



Avaya Aura™ Contact Center
Commissioning

NN44400-312

Document status: Standard
Document issue: 02.05
Document date: 02 March 2011
Product release: Release 6.0/6.1
Job function: Commissioning
Type: Technical Publication
Language type: English

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/](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

New in this release	7
Features	7
SIP-enabled contact center features	7
Communication Control Toolkit console	8
High Availability	8
Licensing options	9
Other changes	9
Internet Explorer	9
Operating system changes	10
Avaya Aura™ Contact Center server commissioning	11
Introduction	15
Networked Avaya Aura™ Contact Center commissioning	17
Contact Center Manager Server commissioning	21
Verifying the success of the installation	23
Enabling Open Queue	24
Enabling Multiplicity	24
Configuring the operating system for remote access	26
Disabling date and time features	26
Disabling the Windows time service	27
Verifying CCMS patches	28
Scheduling Weekly Disk Defragmentation	28
Configuring the Multicast controller	29
Confirming the CCMS services start	30
Network Control Center commissioning	33
Configuring the sites	34
Contact Center Manager Administration commissioning	37
Configuring the License Manager Service	41
Configuring Real-Time Reporting	42
Updating the iceAdmin user password	44
Configuring domain accounts to allow scheduling Historical Reports to a Network Server	45
Creating a shared folder to export historical reports	45
Creating a shared folder on the client with read permissions for the domain	46
Creating a shared folder on the client with read permissions for a user	47
Creating a shared folder on the client PC with read permissions for the IUSR_SWC and iceAdmin accounts	48
Configuring Agent Desktop Display parameters on the server	49
Downloading the latest documentation to the CCMA server	52
Verifying the Web Services	53
Logging on to Contact Center Manager Administration for the first time	53
Installing the Service Creation Environment client	55

Security Framework commissioning	57
Configuring the admin user for the Unified Communication Manager	59
Configuring the communication between CCMA and UCM	61
Creating Unified Communication Management local accounts	63
Mapping Unified Communication Management users to CCMA users	65
Starting Contact Center Manager Administration client	66
Configuring the admin user for the backup server	67
Configuring the communication between CCMA and the backup UCM	69
Contact Center Manager Administration client commissioning	73
Configuring the display settings	75
Configuring Internet Explorer	76
Configuring display settings in Internet Explorer	77
Adding Internet Explorer to the firewall exceptions list	78
Opening multicast and unicast ports	78
Installing the ActiveX Controls	80
Applying the ActiveX Controls	81
Communication Control Toolkit commissioning for Contact Center	83
Confirming that the CCT services start	85
Configuring the licensing for CCT	86
Configuring the deployment type for CCT	88
Adding the CCT Server in CCMA	89
Configuring the Avaya Communication Server 1000 service provider	90
Importing workstations from the domain	93
Importing Avaya Communication Server 1000 data	93
Adding a TDM agent in CCMA	96
Assigning resources	97
Configuring Hotdesking (Agent Roaming)	99
Adding agent in CCMA	100
Verifying CCT using the Reference Client	101
Communication Control Toolkit commissioning for Knowledge Worker	103
Confirming that the CCT services start	105
Configuring the licensing for CCT	106
Configuring the Avaya Communication Server 1000 service provider	107
Starting the CCT Web Administration application	110
Importing Avaya Communication Server 1000 Data	110
Importing Windows users from the CCT domain	113
Importing workstations from the domain	115
Assigning resources	115
Configuring Hotdesking (Agent Roaming)	117
Verifying CCT using the Reference Client	118
Contact Center Multimedia server commissioning	121
Providing local users with the Log on as a service right	123

Verifying the Multimedia database installation	124
Verifying that Contact Center Multimedia services start	124
Adding the multimedia servers to Contact Center Manager Administration	125
Logging on to the Multimedia Administration tool for the first time	126
Configuring server settings	127
Configuring multimedia license	129
Configuring e-mail recipient addresses	129
Configuring e-mail attachment file locations	132
Configuring the multimedia skillsets	133
Configuring the MIME types	135
Agent Desktop client commissioning	137
Configuring hotdesking (optional)	139
Configuring the pop-up window for a Citrix environment	139
External Web communication server commissioning	141
Assigning the properties for the sample customer interface Web site	143
Creating a customer	144
Testing request text chat	145
Testing request callback	146
Testing e-mail	147
Transferring your Web interface to the production server	148
High Availability Campus co-resident server commissioning	149
Resolving the Managed CLAN Name Server to the Managed CLAN IP Address	154
Verifying services are ready for High Availability	155
Configuring High Availability on the Active Server	155
Configuring E-mail notification on the Active Server	157
Configuring service monitoring on the Active Server	158
Backing up the database on the Active Server	161
Restoring the database on the Standby Server	161
Configuring High Availability on the Standby Server	163
Starting the Active Server	164
Starting shadowing on the Standby Server	165
Verifying shadowing is running on the Active Server	166
Testing switch overs	168
High Availability Geographic co-resident server commissioning	171
Verifying services are ready for High Availability	175
Configuring High Availability on the Active Server	175
Configuring E-mail notification on the Active Server	177
Configuring service monitoring on the Active Server	178
Backing up the database on the Active Server	181
Restoring the database on the Standby Server	181
Configuring High Availability on the Standby Server	183
Starting the Active Server	184
Starting shadowing on the Standby Server	185
Verifying shadowing is running on the Active Server	186

Testing switch overs	188	
High Availability Campus CCMM commissioning		191
Configuring CCMM General Administration	195	
Configuring the Active Server	195	
Backing-up the CCMM Active Server database	196	
Restoring the database on the Standby Server	197	
Configuring the Standby Server	198	
Starting the Active Server	199	
Starting shadowing on the Standby Server	199	
Verifying Shadowing is running on the Active Server	200	
Testing switch over on the CCMM solution	201	
Common procedures		203
Stopping individual services	203	
Starting services	204	
Disabling services	204	
Enabling services	205	
Stopping and restarting the core Communication Control Toolkit services	205	
Stopping and restarting the Contact Center Manager Server services	206	
Adding a server to a domain	206	
Starting the Contact Center	207	
Shutting down the Contact Center	208	
Integrated Reporting commissioning		209
Configuring Licensing	212	
Configuring Open Networking Web Service	213	
Configuring Integrated Reporting Server	214	
Enabling Communication Control Toolkit Open Queue	216	
Configuring Landing Pads	217	
Enabling Contact Summary Reporting	220	
Contact Center Manager Server Web service configuration		221
Generating a Certificate Signing Request	221	
Importing the CSR-Related Certificates	222	
Configuring SOA OpenQueue and OpenNetworking Web Services	223	
Removing Certificate Configuration	226	
Communication Control Toolkit Web service configuration		227
Configuring SIP Call Recording	228	
Generating a Certificate Signing Request	229	
Importing CSR-related Certificates	230	
Configuring SOA CCT Web Services	231	
Removing Certificate Configuration	232	

New in this release

The following sections detail what is new in the *Avaya Aura™ Contact Center Commissioning* (NN44400-312).

- [Features \(page 7\)](#)
- [Other changes \(page 9\)](#)

Features

See the following sections for information about feature changes:

- [SIP-enabled contact center features \(page 7\)](#)
- [Communication Control Toolkit console \(page 8\)](#)
- [High Availability \(page 8\)](#)
- [Licensing options \(page 9\)](#)

SIP-enabled contact center features

The following is a list of new features in a SIP-enabled contact center:

- Transferring DN calls to a Route Point
- Call Forward settings on agent telephones
- Music on hold for transfers

Let Call Ring, as an option in the Call Presentation Class of Service, is not supported for SIP-enabled contact centers.

For more information about SIP commissioning, see *Avaya Aura™ Contact Center SIP Commissioning* (NN44400-511).

Communication Control Toolkit console

This release contains several changes to the Communication Control Toolkit (CCT) Console. The updated CCT Snap-in is used for server-side and bulk configuration tasks only. It provides the following components:

- a bulk import and export tool

The bulk provisioning tool is updated to replace the Import Configuration and Export Configuration tools of the previous release. This tool exports any or all data in the CCT database to an XML file using one of two possible XML schema definitions; a standard data schema definition and a flat schema definition.

The flat schema definition file is suitable for use with Microsoft Excel. When you export a file using this tool, the schema definition file (XSD file) for the selected export format is created in the output location, along with the requested export file.

Due to changes to the database schema in the current release, the file formats (both TAB and XML) used in the previous release are incompatible with the current Database Import/Export tool.

- a Web administration interface

Use the Communication Control Toolkit Web Administration interface to configure the day-to-day administration interface for CCT. The Administrator can add, delete and edit IVRs and configure provider information. The Administrator can add, delete, edit and assign functionality on the following resources:

- Users, User Groups
- Terminals, Terminal Groups
- Addresses, Address Groups
- Workstations

High Availability

Contact Center supports High Availability (HA) hot standby resiliency for Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), Contact Center Multimedia (CCMM), and Contact Center Manager Administration (CCMA).

One set of Contact Center applications (a CCMS, a CCT, a CCMA, and an optional CCMM) actively processes scripts and contacts. This set of applications is called the active set. Another set of Contact Center applications in the same contact center system, runs in hot standby mode. This standby set of Contact Center applications monitors and shadows the active applications in the system but does not process calls. The standby CCMS monitors the active primary CCMS. The standby CCT monitors the active CCT. The standby CCMM monitors the active CCMM. Each active and standby pair of applications forms

a resilient or replication pair. If any active applications fails, the standby application recognizes the failure and starts processing contacts. You must configure the standby applications exactly the same as the active applications. Configuration changes to the active system during normal operation are automatically copied to the standby applications and the standby applications are configured to take over processing from the active system. Statistical data is also automatically copied to the standby applications.

Use the High Availability utility in Database Utilities to configure High Availability for CCMS, CCT and CCMM. Configure High Availability for CCMA when you install CCMA.

For information about High Availability Campus co-resident CCMS and CCT, see [High Availability Campus co-resident server commissioning \(page 149\)](#).

For information about High Availability Geographic co-resident CCMS and CCT, see [High Availability Geographic co-resident server commissioning \(page 171\)](#).

For information about High Availability CCMM, see [High Availability Campus CCMM commissioning \(page 191\)](#).

Licensing options

Contact Center now supports Essential, Nodal Enterprise, Corporate Enterprise, Nodal NCC, and Corporate NCC licensing modes. Essential licensing supports a single server voice only contact center with less than 100 agents. Nodal Enterprise licensing supports a single contact center installation. Corporate Enterprise licensing supports a network of contact center installations. Nodal and Corporate NCC licensing supports a Network Control Center.

You can maintain a secondary License Manager, which takes over the licensing if the primary License Manager fails.

Other changes

See the following section for other changes in Contact Center:

- [Internet Explorer \(page 9\)](#)
- [Operating system changes \(page 10\)](#)

Internet Explorer

Contact Center Manager Administration supports Internet Explorer 7.0. When you configure Internet Explorer, you must ensure that encoding settings are Western European.

- [Contact Center Manager Administration commissioning \(page 37\)](#)

Operating system changes

Contact Center is now supported on Windows Server 2008 Release 2. All procedures are updated to reflect the controls in the new operating system.

Avaya Aura™ Contact Center server commissioning

Commission the Contact Center software to prepare the features of the software for basic operation.

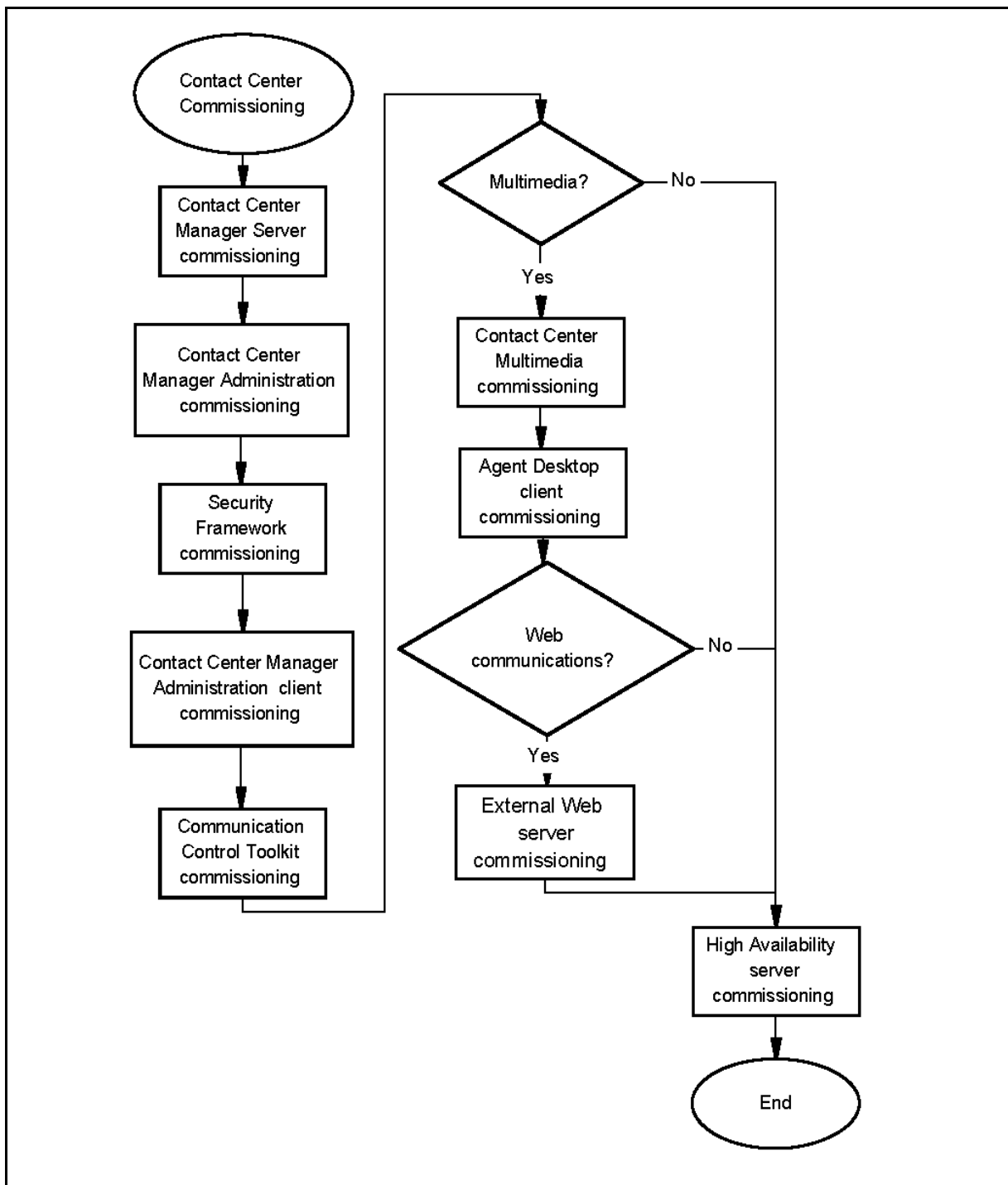
Prerequisites to stand-alone server commissioning

- Install or migrate your Contact Center software.

Stand-alone server commissioning tasks

This work flow shows you the sequence of tasks you perform to commission the Contact Center software. To link to any tasks, go to [Stand-alone Contact Center commissioning navigation \(page 12\)](#).

Stand-alone commissioning work flow



Stand-alone Contact Center commissioning navigation

- [Contact Center Manager Server commissioning \(page 21\)](#)
- [Contact Center Manager Administration commissioning \(page 37\)](#)

- [Security Framework commissioning \(page 57\)](#)
- [Contact Center Manager Administration client commissioning \(page 73\)](#)
- [Communication Control Toolkit commissioning for Contact Center \(page 83\)](#)
- [Contact Center Multimedia server commissioning \(page 121\)](#)
- [Agent Desktop client commissioning \(page 137\)](#)
- [External Web communication server commissioning \(page 141\)](#)
- [High Availability Campus co-resident server commissioning \(page 149\)](#)

Introduction

Avaya Aura™ Contact Center Commissioning (NN44400-312) describes how to prepare the Avaya Aura™ Contact Center Release 6.0/6.1 server and client software to handle inbound and outbound voice and multimedia contacts. Commissioning the server and client software prepares the hardware to run the contact center. If you want to make additional changes to the contact center server configuration, see the *Avaya Aura™ Contact Center Server Administration* (NN44400-610).

Prerequisites

- Read the *Avaya Aura™ Contact Center Overview* (NN44400-111).
- Read the *Avaya Aura™ Contact Center Fundamentals* (NN44400-110).
- Read the *Avaya Aura™ Contact Center Planning and Engineering* (NN44400-210).
- Complete the *Avaya Aura™ Contact Center Installation Checklist* (NN44400-310).
- Ensure that you understand the Contact Center features that you purchased.
- Install or migrate your Contact Center Release 6.0/6.1 software.
- Ensure that you know where each Contact Center component is installed.

Navigation

- [Avaya Aura™ Contact Center server commissioning \(page 11\)](#)
- [Networked Avaya Aura™ Contact Center commissioning \(page 17\)](#)
- [Contact Center Manager Server commissioning \(page 21\)](#)
- [Network Control Center commissioning \(page 33\)](#)
- [Contact Center Manager Administration commissioning \(page 37\)](#)
- [Security Framework commissioning \(page 57\)](#)
- [Contact Center Manager Administration client commissioning \(page 73\)](#)
- [Communication Control Toolkit commissioning for Contact Center \(page 83\)](#)
- [Contact Center Multimedia server commissioning \(page 121\)](#)
- [Agent Desktop client commissioning \(page 137\)](#)
- [External Web communication server commissioning \(page 141\)](#)
- [High Availability Campus co-resident server commissioning \(page 149\)](#)
- [High Availability Campus CCMM commissioning \(page 191\)](#)
- [Common procedures \(page 203\)](#)

Introduction

- [Integrated Reporting commissioning \(page 209\)](#)
- [Contact Center Manager Server Web service configuration \(page 221\)](#)
- [Communication Control Toolkit Web service configuration \(page 227\)](#)

Networked Avaya Aura™ Contact Center commissioning

Commission the Contact Center Manager Server and Contact Center Manager Administration components on a networked server to manage your contact center environment.

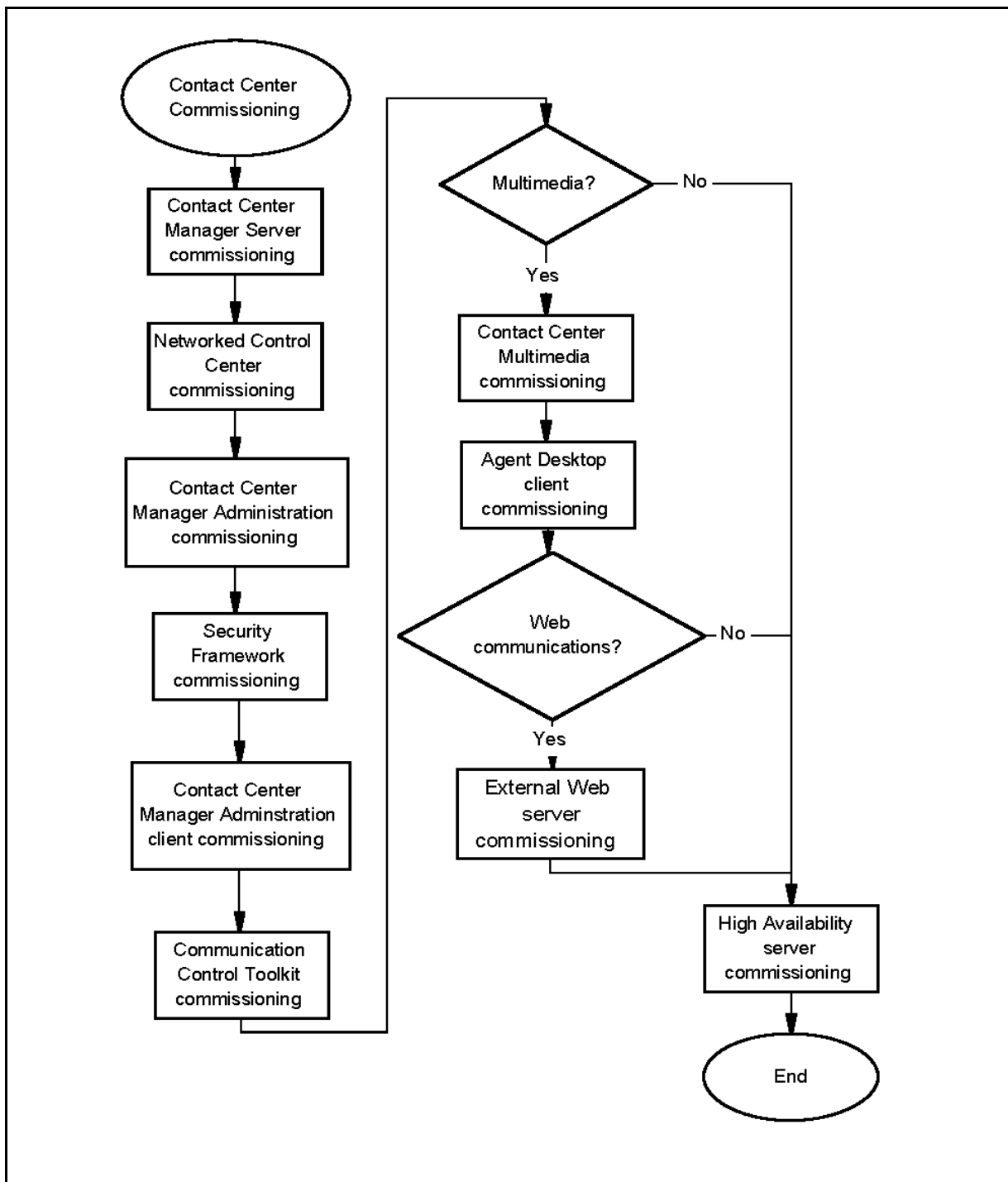
Prerequisites to commission the networked contact center

- Install or migrate your Contact Center software.
- Install more than one Contact Center Manager Server.

Contact Center commissioning tasks

This work flow shows you the sequence of tasks you perform to commission the networked Contact Center. To link to any tasks, go to [Networked Contact Center commissioning work flow \(page 18\)](#).

Networked Contact Center commissioning work flow



Networked Contact Center commissioning navigation

- [Contact Center Manager Server commissioning \(page 21\)](#)
- [Network Control Center commissioning \(page 33\)](#)

- [Contact Center Manager Administration commissioning \(page 37\)](#)
- [Security Framework commissioning \(page 57\)](#)
- [Contact Center Manager Administration client commissioning \(page 73\)](#)
- [Communication Control Toolkit commissioning for Contact Center \(page 83\)](#)
- [Contact Center Multimedia server commissioning \(page 121\)](#)
- [Agent Desktop client commissioning \(page 137\)](#)
- [External Web communication server commissioning \(page 141\)](#)
- [High Availability Campus co-resident server commissioning \(page 149\)](#)

Contact Center Manager Server commissioning

Use the procedures in this section to configure the Contact Center Manager Server software in your Avaya Aura™ Contact Center. The procedures outlined include configuring your passwords, configuring features and verifying the success of your installation to prepare your server for Contact Center operations.

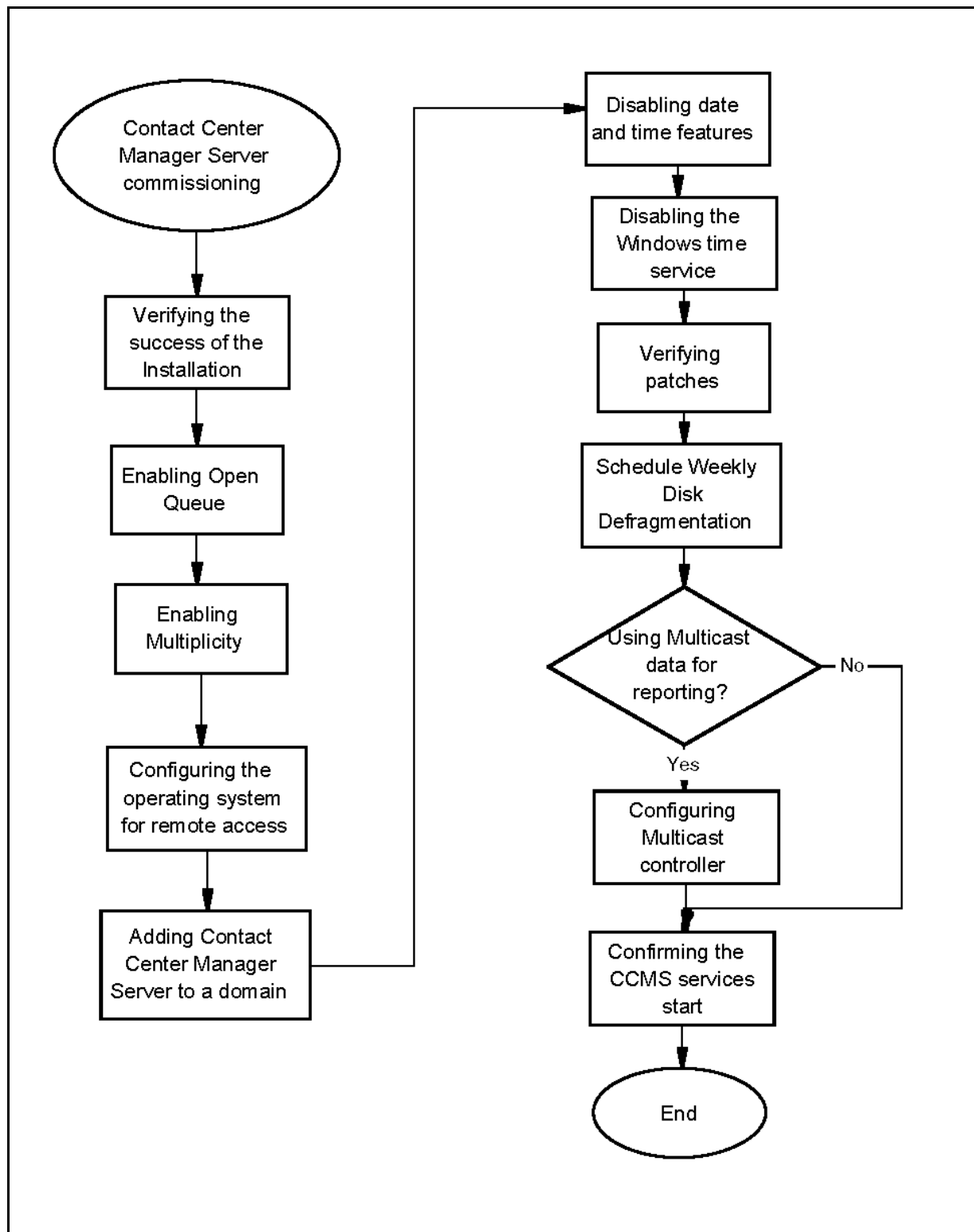
Prerequisites for Contact Center Manager Server commissioning

- Read the *Avaya Aura™ Contact Center Planning and Engineering* (NN44400-210).
- Complete the *Avaya Aura™ Contact Center Installation Checklist* (NN44400-310).
- Install the Contact Center Manager Server software.
- Install the other Contact Center components on your server.

Commissioning Contact Center Manager Server

This task flow shows you the sequence of procedures you perform to configure Contact Center Manager Server. To link to any task, go to [Navigation for commissioning Contact Center Manager Server \(page 23\)](#).

Contact Center Manager Server commissioning procedures



Navigation for commissioning Contact Center Manager Server

- [Verifying the success of the installation \(page 23\)](#)
- [Enabling Open Queue \(page 24\)](#)
- [Enabling Multiplicity \(page 24\)](#)
- [Configuring the operating system for remote access \(page 26\)](#)
- [Adding a server to a domain \(page 206\)](#)
- [Disabling date and time features \(page 26\)](#)
- [Disabling the Windows time service \(page 27\)](#)
- [Verifying CCMS patches \(page 28\)](#)
- [Scheduling Weekly Disk Defragmentation \(page 28\)](#)
- [Configuring the Multicast controller \(page 29\)](#)
- [Confirming the CCMS services start \(page 30\)](#)

Job aid: Timing

The estimated time to commission Contact Center Manager Server is 1 hour.

Verifying the success of the installation

Verify the success of your installation to ensure that all components are installed. To verify the success of the installation, ensure that the Contact Center Manager Server services are running.

Prerequisites

- Install the Contact Center Manager Server software.

Procedure steps

Step	Action
1	Log on to the server on which you installed Contact Center Manager Server as administrator.
2	Click Start, All Programs, Avaya, Contact Center, Common Utilities, System Control and Monitor Utility .
3	On the CCMS tab, check that all relevant services are in the Up state.
4	If you install a SIP-enabled Contact Center, verify that the SIP services started.
5	Close the System Control and Monitor Utility window.

--End--

Enabling Open Queue

Enable Open Queue to allow third parties including Contact Center Manager Multimedia to create, read, and delete multimedia and voice contacts in Contact Center Manager Server.

Prerequisites

- Install the Open Queue feature.
- Ensure that the Contact Center License Manager is licensed to provide Open Queue session licenses.
- Ensure that the Contact Center License Manager is licensed to provide agent licenses for the required contact types.

Attention: You must restart your server at the end of this procedure.

Procedure steps

Step	Action
1	Log on to the server on which you installed Contact Center Manager Server.
2	Click Start, All Programs, Avaya, Contact Center, Manager Server, Server Configuration .
3	Click the Licensing tab.
4	From the CCMS Optional Packages list, select Open Queue .
5	Click OK .
6	Click Yes to restart the server.

--End--

Procedure job aid

After you restart Contact Center Manager Server, Open Queue is enabled. You must configure Controlled Directory Numbers (CDNs), also known as route points. The server uses these route points to route multimedia contacts. For more information, see the [Contact Center Multimedia server commissioning \(page 121\)](#).

Enabling Multiplicity

Enable Multiplicity to allow agents manage multiple contact types at the one time. Configure multiplicity presentation classes (MPC) in CCMA. Each agent is assigned either the default MPC or a customized MPC. Enable multiplicity in the licensing tab of the Server Configuration utility.

Prerequisites

- Ensure that the Contact Center License Manager is licensed to provide Multiplicity.
- Ensure that the Contact Center License Manager is licensed to provide agent licenses for the required contact types.

Attention: You must restart your server at the end of this procedure.

Procedure steps

Step	Action
1	Log on to the server on which you installed Contact Center Manager Server.
2	Click Start, All Programs, Avaya, Contact Center, Manager Server, Server Configuration .
3	Click the Licensing tab.
4	From the CCMS Optional Packages list, select Multiplicity .
5	Click OK .
6	Click Yes to restart the server.

--End--

Procedure job aid

After you restart Contact Center Manager Server, Multiplicity is enabled. Configure contact center agents for multiplicity in Contact Center Manager Administration using Multiplicity Presentation Classes. For more information, see the *Avaya Aura™ Contact Center Manager Administration – Client Administration* (NN44400-611).

Configuring the operating system for remote access

Configure remote access for your server to allow technical support to access the server.

Prerequisites

- If you use Contact Center Manager Server in a domain, add your Contact Center Manager Server to the domain before you configure remote access.

Procedure steps

Step	Action
1	Log on to the server on which you installed Contact Center Manager Server.
2	Click Start, Control Panel, System and Security, System .
3	Click Remote settings .
4	In System Properties , select the Remote tab.
5	Under Remote Desktop , select Allow connections from computers running any version of Remote Desktop (less secure) .
6	Click OK .

--End--

Disabling date and time features

Disable the date and time features in Microsoft Windows to avoid potential call processing outages.

The contact center applications do not support time changes other than the Daylight Savings Change. Changing time causes issues with states of contacts.

If the Contact Center Manager Server is in a SIP environment, or is a Non Voice Multimedia installation, or is the Network Control Center server, skip this procedure.

Procedure steps

Step	Action
1	Click Start, Control Panel .
2	Under Clock, Language, and Region , click Set the time and date .
3	In the Date and Time dialog box, click Change time zone .
4	Clear the Automatically adjust clock for daylight saving changes check box.
5	Click OK .

- 6 Click the **Internet Time** tab.

Attention: If you click this tab and click OK without making changes, the Startup type for the Windows Time service is configured to Automatic.

- 7 Click **Change Settings**.
- 8 Clear the **Synchronize with an Internet time server** check box.
- 9 Click **OK**.
- 10 Click **OK** to close the dialog box.

--End--

Disabling the Windows time service

The Windows Time service could attempt to synchronize the CCMS server time with a time source, this could cause potential call processing outages. To avoid these potential problems, disable the Windows Time service.

If the Contact Center Manager Server is in a SIP environment, or is a Non Voice Multimedia installation, or is the Network Control Center server, skip this procedure.

Prerequisites

- Disable Date and Time features. See [Disabling date and time features \(page 26\)](#).

Procedure steps

- | Step | Action |
|------|--|
| 1 | Click Start, Administrative Tools, Services . |
| 2 | In the Services window, in the right pane, double-click Windows Time . |
| 3 | In the Windows Time Properties dialog box, on the General tab, from the Startup type list, select Disabled . |
| 4 | Click Stop . |
| 5 | Click Apply to save your changes. |
| 6 | Click OK to close the Windows Time Properties dialog box. |
| 7 | Close the Services window. |

--End--

Verifying CCMS patches

Verify that you have the most recent patches for the Contact Center Manager Server software to ensure that your system runs the most up-to-date software.

