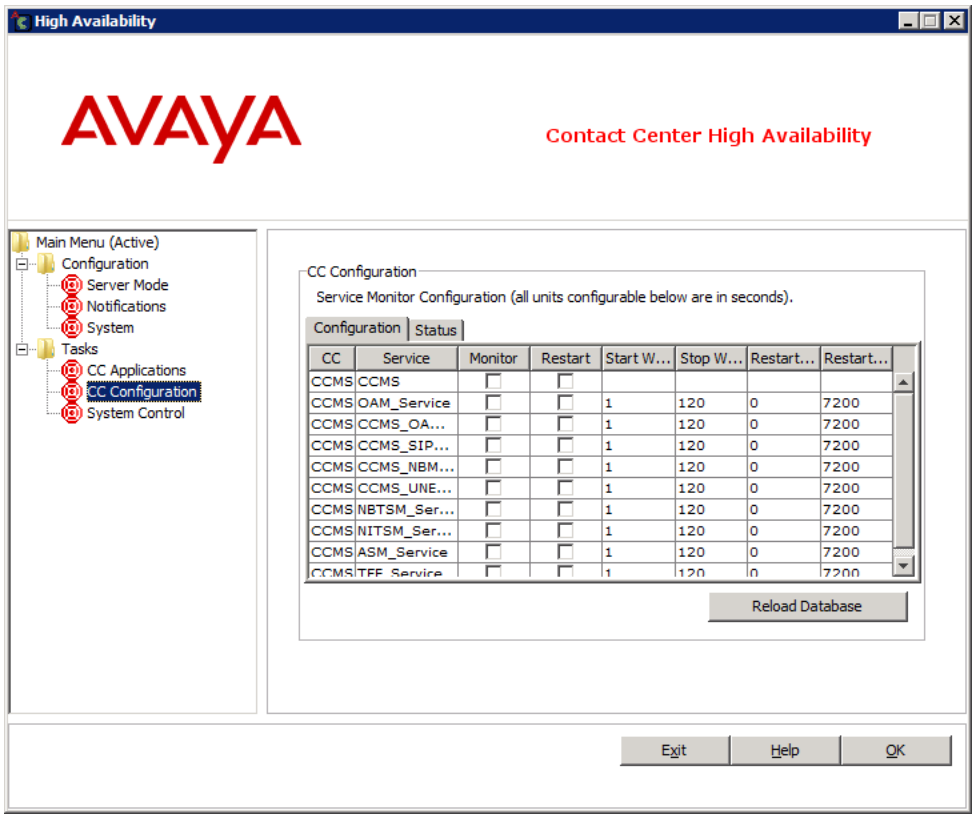
If the services are selected for Monitor and Restart and one or more services fail, either the same or more number of times as the Restart Limit value, then a switchover to the Standby Server occurs.

For switchover to occur, both the Active and the Standby servers must have their respective switchover check box selected, a valid license file, and shadowing must be running. If the switchover is not enabled, then all internal monitoring counters are reset and the monitoring restarts.

The Restart Threshold is the time period within which the services are monitored and the counters are increased when services fail. When this threshold is met, the counters are reset to zero, monitoring restarts, and the restart threshold timer resets.

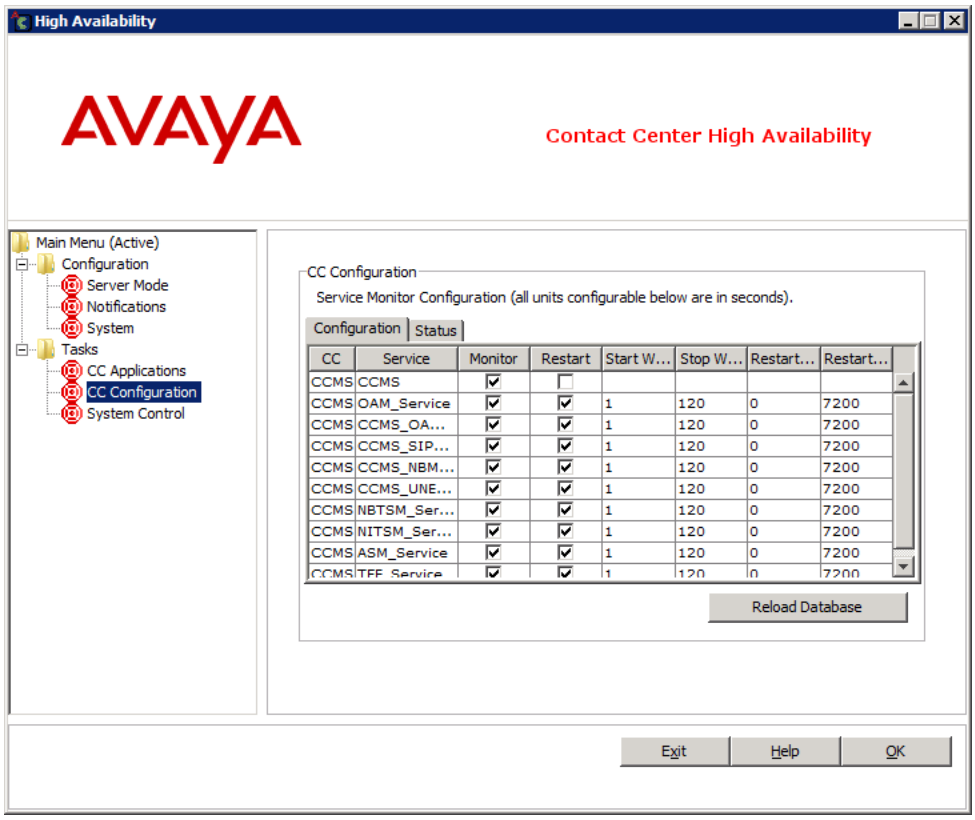
Procedure steps

Step	Action
1	In the **High Availability** window, in the left pane, expand the **Tasks** folder.
2	Double-click **CC Configuration**.



3 For the CCMS row, select the **Monitor** checkbox.

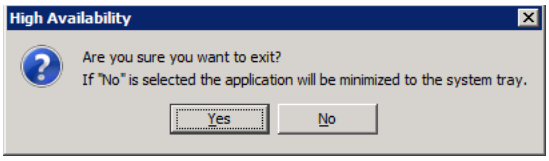
Contact Center automatically selects all the services.



4 Leave the defaults in the **Start Wait Time**, **Stop Wait Time**, **Restart Limit**, and **Restart Threshold** columns.

5 Click **OK**.

6 Click **Yes** on any **Save Data** confirmation dialog boxes that appear.



--End--

Procedure job aid

For this configuration, the example is using the defaults. This job aid provides an example of customizing a service monitor configuration in the High Availability Utility.

The required business rule is when the CCMS OAM service has stopped 3 times for longer than 60 seconds in a period of 12 hours, initiate an automatic switchover. This requirement is achieved by setting the OAM service configuration values to the following settings:

CC	CCMS
Service	OAM_Service
Monitor	Selected
Restart	Selected
Start Wait Timer	60 Seconds
Restart Limit	3
Restart Threshold	43200 Seconds (12 hours)

Backing up the Contact Center Manager Administration component on the Active server

Back up Contact Center Manager Administration to a folder to create a snapshot of the preselected CCMA data files.

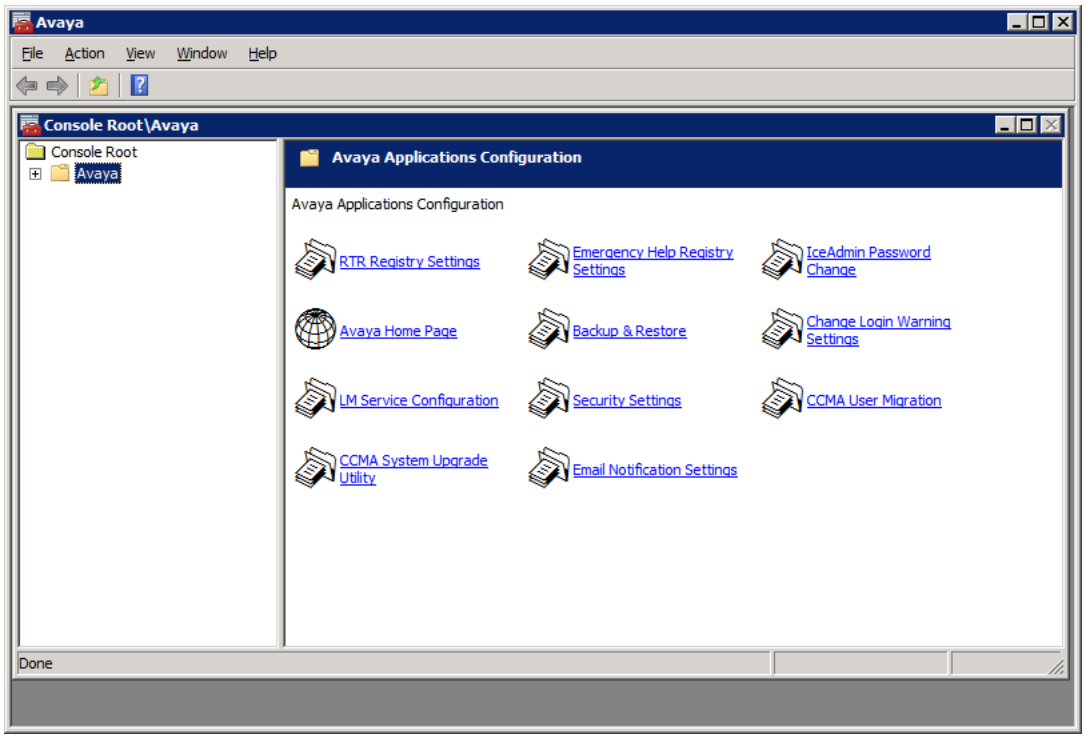
You use this utility to back up the files located in the following folders (where D: is the drive on which you installed CCMA):

- 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\

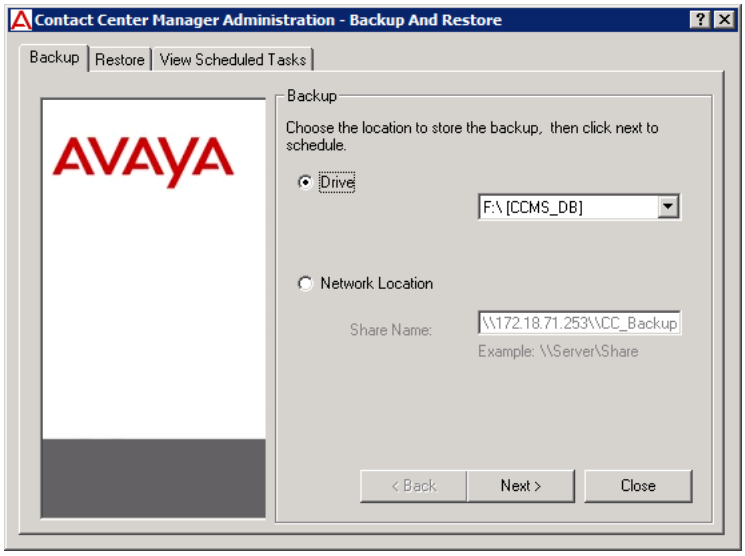
Attention: If the primary CCMA server has a failure that requires a complete rebuild of the server, you must use a backup created from the primary server to rebuild the CCMA database, because the database contains the schema and settings of a primary server. You cannot use a backup from a secondary CCMA server to rebuild a primary CCMA server. Ensure you permanently keep a backup of the primary CCMA server to allow for this situation.

Procedure steps

Step	Action
1	Log on to the Active server using the Avaya Aura® CC installer domain account, for example AACCinstaller.
2	Choose **Start, All Programs, Avaya, Contact Center, Manager Administration, Configuration**.

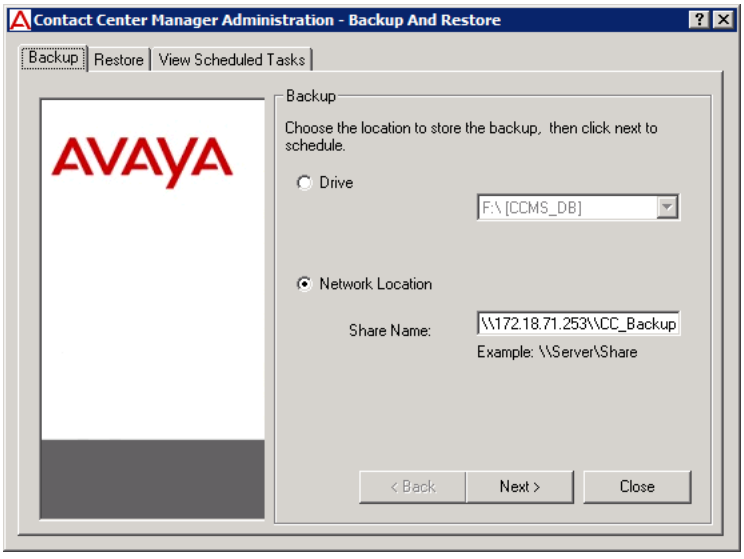


3	In the right-hand pane, click **Backup & Restore**.
4	In the **Contact Center Manager Administration - Backup and Restore** utility, select the **Backup** tab.

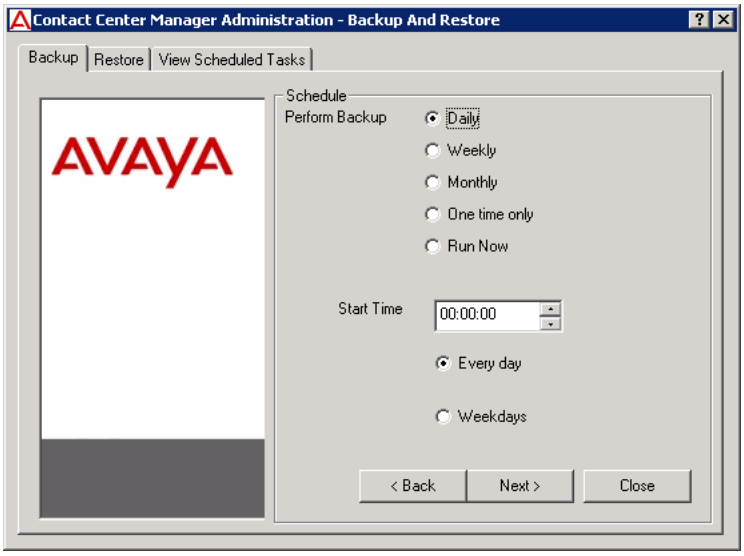


5 In the **Backup** window, select **Network Location**.

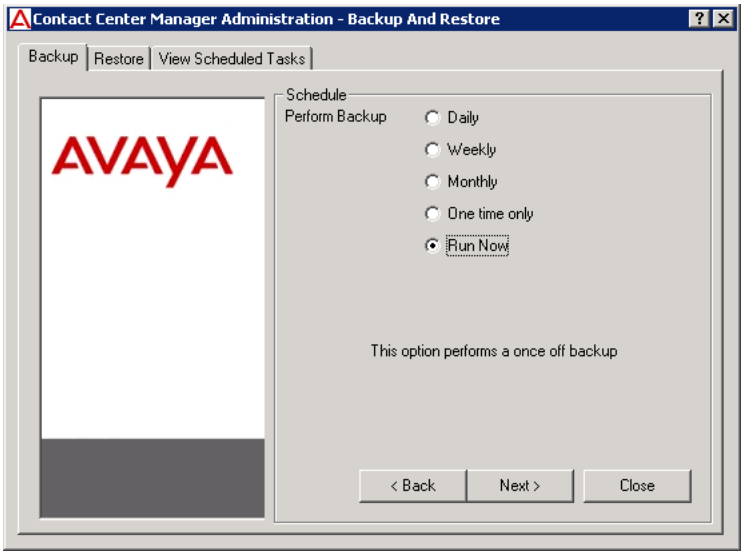
6 In the **Share Name** box, specify the Network Location where you want to store the backup, for example **\\172.18.71.253\CC_Backup**.



7 Click **Next**.



8 On the **Schedule** page, select **Run Now**.

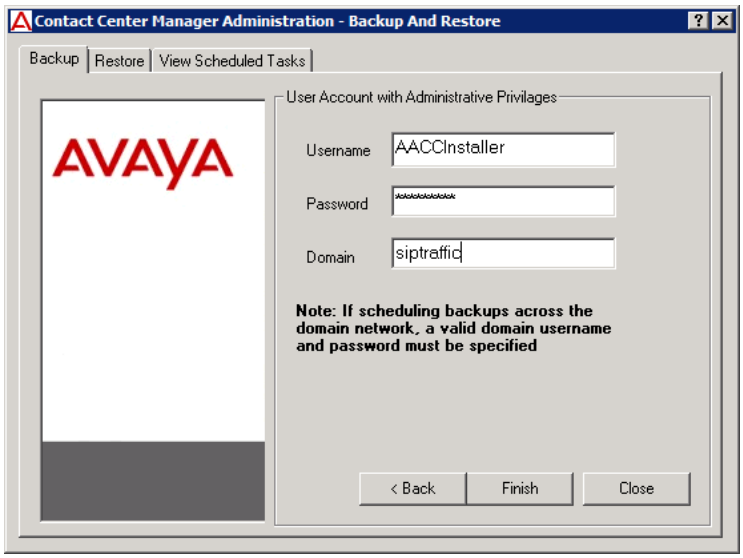


9 Click **Next**.

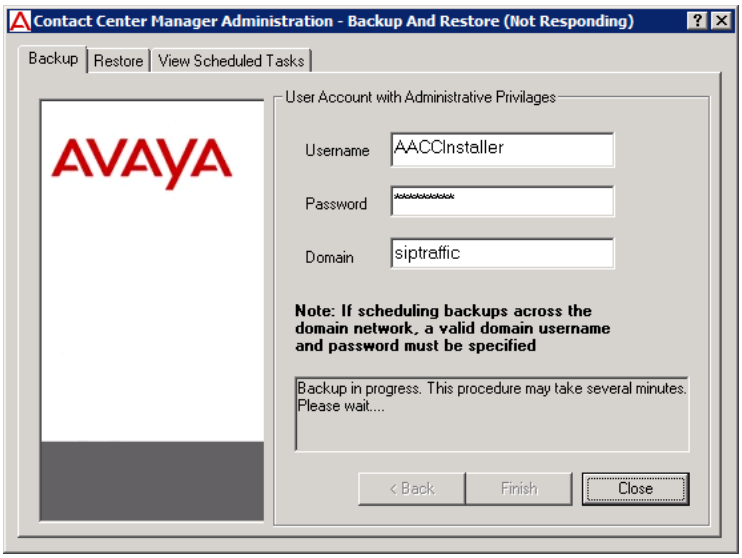
10 In the **Username** box on the **User Account with Administrative Privileges** page, type a valid administrator user name for the server on which you want to store the backup, for example **SIPTRAFFIC\AACCinstaller**.

11 In the **Password** box, type a the password for the specified administrator user, for example **AACCInstPass1**.

12 In the **Domain** field, type the domain on which you created the network backup location, for example **siptraffic**.



13 Click **Finish**.



14 When the backup completes, click **Close**.

All backups are saved as files in the format CCMAFilesBackup<BackupDateTime>.package.

--End--

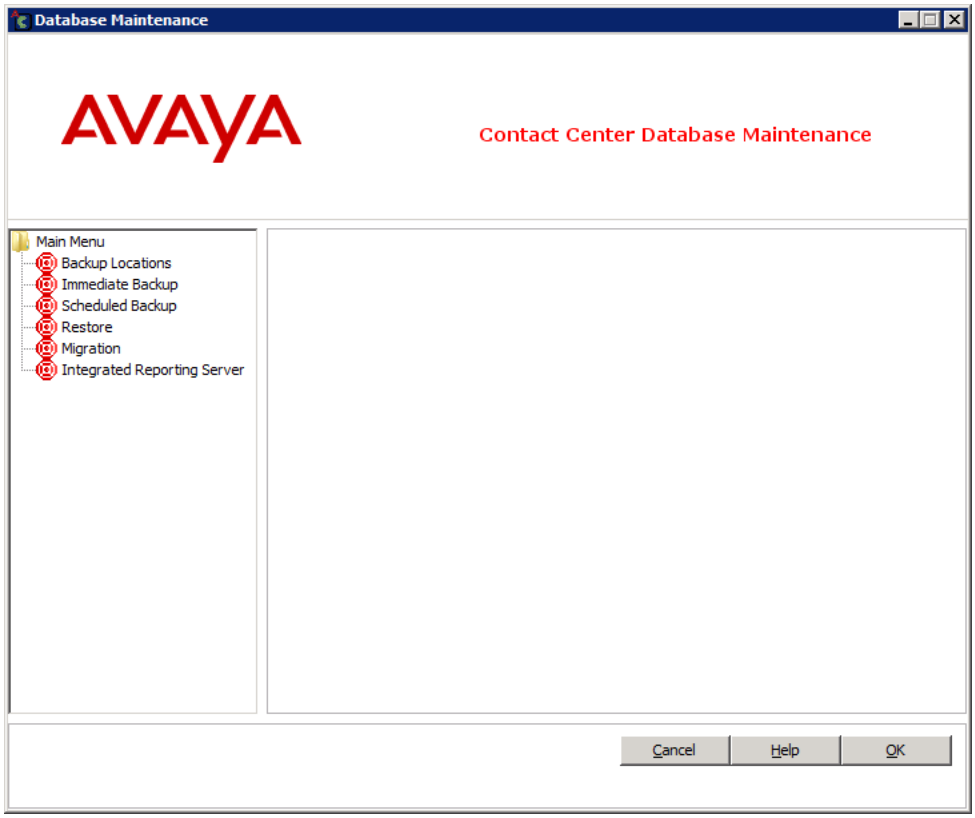
Backing up the Contact Center databases on the Active Server

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 databases, which you can restore to the Standby Server. On the active Contact Center server you must back up all databases.

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 using the Avaya Aura® CC installer domain account, for example AACCinstaller.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Database Utilities**, **Database Maintenance**.



3 Click **Backup Locations**.

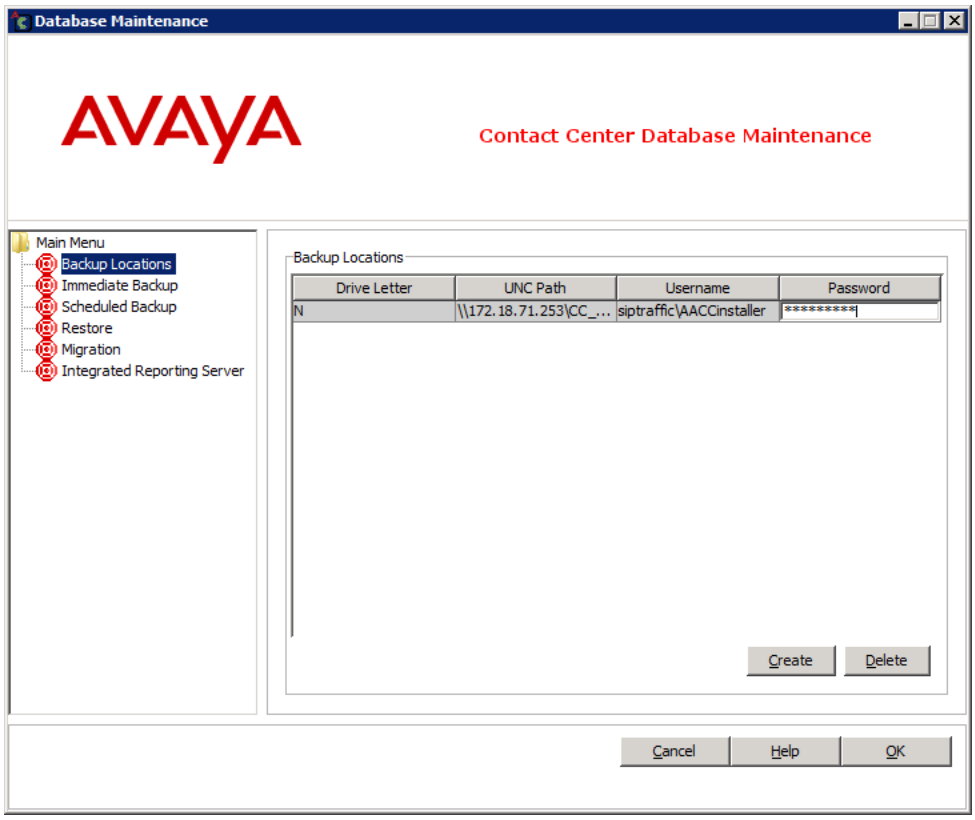
4 Click **Create**.

5 From the **Drive Letter** list, select the network drive on which you want to store the CCMS, CCT, and ADMIN databases, for example **N**.

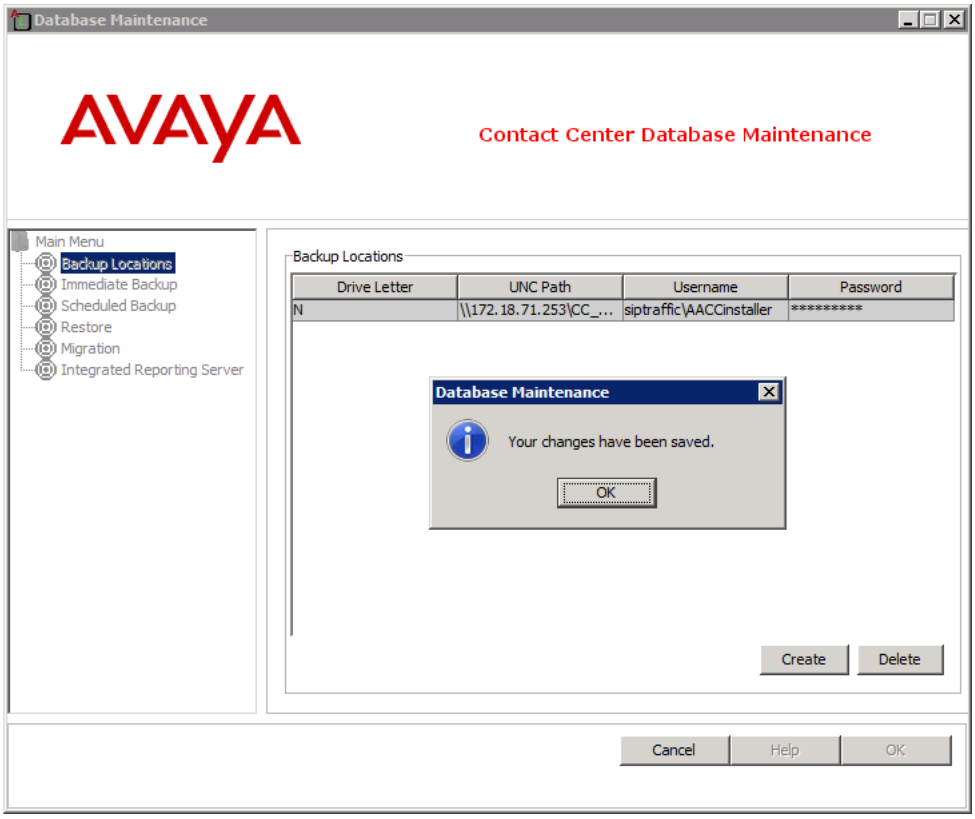
6 In the **UNC Path** box, type the network location on which to store the backup, in the format \\Computer Name\Backup Folder, for example **172.18.71.253\CC_Backup**.

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\AACCinstaller**.

8 In the **Password** box, type the password of the UNC backup location, for example **AACCInstPass1**.


Database Maintenance
AVAYA
Contact Center Database Maintenance
Main Menu
Backup Locations
Immediate Backup
Scheduled Backup
Restore
Migration
Integrated Reporting Server
Backup Locations
Drive Letter
UNC Path
Username
Password
N
\\172.18.71.253\CC_...
siptraffic\AACCinstaller
Create
Delete
Cancel
Help
OK

9 Click **OK**.



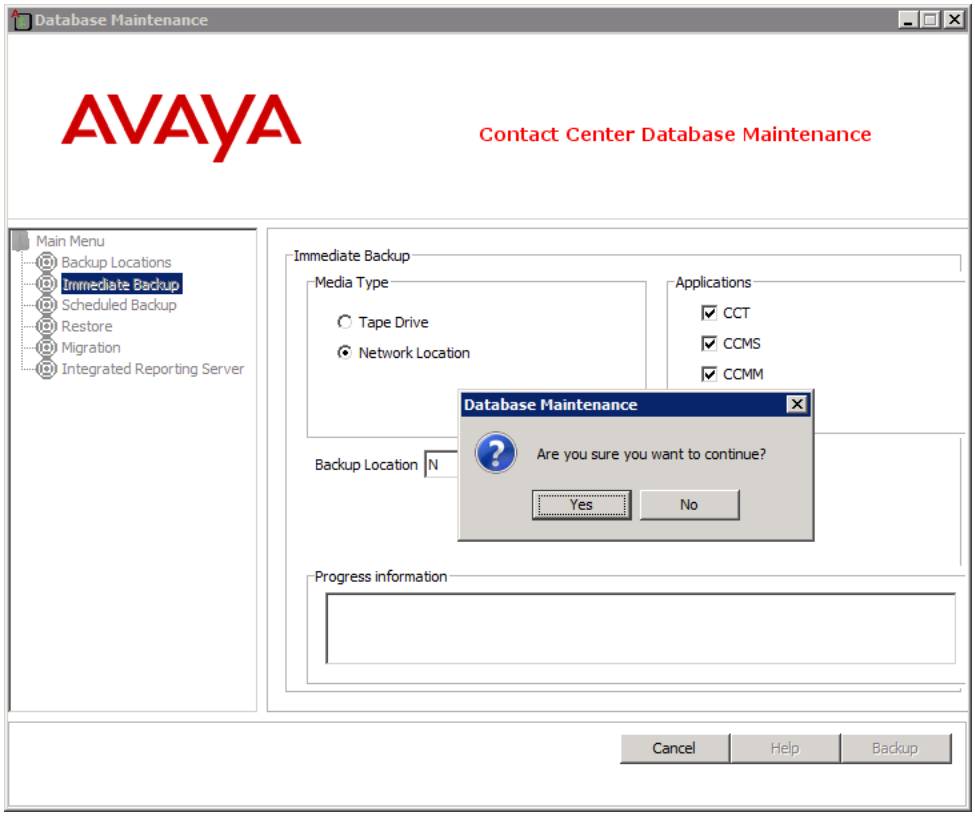
10 In the left pane, click **Immediate Backup**.

11 In the **Media Type** section, select **Network Location**.

12 In the **Applications** section, select **CCMS**, **CCT**, **CCMM,** and **ADMIN**.

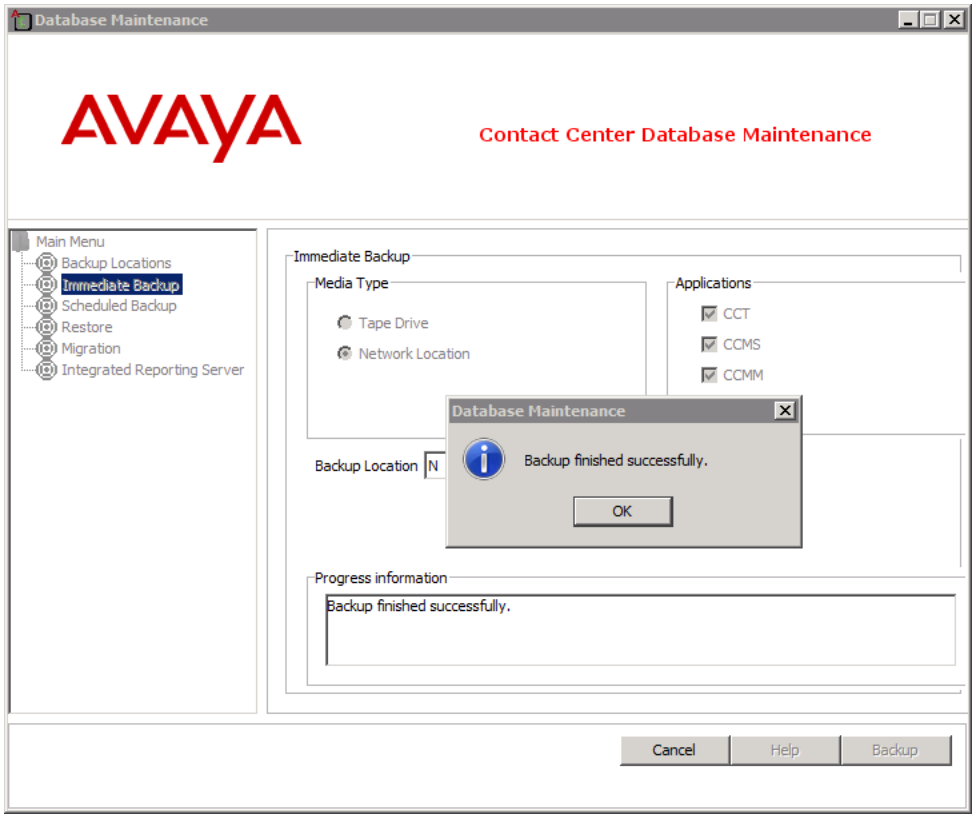
13 From the **Backup Location** list, select the network drive on which to store the backup, for example **N**.

14 Click **Backup**.



15 Click **Yes** to continue with the backup.

16 The database backup completes.



17 Click **OK**.

18 Exit the Database Maintenance utility.

--End--

Restoring the Contact Center databases 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 CCMS, CCT, CCMM, and ADMIN databases.

You must restore the CCMS, CCT, CCMM, and ADMIN databases onto the Standby Server. You must restore the ADMIN database last.

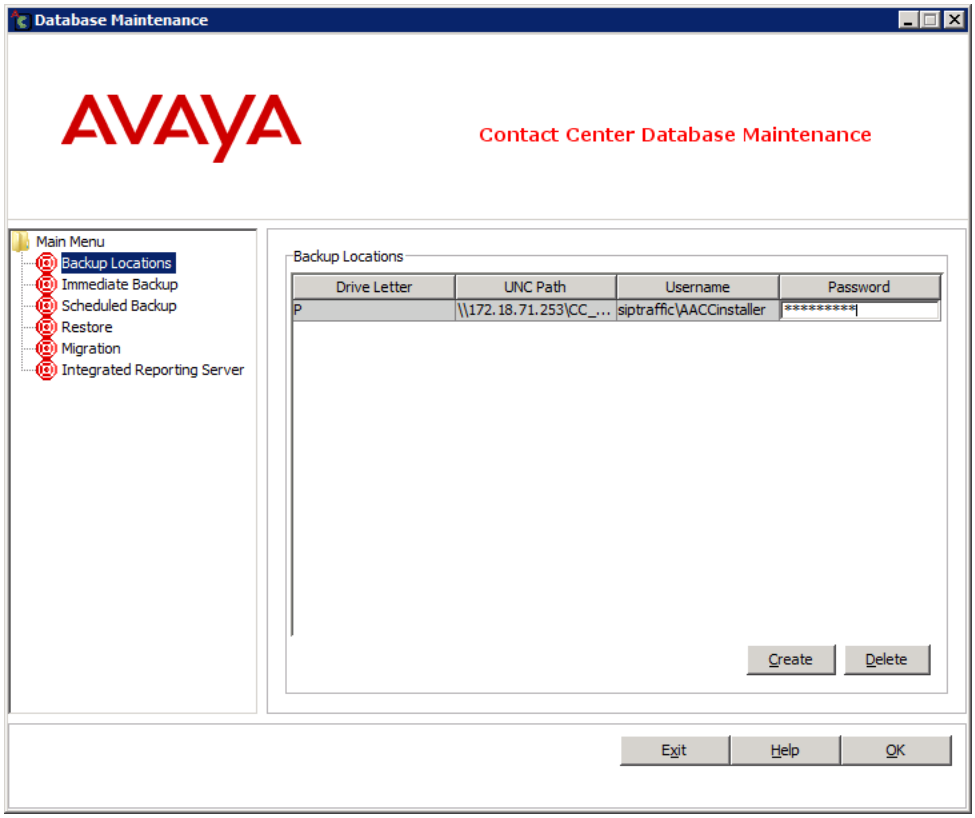
Attention: You must backup the Active server database, restore it onto the Standby server, and enable shadowing within 24 hours. If the difference in time between the Active and Standby server database content is greater than 24 hours then database shadowing does not work.

Attention: You must restore all databases to the Contact Center server. Restoring only CCMS, and not CCT, CCMM, or ADMIN, may leave an inconsistent server database and prevent HA from shadowing data correctly.

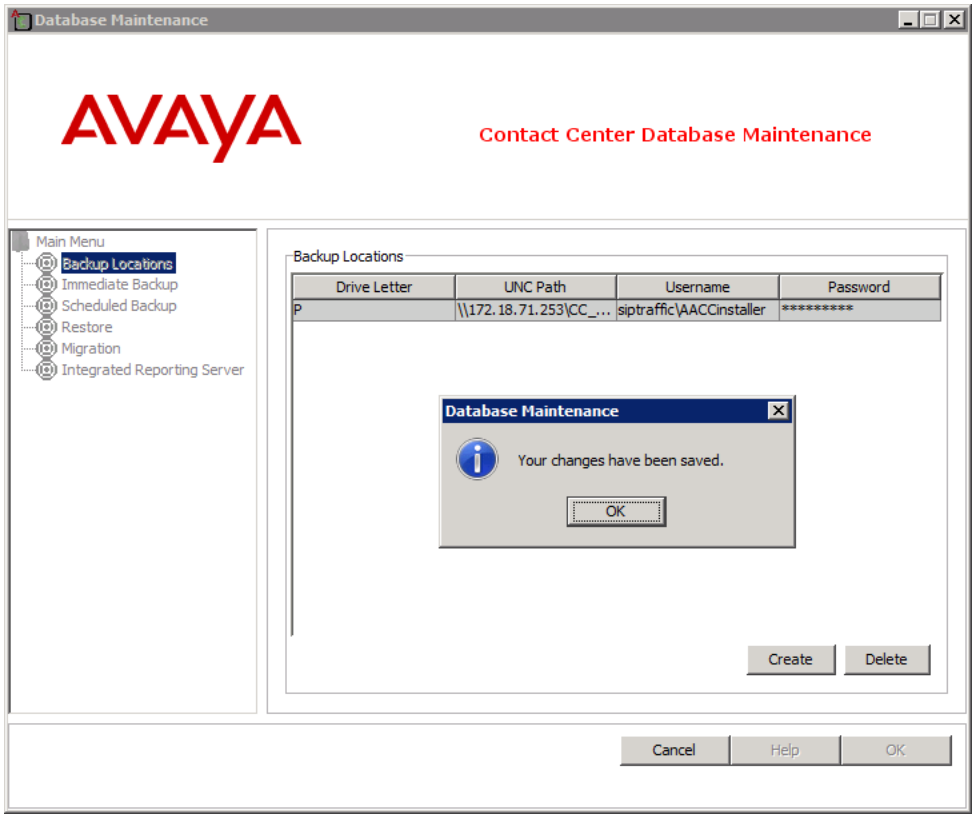
Attention: Restoring the Administration (ADMIN) database can change configuration of Backup locations on the Standby Server if the Active Server and Standby Server backup locations are different. Therefore, after you restore the ADMIN database, close and reopen the Database and Maintenance utility.

Procedure steps

Step	Action
1	Log on to the Standby server (for example, **CCCORESTWO**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Database Utilities**, **Database Maintenance**.
3	Click **Backup Locations**.
4	Click **Create**.
5	From the **Drive Letter** list, select the a network drive letter to use to restore the CCMS, CCT, CCMM, and ADMIN databases, for example **P**.
6	In the **UNC Path** box, type the location from which to restore the backup, in the format \\Computer Name\Backup Location, for example **\\172.18.71.253\CC_Backup**.
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\AACCinstaller**.
8	In the **Password** box, type the password of the UNC backup location, for example **AACCInstPass1**.


Database Maintenance
AVAYA
Contact Center Database Maintenance
Main Menu
Backup Locations
Immediate Backup
Scheduled Backup
Restore
Migration
Integrated Reporting Server
Backup Locations
Drive Letter
UNC Path
Username
Password
P
\\172.18.71.253\CC_...
siptraffic\AACCinstaller
Create
Delete
Exit
Help
OK

9 Click **OK**.



10 In the **Database Maintenance** dialog box, in the left pane, click **Restore**.

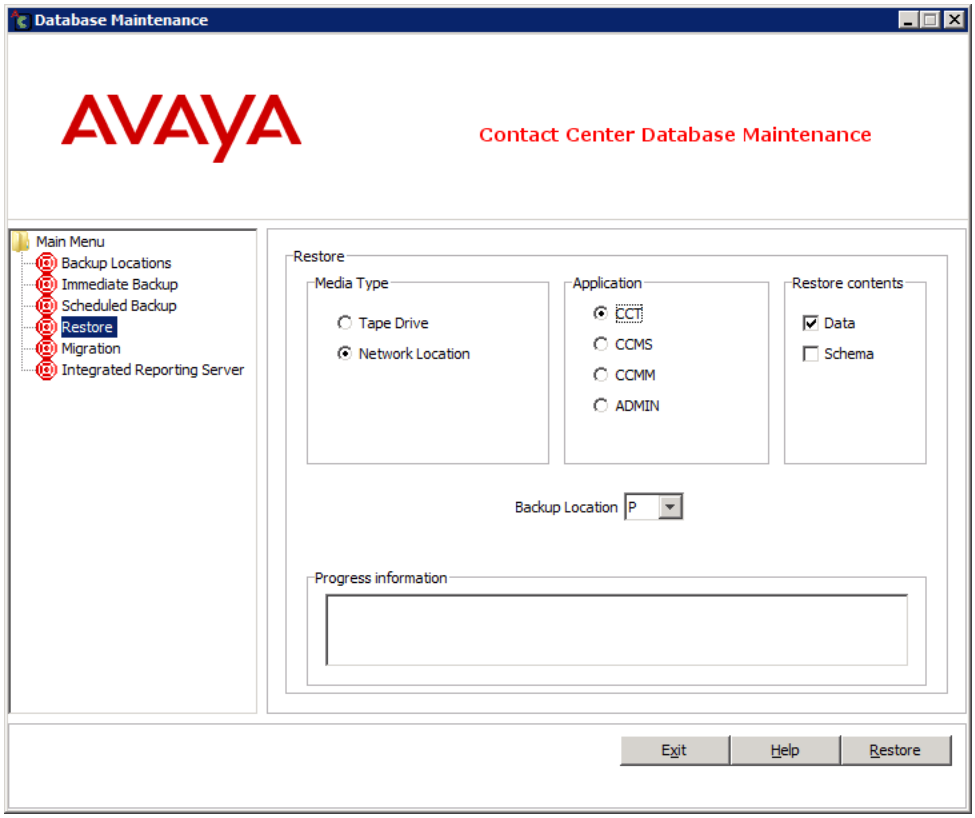
11 In the right pane, under **Media Type**, select the media type from which to restore the backup, for example **Network Location**.

12 From the **Backup Location** list, select the drive you created on the **Backup Locations** tab, for example **P**.

13 Under **Application**, select **CCT**.

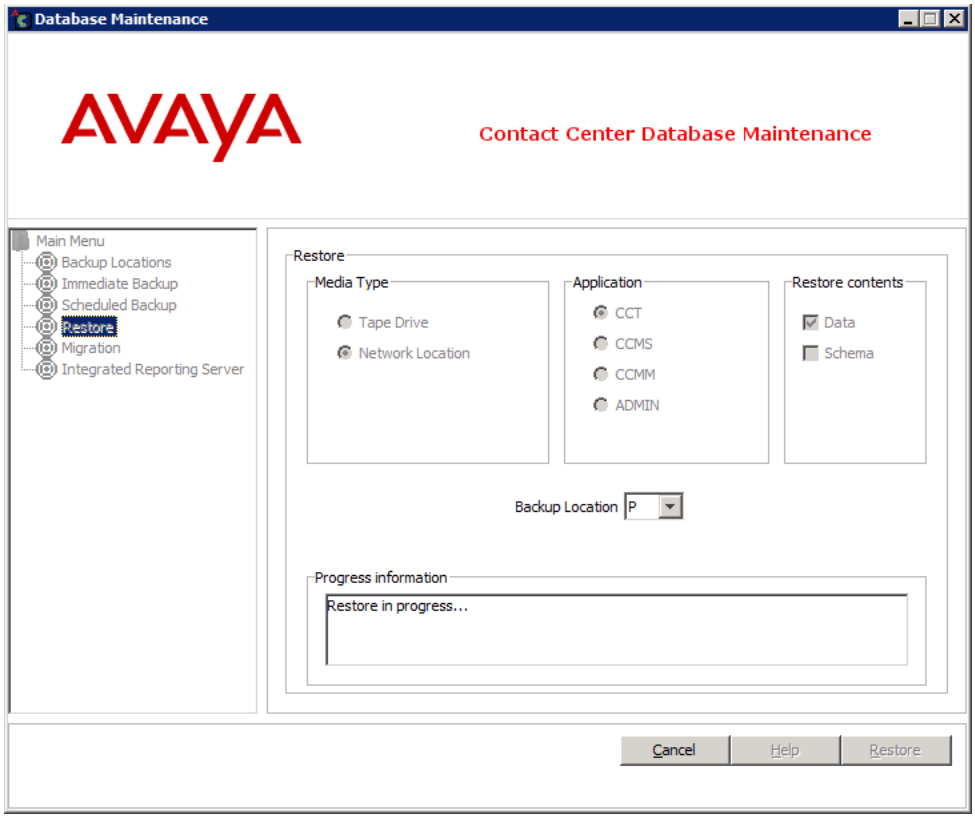
14 Under **Restore contents**, select **Data**.

15 Click **Restore**.



16 On the **Restore Database** dialog, click **Yes**.

17 Use the **Progress information** field to monitor the progress of the restoration.



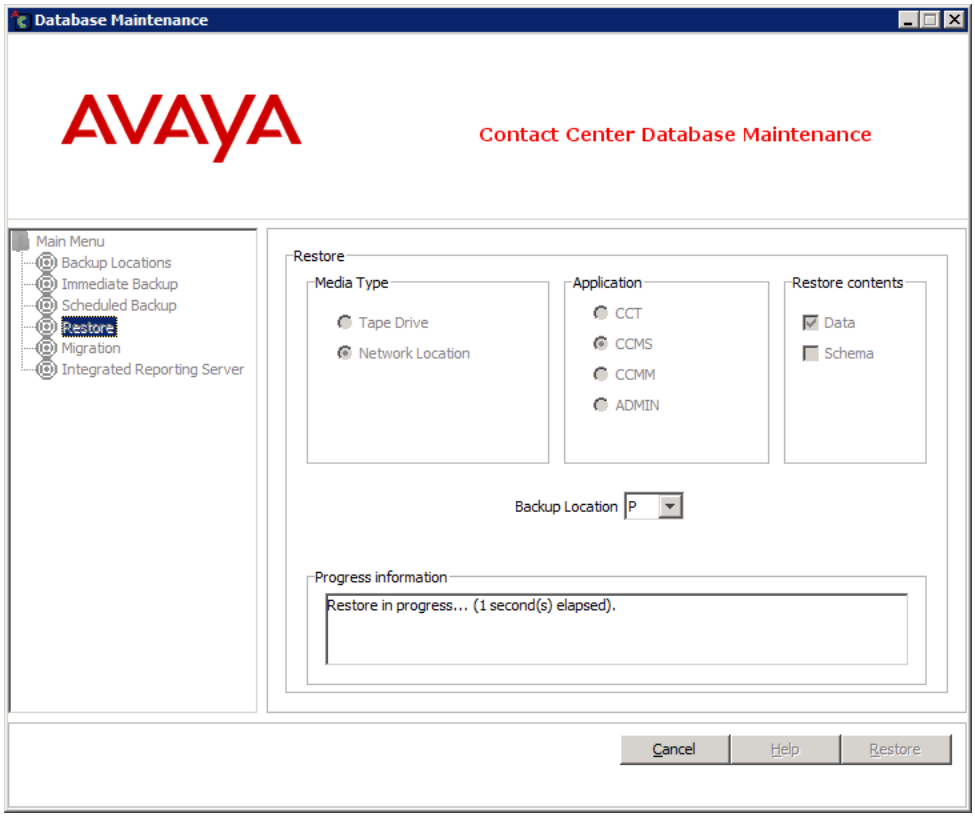
18 On the **Database Maintenance** dialog, click **OK**.