Prerequisites

- Look up the most recent patches and upgrades for Contact Center Manager Server at www.avaya.com/support.
- Review *Avaya Aura™ Contact Center Upgrade and Patches* (NN44400-410) to understand how to install patches and service packs.

Procedure steps

Step	Action
1	Log on to the server on which you installed Contact Center Manager Server.
2	Click Start, All Programs, Avaya, Contact Center, Common Utilities, Contact Center Patch Manager .
3	Click the Contact Center Manager Server tab.
4	View the Update Name .
5	Compare the update name in the Patch Manager with the most recent patch or upgrade listed on the Avaya Web site.
6	Click Close .
7	Install missing updates and patches from the Web site.

--End--

Scheduling Weekly Disk Defragmentation

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

Perform this procedure twice to create two scheduled tasks: one for drive C and one for drive D. Make sure you give each task a different start time to allow the previous task to finish.

Procedure steps

Step	Action
1	Click Start, Computer .
2	Right-click drive C , 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 if you plan 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.

If you plan to use the unicast delivery method, no configuration of the Contact Center Manager Server is required 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 server on which you installed Contact Center Manager Server as administrator. |
| 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 | In the Compression section of the window, select the RTD Compression check box. |

- 5 Clear the **RSM Compression** check box.
- 6 Click **Apply**.
- 7 Click **OK**.
- 8 Click **Start, All Programs, Avaya, Contact Center, Manager Server, Multicast Address and Port Configuration**.
- 9 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.

This is the same address as the Contact Center Manager Administration server receiving IP multicast address.
- 10 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.

Attention: Do not change the ports.

- 11 For the **Interval to Date, Moving Window IP Port**, and **Multicast Rate** boxes, accept the default values.
- 12 Click **Apply**.
- 13 Click **OK**.
- 14 Click **Start, All Programs, Administrative Tools, Services**.
- 15 Scroll down to **CCMS SDP_Service**.
- 16 Click **Restart**.

--End--

Confirming the CCMS 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 Manager Server. |

- 2 Click **Start, All Programs, Avaya, Contact Center, Common Utilities, System Control and Monitor Utility**.
- 3 Click the **Contact Center** tab.
- 4 Select the applications to start on the current server by selecting the application name check boxes.
- 5 Click **Start Contact Center**.
- 6 Click the **CCMS** tab.
- 7 Ensure that all services in the **Profile** box have a green circle next to them.
- 8 If some of the services do not start, click **Start CCMS**.
- 9 Click **Close**.

--End--

Network Control Center commissioning

Configure the communications database to enable the distribution of information from the Network Control Center (NCC) database to all servers on the network and to enable communication and network skill-based routing (NSBR) among multiple sites. The communications database lists all servers in the network, including each IP addresses and status.

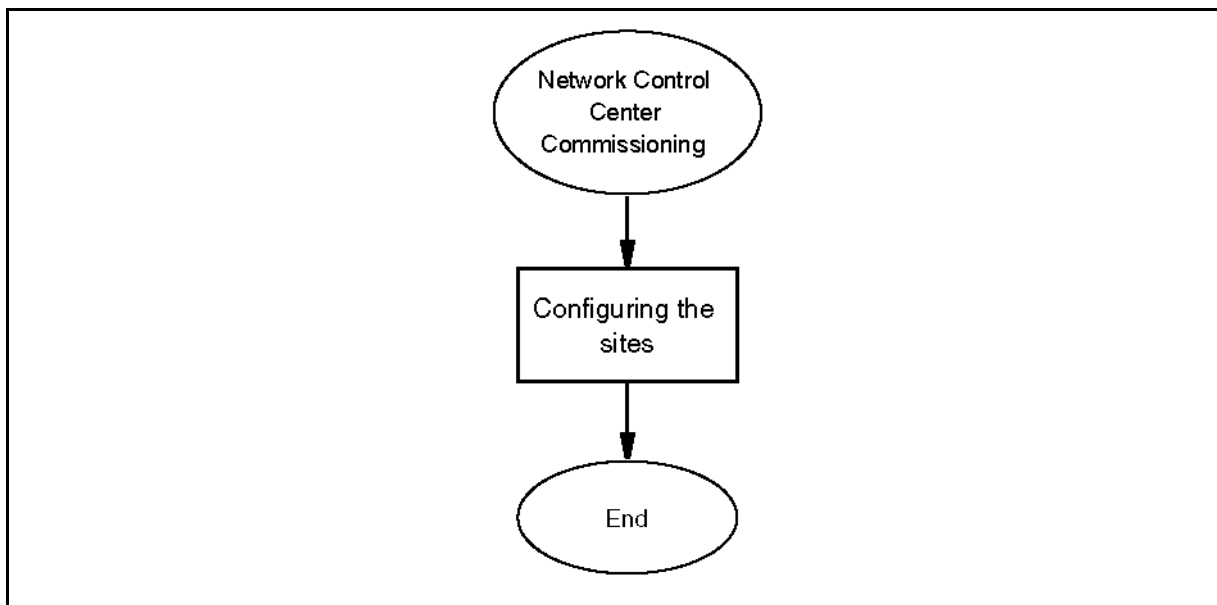
Prerequisites for Network Control Center commissioning

- Install the Network Control Center server software.
- Install a Contact Center Manager Server at each site.
- Install and commission the Contact Center License Manager software.
- Install and commission Contact Center Manager Administration.
- If you use an Avaya Communication Server 1000, configure the following elements:
 - NACD (not required for Universal Networking)
 - a CDN for the server to use as an MCDN Network CDN (not required for Universal Networking)
 - Landing Pads (required for Universal Networking only)
 - a dialing plan to facilitate call routing between the telephony switches
- If you use a Microsoft Office Communications Server (with a Communication Server 1000 PABX for voice calls), configure a dialing plan to facilitate call routing between the telephony switches (on the Avaya Communication Server 1000).
- Ensure that all site names and the CLAN IP addresses are unique.

Network Control Center commissioning procedures

This task flow shows you the sequence of procedures you perform to commission the Network Control Center to use for the first time. To link to any task, go to [Network Control Center commissioning navigation \(page 34\)](#).

Network Control Center commissioning navigation



Network Control Center commissioning navigation

- [Configuring the sites \(page 34\)](#)

Configuring the sites

Configure the sites on the networked Avaya Aura™ Contact Center on the Network Control Center server to designate the site names and locations.

Procedure steps

- | Step | Action |
|------|--|
| 1 | On the Network Control Center server, choose Start, Run . |
| 2 | In the Open box, type nbconfig –admin . |
| 3 | Click OK . |
| 4 | Click the Site Table tab. |

Attention: Do not select the Force Synchronization check box. When you force synchronization, you force each site in the network to request address table information from every other site in the network. This can result in unnecessary use of network bandwidth. (Normally, servers request address table updates only when the NCC notifies them that the site list changed.) Use the Force Synchronization option if information at a site is not updated.

- | | |
|---|--------------------|
| 5 | Click Add . |
|---|--------------------|

- 6 In the **CLAN IP Address** box, enter the CLAN IP address of the server.

Attention: Each server must have a unique CLAN IP address.

- 7 Click **OK**.
- 8 Repeat [step 5](#) to [step 7](#) for each server on your network.
- 9 After you add the servers, click **Verify** to validate the connection to the nodal servers.
- 10 If all site names are correct, click **Apply** to update the database and synchronize the site table.
The Flags column shows the progress of synchronization.
- 11 Click **Refresh** to update the status of the flags. Synchronization is complete when an N appears in the Flags column beside the NCC, and an S appears beside each server.
- 12 Click the **Address Table** tab.
The communication addresses of the new servers appear on the Address Table page.

--End--

Contact Center Manager Administration commissioning

Commission Contact Center Manager Administration (CCMA) after you install Contact Center Manager Administration server software to prepare your server for Avaya Aura™ Contact Center operations.

Contact Center Manager Administration security access allows a user with full access to configure your Contact Center. If you plan to use the Security Framework for your Contact Center, Avaya recommends that you do not use the Contact Center Manager Administration security. For more information about the Security Framework configuration, see [Security Framework commissioning \(page 57\)](#).

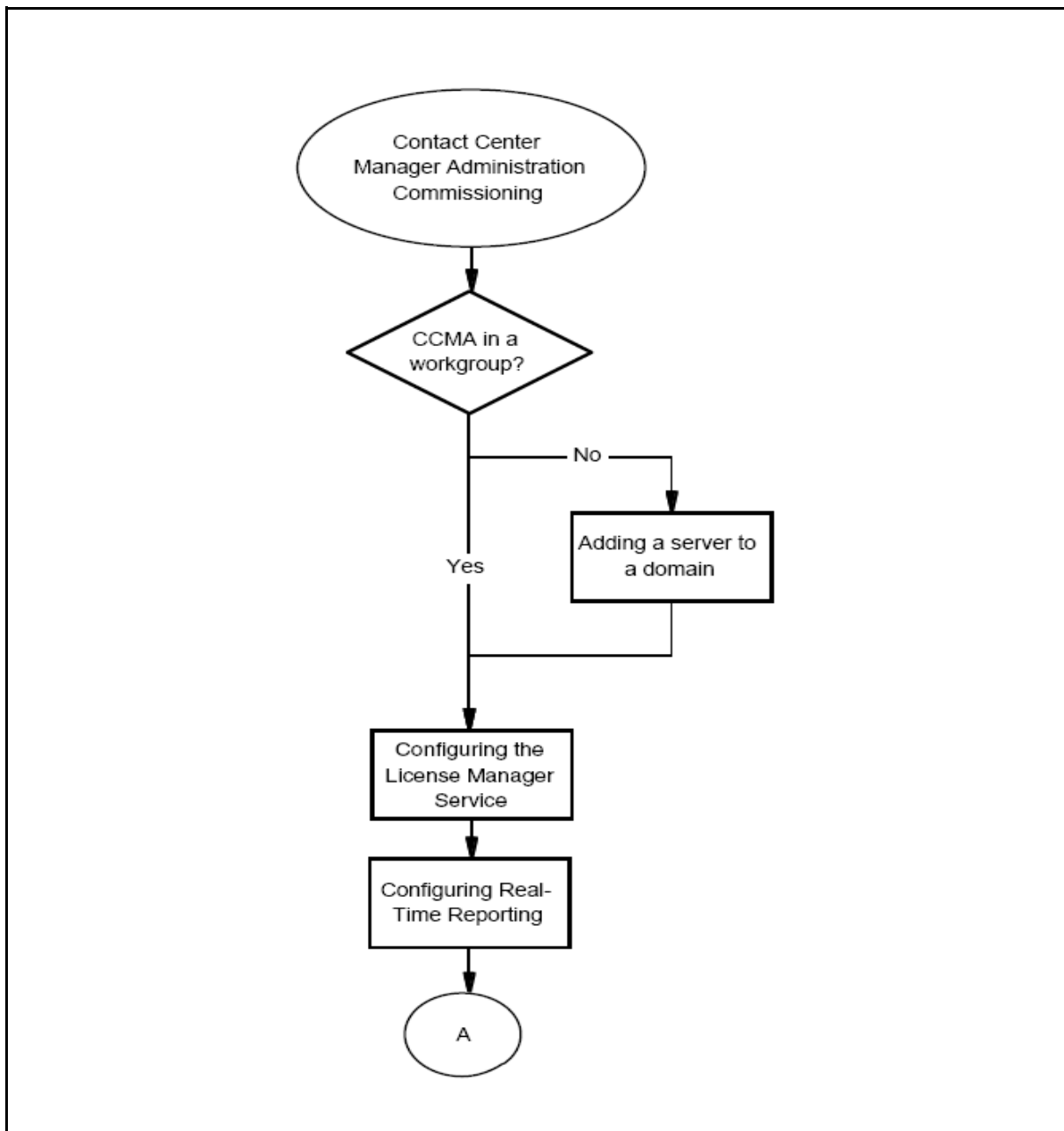
Prerequisites for Contact Center Manager Administration commissioning

- Install the Contact Center Manager Administration software.
- Read *Avaya Aura™ Contact Center Fundamentals* (NN44400-110).
- Ensure that you have administrator privileges on the server on which you installed the Contact Center Manager Administration server software.

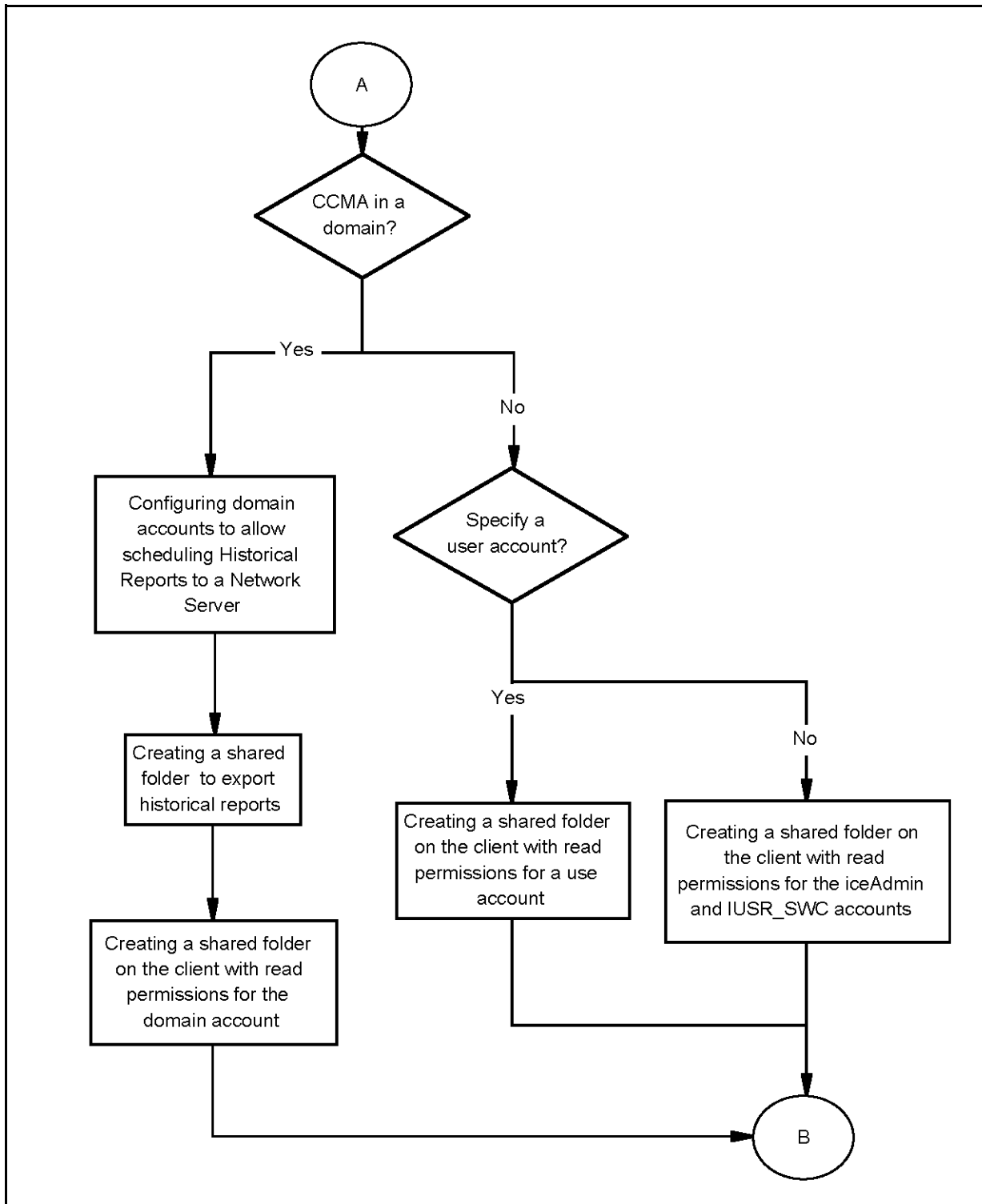
Contact Center Manager Administration commissioning procedures

This task flow shows you the sequence of procedures you perform to commission Contact Center Manager Administration. To link to any task, go to [Contact Center Manager Administration commissioning navigation \(page 40\)](#).

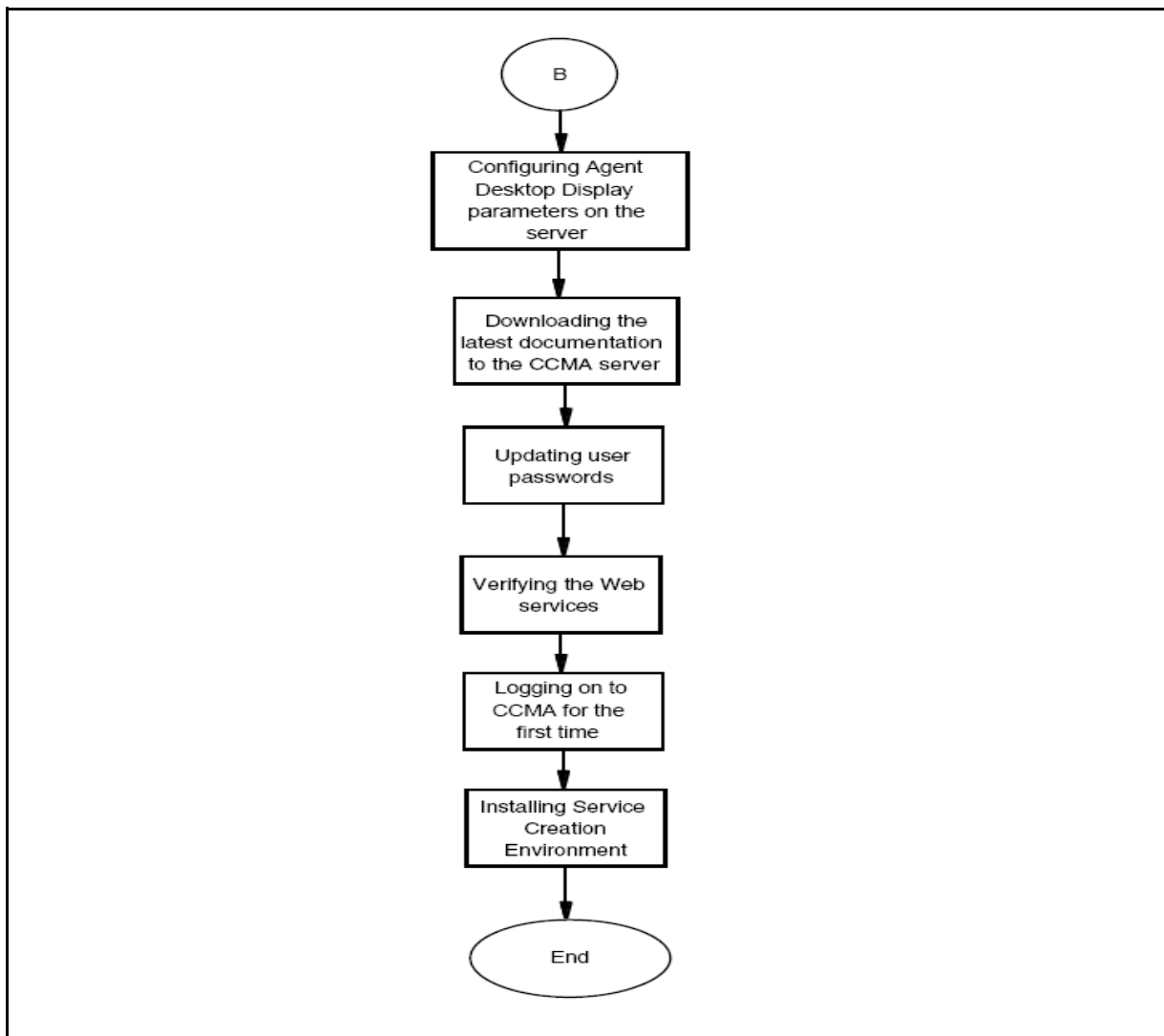
Contact Center Manager Administration commissioning procedures



Contact Center Manager Administration commissioning procedures (continued)



Contact Center Manager Administration commissioning procedures (continued)



Contact Center Manager Administration commissioning navigation

- [Configuring the License Manager Service \(page 41\)](#)
- [Configuring Real-Time Reporting \(page 42\)](#)
- [Updating the iceAdmin user password \(page 44\)](#)
- [Configuring domain accounts to allow scheduling Historical Reports to a Network Server \(page 45\)](#)
- [Creating a shared folder to export historical reports \(page 45\)](#)
- [Creating a shared folder on the client with read permissions for the domain \(page 46\)](#)

- [Creating a shared folder on the client with read permissions for a user \(page 47\)](#)
- [Creating a shared folder on the client PC with read permissions for the IUSR_SWC and iceAdmin accounts \(page 48\)](#)
- [Configuring Agent Desktop Display parameters on the server \(page 49\)](#)
- [Downloading the latest documentation to the CCMA server \(page 52\)](#)
- [Verifying the Web Services \(page 53\)](#)
- [Logging on to Contact Center Manager Administration for the first time \(page 53\)](#)
- [Installing the Service Creation Environment client \(page 55\)](#)

Job aid: Timing

The estimated time to commission Contact Center Manager Administration is 1 hour.

Configuring the License Manager Service

Configure the License Manager Service for the Report Creation Wizard component to function if your Contact Center Manager Administration server is not co-resident with another Contact Center application.

If you installed the Contact Center Manager Administration server software co-resident with Contact Center Manager Server, the IP address and port number are set up by the Contact Center Manager Server installation procedure.

Prerequisites

- Install the Contact Center Manager Administration server software on a stand-alone server.
- Ensure that you have administrator privileges on the server on which you installed the Contact Center Manager Administration server software.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server as an administrator.
2	Click Start, All Programs, Avaya, Contact Center, Manager Administration, Configuration .
3	In the left pane, expand Avaya, Applications, LM Service Configuration .
4	In the right pane, click the LM Service Configuration icon.

- 5 In the **LM Service – Configuration Setup** dialog box, in the **Primary Server's IP Address** boxes, type the IP address for the primary License Manager server.
- 6 In the **Primary Server's Port** box, type port number for the primary License Manager server.
- 7 If you have a standby License Manager server, in the **Standby Server's IP Address** boxes, type the IP address for the standby License Manager server.
- 8 If you have a standby License Manager server, in the **Standby Server's Port** box, type the port number for the standby License Manager server.
- 9 Click **OK** to submit the information.
- 10 In the **Configuration Completed** dialog box, click **OK**.
A dialog box appears and prompts you to restart the License Manager Service.
- 11 Click **Yes**.
- 12 Click **OK**.
- 13 Close all windows.

--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 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.

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.
- If the Contact Center Manager Server is part of a networked Contact Center, ensure that all Contact Center Manager Servers within the network have the same multicast IP address.

Procedure steps

- | Step | Action |
|------|--|
| 1 | Log on to the server on which you installed the Contact Center Manager Administration server software. |
| 2 | Click Start, All Programs, Avaya, Contact Center, Manager Administration, Configuration . |
| 3 | In the Avaya Applications Configuration window, in the left pane, 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. |
| 6 | In the IP Send Address box, type the Contact Center Manager Administration server sending IP multicast address. |
| 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: <ul style="list-style-type: none"> 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 .

<i>The Restart ICERTdService status window appears while the service is restarting, and closes after the service successfully restarts.</i> |
| 15 | Close all windows to complete the procedure. |

--End--

Procedure job aid

You may need to increase the OAM Timeout value if the following situations occur:

- You can see no partition elements in the right pane when you create or view a partition in Access and Partition Management. This can occur when a large amount of data is stored on Contact Center Manager Server and the network is slow.
- Your Contact Center has a large numbers of agents or skillsets. In this case, it may not be possible to return a large list of agents or skillsets when you view a report using the Historical Reporting component.

If you increase the OAM Timeout value, this provides more time to collect the partition elements on each server. Avaya recommends that you increase this value in increments of 10 000 (milliseconds).

Updating the iceAdmin user password

Update the iceAdmin account password on your Contact Center Manager Administration server using the ICEADMIN password change utility.

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

Procedure steps

Step	Action
1	Log on the server on which you installed the Contact Center Manager Administration server software.
2	Click Start, All Programs, Avaya, Contact Center, Manager Administration, Configuration .
3	In the Avaya Applications Configuration window, in the left pane, expand Avaya, Applications, iceAdmin Password Change .
4	In the right pane, click the iceAdmin Password Change icon.
5	In the Old Password box, type the current password for the iceAdmin user account.

Attention: If you use this utility for the first time, you cannot enter the old password because the box is dimmed.

6	In the New Password box, type the new password for the iceAdmin user account.
7	In the Confirm Password box, type the new password again.

8 Click **OK**.

--End--

Configuring domain accounts to allow scheduling Historical Reports to a Network Server

If Contact Center Manager Administration is on a domain, configure domain accounts to allow Historical Reports to run and be saved on a network server.

Prerequisites

- Understand how to update the iceAdmin user password; see [Updating the iceAdmin user password \(page 44\)](#).

Procedure steps

Step	Action
1	Run the iceAdminPasswordChange utility.
2	Click the Domain Account icon.
3	Update the Domain Name, Domain User and Password.
4	Click OK .

--End--

Creating a shared folder to export historical reports

Create a shared folder to export historical reports if you want multiple users to access scheduled historical reports stored in this folder from other computers.

Prerequisites

- Grant change and read permissions to users who can access the scheduled report account; for example, the iceAdmin account or the domain account.

Procedure steps

Step	Action
1	Log on to the server on which you installed the Contact Center Manager Administration server software.
2	Create a folder. Name the folder Exported Reports .
3	Right-click the new folder and select Properties .
4	In the Properties dialog box, on the Sharing page, click Advanced Sharing .

- 5 Select **Share this folder**.
- 6 Click **Permissions**.
- 7 Click **Add**.
- 8 In the **Select Users or Groups** dialog box, click **Advanced**.
- 9 Click **Find Now**.
- 10 In the expanded portion of the **Select Users or Groups** dialog box, locate and select the **iceAdmin** account.
OR
Select the domain account used for IIS directory security.
- 11 Click **OK**.
- 12 In the **Select Users or Groups** dialog box, click **OK**.
- 13 In the **Permissions** dialog box, select the account that you selected in [step 10](#).
- 14 Select the **Allow** check box for the following:
 - **Change**
 - **Read**
- 15 Click **Apply**.
- 16 Click **OK** to close the **Permissions for Exported Reports** dialog box.
- 17 Click **OK** to close the **Advanced Sharing** dialog box.
- 18 Click **OK** to close the **Exported Reports Properties** dialog box.

--End--

Creating a shared folder on the client with read permissions for the domain

Create a shared folder with read permissions on the client for the domain account if Contact Center Manager Administration is part of a network domain. Use the shared folder to synchronize historical reports.

Prerequisites

- Ensure that Contact Center Manager Administration is part of a network domain.
- Configure the domain account. See [Configuring domain accounts to allow scheduling Historical Reports to a Network Server \(page 45\)](#).

Procedure steps

Step	Action
------	--------

- 1 On the client, create a folder.
- 2 Right-click the shared folder, and select **Properties**.
- 3 In the **New folder Properties** dialog box, click the **Sharing** tab.
- 4 Click **Advanced Sharing**.
- 5 Click **Share this folder**.
- 6 Click **Permissions**.
- 7 In the **Permissions for New folder** dialog box, Select **Everyone**.
- 8 Click **Remove** to remove the Everyone account.
- 9 Click **Add**.
- 10 In the **Select Users or Groups** dialog box, click **Advanced**.
- 11 Click **Find Now**.
- 12 In the expanded portion of the **Select Users or Groups** dialog box, locate and select the domain or directory security user account used to join the Contact Center Manager Administration server to the network domain.
- 13 Click **OK**.
- 14 In the **Select Users or Groups** dialog box, click **OK**.
- 15 In the **Permissions for New folder** dialog box, select the newly added group or user name account.
- 16 Select the **Allow** check box for **Read**.
- 17 Click **OK**.
- 18 Click **OK**.
- 19 Click **OK** to save your changes and close the **New folder Properties** dialog box.

--End--

Creating a shared folder on the client with read permissions for a user

Create a shared folder with read permissions on the client for a user account to ensure that the user can access the folder on the client.

Prerequisites

- If Contact Center Manager Administration is part of a domain, configure the domain account. See [Configuring domain accounts to allow scheduling Historical Reports to a Network Server \(page 45\)](#).

Procedure steps

Step	Action
------	--------

- 1 On the client, create a folder.
- 2 Right-click the folder, and select **Properties**.
- 3 In the **New folder Properties** dialog box, click the **Sharing** tab.
- 4 Click **Advanced Sharing**.
- 5 Click **Share this folder**.
- 6 Click **Permissions**.
- 7 In the **Permissions for New folder** dialog box, select the user login name.
- 8 Select the **Allow** check box for **Read**.
- 9 Clear all other check boxes.
- 10 Click **Apply**.
- 11 Click **OK**.
- 12 Click **OK**.
- 13 In the **New folder Properties** dialog box, click **Close**.

--End--

Creating a shared folder on the client PC with read permissions for the IUSR_SWC and iceAdmin accounts

If Contact Center Manager Administration is part of a workgroup, create a shared folder on the client PC with Read permissions for the IUSR_SWC and iceAdmin accounts.

If you choose this option, you must maintain two additional accounts on the client PC. Security issues can arise because the Contact Center Manager Administration server uses these accounts to run the Web site.

Prerequisites

- Ensure that Contact Center Manager Administration is part of a workgroup.

Procedure steps

- | Step | Action |
|------|---|
| 1 | On the client, create a folder. |
| 2 | Right-click the folder, and select Properties . |
| 3 | In the New folder Properties dialog box, click the Sharing tab. |
| 4 | Click Advanced Sharing . |
| 5 | Click Share this folder . |

- 6 Click **Permissions**.
- 7 In the **Permissions for New folder** dialog box, Select **Everyone**.
- 8 Click **Remove** to remove the Everyone account.
- 9 Click **Add**.
- 10 In the **Select Users or Groups** dialog box, click **Advanced**.
- 11 Click **Find Now**.
- 12 In the expanded portion of the **Select Users or Groups** dialog box, locate and select the **IUSR_SWC** user account.
- 13 Click **OK**.
- 14 In the **Select Users or Groups** dialog box, click **OK**.
- 15 In the **Permissions** dialog box, select **IUSR_SWC**.
- 16 Select the **Allow** check box for **Read**.
- 17 Click **Apply**.
- 18 Perform [step 9](#) to [step 17](#) to add read permissions for the iceAdmin user account.
- 19 Click **OK**.
- 20 Click **OK** to close the **Advanced Sharing** dialog box.
- 21 Click **Close** to close the **New folder Properties** dialog box.

--End--

Configuring Agent Desktop Display parameters on the server

Configure parameters on the Contact Center Manager Administration server to use Agent Desktop Display on a client.

Prerequisites

- Ensure that you have administrative privileges on the server on which you installed the Contact Center Manager Administration server software.

Procedure steps

- | Step | Action |
|------|--|
| 1 | Log on to the server on which you installed the Contact Center Manager Administration server software. |
| 2 | Click Start, All Programs, Avaya, Contact Center, Manager Administration, Agent Desktop Displays, Server Configuration Parameters . |

- 3 In the **Configuration Parameters** dialog box, in the **IP multicast address** box, confirm that the address is the Contact Center Manager Administration server IP send address that you configured in the RTR Configuration Tool.
- 4 In the **Refresh rate (seconds)** box, type the rate in seconds at which you want the real-time data in the displays to be refreshed.
- 5 In the **Max agents** box, type the maximum number of agents who can simultaneously log on to the Agent Desktop Display component and view the real-time statistics.
- 6 From the **View mode** list, select the mode in which you want to view the collected data:
 - **Moving window**
 - **Interval-to-date**
- 7 To require agents to log on to their phones before they can start Agent Desktop Display, select the **Agents phoneset login required for ADD** check box.
If this check box is clear, when an agent logs on to Agent Desktop Display, the agent sees data only if other agents log on to skillsets to which that agent is assigned.
- 8 To disable automatic notifications for Agent Desktop Display client upgrades, select the **Disable Automatic ADD Client Upgrade** check box .
If you select this check box, agents receive no prompts to download available Agent Desktop Display client upgrades.
- 9 In the **Statistics Configuration** table, choose the statistics to appear in the Agent Desktop Display. You can add statistics columns to the displays or remove columns that you no longer want to show.
- 10 To add the statistics column to the displays, select the **Show** check box for each statistic.
- 11 Use the column order buttons to arrange the order in which the statistics columns appear. Select the statistic to move, and then click the up or down button to change its position.

The statistic that you place at the top of the Statistics Configuration table appears in the first column of the display.
- 12 To assign the threshold display color, select a statistic.
- 13 From the following lists, select the threshold color for the highlighted statistic:
 - **Less than Level 1**
 - **Between Level 1 and Level 2**
 - **Greater than Level 2**
If you configure no threshold levels in the Configuration component of Contact Center Manager Administration or in Contact Center Manager Server, the values appear in white in the Agent Desktop Display.

- 14 Repeat [step 12](#) to [step 13](#) for each statistic for which you want to configure threshold display colors.
- 15 If you want the selected statistic to blink in the Agent Desktop Display when its value reaches the threshold, select the **Blink** check box.
- 16 If you want the Agent Desktop Display to beep when the threshold value reaches the threshold, select the **Beep** check box.
- 17 If you did not select the **Beep** check box, proceed to [step 20](#).
- 18 To indicate that a beep occurs only once, select **Once**.
- 19 To indicate that a beep occurs continuously until the statistic reaches an acceptable value, select **Continuously**.
- 20 Click **Save**.

--End--

Variable definitions

Variable	Value
IP multicast address	The IP multicast addresses that you select for RSM sending and receiving must be in the 224.0.1.0 to 239.255.255.255 range. Check with your network administrator for acceptable IP multicast addresses for your specific network.
Max agents	When the number of agents who log on to the application reaches this number, additional agents who try to log on receive a message informing them to try again later. If you leave this box empty, the system uses the default value of 1000 agents. The maximum value that you can type in this box is 3000 agents. For information about performance and sizing requirements for Contact Center Manager Administration, see the <i>Avaya Aura™ Contact Center Planning and Engineering</i> (NN44400-210).
Refresh rate	The minimum value that you can type in this box is 2 seconds. You must specify a value for the refresh rate.
View mode	Select one of the following view modes: • Moving window—In moving window mode, statistics represent the last 10 minutes of system activity. • Interval-to-date—In interval-to-date mode, statistics are collected only for the current interval. When the interval ends, data fields reset to 0 and collection begins for the next interval. The interval can correspond to a work shift or to another system-defined period.

Downloading the latest documentation to the CCMA server

Download the documentation related to the Contact Center Manager Administration server directly through the Help menu. You must copy the guides to the Documentation folder on the Contact Center Manager Administration server.

Because customer documentation is updated on a regular basis, you must download the latest versions of the documentation from the support site to the Documentation folder regularly to ensure that you have the most up-to-date information.

Prerequisites

- Download Adobe Acrobat Reader on the client to open the documents from the Contact Center Manager Administration server.

Procedure steps

Step	Action
1	Browse to www.avaya.com/support .
2	In the appropriate boxes, type your username and password.
3	Press Enter .
4	Click Customer Contact .
5	Click Contact Center Manager Server .
6	Locate the Documentation banner and click Show All .
7	Select the documents that you can access from the Contact Center Manager Administration: • Contact Center Manager Administration-Client Administration.pdf • Contact Center Fundamentals.pdf • Contact Center Performance Management.pdf • Contact Center Performance Management Data Dictionary.pdf • Contact Center Configuration-Service Creation Environment Application Development.pdf
8	Copy the documents to the Contact Center Manager Administration server.
9	Rename the documents to match the document names in step 7.
10	Move the documents to the document folder on the Contact Center Manager Administration server: <INSTALLDIR>\Avaya\Contact Center\Manager Administration\Apps\documentation\guides

Attention: The downloaded documents replace existing documents in the document folder.

--End--

Variable definitions

Variable	Value
<INSTALLDIR>	The Contact Center Manager Administration installation drive. The installer chooses the location during installation.

Verifying the Web Services

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

Procedure steps

Step	Action
1	Start Internet Explorer.
2	Enter the following: http://<ccmaservername>/supportutil/testwebservices.asp. The web services that appear in green are running correctly.

--End--

Logging on to Contact Center Manager Administration for the first time

When you log on to Contact Center Manager Administration for the first time, you must log on as the default administrator, webadmin. For security reasons, Avaya highly recommends that you change the default password when you first log on to the application. Contact Center Manager Administration user passwords can contain only English characters and special characters.

Prerequisites

- Configure Internet Explorer.
- Ensure that the Contact Center Manager Server name is registered with either the Domain Name Service (DNS) or the HOSTS table.

Procedure steps

Step	Action
1	Start Internet Explorer.

- 2 In the **Address** box, type the server name. For example, `http://<server name>`.

Attention: You must log on using the Contact Center Manager Administration server name instead of the IP address.

- 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 the default user name. For information about default login values, see *Avaya Aura™ Contact Center Server Administration* (NN44400-610).
- 6 In the **Old password** box, type the default password.
- 7 In the **New password** box, type a new password.

Contact Center Manager Administration user passwords can contain English characters and special characters only.
- 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, webadmin.

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, please contact support to have the webadmin password reset.

- 9 Click **Submit**.
- 10 In the main logon window, in the **User ID** box, type the user name.
- 11 In the **Password** box, type the new password.
- 12 Click **Login**.
- 13 Click **OK**.
- 14 In the **Server Name** box, type the computer name of the Contact Center Manager Server. Do not enter the fully qualified domain name.
- 15 Press **Tab**.

The server IP address automatically appears in the IP Address box.
- 16 In the **Display Name** box, type the name of the Contact Center Manager Server as you want it to appear in the system tree in Contact Center Manager Administration.

Attention: You must use the server name, not the server IP address, because using an IP address causes errors in Real-Time Reporting functionality. The system automatically assigns a display name that is the same as the server name. If you enter a different display name, the name must be unique.

- 17** In the **Login ID** box, type the sysadmin user name.
- 18** In the **Password** box, type the password for the Contact Center Manager Server. For information about default login values, see *Avaya Aura™ Contact Center Server Administration* (NN44400-610).
- 19** If you receive a logon sequence error message, log on to Server Utility to check your user name and password.
- 20** Click **Submit**.

The Contact Center Manager Administration launchpad appears.

--End--

Variable definitions

Variable	Value
<Contact Center Manager Administration Server name>	The name of the Contact Center Manager Administration server.

Installing the Service Creation Environment client

Install the Service Creation Environment to manage Contact Center applications. Applications are used to route contacts based on certain criteria from the contact such as skillset or customer name.

Perform the following procedure to ensure that the version of the Service Creation Environment that you start from within the Contact Center Manager Administration application is current. You can also install the Service Creation Environment on any client to work with script or flow applications without affecting the Contact Center environment. For instructions to install the Service Creation Environment on a client, see *Avaya Aura™ Contact Center Installation* (NN44400-311).

Procedure steps

- | Step | Action |
|----------|---|
| 1 | Start Internet Explorer. |
| 2 | In the Address box, type the server name. For example, <code>http://<Contact Center Manager Administration Server name></code> . |
| 3 | Press Enter . |

Contact Center Manager Administration commissioning

- 4 Log on to the Contact Center Manager Administration browser using the configured password
- 5 On the **Launchpad**, click **Scripting**.
- 6 In the **Scripting** window, on the menu, click **Service Creation**, and then click **Launch Service Creation**.
- 7 In the message box requesting you to download a .msi file, click **OK**.
- 8 In the dialog box, click **Run**.
- 9 In the **Service Creation Environment - InstallShield Wizard**, click **Next**.
- 10 In the **User Name**, type a name.
- 11 In the **Organization**, type your company name.
- 12 Select one of the following options:
 - **Anyone who uses this computer (all users)**
 - **Only for me (User Name)**
- 13 Click **Next**.
- 14 Accept the default **Destination Folder**.
OR
Click **Browse** to select a different location.
- 15 Click **Next**.
- 16 Click **Install**.
- 17 Click **Finish**.

--End--

Procedure job aid

Information about the Service Creation Environment is in *Avaya Aura™ Contact Center Configuration – Service Creation Environment Application Development* (NN44400-510).

Security Framework commissioning

Perform the procedures in this chapter to commission the Security Framework after you install Security Framework server software.

Use the Unified Communication Management utility to configure the Security Framework server software after you install it.

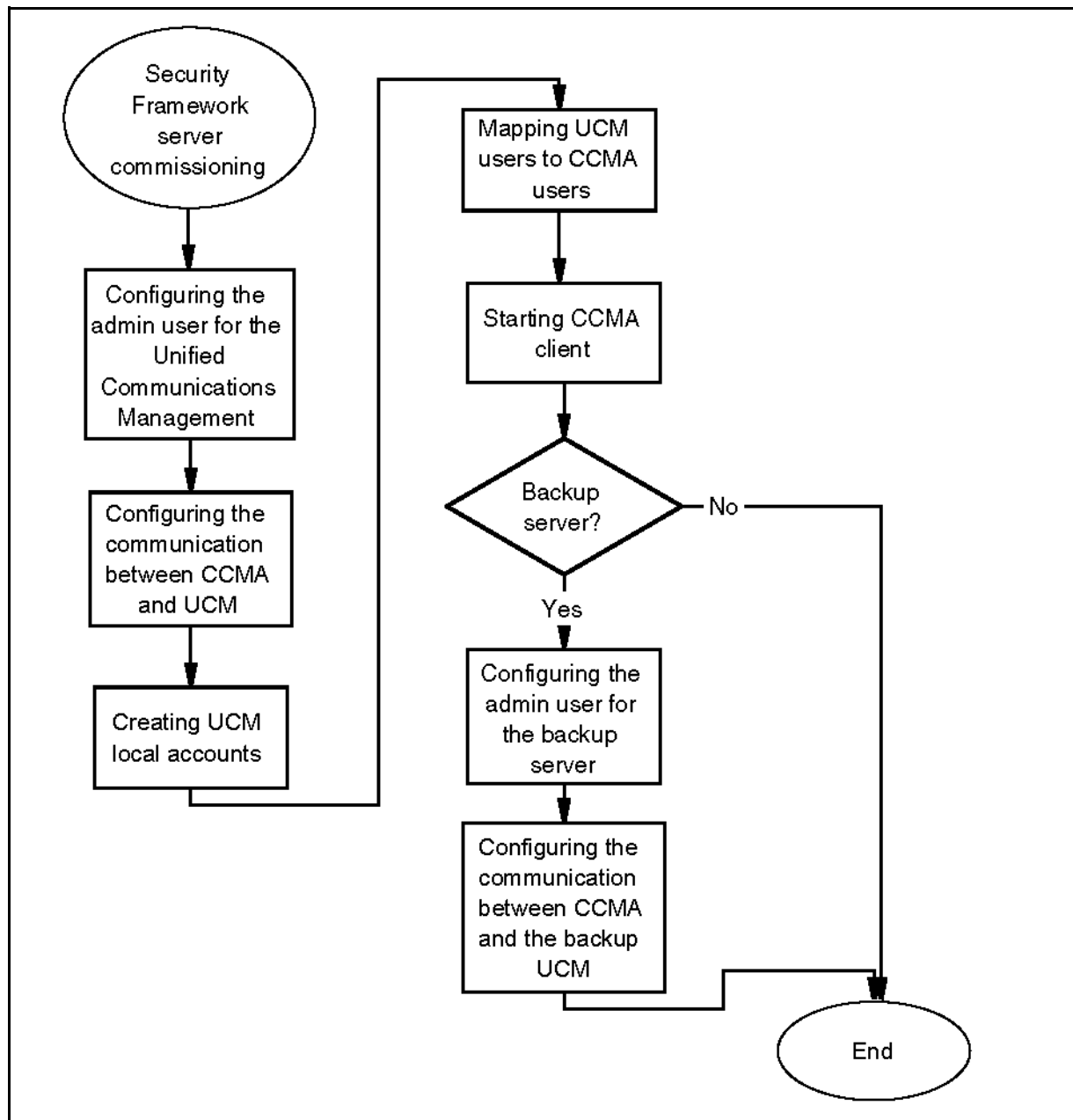
Prerequisites for Security Framework commissioning

- Install or upgrade the Contact Center Manager Administration software. See *Avaya Aura™ Contact Center Installation* (NN44400-311).
- Install the Security Framework either co-resident with Contact Center Manager Administration or on a stand-alone server.
- Read *Avaya Aura™ Contact Center Fundamentals* (NN44400-110).
- Ensure that you have administrator privileges on the server on which you installed the Contact Center Manager Administration server software.
- Ensure that you have administrator privileges on the server on which you installed the Security Framework software.

Security Framework commissioning procedures

This task flow shows you the sequence of procedures you perform to commission Security Framework. To link to any task, go to [Security Framework commissioning navigation \(page 58\)](#).

Security Framework commissioning procedures



Security Framework commissioning navigation

- [Configuring the admin user for the Unified Communication Manager \(page 59\)](#)
- [Configuring the communication between CCMA and UCM \(page 61\)](#)
- [Creating Unified Communication Management local accounts \(page 63\)](#)

- [Mapping Unified Communication Management users to CCMA users \(page 65\)](#)
- [Starting Contact Center Manager Administration client \(page 66\)](#)
- [Configuring the admin user for the backup server \(page 67\)](#)
- [Configuring the communication between CCMA and the backup UCM \(page 69\)](#)

Job aid: Timing

The estimated time to commission Security Framework is 1 hour.

Configuring the admin user for the Unified Communication Manager

Log on to the Security Framework Unified Communication Manager (UCM) for the first time and configure the administrator account used to secure Web traffic before you set up users.

Procedure steps

Step	Action
1	Log on to the server where the Security Framework is installed.
2	Start Internet Explorer .
3	In the URL box, type https://FQDN:<security port> . The FQDN is the fully qualified domain name for your server.
4	If the Digital Certificate window appears, click OK .
5	If any Security Alert message boxes appear, click Yes .
6	In the User ID box, type a local user name you use to log on to the server.
7	In the Password box, type the password for the account you use to log on to the server.
8	Click Log In .
9	Click Security Configuration .
10	Verify the Fully Qualified Domain Name and the Web Server IP address by selecting Yes . OR If your server is not on a domain, click No , and configure the Fully Qualified Domain Name and IP address for your server.
11	Click Next .
12	Select the Primary security server .

- 13 Click **Next**.
- 14 In the **Administrator password** box type a password for the admin account for the Unified Communication Management utility.
- 15 In the **Confirm Administrator password** box, retype the password.
- 16 Click **Next**.
- 17 In the **Certificate Information** window, in the **Friendly name** box, type a name for the certificate.
- 18 From the **Bit length** list, select the bit length.
- 19 In the **Organization** box, type the name for the organization using the security certificate.
- 20 In the **Organizational unit** box, type the name of the group of users using the security certificate.
- 21 In the **Common name** box, type the fully qualified domain name for the server.
- 22 From the **Country/Region** list, select your country or region.
- 23 In the **State/Province** box, type the name of your state or province.
- 24 In the **City/Locality** box, type the name of your city.
- 25 Click **Finish**.
- 26 After the configuration completes, click **Restart**.

--End--

Variable definitions

Variable	Value
Admin user password	The administrator password using standard password definitions for your system. When a user logs on with the admin password, they are forced to change the default password.
Bit length	Number of bits to use to encrypt the security certificate. You can choose from the predefined values of 512, 1024, and 2048. The more bits required for encryption, the more CPU cycles are required to process the access.
City/Locality	The city or locality in which you are located.
Common name	The fully qualified domain name (FQDN) of the server. For Windows, it is a combination of the COMPUTERNAME and USERDNSDOMAIN environment variables. This field must match the host name of the system for the certificate.
Country/Region	The country or region in which you are located.
Friendly name	Identify the security certificate using a name.
Organization	Your company name.
Organizational unit	Unit within the company for the security certificate.
State/Province	The state or province in which you are located.
<security port>	The security port number for the Security Framework/Unified Communication Manager. The default value is 8443.

Configuring the communication between CCMA and UCM

Configure the communication information between Contact Center Manager Administration (CCMA) and the Unified Communication Manager (UCM) to ensure that the two applications work with each other.

Prerequisites

- Commission the CCMA server. See [Contact Center Manager Administration commissioning \(page 37\)](#).
- Configure the password for the admin user of the Unified Communication Manager. See [Configuring the admin user for the Unified Communication Manager \(page 59\)](#).

Procedure steps

- | Step | Action |
|------|--|
| 1 | Log on to the server on which you installed the Contact Center Manager Administration server software. |
| 2 | Click Start, All Programs, Avaya, Contact Center, Manager Administration, Configuration . |
| 3 | In the Configuration window, in the left pane, expand Avaya and Applications . |
| 4 | Select Security Settings . |
| 5 | In the right pane, click Security Settings . |
| 6 | In the Security Details dialog box, choose the location of your Primary Security Server. |
| 7 | In the Web Site Identifier list, select CCMA, 33 . |
| 8 | For CCMA Server Protocol , if SSL is enabled, you can select https ; otherwise, http is selected by default. |
| 9 | Accept the default IIS Port Number . |
| 10 | If the Security Framework Server is installed on another server, type the CCMA FQDN in the Security Server FQDN box, in the Security Server Details section. |
| 11 | In the Security Server Port Number box, type the security server port number. |
| 12 | In the Cache Interval box, type a number. This represents the number of local sessions of information cached on the server. |
| 13 | Click Enable . |
| 14 | On the Information box, click Yes . |
| 15 | Click OK to accept the updates. |
| 16 | Click Close . |

--End--

Variable definitions

Variable	Value
Security Details	Information about whether the Security Framework is installed on the same server as the Contact Center Manager Administration server or not. You can choose from two options: • Stand-alone security server—Security Framework and CCMA are on separate servers. • Co-res security server—Security Framework and CCMA are installed on the same server.
Security Server Details	The fully qualified domain name for the Contact Center Manager Administration server.
Cache Interval	The number of local sessions of information cached on the server.
Security Server Port Number	The port number used on the Security Framework server for communication between the Security Framework and the Contact Center Manager Administration server. The default number is 8443.
CCMA Server Protocol	The protocol used to communicate between the Contact Center Manager Administration server and the internet. If SSL is enabled, select https. Otherwise, http is selected by default.

Creating Unified Communication Management local accounts

Create local administrative users in Unified Communication Manager for authentication and authorization of application users in the Avaya Aura™ Contact Center. Administrators have a single sign-on to the security framework to minimize the necessity for users to provide separate logon credentials across multiple applications.

The first account you must create is a local account on the Unified Communication Network that is associated the webadmin account in Contact Center Manager Administration.

Prerequisites

- Know the admin password you configured in [Configuring the admin user for the Unified Communication Manager \(page 59\)](#) for the Unified Communication Manager.
- Configure the server security settings. See [Configuring the communication between CCMA and UCM \(page 61\)](#).

Procedure steps

Step	Action
1	Log onto the server where the Security Framework is installed.
2	Start Internet Explorer .
3	In the URL box, type https://FQDN:<security port> . The FQDN is the fully qualified domain name for your server.
4	If the Digital Certificate window appears, click OK .
5	If any Security Alert message boxes appear, click Yes .
6	In the User ID box, type admin.
7	In the Password box, type the administrator password for the Unified Communication Manager.
8	Click Log In .
9	Under User Services , select Administrative Users .
10	Click Add .
11	Type the account details for your user as required. Your first local account is associated with the webadmin account to access Contact Center Manager Administration.
12	Beside Authentication type , select Local .
13	Click Save and Continue .
14	Click Finish .

--End--

Variable definitions

Variable	Value
User ID	The user ID for the new Unified Communication Management user.
Authentication Type	Type of access granted to the user. You can choose local access or external.
Full Name	The name representing the user in the Unified Communication Management.
Temporary password	The temporary password for the new Unified Communication Management user. The password must be changed when the user logs on to the UCM for the first time.

Mapping Unified Communication Management users to CCMA users

Map all Unified Communication Manager users to Contact Center Manager Administration users to ensure the single sign on feature is enabled for all applications.

When you create users in Contact Center Manager Administration, you can use this utility to map CCMA users to UCM users.

Procedure steps

- | Step | Action |
|------|--|
| 1 | On the CCMA server, click Start, All Programs, Avaya, Contact Center, Manager Administration, Configuration . |
| 2 | In the Configuration window, in the left pane, expand Avaya, Applications . |
| 3 | Select CCMA User Migration . |
| 4 | In the right pane, click CCMA User Migration . |
| 5 | Under Search Type , select Local Security Server or Domain . |
| 6 | Under Search Options , specify the details for the users you want to find. |
| | OR |
| | On the right side of the window, click List All . |
| 7 | Under the Map User Accounts list, select a configured Unified Communication Manager account you want to map. |
| 8 | Under the Unassigned CCMA Users list, select a CCMA user that you want to map to the Unified Communication Manager account. |

- 9 Click **Map User**.
- 10 Click **Save**.
- 11 Click **Close**.

--End--

Variable definitions

Variable	Value
Search Type	Search for users configured on the system. Local Security Server Accounts—find all accounts configured on the server. Domain—find all external users on a domain, such as an LDAP or database.

Starting Contact Center Manager Administration client

Start Contact Center Manager Administration client in a manner different from that described previously now that the Security Framework is installed.

Prerequisites

- Map the CCMA user accounts in the Unified Communication Management utility. See [Mapping Unified Communication Management users to CCMA users \(page 65\)](#).

Procedure steps

- | Step | Action |
|------|--|
| 1 | On the CCMA server, start Internet Explorer. |
| 2 | Type http://fqdn:<security port> . |
| 3 | Log on using an account mapped in the Unified Communication Management utility. |
| 4 | If you are prompted to change your password, change the password for the user account. |

--End--

Configuring the admin user for the backup server

Configure the admin user for the optional secondary security framework server. You must configure the administrator account that is used to secure Web traffic before you set up users.

You can configure UCM users only on the primary security server. If your system security is managed by the backup Security Framework server, then you cannot change a user account.

Procedure steps

- | Step | Action |
|------|--|
| 1 | Log on to the server where the Security Framework is installed. |
| 2 | Start Internet Explorer . |
| 3 | In the URL box, type https://FQDN:<security port> .
The FQDN is the fully qualified domain name for your server. |
| 4 | If the Digital Certificate window appears, click OK . |
| 5 | If any Security Alert message boxes appear, click Yes . |
| 6 | In the User ID box, type a local user name you use to log on to the server. |
| 7 | In the Password box, type the password for the account you use to log on to the server. |
| 8 | Click Log In . |
| 9 | Click Security Configuration . |
| 10 | Verify the Fully Qualified Domain Name and the Web Server IP address by selecting Yes . |
| | OR |
| | If your server is not on a domain, click No , and configure the Fully Qualified Domain Name and IP address for your server. |
| 11 | Click Next . |
| 12 | Select the Backup security server . |
| 13 | Click Next . |
| 14 | In the Address of the Primary security server box, type the fully qualified domain name of the primary security server. |
| 15 | In the Confirm Administrator password box, retype the password. |
| 16 | Click Next . |
| 17 | In the Address of the Primary security server box, type the fully qualified domain name of the primary security server. |
| 18 | Click Next . |
| 19 | Type the Primary Security server user ID and the Primary Security server password . |

Security Framework commissioning

- 20 Click **Next**.
- 21 In the **Certificate Information** window, in the **Friendly name** box, type a name for the certificate.
- 22 From the **Bit length** list, select the bit length.
- 23 In the **Organization** box, type the name for the organization using the security certificate.
- 24 In the **Organizational unit** box, type the name of the smaller group of users using the security certificate.
- 25 In the **Common name** box, type the fully qualified domain name for the server.
- 26 From the **Country/Region** list, select your country or region.
- 27 In the **State/Province** box, type the name of your state or province.
- 28 In the **City/Locality** box, type the name of your city.
- 29 Click **Finish**.
- 30 After the configuration completes, click **Restart**.

--End--

Variable definitions

Variable	Value
Admin user password	The administrator password using standard password definitions for your system. When a user logs on with the admin password, they are forced to change the default password.
Bit length	Number of bits to use to encrypt the security certificate. You can choose from the predefined values of 512, 1024, and 2048. The more bits required for encryption, the more CPU cycles are required to process the access.
City/Locality	The city or locality in which you are located.
Common name	The fully qualified domain name (FQDN) of the server. For Windows, it is a combination of the COMPUTERNAME and USERDNSDOMAIN environment variables. This field must match the host name of the system for the certificate.
Country/Region	The country or region in which you are located.
Friendly name	Identify the security certificate using a name.
Organization	Your company name.
Organizational unit	Unit within the company for the security certificate.
State/Province	The state or province in which you are located.
<security port>	The security port number for the Security Framework Unified Communication Manager. The default value is 8443.

Configuring the communication between CCMA and the backup UCM

Configure the communication information between Contact Center Manager Administration (CCMA) and the backup Unified Communication Manager (UCM) to ensure that the two applications work together.

Prerequisites

- Commission the CCMA server. See [Contact Center Manager Administration commissioning \(page 37\)](#).
- Configure the password for the admin user of the backup Unified Communication Manager. See [Configuring the admin user for the backup server \(page 67\)](#).

Procedure steps

- | Step | Action |
|------|---|
| 1 | Log on to the server on which you installed the Contact Center Manager Administration server software. |
| 2 | Click Start, All Programs, Avaya, Contact Center, Manager Administration, Configuration . |
| 3 | In the Configuration window, in the left pane, expand Avaya and Applications . |
| 4 | Select Security Settings . |
| 5 | In the right pane, click Security Settings . |
| 6 | In the Resiliency Security Details box, select Failover Security Server . |
| 7 | In the Security Server Details section, in the Security Server FQDN box, type in the CCMA FQDN. |
| 8 | In the Security Server Port Number box, type the security server port number |
| 9 | Click Add . |
| 10 | Click Enable . |
| 11 | On the Information box, click Yes . |
| 12 | Click OK to accept the updates. |
| 13 | Click Close . |

--End--

Variable definitions

Variable	Value
Security Details	Information about whether the Security Framework is installed on the same server as the Contact Center Manager Administration server or not. You can choose from two options: • Stand-alone security server—Security Framework and CCMA are on separate servers. • Co-res security server—Security Framework and CCMA are installed on the same server.
Security Server Details	The fully qualified domain name for the Contact Center Manager Administration server.
Cache Interval	The number of local sessions of information cached on the server.

Variable	Value
Security Server Port Number	The port number used on the Security Framework server for communication between the Security Framework and the Contact Center Manager Administration server. The default number is 8443.
CCMA Server Protocol	The protocol used to communicate between the Contact Center Manager Administration server and the internet. If SSL is enabled, select https. Otherwise, http is selected by default.

Contact Center Manager Administration client commissioning

After you install Contact Center Manager Administration server software, commission the client PCs to access Contact Center applications.

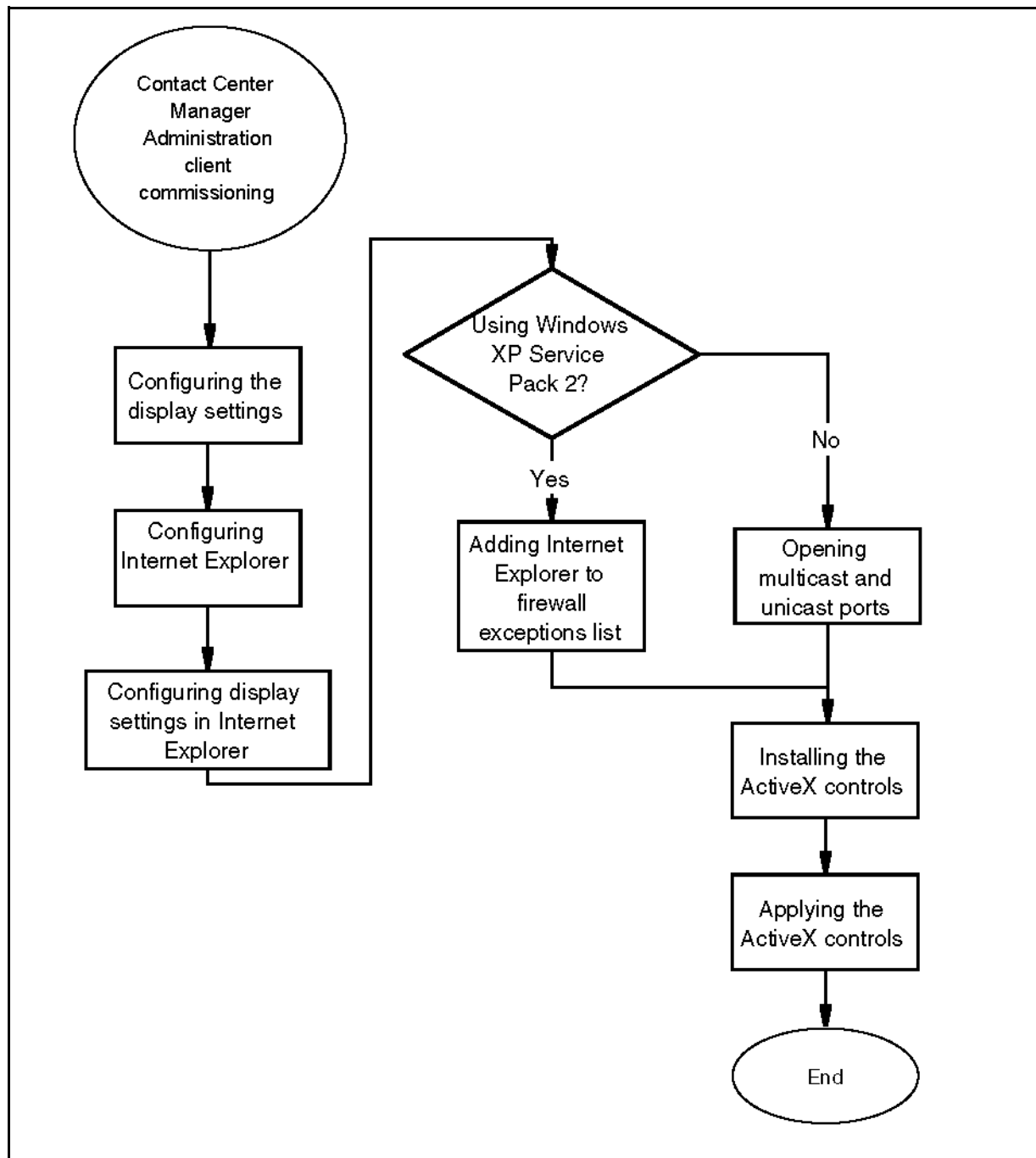
Prerequisites for client commissioning

- Install or update the Contact Center Manager Administration server software. For more information, see *Avaya Aura™ Contact Center Installation* (NN44400-311) or *Avaya Aura™ Contact Center Upgrade and Patches* (NN44400-410).
- Install or update the required client applications. For more information, see *Avaya Aura™ Contact Center Installation* (NN44400-311) or *Avaya Aura™ Contact Center Upgrade and Patches* (NN44400-410).
- Install Internet Explorer 6.0 or later.

Client commissioning procedures

This task flow shows you the sequence of procedures you perform to commission the client. To link to any procedure, go to [Client commissioning navigation \(page 74\)](#).

Client commissioning procedures



Client commissioning navigation

- [Configuring the display settings \(page 75\)](#)
- [Configuring Internet Explorer \(page 76\)](#)
- [Configuring display settings in Internet Explorer \(page 77\)](#)

- [Adding Internet Explorer to the firewall exceptions list \(page 78\)](#)
- [Opening multicast and unicast ports \(page 78\)](#)
- [Installing the ActiveX Controls \(page 80\)](#)
- [Applying the ActiveX Controls \(page 81\)](#)

Job aid: Timing

The estimated time to commission the client is 20 minutes.

The time can vary depending on the server, network infrastructure, and your confidence level with the software.

Configuring the display settings

Configure the display settings on each client PC so that all Contact Center Manager Administration components such as reports appear correctly in the browser window.

Procedure steps

- | Step | Action |
|------|---|
| 1 | On the client PC, click Start, Control Panel, Display |
| 2 | In the Display Properties dialog box, click the Appearance tab. |
| 3 | From the Font size list, select Normal . |

Attention: If you do not select Normal, some items may not display correctly in the browser.

- | | |
|---|--|
| 4 | Click the Settings tab. |
| 5 | Configure the screen resolution to 1024 X 768 . |

Attention: Avaya recommends this resolution to accommodate Real-Time Display billboard collections.

- | | |
|---|----------------------|
| 6 | Click Apply . |
| 7 | Click OK . |

--End--

Configuring Internet Explorer

Configure Internet Explorer on each client to access Contact Center Manager Administration.

Procedure steps

- | Step | Action |
|------|---|
| 1 | 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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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) for your Contact Center Manager Administration server. |

OR

If you used the fully qualified domain name when you installed Contact Center Manager Administration on the Contact Center Manager Administration server, in the **Add this Web site to the zone** box, type the fully qualified domain name.

- 17 Click **Add**.
- 18 In the **Add this Web site to the zone** box, type the server name (not the IP address) for your Contact Center Multimedia server.
- 19 Click **Add**.
- 20 Click **OK** to return to the **Internet Options** dialog box.
- 21 Click the **Privacy** tab.
- 22 In the **Pop-up Blocker** section, select the **Block pop-ups** check box.
- 23 Click **Settings**.
- 24 In the **Pop-up Blocker Settings** dialog box, in the **Address of website to allow** box, type the Contact Center Manager Administration URL, http://<server name>/.
- 25 Click **Add**.
- 26 Click **Close**.
- 27 In the **Internet Options** dialog box, click the **Advanced** tab.
- 28 Under **Browsing**, clear the **Reuse windows for launching shortcuts** check box.
- 29 Click **Apply**.
- 30 Click **OK** to exit the **Internet Options** dialog box.
- 31 Restart Internet Explorer to activate your changes.

--End--

Configuring display settings in Internet Explorer

Configure display settings for Western European (ISO) countries in Internet Explorer to properly view characters and windows.

Procedure steps

- | Step | Action |
|------|---|
| 1 | Open Internet Explorer. |
| 2 | Click View, Encoding, Western European (ISO) . |
| 3 | Close Internet Explorer. |

--End--

Adding Internet Explorer to the firewall exceptions list

Add Internet Explorer to the firewall exceptions list if the client is running Windows XP Service Pack 2 to ensure data can move between the clients and the server for reporting.

Alternatively, you can open multicast and unicast ports. To open multicast and unicast ports, see [Opening multicast and unicast ports \(page 78\)](#).