19 Under **Application**, select CCMS.

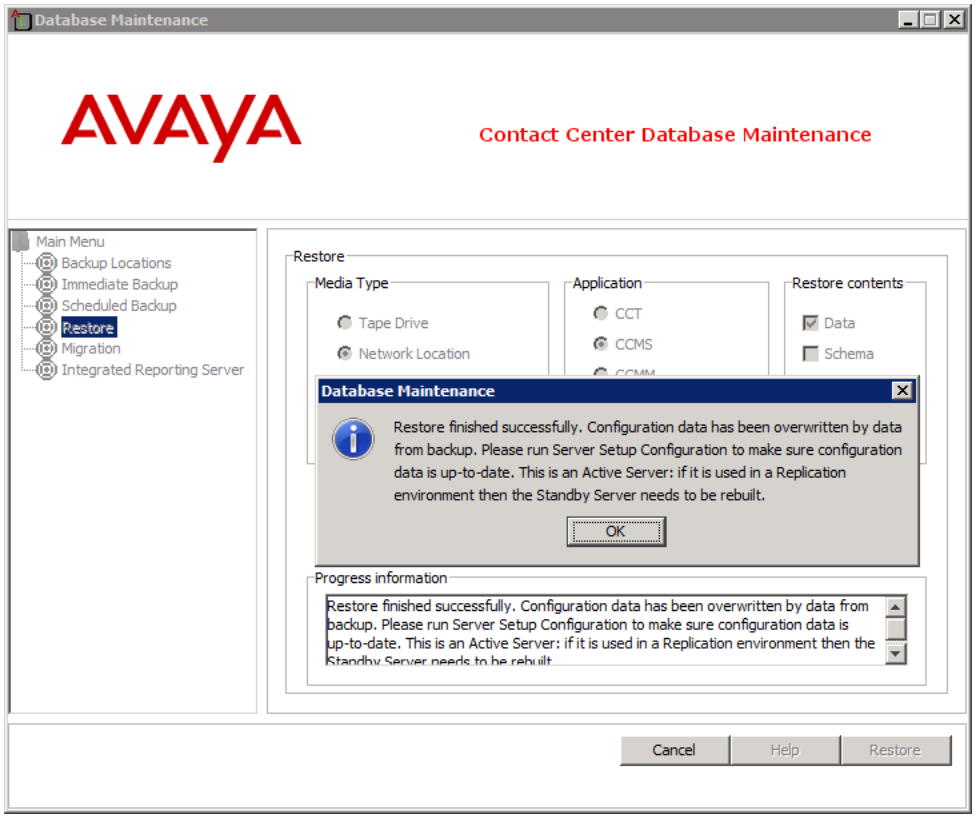
20 Click **Restore**.

21 On the **Restore Database** dialog, click **Yes**.

22 Use the **Progress information** field to monitor the progress of the restoration.



23 On the **Database Maintenance** dialog, click **OK**.

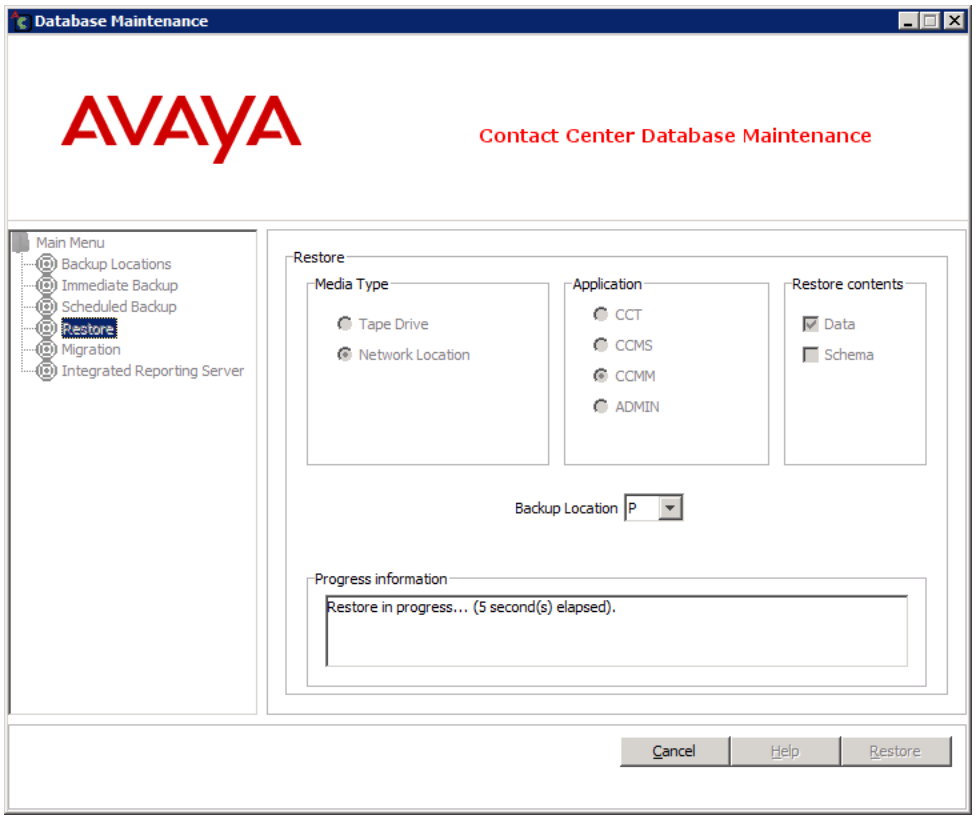


24 Under **Application**, select **CCMM**.

25 Click **Restore**.

26 On the **Database Maintenance** dialog, click **Yes**.

27 Use the **Progress information** field to monitor the progress of the restoration.



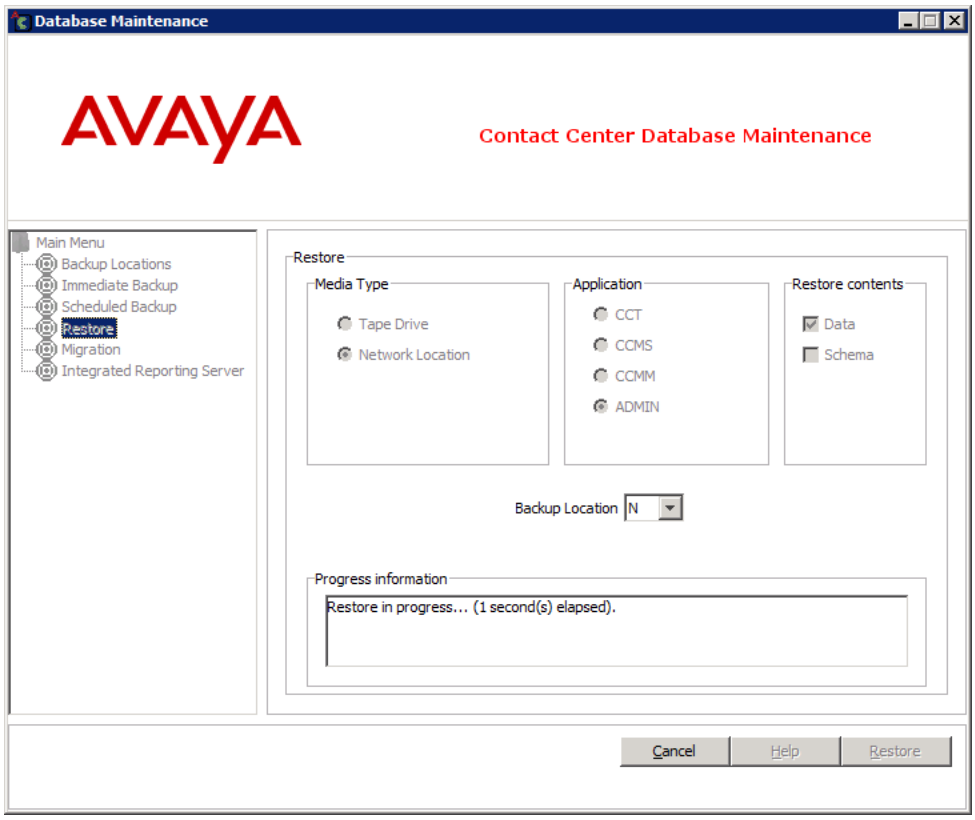
28 On the **Database Maintenance** dialog, click **OK**.

29 Under **Application**, select **ADMIN**.

30 Click **Restore**.

31 On the **Restore Database** dialog, click **Yes**.

32 Use the **Progress information** field to monitor the progress of the restoration.



33 Click **Exit** to close the Database Maintenance utility.

34 Click **Yes**.

--End--

Creating a drive mapping to the network backup location from the Standby server

The CCMA Restore utility is easier to use if you create a mapping to the network location where you created the Active server CCMA backup. Follow this procedure to create a network drive on the Standby server.

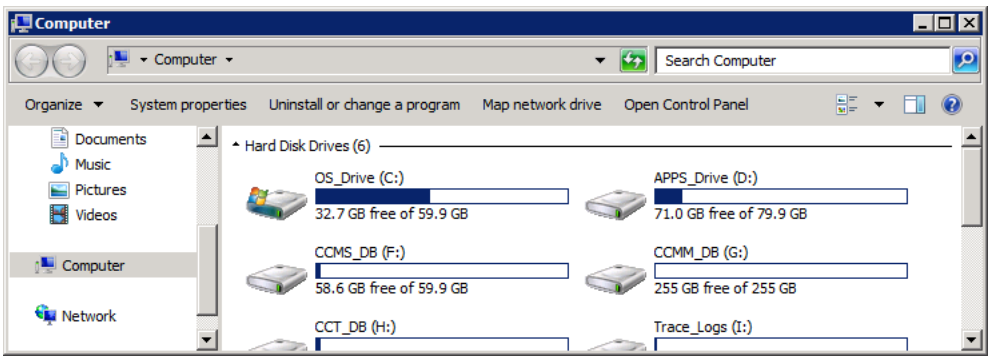
Prerequisites

Procedure steps

Step	Action

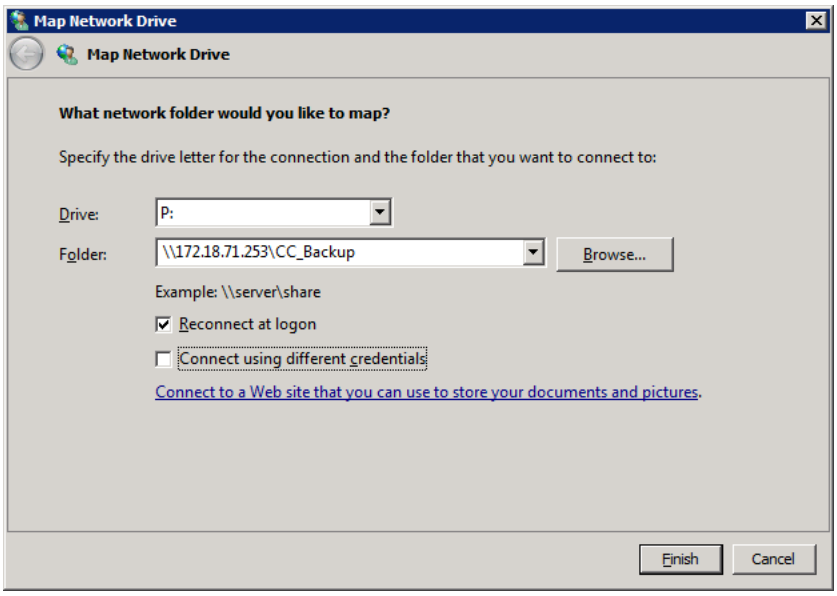
1 On the Standby server, choose **Start**, **Computer**.

2 On the **Computer** window, click **Map network drive**.



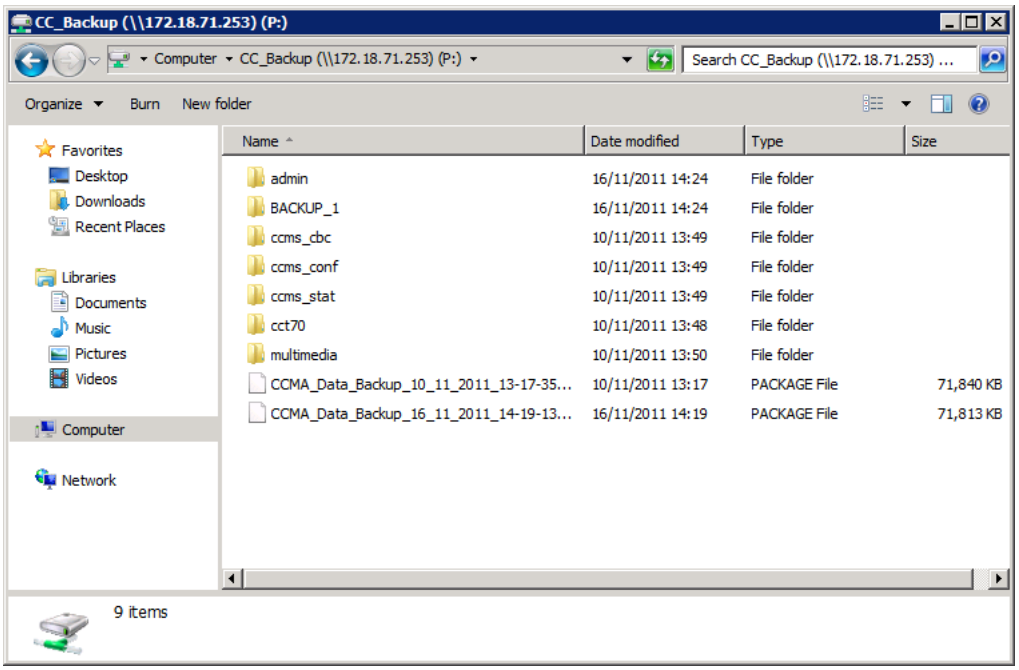
3 On the **Map Network Drive** dialog, from the **Drive** list, select a letter for the drive, for example **P:**.

4 In the **Folder** box, type the location to which you want to map the drive letter, in the format \\<Computer IP address>\<Backup Folder>, for example **\\172.18.71.253\CC_Backup**.

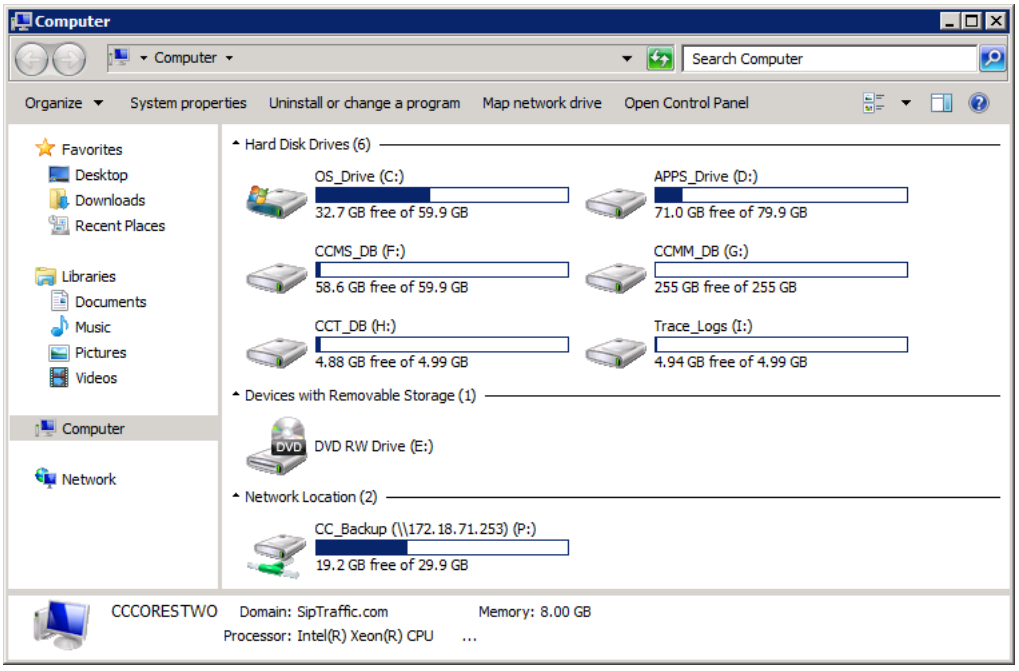


5 Click **Finish**.

Windows opens the specified network location in a new window.



6 Close the drive window. You can see the new drive in the **Computer** window.



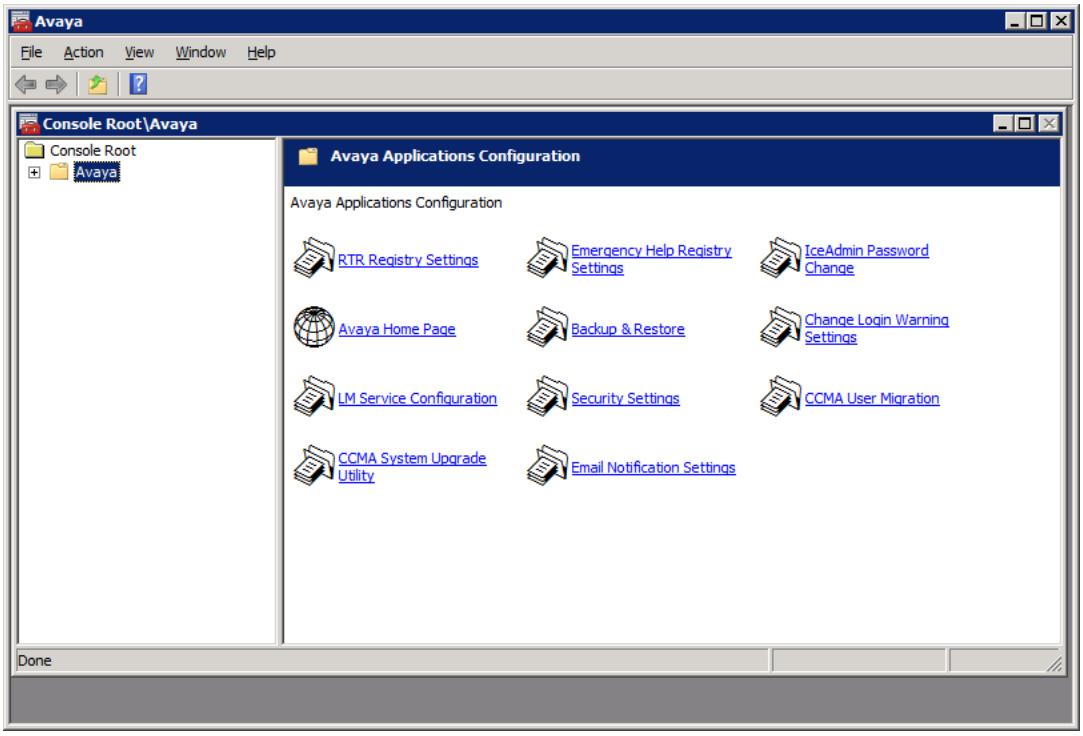
--End--

Restoring CCMA data to the Standby server

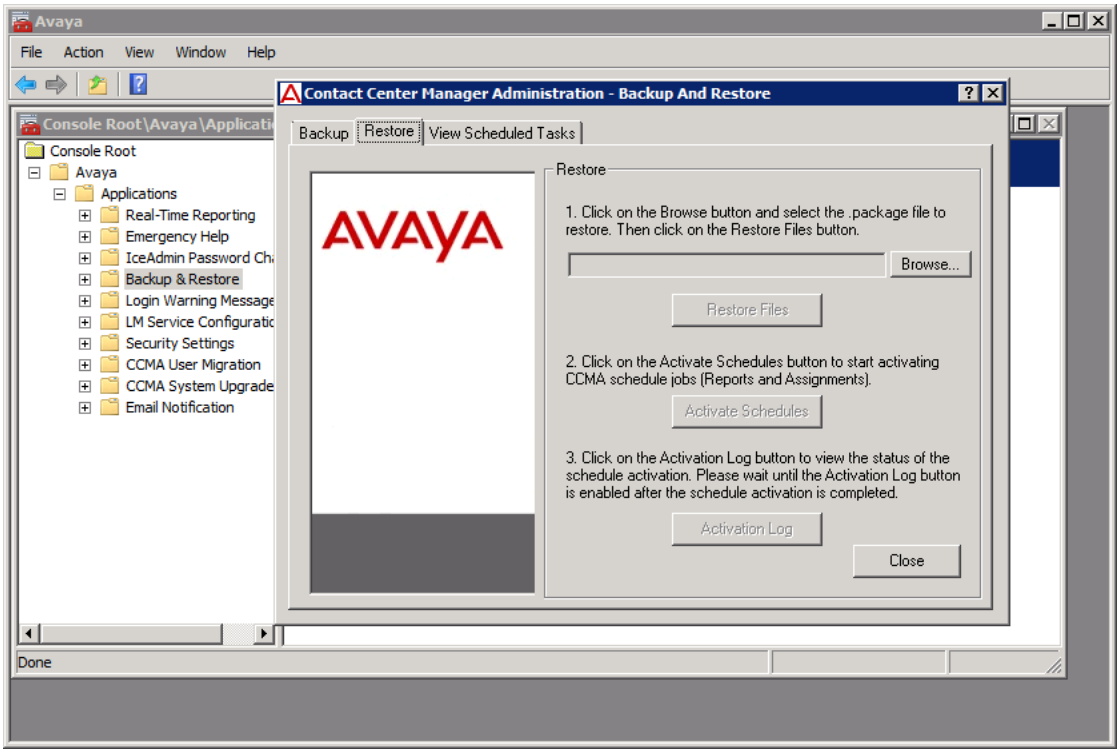
Restore the Contact Center Manager Administration data to the Standby server.

Procedure steps

Step	Action
1	On the Standby server, choose **Start**, **All Programs**, **Avaya, Contact Center**, **Manager Administration**, **Configuration**.



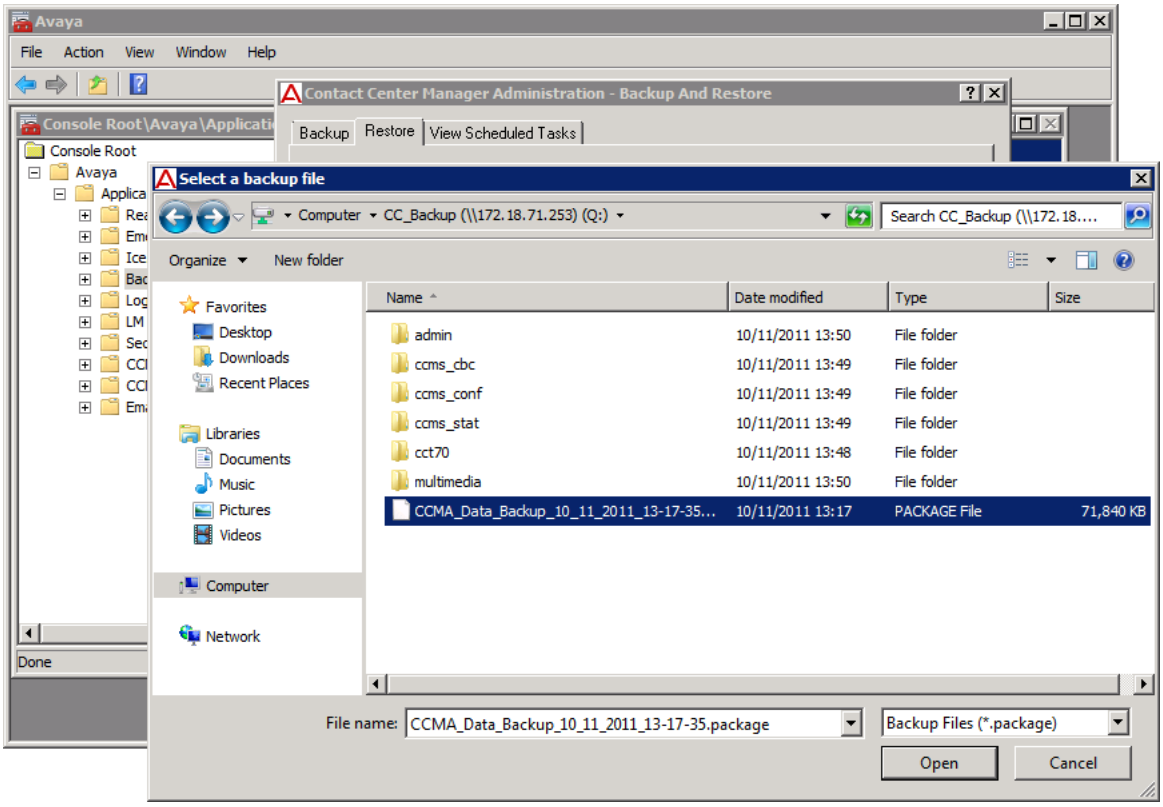
2	In the left pane of the **Avaya Configuration** window, expand **Avaya, Applications, Backup & Restore**.
3	In the right pane, click **Backup & Restore**.
4	In the **Contact Center Manager Administration - Backup And Restore** dialog box, click the **Restore** tab.



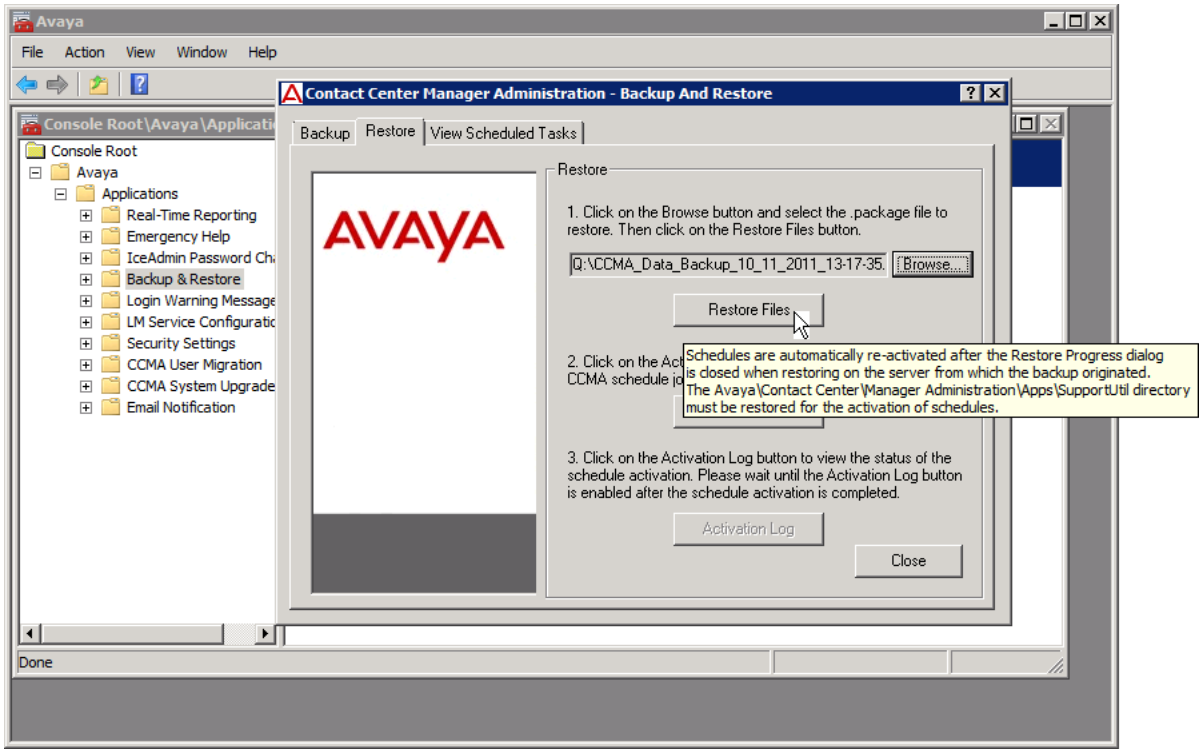
5 To select a backup file to restore from, click **Browse**.

6 In the **Select a backup file** dialog box, browse to the location where you backed up the CCMA data, and select the .package file.

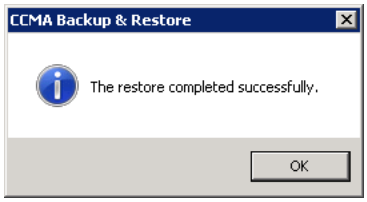
7 Click **Open**.



8 Click **Restore Files**.



When the restore is finished, a ***CCMA Backup & Restore*** *message box appears.*



9 On the **CCMA Backup & Restore** message box, click **OK**.

10 Click **Close**.

--End--

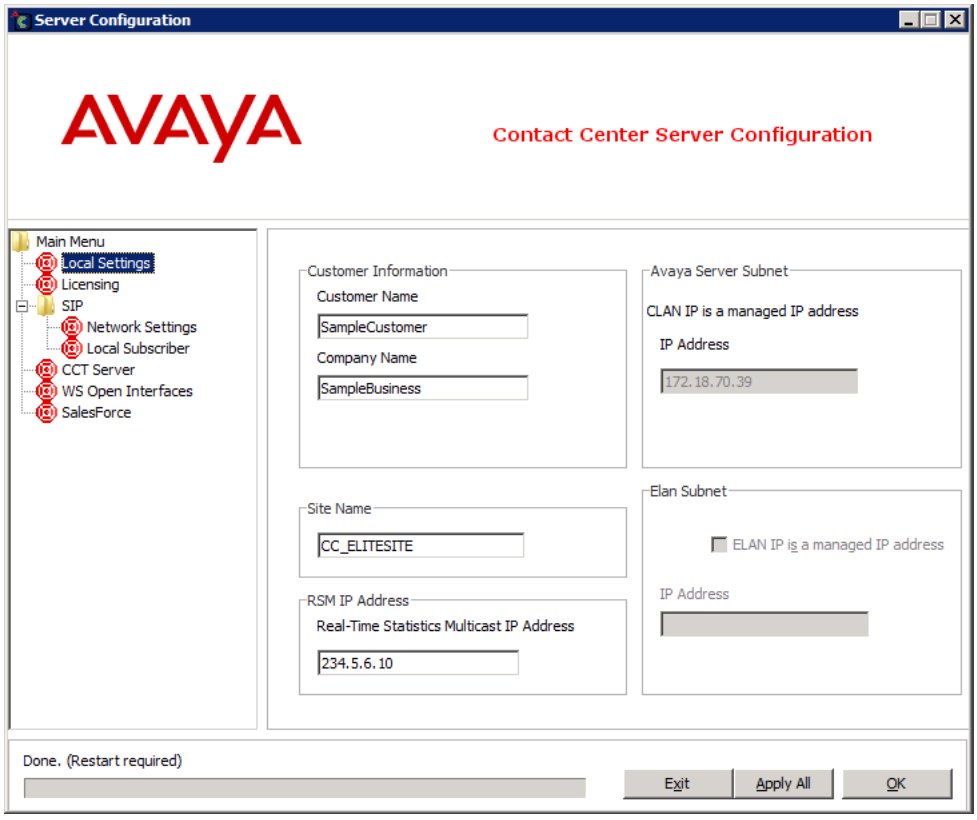
Verifying the server details and restarting the Standby Server

After you restore the Active Server database onto the Standby Server, the Standby Server database contains the same agent and statistical data as the Active Server. Verify that the Standby Server configuration details are correct.

Attention: This procedure forces a server restart.

Procedure steps

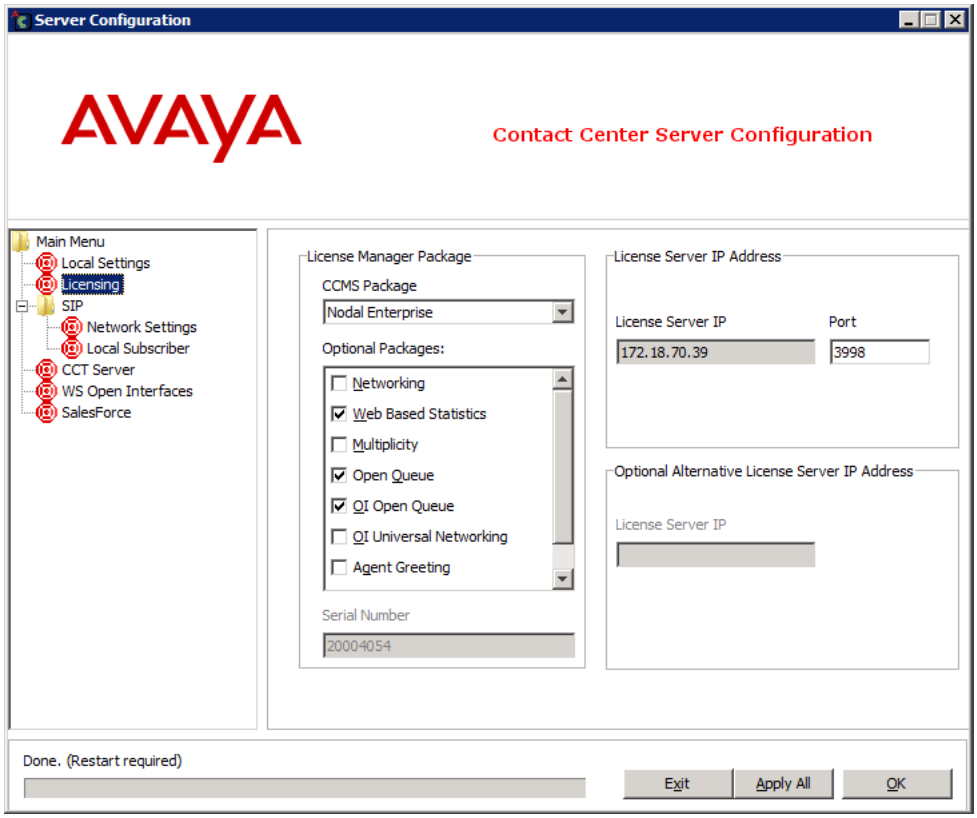
Step	Action
1	On the Standby server, click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Manager Server**, **Server Configuration**.
2	In the **Server Configuration** dialog box, click the **Local Settings** tab.
3	Under **Avaya Server Subnet** verify that the **IP Address** box contains the managed IP address, for example **172.18.70.39**.
4	Verify that the **Site Name** box contains the correct site name, for example **CC_ELITESITE**.



5	In the **Server Configuration** dialog box, click the **Licensing** tab.

6 On the **Updated IP Warning** message box, click **OK**

7 Verify that the Standby Server licensing details match the Active server licensing details.



8 Click **Apply All**.

9 On the **Updated IP Warning** message box, click **OK**

10 On the **Restart Required** message box, click **Yes**.

11 On the **HA System** message box, click **OK**.

Contact Center forces a shutdown of the Windows server.

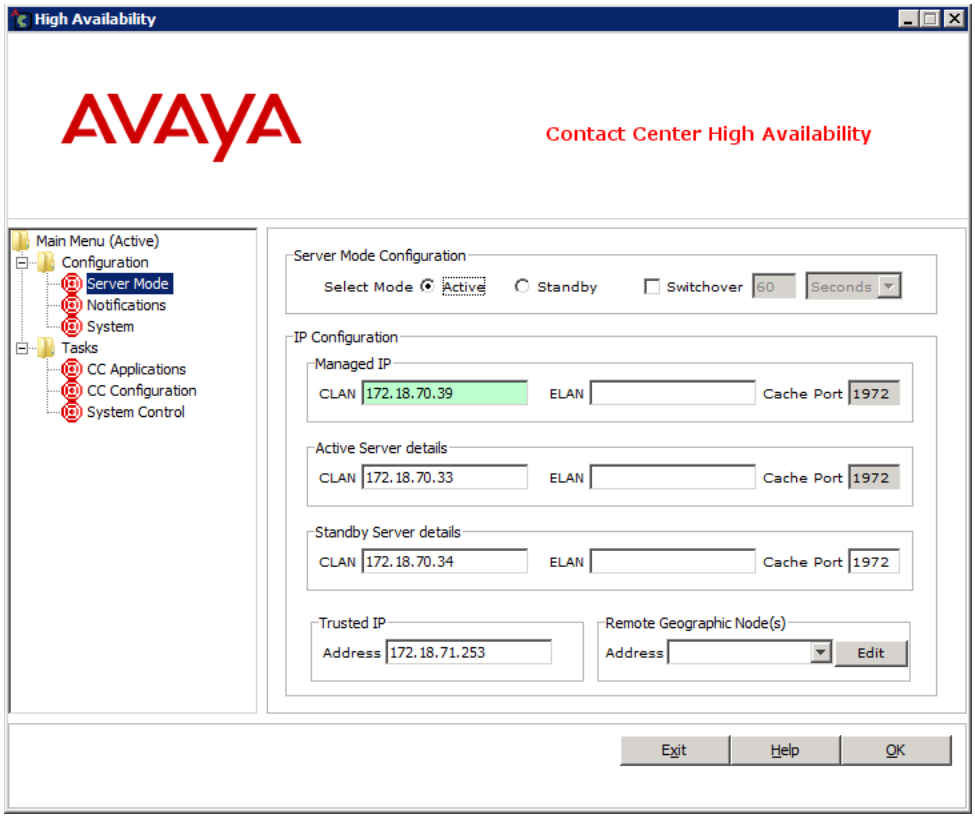
--End--

Configuring High Availability on the Standby Server

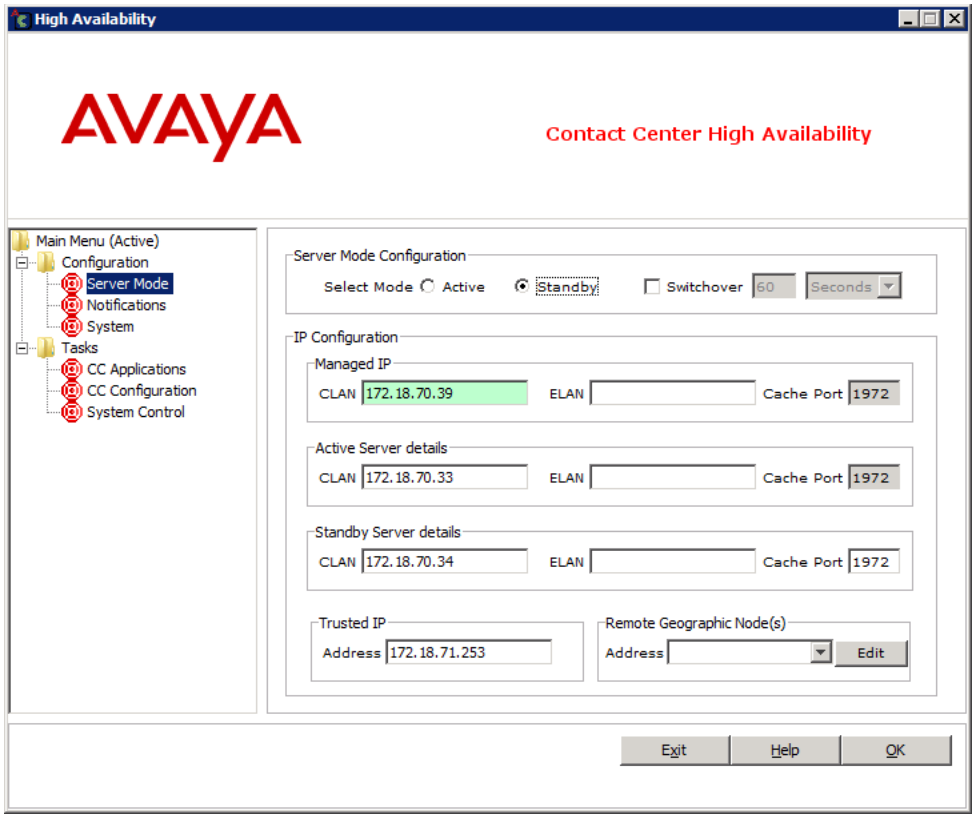
Configure High Availability resiliency on the Standby Server using the High Availability utility. The co-resident CCMS and CCT Standby Server shadows the Active Server and takes over processing if the Active Server fails.

Procedure steps

Step	Action
1	Log on to the Standby server (for example, **CCCORESTWO**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Database Utilities**, **High Availability**.
3	Expand **Configuration**.
4	Double-click **Server Mode**.

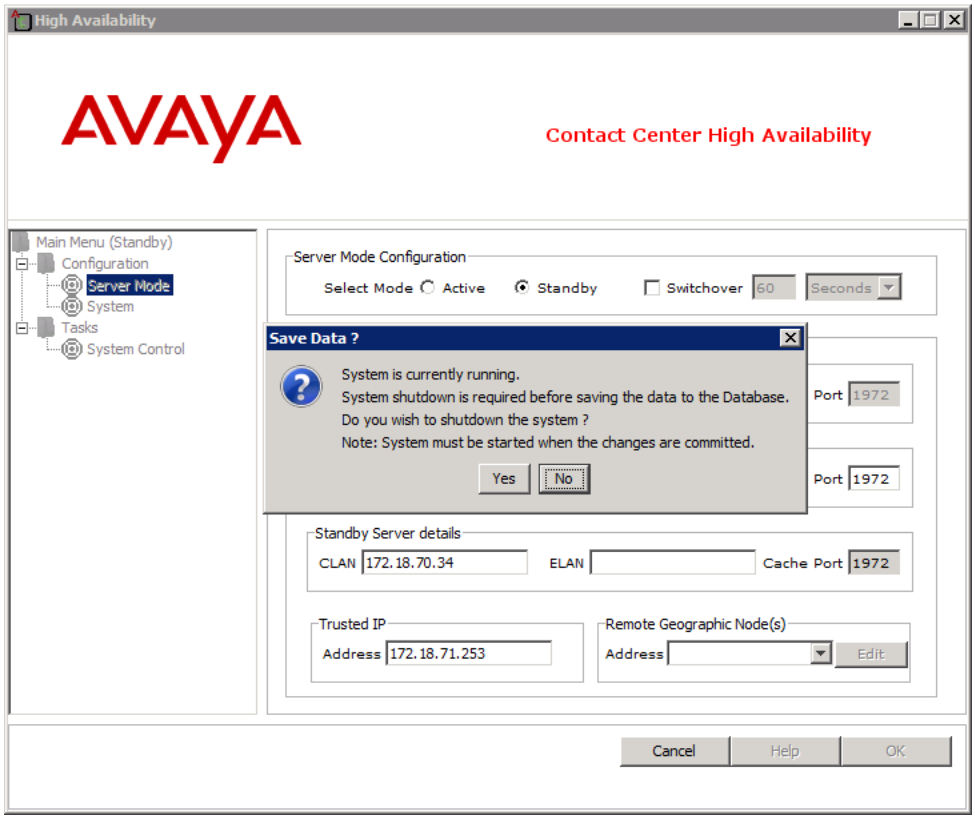


5	Under **Server Mode**, select **Standby**.
6	Under **IP Configuration**, in the **Active Server details CLAN** box, type the IP address for the active server, for example 172.18.70.33.
7	Under **IP Configuration,** in the **Standby Server details CLAN** box, type the IP address for the standby server, for example **172.18.70.34**.



8 Click **OK**.

9 On the **Save Data** message box, click **Yes**.



*The **High Availability** dialog box greys out, and the **Exit** button changes to **Cancel** while the HA services restart.*

10 Click the **Exit** button when it becomes available.

11 On the **High Availability** message box, click **Yes**.

--End--

Checking the server configuration on the Standby Server

After the Standby server restarts, ensure that you completed the server configuration successfully. If you forgot to apply the changes in Server Configuration, Contact Center does not write the CMF file correctly. In this case, the Standby server does not start fully after it initiates a switchover.

Procedure steps

Step	Action

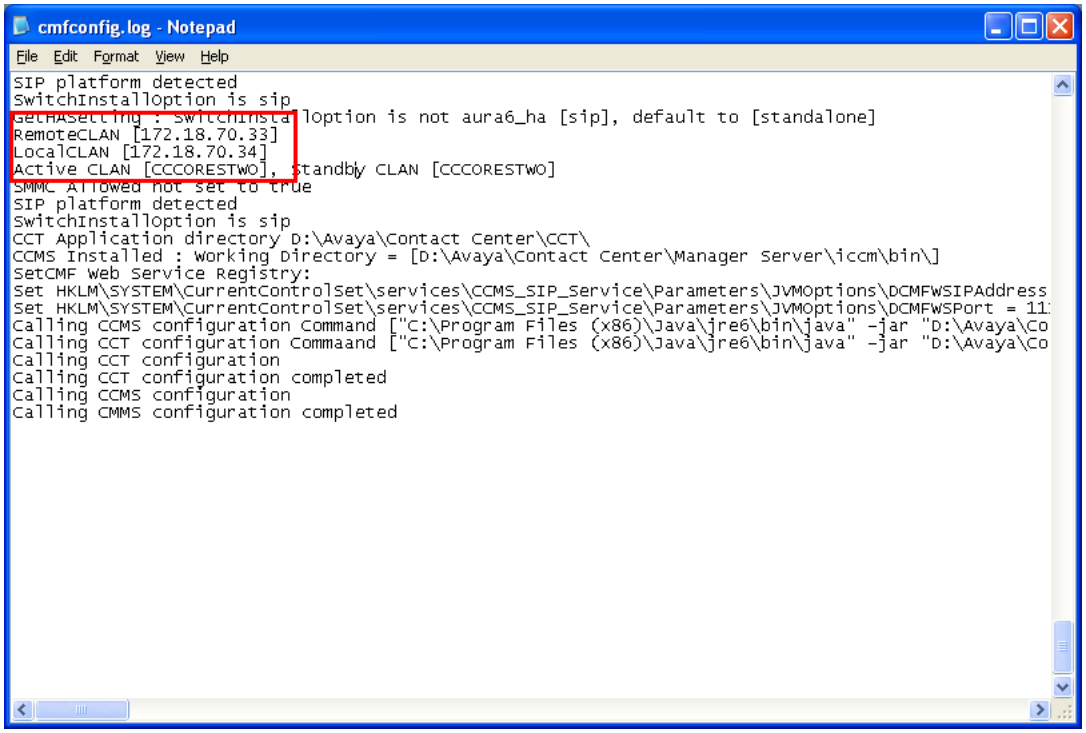
1 Log on to the Standby server (for example, **CCCORESTWO**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.

2 Open the CMF Configuration log file, C:\cmfconfig.log, using a text editor.

3 Scroll to the end of the log file, and search back up the file for the lines "RemoteCLAN [<Active server IP Address>]" and "LocalCLAN [<Active server IP Address>]".

4 Check that the RemoteCLAN value matches the Active server IP address, for example **172.18.70.33**.

5 Check that the LocalCLAN value matches the Standby server IP address, for example **172.18.70.34**.



6 If the RemoteCLAN and LocalCLAN values are not correct, run the Server Configuration utility again. For more information, see Verifying the server details and restarting the Standby Server (page 507).