Prerequisites

- Ensure that the client PC is running Windows XP Service Pack 2 or later.
- Ensure that the Windows Firewall/Internet Connection Sharing (ICS) is running.

Procedure steps

Step	Action
1	On the client PC, click Start, Control Panel, Windows Firewall .
2	Click the Exceptions tab.
3	In the Programs and Services list, select Internet Explorer .
4	If Internet Explorer is not listed, click Add Program .
5	In the Add a Program dialog box, click Internet Explorer .
6	Click OK to close the Add a Program dialog box.
7	Click OK .

--End--

Opening multicast and unicast ports

Open multicast and unicast ports to ensure data can move between the clients and the server for reporting.

If the client PC is running Windows XP Service Pack 2 or later, you can add Internet Explorer to the firewall exceptions list, or open a specific set of ports. See [Adding Internet Explorer to the firewall exceptions list \(page 78\)](#).

Prerequisites

- Ensure that the client PC is not running Windows XP Service Pack 2 or later.

Procedure steps

- | Step | Action |
|------|--|
| 1 | On the client, double-click My Network Places . |
| 2 | In the My Network Places window, in the left pane, under the Network Tasks list, click View Network Connections . |
| 3 | In the Network Connections window, right-click the connection that you use to connect to the Internet and click Properties . |
| 4 | In the <connection> Properties dialog box, click the Advanced tab. |
| 5 | In the Windows Firewall section, click Settings . |

Attention: If the Settings button is unavailable, Internet Connection Firewall is not enabled on this connection, and you cannot open any ports (because they are all already open).

- | | |
|----|--|
| 6 | In the Windows Firewall dialog box, click the Exceptions tab. |
| 7 | Click Add Port to open a new port. |
| 8 | In the Add a port dialog box, in the Name box, type 127.0.0.1 .
You can specify the IP address of an internal computer, but you typically use 127.0.0.1. |
| 9 | In the Port number box, type the port number. |
| 10 | Select a communication option. |
| 11 | Click OK . |
| 12 | Repeat step 7 to step 11 for each port to open. |
| 13 | Click OK to close the Windows Firewall dialog box. |
| 14 | Click OK to close <connection> Properties dialog box. |
| 15 | Close the Network Connections window. |

--End--

Variable definitions

Variable	Value
<connection>	The connection that you use to connect to the Internet.
Communication options	The mechanism for communicating between the server and clients for reporting. TCP - Transmission Control Protocol UDP - User Datagram Protocol

Procedure job aid

If the client PC is running Windows XP Service Pack 2, open the following ports:

- Emergency Help: UDP 8200
- Multicast real-time reports: UDP 7020; 7030; 7040; 7050; 7060; 7070; 7080; 7090; 7100; 7110; 7120; 7130
- Unicast real-time reports: UDP 7025; 7035; 7045; 7055; 7065; 7075; 7085; 7095; 7105; 7115; 7125; 7135

Installing the ActiveX Controls

Install the ActiveX Controls.msi file on each client as an administrator if your company security policy prevents agents from logging on to clients as administrator.

The ActiveX controls are rules that specify how applications share information using the Web browser. In Contact Center, ActiveX controls allow communication between the clients and servers to report data and display information from the database.

Controls downloaded using the ActiveX Controls.msi file do not appear in the Internet Explorer Downloaded Program Files window.

Prerequisites

- Configure the Web browser to enable initialize and script ActiveX Controls not marked as safe. See [Configuring Internet Explorer \(page 76\)](#).

Procedure steps

Step	Action
1	Log on to the client PC with administrator privileges.

- 2 Insert the Contact Center Installation DVD into the client, and navigate to **x:\Install Software\CCMA\ActiveX Controls_<patchID>**; <x> is the drive letter of your DVD drive and <patchID> is the ID of the selected patch installed on the Contact Center Manager Administration server.
- 3 In the this directory, double-click **ActiveX Controls.msi** to begin the installation.
- 4 Click **Next**.
- 5 Select a **Destination Folder** or accept the default installation folder.
- 6 Click **Next**.
- 7 In the **Ready to Install the Program** window, click **Install**.
- 8 Click **Finish**.
- 9 Repeat steps 2 to 8 for each client.

--End--

Applying the ActiveX Controls

Apply the ActiveX Controls.msi file you installed to the clients in your Contact Center to permit communication between the clients and servers in your network.

Because installation procedures performed through an SMS system can vary from one company to the next, this procedure offers general guidelines only.

In addition to using an SMS server, a system administrator can install this package on clients within the same domain using the Windows Group Policy.

For details, see the documentation on the Microsoft Web site at www.microsoft.com.

Prerequisites

- Install the ActiveX.msi controls on your client. See [Installing the ActiveX Controls \(page 80\)](#).
- Ensure that you have administrator privileges to apply the ActiveX Controls.msi file to clients by using an SMS server or Group Policy.
- Configure the Web browser to enable initialize and script ActiveX Controls not marked as safe. See [Configuring Internet Explorer \(page 76\)](#).

Procedure steps

- | Step | Action |
|------|--|
| 1 | Log on to the SMS server with administrator privileges. |
| 2 | Insert the Contact Center Manager installation DVD into the PC, and navigate to x:\Install Software\CCMA\ActiveX Controls_<patchID> ; <x> is the drive letter of your DVD drive and <patchID> is the ID of the selected patch installed on the Contact Center Manager Administration server. |
| 3 | From the Contact Center Manager installation DVD, copy ActiveX Controls.msi to the desired directory on the SMS server. |
| 4 | Double-click ActiveX Controls.msi to run the installation and install the files on all SMS client PCs in your network. |

--End--

Communication Control Toolkit commissioning for Contact Center

Use the procedures in this section to commission the Communication Control Toolkit (CCT) software in your Contact Center. A Contact Center supports voice and multimedia on a SIP or TDM-based PABX.

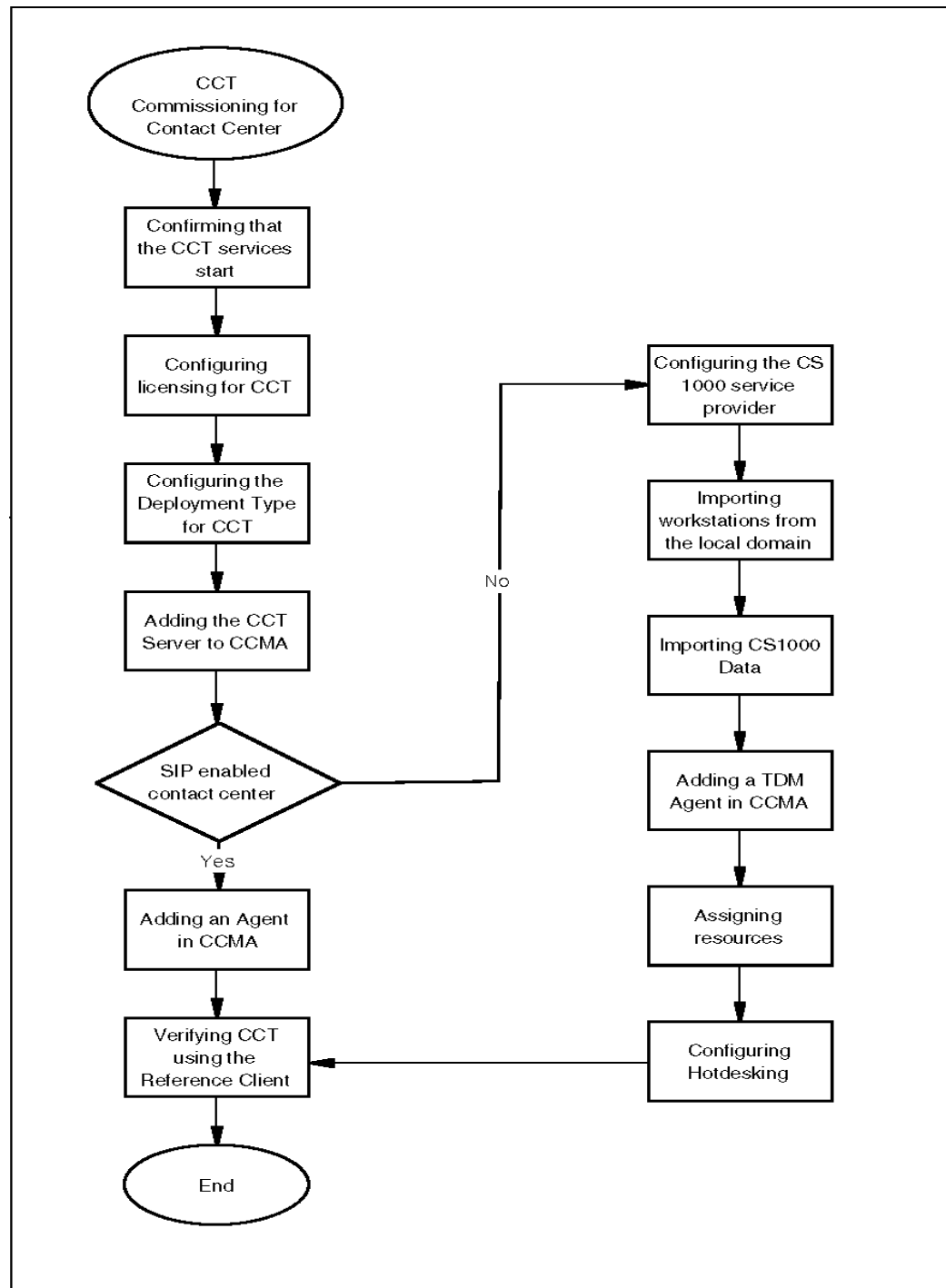
Prerequisites to CCT commissioning for Contact Center

- Read *Avaya Aura™ Contact Center Planning and Engineering* (NN44400-210).
- Complete *Avaya Aura™ Contact Center Installation Checklist* (NN44400-310).
- Install all of the components required for the Communication Control Toolkit software for your network configuration, including the updates. For more information, see *Avaya Aura™ Contact Center Installation* (NN44400-311).
- Install Contact Center Manager Server if Communication Control Toolkit is installed for Avaya Aura™ Contact Center. Contact Center Manager Server is not required if Communication Control Toolkit is installed for Knowledge Worker.
- Ensure the appropriate PABX is installed and configured for your system.
- Install CCT and all current updates.
- Install License Manager software and all current updates.
- Install and configure Contact Center Manager Server (CCMS) and Contact Center Manager Administration (CCMA).

Communication Control Toolkit commissioning for Contact Center procedures

This task flow shows you the sequence of procedures you perform to commission the Communication Control Toolkit in a contact center environment. To link to any task, go to [Communication Control Toolkit commissioning for Contact Center navigation](#) (page 85).

Communication Control Toolkit commissioning for Contact Center procedures



Communication Control Toolkit commissioning for Contact Center navigation

- [Confirming that the CCT services start \(page 85\)](#)
- [Configuring the licensing for CCT \(page 86\)](#)
- [Configuring the deployment type for CCT \(page 88\)](#)
- [Adding the CCT Server in CCMA \(page 89\)](#)
- [Configuring the Avaya Communication Server 1000 service provider \(page 90\)](#)
- [Importing workstations from the domain \(page 93\)](#)
- [Importing Avaya Communication Server 1000 data \(page 93\)](#)
- [Adding a TDM agent in CCMA \(page 96\)](#)
- [Assigning resources \(page 97\)](#)
- [Configuring Hotdesking \(Agent Roaming\) \(page 99\)](#)
- [Adding agent in CCMA \(page 100\)](#)
- [Verifying CCT using the Reference Client \(page 101\)](#)

Confirming that the CCT services start

Confirm that the Communication Control Toolkit services start so you can configure the Communication Control Toolkit database.

Procedure steps

Step	Action
1	Click Start, All Programs, Avaya, Contact Center, Common Utilities, System Control and Monitor Utility .
2	Select the CCT tab.
3	Confirm that the Communication Control Toolkit services are running.
4	If a Communication Control Toolkit service is not running, re-start CCT.
5	Close the System Control and Monitor Utility SCMU utility.

--End--

Procedure job aid

For a functional CCT server the following CCT services must start:

- Caché Service
- NCCT SMON

- NCCT Logging Service
- NCCT Data Access Layer
- NCCT Server
- NCCT OI Service

For a functional CCT server in a TDM based contact center, the following CCT services must start:

- Caché Service
- NCCT SMON
- NCCT Logging Service
- ACD Proxy
- Telephony
- NCCT Data Access Layer
- NCCT TAPI Connector
- NCCT Server
- NCCT OI Service

Configuring the licensing for CCT

Configure CCT licensing with the IP address of the server where Contact Center License Manager is installed and configured.

CCT consumes licenses as required. For example, every time a CCT client logs in and opens a terminal, CCT automatically uses a license. When a terminal is released the license is released.

CCT License Configuration is disabled when CCT is installed co-resident with CCMS. Use the CCMS Server Configuration tool to configure licensing on a co-resident server.

Prerequisites

- Contact Center License Manager is installed.
- Communication Control Toolkit is not co-resident with Contact Center Manager Server.

Procedure steps

Step	Action
------	--------

- 1 Log on to the Communication Control Toolkit server.
 - 2 Click **Start, All Programs, Avaya, Contact Center, Communication Control Toolkit, CCT Console**.
 - 3 Expand Communication Control Toolkit.
 - 4 Expand **Server Configuration**.
 - 5 Click **License Configuration**.
 - 6 In the right pane License Configuration, under **Primary License Manager Server**, in the **IP Address** box, type the IP address for the server on which the License Manager is installed.
 - 7 Under **Secondary License Manager Server**, in the **IP Address** box, type the IP Address for the server on which the secondary License Manager is installed.
- Attention:** The Secondary License Manager Server IP Address section is available only if corporate licenses are installed.
- 8 From the **License Type** list, select Nodal or Corporate.
 - 9 In the Actions pane on the right, select **Apply changes**.

--End--

Variable definitions

Variable	Value
License Type	The type of license for the License Manager. Nodal—The license applies to only one installation of CCMS. You cannot configure the Secondary License Manager for a Nodal license. Corporate—The license applies to a collection of Contact Center Manager Servers. Secondary License Manager is available only for Corporate licenses.
Primary License Manager Server IP Address	The IP address of the server on which the License Manager application is installed. CCT License Configuration is disabled when CCT is installed co-resident with CCMS.
Secondary License Manager Server IP Address	The optional IP address of the server on which the backup License Manager application is installed. CCT License Configuration is disabled when CCT is installed co-resident with CCMS.

Configuring the deployment type for CCT

Configure the deployment type for the CCT server to manage the contact routing for your network configuration.

CCT deployment type is disabled when CCT is installed co-resident with CCMS.

Prerequisites

- Understand the network requirements for your installation of CCT (co-resident, stand-alone, or multimedia).
- Know how to stop and restart the CCMS services. [Stopping and restarting the Contact Center Manager Server services \(page 206\)](#).
- Know how to stop and restart the CCT services. See [Stopping and restarting the core Communication Control Toolkit services \(page 205\)](#).

Procedure steps

- | Step | Action |
|------|--|
| 1 | Log on to the Communication Control Toolkit server. |
| 2 | Click Start, All Programs, Avaya, Contact Center, Communication Control Toolkit, CCT Console . |
| 3 | Expand Communication Control Toolkit. |
| 4 | Expand Server Configuration . |
| 5 | Select Deployment Type . |
| 6 | In the Deployment Type dialog box, select the deployment type for your Communication Control Toolkit. |
| 7 | In the CCMS Server Hostname box, type the name of the Contact Center Manager Server. |
| 8 | In the Actions pane on the right, select Apply changes . |
| 9 | Stop and restart the Communication Control Toolkit services. |

--End--

Variable definitions

Variable	Value
Communication Control Toolkit Deployment Type	Choose the deployment type for Communication Control Toolkit based on your network configuration. This option is always disabled if CCT is co-resident with CCMS. CCT Installation (Contact Center only) if your Contact Center is licensed for multimedia contacts and the CCT server software is installed on the same server as CCMS. Choose Stand-alone CCT installation (Contact Center only) if your Contact Center is licensed for multimedia contacts and the CCT server software is not installed on the same server as CCMS. Choose CCT installation (Contact Center only) co-resident with CCMS where CCMM is not part of the solution and OpenQ feature is disabled on the CCMS server OR Standalone CCT installation (Contact Center or Knowledge Worker) where CCMM is not part of the solution and the OpenQ feature is disabled on the CCMS server.

Adding the CCT Server in CCMA

Add the CCT server to CCMA then associate it to a CCMS server, to administer the CCT server from the CCMA client application. This is a summary of the full procedure outlined in the *Avaya Aura™ Contact Center Manager Administration – Client Administration* (NN44400-611) guide.

Prerequisites

- To add a CCT server, you must first have added a CCMS with Open Queue enabled.
- Ensure you know the CCT Tomcat Web site port number. The default CCT Tomcat Web site port number is 8081.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration server.
2	On the Launchpad, click Configuration .
3	From the Server menu, click Add Server .
4	Enter details for the CCT server.

- 5 In the Associated CCMS Servers list, select the CCMS with which you want to associate this CCT server.
- 6 Click **Submit**.

--End--

Configuring the Avaya Communication Server 1000 service provider

Configure the Avaya Communication Server 1000 service provider details to enable connection to the PABX. A polling message is sent every ten seconds to monitor the connection the PABX. The polling interval detail is configured in the Communication Server 1000 service provider details. Ten seconds is the default polling time.

Prerequisites

- Understand the server provider details for the switch.

Procedure steps

- | Step | Action |
|------|---|
| 1 | Log on to Contact Center Manager Administration server. |
| 2 | Start Communication Control Toolkit Web Administration client. |
| 3 | In the resource menu, select Providers .
<i>The details of the providers appear.</i> |
| 4 | From the list of providers, select Passive . |
| 5 | In the Basic Provider Information section, in the Passive Name box, type the Provider name. |

Attention: The provider name must be Passive.

- 6 In the **IP Address** box, type the IP address of the provider.
- 7 In the **Port** box, type the port number.
- 8 In the **Provider Configuration** section, select the **Transport** type, **TCP**.
- 9 In the **Customer Number**, type the customer number.
- 10 In the **CS1000 Software Release**, select the correct version.
- 11 In the **Call Data Life Span (minutes)**, type the required value in minutes.
- 12 Select or clear the **Disable Copy of Data to Consult Call** check box.
- 13 In the **CS1000 Home location Code (HLOC)**, type the HLOC value.
- 14 In the **Network IVR Port**, type the port value.

Communication Control Toolkit commissioning for Contact Center

- 15 In the **Initialization Timeout (seconds)** box, type the **Initialization timeout** setting in seconds.
- 16 In the **Command Timeout (seconds)** box, type the **Command** timeout setting in seconds.
- 17 Select **Save**.

--End--

Variable definitions

Variable	Value
Provider Name	Name of the Provider, Passive.
IP Address	In a Contact Center environment, the IP address of the CCMS.
Port	In a Contact Center environment, the default port value is 3000.
Transport	Transport protocol, default is TCP.
Customer Number	The customer number for the switch. If multiple customers are configured, you must specify a specific one in this box.
CS1000 Software Release	The release number of Avaya Communication Server 1000 software.
Call data	Call data is the information attached to calls routed from the switch. The Life Span default is 10 minutes. This value must be less than the time it takes to recycle the Communication Server 1000 Call IDs. Use the Disable copy of call data to consultative call check box to avoid copying call data during consultative calls, but you can still copy call data when calls are transferred or conferenced.
CS1000 Home Location Code (HLOC)	Avaya Communication Server 1000 Home Location Code (HLOC) of the switch is the address digits that specify a location node.
Network IVR Port	Port for the CCT network call attached data and for IVR call attached data.
Timeout in Seconds	Initialization—The length of time that the service provider waits to establish communication with the switch before generating an error. The default and minimum value is 32 seconds. If you use a large number of lines, you must increase this value accordingly. Command—The length of time that the service provider waits for a command response before generating an error. The default and minimum value is 5 seconds.

Importing workstations from the domain

All Contact Center applications are in a contact center domain. Import workstations from the contact center domain to the Communication Control Toolkit server using the Import Workstations tool.

Prerequisites

- A local administrator must have access to the contact center domain to import domain resources to the CCT Console. Ensure the local administrator has access to the contact center domain.

Procedure steps

Step	Action
1	Log on to the Communication Control Toolkit server.
2	Click Start, All Programs, Avaya, Contact Center, Communication Control Toolkit, CCT Console .
3	Expand Communication Control Toolkit.
4	Click Import Work Stations .
5	From the Search Type list, select All WorkStations .
6	Select the workstations to import from the Available Work Stations list.
7	Click Add .
8	Click OK .

--End--

Importing Avaya Communication Server 1000 data

You can use the CCT Import CS 1000 Data tool to perform either of the following activities:

- Perform the first step of the import process: convert data capture text file to an XML file by un-checking the Automatically import data after conversion check box.
- Perform both steps of the import process, convert text file to XML file and import data to the database. This is done by leaving the default setting Automatically import data after conversion.

You can convert the text file to an XML file to test the data import facility without modifying the database contents; or, you can postpone the actual import of the data to an off peak time. You can later import the intermediate XML data file generated by using the CCT Data Import/Export Tool, by selecting the Standard XML format option.

Before importing the Avaya Communication Server 1000 data to CCT, you must first retrieve the data from the switch. To do this, create a switch configuration text file to capture the Communication Server 1000 data required to configure Communication Control Toolkit.

Do not use the Communication Control Toolkit server to import the information directly from the switch. Hyperterminal, when installed, interferes with the Telephony services and they remain running.

Prerequisites

- Connect a COM cable from a server (not the Communication Control Toolkit server) or workstation to the switch.
- Know the user ID and password to log on to the Avaya Communication Server 1000.
- Apply all Avaya Communication Server 1000 patches, specifically patch MPLR26704. Patch MPLR26704 significantly reduces the time to import address and terminal information into the text file. Only information that is relevant to Communication Control Toolkit is imported.
- Only PABX keys that are AST and IAPG enabled are imported.

Procedure steps

- | Step | Action |
|------|---|
| 1 | Open a text editor on the server on which Hyperterminal is installed. |
| 2 | Create a new text file called download.txt . |
| 3 | Click Start, All Programs, Accessories, Communications, HyperTerminal to connect to the Avaya Communication Server 1000. |
| 4 | Type a name for the connection. |
| 5 | Click OK . |
| 6 | On the Connect To dialog box, in the Connect using list, select COM1 or the COM port connected to the Avaya Communication Server 1000 switch. |
| 7 | Click OK . |
| 8 | In the COM properties dialog box, verify the data is correct or make necessary changes. |
| 9 | Click OK . |
| 10 | From the Transfer menu, select Capture Text . |
| 11 | In the Capture Text dialog box, type the location and name of the text capture file in the File box, for example, type the location and name of the download.txt file created in step 2. |
| 12 | Click OK . |
| 13 | At the prompt, type logi admin1 to log on to the switch. |

- 14 Type the user ID and password for the switch.
- 15 If the prompt does not appear, continue to press **Enter** until the prompt appears.
- 16 Browse to the download.txt file, and then click **Start**.
- 17 Type these commands at the following prompts:
>LD 20
REQ: PRT
TN: TNB
TN: Press enter
CDEN: Press enter
CUST: 0 (or the customer number)
DATE: Press enter
PAGE: ON
DES: Press enter
Downloading information from the Communication Server 1000 overlay can take a several minutes.
- 18 To return to the prompt, enter ******** (Shift + 8888).
- 19 Press **Enter**.
- 20 Type these commands at the following prompts:
>LD 23
REQ: PRT
TYPE: CDN
CUST: 0 (or the customer number)
CDN: Press enter
The information is downloaded from the overlays.
- 21 Type **logo**.
- 22 Press **Enter**.
- 23 Copy the download.txt to the Communication Control Toolkit server.
- 24 Log on to the Communication Control Toolkit server.
- 25 Click **Start, All Programs, Avaya, Contact Center, Communication Control Toolkit, CCT Console**.
- 26 Expand Communication Control Toolkit.
- 27 Expand **Bulk Provisioning**.
- 28 Select **Import CS 1000 Data**.
- 29 Select **Passive** for the Communication Server 1000 Provider.

- 30 Select **Input File**. This opens a file explorer to select the Communication Server 1000 data capture file you copied in [step 23](#).
- 31 Select the Communication Server 1000 data capture file, click **Open**. A default path and file name appears in the **Output file**, change the location if necessary.
- 32 To import the data into the database select **Automatically import data after conversion**.
- 33 In the Actions pane on the right hand side, select **Convert/Import**. A progress bar in the Status area indicates the progress made by the tool in three phases:
 - Conversion of the data capture file
 - Generation of the output file
 - Import of the data into the database
- 34 The status area displays data imported and the conversion results, including the number of TNs, DNS, and CDNs found. If applicable, a list of errors are also displayed. This list includes line numbers where the errors were discovered in the supplied data capture file.

Attention: An error dialog shows errors in the conversion step. The error dialog appears prior to beginning the automatic import. The user can choose to cancel the import step or proceed.

--End--

Adding a TDM agent in CCMA

Create TDM agents on the CCMA server and associate them with the appropriate contact center windows users. This is a brief summary of the full procedure outlined in the *Avaya Aura™ Contact Center Manager Administration – Client Administration* (NN44400-611) guide.

Prerequisites

- If you have a CCT server in the contact center, ensure that you have a domain user account for your contact center domain with privileges to list the domain users.
- Add CCT server to CCMA configuration.
- Log on to CCMA. For more information, see *Avaya Aura™ Contact Center Manager Administration – Client Administration* (NN44400-611).
- Open the Contact Center Management component.

Procedure steps

Step	Action
1	In the left pane, click the Contact Center Manager Server under which to add the agent.
2	From the Add menu, select Agent .
3	In the New Agent Details window, enter the mandatory information about the agent, First Name, Last Name, Login ID, Create CCT Agent, Primary Supervisor, Call Presentation and threshold.
4	Enter any optional information about the agent (for example, Title, Department, or Comments).
5	Select Create CCT Agent .
6	Click Associate User Account , and complete the Associate User Account fields to create a CCT user for this agent.
7	Configure Multiplicity and Open Q if these features are enabled.
8	Configure the Skillsets for the agent.
9	Click Submit to save your changes.

--End--

Assigning resources

Resources in CCT are users, terminals, addresses, and workstations. Create the contact center agents in CCMA before assigning resources in CCT. Creating the contact center agents in CCMA stores the contact center windows user and agent information to the CCT database. This ensures all the data needed for assigning resources is in the CCT database, ready for configuration.

To enable CCT to work in a contact center follow the basic configuration:

- assign a terminal to one or two addresses
- assign a terminal to a workstation
- assign a terminal to a user.

Make configuration changes quickly in your contact center by organizing users, terminals and addresses into groups. This allows you to map your resource groups to functional roles in your contact center.

Use the Communication Control Toolkit Web Administration client to assign resources.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration server.
2	Start the Communication Control Toolkit Web Administration .
3	Click the resource type.
4	Click the single resource to configure.
5	Select one of the Resource Assignments to assign to this resource.
6	Select the appropriate resources from those in the Available Resources column. Click each resource to select more than one resource or resource group. Select the resource again to clear it.
7	Click the Right Arrow to move the selected resource and resource groups to the Assigned Resources column.
8	Click Save .

--End--

Example of assigning resources

In a hotdesking configuration, CCT the resources are configured into groups.

Create a terminal group called hotdesking_terminals and assign all terminals to this group.

Assigning Terminals to a Terminal Group

Step	Action
1	Log on to the CCMA server.
2	Start the Communication Control Toolkit Web Administration client.
3	Select Groups .
4	Select Terminal Groups .
5	Select the hotdesking_terminals terminal group.
6	Select the all terminals in the Available Resources column. Click each resource to select more than one resource.
7	Click the Right Arrow to move the selected terminals to the Assigned Resources column.
8	Click Save .

--End--

Configuring Hotdesking (Agent Roaming)

In a contact center an agent may not have a fixed desk and phone. An agent might pick a desk that is not being used and log into the phone and workstation. An agent must be able to log onto any phone and workstation in this environment.

In a hotdesking environment using any configured workstation, agents can control the terminal and addresses associated with that workstation.

To enable hotdesking in CCT, a Windows user is assigned to multiple terminals; each terminal is assigned to its respective workstation. The user's terminal is determined by the workstation that the user logs on to, as shown in the following example.

- Terminal_1 maps to workstation_1.
- Terminal_2 maps to workstation_2.

For example, assume that User_1 is assigned to Terminal_1 and Terminal_2 and the respective addresses. If User_1 logs on to workstation_2, then the user also logs on to Terminal_2.

Prerequisites

- Create agents on the CCMA server and associate them with domain users.
- Assign each terminal to a workstation.
- Add terminals to a terminal group.
- Ensure that all terminals have a correctly mapped address.
- If you require additional terminals (and therefore addresses) in the hotdesking group, add the new terminals to the terminal group and the new addresses to the address group. Follow this process to ensure that the correct resources are available to all roaming CCT agents at all times.

Procedure steps

Step	Action
1	Place all select terminals for hotdesking into a terminal group.
2	Ensure that all terminals have a correctly mapped address.
3	Place all the addresses associated with the terminals into an address group.
4	Place all select users for hotdesking into a user group.
5	Assign the terminal group from step 1 to the user group from step 4 with the automatic mapping of addresses check box cleared.
6	Assign the address group from step 3 to the user group from step 4.
7	Assign each terminal to a workstation.

Attention: You can assign a terminal to only one workstation.

--End--

Adding agent in CCMA

Create a SIP agent on the CCMA server and associate them with the appropriate contact center windows users. This is a brief summary of the full procedure outlined in the *Avaya Aura™ Contact Center Manager Administration – Client Administration* (NN44400-611) guide.

Prerequisites

- If you have a CCT server in the contact center, ensure that you have a domain user account for your contact center domain with privileges to list the domain users.
- Add CCT server to CCMA configuration.
- Log on to CCMA. For more information, see *Avaya Aura™ Contact Center Manager Administration – Client Administration* (NN44400-611).
- Open the Contact Center Management component.

Procedure steps

Step	Action
1	In the left pane, click the Contact Center Manager Server under which to add the agent.
2	From the Add menu, select Agent .
3	In the New Agent Details window, enter the mandatory information about the agent, login ID, Voice URI, Create CCT Agent, Primary Supervisor, Call Presentation and threshold.
4	Enter any optional information about the agent (for example, Title, Department, or Comments).
5	Select Create CCT Agent .
6	Click Associate User Account , and complete the Associate User Account fields to create a CCT user for this agent.
7	Configure Multiplicity and Open Q if these features are enabled.
8	Configure the Skillsets for the agent.
9	Click Submit to save your changes.

--End--

Verifying CCT using the Reference Client

Verify Communication Control Toolkit configuration by using the Reference Client to ensure that all resources are available and accessible to route contacts for CCMS. The Reference Client is an installation testing tool; do not deploy it for production contact center use.

Prerequisites

- Create a Windows user for testing.
- Configure CCT for your contact center.

Procedure steps

Step	Action
1	Log on to the Communication Control Toolkit server with the Local Administrator user ID and password.
2	Click Start, All Programs, Avaya, Contact Center, Communication Control Toolkit, Ref Client .
3	In the Server Settings dialog box, click OK .
4	From the Session menu, choose Connect .
5	In the User Credentials dialog box, select either the Current Windows User or specify a User ID, Domain and Password .
6	Click OK .
7	In the Available Devices box, select the address you want to use for the test call.
8	Enter the Destination Address in the text box to the right of the Originate button.
9	Click Originate . The destination address shows a Local State of Ringing in the Reference Client
10	Select the Ringing Address on the Reference Client, and click Answer .
11	Release the call.

--End--

Communication Control Toolkit commissioning for Knowledge Worker

Use the procedures in this section for commissioning the Communication Control Toolkit software in your knowledge worker or direct-connect environment. A knowledge worker configuration supports telephony service routing directly with the Communication Server 1000 PABX.