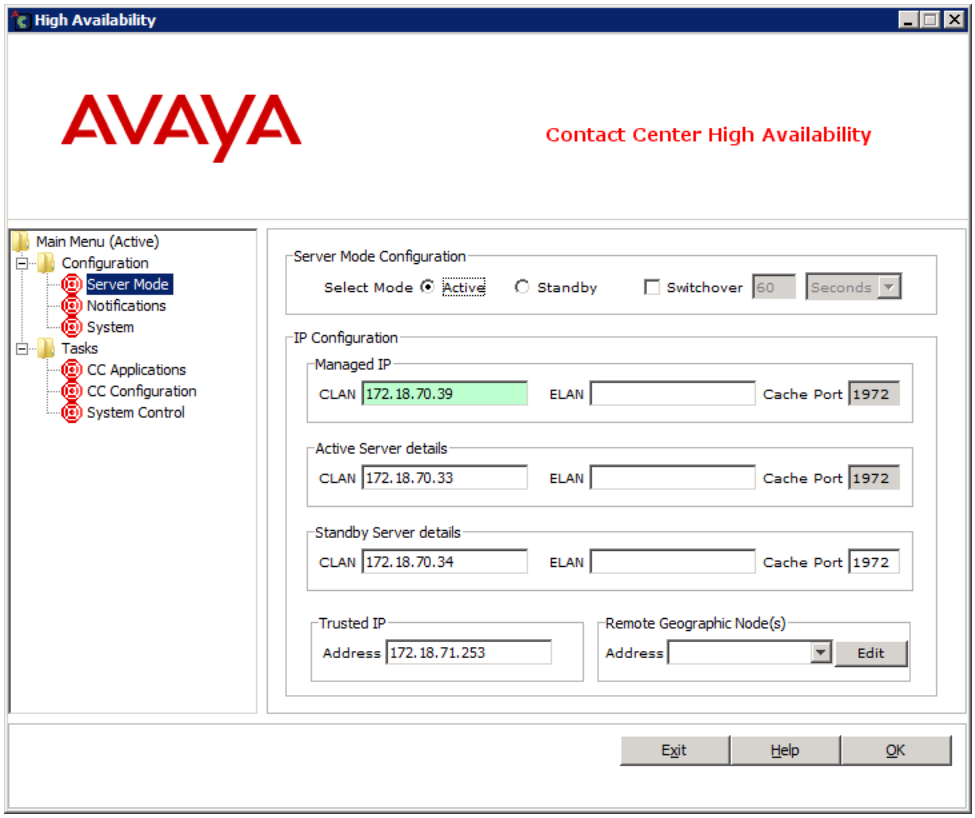
--End--

Starting High Availability on the Active Server

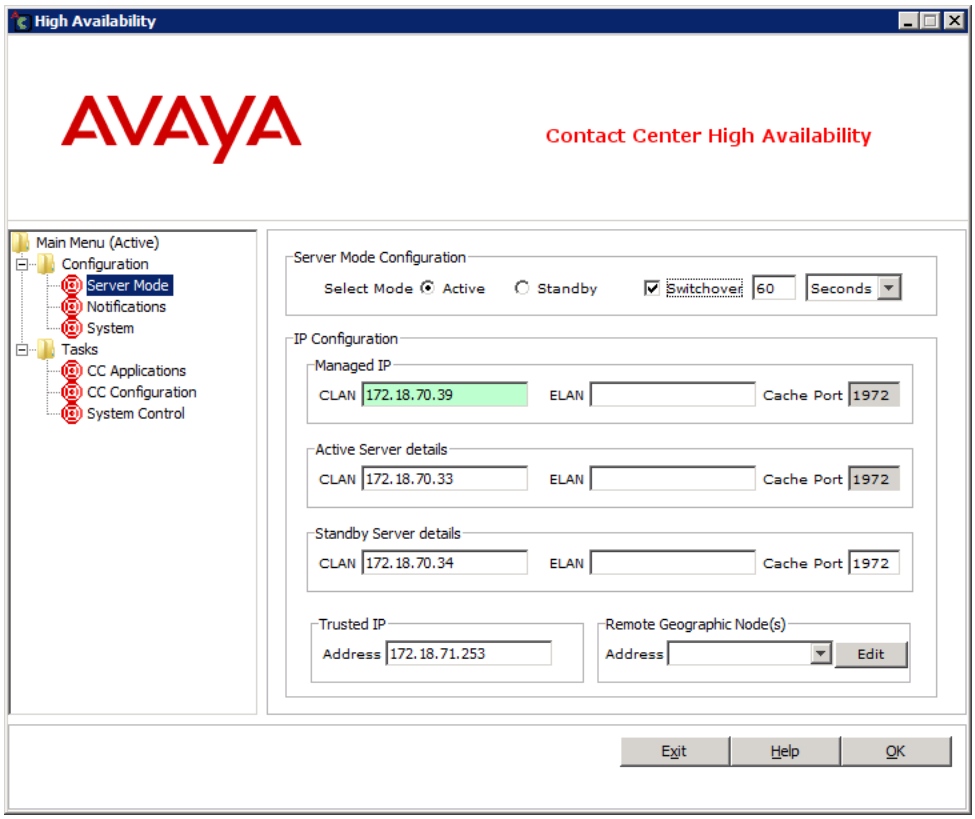
Start the Active Server using the High Availability utility. Starting the Active Server starts CCMS, CCT, and system processes. Enable automatic switchover so the Standby server can take over if the Active server fails or is stopped.

Procedure steps

Step	Action
1	Log on to the Active server using the Avaya Aura® CC installer domain account, for example AACCinstaller.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Database Utilities**, **High Availability**.
3	In the left pane, expand **Configuration, Server Mode**.

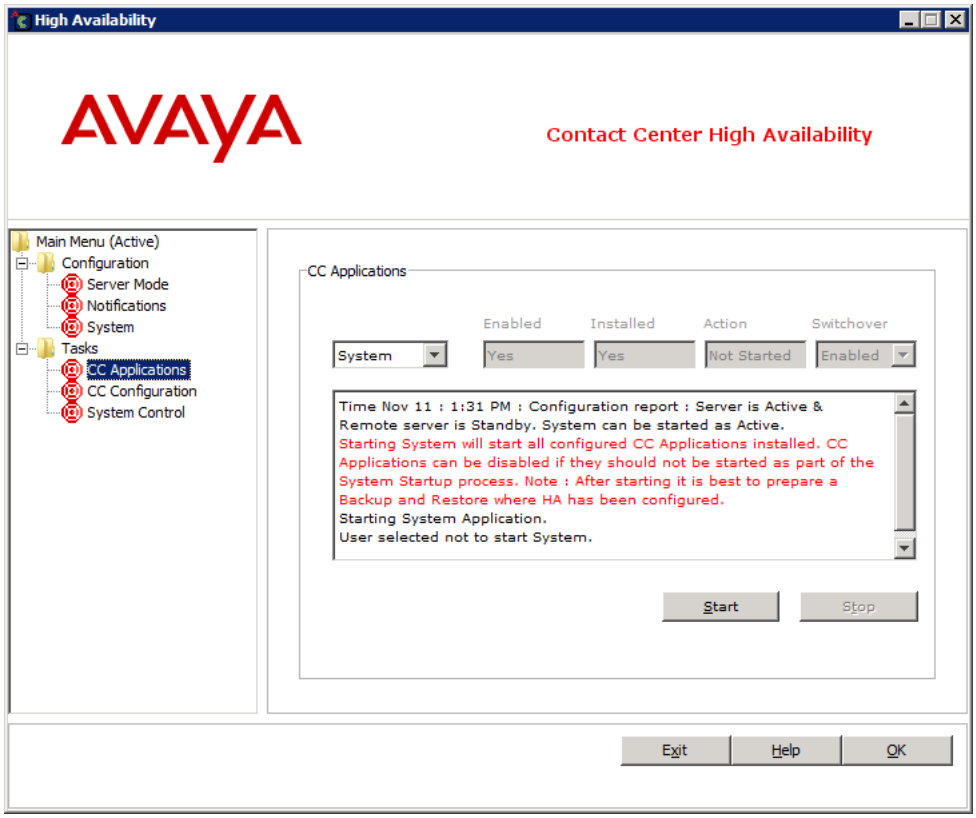


4	Verify that the mode selected is **Active**.
5	Under **Server Mode Configuration**, select **Switchover**.
6	Click **OK**.

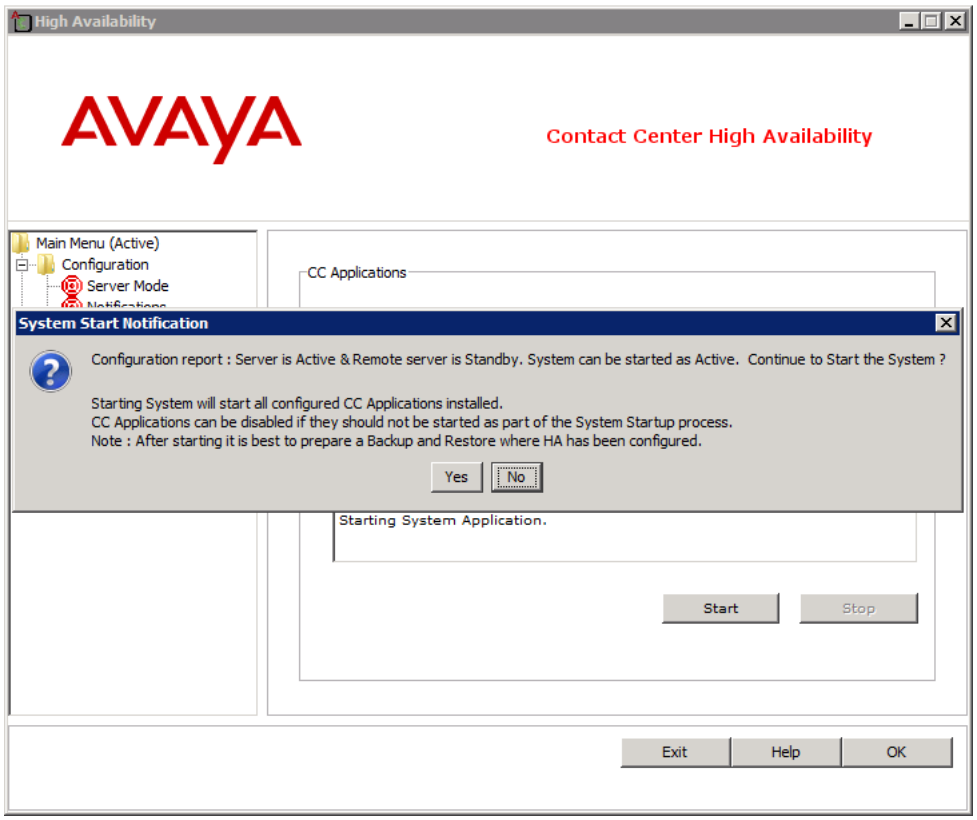


7 In the left pane, expand **Tasks, CC Applications**.

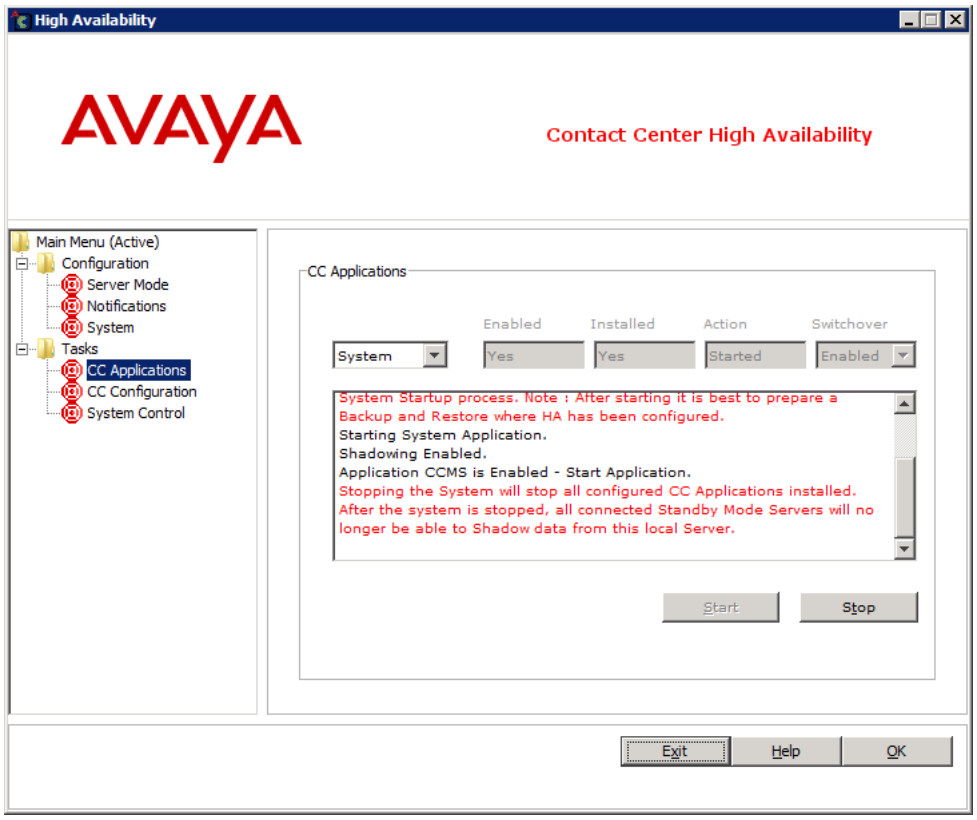
8 Click **Start**.



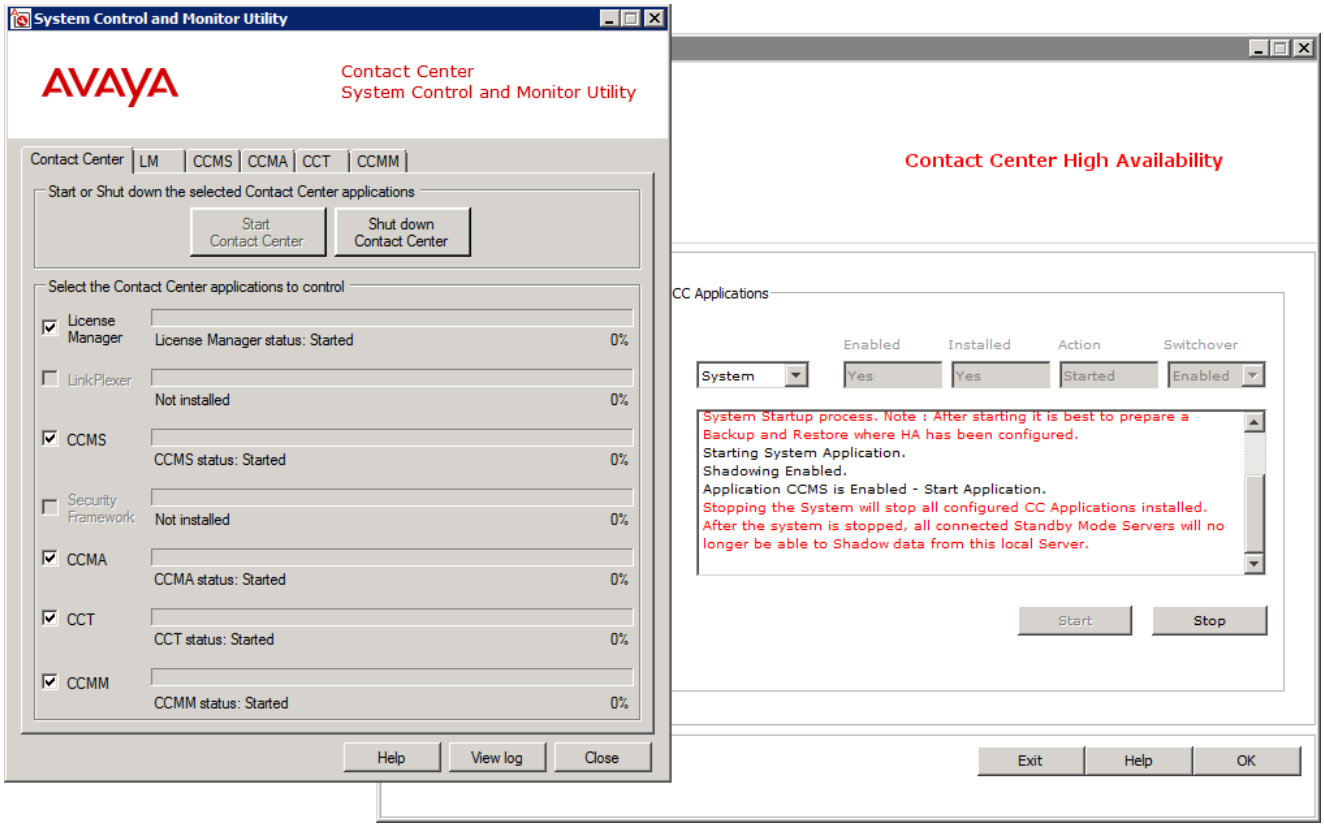
9 On the **System Start Notification** message box, click **Yes**.



The High Availability system starts, and displays the progress in the CC Applications box.



10 To verify that the Contact Center services are running using the SCMU, select **Avaya**, **Contact Center**, **Common Utilities**, **System Control and Monitor Utility**, and check that the Contact Center services start up.



11 On the **System Control and Monitor Utility**, click **Close**.

12 On the **High Availability**, window click **Exit**.

--End--

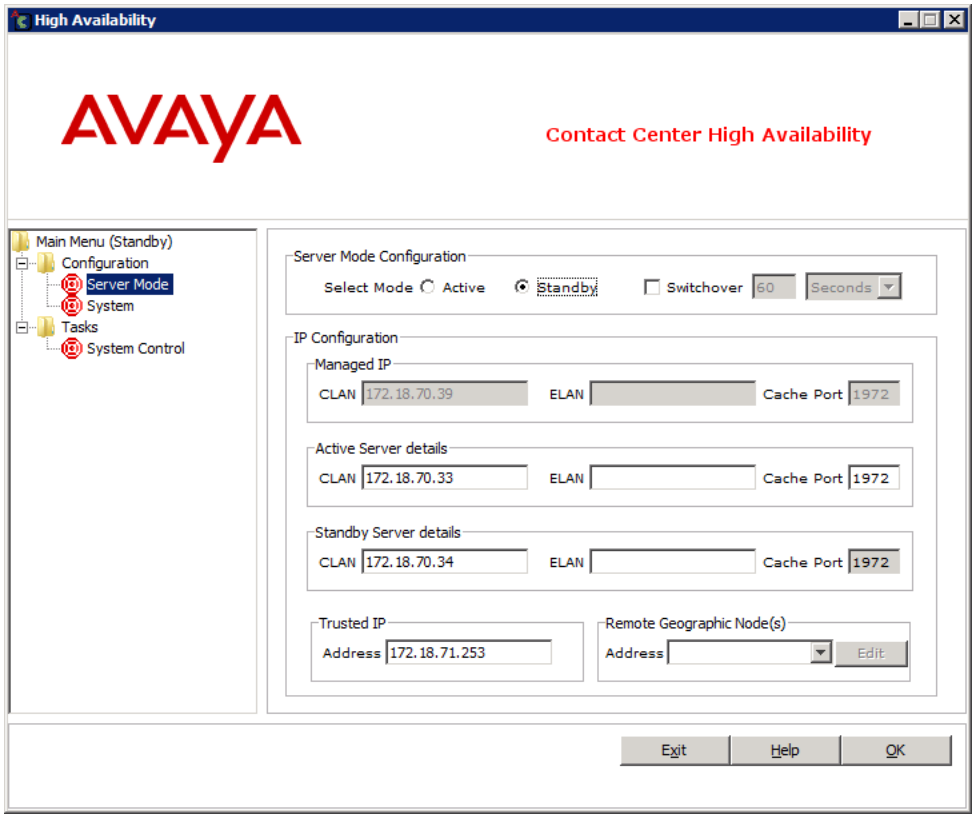
Starting High Availability on the Standby Server

Start the Active Server using the High Availability utility. Starting the Active Server starts CCMS, CCT, and system processes. Enable automatic switchover so the Standby server can take over if the Active server fails or is stopped.

Procedure steps

Step	Action
1	Log on to the Standby server (for example, **CCCORESTWO**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Database Utilities**, **High Availability**.

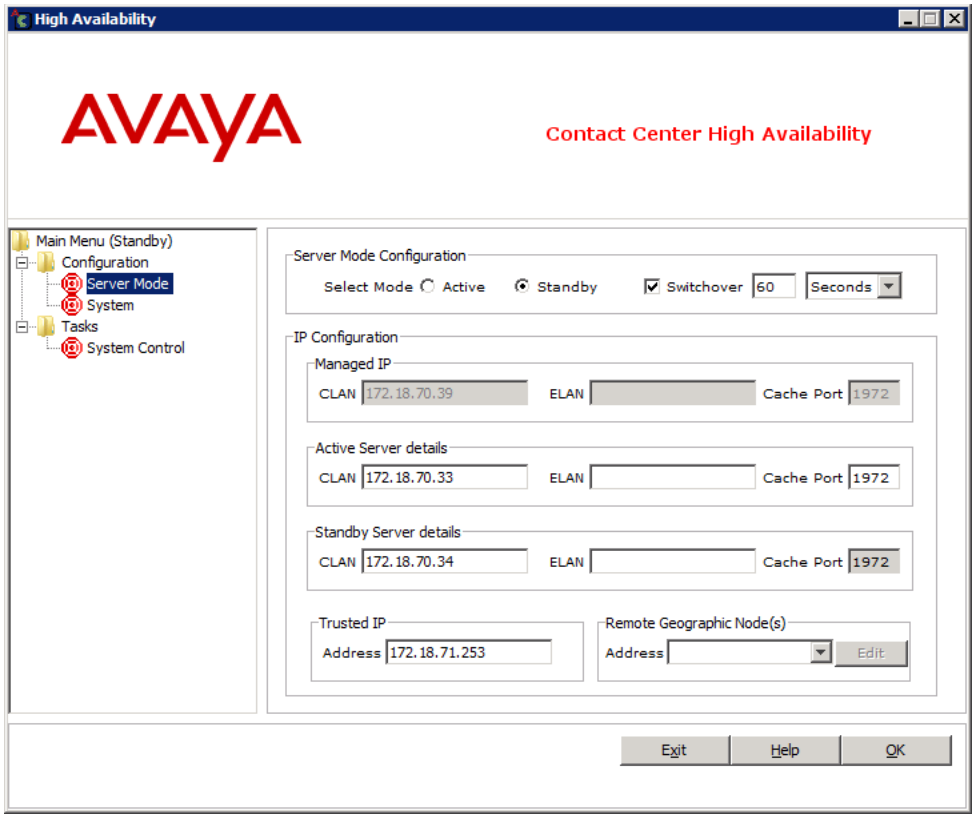
3 In the left pane, expand **Configuration, Server Mode**.



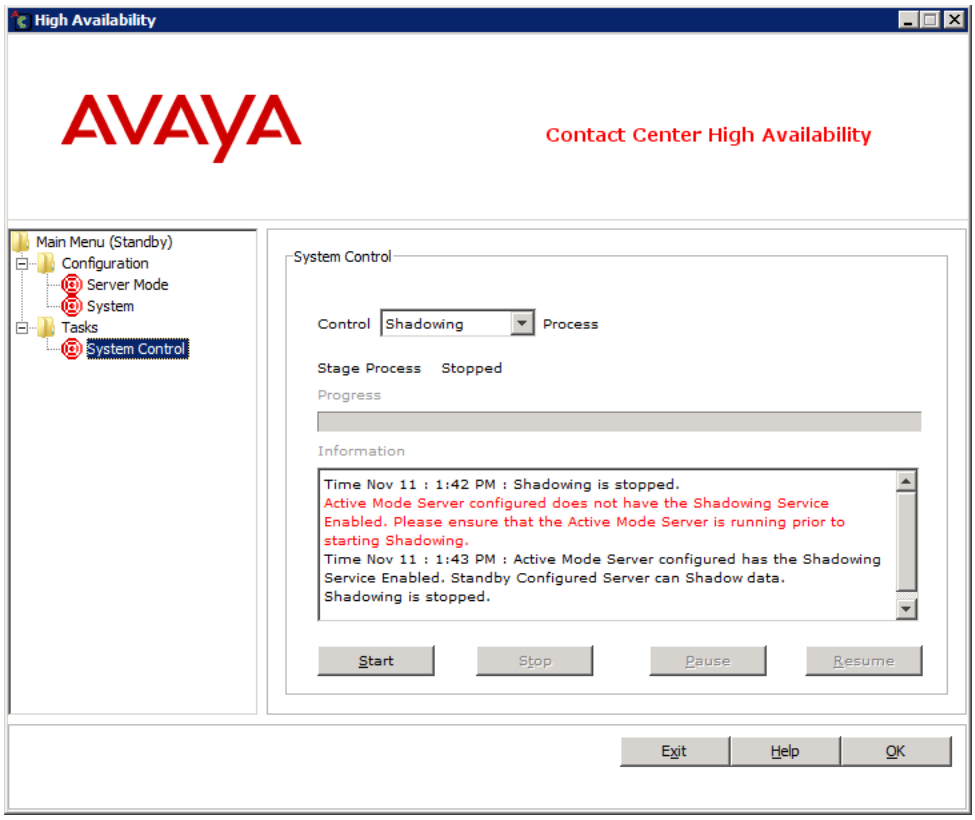
4 Verify that the mode selected is **Standby**.

5 Under **Server Mode Configuration**, select **Switchover**.

6 Click **OK**.

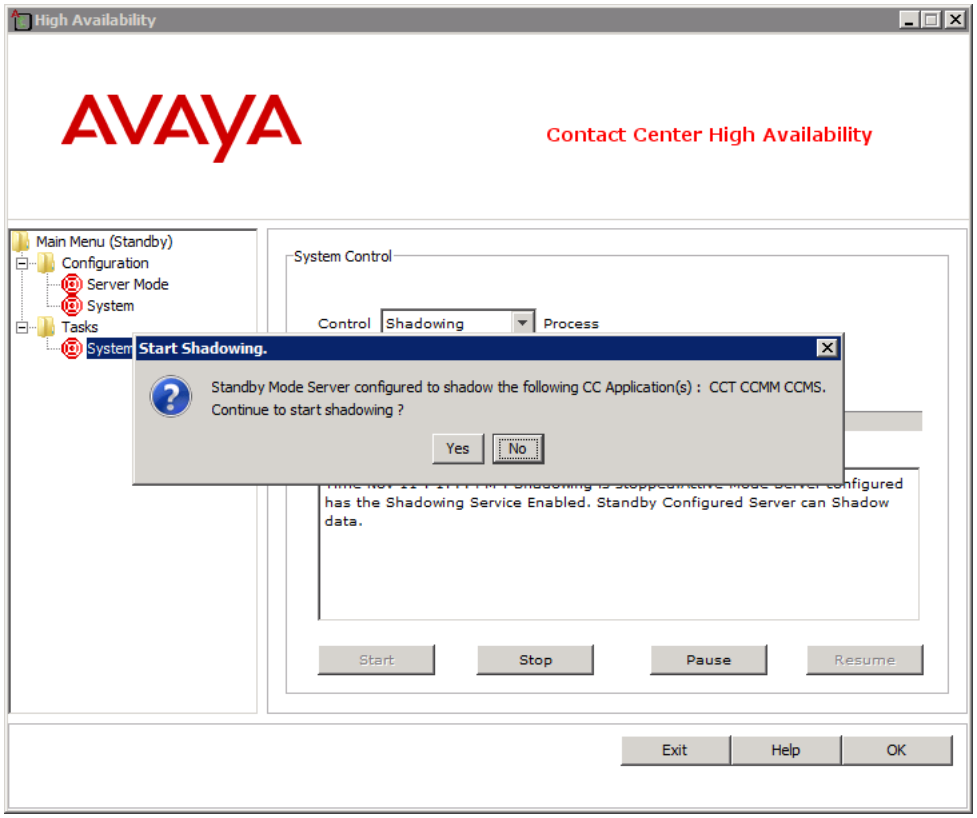


7 In the left pane, expand **Tasks, System Control**.



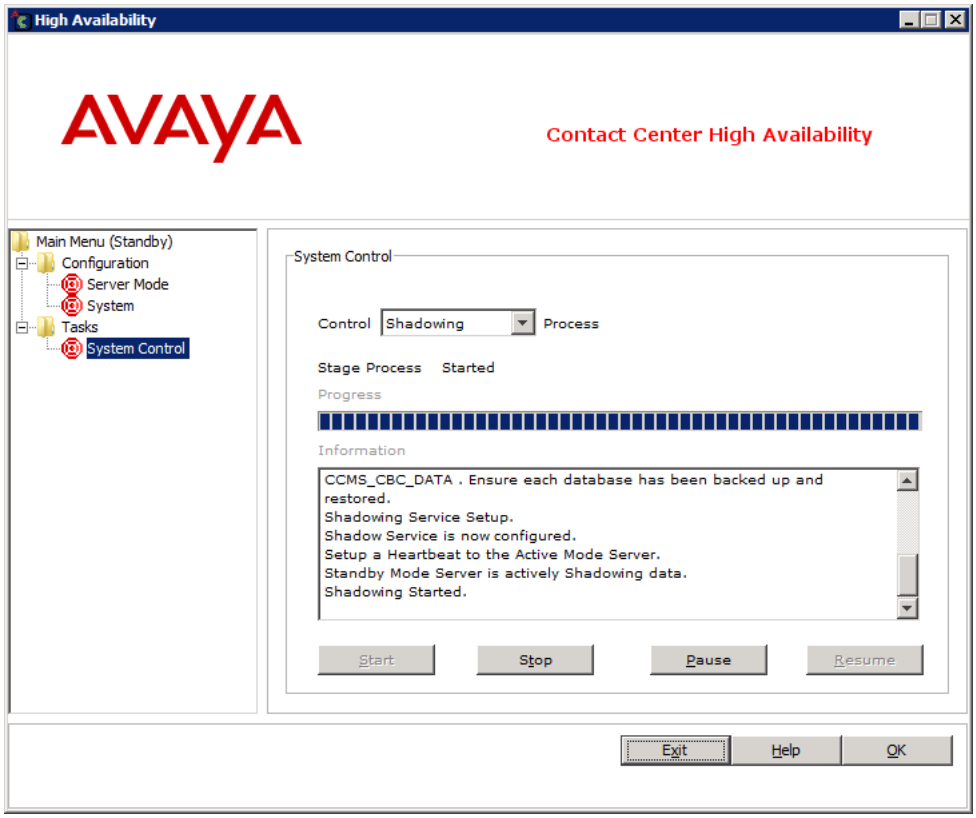
8 Click **Start**.

9 On the **Start Shadowing** message box, click **Yes**.



10 In the information box, verify that shadowing has started, by checking for text similar to the following:
"Time Nov 18:3:12 PM : Standby Mode Server is actively Shadowing data. Setup a Heartbeat to the Active Mode Server."

11 Click **Exit**.



--End--

Verifying shadowing is running on the Active Server

Use the High Availability utility to verify that the Standby server is shadowing the Active server. The System dialog box of the High Availability utility displays system information about the Active and the Standby servers.

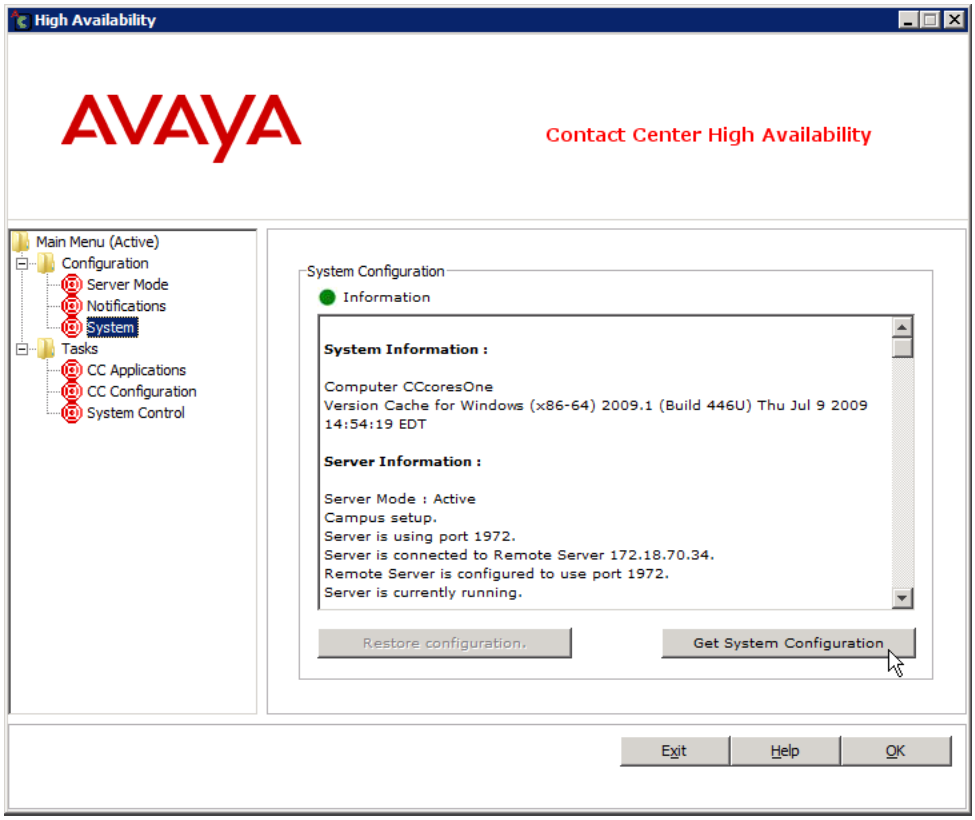
The dialog box displays the following information categories:

- Computer name and operating system version
- Server mode
- Server configuration type
- Port information
- Remote server connection status
- Remote server port information

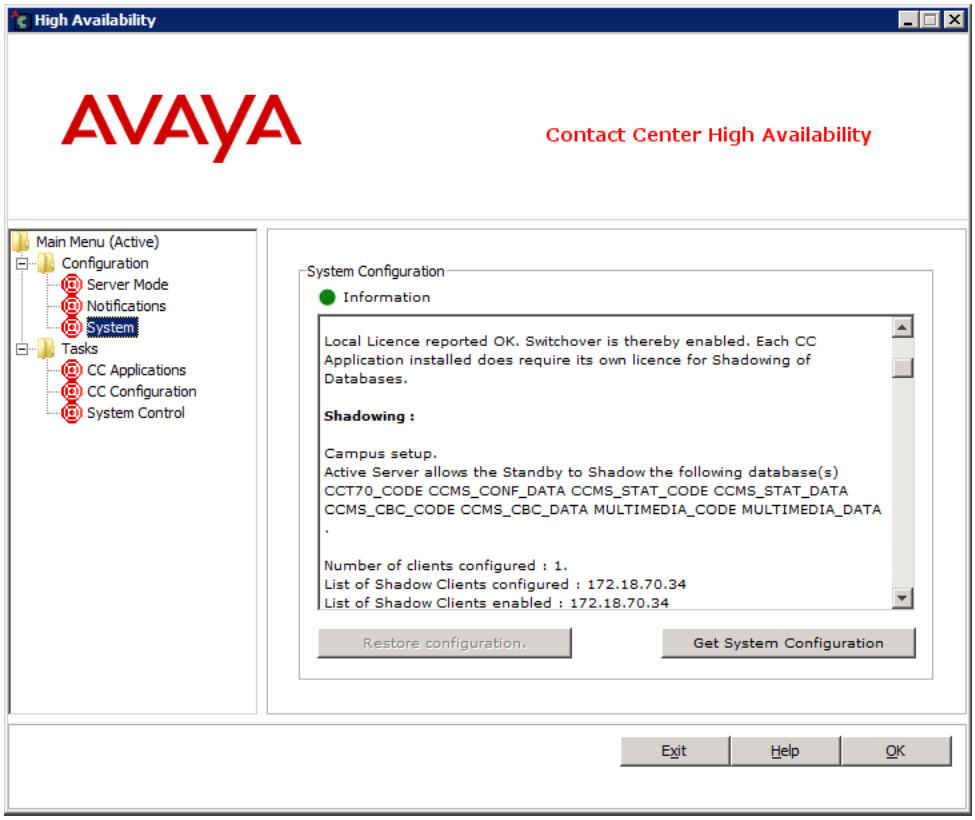
- License information
- Databases shadowed
- Time of last record shadowed
- Database namespaces
- Local and remote information on system status, switchover, shadowing and network.
- CC Application install information
- Database space and journaling information
- Database processes information

Procedure steps

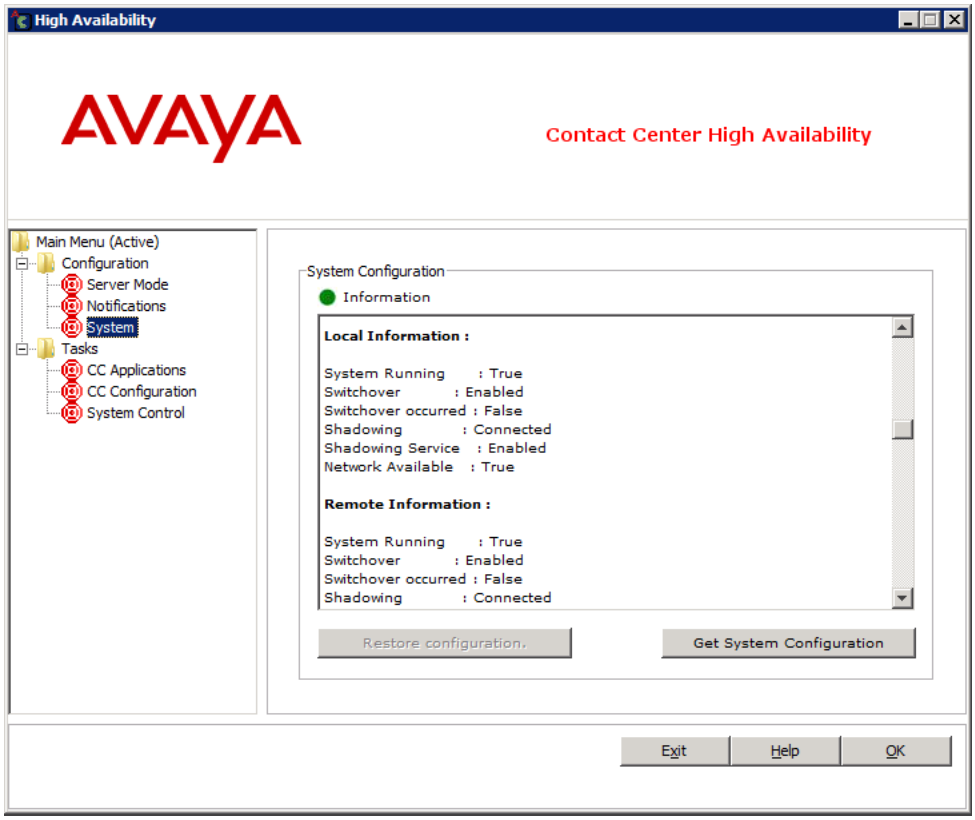
Step	Action
1	Log on to the Standby server (for example, **CCCORESTWO**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Database Utilities**, **High Availability**.
3	In the left pane, expand **Configuration**.
4	Select **System**.
5	Click **Get System Configuration**.



6 Scroll down to the **Shadowing** section. Check that the number of clients configured is **1** and that the Standby server IP address is listed beside **List of Shadow Clients enabled**.



7 Scroll down to the **Local Information** and **Remote Information** sections. Under **Local Information** check that the shadowing service is **Enabled**. Under **Remote Information** check that Shadowing is **Connected**.



8 Click **Exit**.

--End--

Changing server details in Contact Center Manager Administration

In Contact Center Manager Administration, change the 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, for example, **CCCORESONE**, using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	In the **Address** box, type the CCMA URL in the format http://<Server name>, for example **http://CCCORESONE**.
3	Press **Enter**.

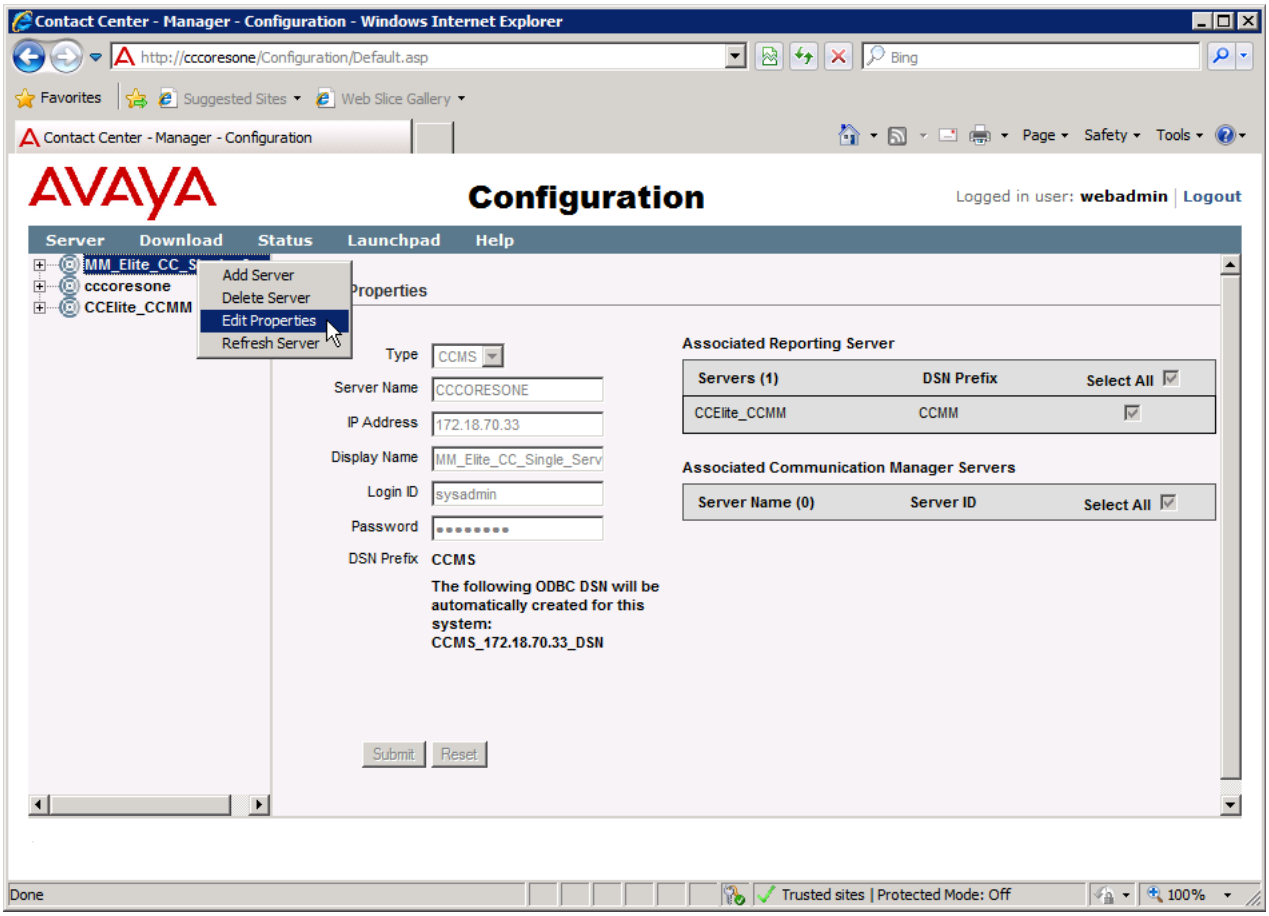
4 In the main logon window, in the **User ID** box, type **webadmin**.

5 In the **Password** box, type the password, for example **nimdabew**.

6 Click **Login**.

7 On the **Launchpad**, click **Configuration**.

8 From the list of servers in the system tree, right-click on the active CCMS server, and select **Edit Properties**.

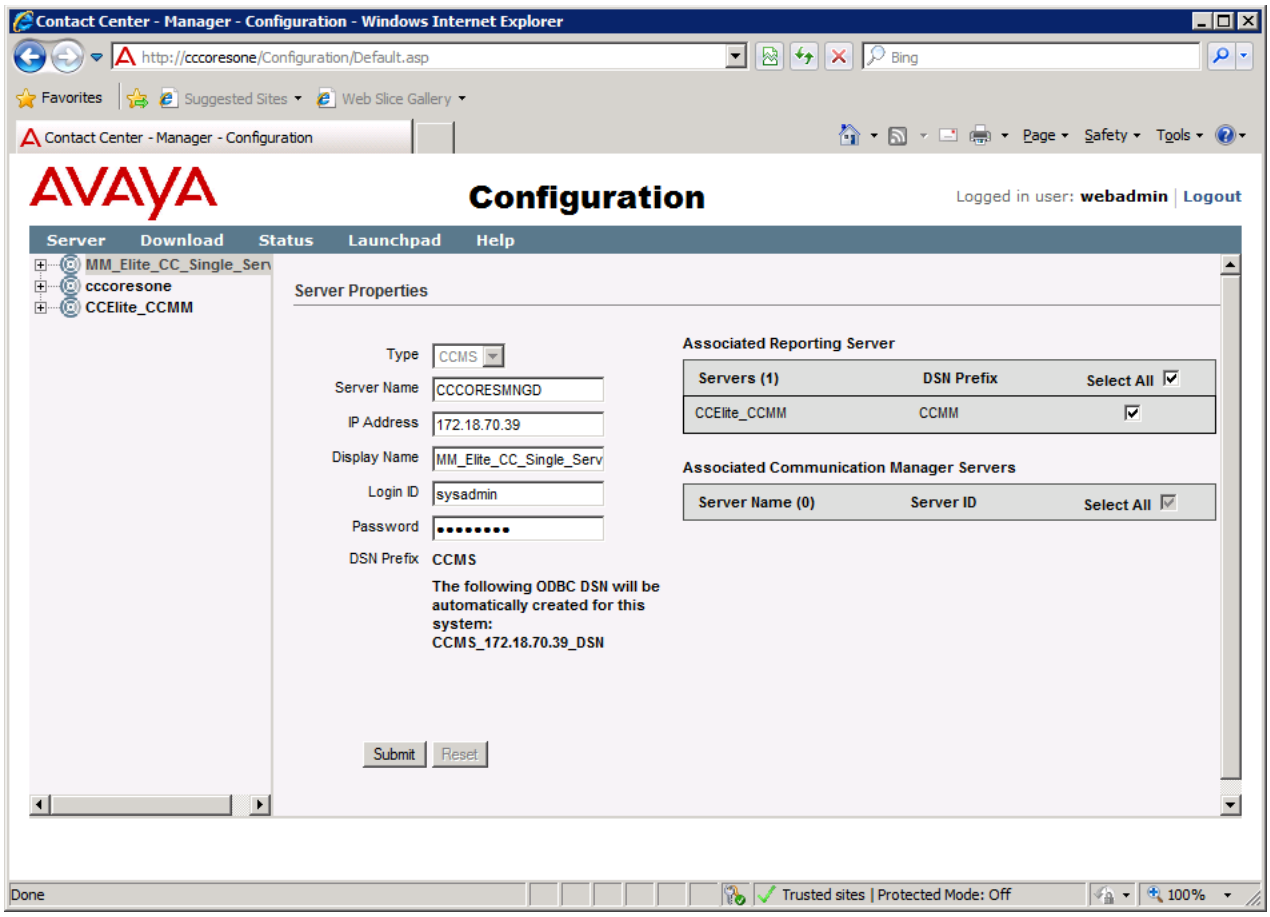


9 In the **Server Name** box, type the High Availability Managed name of the Contact Center Manager Server, for example **CCCORESMNGD**.

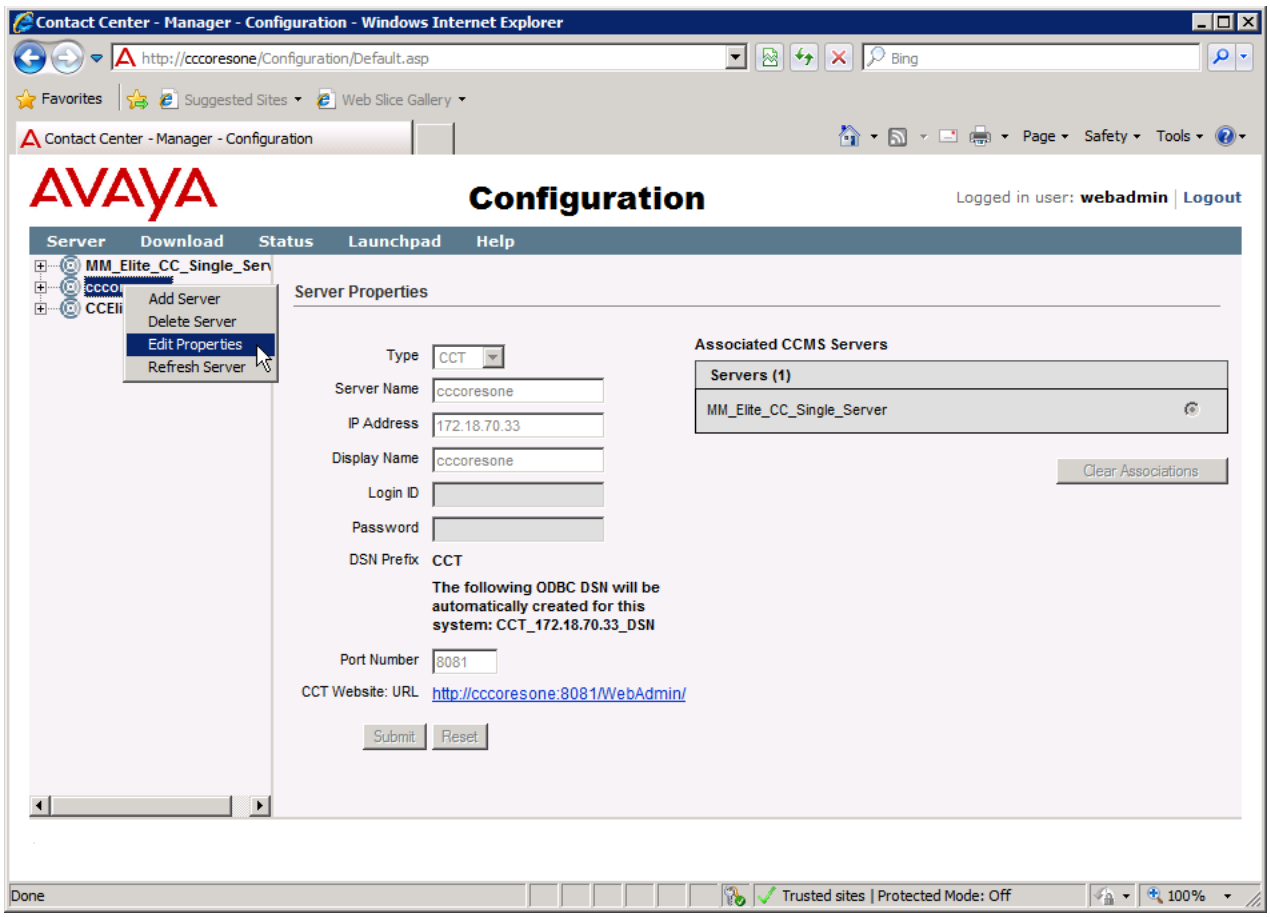
10 Press **Tab.**

Contact Center updates the IP Address with the High Availability Managed IP address for example 172.18.70.39

11 Click **Submit**.



12 From the list of servers in the system tree, right-click on the active CCT server, and select **Edit Properties**.

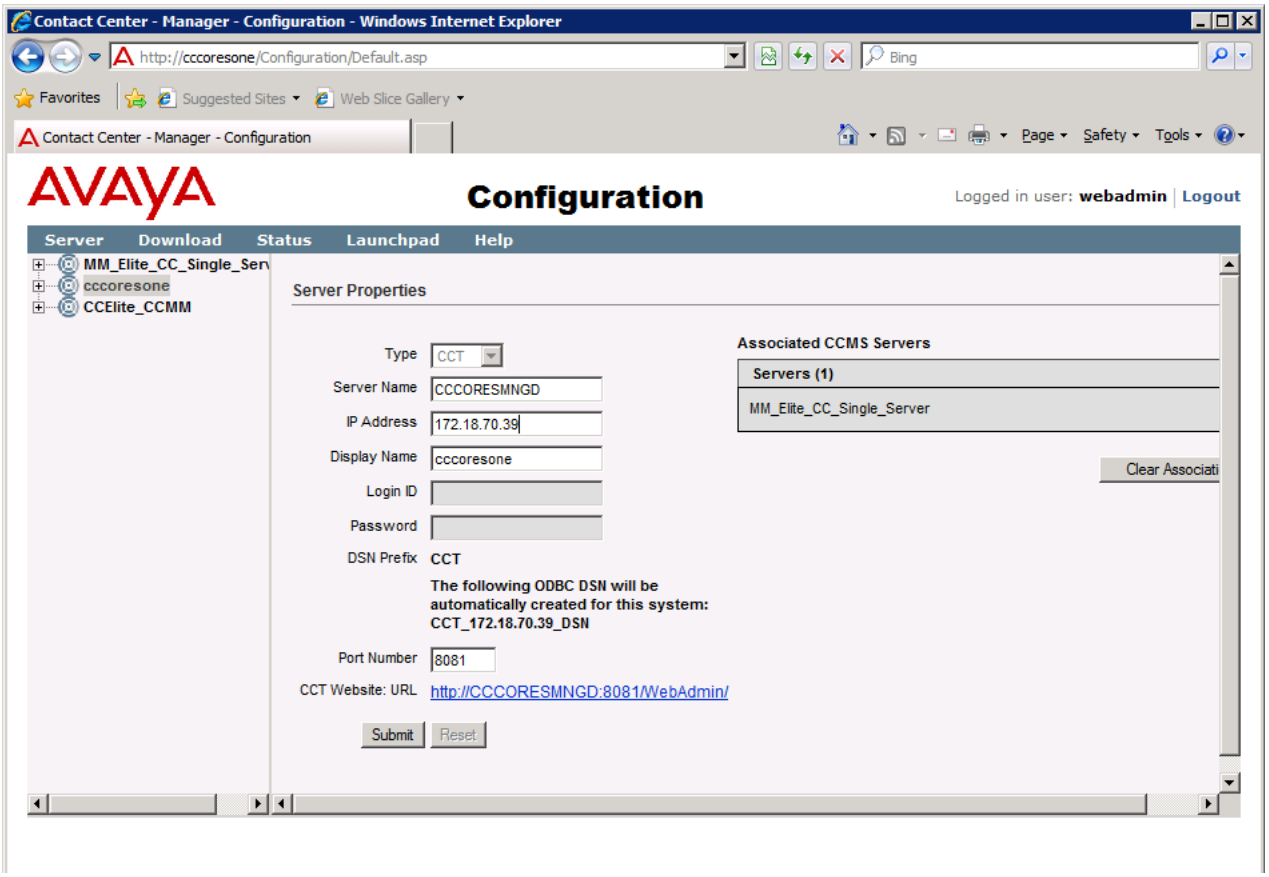


13 In the **Server Name** box, type the High Availability Managed name of the Communication Control Toolkit server, for example **CCCORESMNGD**.

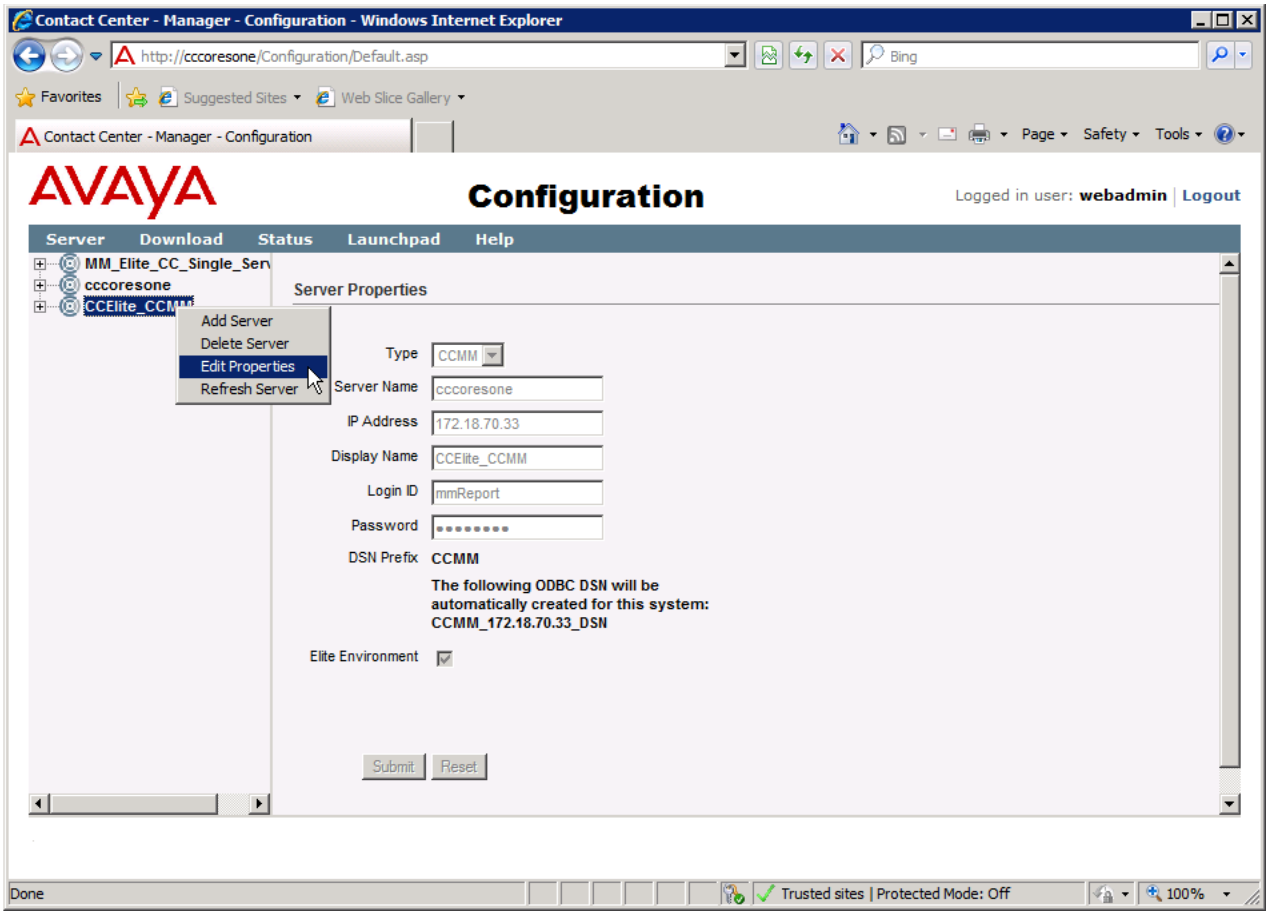
14 Press **Tab.**

Contact Center updates the IP Address with the High Availability Managed IP address, for example 172.18.70.39

15 Click **Submit**.



16 From the list of servers in the system tree, right-click on the active CCMM server, and select **Edit Properties**.



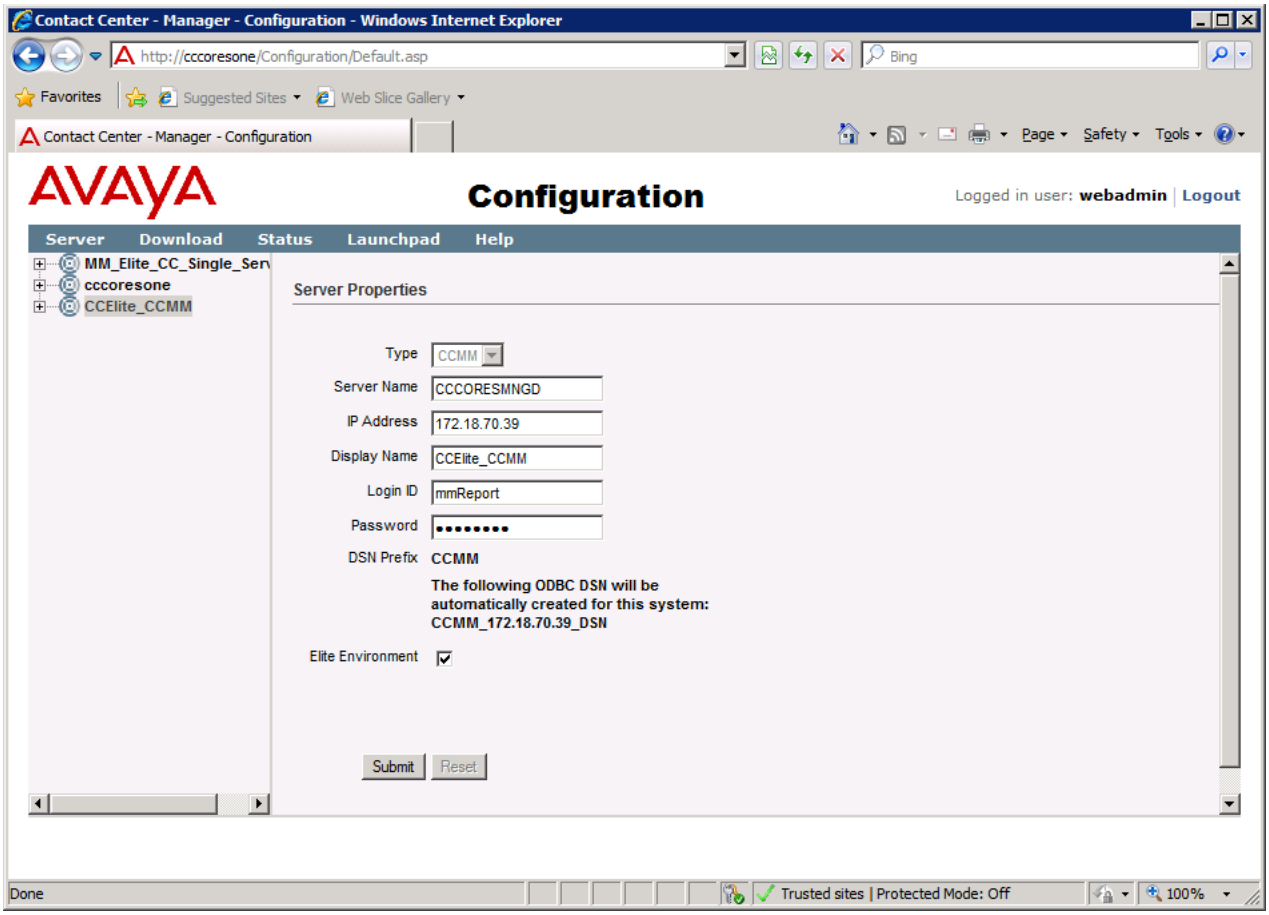
17 In the **Server Name** box, type the High Availability Managed name of the Contact Center Multimedia server, for example **CCCORESMNGD**.

18 Press **Tab.**

Contact Center updates the IP Address with the High Availability Managed IP address, for example 172.18.70.39

Attention: After changing the server details, you are not able to access the Multimedia component in CCMA: you must carry out a subsequent procedure to change the server details in the Multimedia database by using the CCMM Dashboard. See Updating server names in CCMM Dashboard (page 533).

19 Click **Submit**.



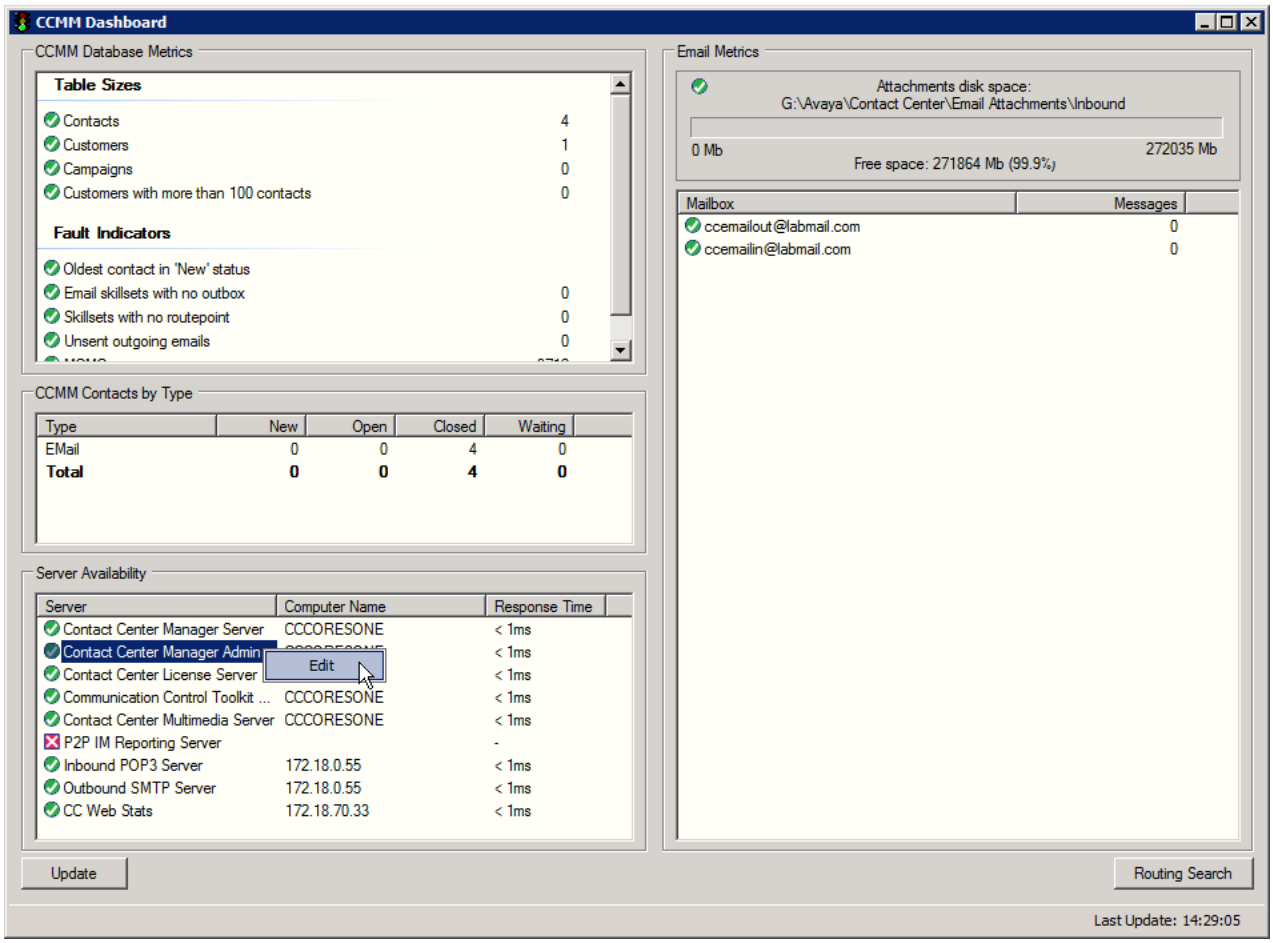
--End--

Updating server names in CCMM Dashboard

Use the Contact Center Multimedia Dashboard utility to update the names of the servers to use the managed server name. You must complete this procedure to be able to access the Multimedia Administration client after changing the server names in CCMA.

Procedure steps

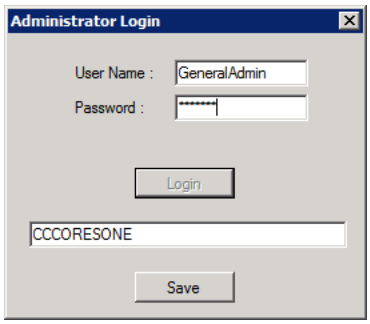
Step	Action
1	Log on to the Standby server (for example, **CCCORESTWO**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Multimedia Server**, **Multimedia Dashboard**.



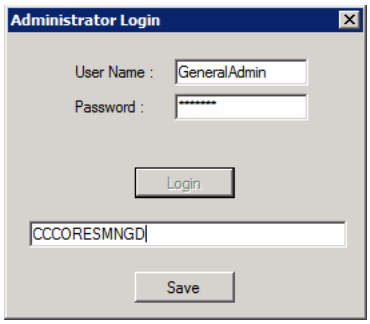
3 Under **Server Availability**, right-click on the Contact Center Manager Administration server and select **Edit**.

4 On the **Administrator Login** dialog, in the **User Name** box, type **GeneralAdmin**.

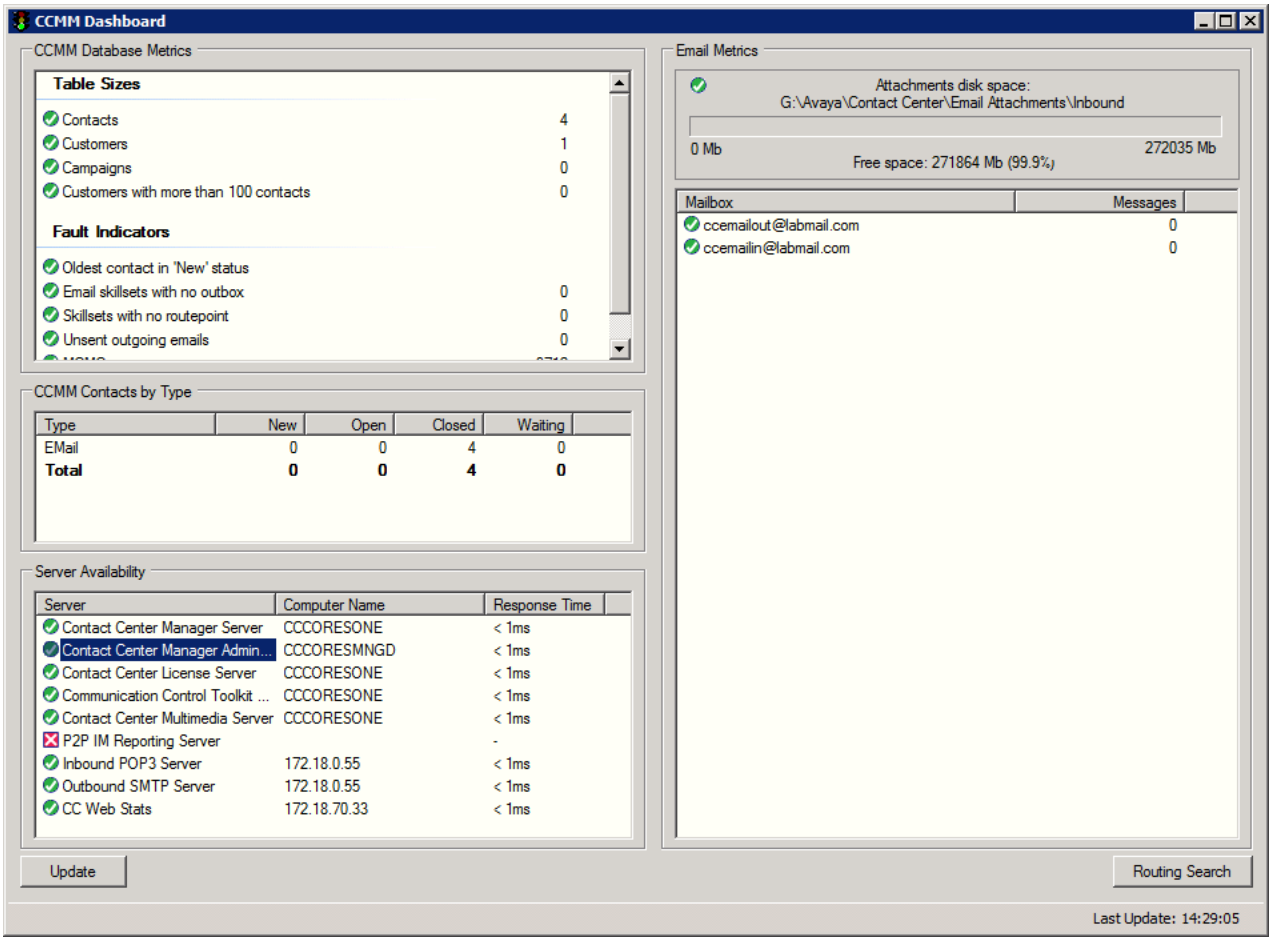
5 On the **Administrator Login** dialog, in the **Password** box, type **__ccmm!** (two underscore characters followed by "ccmm!").



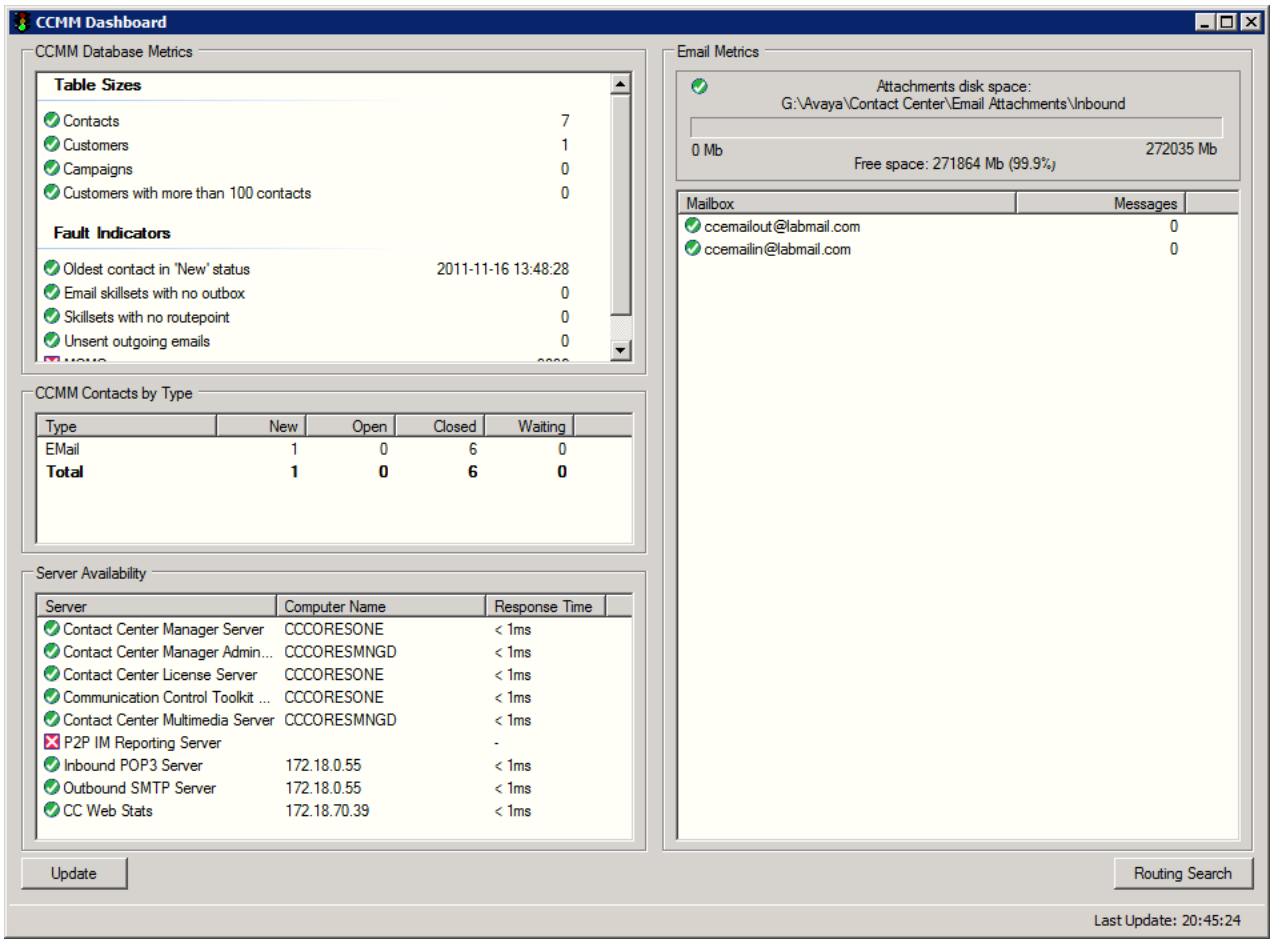
6 Change the Contact Center Manager Administration IP address to the Managed IP name, for example **CCCORESMNGD**.



7 Click **Save**.



8 Repeat steps 3 to 7 for the CCMM server.



--End--

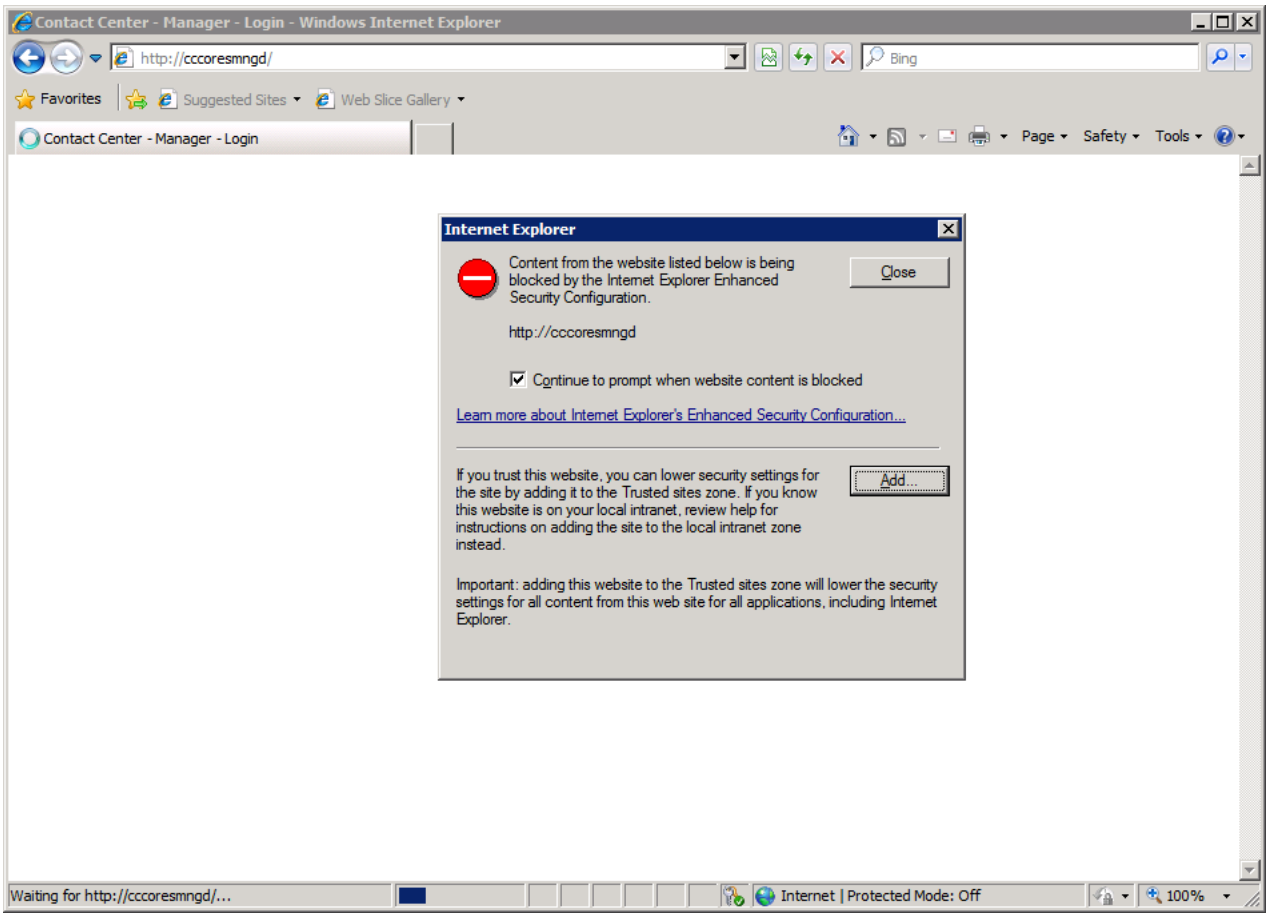
Using the Contact Center Manager Administration server Managed name

Use the High Availability Managed name of the Contact Center Manager Administration server to access the CCMA application. When you enable the Avaya Aura® Contact Center High Availability feature, re-direct all Contact Center Manager Administration client Web browsers to use the Managed server name of the CCMA server.

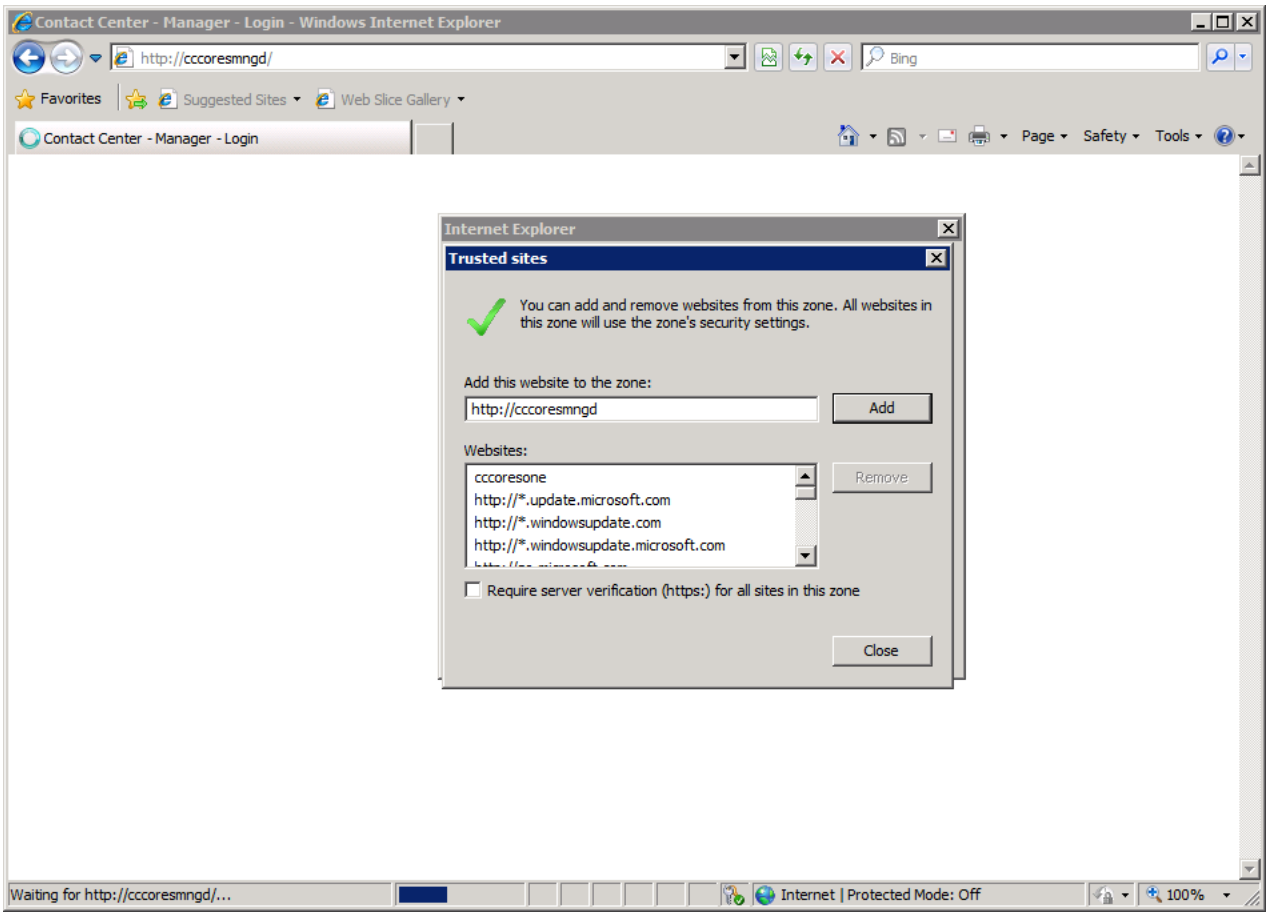
Attention: Do not type the real or Managed IP address in the Address box. Using an IP address results in problems with Scripting, Historical Reporting, Configuration, Contact Center Management, and Access and Partition Management.

Procedure steps

Step	Action
1	Start Internet Explorer.
2	In the **Address** box, type the URL of the CCMA server, using the managed IP address, for example **http://CCCORESMNGD**.
3	On the **Internet Explorer** dialog, click **Add** to add the managed server name to the list of trusted websites.

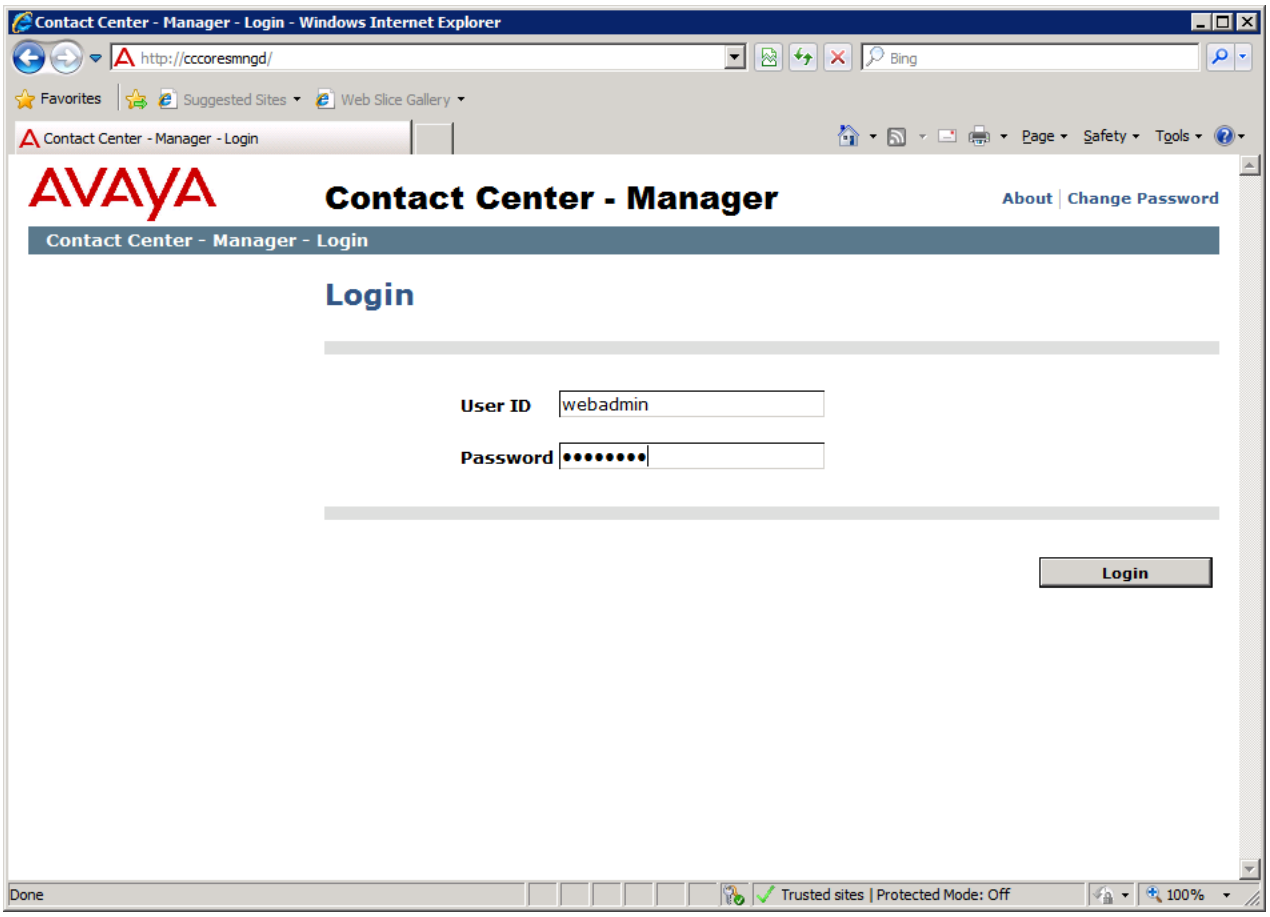


4	On the **Trusted Sites** dialog, click **Add**.



5 In the **User ID** box, type the CCMA administrator user ID, for example **webadmin**.

6 In the **Password** box, the CCMA administrator password, for example **nimdabew**.



7 Click **Login**.

--End--

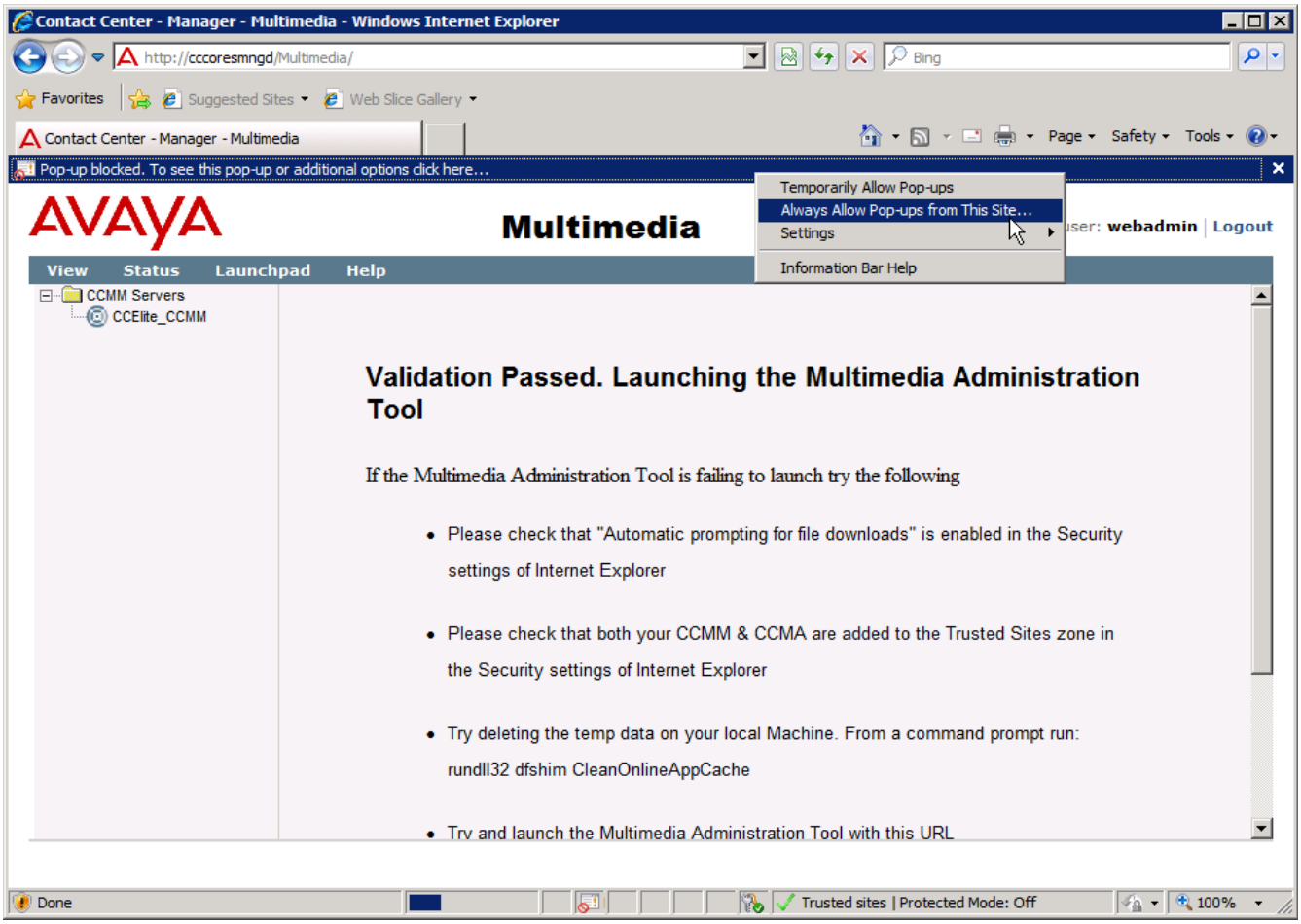
Configuring CCMM General Administration

In a Multimedia Complement solution Avaya Aura® Agent Desktop client software is downloaded from the Contact Center Multimedia (CCMM) component on the Contact Center server. Agent Desktop then communicates with that server to handle e-mail based contacts.

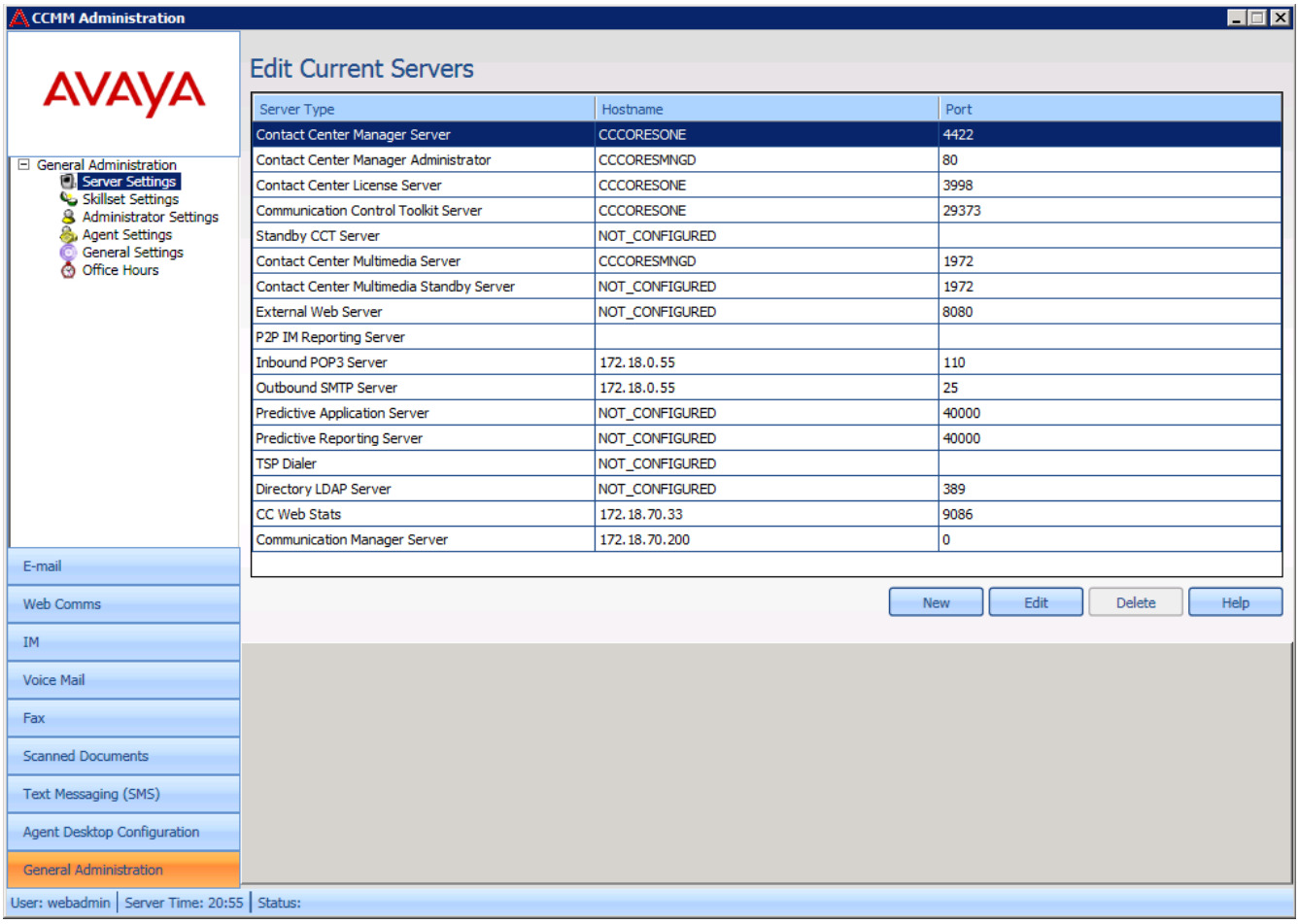
In a multimedia-enabled High Availability solution use the CCMM Administration tool to configure the server details to use the High Availability Managed name so that Agent Desktop communicates with the standby server after a switchover.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration **Launchpad**, click **Multimedia**.
2	In the left column, select the Multimedia server on which you want to configure server settings, for example **CCElite_CCMM**.