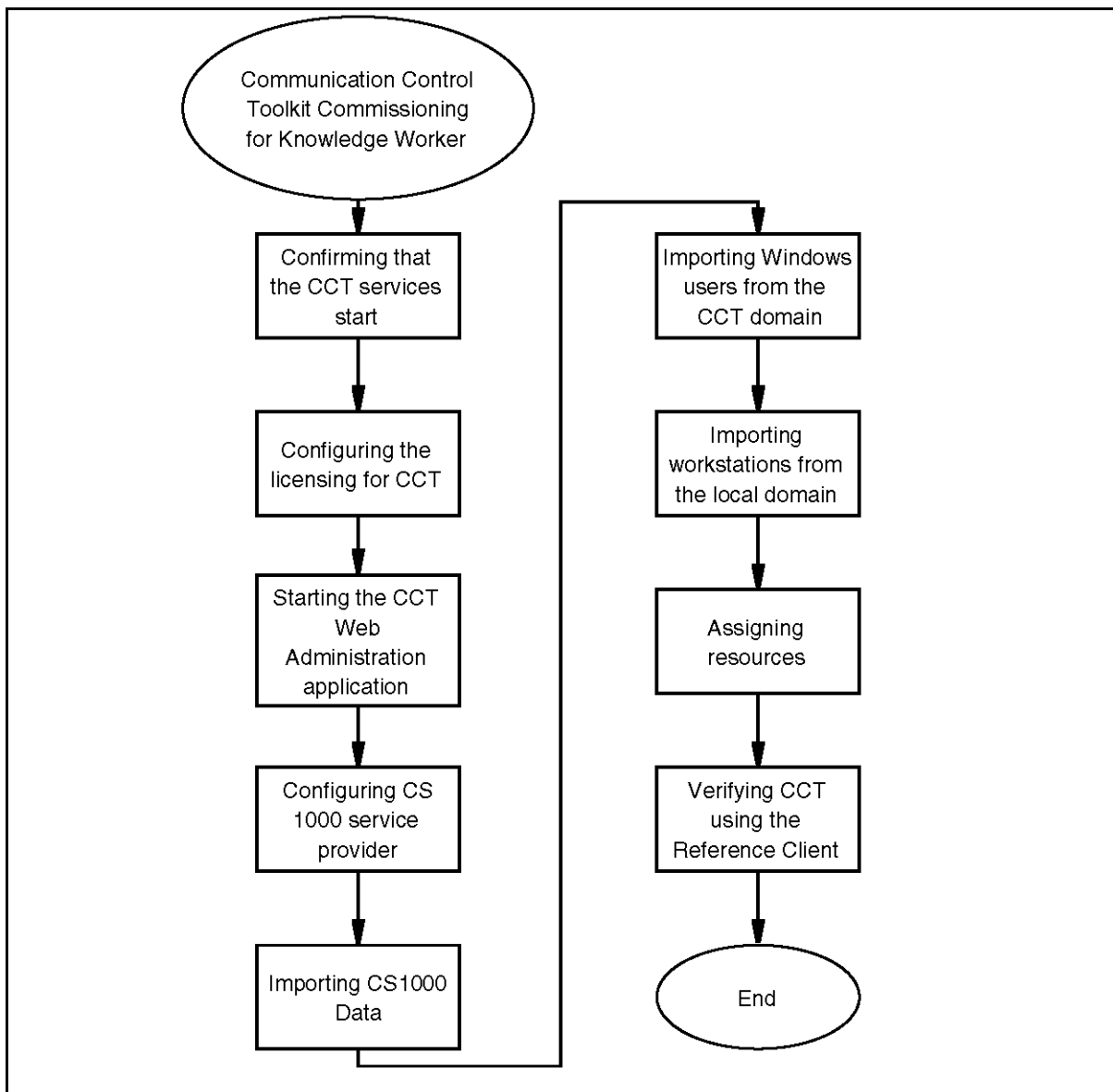
Prerequisites to CCT commissioning for Knowledge Worker

- Read *Avaya Aura™ Contact Center Planning and Engineering* (NN44400-210).
- Complete *Avaya Aura™ Contact Center Installation Checklist* (NN44400-310).
- Install all of the components required for the Communication Control Toolkit software for your network configuration, including the updates. For more information, see *Avaya Aura™ Contact Center Installation* (NN44400-311).
- Install Contact Center Manager Server if Communication Control Toolkit is installed for Avaya Aura™ Contact Center. Contact Center Manager Server is not required if Communication Control Toolkit is installed for Knowledge Worker.
- Ensure the appropriate PABX is installed and configured for your system.
- Install Communication Control Toolkit and all current updates.
- Install License Manager software and all current updates.

Communication Control Toolkit commissioning for Knowledge Worker procedures

This task flow shows you the sequence of procedures you perform to configure Communication Control Toolkit in a Knowledge Worker or direct-connect environment. To link to any task, go to [Communication Control Toolkit commissioning for Knowledge Worker navigation \(page 104\)](#).

Communication Control Toolkit commissioning for Knowledge Worker procedures



Communication Control Toolkit commissioning for Knowledge Worker navigation

- [Confirming that the CCT services start \(page 105\)](#)
- [Configuring the licensing for CCT \(page 106\)](#)
- [Configuring the Avaya Communication Server 1000 service provider \(page 107\)](#)
- [Starting the CCT Web Administration application \(page 110\)](#)
- [Importing Avaya Communication Server 1000 Data \(page 110\)](#)

- [Importing Windows users from the CCT domain \(page 113\)](#)
- [Importing workstations from the domain \(page 115\)](#)
- [Assigning resources \(page 115\)](#)
- [Configuring Hotdesking \(Agent Roaming\) \(page 117\)](#)
- [Verifying CCT using the Reference Client \(page 118\)](#)

Confirming that the CCT services start

Confirm that the CCT services start so you can configure the Communication Control Toolkit database.

Procedure steps

Step	Action
1	Click Start, All Programs, Avaya, Contact Center, Common Utilities, System Control and Monitor Utility .
2	Select the CCT tab.
3	Confirm that the Communication Control Toolkit services are running.
4	If a Communication Control Toolkit service is not running, re-start CCT services.
5	Close the SCMU utility.

--End--

Procedure job aid

The following Communication Control Toolkit services must start:

- Caché Service
- NCCT SMON
- NCCT Logging Service
- ACD Proxy Service
- Telephony
- NCCT Data Access Layer
- NCCT TAPI Connector
- NCCT Server
- NCCT OI Service
- Contact Center Tomcat Instance

Configuring the licensing for CCT

Configure CCT licensing with the IP address of the server where Contact Center License Manager is installed and configured.

CCT consumes licenses as required. For example, every time a CCT client logs in as a CCT user and opens a terminal, CCT automatically uses a license. When a terminal is released the license is released.

Prerequisites

- Contact Center License Manager is installed.

Procedure steps

Step	Action
1	Log on to the Communication Control Toolkit server.
2	Click Start, All Programs, Avaya, Contact Center, Communication Control Toolkit, CCT Console .
3	Expand Communication Control Toolkit.
4	Expand Server Configuration .
5	Click License Configuration .
6	In the right pane, under Primary License Manager Server , in the IP Address box, type the IP address for the server on which the License Manager is installed.
7	Under Secondary License Manager Server , in the IP Address box, type the IP Address for the server on which the secondary License Manager is installed.

Attention: The Secondary License Manager Server IP Address section is only available if corporate licenses are installed.

- | | |
|---|---|
| 8 | From the License Type list, select Nodal or Corporate. |
| 9 | In the Actions pane on the right, select Apply changes . |

--End--

Variable definitions

Variable	Value
License Type	The type of license for the License Manager. Nodal—The license applies to only one installation of CCMS. You cannot configure the Secondary License Manager for a Nodal license. Corporate—The license applies to a collection of Contact Center Manager Servers. Secondary License Manager is only available for Corporate licenses.
Primary License Manager Server IP Address	The IP address of the server on which the License Manager application is installed.
Secondary License Manager Server IP Address	The optional IP address of the server on which the backup License Manager application is installed.

Configuring the Avaya Communication Server 1000 service provider

Configure the Avaya Communication Server 1000 service provider details to enable connection to the PABX. A polling message is sent every ten seconds to monitor the connection the PABX. The polling interval detail is configured in the Communication Server 1000 service provider details.

Prerequisites

- Understand the server provider details for the switch.

Procedure steps

Step	Action
1	Start Communication Control Toolkit Web Administration.
2	In the resource menu list, select Providers . <i>The details of the providers are displayed.</i>
3	From the list of providers, select Passive .
4	In the Basic Provider Information section, in the Passive Name box, type the Provider name.

Attention: The provider name must be *Passive*.

- | | |
|---|--|
| 5 | In the IP Address box, type the IP address of the provider. |
| 6 | In the Port box, type the port number. |
| 7 | In the Provider Configuration section, select the Transport type, TCP . |

Communication Control Toolkit commissioning for Knowledge Worker

- 8** In the **Customer Number**, type the customer number.
- 9** In the **CS1000 Software Release**, select the correct version.
- 10** In the **Call Data Life Span (minutes)**, type the required value in minutes.
- 11** Select or clear the **Disable Copy of Data to Consult Call** check box.
- 12** In the **CS1000 Home location Code (HLOC)**, type the HLOC value.
- 13** In the **Network IVR Port**, type the port value.
- 14** In the **Initialization Timeout (seconds)** box, type the **Initialization timeout** setting in seconds.
- 15** In the **Command Timeout (seconds)** box, type the **Command** timeout setting in seconds.
- 16** Select **Save**.

--End--

Variable definitions

Variable	Value
Provider Name	Name of the Provider, Passive.
IP Address	In a Knowledge Worker environment, the IP address of the Avaya Communication Server 1000.
Port	In a Knowledge Worker environment, the port value is 8888.
Transport	Transport protocol, default is TCP.
Customer Number	The customer number for the switch. If multiple customers are configured, you must specify a specific one in this box.
CS1000 Software Release	The release number of Avaya Communication Server 1000 software.
Call data	Call data is the information attached to calls routed from the switch. The Life Span default is 10 minutes. This value must be less than the time it takes to recycle the Communication Server 1000 Call IDs. Use the Disable copy of call data to consultative call check box to avoid copying call data during consultative calls, but you can still copy call data when calls are transferred or conferenced.
CS1000 Home Location Code (HLOC)	Avaya Communication Server 1000 Home Location Code (HLOC) of the switch is the address digits that specify a location node.
Network IVR Port	Port for the CCT network call attached data and for IVR call attached data.
Timeout in Seconds	Initialization—The length of time that the service provider waits to establish communication with the switch before generating an error. The default and minimum value is 32 seconds. If you use a large number of lines, you must increase this value accordingly. Command—The length of time that the service provider waits for a command response before generating an error. The default and minimum value is 5 seconds.

Starting the CCT Web Administration application

CCT Web Administration starts from the Contact Center Manager Administration (CCMA) server. In a knowledge worker environment without CCMA installed, the CCT Web Administration application is accessed on the CCT server by using a URL.

Procedure steps

Step	Action
1	Open Internet Explorer.
2	Type the URL <code>http://<CCT IP address>:8081/WebAdmin/</code> .

--End--

Importing Avaya Communication Server 1000 Data

You can use the CCT Import CS 1000 Data tool to perform either of the following activities:

- Perform the first step of the import process, convert data capture text file to an XML file. This is done by un-checking the “Automatically import data after conversion” checkbox (this is checked by default).
- Perform both steps of the import process, convert text file to XML file and import data to the database. This is done by leaving the default setting “Automatically import data after conversion”.

You can convert the text file to an XML file to test the data import facility without modifying the database contents; or, you can postpone the actual import of the data to an off peak time. The intermediate XML data file generated can be imported at a later stage using the CCT Data Import/Export Tool, by selecting the “Standard XML” format option.

Before you import the Avaya Communication Server 1000 data to CCT, you must first retrieve the data from the switch. To retrieve the data, create a switch configuration text file to capture the Communication Server 1000 data required to configure Communication Control Toolkit.

Do not use the Communication Control Toolkit server to import the information directly from the switch. Hyperterminal, when installed on the CCT server, interferes with the Telephony services and they remain running.

Prerequisites

- Connect a COM cable from a server (not the Communication Control Toolkit server) or workstation to the switch.

- Know the user ID and password to log on to the Avaya Communication Server 1000.
- Apply all Avaya Communication Server 1000 patches, specifically patch MPLR26704. Patch MPLR26704 significantly reduces the time to import address and terminal information into the text file. Only information that is relevant to Communication Control Toolkit is imported.
- Only PABX keys that are AST and IAPG enabled are imported.

Procedure steps

- | Step | Action |
|------|---|
| 1 | Open a text editor on the server where the Hyperterminal is installed. |
| 2 | Create a new text file called download.txt . |
| 3 | Click Start, All Programs, Accessories, Communications, HyperTerminal to connect to the Avaya Communication Server 1000. |
| 4 | Type a name for the connection. |
| 5 | Click OK . |
| 6 | On the Connect To dialog box, in the Connect using list, select COM1 or the COM port connected to the Avaya Communication Server 1000 switch. |
| 7 | Click OK . |
| 8 | In the COM properties dialog box, verify the data is correct or make necessary changes. |
| 9 | Click OK . |
| 10 | From the Transfer menu, select Capture Text . |
| 11 | In the Capture Text dialog box, type the location and name of the text capture file in the File box, for example, type the location and name of the download.txt file created in step 2. |
| 12 | Click OK . |
| 13 | At the prompt, type logi admin1 to log on to the switch. |
| 14 | Type your user ID and password for the switch. |
| 15 | If the prompt does not appear, continue to press Enter until the prompt appears. |
| 16 | Browse to the download.txt file, and then click Start . |
| 17 | Type these commands at the following prompts:

>LD 20

REQ: PRT

TN: TNB

TN: Press enter

CDEN: Press enter |

CUST: 0 (or the customer number)

DATE: Press enter

PAGE: ON

DES: Press enter

Downloading information from the Communication Server 1000 overlay can take a several minutes.

18 To return to the prompt, enter ******** (Shift + 8888).

19 Press **Enter**.

20 Type these commands at the following prompts:

>LD 23

REQ: PRT

TYPE: CDN

CUST: 0 (or the customer number)

CDN: Press enter

The information is downloaded from the overlays.

21 Type **logo**.

22 Press **Enter**.

23 Copy the download.txt to the Communication Control Toolkit server.

24 Log on to the Communication Control Toolkit server.

25 Click **Start, All Programs, Avaya, Contact Center, Communication Control Toolkit, CCT Console**.

26 Expand Communication Control Toolkit.

27 Expand **Bulk Provisioning**.

28 Select **Import CS 1000 Data**.

29 Select **Passive** for the Communication Server 1000 Provider.

30 Select **Input File**. This opens a file explorer to select the Communication Server 1000 data capture file you copied in [step 23](#).

31 Select the Communication Server 1000 data capture file, click **Open**. A default path and file name appears in the **Output file**, change this if necessary.

32 To import the data into the database, select **Automatically import data after conversion**.

33 In the Actions pane on the right, select **Convert/Import**. A progress bar in the Status area indicates the progress made by the tool in three phases:

- Conversion of the data capture file
- Generation of the output file
- Import of the data into the database

- 34** The status area displays data imported and the conversion results, including the number of TNs, DNS, and CDNs found. If applicable, a list of errors are also displayed. This list includes line numbers where the errors were discovered in the supplied data capture file.

Attention: An error dialog shows errors in the conversion step. The error dialog appears prior to beginning the automatic import. The user can choose to cancel the import step or proceed.

--End--

Importing Windows users from the CCT domain

Import windows users from the contact center domain server to Communication Control Toolkit using the Import Windows Users tool. After the users are imported in the CCT Snap-in Console, you can configure the resources in the CCT Web Administration client.

Prerequisites

- Ensure that the local administrator has user access for the contact center domain. The local administrator needs domain access to import domain users using the CCT Snap-in Console.

Procedure steps

Step	Action
1	Log on to the Communication Control Toolkit server.
2	Click Start, All Programs, Avaya, Contact Center, Communication Control Toolkit, CCT Console .
3	Expand Communication Control Toolkit.
4	Expand Bulk Provisioning .
5	Select Import Windows Users .
6	In the Location box, select the domain or server on which you want to look for Windows users.
7	In the Search Type box, select the group of users you want to display. You can look for All Users , a Login Name , a First Name , or a Last Name .
8	In the Begins With box, type the text to use in a search for Windows Users.
9	In the Actions Pane on the right, select Search For Users .
10	In the Search Results box, select the Windows users to import. To select multiple users, press the Ctrl key while you select each user. To select all Windows users, click Add All .

11 Click **Add**.

12 In the Actions pane, select **Import Selected Users**.

--End--

Variable definitions

Variable	Value
Search Type	The criteria for selecting a small group of Windows user accounts to import to the Communication Control Toolkit. You can choose one of the following options: • Find All Users—find all Windows user accounts on the CCT server. • Login Name—find all Windows user accounts where the user name or logon ID matches or contains the value in the Begins With box. • First Name—find all Windows user accounts where the first name matches or contains the value in the Begins With box. • Last Name—find all Windows user accounts where the last name matches or contains the value in the Begins With box.
Begins With	A string of characters to match the beginning of the text with in the search for the selected Search Type.

Importing workstations from the domain

All Contact Center applications are in a contact center domain. Import workstations from the contact center domain to the Communication Control Toolkit server using the Import Workstations tool.

Prerequisites

- A local administrator must have access to the contact center domain to import domain resources to CCT. Domain resources that can be imported are domain users and domain workstations. Ensure the local administrator has access to the contact center domain.

Procedure steps

Step	Action
1	Log on to the Communication Control Toolkit server.
2	Click Start, All Programs, Avaya, Contact Center, Communication Control Toolkit, CCT Console .
3	Expand Communication Control Toolkit.
4	Click Import Work Stations .
5	From the Search Type list, select All WorkStations .
6	From the Available Work Stations list, select the workstations to import.
7	Click Add .
8	Click OK .

--End--

Assigning resources

Resources in CCT are users, terminals, addresses, and workstations. To enable CCT to work follow the basic configuration:

- assign a terminal to one or two addresses
- assign a terminal to a workstation
- assign a terminal to a user.

Make configuration changes quickly in your contact center by organizing users, terminals and addresses into groups. This allows you to map your resource groups to functional roles in your contact center.

Use the Communication Control Toolkit Web Administration client to assign resources.

Procedure steps

- | Step | Action |
|------|---|
| 1 | Launch the CCT Web Administration client . |
| 2 | Click the resource type. |
| 3 | Click the single resource to configure. |
| 4 | Select one of the Resource Assignments to assign to this resource. |
| 5 | Select the appropriate resources from those in the Available Resources column.

Click each resource to select more than one resource or resource group.
Select the resource again to deselect it. |
| 6 | Click the Right Arrow to move the selected resource and resource groups to the Assigned Resources column. |
| 7 | Click Save . |

--End--

Example of assigning resources

In a hotdesking configuration, CCT the resources are configured into groups.

Create a terminal group called hotdesking_terminals and assign all terminals to this group.

Assigning Terminals to a Terminal Group

- | Step | Action |
|------|---|
| 1 | Launch the CCT Web Administration client . |
| 2 | Select Groups . |
| 3 | Select Terminal Groups . |
| 4 | Select the hotdesking_terminals terminal group. |
| 5 | Select the all terminals in the Available Resources column.

Click each resource to select more than one resource. |
| 6 | Click the Right Arrow to move the selected terminals to the Assigned Resources column. |
| 7 | Click Save . |

--End--

Configuring Hotdesking (Agent Roaming)

In a contact center an agent may not have a fixed desk and phone. An agent might pick a desk that is not being used and log into the phone and workstation. An agent must be able to log onto any phone and workstation in this environment.

In a hotdesking environment using any configured workstation, agents can control the terminal and addresses associated with that workstation.

To enable hotdesking in CCT, a Windows user is assigned to multiple terminals; each terminal is assigned to its respective workstation. The user's terminal is determined by the workstation that the user logs on to, as shown in the following example.

- Terminal_1 maps to workstation_1.
- Terminal_2 maps to workstation_2.

For example, assume that User_1 is assigned to Terminal_1 and Terminal_2 and the respective addresses. If User_1 logs on to workstation_2, then the user also logs on to Terminal_2.

Prerequisites

- Assign each terminal to a workstation.
- Add terminals to a terminal group.
- Ensure that all terminals have the correct address assigned to them.
- If you require additional terminals (and therefore addresses) in the hotdesking group, add the new terminals to the terminal group and the new addresses to the address group. Follow this process to ensure that the correct resources are available to all roaming CCT agents at all times.

Procedure steps

Step	Action
1	Place all select terminals for hotdesking into a terminal group.
2	Ensure that all terminals have the correct address assigned to them.
3	Place all the addresses associated with the terminals into an address group.
4	Place all select users for hotdesking into a user group.
5	Assign the terminal group from step 1 to the user group from step 4 with the automatic mapping of addresses check box cleared.
6	Assign the address group from step 3 to the user group from step 4.
7	Assign each terminal to a workstation.

Attention: A terminal can only be assigned to one workstation.

--End--

Verifying CCT using the Reference Client

Verify Communication Control Toolkit by using the Reference Client to ensure that all resources are available and accessible. The Reference Client is only an installation testing tool and not to be deployed for production contact center use.

You can use several user IDs to log on to the Reference Client to make calls between them to test connections, transfers, and other call functions.

Prerequisites

- Import the resources from the external sources to the Communication Control Toolkit Console. See the following sections:
 - [Importing Avaya Communication Server 1000 Data \(page 110\)](#)
 - [Importing Windows users from the CCT domain \(page 113\)](#)
 - [Importing workstations from the domain \(page 115\)](#)
- Assign the required resources in the Communication Control Toolkit Console. See [Assigning resources \(page 115\)](#).
- Create a Windows user for testing.

Procedure steps

Step	Action
1	Log on to the Communication Control Toolkit server with the Local Administrator user ID and password.
2	Click Start, All Programs, Avaya, Contact Center, Communication Control Toolkit, Ref Client .
3	In the Server Settings dialog box, click OK .
4	From the Session menu, choose Connect .
5	In the User Credentials dialog box, select either the Current Windows User or specify a User ID, Domain and Password .
6	Click OK .
7	In the Available Devices box, select the address you want to use for the test call.
8	Enter the Destination Address in the text box to the right of the Originate button.
9	Click Originate . The destination address shows a Local State of Ringing in the Reference Client
10	Select the Ringing Address on the Reference Client, and click Answer .

11 Release the call.

--End--

Contact Center Multimedia server commissioning

Commission the Contact Center Multimedia server to manage multimedia contacts in your Avaya Aura™ Contact Center.

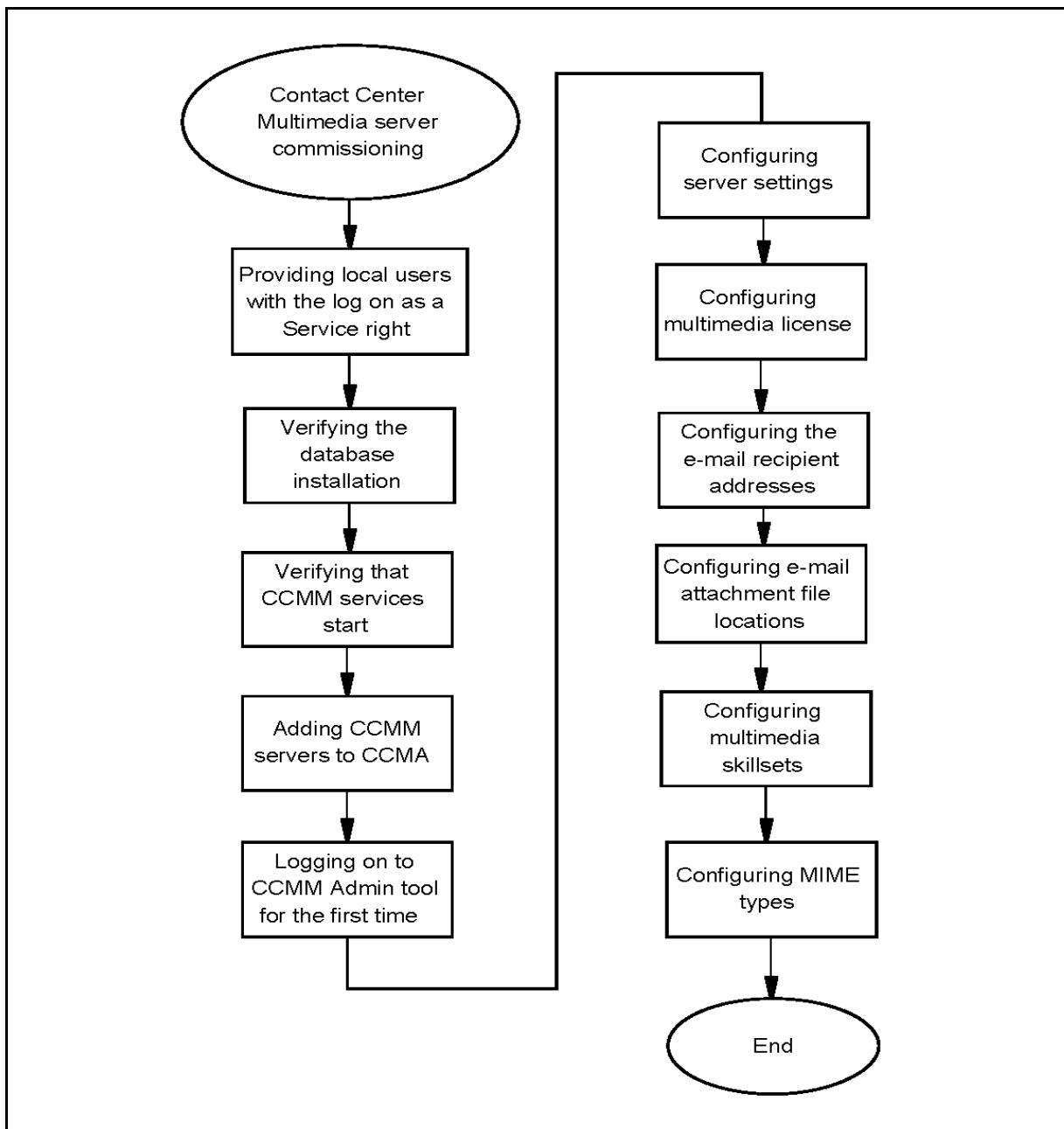
Contact Center Multimedia server commissioning prerequisites

- Install Contact Center Manager Server in the Contact Center. See *Avaya Aura™ Contact Center Installation* (NN44400-311).
- Install Contact Center Manager Administration server software in the Contact Center. See *Avaya Aura™ Contact Center Installation* (NN44400-311).
- Install Communication Control Toolkit server software in your Contact Center. See *Avaya Aura™ Contact Center Installation* (NN44400-311).
- Install Contact Center Multimedia server software in your Contact Center. See *Avaya Aura™ Contact Center Installation* (NN44400-311).
- Configure Open Queue as a feature in the Contact Center Manager Server installation. See *Avaya Aura™ Contact Center Installation* (NN44400-311).
- Configure Communication Control Toolkit on the Contact Center Manager Server configuration window. See *Avaya Aura™ Contact Center Installation* (NN44400-311).
- Commission the Communication Control Toolkit server. See [Communication Control Toolkit commissioning for Contact Center \(page 83\)](#).
- Apply the most recent service packs for Contact Center Multimedia. See *Avaya Aura™ Contact Center Upgrade and Patches* (NN44400-410).

Contact Center Multimedia server commissioning procedures

To commission the Contact Center Multimedia server, you must perform the following procedures. To link to any procedure, go to [Contact Center Multimedia server commissioning navigation \(page 122\)](#).

Contact Center Multimedia server commissioning procedures



Contact Center Multimedia server commissioning navigation

- [Providing local users with the Log on as a service right \(page 123\)](#)
- [Verifying the Multimedia database installation \(page 124\)](#)
- [Verifying that Contact Center Multimedia services start \(page 124\)](#)
- [Adding the multimedia servers to Contact Center Manager Administration \(page 125\)](#)

- [Logging on to the Multimedia Administration tool for the first time \(page 126\)](#)
- [Configuring server settings \(page 127\)](#)
- [Configuring multimedia license \(page 129\)](#)
- [Configuring e-mail recipient addresses \(page 129\)](#)
- [Configuring e-mail attachment file locations \(page 132\)](#)
- [Configuring the multimedia skillsets \(page 133\)](#)
- [Configuring the MIME types \(page 135\)](#)

Job aid: Timing

The estimated time to commission Contact Center Multimedia is 1 hour.

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 | Under Security Settings , in the left pane, double-click Local Policies . |
| 3 | In the left pane, click User Rights Assignment . |
| 4 | In the right pane, double-click Log on as a service . |
| 5 | Click Add User or Group . |
| 6 | Click Locations . |
| 7 | In the Locations dialog box, select the 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 | Click Apply to save the changes. |
| 13 | Click OK . |
| 14 | Close the Local Security Settings window. |

--End--

Variable definitions

Variable	Value
IUSR	An Internet Information Services (IIS) account used for all communication between the Multimedia server and the Contact Center Agent Desktop over HTTP.

Verifying the Multimedia database installation

Verify that the Multimedia database is installed and configured correctly.

Prerequisites

- Install Contact Center Multimedia.
- Log on to the Contact Center Multimedia/Outbound server.

Procedure steps

Step	Action
1	On the Multimedia/Outbound Server, open Internet Explorer.
2	Browse to http://<servername>/csp/multimedia/ws.Contact.cls .
3	If a Web page does not appear, contact your Avaya technical support prime.

--End--

Variable definitions

Variable	Value
servername	Name of the Multimedia server.

Verifying that Contact Center Multimedia services start

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

Prerequisites

- Log on to the Contact Center Multimedia server.

Procedure steps

- | Step | Action |
|------|--|
| 1 | On the Contact Center Multimedia 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 . |
| 4 | Verify that the following services started: <ul style="list-style-type: none"> • CCMM Multimedia Contact Manager • CCMM OAM service • CCMM Campaign Scheduler service |
| 5 | If any service does not start, in the Services window, right-click the service name, and then click Start . |

--End--

Adding the multimedia servers to Contact Center Manager Administration

Add the servers necessary to manage multimedia contacts to the Contact Center Manager Administration to provide reporting and connectivity support.

Prerequisites

- Obtain a user ID and password for the Contact Center Manager Administration client application.
- Know the computer name of the server to add.

Procedure steps

- | Step | Action |
|------|--|
| 1 | Log on to the Contact Center Manager Administration server. |
| 2 | Log on to Contact Center Manager Administration. |
| 3 | On the Launchpad, click Configuration . |
| 4 | On the configuration menu, select Server, Add Server . |
| 5 | In the Server Name box, type the computer name of the Multimedia or Predictive Outbound server. |
| 6 | Press the Tab key.
<i>The server IP address automatically appears in the IP Address box.</i> |

Contact Center Multimedia server commissioning

- 7 In the **Display Name** box, type the name of the Multimedia or Predictive Outbound server as you want it to appear in the system tree in Contact Center Manager Administration.

The system automatically assigns a display name that is the same as the server name. To enter a different display name, you must enter a unique name.
 - 8 To add a Contact Center Multimedia server, in the **Login ID** box, type **mmReport**.
 - 9 In the **Password** box, type your password
- Attention:** You must change this password if the system sends a message that contains a logon request for validation.
- 10 From the **Type** list, select CCMM.
 - 11 Click **Submit**.
 - 12 Click the plus symbol (+) beside the server name to access the server.
 - 13 In the left pane, select the Contact Center Manager Server with which you want to associate the Contact Center Multimedia server.
 - 14 Right-click the Contact Center Manager Server and then click **Edit Properties**.
 - 15 Under **Associated Reporting Server**, select the check box next to the current active Contact Center Multimedia server name.
 - 16 Click **Submit**.

--End--

Variable definitions

Variable	Value
Login ID	For Contact Center Multimedia, the Login ID corresponds to the user in running historical reports in Contact Center Manager Administration. This user is configured in the Multimedia database and has access to data within that database. The Login ID is always mmReport.
Password	For Contact Center Multimedia, the default password is mmRep. To change this password, use the Contact Center Multimedia Administrator.

Logging on to the Multimedia Administration tool for the first time

Log on to Contact Center Multimedia Administration tool to configure the Contact Center.

Prerequisites

- Obtain a user ID and password for the Contact Center Manager Administration client application.

Procedure steps

- | Step | Action |
|------|---|
| 1 | Log on to the Contact Center Manager Administration server. |
| 2 | Start Internet Explorer. |
| 3 | In Internet Explorer, choose Tools, Internet Options, Trusted Sites, Custom Level . |
| 4 | Under Downloads , for Automatic prompting for file downloads , select Enable . |
| 5 | In Internet Explorer , choose Tools, Internet Options, Trusters Sites, Sites . |
| 6 | Under Add this website to the zone , type the name of the CCMM server. |
| 7 | Click Close . |
| 8 | Click OK . |
| 9 | Log on to Contact Center Manager Administration application with administrative privileges. |
| 10 | On the Launchpad , click Multimedia . |
| 11 | In the left pane, select the Contact Center Multimedia to which you want to log on. |
| 12 | On the File Download window, click Run . |
| 13 | On the Internet Explorer window, click Run . |

The Contact Center Multimedia Administration tool appears.

--End--

Configuring server settings

Configure the Contact Center application servers, Web communications, and e-mail servers to ensure that you can connect the Contact Center Multimedia server to the external servers for handling e-mail, voice mail, fax, scanned documents, and Web communications contacts.

Prerequisites

- Ensure that you understand for which contact types your Contact Center is licensed.
- Install the required software on your Web server and E-mail servers (if applicable).

Procedure steps

- | Step | Action |
|------|---|
| 1 | Log on to the Contact Center Manager Administration server. |
| 2 | Open the Contact Center Manager Administration application. |
| 3 | Type your user ID and password. |
| 4 | Click Multimedia . |
| 5 | In the left column, select General Administration . |
| 6 | Click Server Settings . |
| 7 | Select the server to update, and click Edit . |
| 8 | In Edit Server , type the details for the server. |
| 9 | Click Save . |

--End--

Variable definitions

Variable	Value
Server Name	The host name of the server.
Server Port	The communications port number for the server.
Server Type	Choose the server type, for example; CCT, CCMS, License Manager, or Standby CCT.
Backup Server	The standby license server name.
MCMC Event Port	The Multimedia Contact Management Client port number.
Primary Hostname	The host name of the primary e-mail server.
Port Number	The primary Inbound POP3 e-mail server port.
Secondary Hostname	The host name of the optional secondary e-mail server.
Username	The LDAP Server access account name.
Password	The LDAP Server access account password.
Search base	The LDAP base search string.
Polling Interval (hrs)	The LDAP polling interval.

Configuring multimedia license

Configure the license for the Contact Center Multimedia server. The license you choose must match the system license purchased for your contact center.