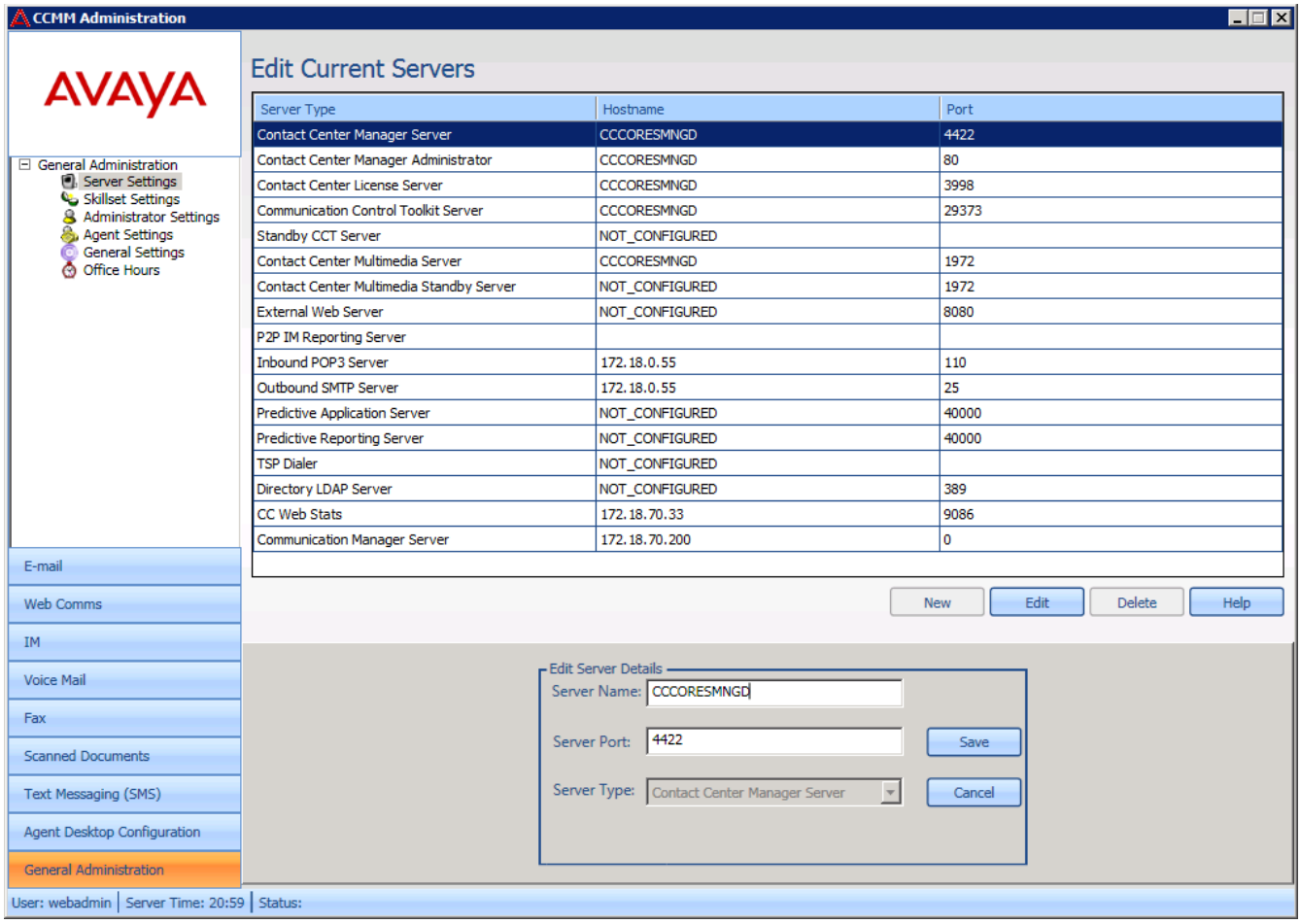


3	In the right pane, click **Launch Multimedia Client**.
4	In the left column, select **General Administration**.
5	Click **Server Settings**.



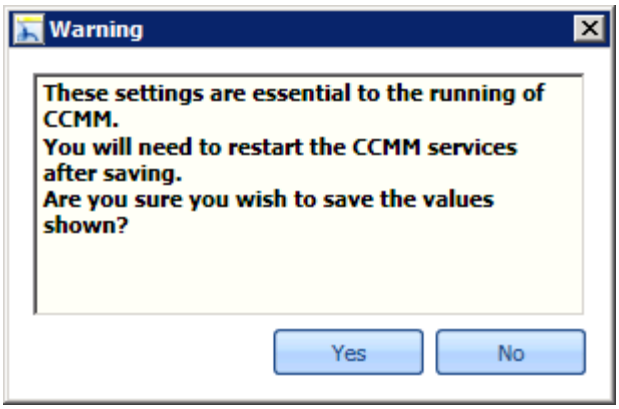
6 Select **Contact Center Manager Server** and click **Edit**.

7 In the **Server Name** box, type the High Availability Managed name, for example **CCCORESMNGD**.



8 Click **Save**.

9 On the **Warning** message box, click **Yes**.



10 Select **Contact Center License Manager** and click **Edit**.

11 In the **Server Name** box, type the High Availability Managed name, for example **CCCORESMNGD**.

12 Click **Save**.

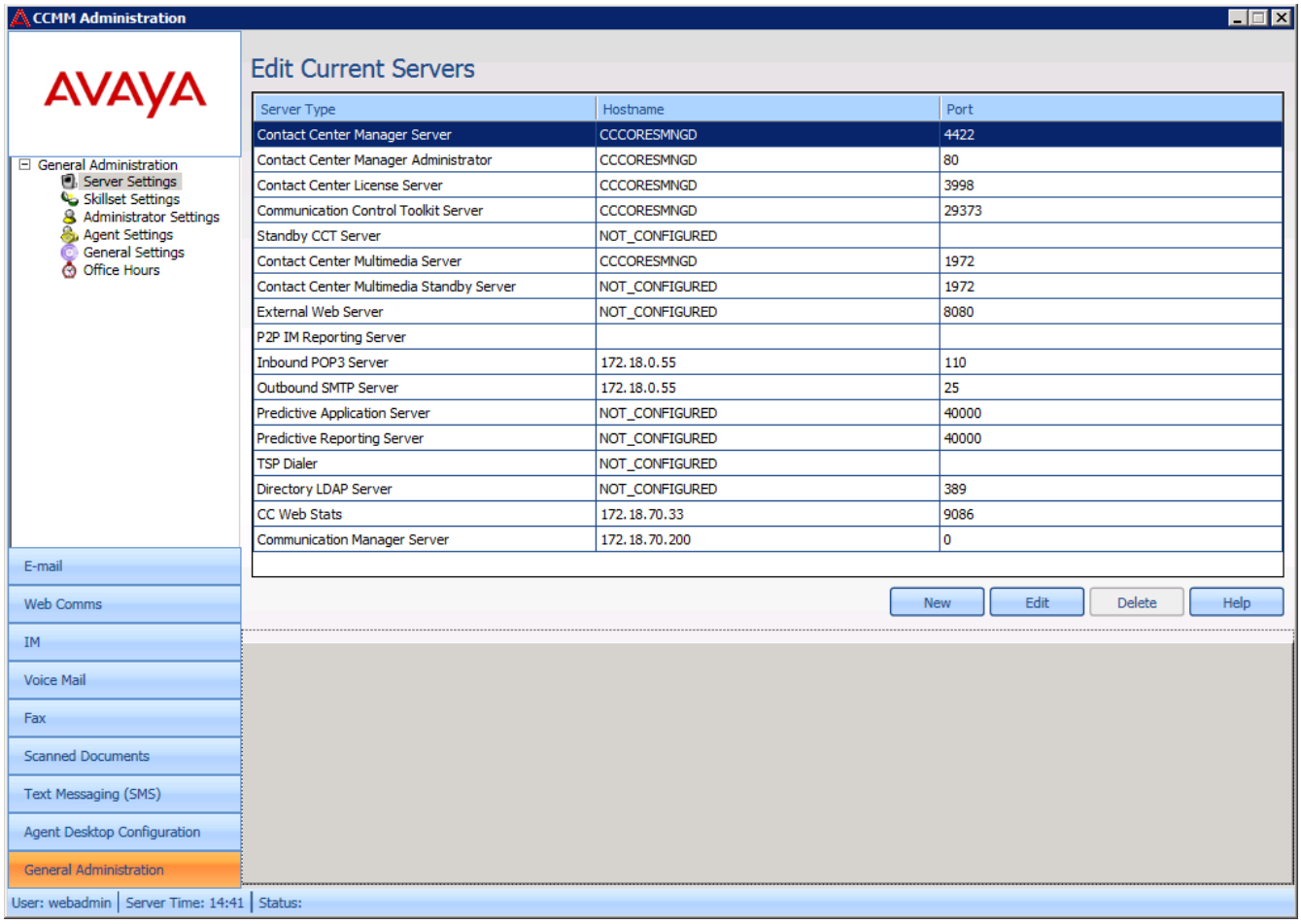
13 On the **Warning** message box, click **Yes**.

14 Select **Communication Control Toolkit Server** and click **Edit**.

15 In the **Server Name** box, type the High Availability Managed name, for example **CCCORESMNGD**.

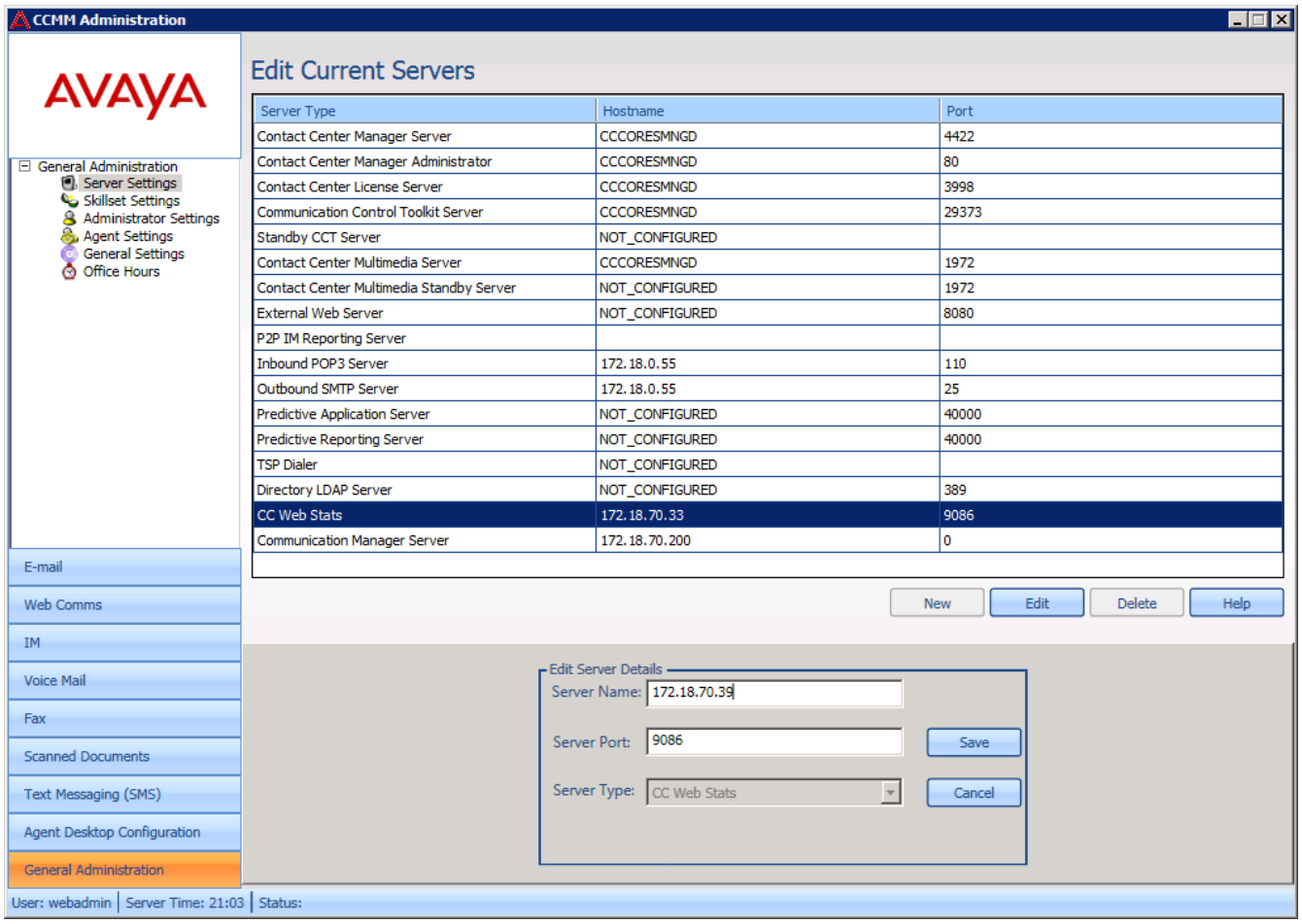
16 Click **Save**.

17 On the **Warning** message box, click **Yes**.



18 Select **CC Web Stats** and click **Edit**.

19 In the **Server Name** box, type the High Availability Managed IP address, for example **172.18.70.39**.



20 Click **Save**.

21 On the **Warning** message box, click **Yes**.

--End--

Configuring e-mail attachment file locations

Update the locations for inbound and outbound e-mail attachments. Update the locations to use the Managed IP address of the CCMM HA pair.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration **Launchpad**, click **Multimedia**.

2 In the left column, select the Multimedia server on which you want to configure server settings, for example **CCElite_CCMM**.

3 In the right pane, click **Launch Multimedia Client**.

The CCMM Administration Tool opens.

4 In the left column, select **E-mail**, **General Settings**.

5 Under **Attachment Files**, in the **Inbound URL** box, type the URL for files attached to inbound e-mail messages in the format http://<Managed IP address>/path, for example **http://172.18.70.39/inboundattachment**.

6 Under **Attachment Files**, in the **Outbound URL** box, type the URL for files attached to outbound e-mail messages in the format http://<Managed IP address>/path, for example **http://172.18.70.39/outboundattachment**.

7 Click **Save**.

--End--

Agent Desktop client software installation for High Availability

Agent Desktop uses Microsoft .NET Framework 3.5 Click Once Deployment technology, which means that you can install and start the application by entering a URL address in Windows Explorer or Internet Explorer. This also means that Agent Desktop clients installed using a URL with the Active server continue to work if you enter a URL with the Contact Center High Availability Managed name.

However, in a High Availability (HA) solution, Agent Desktop clients installed using a URL with the Active server name do not download updates from the Contact Center if it is running on the Standby server. Therefore, uninstall all clients that you installed before commissioning HA, and reinstall them using a a URL with the Contact Center High Availability Managed name.

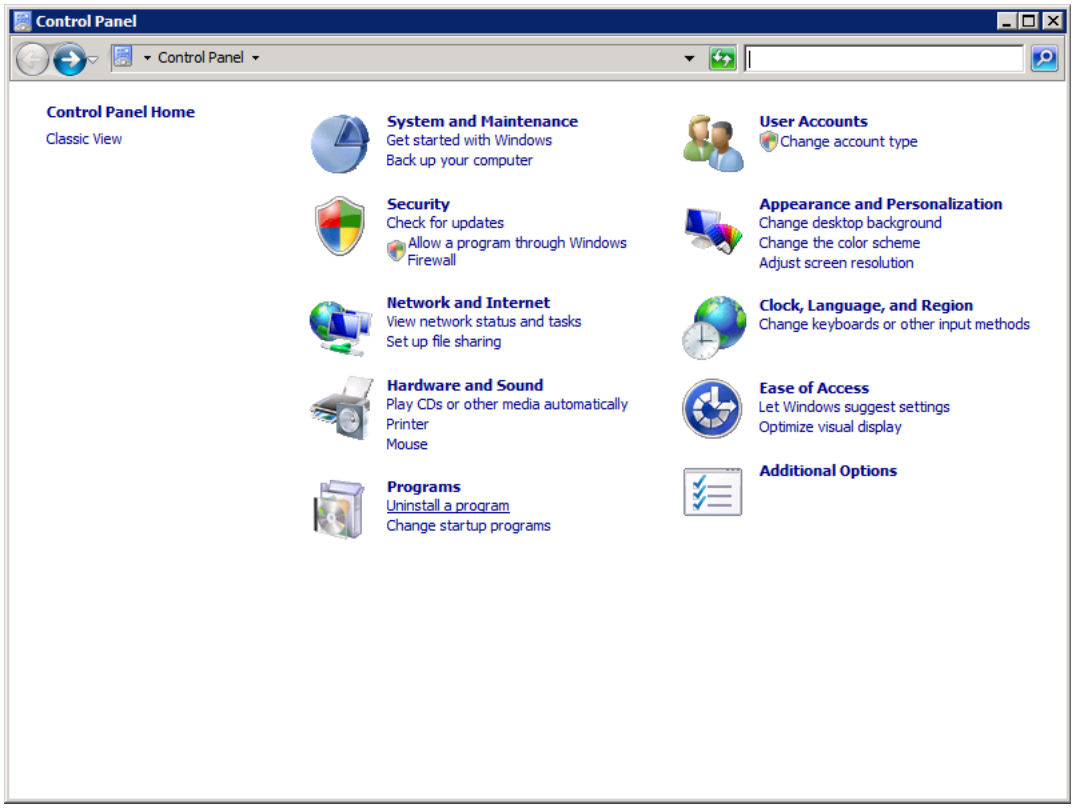
Uninstalling Agent Desktop

Use this procedure to uninstall Agent Desktop from a desktop computer which you installed before configuring HA.

Attention: If many Agent Desktop users share the desktop computer, each one has to separately uninstall the application. The .NET Click-Once Deployment technology creates a separate instance of the application for each user who accesses Agent Desktop from the computer.

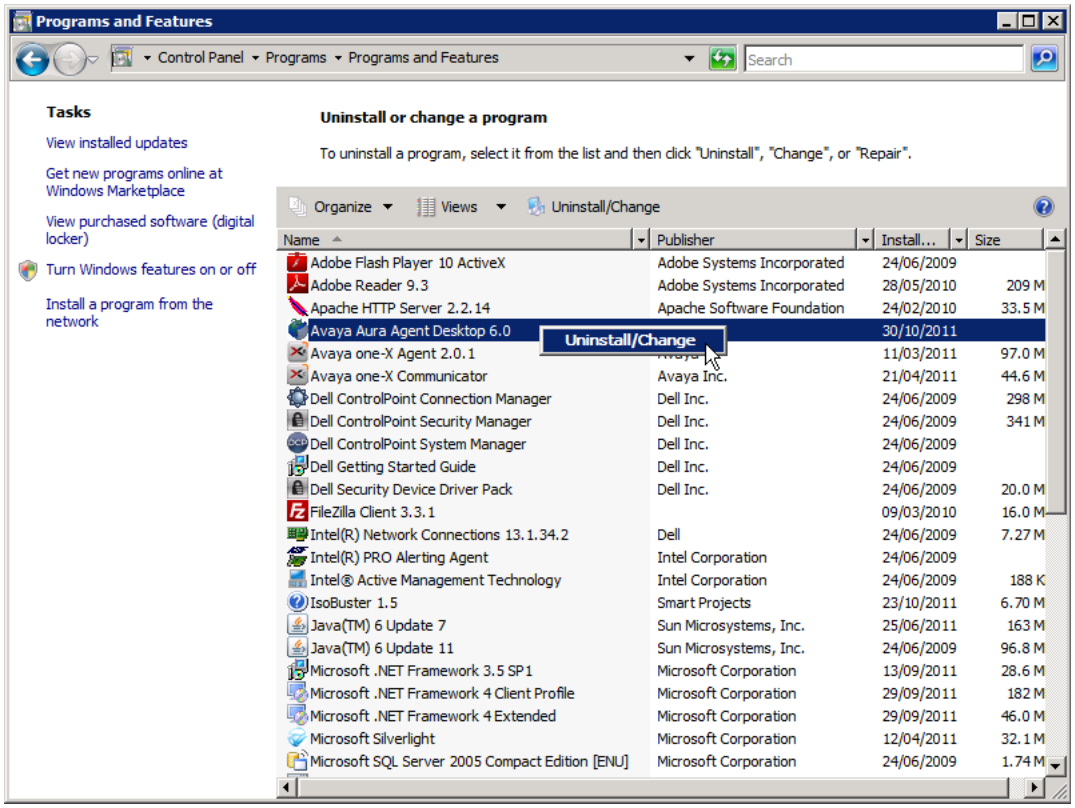
Procedure steps

Step	Action
1	Log on to the desktop computer using the agent's domain username and password, for example **CCAgentOne**, **AG1_pass~2**.
2	Select **Start, Settings, Control Panel**.
3	On the **Control Panel**, under **Programs**, select **Uninstall a Program**.

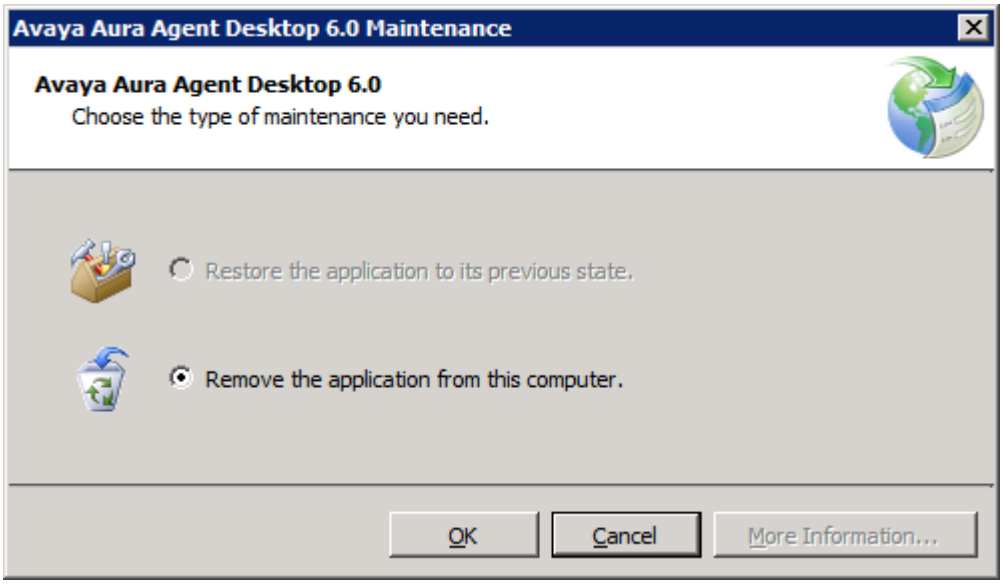


4 On the **Programs and Features** window, scroll down to **Avaya Aura Agent Desktop 6.0**.

5 Right-click **Avaya Aura Agent Desktop 6.0**, and select **Uninstall/Change**.



6 On the **Avaya Aura Agent Desktop 6.0**, select **Remove the application from this computer**, and click **OK**.



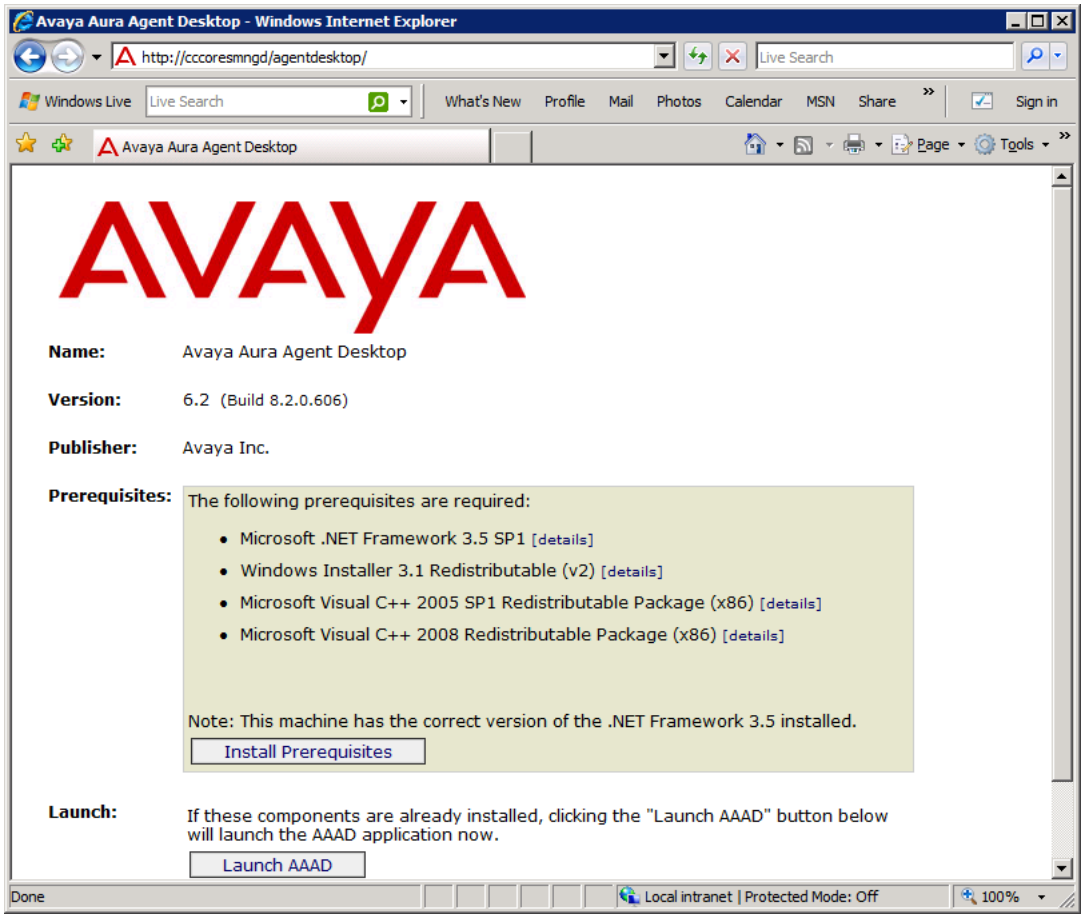
--End--

Installing the Agent Desktop client software using the HA Managed name

Use a URL with the HA managed name to reinstall the Agent Desktop software. This ensures that Agent Desktop downloads any software updates applied when Contact Center is running on the Standby server.

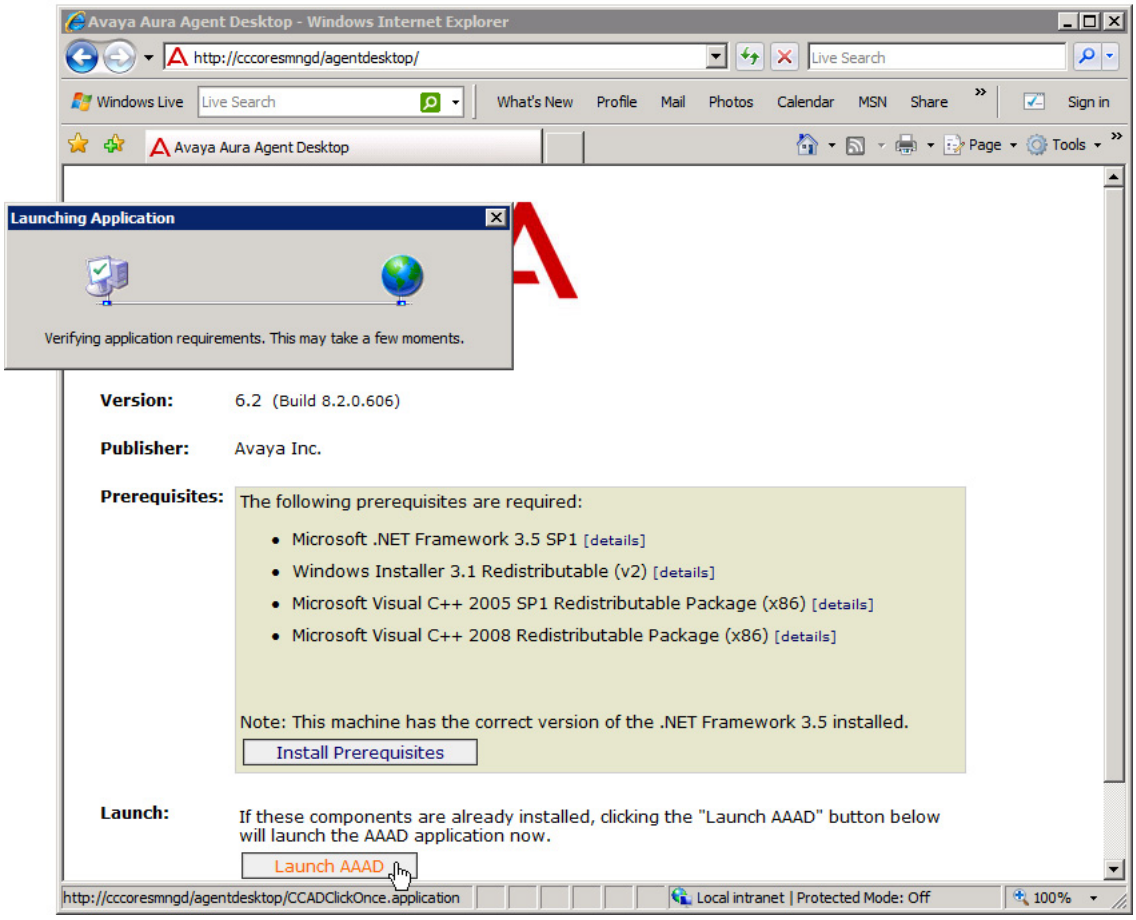
Procedure steps

Step	Action
1	Log on to the desktop computer using the agent's domain username and password, for example **CCAgentOne**, **AG1_pass~2**.
2	On the client computer, start Internet Explorer.
3	In Internet Explorer, in the **Address** box, type the link to the installer on the Multimedia server in the form **http://<HA Managed name>/agentdesktop**, for example **http://cccoresmngd/agentdesktop**, and press **Enter**.

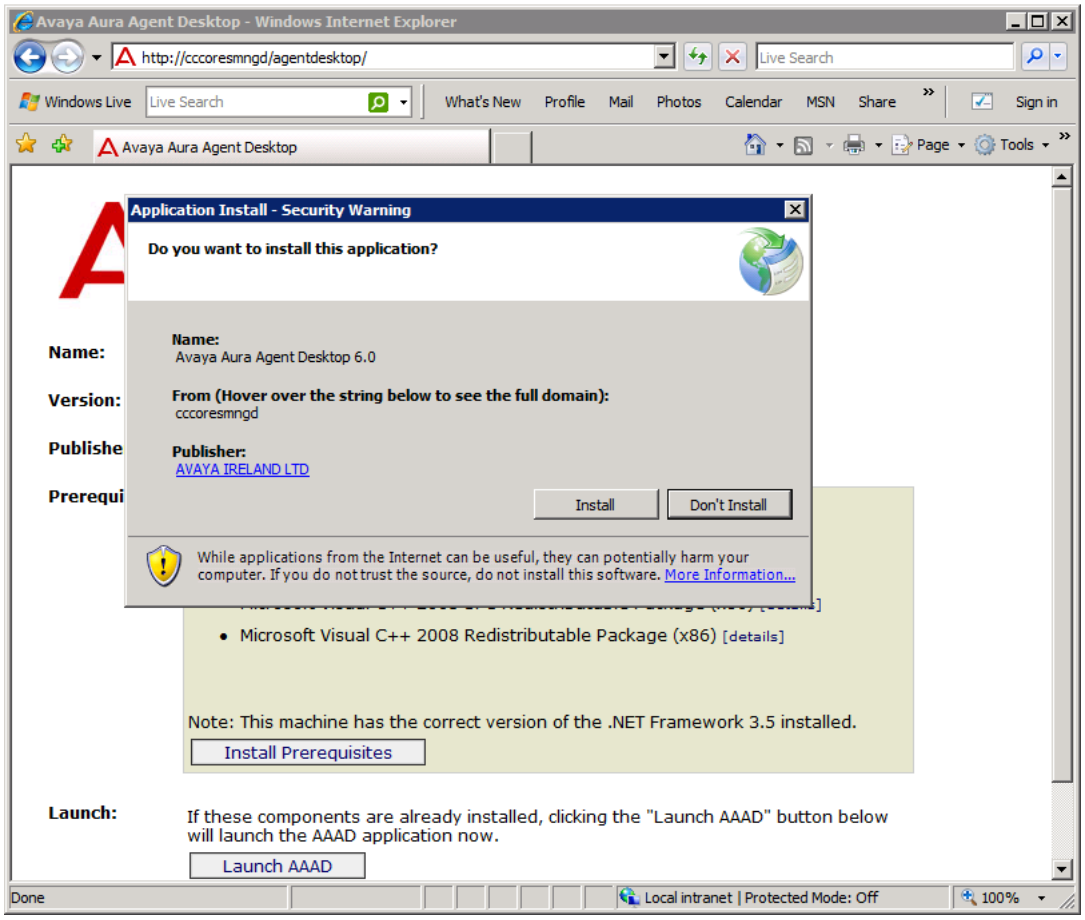


4 On the **Avaya Aura Agent Desktop** web page, select **Launch AAAD**.

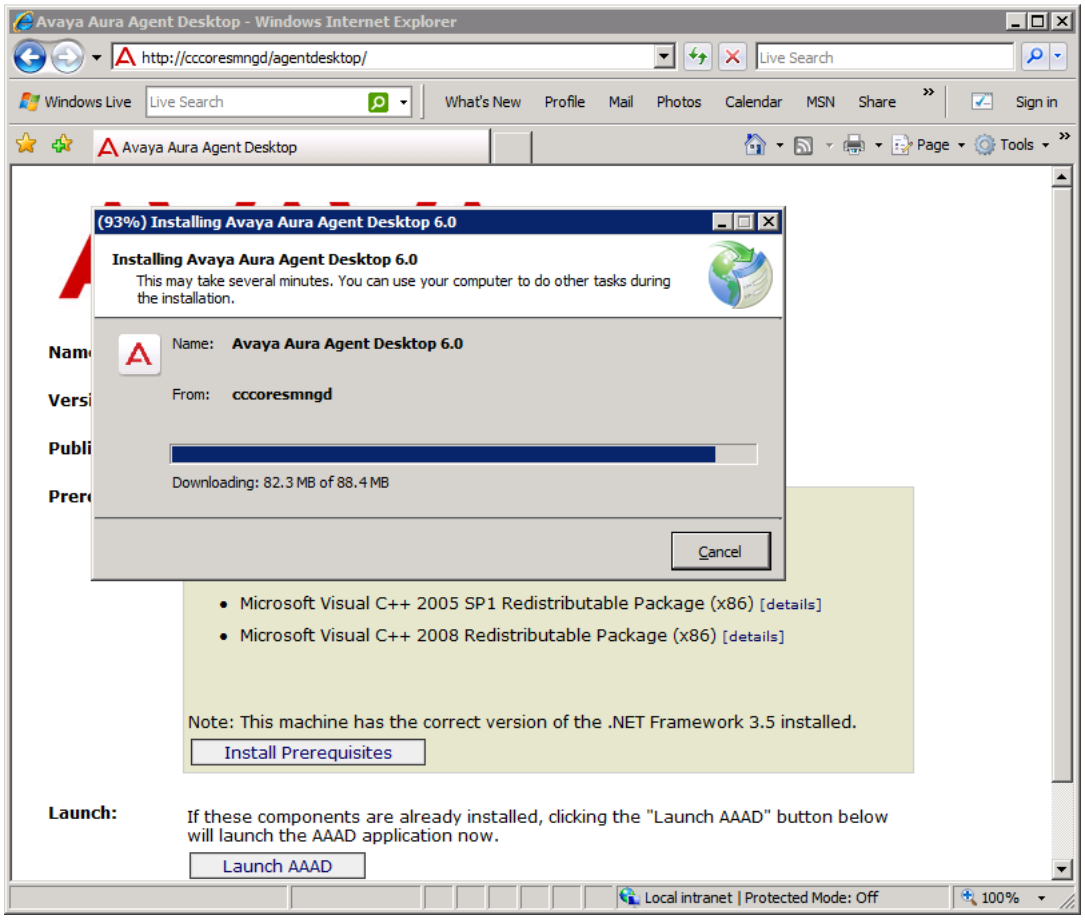
The installer displays the Launching Application dialog while it checks the application prerequisites.



5 On the **Application Install - Security Warning** dialog, select **Install**.

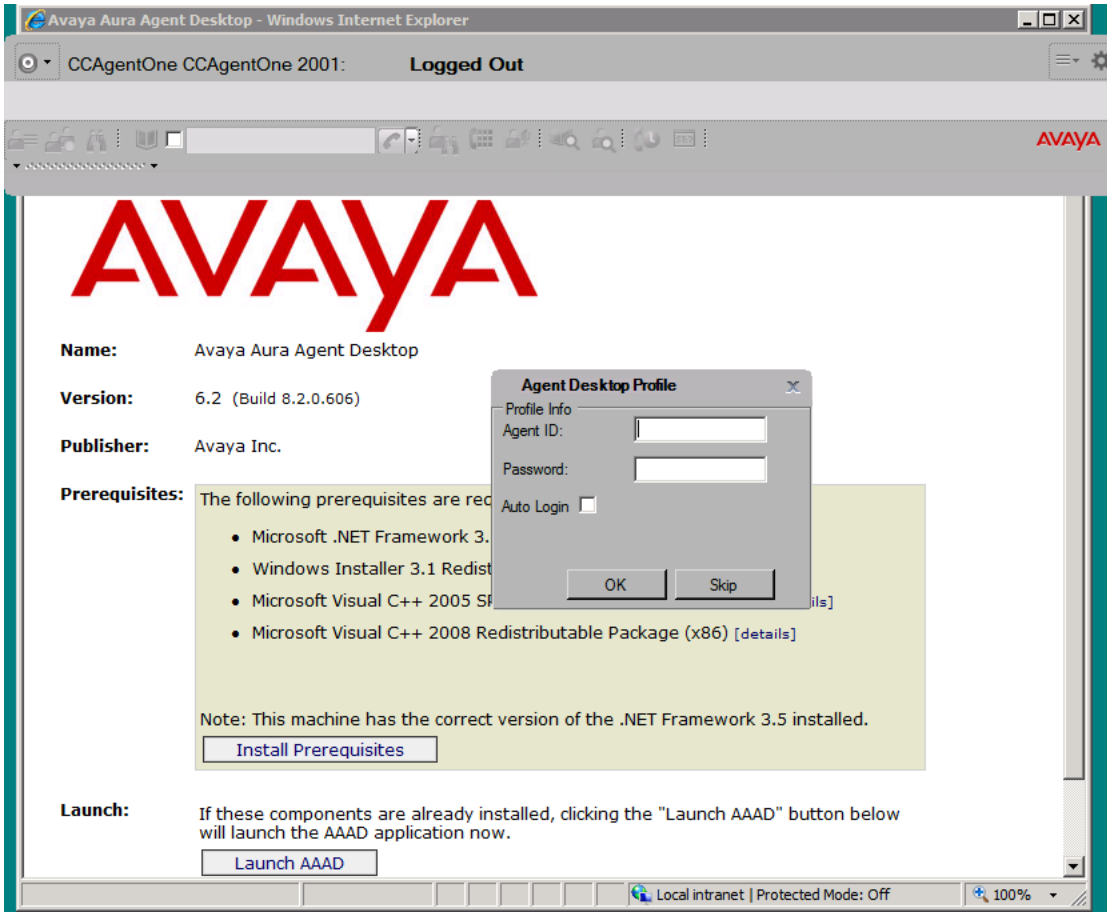


The installer displays a dialog showing the progress of the client installation.



When the installation is complete, Agent Desktop initializes and starts.

6 In the **Agent Desktop Profile** dialog, enter the CCMM login ID and password for the agent, for example **2001**, **2001**.

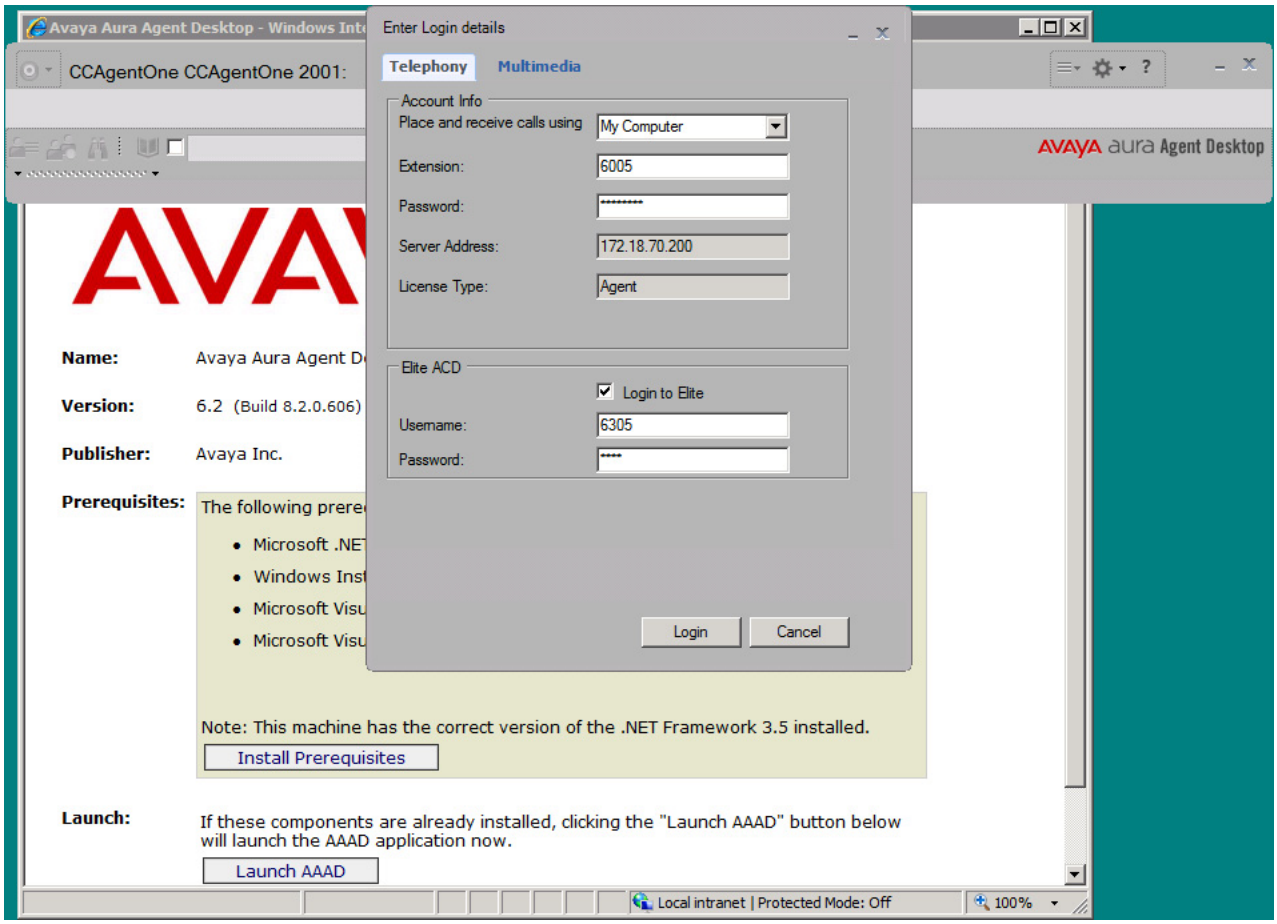


7 Click **OK**.

8 On the Agent Desktop Telephony Toolbar, from the **Status** list, select **Login**.

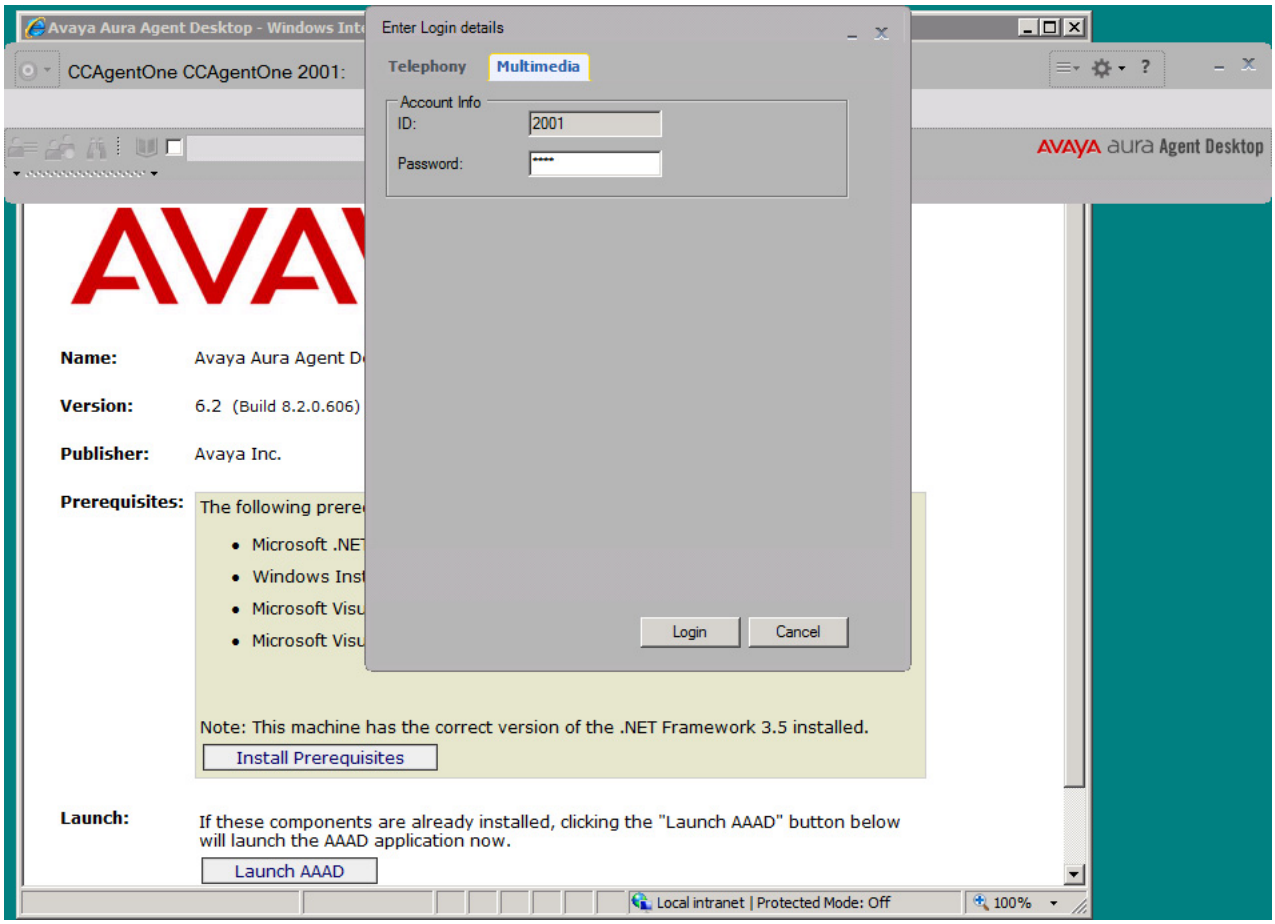


*Agent Desktop displays the **Enter Login details** dialog, pre-populated with the settings from the agent's default profile.*



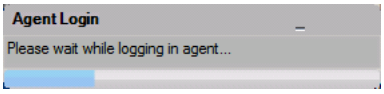
9 Click **Multimedia**.