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

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
1	In the Contact Center Manager Administration launchpad, click Multimedia .
2	In the left column, click General Administration .
3	Click General Settings .
4	Under License Type , select the type of license used in your contact center.
5	Click Save .

--End--

Configuring e-mail recipient addresses

Configure the recipients in your contact center to handle e-mail, voice mail, fax, scanned documents, and SMS contacts. Each type of contact is scanned and attached to an e-mail that is received by the contact center and routed. You must configure the recipient mailboxes to ensure the contacts are routed.

Prerequisites

- Ensure that you understand for which contact types your Contact Center is licensed.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Open the Contact Center Manager Administration application.
3	Type your user ID and password.
4	Click Multimedia .
5	In the left column, select E-mail .
6	Click Recipient Addresses .
7	Click New .

Contact Center Multimedia server commissioning

- 8 From the **Mailbox Type** list, select **Mail Store** or **Alias**.
- 9 Enter the mailbox details.
- 10 Click **Save**.

--End--

Variable definitions

Variable	Value
Display name	The name to appear in the e-mail From address.
E-mail Domain	The domain for your e-mail server.
Mail Store or Alias	Select the Mail Store or Alias option. - Select Mail Store to include the e-mail mailbox in the set of mailboxes from which incoming e-mail is retrieved. - Select Alias to configure this mailbox as an alias. The address of an alias can be used in rules configuration and outbox mapping, but a recipient box configured as an alias address not contain e-mail.
Mailbox Name	The name of the mailbox that receives incoming e-mail to the Contact Center. If the Contact Center Multimedia/Outbound server is not in the same domain as the e-mail server, you must also include the domain. Include the domain in the format domain\user (Windows 2000) or user@domain (post- Windows 2000) in the Mailbox Name box. Example: To enter the e-mail address sales@avaya.com, in the Mailbox Name box, type sales, and in the E-mail Domain box, type avaya.com. Example: To enter the e-mail address sales@europe.avaya.com, in the Mailbox Name box, type europe\sales or sales@europe.avaya.com, and in the E-mail Domain box, type europe.avaya.com.
Password	The password for your mailbox.
Confirm	When you change a password on the e-mail server, you must update this password in the Multimedia Administrator.
POP3 Server	The name of the mail server that handles the e-mail into the Contact Center.
Inbound Mail Threshold	The maximum number of e-mail messages the mailbox can accept every time it scans the database. You can enter a different value for this variable for each mailbox. The default value is 10.
Rule Group	The name of the rule group that applies to this recipient mailbox.
SMTP Server	The name of the mail server that handles the e-mail that leaves the Contact Center.

Variable	Value
Use alternative user name for SMTP Authentication	Select this box if you are configure an inbox as an alias. If SMTP authentication is enabled on your E-mail Server, and you use aliases, you log on to the SMTP server with a different user name.
Username	The logon name for the SMTP server. You can have mailboxes on multiple e-mail servers. You can have multiple e-mail servers for e-mail or fax messages, load balancing, and managing e-mail subtypes. Each e-mail server is polled for the mailboxes that it hosts. Configure additional e-mail servers using the Server Configuration window. For instructions about configuring additional e-mail servers, see <i>Avaya Aura™ Contact Center Server Administration</i> (NN44400-610).

Configuring e-mail attachment file locations

Configure the locations for inbound and outbound e-mail attachments.

Procedure steps

- | Step | Action |
|------|---|
| 1 | Log on to the Contact Center Manager Administration server. |
| 2 | Open the Contact Center Manager Administration application. |
| 3 | Type your user ID and password. |
| 4 | On the Launchpad , click Multimedia . |
| 5 | In the left column, select E-mail . |
| 6 | Under Attachment Files , in the Inbound URL box, type the URL for files attached to inbound e-mail messages. |
| 7 | Under Attachment Files , in the Inbound Share box, type the share location for files attached to inbound e-mail messages. |
| 8 | Under Attachment Files , in the Outbound URL box, type the URL for files attached to outbound e-mail messages. |
| 9 | Under Attachment Files , in the Outbound Share box, type the share location for files attached to outbound e-mail messages. |
| 10 | Click Save . |

--End--

Variable definitions

Variable	Value
Inbound URL	The URL for files attached to inbound e-mail messages. For contact centers using the Avaya Aura™ Contact Center High Availability feature, Avaya recommends using: http://<managedIPAddress>/InboundAttachment Where managedIPAddress is the managed IP address of the CCMM server.
Inbound Share	The share location for files attached to inbound e-mail messages. Avaya recommends using: <driveLetter>:\Avaya\Contact Center\Email Attachments\Inbound
Outbound URL	The URL for files attached to outbound e-mail messages. For contact centers using the Avaya Aura™ Contact Center High Availability feature, Avaya recommends using: http://<managedIPAddress>/OutboundAttachment Where managedIPAddress is the managed IP address of the CCMM server.
Outbound Share	The share location for files attached to outbound e-mail messages. Avaya recommends using: <driveLetter>:\Avaya\Contact Center\Email Attachments\Outbound

Configuring the multimedia skillsets

Configure multimedia skillsets to ensure that you can route multimedia contacts in your contact center. Multimedia contacts include e-mail, fax, scanned documents, SMS text messages, voice mail, Web communications, outbound contacts, and instant messages. You must configure a route point for each default skillset, and add any other skillset you intend to use for routing contacts.

Prerequisites

- Ensure that you understand for which contact types your Contact Center is licensed.

- Configure the route points in Contact Center Manager Administration that you plan to use for the multimedia skillsets.

Procedure steps

Step	Action
------	--------

- | | |
|---|---|
| 1 | Log on to the Contact Center Manager Administration server. |
| 2 | Open the Contact Center Manager Administration application. |
| 3 | Type your user ID and password. |
| 4 | Click Multimedia . |
| 5 | In the left column, select General Administration . |
| 6 | Click Skillset Settings . |
| 7 | Select the skillset to update, and click Edit . |

Attention: You must configure at least one skillset for each type of contact for which your contact center is licensed. You must configure the default skillset.

- | | |
|---|---|
| 8 | In the Route Point box, select a Route Point for the skillset. |
| 9 | Repeat step 7 and step 8 for each default skillset. |

--End--

Variable definitions

Variable	Value
Route Point	An equivalent routing number for a non voice contact. You must configure Route points in Contact Center Manager Administration.
Skillsets	You must configure at least one skillset for each contact type for which you are licensed. • Voice skillsets are prefixed by VO_ or do not contain a prefix. • E-mail skillsets are prefixed by EM_. You can also configure an optional automatic response for an e-mail skillset that is used to respond immediately to an e-mail message from a customer. • Outbound skillsets are prefixed with OB_. • Web Communication skillsets are prefixed with WC_. • SMS text message skillsets are prefixed with SM_. • Instant Message skillsets are prefixed with IM_. • Voice mail skillsets are prefixed with VM_. • Fax skillsets are prefixed with FX_. • Scanned document skillsets are prefixed with SD_.

Configuring the MIME types

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

Prerequisites

- Install Contact Center Multimedia server software.
- Log on to the Contact Center Multimedia server.

Procedure steps

- | Step | Action |
|------|---|
| 1 | From the Start menu of the Contact Center Multimedia server, click Administrative Tools, Computer Management . |
| 2 | In the Computer Management dialog box, expand Services and Applications, Internet Information Services, Sites . |
| 3 | Select Default Web Site . |
| 4 | Under IIS , select MIME Types . |
| 5 | Double-click MIME Types . |
| 6 | On the Actions list on the right, click Add . |
| 7 | In the File name extension box, type .dic . |
| 8 | In the MIME Type box, type application/octet-stream . |
| 9 | Click OK . |
| 10 | On the Actions list on the right, click Add . |
| 11 | In the File name extension box, type .eml . |
| 12 | In the MIME Type box, type application/octet-stream . |
| 13 | Click OK . |
| 14 | On the Actions list on the right, click Add . |
| 15 | In the File name extension box, type .dat . |
| 16 | In the MIME Type box, type application/octet-stream . |
| 17 | Click OK . |
| 18 | Close the Computer Management window. |

--End--

Variable definitions

Variable	Definition
Extension	The Multipurpose Internet Mail Extension (MIME) types required by Avaya Aura Agent Desktop. • .dic • .eml • .dat
MIME Type	The Multipurpose Internet Mail Extension (MIME) information required by Avaya Aura Agent Desktop: application/octet-stream.

Agent Desktop client commissioning

Commission each Avaya Aura™ Agent Desktop client in your Avaya Aura™ Contact Center to run the Avaya Aura™ Agent Desktop application.

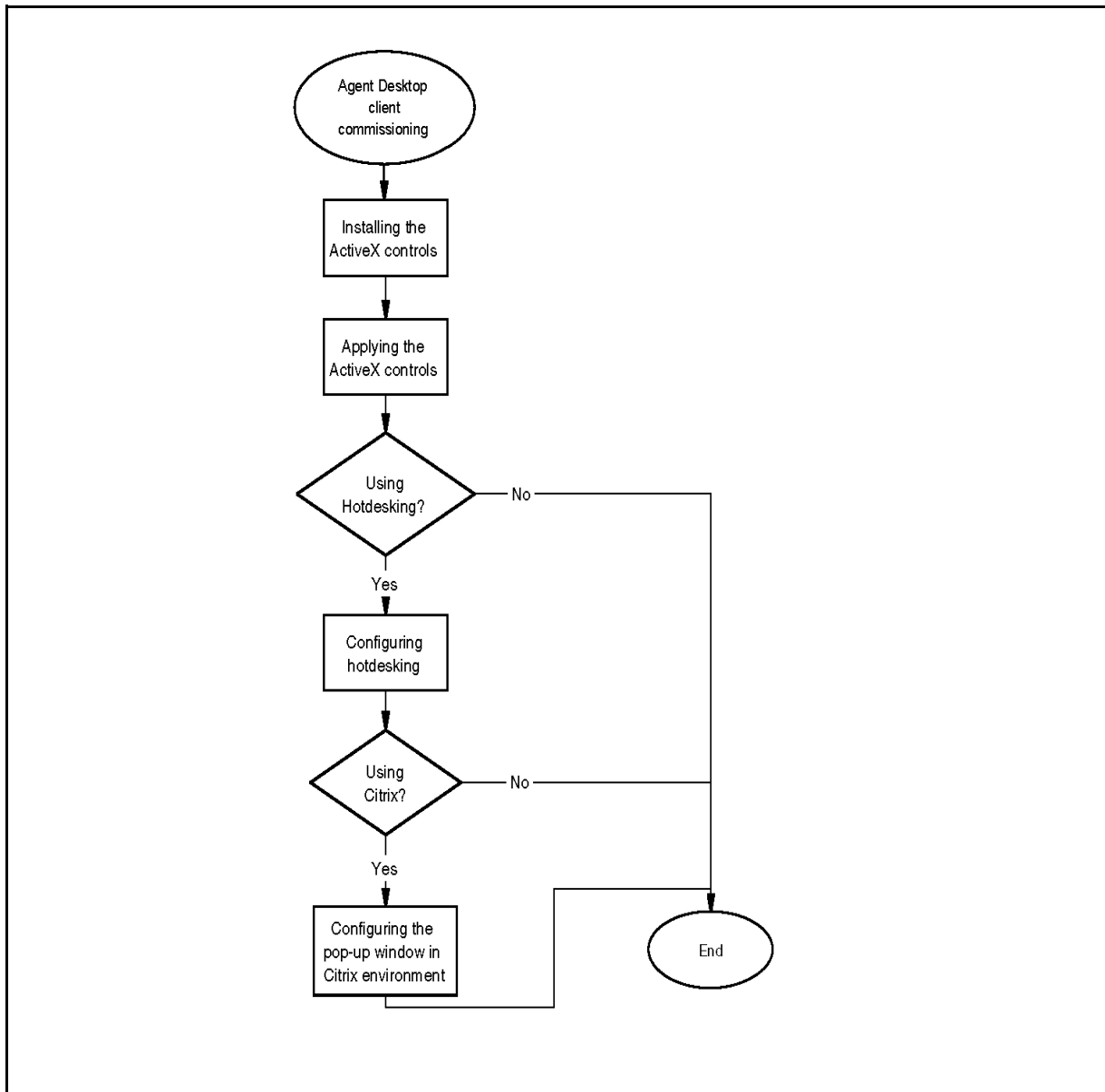
Prerequisites for Agent Desktop client commissioning

- Install Contact Center Multimedia or Agent Desktop. See *Avaya Aura™ Contact Center Installation* (NN44400-311).

Agent Desktop client communications server commissioning procedures

This task flow shows you the sequence of procedures you perform to commission or set up the Agent Desktop clients. To link to any procedure, go to [Agent Desktop client commissioning navigation \(page 138\)](#).

Avaya Aura™ Agent Desktop client commissioning procedures



Agent Desktop client commissioning navigation

- [Installing the ActiveX Controls \(page 80\)](#)
- [Applying the ActiveX Controls \(page 81\)](#)
- [Configuring hotdesking \(optional\) \(page 139\)](#)
- [Configuring the pop-up window for a Citrix environment \(page 139\)](#)

Configuring hotdesking (optional)

Configure hotdesking in your Contact Center so that an agent can sit at any desk and log on to the Agent Desktop.

With hotdesking enabled and configured, when agents start the Agent Desktop, they automatically map to the relevant terminal and addresses without user intervention.

If you use a Citrix environment, you must configure the prompt for the workstation. For more information, see [Configuring the pop-up window for a Citrix environment](#).

Prerequisites

- Install Contact Center Multimedia or Agent Desktop. See *Avaya Aura™ Contact Center Installation* (NN44400-311).
- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
1	Click Multimedia .
2	In the left column, select Agent Desktop Configuration .
3	Choose General Settings .
4	Under Hot Desking , select the Enabled check box.

--End--

Configuring the pop-up window for a Citrix environment

Configure the pop-up window to allow agents to log on to their computer using their own user ID and password in a Citrix environment.

Prerequisites

- Install Contact Center Multimedia or Agent Desktop. See *Avaya Aura™ Contact Center Installation* (NN44400-311).
- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
1	Click Multimedia .
2	In the left column, select Agent Desktop Configuration .
3	Choose General Settings .

- 4 Under **Hot Desking**, select the **Prompt for Workstation** check box.

--End--

External Web communication server commissioning

After you install the external Web server, you can use it to develop Web pages for your corporate Web site. Perform the procedures in this section to configure your production Web server.

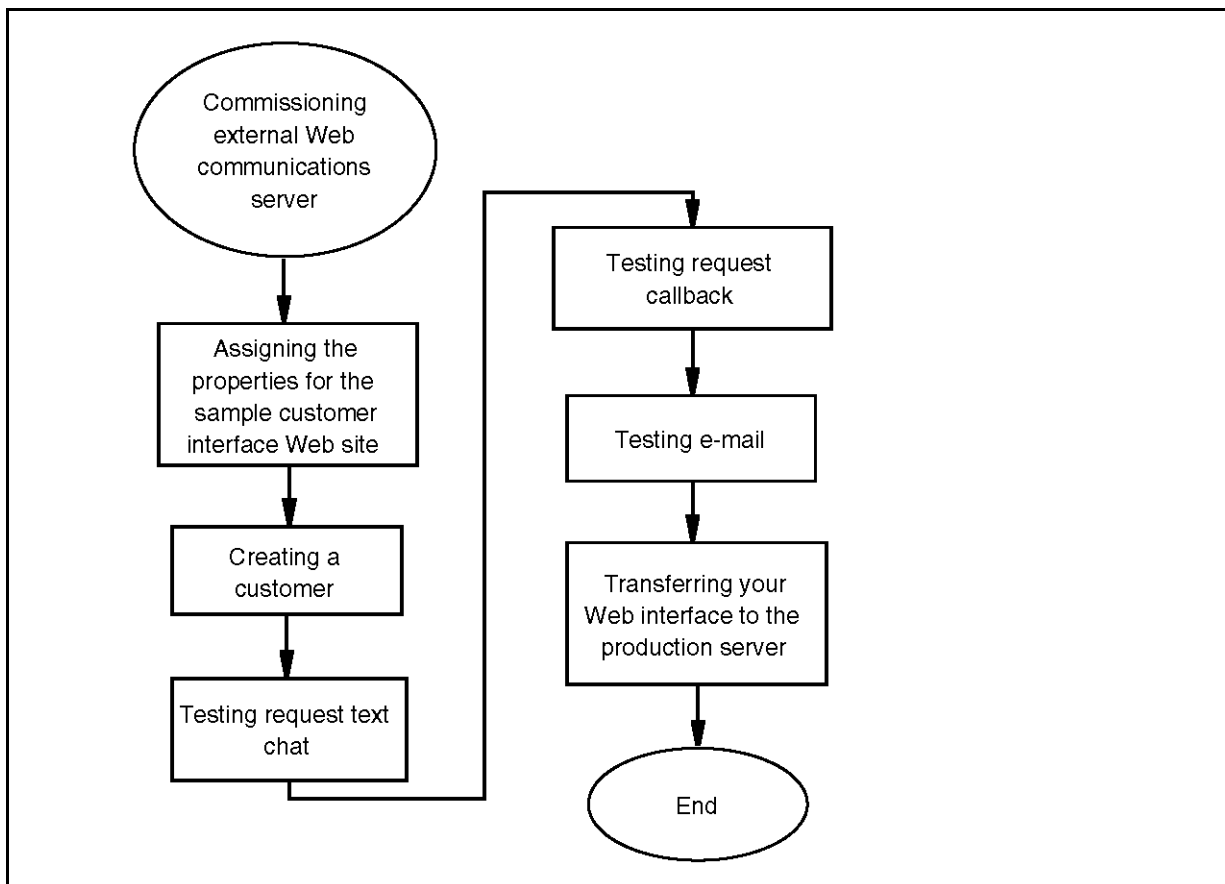
External Web communication server commissioning prerequisites

- Install the Multimedia server software on the external Web server. See *Avaya Aura™ Contact Center Installation* (NN44400-311).
- Ensure that the Web server meets the minimum requirements to install Apache Tomcat 5.5.
- Ensure that the Apache Tomcat 5.5 Servlet engine is installed on the Web server. For more information and instructions to install Apache Tomcat 5.5, see www.apache.org.
- Ensure that the Web server has J2SE 5.0.

External Web communication server commissioning procedures

This task flow shows you the sequence of procedures you perform to commission the external Web communication server. To link to any procedure, go to [External Web communication server commissioning navigation \(page 142\)](#).

External Web communication server commissioning procedures



External Web communication server commissioning navigation

- [Assigning the properties for the sample customer interface Web site \(page 143\)](#)
- [Creating a customer \(page 144\)](#)
- [Testing request text chat \(page 145\)](#)
- [Testing request callback \(page 146\)](#)
- [Testing e-mail \(page 147\)](#)
- [Transferring your Web interface to the production server \(page 148\)](#)

Assigning the properties for the sample customer interface Web site

Assign the properties for the sample customer interface Web site to ensure the sample Web site uses the correct variables and code developed for your Web site on the practice server.

The web.xml file for the sample customer interface Web site is in the webapps\CI_Sample_Website\WEB_INF folder of the Tomcat Servlet folder.

Prerequisites

- Install the Multimedia server software on the External Web server. See *Avaya Aura™ Contact Center Installation* (NN44400-311).

Procedure steps

- | Step | Action |
|------|---|
| 1 | On the Contact Center Multimedia server, browse to webapps\CI_Sample_Website\WEB_INF in the Tomcat Servlet container. |
| 2 | In the WEB_INF folder, open the web.xml file. |
| 3 | Configure the following items: <ul style="list-style-type: none">• CCMM_HOSTNAME• EMAILSERVER_HOSTNAME• PASSWORD_REMINDER_SKILLSET• WEBCOMMS_HOSTNAME• WEBCOMMS_PORT• WEBCOMMS_PATH• HTML_FORM_TO_ADDRESS• HTML_FORM_SUBJECT |

--End--

Variable definitions

Variable	Value
CCMM_HOSTNAME	The sample CI Web site uses the customer interface Web services located on your Contact Center Multimedia server.
EMAILSERVER_HOSTNAME	The host name of the e-mail server used to send e-mail by using Java mail and Standard Mail Transfer Protocol (SMTP). The sendmail.jsp page uses SMTP to send e-mail messages to a Multimedia recipient address. The e-mail server must be able to relay e-mail messages to an e-mail server configured in Contact Center Multimedia.
HTML_FORM_TO_ADDRESS	The default To e-mail address on the page submitHTMLForm.jsp. The HTML_FORM_TO_ADDRESS must be a valid Multimedia recipient address.
HTML_FORM_SUBJECT	The default subject on the page submitHTMLForm.jsp. The default subject is HTML Form Submitted from the Web.
PASSWORD_REMINDER_SKILLSET	The password reminder e-mail contacts are created as closed contacts within this defined skillset. By default, the password reminder skillset is assigned to EM_Default_Skillset. The value of PASSWORD_REMINDER_SKILLSET is used by the passwordReminder_WSCient.jsp page.
WEBCOMMS_HOSTNAME	The host name of the Web server hosting the Web communications application.
WEBCOMMS_PATH	The URL path used to access the Web communications application. The default path is /WebComms/jsp/index.jsp.
WEBCOMMS_PORT	The port number used by the Web communications application. The default value is 8080.

Creating a customer

Create a customer to test Web communications on the external test Web site.

Prerequisites

- Assign the properties for the sample customer interface Web site. See [Assigning the properties for the sample customer interface Web site \(page 143\)](#).

Procedure steps

Step	Action
1	Start your Web browser at the Tomcat homepage. Typically, the URL for the Tomcat homepage is http://<webservername>:8080 .
1	Open the sample customer interface homepage which is http://<webservername>:8080/CI_Sample_Website/ .
2	Click Register New Customer .
3	In the First Name box, type the first name.
4	In the Last Name box, type the last name.
5	In the Username box, type an e-mail address as the user name.
6	In the Password box, type a password.
7	In the E-mail Address box, type the e-mail address that you typed in the Username box.
8	In the Confirm Password box, type the password again.
9	In the Number box, type the phone number.
10	Select the Login Customer check box to log this customer on immediately after you register the customer.
11	Click Register .

--End--

Testing request text chat

Test the request text chat functionality by using the Customer interface to ensure that the Web pages work correctly.

Prerequisites

- Create a test customer. See [Creating a customer \(page 144\)](#).
- Ensure that you have an agent who is assigned to a Web communications skillset.

Procedure steps

Step	Action
1	On the sample customer interface homepage, click Log in Customer .
2	In the Username box, type the test customer user name.
3	In the Password box, type the test customer password.
4	Click Log on .

- 5 Log on an agent who can handle a Web communications skillset on to the Contact Center Agent Desktop. Make the agent available to receive contacts.
- 6 Click **Request Text Chat** to create a text chat contact.
- 7 From the **Skillset** list, select the skillset that your logged on agent is eligible to handle.
- 8 In the **Subject** box, type the subject of the text chat.
- 9 Click **Submit**.
On the Agent Desktop, your logged on agent receives the Web communications contact.
- 10 Close the test contact window.
- 11 Click **Logoff Customer** to log off the test customer.

--End--

Testing request callback

Test request callback functionality to test ensure the functions work on your Web communications interface.

Prerequisites

- Create a test customer. See [Creating a customer \(page 144\)](#).
- Ensure that you have an agent who can handle an Outbound skillset.

Procedure steps

- | Step | Action |
|------|--|
| 1 | On the sample customer interface homepage, click Log in Customer . |
| 2 | In the Username box, type the test customer user name. |
| 3 | In the Password box, type the test customer password. |
| 4 | Click Log on . |
| 5 | Log on an agent who can handle an Outbound skillset on to the Agent Desktop. Make the agent available to receive contacts. |
| 6 | Click Request Immediate Callback to create an outbound contact. |
| 7 | From the Skillset list, select the skillset that your agent is eligible to handle. |
| 8 | In the Subject box, type the subject of the outbound contact. |
| 9 | In the Objective box, type a summary of the reason for the callback. |
| 10 | Click Submit .
<i>On the Agent Desktop, your logged on agent receives the outbound contact.</i> |

- 11 Close the test contact.
- 12 Click **Logoff Customer** to log off the test customer.

--End--

Testing e-mail

Test e-mail functionality to test ensure the e-mail functions work on your Web communications interface.

Prerequisites

- Create a test customer. See [Creating a customer \(page 144\)](#)
- Configure an e-mail message box that assigns e-mail messages to the skillset to which you log your agent on.
- Ensure that you have an agent who can handle an e-mail message.

Procedure steps

- | Step | Action |
|------|--|
| 1 | On the sample customer interface homepage, click Log in Customer . |
| 2 | In the Username box, type the test customer user name. |
| 3 | In the Password box, type the test customer password. |
| 4 | Click Log on . |
| 5 | Log on an agent who can handle an e-mail message skillset on to the Agent Desktop. Make the agent available to receive contacts. |
| 6 | Click Submit HTML Form to create an e-mail contact. |
| 7 | In the Mail To box, type the e-mail address that is forwarded to the agent who is logged on. |
| 8 | In the Subject box, type the subject of the e-mail message. |
| 9 | Click Submit . |
| | <i>On the Agent Desktop, your logged on agent receives the outbound contact.</i> |
| 10 | Close the test contact. |
| 11 | Click Logoff Customer to log off the test customer. |

--End--

Transferring your Web interface to the production server

Transfer your Web interface by assigning a name to the production server or corporate server to make the Web communication system live and available to the public in your corporate setting.

Prerequisites

- Develop your Web pages for your corporate Web site.
- Test your corporate Web interface. See [Testing request text chat \(page 145\)](#), [Testing request callback \(page 146\)](#), and [Testing e-mail \(page 147\)](#).
- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
1	Click Outbound and Multimedia .
2	In the left column, select General Administration .
3	Click Server Settings .
4	In the Server Settings dialog box, select External Web Server (HTTP) .
5	Click Edit .
6	In the Server Name box, type the name of the external Web server that customers can access for Web communications.
7	In the Port box, type the port number for the external Web server that customers can access for Web communications.

The changes are automatically saved after you leave the window.

--End--

High Availability Campus co-resident server commissioning

This section describes how to configure High Availability (HA) hot standby resiliency for a pair of co-resident Contact Center Manager Server (CCMS) and Communication Control Toolkit (CCT) servers in a campus environment.

High Availability Campus server commissioning overview

In a co-resident CCMS and CCT server configuration, one co-resident server is the active server and one is the standby server. The active CCMS and CCT 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 hot standby mode, recognizes the failure and starts processing contacts. The active and standby co-resident CCMS and CCT servers are part of the same Avaya Aura™ Contact Center and they must be in the same subnet IP address range for campus High Availability resiliency to work.

The standby server must be configured the same as the active server. The standby and active servers must have the same patch level and the same hard disk drive partitions. Configuration changes made to the active CCMS and CCT server during normal operation are automatically copied to the standby server so that the standby server can take over processing from the active server when necessary.

In a campus co-resident solution, a CCT service failure does not initiate an automatic switchover; CCT simply restarts. In a campus co-resident solution, only a CCMS service failure, hardware, network, or database failure can initiate a switchover but only in the following situations:

- The switchover check box on both servers is selected.
- The standby server is shadowing the active server.
- A valid licence file containing standby server licence information for CCMS and CCT exists to allow switchover.

Geographic Redundancy Nodes

The High Availability feature supports Geographic Redundancy nodes. Geographic Redundancy nodes are similar to the standby servers but they are used only to shadow data from the active server—they have no other responsibility. Geographic Redundancy nodes do not automatically take over if the active system fails. If the standby server and active server are in the same building, then a Geographic Redundancy node on a remote site provides additional data protection by maintaining a remote copy of the configuration and statistical information.

Managed IP Address

A Managed IP address is a virtual IP address that is attached to a network adaptor on the active server. Each High Availability application server is assigned a static IP address. After the active server in each replication pair is determined, the active server attaches a Managed IP address to the network interface. The managed IP address is only assigned to the active server and it is used by all other contact center applications and clients to connect to that application. The standby server assumes this same managed IP address if it takes over processing and becomes the active application. The active server stops using the Managed IP when it stops being the active server.

High Availability Utility

Configure High Availability resiliency for CCMS and CCT using the High Availability Utility in the Database Utilities. The High Availability Utility is used to configure which server is the active and which is the standby server. The HA utility also configures the Managed IP of the active server.

The High Availability Utility on an Active Server has the following dialogs under the Configuration tab:

- Server Mode
 - Configure the IP address for the Active and Standby servers
 - Configure the IP address for Trusted servers
 - Configure the IP address for Geographic Redundancy nodes
 - Identify if the server is Active or Standby
 - Enable Automatic Switchover
 - Configure the switchover time-out. This is the wait time if a network outage occurs before an automatic switchover occurs
- Notifications
 - 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
 - Display information on the system status
 - Verify that shadowing is running

The High Availability utility on an Active Server has the following dialogs under the Tasks tab:

- CC Applications
 - Start or stop the system
 - Enable or disable CC applications

- Enable or disable switchover on the CC applications
- Display system information
- CC Configuration
 - Monitor application service status
 - Define which application services are stopped or started
 - Configure how often a service restarts before switching over to the standby server
- System Control
 - Initiate a manual switchover for the Active Server
 - Initiate Standby Server shadowing

To commission CCMS, CCT and CCMA see the following sections in this document:

- Contact Center Manager Server commissioning, see [Contact Center Manager Server commissioning \(page 21\)](#)
- Contact Center Manager Administration commissioning, see [Contact Center Manager Administration commissioning \(page 37\)](#)
- Communication Control Toolkit commissioning, see [Communication Control Toolkit commissioning for Contact Center \(page 83\)](#)

Prerequisites

- The active and standby servers must meet the planning and engineering specifications. For more information, see *Avaya Aura™ Contact Center Planning and Engineering* (NN44400-210).
- CCMS is installed on the Active and Standby Servers using the same drive specification on each server. For more information, see *Avaya Aura™ Contact Center Installation* (NN44400-311).
- CCT is installed on the Active and Standby Servers using the same drive specification on each server. For more information, see *Avaya Aura™ Contact Center Installation* (NN44400-311).
- CCMA is installed on the Active and the Standby Servers. For more information, see *Avaya Aura™ Contact Center Installation* (NN44400-311).
- CCMA replication is configured. CCMA Replication is setup at install time. For more information, see *Avaya Aura™ Contact Center Installation* (NN44400-311).
- CCMS is configured on the Active Server. For more information, see [Contact Center Manager Server commissioning \(page 21\)](#).
- CCT is configured on the Active Server. For more information, see [Communication Control Toolkit commissioning for Contact Center \(page 83\)](#).

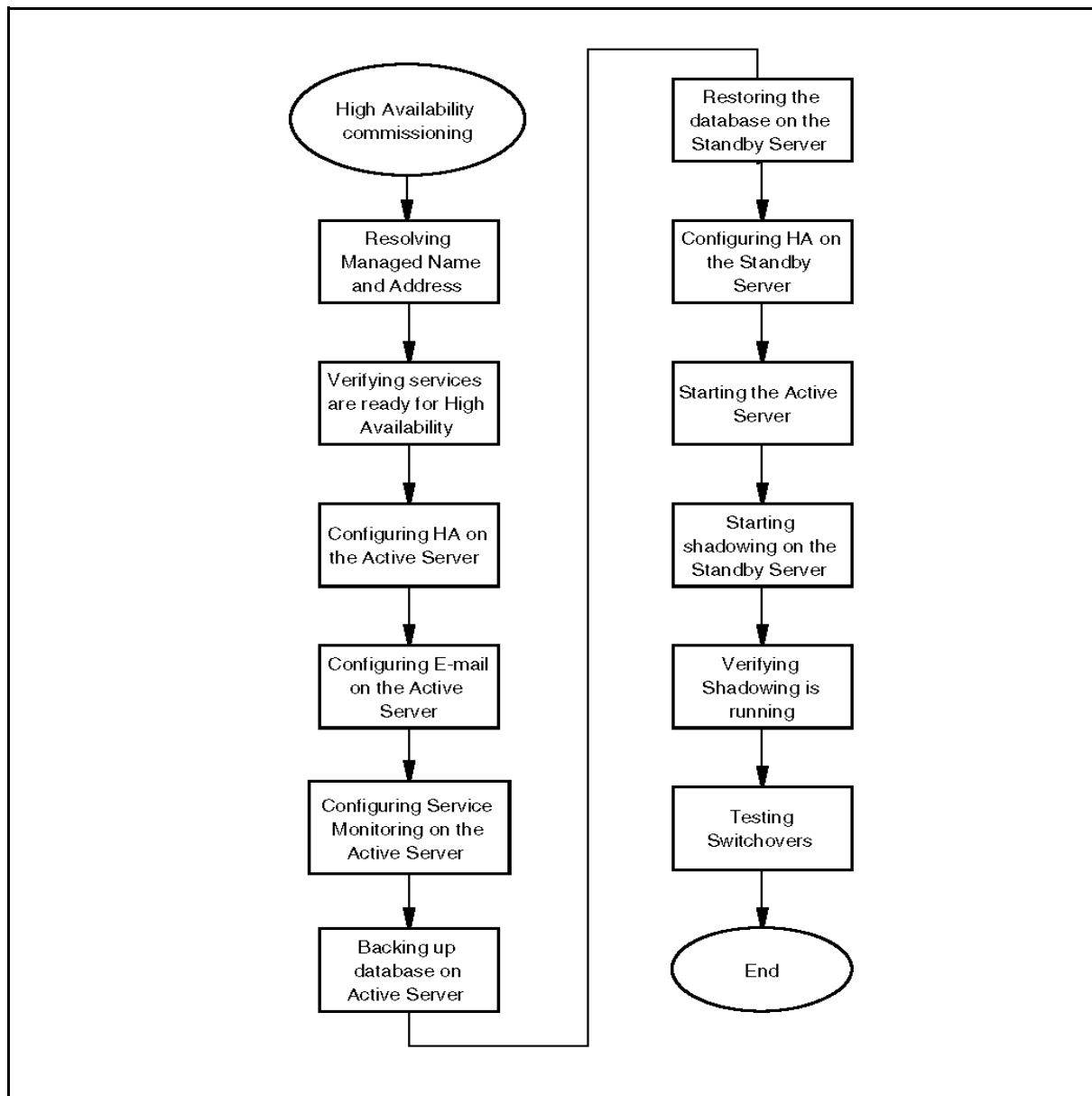
High Availability Campus co-resident server commissioning

- CCMA is configured on the Active Server. For more information, see [Contact Center Manager Administration commissioning \(page 37\)](#)
- Licence Manager is installed on the Active and the Standby Server. For more information, see *Avaya Aura™ Contact Center Installation* (NN44400-311).
- Have a valid standby server licence file on the Active and Standby Server.
- Ensure the Communication Control Toolkit server is on a domain. This is to allow the CCT clients automatically re-connect after a switchover.
- Before you commission High Availability, use System Control and Monitoring Utility (SCMU) to shut down all CCMS and CCT services on both the active and standby servers.

High Availability Campus server commissioning procedures

This task flow shows the sequence of procedures to commission High Availability Campus servers. To link to any task, go to [High Availability Campus server commissioning navigation \(page 153\)](#).

High Availability Campus server commissioning procedures



High Availability Campus server commissioning navigation

- [Resolving the Managed CLAN Name Server to the Managed CLAN IP Address \(page 154\)](#)
- [Verifying services are ready for High Availability \(page 155\)](#)
- [Configuring High Availability on the Active Server \(page 155\)](#)
- [Configuring E-mail notification on the Active Server \(page 157\)](#)
- [Configuring service monitoring on the Active Server \(page 158\)](#)

- [Backing up the database on the Active Server \(page 161\)](#)
- [Restoring the database on the Standby Server \(page 161\)](#)
- [Configuring High Availability on the Standby Server \(page 163\)](#)
- [Starting the Active Server \(page 164\)](#)
- [Starting shadowing on the Standby Server \(page 165\)](#)
- [Verifying shadowing is running on the Active Server \(page 166\)](#)
- [Testing switch overs \(page 168\)](#)

Resolving the Managed CLAN Name Server to the Managed CLAN IP Address

Complete the following procedure on the Active and Standby Servers to resolve the managed CLAN server name to the managed IP address using the Windows hosts file.

For information about saving the managed CLAN server name to the DNS server, contact your System Administrator.

Perform this procedure on the Active and Standby Servers.

Procedure steps

- | Step | Action |
|------|---|
| 1 | Open Windows Explorer. |
| 2 | Go to the folder C:\Windows\system32\drivers\etc. |
| 3 | Right-click on the hosts file, select Open , and select Notepad .
<i>The hosts file opens in Notepad.</i> |
| 4 | Add the CLAN managed IP address and the server name to the hosts file. |

Attention: The Managed Server name can be a full name or netbios server name.

--End--

Verifying services are ready for High Availability

Verify that all CCMS and CCT services stop before you configure High Availability. This ensures that all Avaya Communication Server 1000 resources are available to the Active Server when it starts.

Perform this procedure on the Active and Standby Servers.

Procedure steps

Step	Action
1	Log onto the Active Server.
2	Click Start, All Programs, Avaya, Contact Center, Common Utilities, System Control and Monitor Utility .
3	On the CCMS tab, check that all services are stopped.
4	If any service is running, click Stop CCMS .
5	On the CCT tab, check that all services are stopped.
6	If any service is running, click Stop CCT .
7	Close the System Control and Monitor Utility window.
8	Repeat this procedure on the Standby server.

--End--

Configuring High Availability on the Active Server

Configure High Availability resiliency on the Active Server using the High Availability Utility. The Active Server is the co-resident CCMS and CCT server that normally processes calls.

Procedure steps

Step	Action
1	Select one co-resident CCMS and CCT server to be the active server and log on.
2	Click Start, All Programs, Avaya, Contact Center, Database Utilities, High Availability .
3	Expand Configuration .
4	Double-click Server Mode .
5	Under Server Mode Configuration , select Active .
6	Under IP Configuration , type the Managed IP, CLAN and ELAN IP addresses.
7	Under IP Configuration , type the Active Server details, CLAN and ELAN IP addresses.

- 8 Under **IP Configuration** type the **Standby Server details**, **CLAN** and **ELAN** IP addresses.
- 9 In the **Address** box, type the IP address of the **Trusted IP** server.
- 10 In the **Address** box, type the IP address of the optional **Remote Geographic Node(s)**.
- 11 Click **OK**.
A system message box appears. You must stop the system before you save any information.
- 12 Click **Yes** to stop the system.

Attention: Enter the ELAN IP information only if the system has an Embedded LAN (ELAN) subnet configured.

--End--

Variable definitions

Variable	Value
Managed IP	The virtual Managed IP (MIP) address that is used by the Active Server for campus resiliency. The Active Server is always assigned the MIP. If a switchover occurs the MIP is assigned to the new Active Server. Agents and other applications are not aware that a switchover occurred because the IP address does not change. A MIP is used only when the Active and Standby Servers are in the same subnet.
Active Server details	The IP address for the server initially configured in Active mode.
Standby Server details	The IP address for the server initially configured in Standby mode.
Trusted Address	The IP address of a trusted server that is not likely to go down so that both Active and Standby servers have a server to ping regularly to verify the network connection. You must enter the trusted IP address. Avaya recommends that you use an IP address from your IT infrastructure as the Trusted Address.
Remote Geographic Node(s) Address	The IP address of the optional Remote Geographic Node(s).

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	Log on to the Active Server.
2	Click Start, All Programs, Avaya, Contact Center, Database Utilities, High Availability .
3	Expand Configuration .
4	Double-click Notification .
5	Select the Email check box.
6	Type the SMTP Server name.
7	Type the Username .
8	Type the Password .
9	Type the From Address .
10	Type the To Address or Addresses .
11	Click OK to save the data.

--End--

Variable definitions

Variable	Value
Email	Enables or disables e-mail notifications.
SMTP Server	The SMTP Server name, which is automatically verified when saving the data.
Username	E-mail User log on name.
Password	E-mail User log on password.
Charset	E-mail character set to use.
From Address	E-mail address to send notifications from.
To Address	E-mail address to send notifications to.

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 licence 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 when 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 | Log on to the Active Server. |
| 2 | Choose Start, All Programs, Avaya, Contact Center, Database Utilities, High Availability . |
| 3 | In the High Availability window, in the left pane, expand the Tasks folder. |
| 4 | Double-click CC Configuration . |
| 5 | For each service to monitor, select the Monitor check box. |
| 6 | For each service to restart, select the Restart check box. |

Attention: By default service monitoring is selected for CCT and is not selected for CCMS.

- | | |
|----|---|
| 7 | In the Start Wait Time column, type the number of seconds to wait before restarting a service. |
| 8 | For CCT only, in the Stop Wait Time column, type the number of seconds to wait before stopping a service. |
| 9 | In the Restart Limit column, type the maximum number of attempts to restart the service before switchover occurs. This Administrator decides the maximum number. |
| 10 | In the Restart Threshold column, type the time in seconds to reset the restart counter (for each service that is restarted) after the threshold is passed. |

--End--

Variable definitions

Variable	Value
CC	The Contact Center application name, CCMS or CCT in this case, because CCMS and CCT are co-resident.
Service	The application service name, for example OAM_Service.
Monitor	Used to enable or disable the service monitoring.
Restart	Restart the service if it stops.
Start Wait Timer	The time in seconds that service monitor waits before attempting to restart or initiating a switch over to the standby server if this service is not running.
Stop Wait Time	The waiting time (in seconds) for the next restart decision. For example, if service monitor stopped this service, service monitor checks the status if the status is not SERVICE_STOPPED, it waits for Stop Wait Time before attempting to start the service.
Restart Limit	The number of times a service can be restarted by the service monitor before initiating a switchover.
Restart Threshold	The time elapsed since the last restart of a call processing service by the Service Monitor. It is the time value in seconds to reset the Restart Counter to the value zero by the Service monitor.

Procedure job aid

This section provides an example of the service monitor configuration in the High Availability Utility.

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 database on the Active Server

The Active Server is configured for High Availability. Now the Standby Server must be prepared for High Availability resiliency. Back up the Active Server to create a snapshot of the database which is then restored to the Standby Server. On the active co-resident server all databases must be backed-up.

Procedure steps

- | Step | Action |
|------|---|
| 1 | Log on to the Active Server. |
| 2 | Click Start, All Programs, Avaya, Contact Center, Database Utilities, Database Maintenance . |
| 3 | Click Backup Locations . |
| 4 | Click Create . |
| 5 | From the Driver Letter list, select the network drive on which you want to store the Contact Center Manager Server, CCT and ADMIN databases. |
| 6 | In the UNC Path box, type the location to store the backup, in the format \\Computer Name\Backup Location. This location must be a shared folder with correct permissions. |
| 7 | In the User Name box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name. |
| 8 | In the Password box, type the Windows password. |
| 9 | Click OK . |
| 10 | In the left pane, click Immediate Backup . |
| 11 | In the Media Type section, select Network Disk . |
| 12 | In the Applications section, select CCMS, CCT and ADMIN . |
| 13 | From the Backup Location list, select the network drive on which to store the backup. |
| 14 | Click Backup . |

--End--

Restoring the database on the Standby Server

Restore the database from the Active Server to the Standby Server to ensure the databases are consistent. The Database Maintenance utility can restore only one application database at a time. Restore the data for the CCMS, CCT, and ADMIN databases

You must restore the CCMS, CCT, and ADMIN database onto the Standby Server. You must restore the ADMIN database last.

Prerequisites

- Know the location of the backup database.
- Ensure no traffic is running on the Standby Server.
- Stop shadowing if shadowing is running on the Standby Server.
- Stop all Contact Center services using the SCMU utility, if services are running.
- Ensure the patch level on the Standby Server is the same as the Active Server.

Attention: Not all CCT data is stored in the database; therefore the following data must be configured on the Standby Server, the CCT Communication Server 1000 service provider, CCT Licence, CCT Contact Management Framework, CCT SOA configuration and CCT logging location. For information about CCT commissioning, see [Communication Control Toolkit commissioning for Contact Center \(page 83\)](#).

Attention: You must restore all databases in a co-resident server. Restoring only CCMS and not CCT or ADMIN may leave an inconsistent server and HA cannot shadow data correctly.

Attention: Restoring the 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.

Attention: The Server Configuration Tool must be run after a database restore has been performed and the data should be checked that it is correct.

Procedure steps

Step	Action
1	Log on to the Standby Server.
2	Click 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 on which the backup is restored.
5	If the backup file is on the network drive, in the Backup Location list, select the backup location.
6	Under Application , select the database to restore, either CCMS, CCT or ADMIN.
7	Under Restore contents , select Data.
8	Click Restore .
9	Use the Progress information field to monitor the progress of the restoration.
10	Repeat steps 6 to 8 to restore all databases.

- 11 Click **Exit** to close the Database Maintenance utility.

--End--

Variable definitions

Variable	Value
Application	The database and applications of Contact Center that you can back up.
Backup Location	The destination of the network disk. The values are configured in the Backup Locations.
Restore contents	The type of content that is stored in the database. Data is in the database. Schema is the data for the database structure, tables and procedures.
Media type	The type of media used for your backup file. You can use a network disk location or a tape drive. If you use a network disk location, you must configure a destination before you can back up the file.

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.

Prerequisites

- The Active Server databases are restored on to the Standby Server.

Procedure steps

Step	Action
1	Log on to the Standby Server.
2	Click Start, All Programs, Avaya, Contact Center, Database Utilities, High Availability .
3	In the left pane of the High Availability dialog box, click Server Mode .
4	In the Server Mode Configuration field, select Standby .
5	Under IP Configuration , type the Managed IP, CLAN and ELAN IP addresses.
6	Under IP Configuration , type the Active Server details, CLAN and ELAN IP addresses.
7	Under IP Configuration , type the Standby Server details, CLAN and ELAN IP addresses.

- 8 Click **OK**.

A system message box appears. You must stop the system before you save any information.

- 9 Click **OK**.

--End--

Variable definitions

Variable	Value
Managed IP	The virtual Managed IP (MIP) address that is used for both the Active and Standby Servers for campus resiliency. The Active Server is always assigned the MIP. If a switchover occurs the MIP is assigned to the new Active Server. Agents and other applications are not aware that a switchover occurred because the IP address does not change. A MIP is used only when the Active and Standby Servers are in the same subnet.
Active Server details	The IP address for the server initially configured in Active mode.
Standby Server details	The IP address for the server initially configured in Standby mode.
Trusted IP Address	The IP address of a trusted server that is not likely to go down so that both Active and Standby servers have a server to ping regularly to verify the network connection. It is mandatory to enter the trusted IP address.

Starting the Active Server

Start the Active Server using the High Availability utility. Starting the Active Server starts CCMS, CCT, and system processes.

Procedure steps

- | Step | Action |
|------|--|
| 1 | Log on to the Active Server. |
| 2 | Click Start, All Programs, Avaya, Contact Center, Database Utilities, High Availability . |
| 3 | Expand Tasks . |
| 4 | Double-click CC Applications . |
| 5 | In the first box under CC Applications , select the system. |

- 6 Click **Start**.
A delay occurs before all Contact Center services start.
- 7 Click **OK**.
- 8 To verify that the Contact Center services are running using the SCMU, select **Avaya, Contact Center, Common Utilities, System Control and Monitor Utility**. Check the CCMS and CCT services are running.

--End--

Procedure job aid

After the system starts, check that the Managed IP (MIP) address is assigned to the network adaptor of the Active Server by opening a command window and entering:

IPCONFIG /all

The IP and the MIP of the Active Server should appear.

Starting shadowing on the Standby Server

Start shadowing on the Standby Server using the High Availability utility. The Standby co-resident CCMS and CCT server must be shadowing the Active CCMS and CCT server for switchover to occur if the Active Server fails. While the Standby server is shadowing the Active server, it maintains a near real-time local copy of the CCMS, CCT, and Administration databases. Therefore, the Standby Server is configured with the most recent data and it can take over from the Active Server if necessary.

Prerequisites

Attention: Enabling the shadowing functionality is available only on the system control dialog box of the High Availability utility on the Standby Server.

Attention: It is advisable on the Standby Server not to stop and start shadowing but to use the pause and resume functionality.

Procedure steps

- | Step | Action |
|------|--|
| 1 | Log on to the Standby Server. |
| 2 | Click Start, All Programs, Avaya, Contact Center, Database Utilities, High Availability . |
| 3 | Expand Tasks . |
| 4 | Double-click System Control . |
| 5 | In the Control box, select Shadowing . |

High Availability Campus co-resident server commissioning

- 6 Click **Start**.
- 7 Click **OK**.
- 8 To verify that the CCMS services are stopped using the SCMU, select **Avaya, Contact Center, Common Utilities, System Control and Monitor Utility**. Check the CCMS services are stopped.
- 9 To verify that the CCT services are running using the SCMU, select **Avaya, Contact Center, Common Utilities, System Control and Monitor Utility**. Check the CCT services are running.

--End--

Procedure job aid

Example of starting shadowing on the standby server.

Starting shadowing on the Standby Server.



Verifying shadowing is running on the Active Server

Verify that the Standby co-resident CCMS and CCT server is shadowing the Active server using the High Availability Utility. The System dialog box of the High Availability utility displays system information about the Active and the Standby Servers.

The dialog box displays the followings information categories:

- Computer name and operating system version
- Server mode
- Server configuration type
- Port information
- Remote server connection status
- Remote server port information
- Licence 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 Active Server.
2	Click Start, All Programs, Avaya, Contact Center, Database Utilities, High Availability .
3	In the left pane, expand Configuration .
4	Select System .
5	Select Get System Configuration .

The most recent system information appears.

--End--

Procedure job aid

To verify that the Standby Server is shadowing the Active Server, examine the Shadowing section of the System Configuration log.

For example, look for the following text:

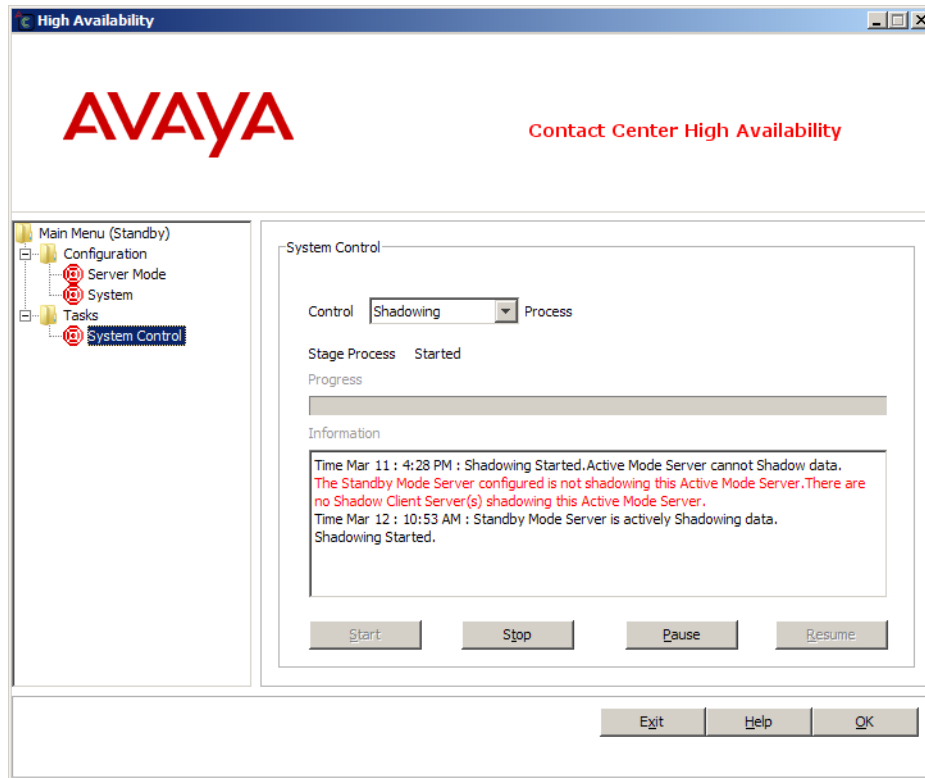
- Shadowing :
- Number of clients connected : 1
- List of Shadow Clients connected :
- **AA.BB.CC.DD** [port Number] Latency : 0 second Shadowing Rate :

High Availability Campus co-resident server commissioning

- Last record of Shadowing was @ date and times shadowing started.

Where **AA.BB.CC.DD** is the IP address of the Standby Server.

High Availability Standby Server shadowing an active server



Testing switch overs

Test the High Availability feature and infrastructure by making a manual switchover from the Active server to the Standby server.

Prerequisites

- Configure High Availability on the Active and Standby Servers.

Procedure steps

- | Step | Action |
|------|---|
| 1 | Log on to the current Active Server. |
| 2 | Click Start, All Programs, Avaya, Contact Center, Database Utilities, High Availability. |
| 3 | In the left pane of the High Availability window, expand Tasks . |

- 4 Under **Tasks**, double-click **System Control**.
- 5 In the **Control** box, select **Switchover**.
- 6 Select the **System** tab.
- 7 Select **Switchover**.
- 8 Click **Start**.

--End--

Procedure job aid

When the Standby Server becomes the new Active Server, test the Standby Server configuration by making a call using the CCT Ref Client. For more details, see [Verifying CCT using the Reference Client \(page 101\)](#).

High Availability Geographic co-resident server commissioning

This section describes how to configure High Availability (HA) resiliency for a pair of co-resident Contact Center Manager Server (CCMS) and Communication Control Toolkit (CCT) servers in a geographic (Wide Area Network) environment.

High Availability Geographic server commissioning overview

In a co-resident CCMS and CCT server configuration, one server is the active server and one is the standby server. The active CCMS and CCT 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 recognizes the failure and starts processing contacts.

The active and standby co-resident CCMS and CCT servers are part of the same Avaya Aura™ Contact Center and they are typically in different geographic locations and subnets.

The standby server must be configured the same as the active server. The standby and active servers must have the same patch level and the same hard disk drive partitions. Configuration changes made to the active CCMS and CCT server during normal operation are automatically copied to the standby server so that the standby server can take over processing from the active server when necessary.

In a geographic solution a service failure or application initiates an automatic switchover, to the other geographic location, in the following situations:

- The switchover check box on both servers is selected.
- The standby server is shadowing the active server.
- A valid licence file containing standby server licence information for CCMS and CCT exists to allow switchover.

High Availability Utility

Configure High Availability resiliency for CCMS and CCT using the High Availability Utility in the Database Utilities. The High Availability Utility is used to configure which server is the active and which is the standby server.

The High Availability Utility on an Active Server has the following dialogs under the Configuration tab:

- Server Mode
 - Configure the IP address for the Active and Standby servers
 - Configure the IP address for Trusted servers

- Configure the IP address for Geographic Redundancy nodes
- Identify if the server is Active or Standby
- Enable Automatic Switchover
- Configure the switchover time-out. This is the wait time if a network outage occurs before an automatic switchover occurs
- Notifications
 - 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
 - Display information on the system status
 - Verify that shadowing is running

The High Availability utility on an Active Server has the following dialogs under the Tasks tab:

- CC Applications
 - Start or stop the system
 - Enable or disable CC applications
 - Enable or disable switchover on the CC applications
 - Display system information
- CC Configuration
 - Monitor application service status
 - Define which application services are stopped or started
 - Configure how often a service restarts before switching over to the standby server
- System Control
 - Initiate a manual switchover for the Active Server
 - Initiate Standby Server shadowing

To commission CCMS, CCT and CCMA see the following sections in this document:

- Contact Center Manager Server commissioning, see [Contact Center Manager Server commissioning \(page 21\)](#)
- Contact Center Manager Administration commissioning, see [Contact Center Manager Administration commissioning \(page 37\)](#)

- Communication Control Toolkit commissioning, see [Communication Control Toolkit commissioning for Contact Center \(page 83\)](#)

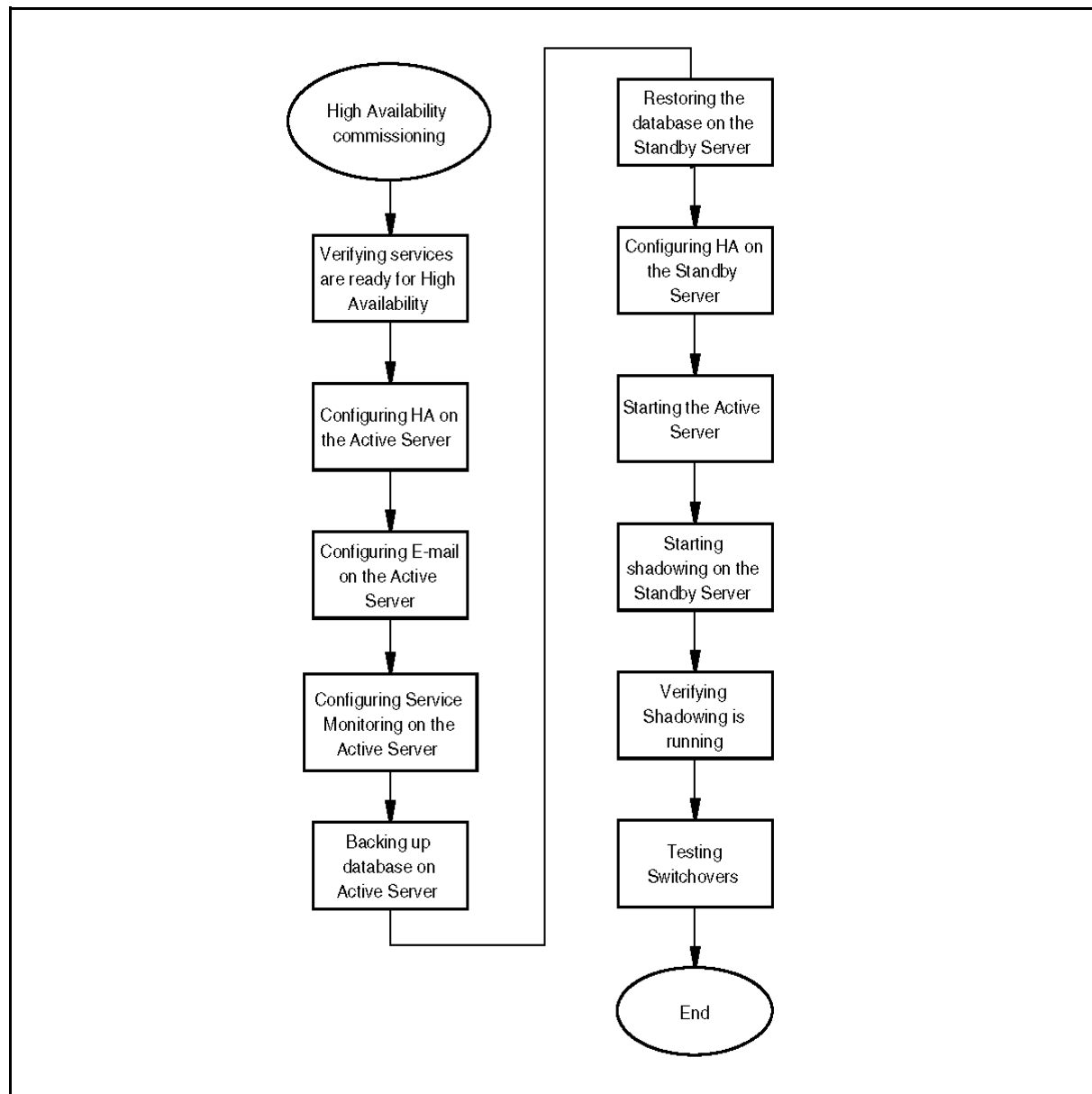
Prerequisites

- The active and standby servers must meet the planning and engineering specifications. For more information, see *Avaya Aura™ Contact Center Planning and Engineering* (NN44400-210).
- CCMS is installed on the Active and Standby Servers using the same drive specification on each server. For more information, see *Avaya Aura™ Contact Center Installation* (NN44400-311).
- CCT is installed on the Active and Standby Servers using the same drive specification on each server. For more information, see *Avaya Aura™ Contact Center Installation* (NN44400-311).
- CCMA is installed on the Active and the Standby Servers. For more information, see *Avaya Aura™ Contact Center Installation* (NN44400-311).
- CCMA replication is configured. CCMA Replication is setup at install time. For more information, see *Avaya Aura™ Contact Center Installation* (NN44400-311).
- CCMS is configured on the Active Server. For more information, see [Contact Center Manager Server commissioning \(page 21\)](#).
- CCT is configured on the Active Server. For more information, see [Communication Control Toolkit commissioning for Contact Center \(page 83\)](#).
- CCMA is configured on the Active Server. For more information, see [Contact Center Manager Administration commissioning \(page 37\)](#)
- Licence Manager is installed on the Active and the Standby Server. For more information, see *Avaya Aura™ Contact Center Installation* (NN44400-311).
- Have a valid standby server licence file on the Active and Standby Server.
- Ensure the Communication Control Toolkit server is on a domain. This is to allow the CCT clients automatically re-connect after a switchover.
- Before you commission High Availability, use System Control and Monitoring Utility (SCMU) to shut down all CCMS and CCT services on both the active and standby servers.

High Availability Geographic server commissioning procedures

This task flow shows the sequence of procedures to commission High Availability Geographic servers. To link to any task, go to [High Availability Geographic server commissioning navigation \(page 174\)](#).

High Availability Geographic server commissioning procedures



High Availability Geographic server commissioning navigation

- [Verifying services are ready for High Availability \(page 175\)](#)
- [Configuring High Availability on the Active Server \(page 175\)](#)
- [Configuring E-mail notification on the Active Server \(page 177\)](#)
- [Configuring service monitoring on the Active Server \(page 178\)](#)
- [Backing up the database on the Active Server \(page 181\)](#)
- [Restoring the database on the Standby Server \(page 181\)](#)

- [Configuring High Availability on the Standby Server \(page 183\)](#)
- [Starting the Active Server \(page 184\)](#)
- [Starting shadowing on the Standby Server \(page 185\)](#)
- [Verifying shadowing is running on the Active Server \(page 186\)](#)
- [Testing switch overs \(page 188\)](#)

Verifying services are ready for High Availability

Verify that all CCMS and CCT services stop before you configure High Availability. This ensures that all Avaya Communication Server 1000 resources are available to the Active Server when it starts.

Perform this procedure on the Active and Standby Servers.

Procedure steps

Step	Action
1	Log onto the Active Server.
2	Click Start, All Programs, Avaya, Contact Center, Common Utilities, System Control and Monitor Utility .
3	On the CCMS tab, check that all services are stopped.
4	If any service is running, click Stop CCMS .
5	On the CCT tab, check that all services are stopped.
6	If any service is running, click Stop CCT .
7	Close the System Control and Monitor Utility window.
8	Repeat this procedure on the Standby server.

--End--

Configuring High Availability on the Active Server

Configure High Availability resiliency on the Active Server using the High Availability Utility. The Active Server is the co-resident CCMS and CCT server that normally processes calls.

Procedure steps

Step	Action
------	--------

High Availability Geographic co-resident server commissioning

- 1 Select one co-resident CCMS and CCT server to be the active server and log on.
- 2 Click **Start, All Programs, Avaya, Contact Center, Database Utilities, High Availability**.
- 3 Expand **Configuration**.
- 4 Double-click **Server Mode**.
- 5 Under **Server Mode Configuration**, select **Active**.
- 6 Under **IP Configuration**, type the **CLAN** and **ELAN** IP addresses.
- 7 Under **IP Configuration**, type the **Active Server details, CLAN** and **ELAN** IP addresses.
- 8 Under **IP Configuration** type the **Standby Server details, CLAN** and **ELAN** IP addresses.
- 9 In the **Address** box, type the IP address of the **Trusted IP** server.
- 10 In the **Address** box, type the IP address of the optional **Remote Geographic Node(s)**.
- 11 Click **OK**.
A system message box appears. You must stop the system before you save any information.
- 12 Click **Yes** to stop the system.

Attention: Enter the ELAN IP information only if the system has an Embedded LAN (ELAN) subnet configured.

--End--

Variable definitions

Variable	Value
Active Server details	The IP address for the server initially configured in Active mode.
Standby Server details	The IP address for the server initially configured in Standby mode.
Trusted Address	The IP address of a trusted server that is not likely to go down so that both Active and Standby servers have a server to ping regularly to verify the network connection. You must enter the trusted IP address. Avaya recommends that you use an IP address from your IT infrastructure as the Trusted Address.
Remote Geographic Node(s) Address	The IP address of the optional Remote Geographic Node(s).

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	Log on to the Active Server.
2	Click Start, All Programs, Avaya, Contact Center, Database Utilities, High Availability .
3	Expand Configuration .
4	Double-click Notification .
5	Select the Email check box.
6	Type the SMTP Server name.
7	Type the Username .
8	Type the Password .
9	Type the From Address .
10	Type the To Address or Addresses .
11	Click OK to save the data.

--End--

Variable definitions

Variable	Value
Email	Enables or disables e-mail notifications.
SMTP Server	The SMTP Server name, which is automatically verified when saving the data.
Username	E-mail User log on name.
Password	E-mail User log on password.
Charset	E-mail character set to use.
From Address	E-mail address to send notifications from.
To Address	E-mail address to send notifications to.

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 licence 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 when 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 | Log on to the Active Server. |
| 2 | Choose Start, All Programs, Avaya, Contact Center, Database Utilities, High Availability . |
| 3 | In the High Availability window, in the left pane, expand the Tasks folder. |
| 4 | Double-click CC Configuration . |
| 5 | For each service to monitor, select the Monitor check box. |
| 6 | For each service to restart, select the Restart check box. |

Attention: By default service monitoring is selected for CCT and is not selected for CCMS.

- | | |
|----|---|
| 7 | In the Start Wait Time column, type the number of seconds to wait before restarting a service. |
| 8 | For CCT only, in the Stop Wait Time column, type the number of seconds to wait before stopping a service. |
| 9 | In the Restart Limit column, type the maximum number of attempts to restart the service before switchover occurs. This Administrator decides the maximum number. |
| 10 | In the Restart Threshold column, type the time in seconds to reset the restart counter (for each service that is restarted) after the threshold is passed. |

--End--

Variable definitions

Variable	Value
CC	The Contact Center application name, CCMS or CCT in this case, because CCMS and CCT are co-resident.
Service	The application service name, for example OAM_Service.
Monitor	Used to enable or disable the service monitoring.
Restart	Restart the service if it stops.
Start Wait Timer	The time in seconds that service monitor waits before attempting to restart or initiating a switch over to the standby server if this service is not running.
Stop Wait Time	The waiting time (in seconds) for the next restart decision. For example, if service monitor stopped this service, service monitor checks the status if the status is not SERVICE_STOPPED, it waits for Stop Wait Time before attempting to start the service.
Restart Limit	The number of times a service can be restarted by the service monitor before initiating a switchover.
Restart Threshold	The time elapsed since the last restart of a call processing service by the Service Monitor. It is the time value in seconds to reset the Restart Counter to the value zero by the Service monitor.