10 On the **Multimedia** tab, in the **Password** box, type the Contact Center password for this agent, for example **2001**.



11 Click **Login**.

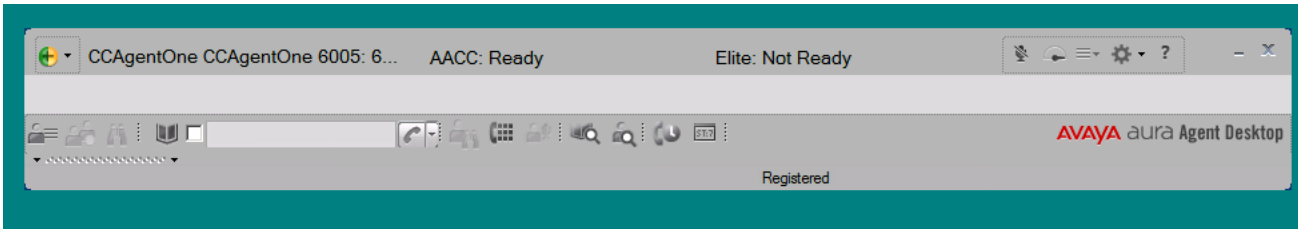
*Agent Desktop displays the **Agent Login** progress window.*



12 On the Agent Desktop Telephony Toolbar, from the **Status** list, select **Go Ready, Multimedia**.



Agent Desktop sets the agent's Avaya Aura® CC status to Ready.



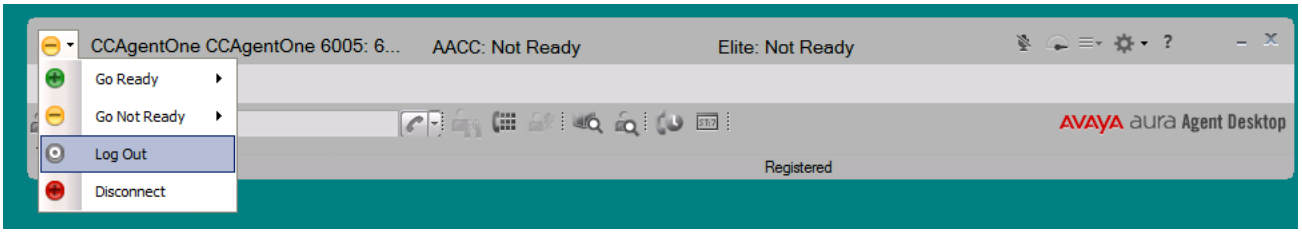
13 On the Agent Desktop Telephony Toolbar, from the **Status** list, select **Go Ready, Voice**.



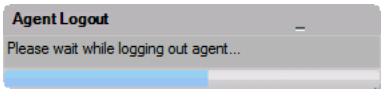
Agent Desktop sets the agent's Elite status to Ready.



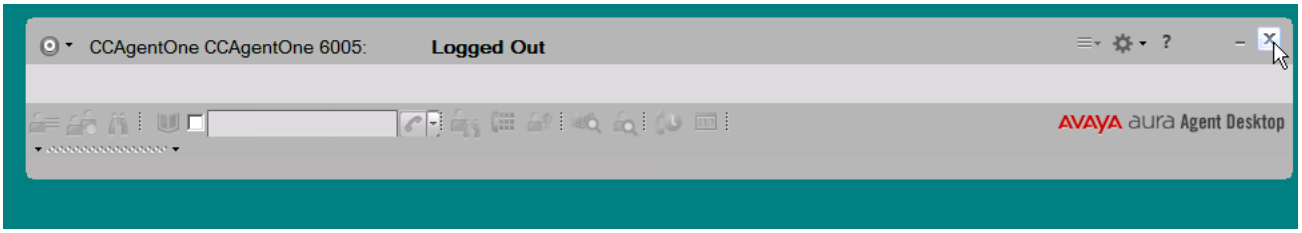
14 On the Agent Desktop Telephony Toolbar, from the **Status** list, select **Logout**.



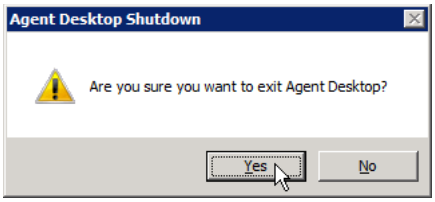
*Agent Desktop displays the **Agent Logout** progress window.*



15 On the Agent Desktop Telephony Toolbar, on the Top Bar, click **Close**.



16 On the Agent Desktop Shutdown dialog, click **Yes**.



--End--

Testing and Troubleshooting High Availability Section

Testing High Availability

Test High Availability (HA) to ensure that a failure on the Active server causes a switchover to the Standby server, and that the Standby server becomes active and processes contacts

In a CCMM complement to Call Center Elite, only the Contact Center elements react to a switchover: the Call Center Elite voice calls are not affected. During a switchover, agents using Agent Desktop receive a message to disconnect. Contact Center re-queues active contacts on which they are working, and when the agents log on to Agent Desktop again, Contact Center presents the contacts to them.

In this example, you use a disconnect of the Contact Center Subnet to force the switchover. Ensure you know which network cable connects to the Active server's Contact Center Subnet Ethernet port.

Logging on to Agent Desktop using the HA Managed name

Log on to Agent Desktop and open an e-mail contact to see the agent experience during a switchover.

Procedure steps

Step	Action
1	Log on to an agent desktop computer using the agent's domain username and password, for example **CCAgentOne**, **AG1_pass~2**.
2	On the client computer, start Internet Explorer.
3	In Internet Explorer, in the **Address** box, type the Agent Desktop URL, for example **http://CCCORESMNGD/agentdesktop**, and press **Enter**.
4	On the **Avaya Aura Agent Desktop** web page, select **Launch AAAD**.
5	In the **Agent Desktop Profile** dialog, enter the CCMM login ID and password for the agent, for example **2001**, **2001**.
6	Click **OK**.
7	On the Agent Desktop Telephony Toolbar, from the **Status** list, select **Login**.
8	Click **Multimedia**.
9	On the **Multimedia** tab, in the **Password** box, type the Contact Center password for this agent, for example **2001**.
10	Click **Login**.

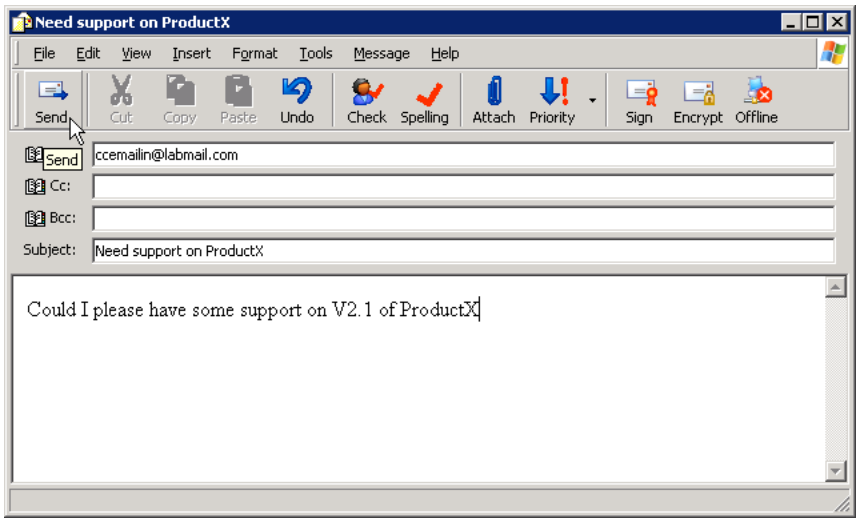
--End--

Sending a test e-mail to the Contact Center e-mail inbox

Send a test e-mail to the Contact Center e-mail inbox to verify the e-mail contact configuration and operation. Review the Multimedia dashboard to check that the e-mail message arrives at the inbox and that Contact Center processes it to create a contact.

Procedure steps

Step	Action
1	Using an e-mail client, create a new e-mail message.
2	In the **To** box, type **ccemailin@labmail.com**.
3	In the **Subject** box, type **Need support on ProductX**.
4	In the e-mail body, type **Could I please have support on V2.1 of ProductX**.



5	Click **Send**.

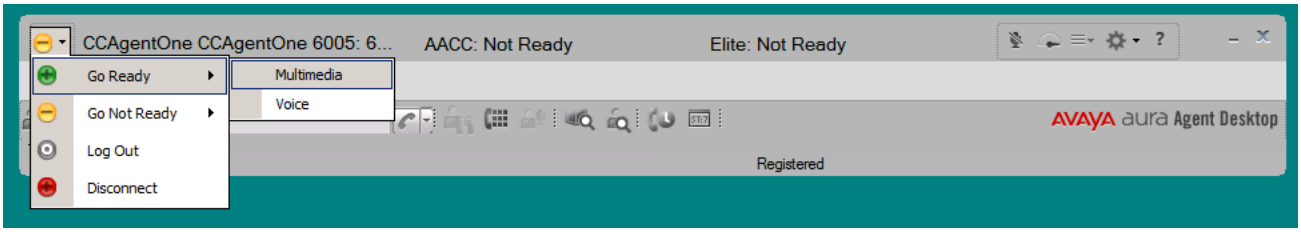
--End--

Making the agent Ready and accepting the e-mail contact

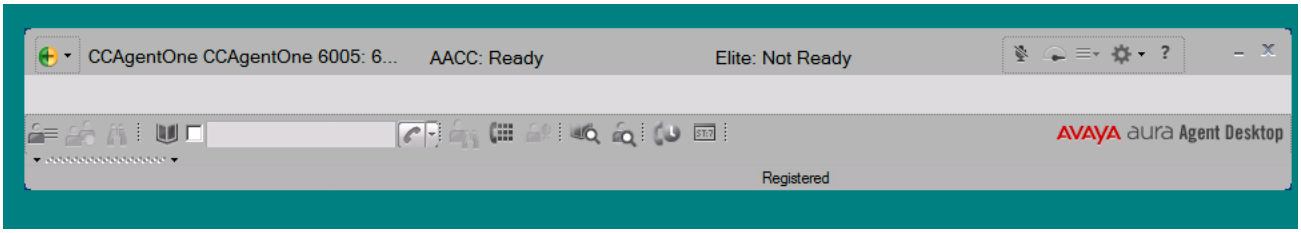
Make the agent ready and accept the e-mail contact that Contact Center offers to the agent.

Procedure steps

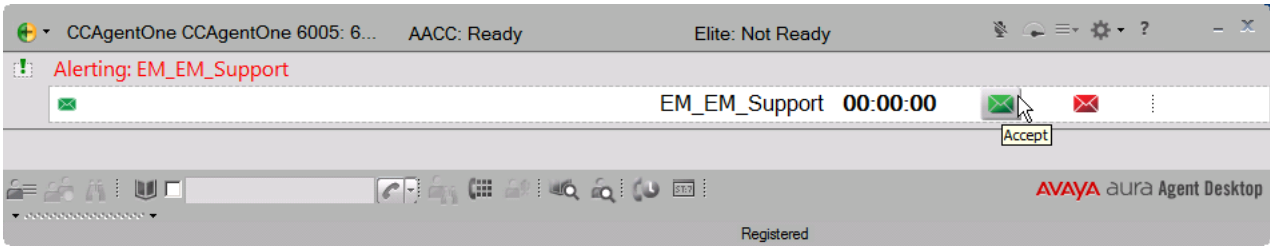
Step	Action
1	On the Agent Desktop Telephony Toolbar, from the **Status** list, select **Go Ready, Multimedia**.



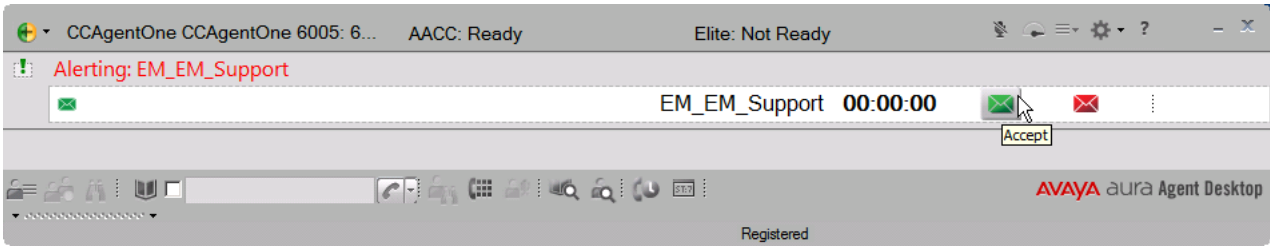
Agent Desktop sets the agent's Avaya Aura® CC status to Ready.



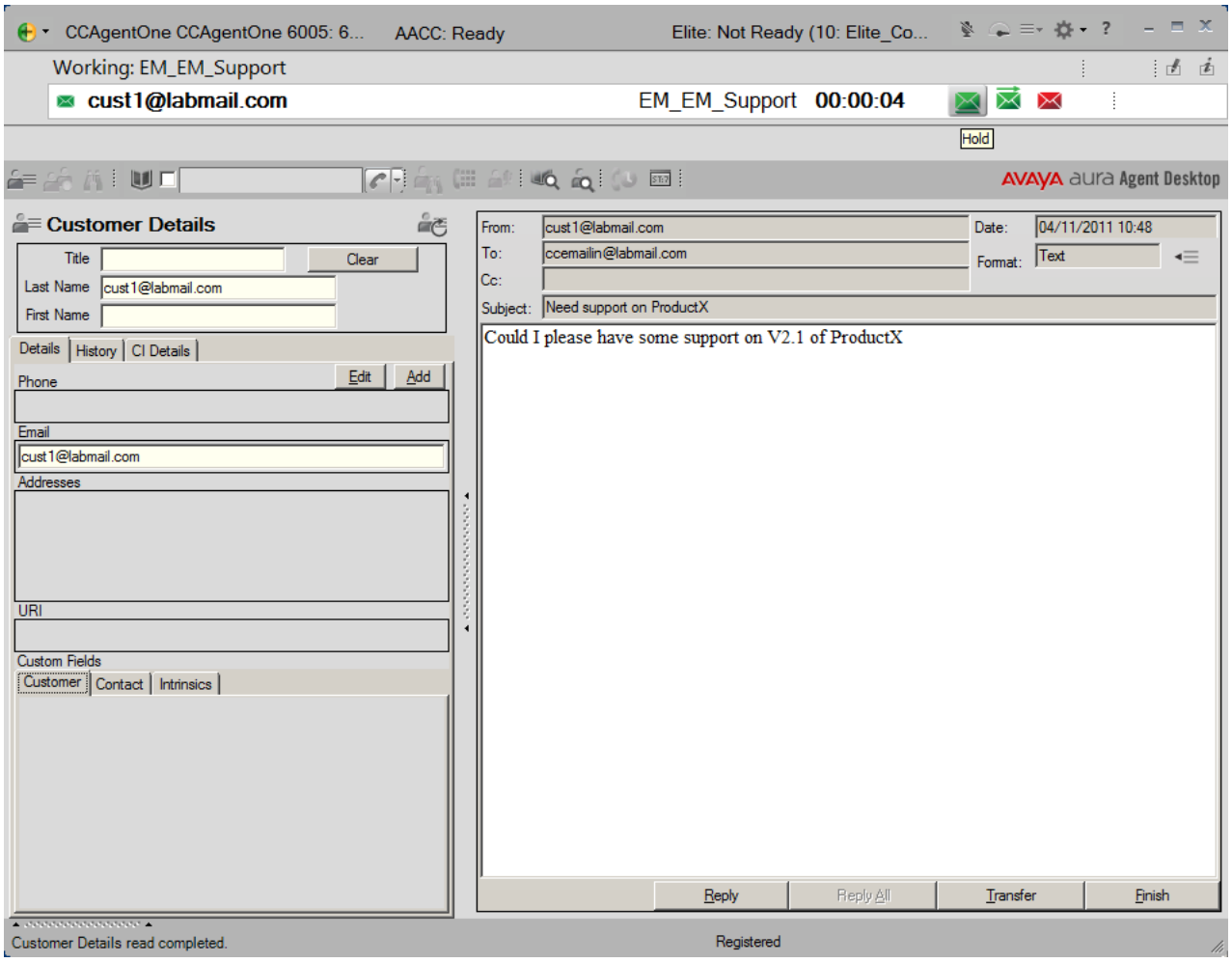
Contact Center routes the e-mail contact to this agent and the Agent Desktop alerts the agent.



2	Click **Accept**.



Agent Desktop displays the contact details.



--End--

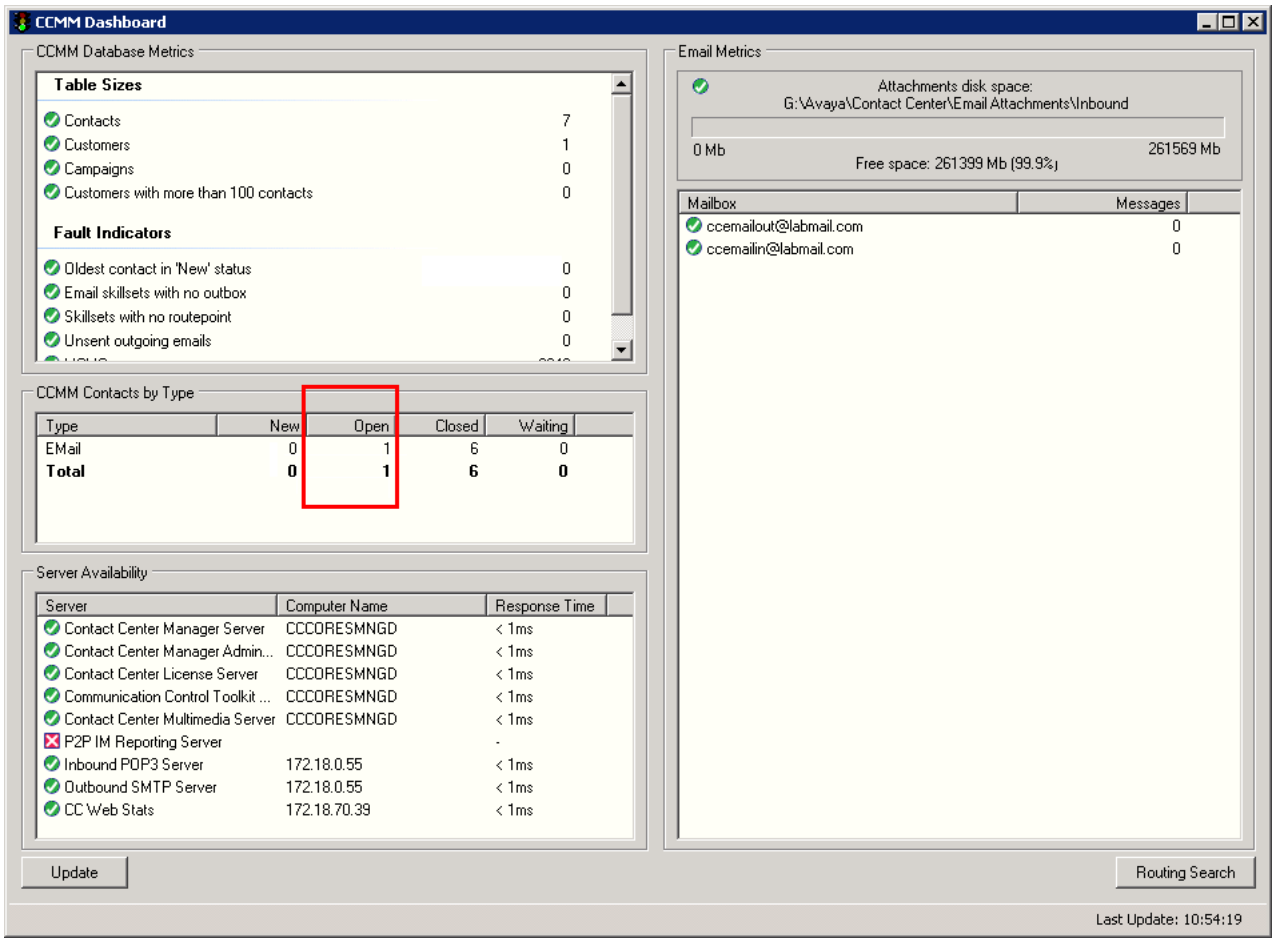
Checking the e-mail contact status in Multimedia Dashboard

Check the Multimedia Dashboard on the Active server to verify the status of the e-mail contact in Contact Center.

Procedure steps

Step	Action
1	Log on to the Active server (for example, **CCCORESONE**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Choose **Start, All Programs, Avaya, Contact Center, Multimedia Server, Multimedia Dashboard**.

3 Verify that the CCMM Contacts by Type pane shows a single open e-mail contact.



--End--

Reviewing the Active server status before switchover

Open the System Control and Monitor Utility and the High Availability Utility on the Active server to review the server status before testing the switchover. Leave these utilities open so that you can monitor the progress of the switchover.

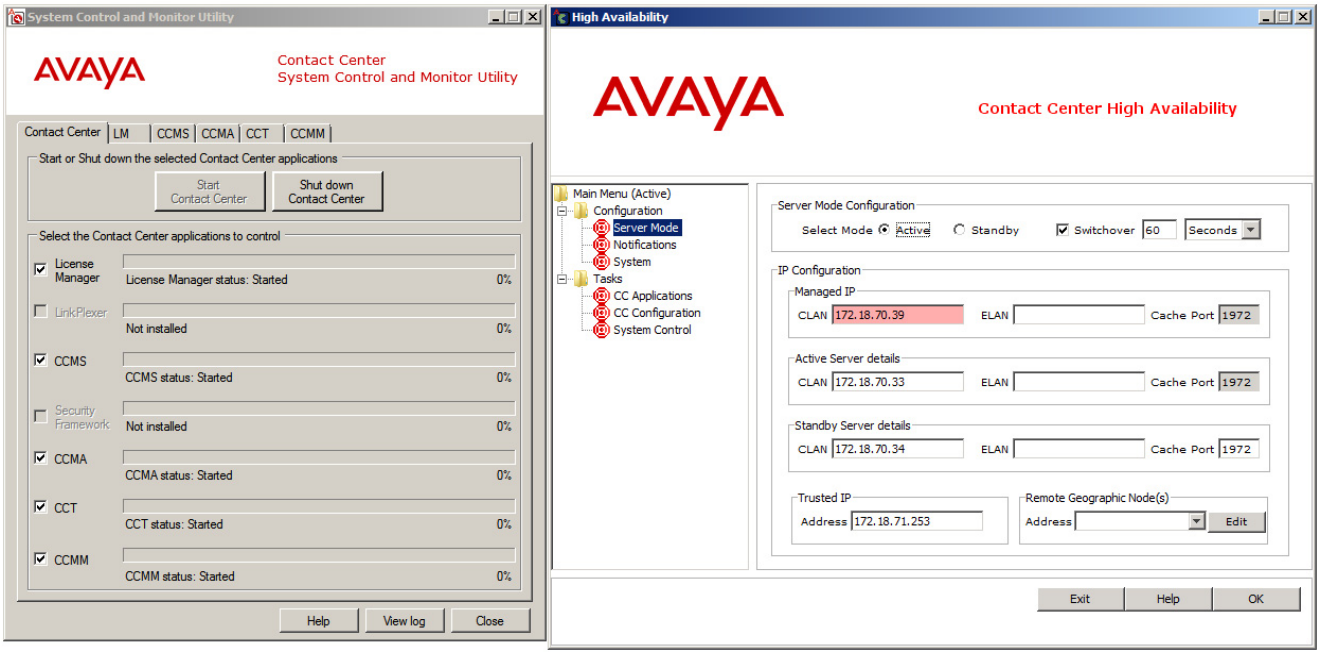
Procedure steps

Step	Action
1	Log on to the Active server (for example, **CCCORESONE**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.

2 Choose **Start, All Programs, Avaya, Contact Center, Common Utilities, System Control and Monitor Utility**.

3 Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Database Utilities**, **High Availability**.

4 In the left pane, select **Server Mode**.



5 Verify that the mode selected is **Active**.

6 Verify that there is a check in select **Switchover** box.

7 Leave both windows open so that you can monitor the switchover progress.

--End--

Reviewing the Standby server status before switchover

Open the System Control and Monitor Utility and the High Availability Utility on the Standby server to review the server status before testing the switchover. Leave these utilities open so that you can monitor the progress of the switchover.

Procedure steps

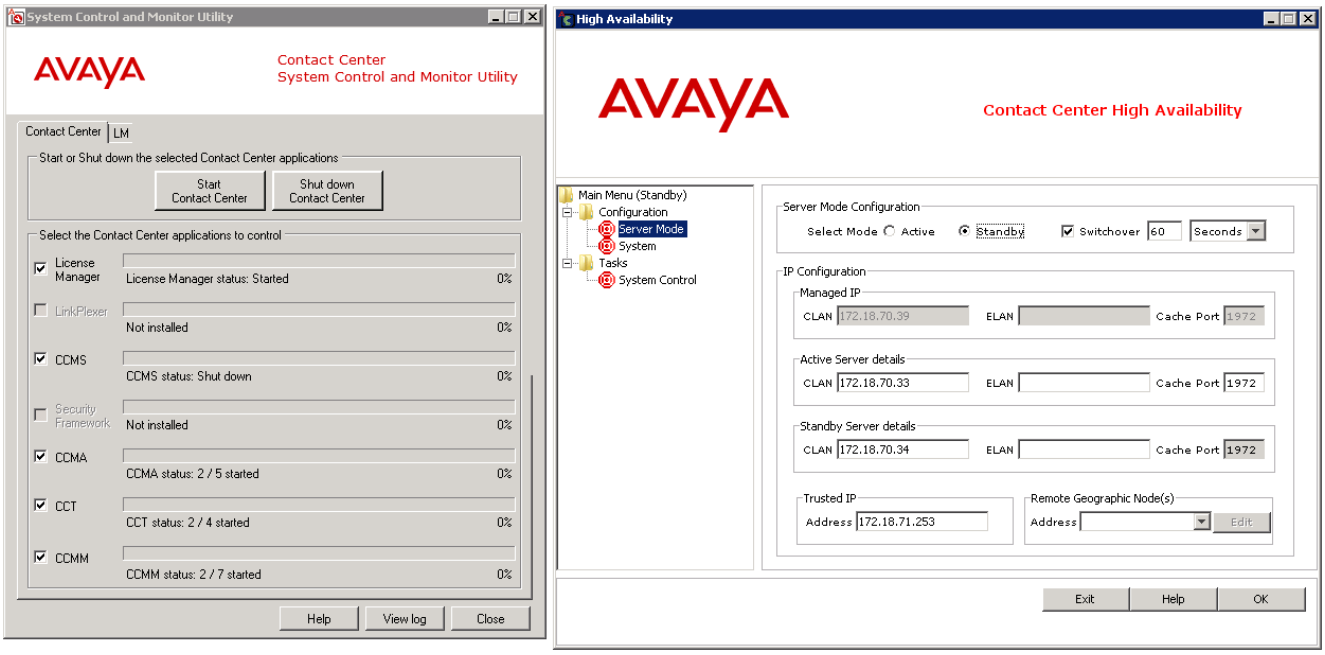
Step	Action
1	Log on to the Standby server (for example, **CCCORESTWO**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.

2 Choose **Start, All Programs, Avaya, Contact Center, Common Utilities, System Control and Monitor Utility**.

3 Verify that the **CCMS Status** is **Shut down**.

4 Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Database Utilities**, **High Availability**.

5 In the left pane, select **Server Mode**.



6 Verify that the mode selected is **Standby**.

7 Verify that there is a check in select **Switchover** box.

8 Leave both windows open so that you can monitor the switchover progress.

--End--

Forcing a switchover and monitoring the results

Force a switchover by removing the Active server Local Area Network (LAN) cable from the Contact Center Subnet Network Interface Card (NIC).

Procedure steps

Step	Action
1	On the Active server, locate the LAN cable in the Contact Center Subnet Network Interface Card (NIC).

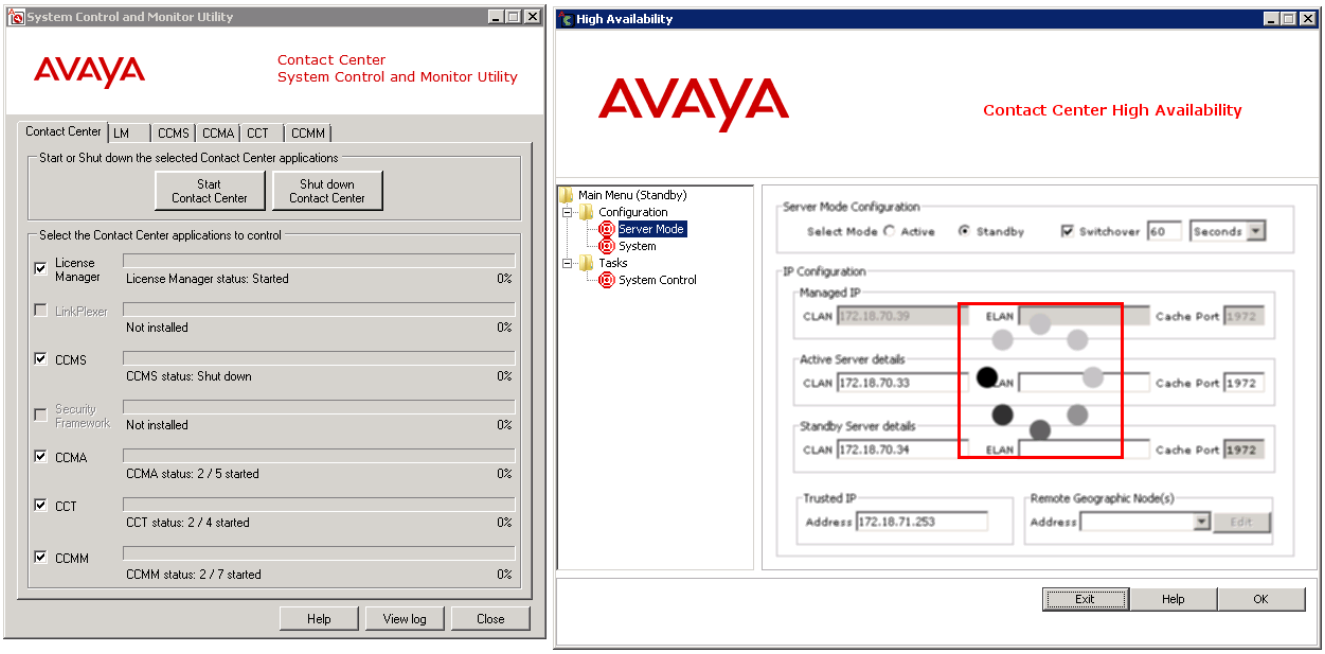
2 Remove the LAN cable from the NIC.

3 Choose **Start, All Programs, Avaya, Contact Center, Common Utilities, System Control and Monitor Utility**.

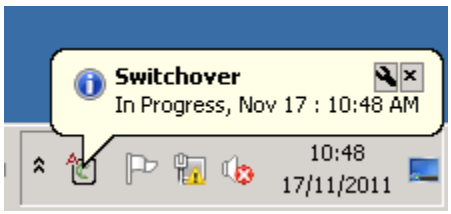
4 Verify that the **CCMS Status** is **Shut down**.

5 Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Database Utilities**, **High Availability**.

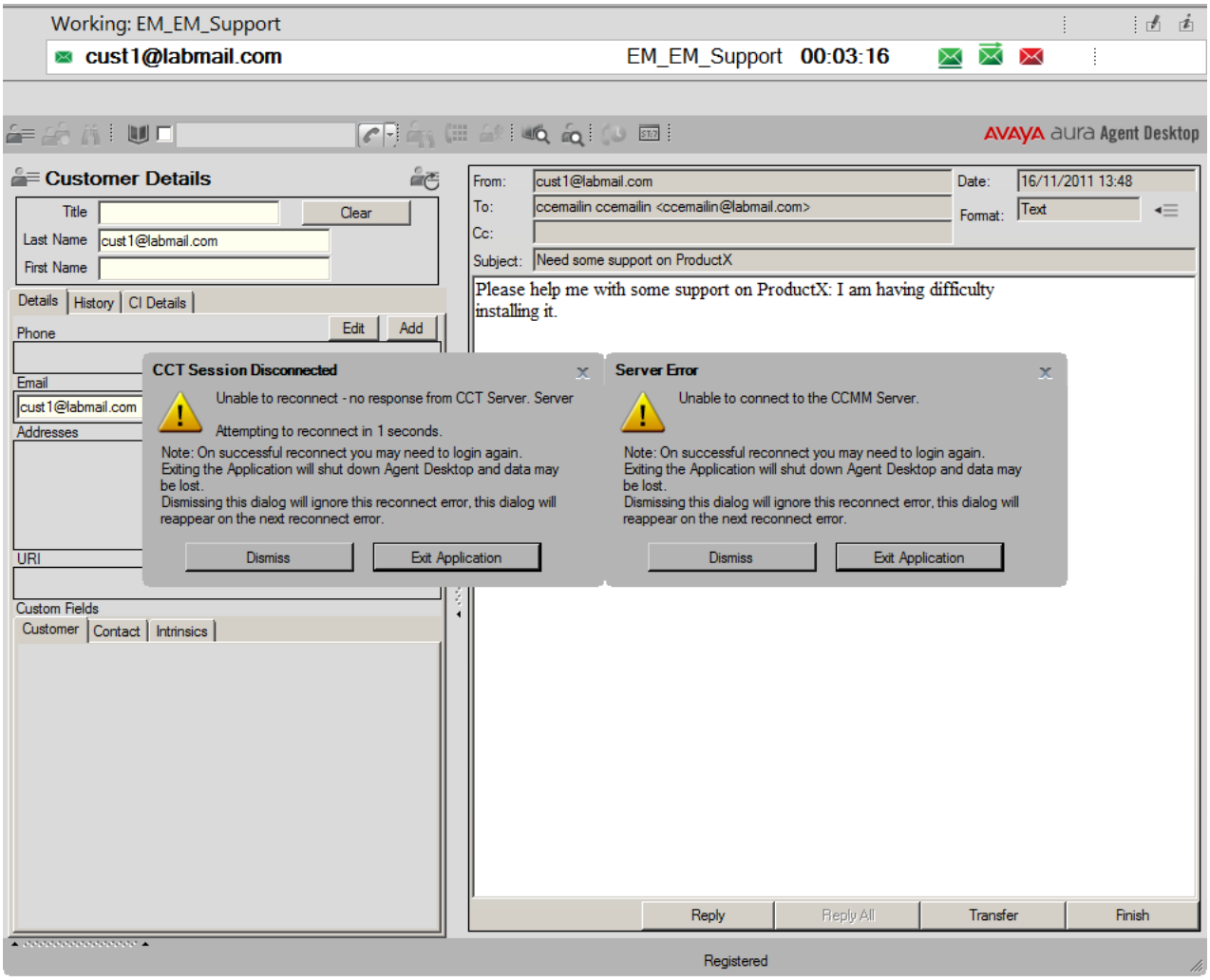
6 On the Standby server, monitor the High Availability Utility. When the switchover starts, a visual indicator appears on the High Availability Utility.



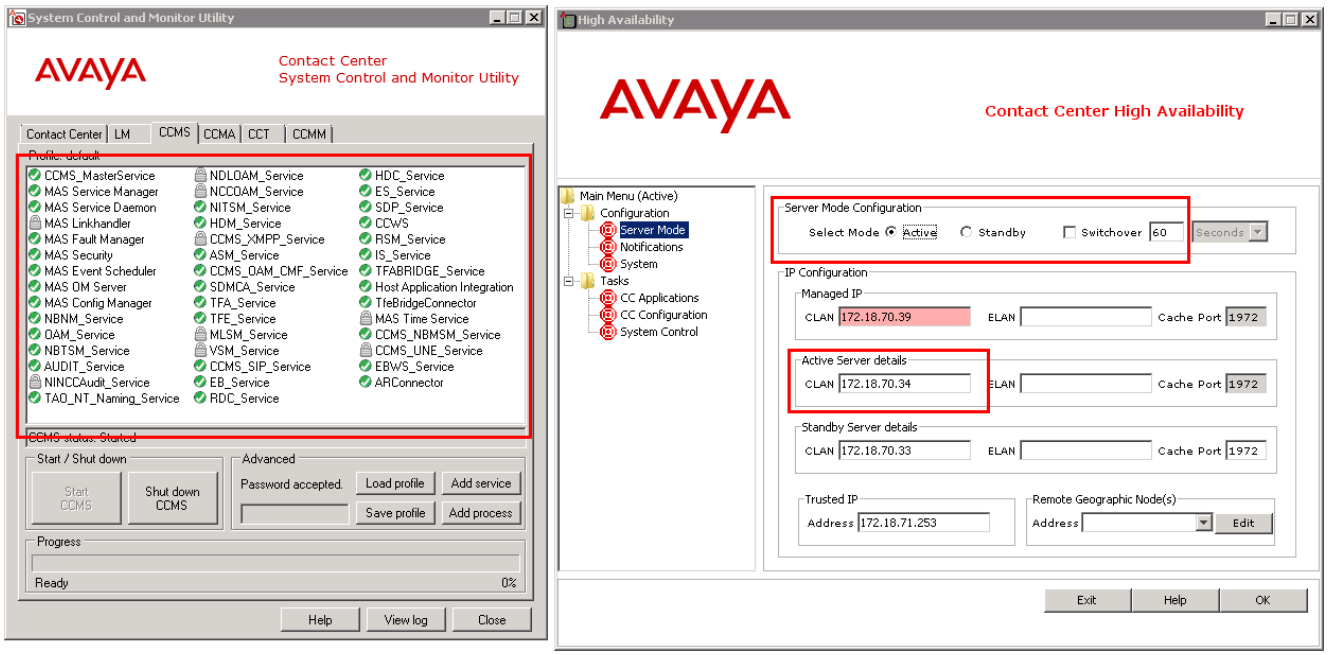
7 On the Standby Server, the Windows Taskbar pops a message indicating that Switchover is in progress.



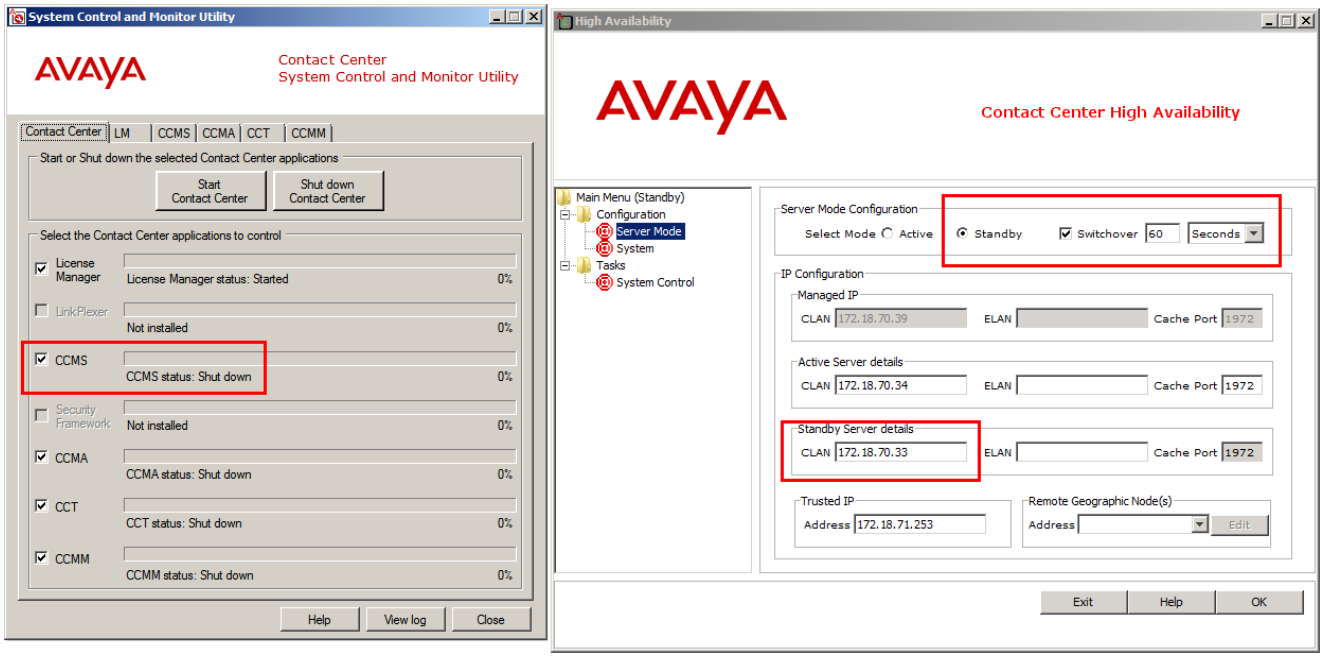
8 Check Agent Desktop: errors appear indicating a loss of connection with the Contact Center server.



9 When the switchover completes, on the Standby Server, look at the SCMU and the HA Utility. Note that all CCMS services are started. Note that the **Server Mode configuration** has changed to **Active** with **Switchover** cleared. Note that the **Active Server Details, CLAN** box now contains the actual IP address of the Standby server, for example **172.18.70.34** the IP address of **CCCORESTWO**.



10 After the switchover completes, on the Active Server, look at the SCMU and the HA Utility. Note that Contact Center has stopped. Note that the **Server Mode configuration** has changed to **Standby** with **Switchover** enabled. Note that the **Standby Server Details, CLAN** box now contains the actual IP address of the Active server, for example **172.18.70.33** the IP address of **CCCORESONE**.



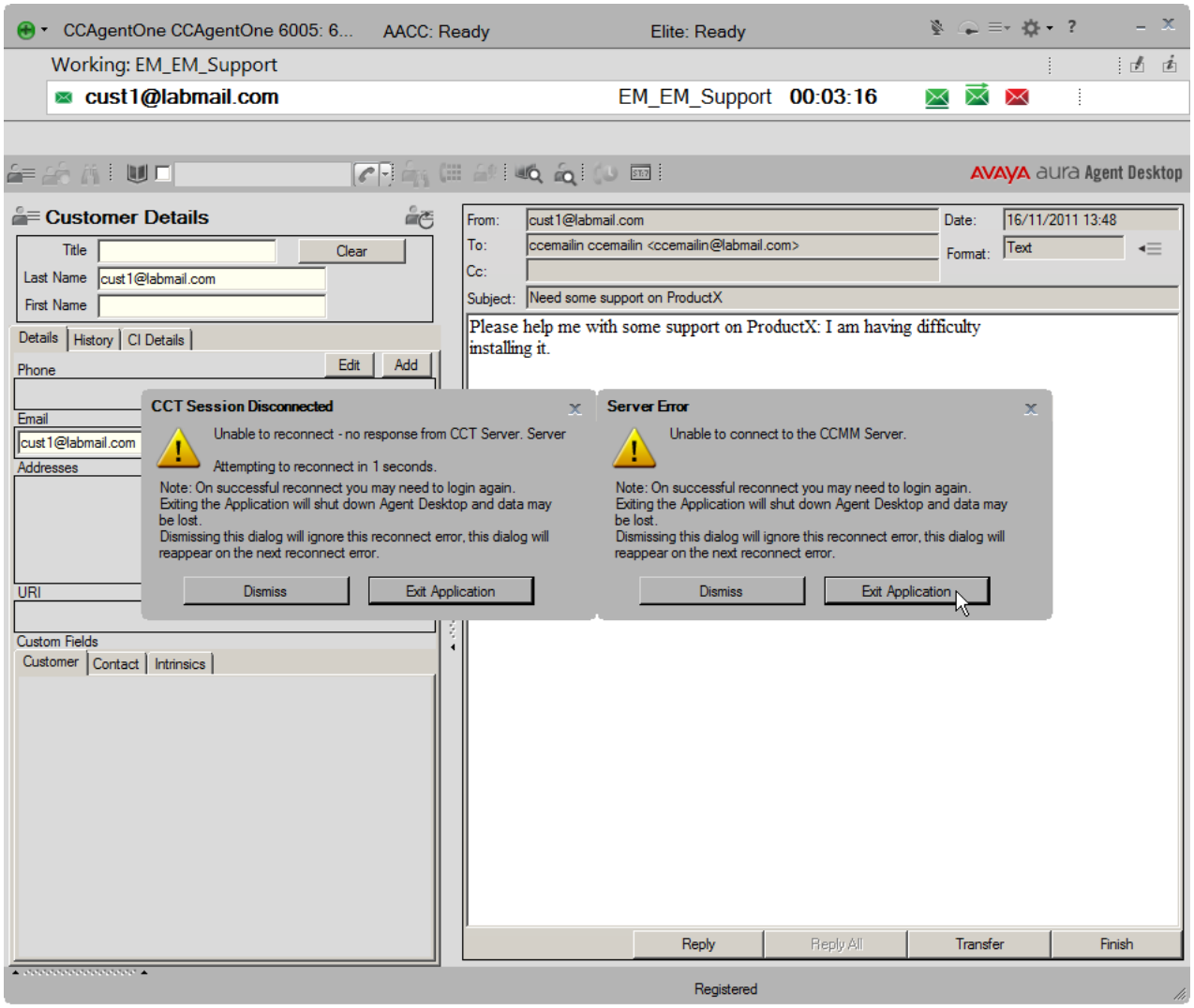
--End--

Closing Agent Desktop

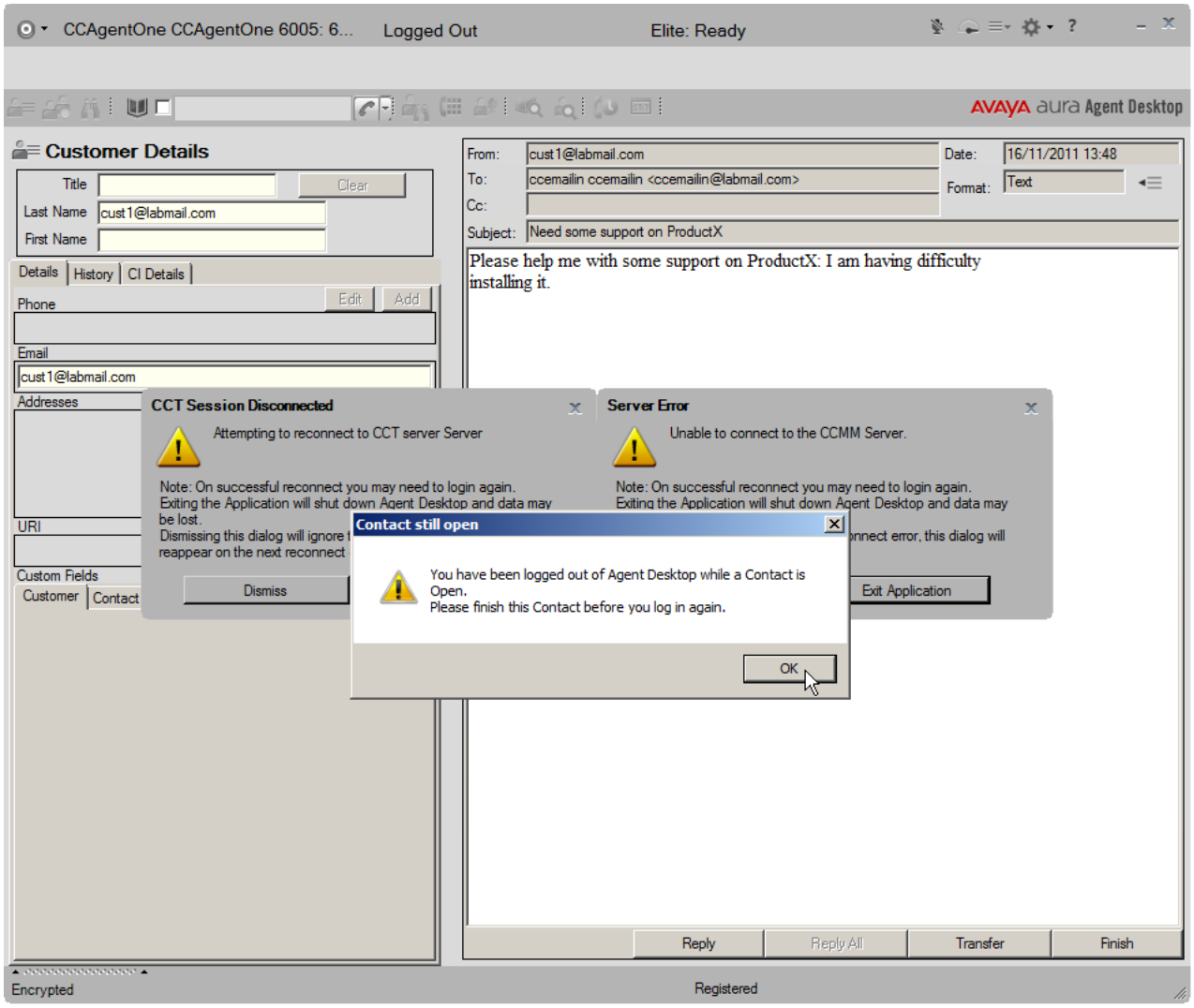
Exit Agent Desktop before logging on to Contact Center again.

Procedure steps

Step	Action
1	On Agent Desktop, on either the **CCT Session Disconnected** or **Server Error** message box, click **Exit Application**.



2 On the **Contact still open** message box, click **OK**.



3 Choose **Start, All Programs, Avaya, Contact Center, Multimedia Server, Multimedia Dashboard**.

4 Verify that the CCMM Contacts by Type pane shows a single new e-mail contact.

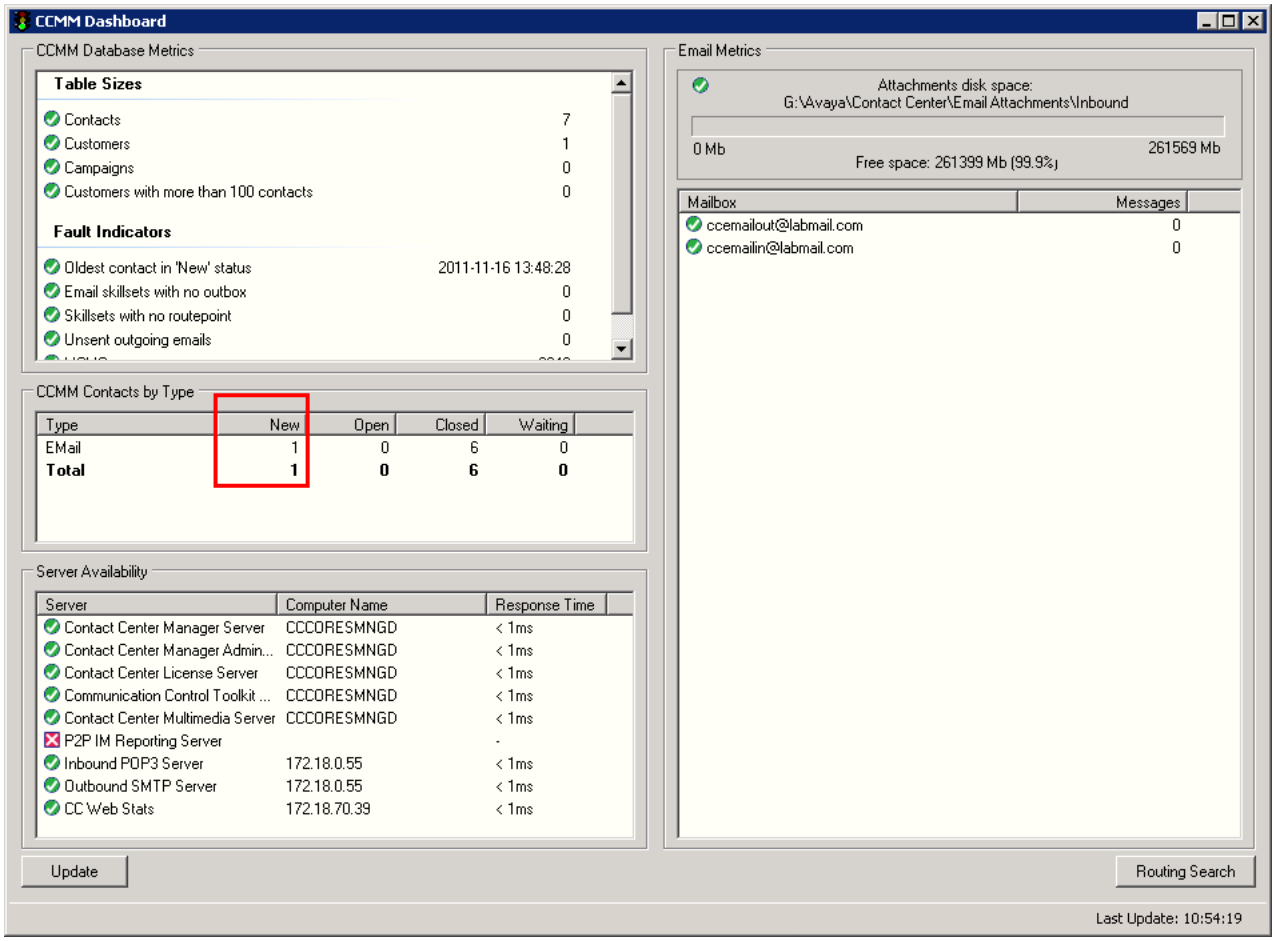
--End--

Checking the e-mail contact status in Multimedia Dashboard after the switchover

Check the Multimedia Dashboard on the Active server to verify that Contact Center has re-queued the e-mail contact that the agent was working on when the switchover occurred.

Procedure steps

Step	Action
1	On the Standby server, choose **Start, All Programs, Avaya, Contact Center, Multimedia Server, Multimedia Dashboard**.
2	Verify that the CCMM Contacts by Type pane shows a single new e-mail contact.



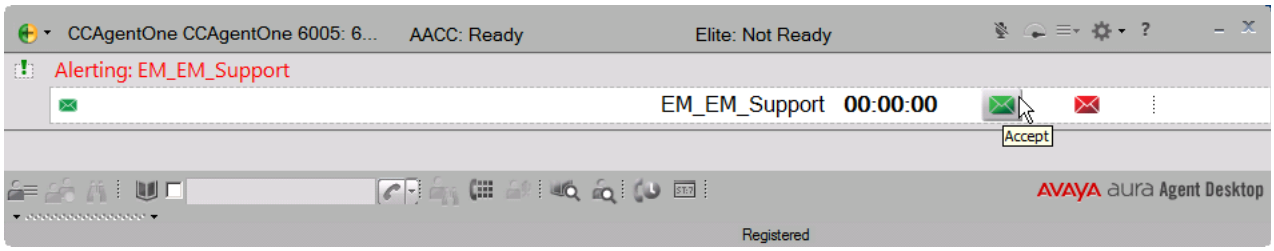
--End--

Logging on the agent and resuming processing of contacts

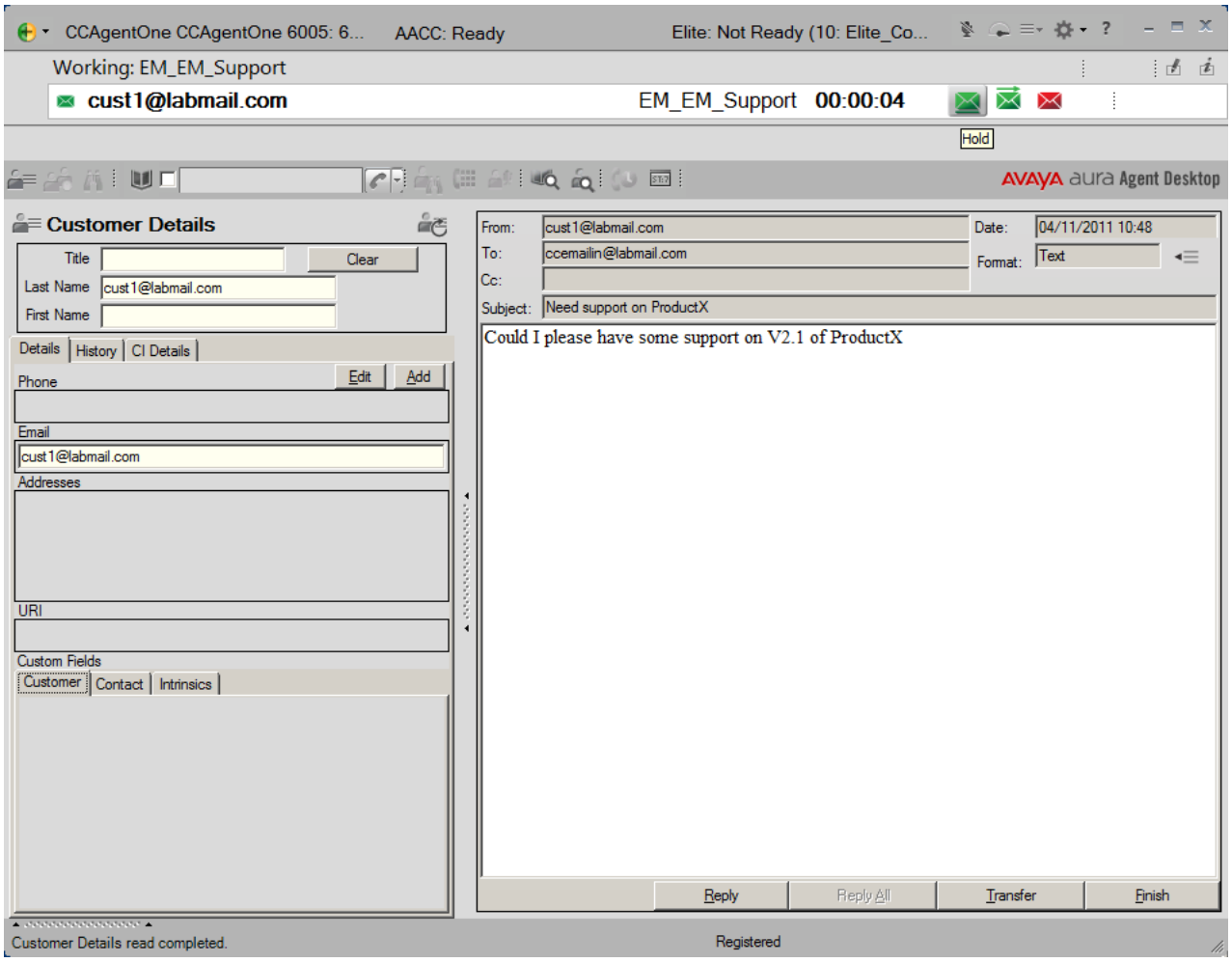
Log the agent on to Agent Desktop and start processing contacts again.

Procedure steps

Step	Action
3	Log on to an agent desktop computer using the agent's domain username and password, for example **CCAgentOne**, **AG1_pass~2**.
4	On the client computer, start Internet Explorer.
5	In Internet Explorer, in the **Address** box, type the Agent Desktop URL, for example **http://cccoresmngd/agentdesktop**, and press **Enter**.
6	On the **Avaya Aura Agent Desktop** web page, select **Launch AAAD**.
7	In the **Agent Desktop Profile** dialog, enter the CCMM login ID and password for the agent, for example **2001**, **2001**.
8	Click **OK**.
9	On the Agent Desktop Telephony Toolbar, from the **Status** list, select **Login**.
10	On the **Enter Login details** dialog, click **Login**.
11	On the Agent Desktop Telephony Toolbar, from the **Status** list, select **Go Ready, Multimedia**. *Agent Desktop sets the agent's Avaya Aura® CC status to Ready.* *Contact Center routes the e-mail contact to this agent and the Agent Desktop alerts the agent.*



12	Click **Accept**. *Agent Desktop displays the contact details.*


CCAgentOne CCAgentOne 6005: 6...
AACC: Ready
Elite: Not Ready (10: Elite_Co...
Working: EM_EM_Support
cust1@labmail.com
EM_EM_Support 00:00:04
Hold
AVAYA aura Agent Desktop
Customer Details
Title
Clear
Last Name
cust1@labmail.com
First Name
Details
History
CI Details
Phone
Edit
Add
Email
cust1@labmail.com
Addresses
URI
Custom Fields
Customer
Contact
Intrinsics
From:
cust1@labmail.com
To:
ccemailin@labmail.com
Cc:
Date:
04/11/2011 10:48
Format:
Text
Subject:
Need support on ProductX
Could I please have some support on V2.1 of ProductX
Reply
Reply All
Transfer
Finish
Customer Details read completed.
Registered

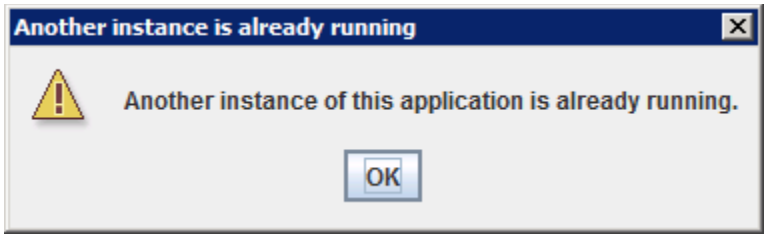
--End--

High Availability and Switchover Troubleshooting

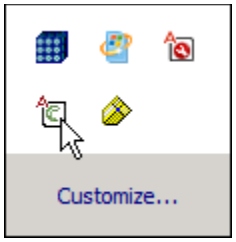
Troubleshoot warnings or errors that you can encounter while configuring High Availability and during switchovers.

Cannot start the HA utility on a server that has had a failure

Troubleshoot if, after a switchover, you cannot start the HA utility on the server that had the failure. When you try to start the HA Utility, the system displays an error that another instance of the application is running. Pressing Atl+Tab does not show any instance of the HA Utility.

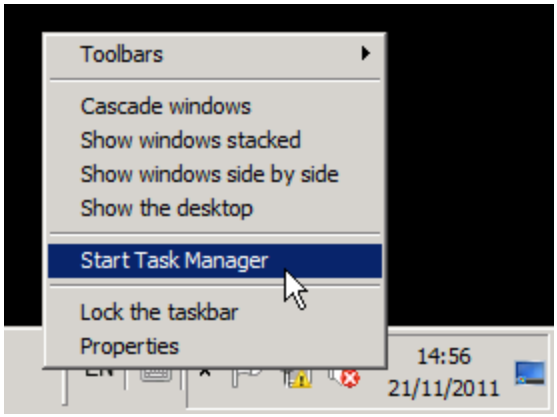


In the Taskbar, you can see the HA icon, but you cannot close it.



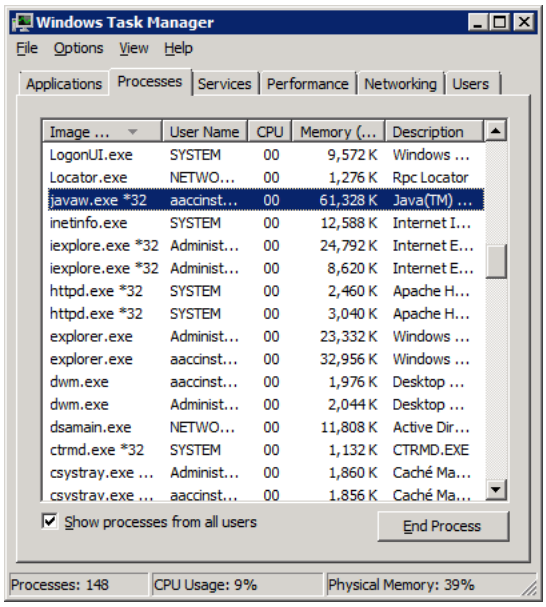
Procedure steps

Step	Action
1	Right-click the Windows Taskbar and select Task Manager.



2 On the **Windows Task Manager** window, select the **Processes** tab.

3 From the list of processes, select **javaw.exe*32**.



4 Click **End Process**.

5 Select **File, Exit Task Manager**.

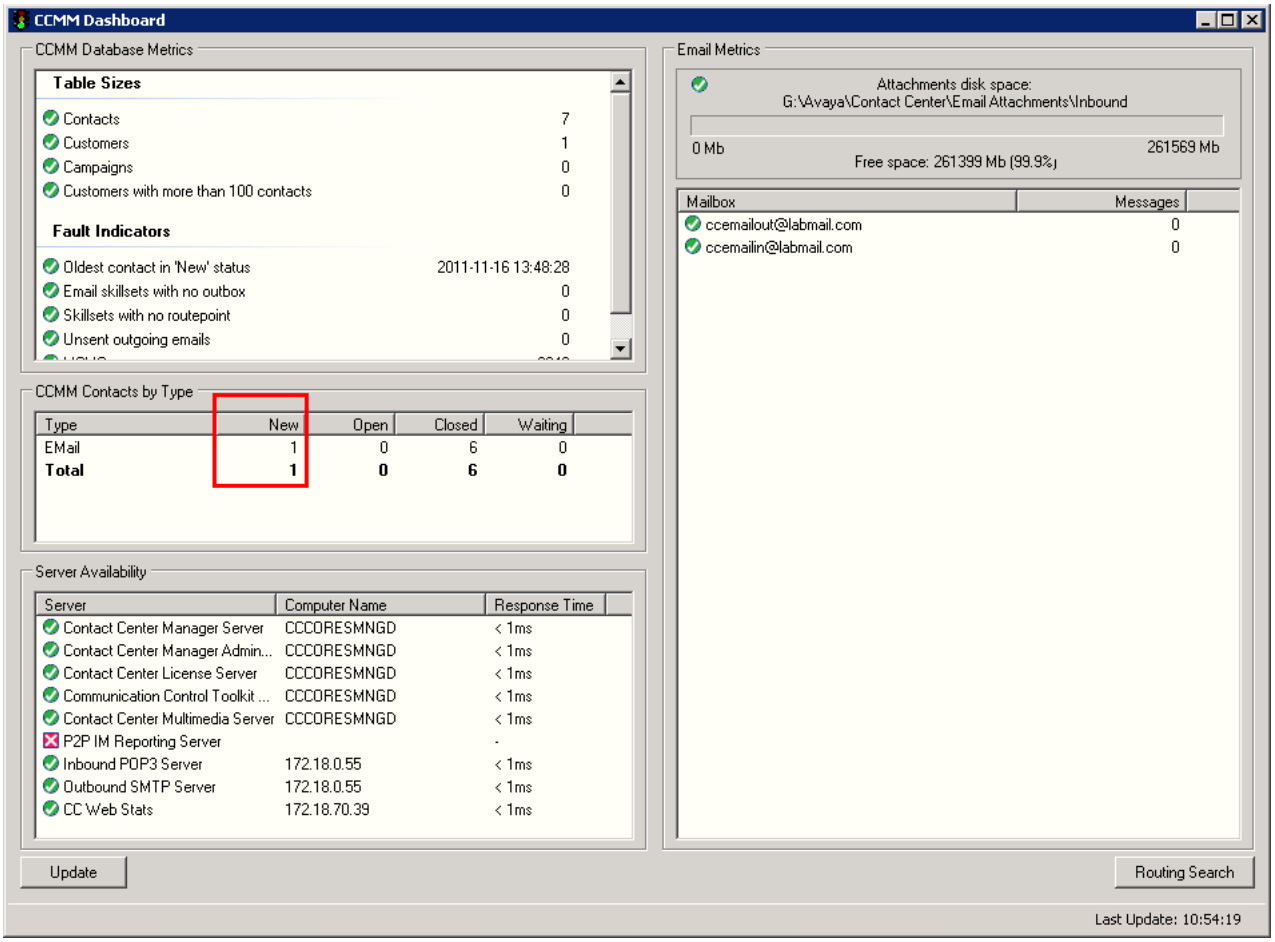
6 Start the HA Utility.

--End--

A Multimedia contact that was active before a switchover does not offer to an agent after switchover

Troubleshoot if, after a switchover, a multimedia contact does not offer to an agent. This issue is usually noticeable when testing HA with just a few contacts at a time.

When the switchover completes, you log an agent on to Agent Desktop and make the agent ready. Contact Center does not present any contacts to the agent, even though the agent was working on an active contact when the switchover occurred. In Multimedia Dashboard, you can see that there are New contacts.



This issue can be caused by a timing mismatch on the start up of certain services on the standby system when it performs the switchover, resulting in a number of stuck contacts. Check the CMF_OAM log for the following error:

```
2011-11-17 10:50:12,275 [Notifier-pool-3-thread-1] ERROR
com.nortelnetworks.portal.cmf.sp.request.SpActiveCreateOpenQContactRequestImpl - execute():caught
exception for request df75653d-2411-4f5a-9cf6-26c0d5d87eb2
com.nortelnetworks.portal.cmf.core.exception.InvalidArgumentException: Error - The
routePointAddress[E-mailsContactsRP] must be in the controlled state to create an OpenQ contact.
providerName[CCMM].
                at
com.nortelnetworks.portal.cmf.sp.request.SpActiveCreateOpenQContactRequestImpl.execute(Unknown Source)
                at
com.nortelnetworks.portal.cmf.sp.request.CmfSpActiveRequestListener.processEntry(Unknown Source)
                at com.nortelnetworks.portal.cmf.core.listener.CmfListener.notify(Unknown Source)
                at com.j_spaces.core.client.NotifyDelegator.notify(NotifyDelegator.java:182)
                at
com.j_spaces.core.client.RemoteEventListenerExporter$TransientDelegator.notify(RemoteEventListenerExpo
rter.java:155)
                at
com.gigaspaces.internal.lrmi.stubs.LRMIRemoteEventListener.notify(LRMIRemoteEventListener.java:96)
                at
com.j_spaces.core.server.processor.RemoteEventBusPacket.notifyListener(RemoteEventBusPacket.java:124)
                at com.gigaspaces.events.SingleNotifyExecutor.execute(SingleNotifyExecutor.java:26)
                at com.j_spaces.core.Notifier.execute(Notifier.java:145)
       at
com.j_spaces.core.server.processor.RemoteEventBusPacket.execute(RemoteEventBusPacket.java:106)
                at com.j_spaces.core.Notifier.dispatch(Notifier.java:69)
                at com.j_spaces.core.Notifier.dispatch(Notifier.java:33)
                at com.j_spaces.kernel.WorkingGroup$TaskWrapper.run(WorkingGroup.java:60)
                at java.util.concurrent.ThreadPoolExecutor$Worker.runTask(Unknown Source)
                at java.util.concurrent.ThreadPoolExecutor$Worker.run(Unknown Source)
                at java.lang.Thread.run(Unknown Source)
```

To release the stuck contacts, send a new Multimedia contact (for example, a new e-mail) to Contact Center.

This situation is unlikely to be noticed on an active Contact Center, as the continuation of new contacts coming into Contact Center automatically releases the stuck contacts.

Procedure steps

Step	Action
1	Send a new contact, which queues to one of the affected agent's skillsets, to Contact Center. For example, send a new e-mail message to one of the inboxes monitored by Multimedia.
2	On Agent Desktop, answer the new contact.
3	When you complete the new contact, the Contact Center services release any stuck contacts.

--End--

A switchover does not occur on the Standby server when the Active fails

Troubleshoot when you test a failure on the Active server, but the Standby server does not initiate a switchover.

There are two main reasons why the Standby server does not initiate a switchover. The first is that the Switchover box is not checked on the Standby server HA Utility. The second is that one of the configurable switchover timers has a time setting that has not expired and thus did not force a switchover.

Procedure steps

Step	Action
1	On the Standby server, open the HA Utility.
2	In the left pane, select **Local Settings**.
3	Check that the **Standby** is selected.
4	Check that **Switchover** is checked.
5	Review the Switchover time and verify that it is not set to an excessively long time.
6	If the failure was a service failure on the Active server, on the Active server, open the HA Utility.
7	In the left pane, select **CC Configuration**.
8	In **Service Monitor Configuration** list, find the service or services that failed.
9	Check whether the **Monitor** and **Restart** boxes for that service are checked.
10	Review the **Restart Limit** setting for the service to ensure it is not set to an excessively long time.

--End--

Recovering High Availability

Recover High Availability (HA) to ensure that Contact Center switches over correctly in case of any future system failures.

The following are the major recovery steps:

- On the Active server, fix the problem that caused the switchover.
- Back up the Contact Center data on the Standby server.
- Restore the Contact Center data to the Active server.
- Bring the Active server back into operation in standby mode, shadowing the Standby server.

Fixing the cause of the failure on the Active server

Troubleshoot and correct the failure that caused the switchover. In this example, this involves replacing the Active server Local Area Network (LAN) cable in the Contact Center Subnet Network Interface Card (NIC)

Procedure steps

Step	Action
1	Locate the LAN cable that connected the Active server to the Contact Center Subnet Network Interface Card (NIC).
2	Replace the LAN cable in the NIC.

--End--

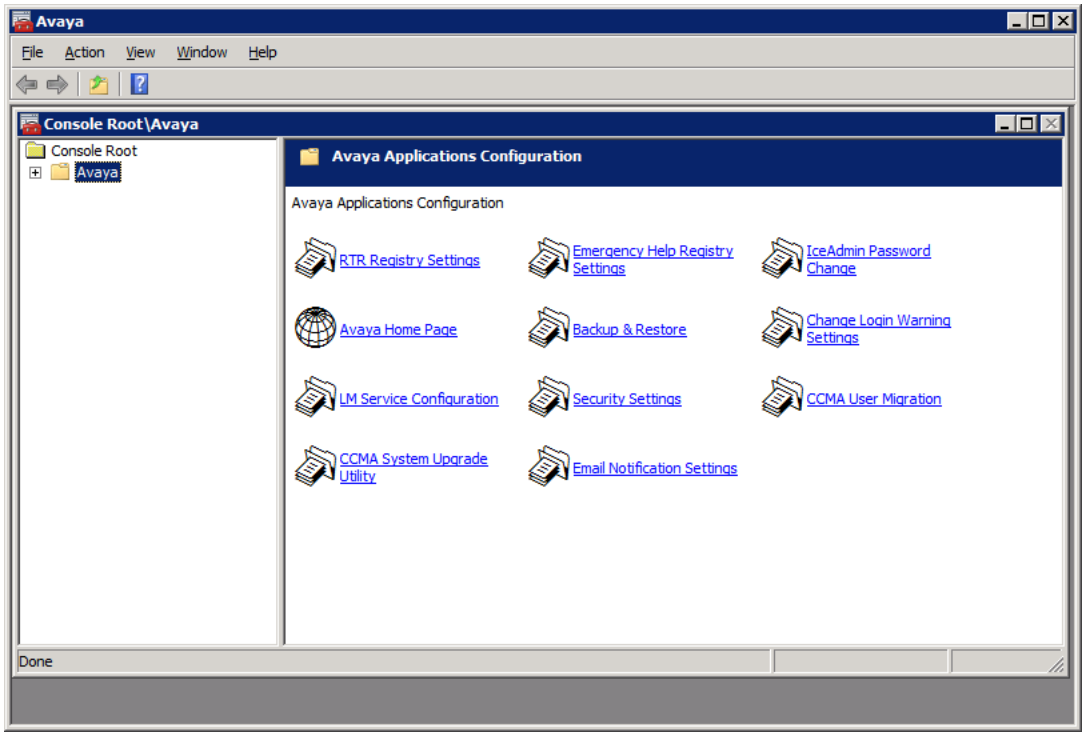
Backing up the Contact Center Manager Administration component on the Standby server

Back up Contact Center Manager Administration to a folder to create a snapshot of the preselected CCMA data files on the Standby server. This allows you to copy any changes made in the CCMA database while the Active server was down.

Procedure steps

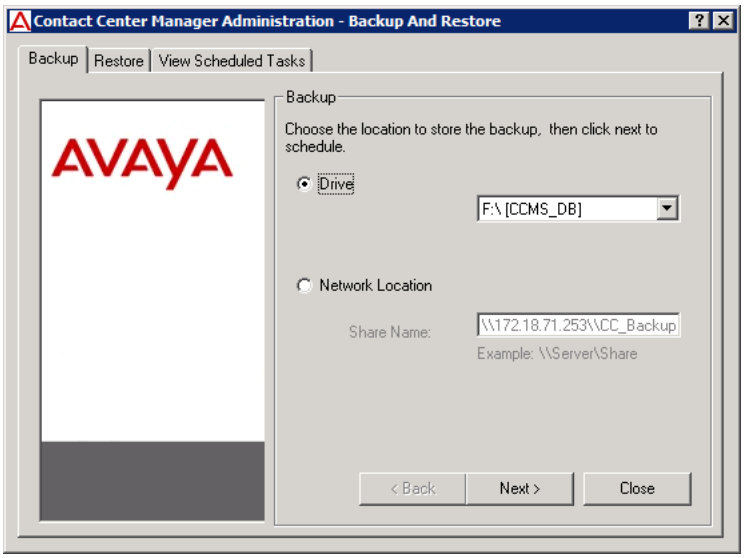
Step	Action
1	Log on to the Standby server (for example, **CCCORESTWO**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.

2 Choose **Start, All Programs, Avaya, Contact Center, Manager Administration, Configuration**.



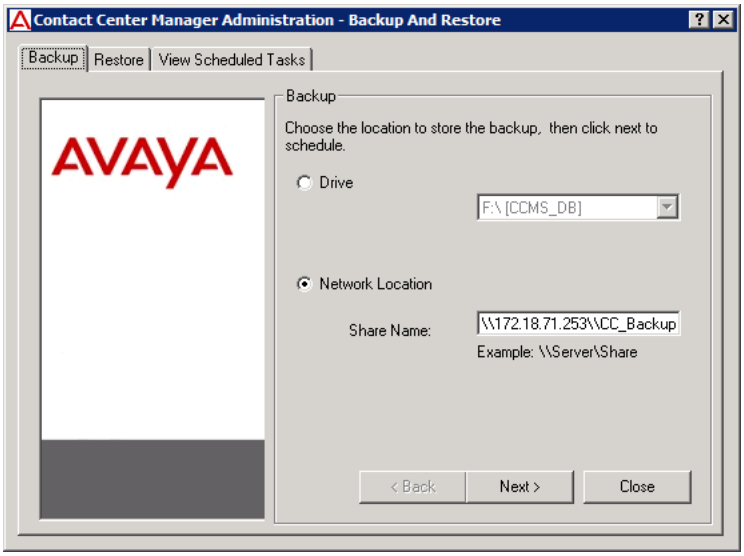
3 In the right-hand pane, click **Backup & Restore**.

4 In the **Contact Center Manager Administration - Backup and Restore** utility, select the **Backup** tab.

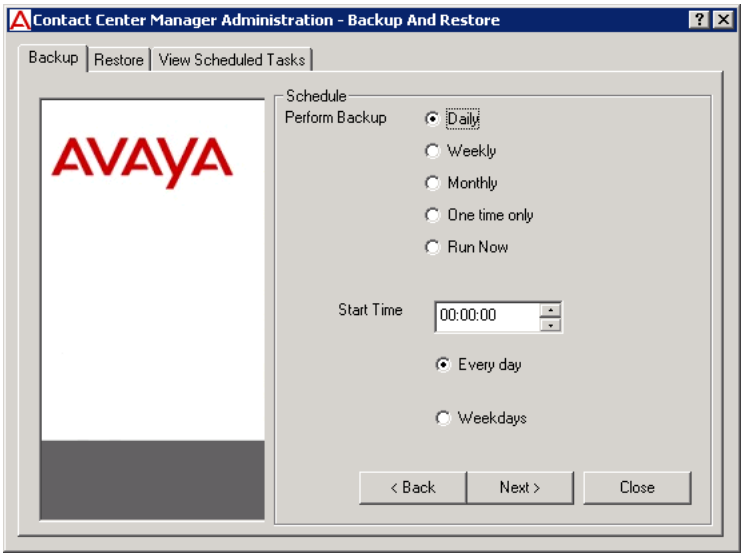


5 In the **Backup** window, select **Network Location**.

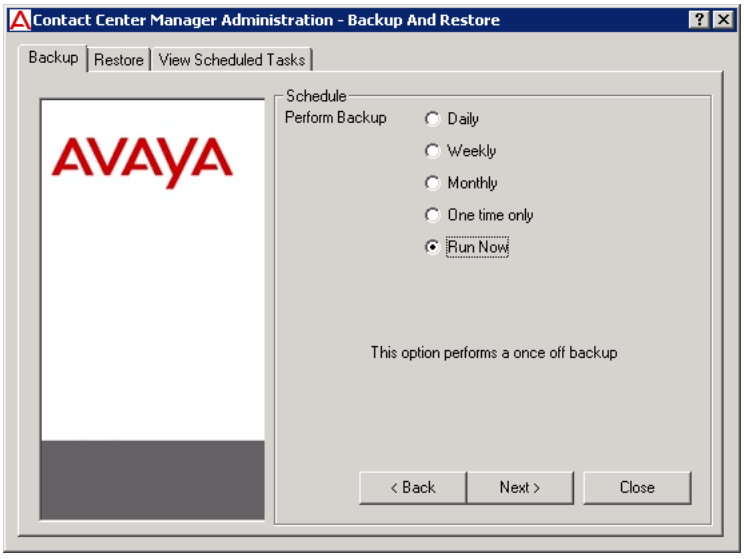
6 In the **Share Name** box, specify the Network Location where you want to store the backup, for example **\\172.18.71.253\CC_Backup**.



7 Click **Next**.



8 On the **Schedule** page, select **Run Now**.

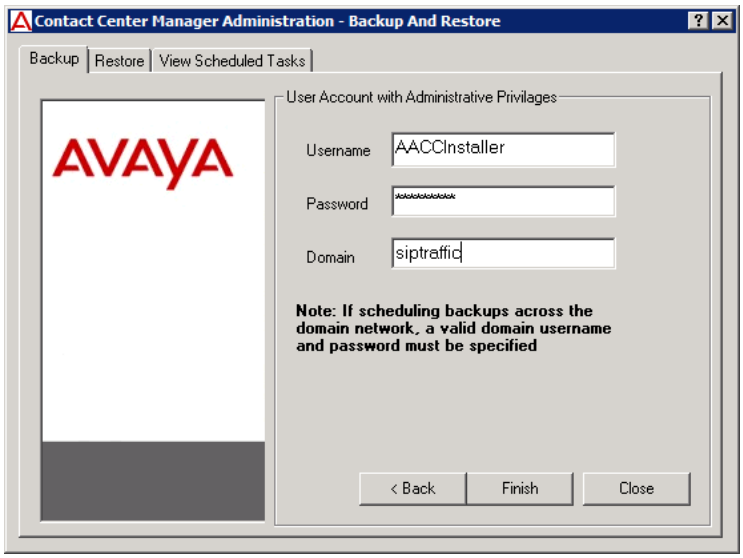


9 Click **Next**.

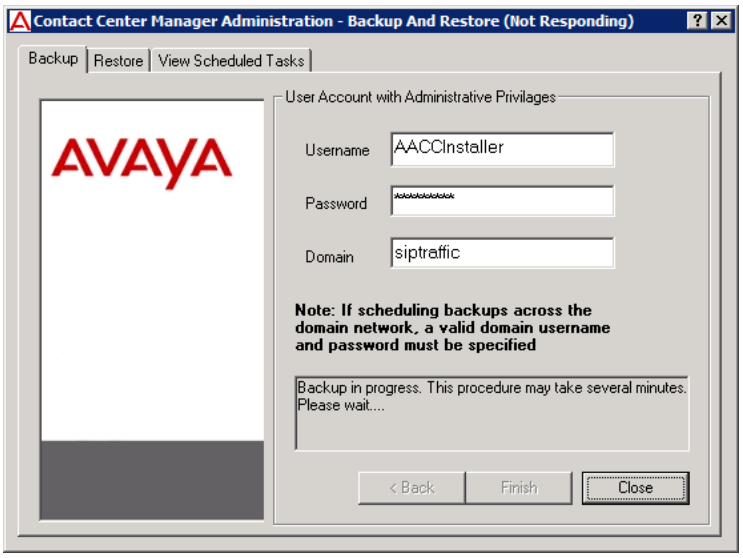
10 In the **Username** box on the **User Account with Administrative Privileges** page, type a valid administrator user name for the server on which you want to store the backup, for example **AACCinstaller**.

11 In the **Password** box, type a the password for the specified administrator user, for example **AACCInstPass1**.

12 In the **Domain** field, type the domain on which you created the network backup location, for example **siptraffic**.



13 Click **Finish**.



14 When the backup completes, click **Close**.

All backups are saved as files in the format CCMAFilesBackup<BackupDateTime>.package.

--End--

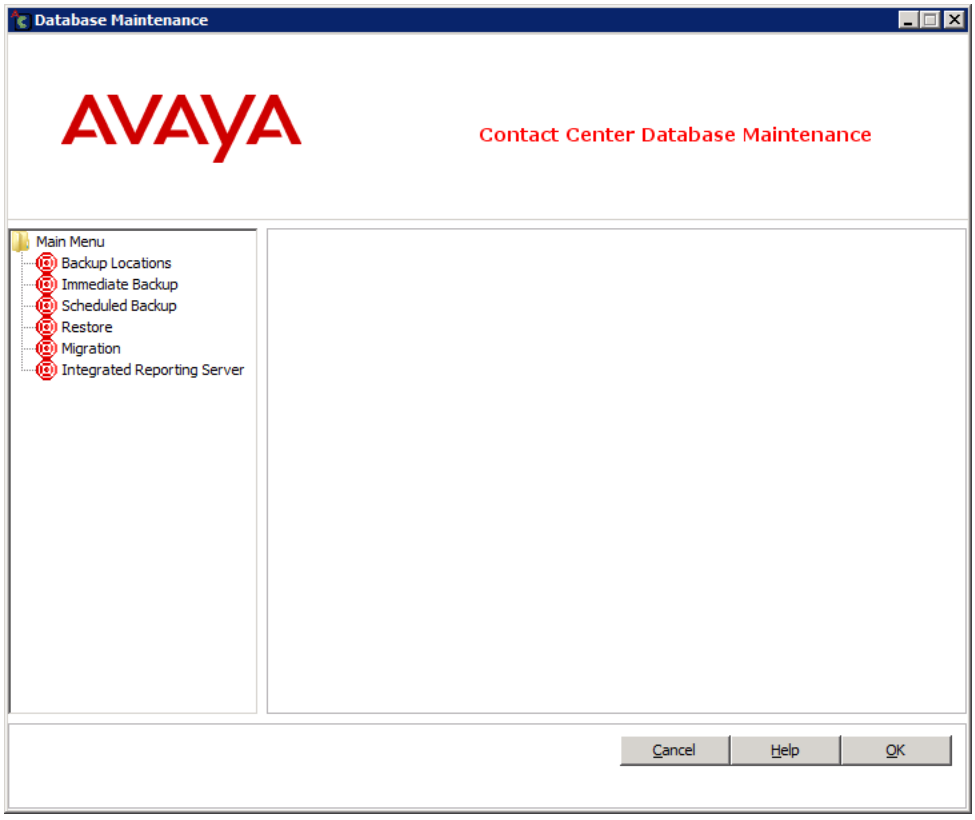
Backing up the Contact Center databases on the Standby Server

After the switchover, the Standby server is in active mode, and continuing to process contacts. This creates a delta between the Standby server database and the Active server databases for the period when the Active server was down. Back up the Standby server to create a snapshot of the databases, which you can restore to the Active server. You must back up all databases.

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.

Procedure steps

Step	Action
1	Log on to the Standby server (for example, **CCCORESTWO**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Choose **Start**, **All Programs**, **Avaya**, **Contact Center**, **Database Utilities**, **Database Maintenance**.



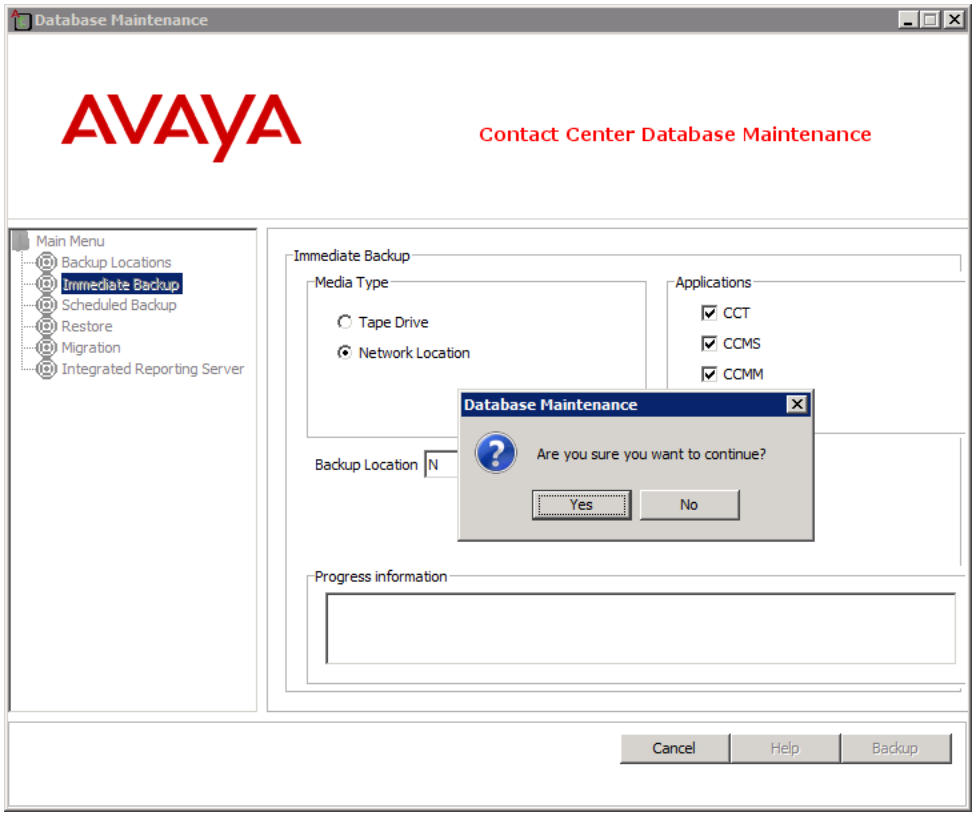
3 In the left pane, click **Immediate Backup**.

4 In the **Media Type** section, select **Network Location**.

5 In the **Applications** section, select **CCMS**, **CCT**, **CCMM,** and **ADMIN**.

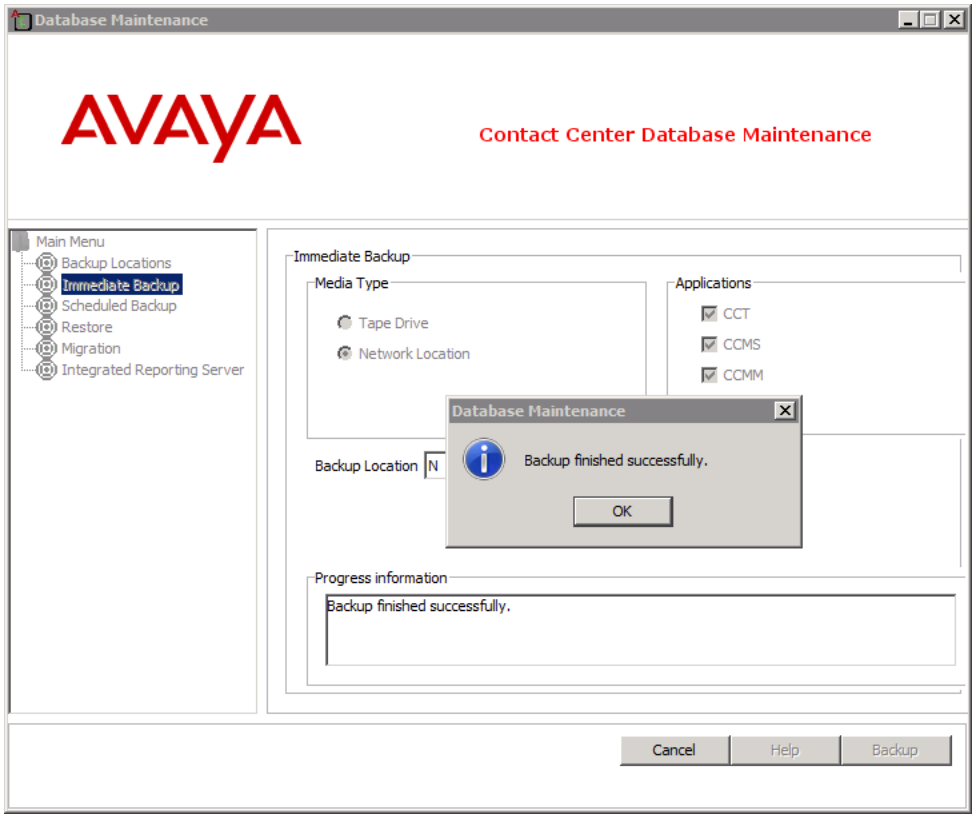
6 From the **Backup Location** list, select the network drive on which to store the backup, for example **N**.

7 Click **Backup**.



8 Click **Yes** to continue with the backup.

9 The database backup completes.



10 Click **OK**.

11 Exit the Database Maintenance utility.

--End--

Restoring the Contact Center databases on the Active Server

Restore the database from the Standby server to the Active server to ensure the databases are consistent so that Shadowing can start. The Database Maintenance utility can restore only one application database at a time. Restore the CCMS, CCT, CCMM, and ADMIN databases.

You must restore the CCMS, CCT, CCMM, and ADMIN databases onto the Active server. You must restore the ADMIN database last.

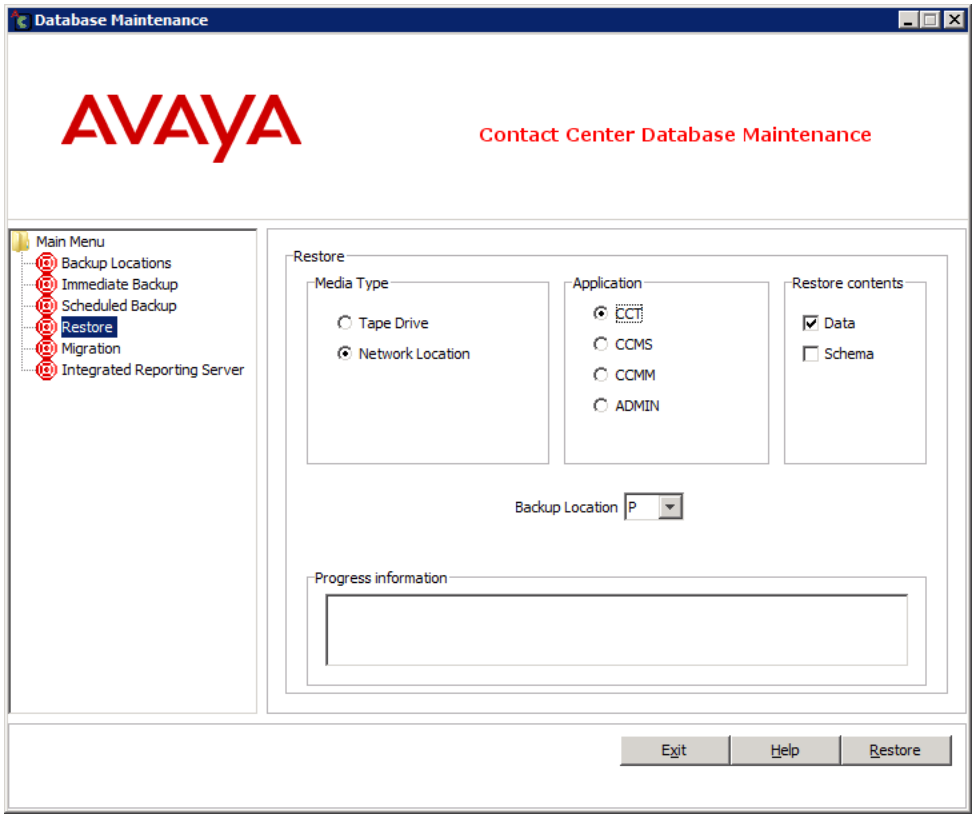
Attention: You must backup the Standby server database, restore it onto the Active server, and enable shadowing within 24 hours. If the difference in time between the Standby and Active server database content is greater than 24 hours, then database shadowing does not work.

Attention: You must restore all databases to the Contact Center server. Restoring only CCMS, and not CCT, CCMM, or ADMIN, may leave an inconsistent server database and prevent HA from shadowing data correctly.

Attention: Restoring the Administration (ADMIN) database can change configuration of Backup locations on the Active server if the Standby server and Active server backup locations are different. Therefore, after you restore the ADMIN database, close and reopen the Database and Maintenance utility.

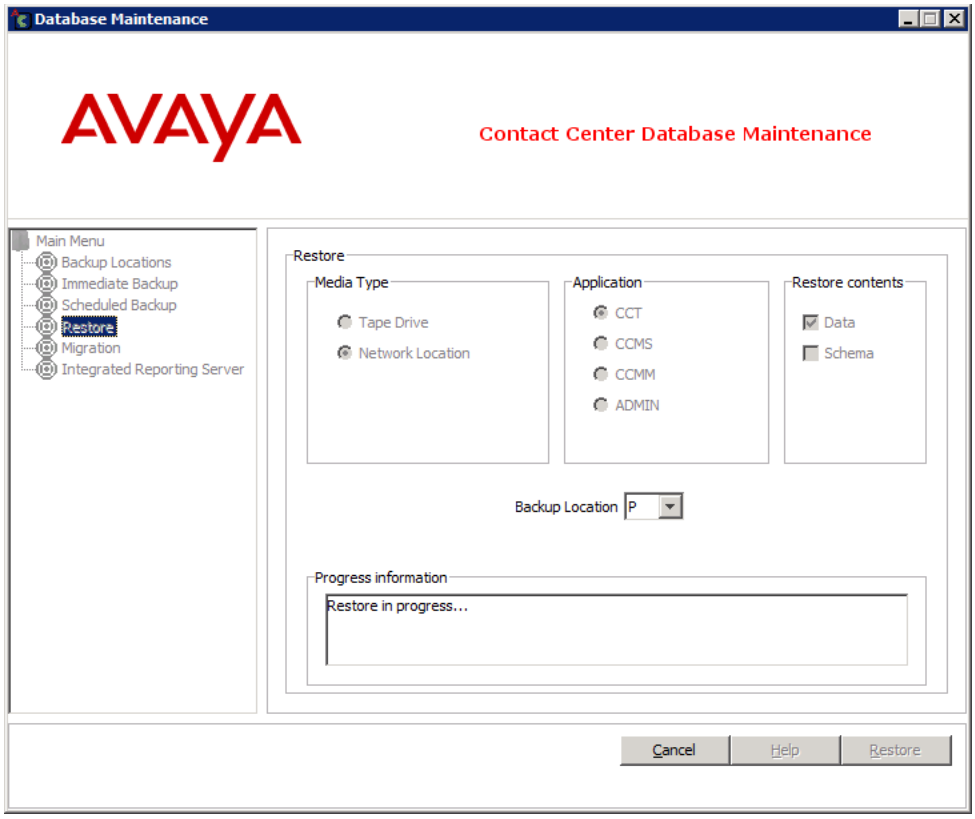
Procedure steps

Step	Action
1	Log on to the Active server (for example, **CCCORESONE**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Choose **Start**, **All Programs**, **Avaya**, **Contact Center**, **Database Utilities**, **Database Maintenance**.
3	In the **Database Maintenance** dialog box, in the left pane, click **Restore**.
4	In the right pane, under **Media Type**, select the media type from which to restore the backup, for example **Network Location**.
5	From the **Backup Location** list, select the drive you created on the **Backup Locations** tab, for example **P**.
6	Under **Application**, select **CCT**.
7	Under **Restore contents**, select **Data**.
8	Click **Restore**.



9 On the **Restore Database** dialog, click **Yes**.

10 Use the **Progress information** field to monitor the progress of the restoration.



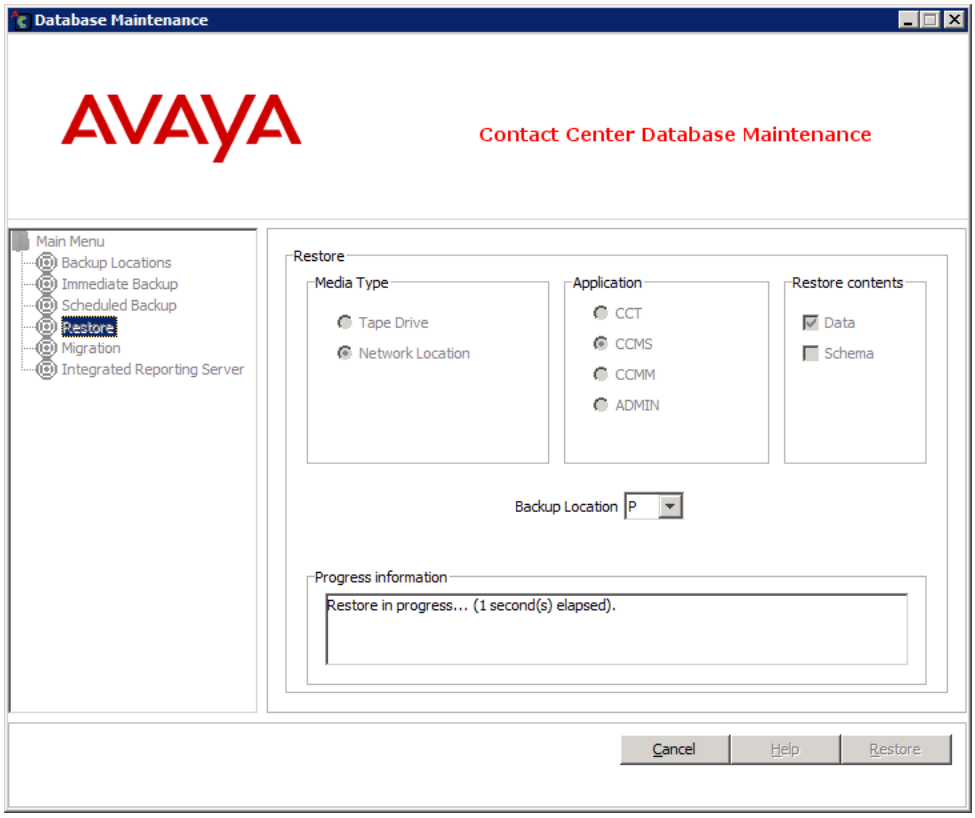
11 On the **Database Maintenance** dialog, click **OK**.

12 Under **Application**, select **CCMS**.

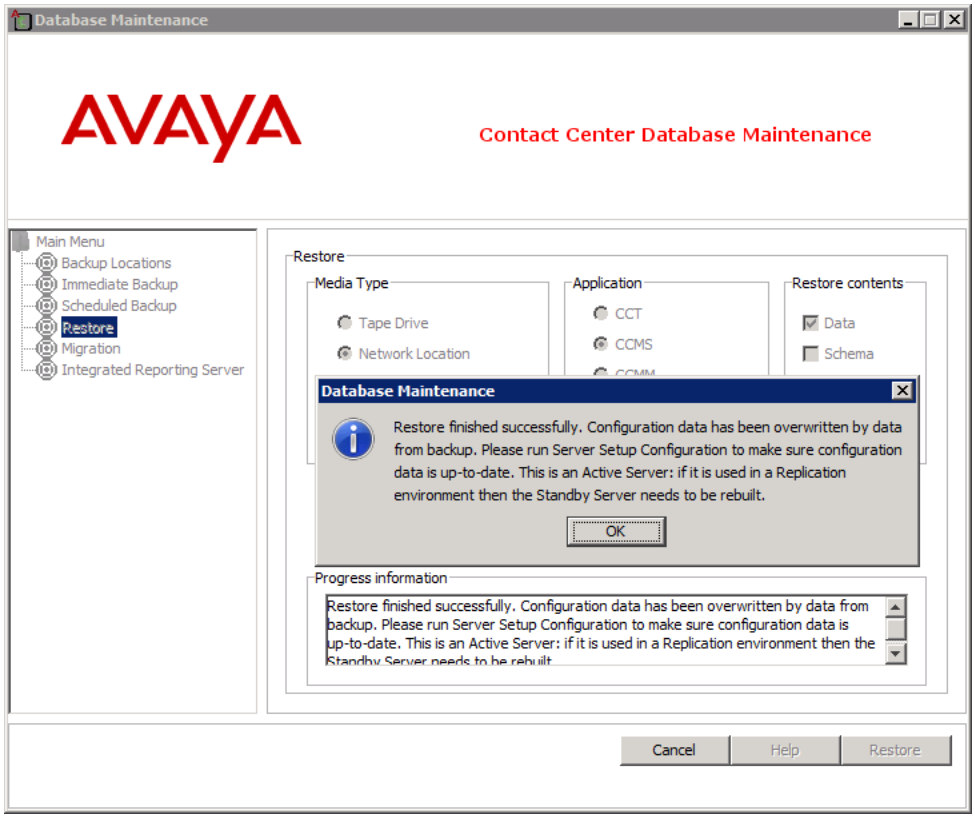
13 Click **Restore**.

14 On the **Restore Database** dialog, click **Yes**.

15 Use the **Progress information** field to monitor the progress of the restoration.



16 On the **Database Maintenance** dialog, click **OK**.

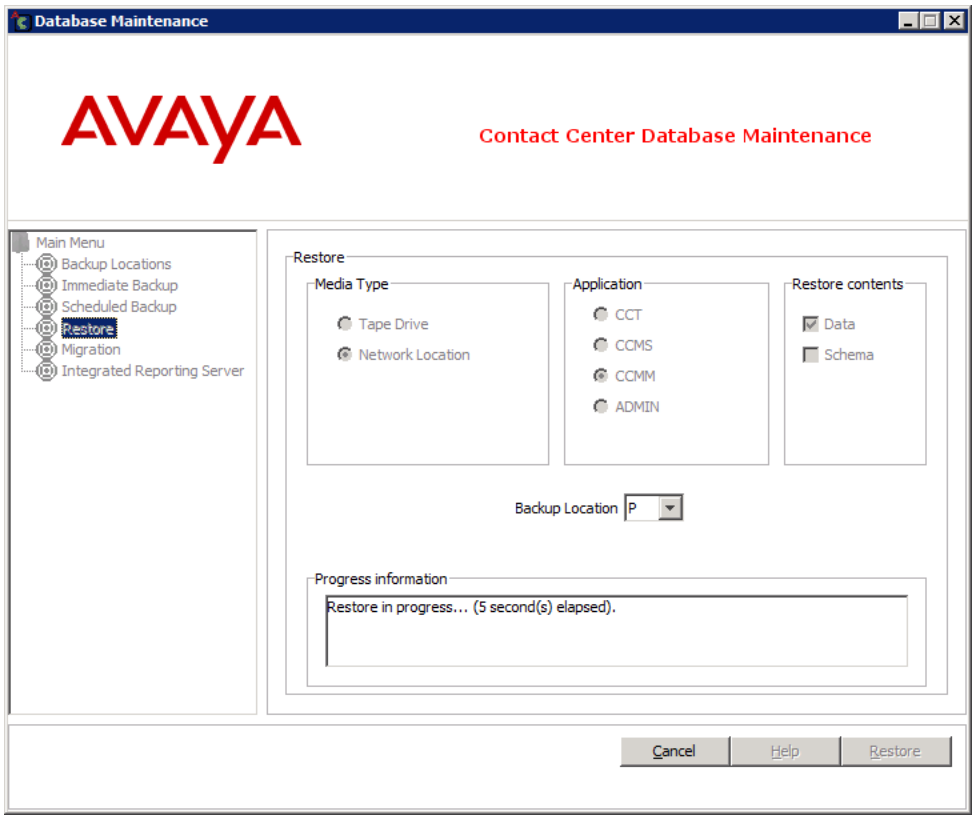


17 Under **Application**, select **CCMM**.

18 Click **Restore**.

19 On the **Database Maintenance** dialog, click **Yes**.

20 Use the **Progress information** field to monitor the progress of the restoration.



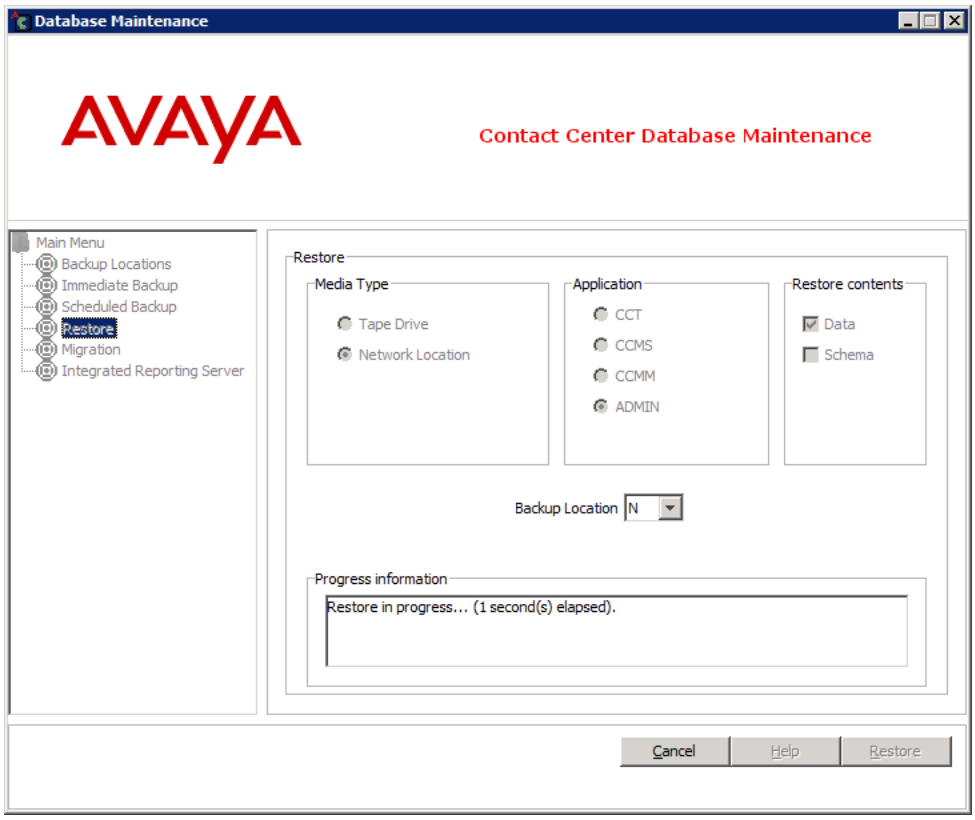
21 On the **Database Maintenance** dialog, click **OK**.

22 Under **Application**, select **ADMIN**.

23 Click **Restore**.

24 On the **Restore Database** dialog, click **Yes**.

25 Use the **Progress information** field to monitor the progress of the restoration.



26 Click **Exit** to close the Database Maintenance utility.

27 Click **Yes**.

--End--

Creating a drive mapping to the network backup location from the Active server

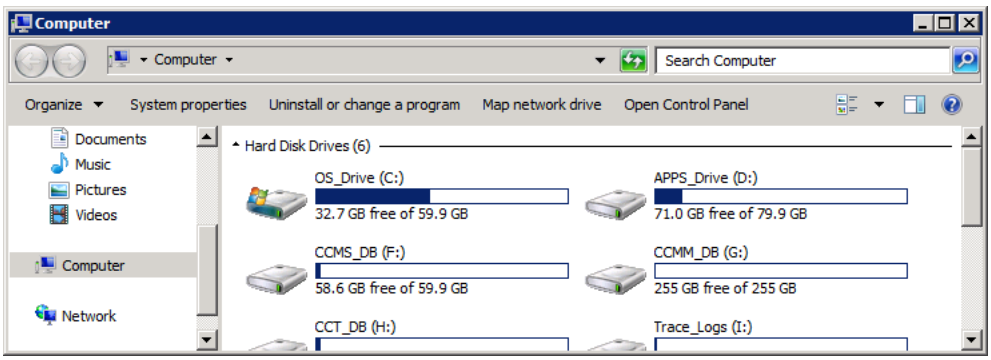
The CCMA Restore utility is easier to use if you create a mapping to the network location where you created the Standby server CCMA backup. Follow this procedure to create a network drive on the Active server.

Procedure steps

Step	Action
1	Log on to the Active server (for example, **CCCORESONE**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.

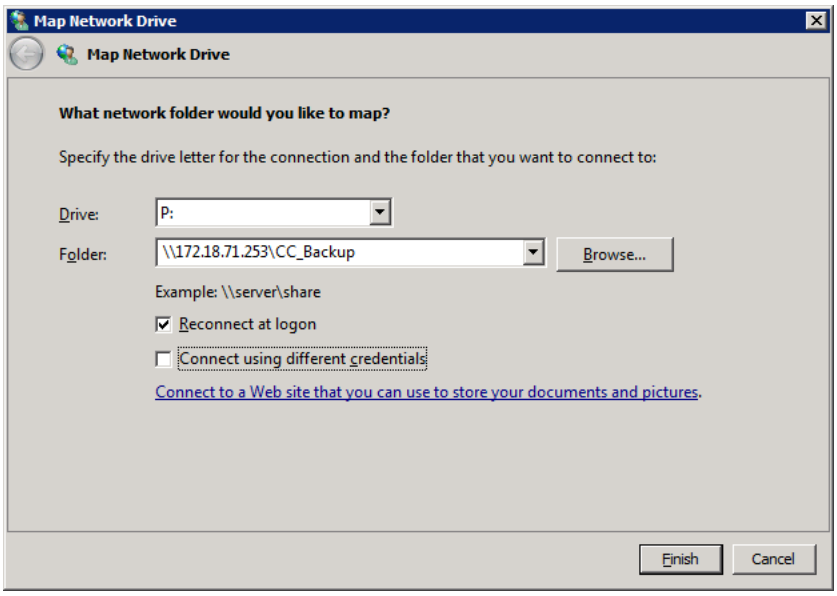
2 Choose **Start**, **Computer**

3 On the Computer window, click Map network drive.



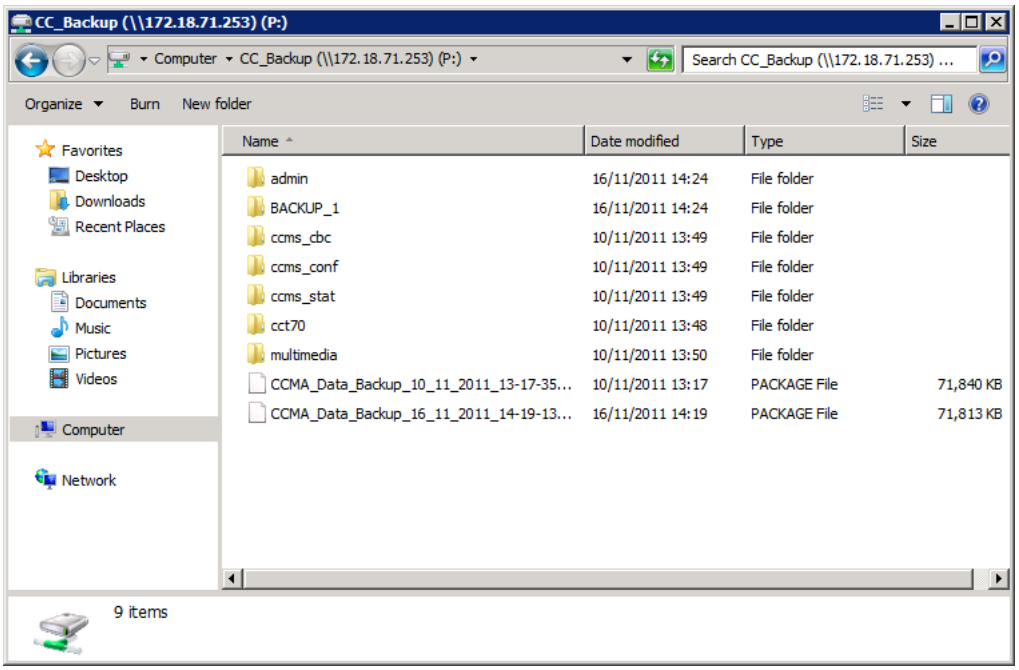
4 On the **Map Network Drive** dialog, from the **Drive** list, select a letter for the drive, for example **P:**.

5 In the **Folder** box, type the type the location to which you want to map the drive letter, in the format \\<Computer IP Address>\<Backup Location>, for example **\\172.18.71.253\CC_Backup**.

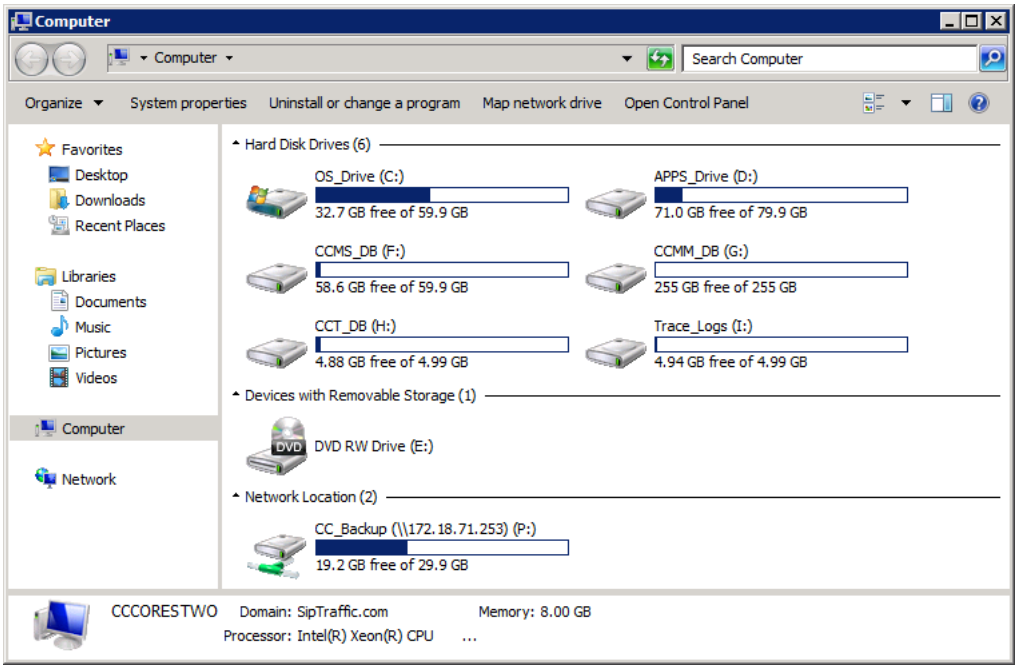


6 Click **Finish**.

Windows opens the specified network location in a new window.



7 Close the drive window. You can see the new drive in the **Computer** window.



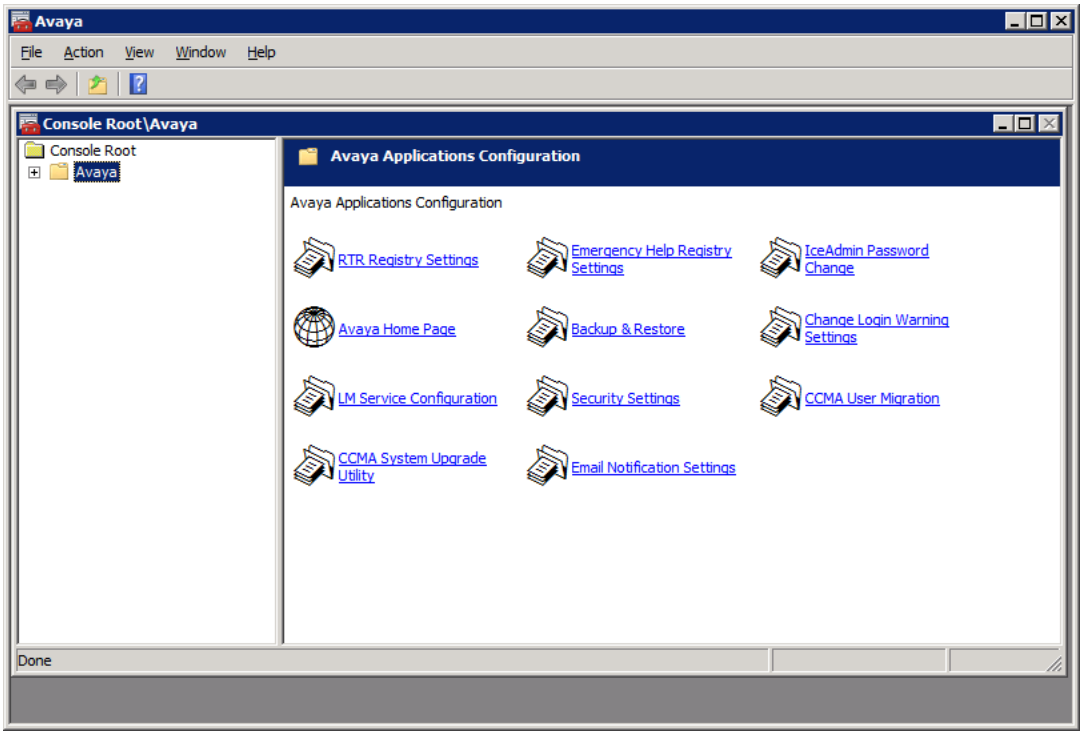
--End--

Restoring CCMA data to the Active server

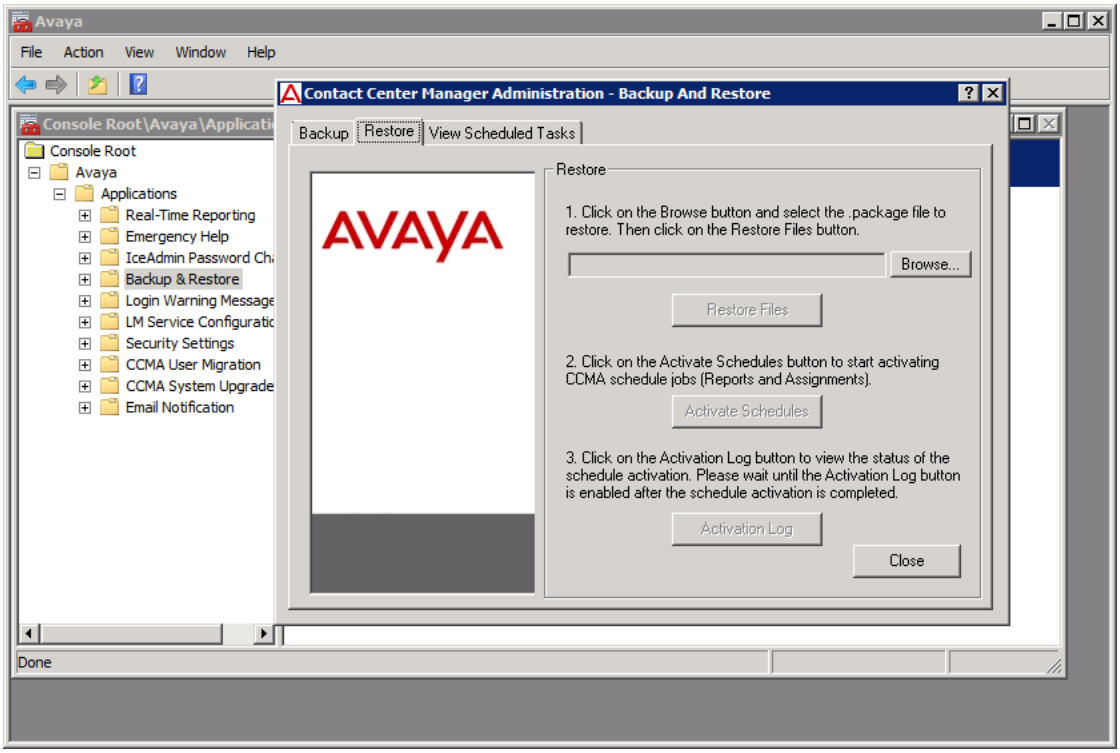
Restore the Contact Center Manager Administration data to the Active server.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, choose **Start**, **All Programs**, **Avaya, Contact Center**, **Manager Administration**, **Configuration**.



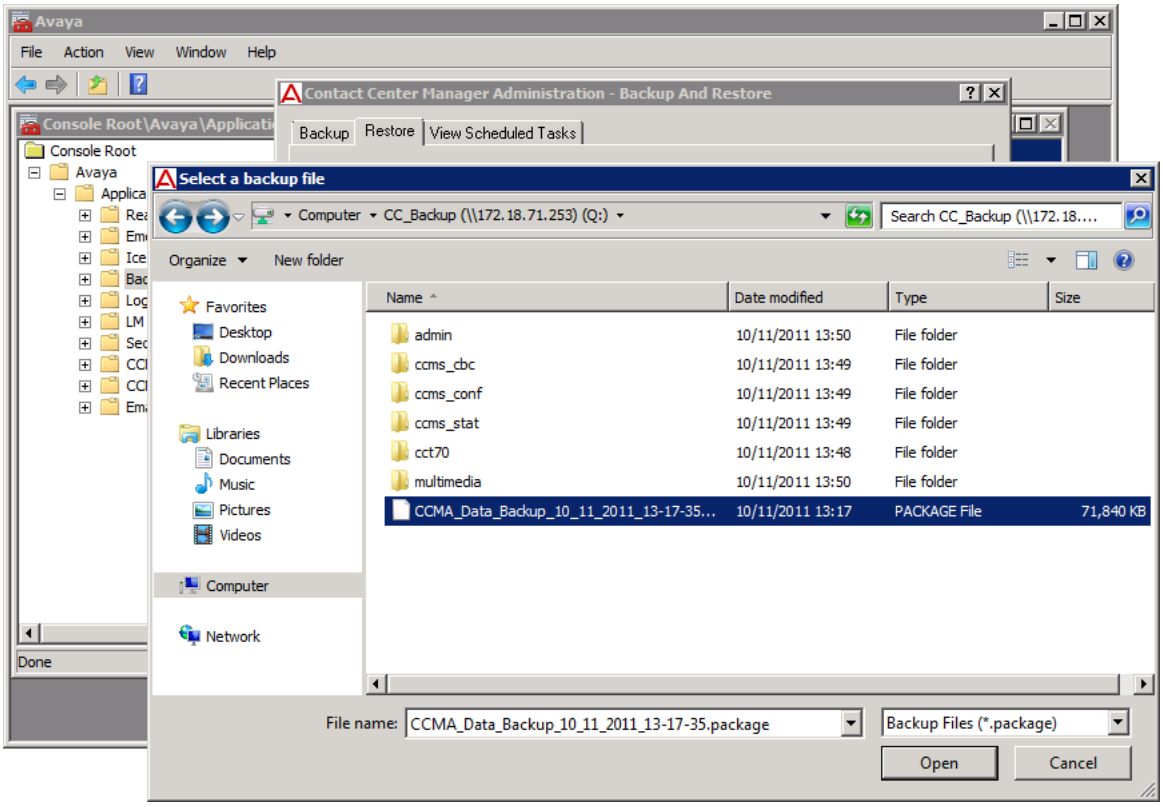
2	In the left pane of the **Avaya Configuration** window, expand **Avaya, Applications, Backup & Restore**.
3	In the right pane, click **Backup & Restore**.
4	In the **Contact Center Manager Administration - Backup And Restore** dialog box, click the **Restore** tab.



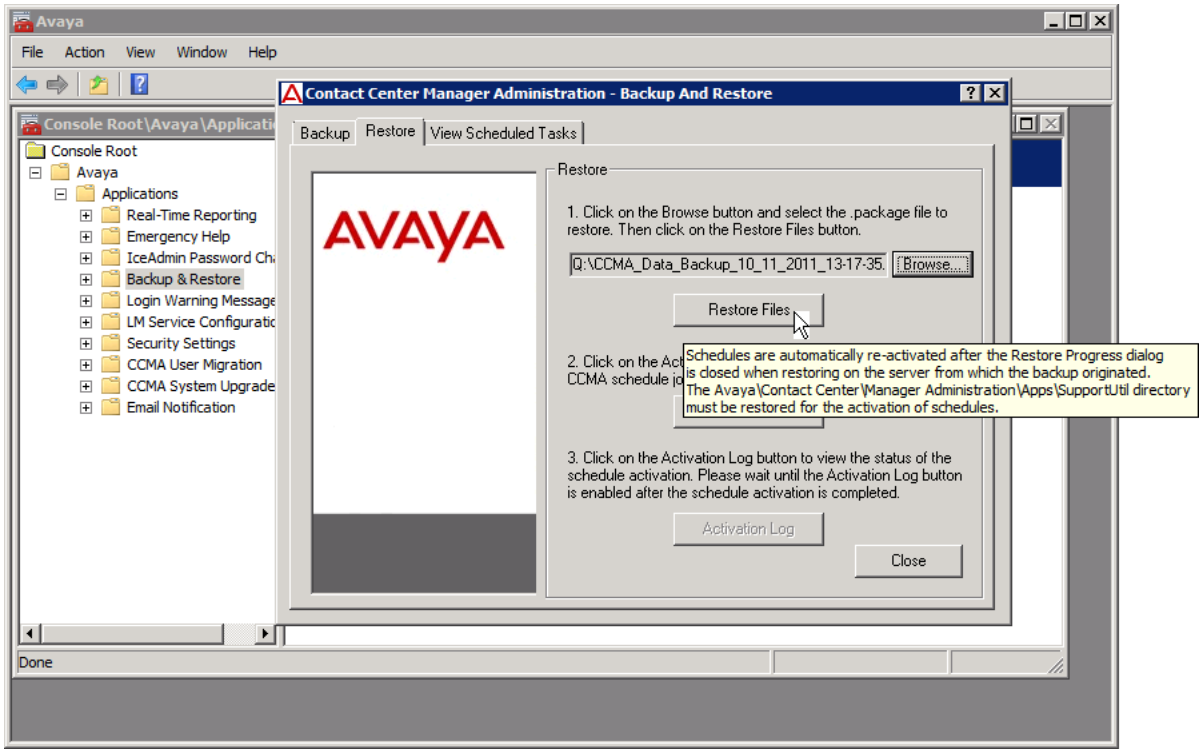
5 To select a backup file to restore from, click **Browse**.

6 In the **Select a backup file** dialog box, browse to the location where you backed up the CCMA data, and select the .package file.

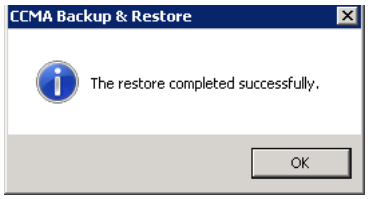
7 Click **Open**.



8 Click **Restore Files**.



When the restore is finished, a ***Close*** *message box appears.*



9 On the **CCMA Backup & Restore** message box, click **OK**.

10 Click **Close**.

--End--

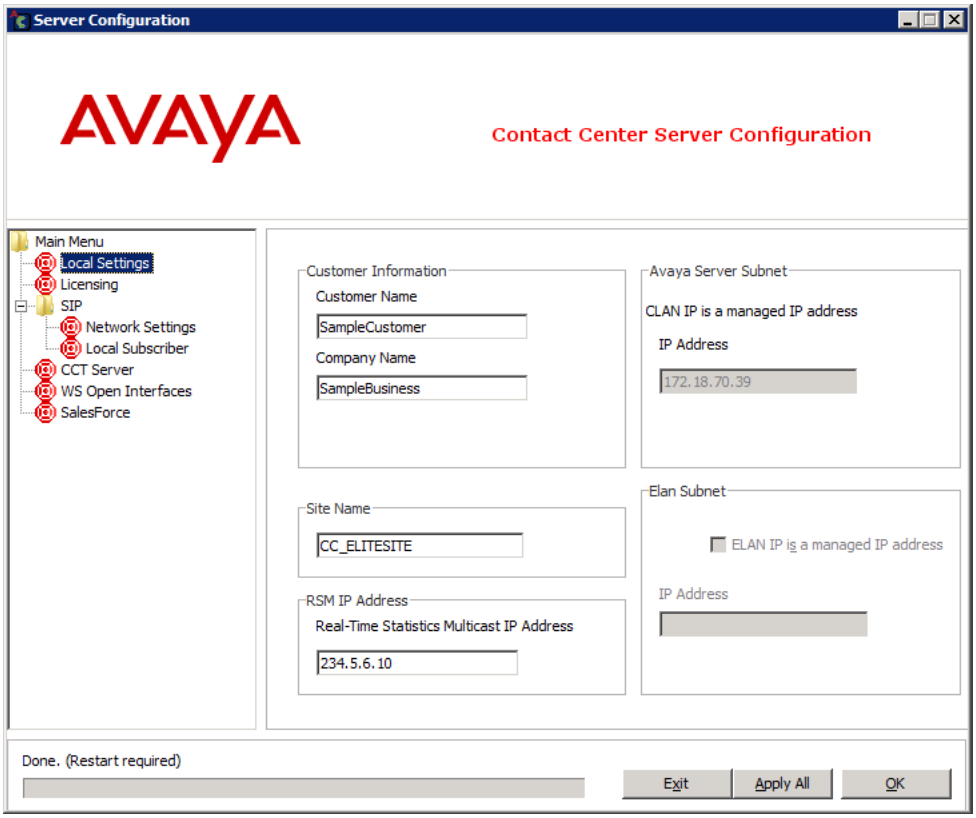
Verifying the server details and restarting the Active server

After you restore the Standby server database on to the Active server, the Active server database contains the same agent and statistical data as the Standby server. Verify that the Active server configuration details are correct.

Attention: This procedure forces a server restart.

Procedure steps

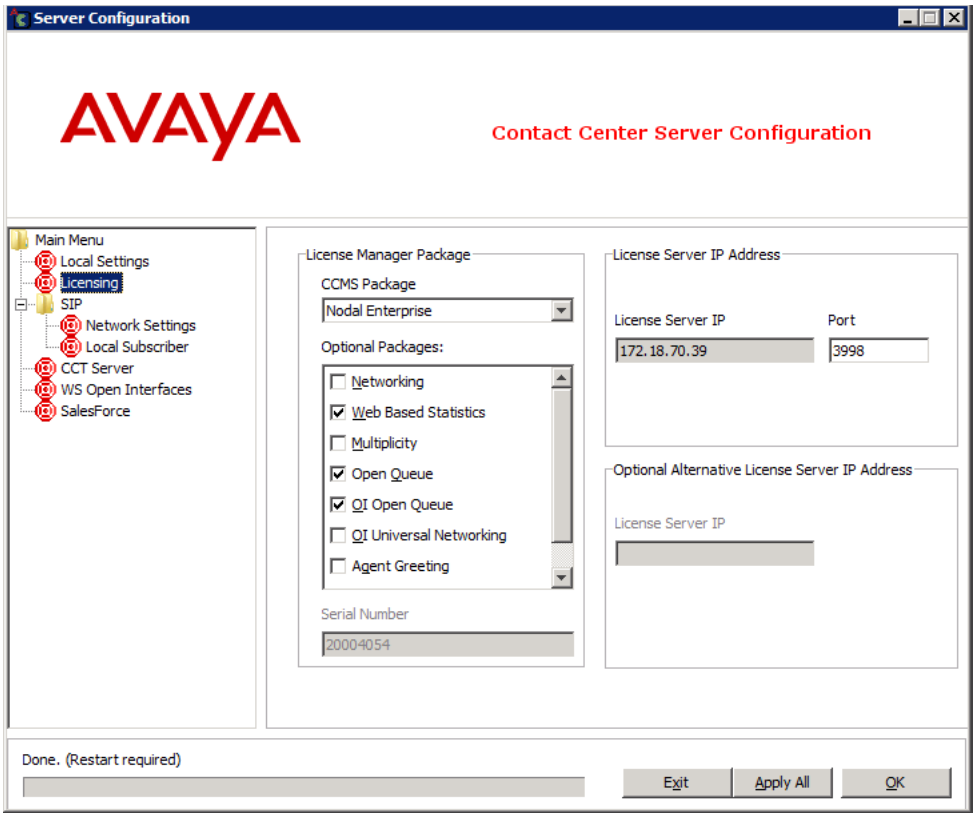
Step	Action
1	Log on to the Active server (for example, **CCCORESONE**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Manager Server**, **Server Configuration**.
3	In the **Server Configuration** dialog box, click the **Local Settings** tab.
4	Under **Avaya Server Subnet** verify that the **IP Address** box contains the managed IP address, for example **172.18.70.39**.
5	Under **Avaya Server Subnet**, verify that the Site Name box contains the correct site name, for example **CC_ELITESITE**.



6 In the **Server Configuration** dialog box, click the **Licensing** tab.

7 On the **Updated IP Warning** message box, click **OK**

8 Verify that the Standby Server licensing details match the Active server licensing details.



9 Click **Apply All**.

10 Click **Exit**.

11 On the **Server Configuration** message box, click **Yes**.

12 On the **HA System** message box, click **OK**.

Contact Center forces a shutdown of the Windows server.

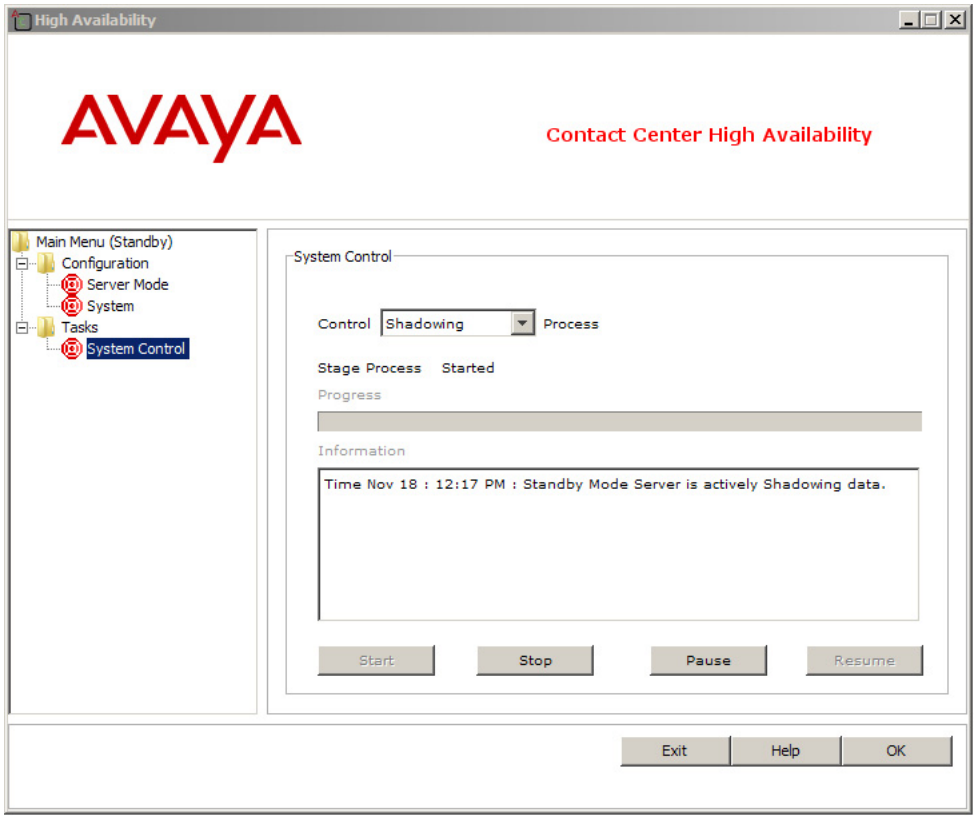
--End--

Verifying that the Active server is running in standby mode and shadowing data

Use the HA utility to check that the Active server is now running in Standby mode and is shadowing the Standby server, which is running in active mode.

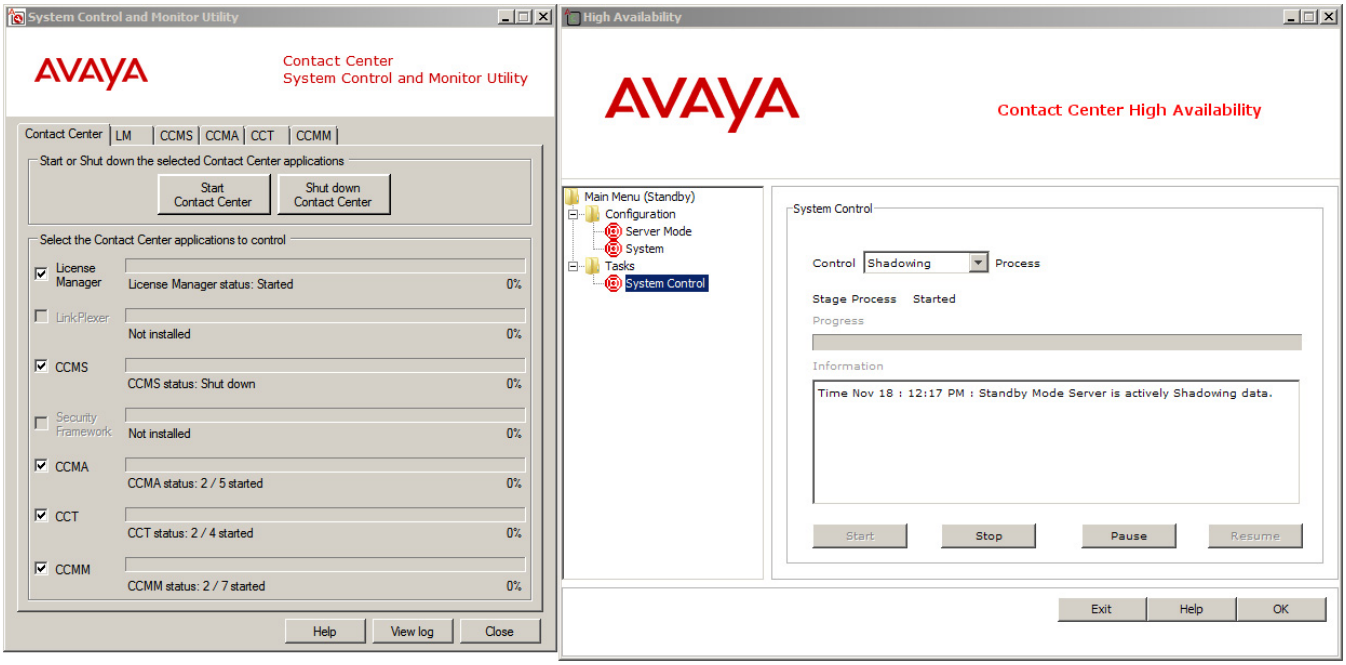
Procedure steps

Step	Action
1	Log on to the Active server (for example, **CCCORESONE**) using the Avaya Aura® CC installer domain account, for example **SIPTRAFFIC\AACCinstaller**.
2	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Database Utilities**, **High Availability**.
3	In the right pane, select **Server Mode**.
4	Verify that the mode selected is **Standby**.
5	Verify that there is a check in the **Switchover** box.
6	In the left pane, select **System Control**.
7	In the right pane, check the **Information** box to see that this server is actively shadowing data.



8 Choose **Start, All Programs, Avaya, Contact Center, Common Utilities, System Control and Monitor Utility**.

9 Verify that the **CCMS Status** is **Shut down**.



--End--