Procedure job aid

This section provides an example of the service monitor configuration in the High Availability Utility.

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 database on the Active Server

The Active Server is configured for High Availability. Now the Standby Server must be prepared for High Availability resiliency. Back up the Active Server to create a snapshot of the database which is then restored to the Standby Server. On the active co-resident server all databases must be backed-up.

Procedure steps

- | Step | Action |
|------|---|
| 1 | Log on to the Active Server. |
| 2 | Click Start, All Programs, Avaya, Contact Center, Database Utilities, Database Maintenance . |
| 3 | Click Backup Locations . |
| 4 | Click Create . |
| 5 | From the Driver Letter list, select the network drive on which you want to store the Contact Center Manager Server, CCT and ADMIN databases. |
| 6 | In the UNC Path box, type the location to store the backup, in the format \\Computer Name\Backup Location. This location must be a shared folder with correct permissions. |
| 7 | In the User Name box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name. |
| 8 | In the Password box, type the Windows password. |
| 9 | Click OK . |
| 10 | In the left pane, click Immediate Backup . |
| 11 | In the Media Type section, select Network Disk . |
| 12 | In the Applications section, select CCMS, CCT and ADMIN . |
| 13 | From the Backup Location list, select the network drive on which to store the backup. |
| 14 | Click Backup . |

--End--

Restoring the database on the Standby Server

Restore the database from the Active Server to the Standby Server to ensure the databases are consistent. The Database Maintenance utility can restore only one application database at a time. Restore the data for the CCMS, CCT, and ADMIN databases

You must restore the CCMS, CCT, and ADMIN database onto the Standby Server. You must restore the ADMIN database last.

Prerequisites

- Know the location of the backup database.
- Ensure no traffic is running on the Standby Server.
- Stop shadowing if shadowing is running on the Standby Server.
- Stop all Contact Center services using the SCMU utility, if services are running.
- Ensure the patch level on the Standby Server is the same as the Active Server.

Attention: Not all CCT data is stored in the database; therefore the following data must be configured on the Standby Server, the CCT Communication Server 1000 service provider, CCT Licence, CCT Contact Management Framework, CCT SOA configuration and CCT logging location. For information about CCT commissioning, see [Communication Control Toolkit commissioning for Contact Center \(page 83\)](#).

Attention: You must restore all databases in a co-resident server. Restoring only CCMS and not CCT or ADMIN may leave an inconsistent server and HA cannot shadow data correctly.

Attention: Restoring the 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.

Attention: The Server Configuration Tool must be run after a database restore has been performed and the data should be checked that it is correct.

Procedure steps

Step	Action
1	Log on to the Standby Server.
2	Click 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 on which the backup is restored.
5	If the backup file is on the network drive, in the Backup Location list, select the backup location.
6	Under Application , select the database to restore, either CCMS, CCT or ADMIN.
7	Under Restore contents , select Data.
8	Click Restore .
9	Use the Progress information field to monitor the progress of the restoration.
10	Repeat steps 6 to 8 to restore all databases.

- 11 Click **Exit** to close the Database Maintenance utility.

--End--

Variable definitions

Variable	Value
Application	The database and applications of Contact Center that you can back up.
Backup Location	The destination of the network disk. The values are configured in the Backup Locations.
Restore contents	The type of content that is stored in the database. Data is in the database. Schema is the data for the database structure, tables and procedures.
Media type	The type of media used for your backup file. You can use a network disk location or a tape drive. If you use a network disk location, you must configure a destination before you can back up the file.

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.

Prerequisites

- The Active Server databases are restored on to the Standby Server.

Procedure steps

Step	Action
1	Log on to the Standby Server.
2	Click Start, All Programs, Avaya, Contact Center, Database Utilities, High Availability .
3	In the left pane of the High Availability dialog box, click Server Mode .
4	In the Server Mode Configuration field, select Standby .
5	Under IP Configuration , type the CLAN and ELAN IP addresses.
6	Under IP Configuration , type the Active Server details, CLAN and ELAN IP addresses.
7	Under IP Configuration , type the Standby Server details, CLAN and ELAN IP addresses.

- 8 Click **OK**.

A system message box appears. You must stop the system before you save any information.

- 9 Click **OK**.

--End--

Variable definitions

Variable	Value
Active Server details	The IP address for the server initially configured in Active mode.
Standby Server details	The IP address for the server initially configured in Standby mode.
Trusted IP Address	The IP address of a trusted server that is not likely to go down so that both Active and Standby servers have a server to ping regularly to verify the network connection. It is mandatory to enter the trusted IP address.

Starting the Active Server

Start the Active Server using the High Availability utility. Starting the Active Server starts CCMS, CCT, and system processes.

Procedure steps

- | Step | Action |
|------|---|
| 1 | Log on to the Active Server. |
| 2 | Click Start, All Programs, Avaya, Contact Center, Database Utilities, High Availability . |
| 3 | Expand Tasks . |
| 4 | Double-click CC Applications . |
| 5 | In the first box under CC Applications , select the system. |
| 6 | Click Start . |
| | <i>A delay occurs before all Contact Center services start.</i> |
| 7 | Click OK . |
| 8 | To verify that the Contact Center services are running using the SCMU, select Avaya, Contact Center, Common Utilities, System Control and Monitor Utility . Check the CCMS and CCT services are running. |

--End--

Starting shadowing on the Standby Server

Start shadowing on the Standby Server using the High Availability utility. The Standby co-resident CCMS and CCT server must be shadowing the Active CCMS and CCT server for switchover to occur if the Active Server fails. While the Standby server is shadowing the Active server, it maintains a near real-time local copy of the CCMS, CCT, and Administration databases. Therefore, the Standby Server is configured with the most recent data and it can take over from the Active Server if necessary.

Prerequisites

Attention: Enabling the shadowing functionality is available only on the system control dialog box of the High Availability utility on the Standby Server.

Attention: It is advisable on the Standby Server not to stop and start shadowing but to use the pause and resume functionality.

Procedure steps

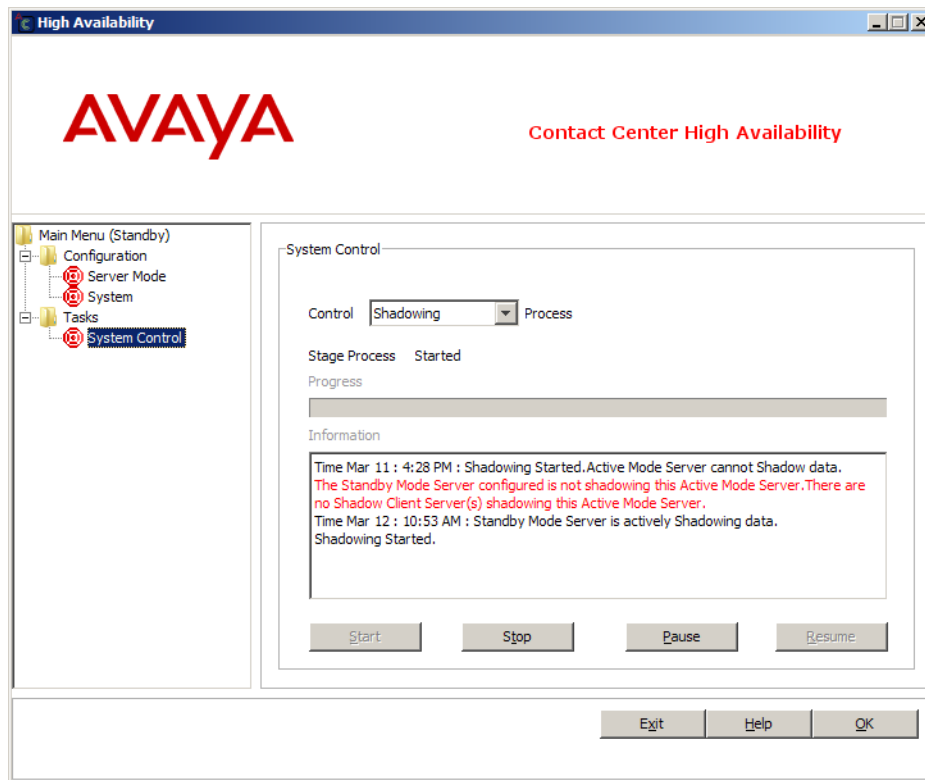
- | Step | Action |
|------|---|
| 1 | Log on to the Standby Server. |
| 2 | Click Start, All Programs, Avaya, Contact Center, Database Utilities, High Availability . |
| 3 | Expand Tasks . |
| 4 | Double-click System Control . |
| 5 | In the Control box, select Shadowing . |
| 6 | Click Start . |
| 7 | Click OK . |
| 8 | To verify that the CCMS services are stopped using the SCMU, select Avaya, Contact Center, Common Utilities, System Control and Monitor Utility . Check the CCMS services are stopped. |
| 9 | To verify that the CCT services are running using the SCMU, select Avaya, Contact Center, Common Utilities, System Control and Monitor Utility . Check the CCT services are running. |

--End--

Procedure job aid

Example of starting shadowing on the standby server.

Starting shadowing on the Standby Server.



Verifying shadowing is running on the Active Server

Verify that the Standby co-resident CCMS and CCT server is shadowing the Active server using the High Availability Utility. The System dialog box of the High Availability utility displays system information about the Active and the Standby Servers.

The dialog box displays the followings information categories:

- Computer name and operating system version
- Server mode
- Server configuration type
- Port information
- Remote server connection status
- Remote server port information
- Licence 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 Active Server. |
| 2 | Click Start, All Programs, Avaya, Contact Center, Database Utilities, High Availability . |
| 3 | In the left pane, expand Configuration . |
| 4 | Select System . |
| 5 | Select Get System Configuration . |
- The most recent system information appears.*

--End--

Procedure job aid

To verify that the Standby Server is shadowing the Active Server, examine the Shadowing section of the System Configuration log.

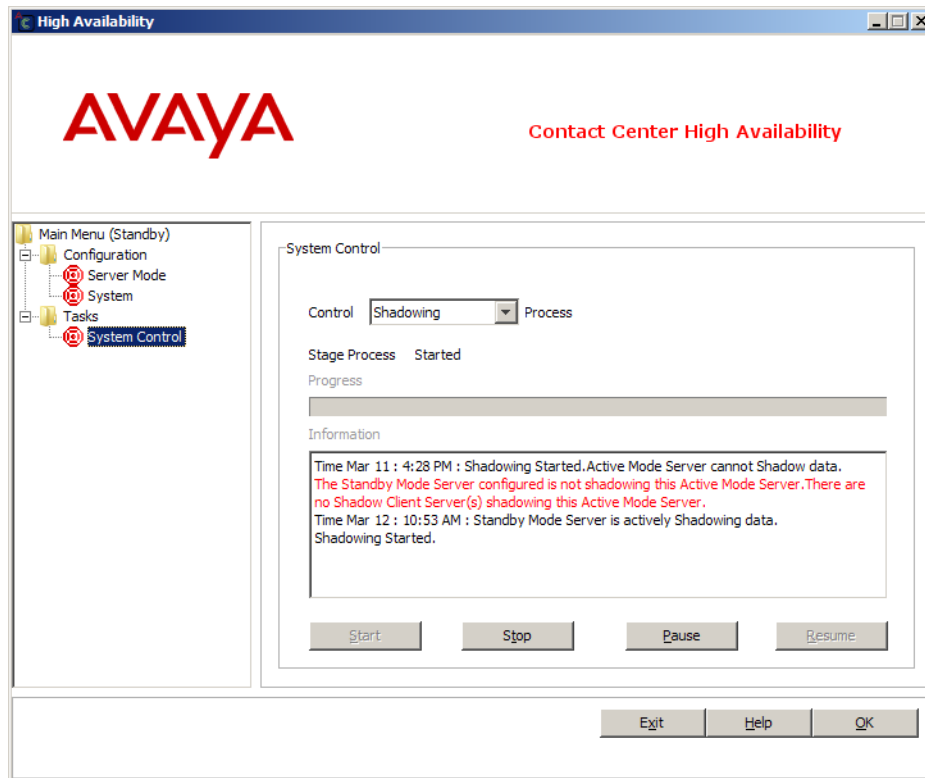
For example, look for the following text:

- Shadowing :
- Number of clients connected : 1
- List of Shadow Clients connected :
- **AA.BB.CC.DD** [port Number] Latency : 0 second Shadowing Rate :
- Last record of Shadowing was @ date and times shadowing started.

Where **AA.BB.CC.DD** is the IP address of the Standby Server.

High Availability Geographic co-resident server commissioning

High Availability Standby Server shadowing an active server



Testing switch overs

Test the High Availability feature and infrastructure by making a manual switchover from the Active server to the Standby server.

Prerequisites

- Configure High Availability on the Active and Standby Servers.

Procedure steps

- | Step | Action |
|------|--|
| 1 | Log on to the current Active Server. |
| 2 | Click Start, All Programs, Avaya, Contact Center, Database Utilities, High Availability . |
| 3 | In the left pane of the High Availability window, expand Tasks . |
| 4 | Under Tasks , double-click System Control . |
| 5 | In the Control box, select Switchover . |

- 6 Select the **System** tab.
- 7 Select **Switchover**.
- 8 Click **Start**.

--End--

Procedure job aid

When the Standby Server becomes the new Active Server, test the Standby Server configuration by making a call using the CCT Ref Client. For more details, see [Verifying CCT using the Reference Client \(page 101\)](#).

High Availability Campus CCMM commissioning

This section describes how to configure High Availability (HA) hot standby resiliency on a pair of Contact Center Multimedia (CCMM) servers in a campus environment.

High Availability CCMM commissioning overview

In a High Availability Campus server configuration, one CCMM server is the active server and one is the standby server. The active CCMM server actively processes contacts. 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 CCMM server fails, the standby CCMM server, running in hot standby mode, recognizes the failure and starts processing contacts. The active and standby CCMM servers are part of the same contact center and they must be in the same subnet IP address range for campus High Availability resiliency to work.

You must configure the standby CCMM server the same as the active server. The standby and active servers must have the same patch level and the same hard disk drive partitions. Configuration changes made to the active CCMM server during normal operation are automatically copied to the standby server so that the standby server can take over processing from the active server when necessary.

In a campus solution, a CCMM hardware, network, or database failure can initiate a switchover but only if:

- The switchover check box on both CCMM servers is selected
- The standby CCMM server is shadowing the active server
- A valid licence file containing standby server licence information for CCMM exists to allow switchover

Managed IP Address

A Managed IP (MIP) address is a virtual IP address that is attached to a network adaptor on the active server. Each Avaya Aura™ Contact Center application server is assigned a static IP address. After the active server in each replication pair is determined, the active server attaches a Managed IP address to its network interface. The managed IP address is assigned only to the active server and it is used by all other Contact Center applications and clients to connect to that application. The standby server assumes this same managed IP address only if it takes over processing and becomes the active application. The active server stops using the Managed IP when it stops being the active server.

High Availability Utility

High Availability resiliency for Contact Center Multimedia is configured using the High Availability Utility in the Database Utilities. Use the High Availability Utility to configure which server is the active and which is the standby server. The HA utility also configures the Managed IP of the active server.

The High Availability Utility on an Active Server has the following information configured on the Configuration tab:

- Server Mode
 - Configure the IP address for the Active and Standby servers
 - Configure the IP address for Trusted servers
 - Configure the IP address for Geographic Redundancy node
 - Identify the Active or Standby server
 - Enable Automatic Switchover
 - Configure the switchover time-out: the wait time if a network outage occurs before an automatic switchover occurs
- Notifications
 - Configure an e-mail server to allow for e-mail notifications
 - Configure where and how often to send e-mail notifications
 - Configure the e-mail character set
- System
 - Display information on the system status
 - Verify that shadowing is running

The High Availability utility on an Active Server has the following dialogs under the Tasks tab:

- CC Applications
 - Start or stop the system
 - Enable or disable CC applications
 - Enable or disable switchover on the CC applications
 - Display system information
- CC Configuration
 - Monitor application service status
 - Define which application services to be stopped or started
 - Configure how often a service to be restarted before switching over to the standby server

- System Control
 - Initiate a manual switchover for the Active Server
 - Initiate Standby Server shadowing

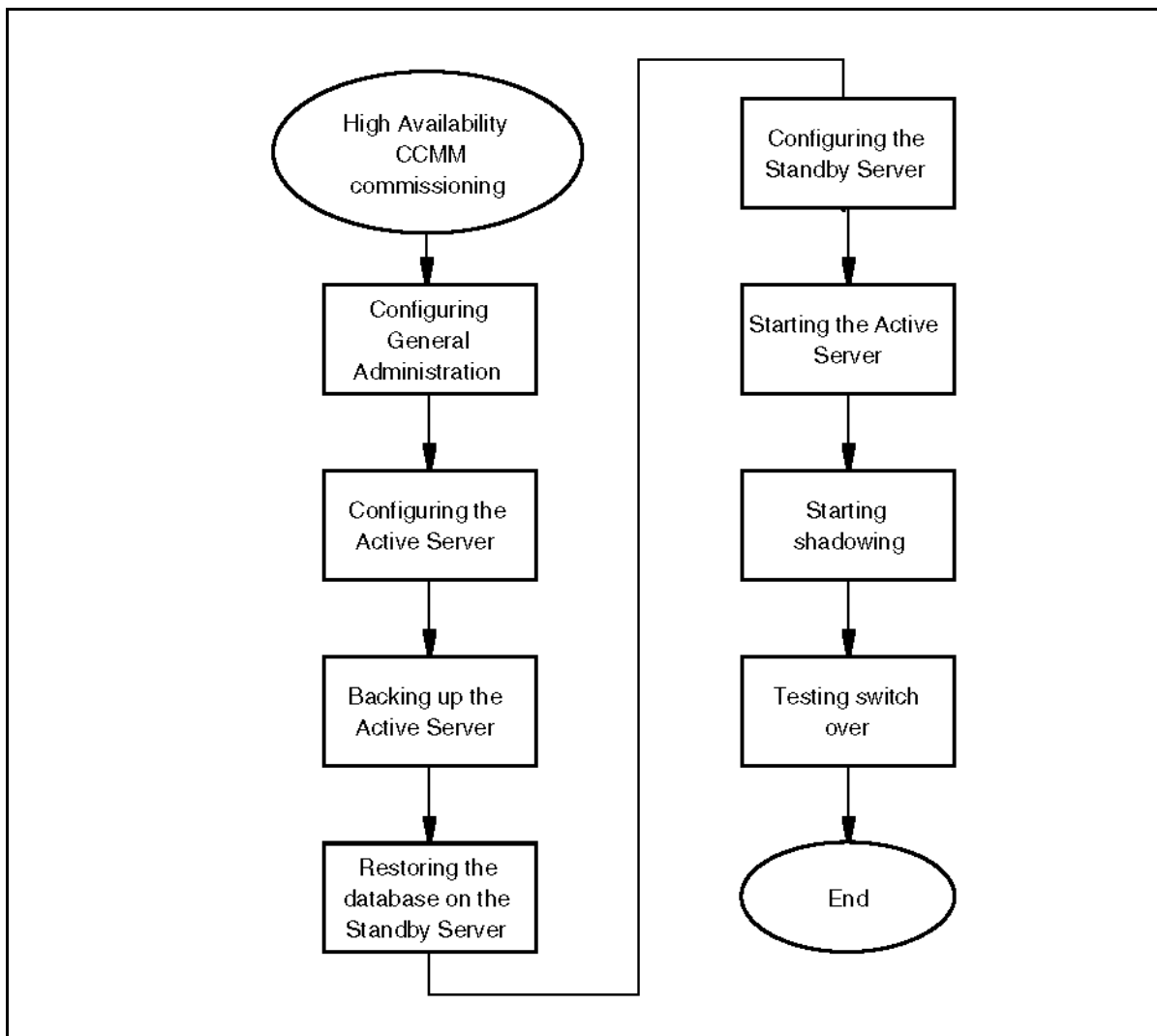
Prerequisites

- Install CCMM software on the active server. See *Avaya Aura™ Contact Center Installation* (NN44400-311).
- Commission Contact Center Multimedia. See [Contact Center Multimedia server commissioning \(page 121\)](#).
- Know how to back up the Contact Center Multimedia database. See *Avaya Aura™ Contact Center Server Administration* (NN44400-610).
- Know how to restore the Contact Center Multimedia database. See *Avaya Aura™ Contact Center Server Administration* (NN44400-610).
- Know how to configure the High Availability settings.
- Install Contact Center Multimedia software on the standby server. See *Avaya Aura™ Contact Center Installation* (NN44400-311).
- CCMM stores license information in the registry. Configure CCMM licensing on the standby CCMM server, after restoring the database from the active server. See [Contact Center Multimedia server commissioning \(page 121\)](#).

High Availability CCMM commissioning procedures

This task flow shows the sequence of procedures performed to commission High Availability for CCMM. To link to any task, go to [High Availability CCMM commissioning procedures \(page 194\)](#)

High Availability CCMM commissioning procedures



High Availability CCMM commissioning procedures

- [Configuring CCMM General Administration \(page 195\)](#)
- [Configuring the Active Server \(page 195\)](#)
- [Backing-up the CCMM Active Server database \(page 196\)](#)
- [Restoring the database on the Standby Server \(page 197\)](#)
- [Configuring the Standby Server \(page 198\)](#)
- [Starting the Active Server \(page 199\)](#)
- [Starting shadowing on the Standby Server \(page 199\)](#)
- [Verifying Shadowing is running on the Active Server \(page 200\)](#)
- [Testing switch over on the CCMM solution \(page 201\)](#)

Configuring CCMM General Administration

Configure CCMM General Administration data.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
1	Click Outbound and Multimedia .
2	In the left column, select General Administration .
3	Click Server Settings .
4	Ensure the Contact Center Multimedia Server is configured with the name of the active server, and the Contact Center Multimedia Redundant Server is configured with the name of the current standby server.

--End--

Configuring the Active Server

The Active Server is configured using the High Availability utility. This utility saves IP information for the Active Server to the database.

Procedure steps

Step	Action
1	Click Start, All Programs, Avaya, Contact Center, Database Utilities, High Availability .
2	Expand Configuration .
3	Double-click Server Mode .
4	Under Server Mode Configuration , select Active .
5	Under IP Configuration , type the Managed IP, CLAN address.
6	Under IP Configuration , type the Active Server details, CLAN IP address.
7	Under IP Configuration , type the Standby Server details, CLAN IP address.
8	In the Trusted IP box, type the IP Address of the trusted server.
9	Click OK .

A system message box appears. You must stop the system before you save any information.

10 Click **Yes** to stop the system.

11 Click **OK** to save the data.

--End--

Variable definitions

Variable	Value
Managed IP	The Managed IP (MIP) address that is used for both the Active and Standby Servers for campus resiliency. The Active Server is always assigned the MIP. If a switchover occurs, the MIP is assigned to the new Active Server. Agents and other applications are not aware that a switchover occurred because the IP address does not change. A MIP is used only when the Active and Standby Servers are in the same subnet.
Active Server details	The IP address for the server initially configured in Active mode.
Standby Server details	The IP address for the server initially configured in Standby mode.
Trusted IP address	The IP address of a trusted server that is not likely to go down so that both Active and Standby servers have a server to ping regularly to verify the network connection. Avaya recommends that you use an IP address from your IT infrastructure as the Trusted Address.

Backing-up the CCMM Active Server database

Use the Database Maintenance utility to back up the Active Server database. The backup of the database is restored to the Standby Server.

Procedure steps

Step	Action
1	Click Start, All Programs, Avaya, Contact Center, Database Utilities, Database Maintenance .
2	Click Backup Locations .
3	Click Create .

- 4 From the **Drive Letter** list, select the network drive on which you want to store the CCMM database.
- 5 In the **UNC Path** box, type the location where you want to store the back up, in the format \\Computer Name\Backup Location. This location should be a shared folder with correct permissions.
- 6 In the **User Name** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
- 7 In the **Password** box, type the domain password.
- 8 Click **OK**.
- 9 In the left pane, click **Immediate Backup**.
- 10 In the **Media Type** section, select **Network Disk**.
- 11 In the **Applications** section, select **CCMM** and **ADMIN**.
- 12 From the **Backup Location** list, select the network drive on which to store the backup.
- 13 Click **OK**.

--End--

Restoring the database on the Standby Server

Restore the database from the Active Server to the Standby Server to ensure the databases are consistent. The Database Maintenance utility can restore only one application's data at a time. Therefore restore the data for the CCMM and ADMIN databases.

You must restore the CCMM and ADMIN databases to the Standby Server. Restore the ADMIN database last.

Prerequisites

- When CCMM is installed the license type is NODAL. If you have a Corporate (CORP) license this will have to be set on the standby server before the active server backup is restored on to the standby machine.

Attention: Restore the CCMM database first and then the ADMIN database.

Attention: Restoring the ADMIN database can change configuration of Backup locations on the Standby Server if the Active Server and Standby Server backup locations are different. After you restore the ADMIN database, close and reopen the Database and Maintenance utility.

Procedure steps

- | Step | Action |
|------|---|
| 1 | Log on to the Standby Server. |
| 2 | Click Start, All Programs, Avaya, Contact Center, Database Utilities, Database Maintenance . |
| 3 | In the Database Maintenance dialog box, in the left pane, click Restore . |
| 4 | In the right pane, under Media Type , select the media type on which the backup is restored. |
| 5 | If the backup file is on the network drive, in the Backup Location list, select the backup location. |
| 6 | Under Application , select the database to restore. |
| 7 | Under Restore contents , select Data. |
| 8 | Click OK . |
| 9 | Use the Progress information field to monitor the restore process. |
| 10 | Click Exit to close the Database Maintenance utility. |

--End--

Configuring the Standby Server

Configure the Standby Server the same as the Active Server.

Prerequisites

- The database from the Active server has been restored to the Standby Server.

Procedure steps

- | Step | Action |
|------|--|
| 1 | Log on to the Standby Server. |
| 2 | Click Start, All Programs, Avaya, Contact Center, Database Utilities, High Availability . |
| 3 | In the left pane, click Server Mode . |
| 4 | Under IP Configuration , type the Managed IP, CLAN address. |
| 5 | Under IP Configuration , type the Active Server details, CLAN IP address. |
| 6 | Under IP Configuration , type the Standby Server details, CLAN IP address. |
| 7 | In the Server Mode Configuration field, select Standby . |
| 8 | Click OK . |

A system message box appears. You must stop the system before you save any information.

- 9 Click **OK**.

--End--

Starting the Active Server

Start the Active Server using the CC Applications tab in the High Availability utility. Starting the Active Server starts the system processes.

Procedure steps

- | Step | Action |
|------|--|
| 1 | Log on to the Active Server. |
| 2 | Click Start, All Programs, Avaya, Contact Center, Database Utilities, High Availability . |
| 3 | Expand Tasks . |
| 4 | Double-click CC Applications . |
| 5 | In the first box under CC Applications , choose the system. |
| 6 | Click Start . |
| 7 | Click OK . |

--End--

Starting shadowing on the Standby Server

Use the High Availability utility to start shadowing on the Standby Server.

Procedure steps

- | Step | Action |
|------|---|
| 1 | Log on to the Contact Center Multimedia standby server. |
| 2 | Choose Start, All Programs, Avaya, Contact Center, Database Utilities, High Availability . |
| 3 | Under Tasks , click System Control . |
| 4 | Beside Control , select Shadowing . |
| 5 | Click Start . |

--End--

Verifying Shadowing is running on the Active Server

The system information tab of the High Availability utility displays system information regarding 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
- Remote server connection status
- Remote server port information
- Port information
- Licence information
- Time of last record shadowed
- Local and remote information on system status, switchover, shadowing and network.
- CC Application install information
- Databases shadowed
- Database namespaces
- Database space and journaling information
- Database processes information

Use this procedure to verify the settings.

Procedure steps

- | Step | Action |
|------|--|
| 1 | Log on to the Active Server. |
| 2 | Click Start, All Programs, Avaya, Contact Center, Database Utilities, High Availability . |
| 3 | Expand Configuration in the left pane. |
| 4 | Select System . |
| 5 | Select Get System Configuration .
<i>The most recent system information appears.</i> |
| 6 | Under the Shadowing section, view the time of the most recent shadowed record, ensure it is an up-to-date time and that it corresponds with when shadowing was started. |

--End--

Testing switch over on the CCMM solution

When the CCMM server commissioning is complete, you can test the CCMM switch over to ensure that it works.

Procedure steps

- | Step | Action |
|------|--|
| 1 | Log on to the Active Server. |
| 2 | Click Start, All Programs, Avaya, Contact Center, Database Utilities, High Availability . |
| 3 | On the Active Server, select System Control . |
| 4 | Under Control , select Switchover to initiate a manual switchover. |
| 5 | Send a test e-mail to one of the CCMM configured mailboxes. After the e-mail is received on the new Active Server, the test is successfully completed. |

--End--

Common procedures

This chapter describes the common procedures that you use when you commission your Avaya Aura™ Contact Center software.

Navigation

- [Stopping individual services \(page 203\)](#)
- [Starting services \(page 204\)](#)
- [Disabling services \(page 204\)](#)
- [Enabling services \(page 205\)](#)
- [Stopping and restarting the core Communication Control Toolkit services \(page 205\)](#)
- [Stopping and restarting the Contact Center Manager Server services \(page 206\)](#)
- [Adding a server to a domain \(page 206\)](#)
- [Starting the Contact Center \(page 207\)](#)
- [Shutting down the Contact Center \(page 208\)](#)

Stopping individual services

During some procedures, you must stop one or more Windows services to manipulate a feature or function.

Prerequisites

- Ensure that you know which server you are working on.
- Ensure that you know which service or services to stop.

Procedure steps

- | Step | Action |
|------|--|
| 1 | Click Start, Administrative Tools, Services . |
| 2 | In the Services window, right-click the name of the service and click Stop . |

--End--

Starting services

During some procedures, you must start one or more Windows services to manipulate a feature or function.

Prerequisites

- Ensure that you know which server you are working on.
- Ensure that you know which service or services to start.

Procedure steps

Step	Action
1	Click Start, Administrative Tools, Services .
2	In the Services window, right-click the name of the service and click Start .

--End--

Disabling services

During some procedures, you must disable one or more Windows services to manipulate a feature or function.

Prerequisites

- Ensure that you know which server you are working on.
- Ensure that you know which service or services to disable.

Procedure steps

Step	Action
1	Click Start, Administrative Tools, Services .
2	In the Services window, right-click the name of the service.
3	Click Properties .
4	On the General tab, from the Startup type list, choose Disabled .
5	Click OK .
6	Restart the computer.

--End--

Enabling services

During some procedures, you must enable one or more Windows services to manipulate a feature or function.

Prerequisites

- Ensure that you know which server you are working on.
- Ensure that you know which service or services to enable.

Procedure steps

Step	Action
1	Click Start, Administrative Tools, Services .
2	In the Services window, right-click the name of the service.
3	Click Properties .
4	On the General tab, from the Startup type list, choose Manual or Automatic/ Automatic (Delayed Start) .
5	Click OK .
6	Restart the computer.

--End--

Stopping and restarting the core Communication Control Toolkit services

Stop and restart the core Communication Control Toolkit services during CCT console configuration to reset the settings.

Prerequisites

- Install Communication Control Toolkit.

Procedure steps

Step	Action
1	Log on to the Communication Control Toolkit server as Administrator.
2	Click Start, All Programs, Avaya, Contact Center, Common Utilities, System Control and Monitor Utility .
3	Select the CCT check box.
4	Ensure the check boxes for other installed applications are cleared.
5	Click Shutdown Contact Center to make CCT services stop.
6	Click Yes .
7	Click Start Contact Center after the CCT Status Shutdown is complete.

8 Click **Yes**.

--End--

Stopping and restarting the Contact Center Manager Server services

Stop and restart the Contact Center Manager Server services to reset the settings.

Prerequisites

- Install Contact Center Manager Server.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Server as Administrator.
2	Click Start, All Programs, Avaya, Contact Center, Common Utilities, System Control and Monitor Utility .
3	Select the CCMS check box.
4	Ensure the check boxes for any other installed applications are cleared.
5	Click Shutdown Contact Center to make CCMS services stop.
6	Click Yes .
7	Click Start Contact Center after the CCMS Status Shutdown is complete.
8	Click Yes .

--End--

Adding a server to a domain

Add your Contact Center Manager Server to an existing domain and ensure that your server works in a domain.

Prerequisites

- Install Contact Center Manager Server.
- Ensure that you have domain administrator privileges, or ask the domain administrator to assign you a domain user account for remote access.

Procedure steps

Step	Action
------	--------

- 1 Log on to the Contact Center Manager Server.
- 2 Click **Start, Administrative Tools, Server Manager**.
- 3 Beside **Computer Information**, click **Change System Properties**.
- 4 In the **System Properties** dialog box, click the **Computer Name** tab.
- 5 Click **Change**.
- 6 In the **Computer Name/Domain Changes** dialog box, click the **Domain** option.
- 7 Type the domain name (you must provide the fully qualified domain name, which includes the prefix and suffix).
- 8 Click **OK**.
- 9 Type your **User name** and **Password**.
- 10 Click **OK**.
- 11 Restart the server when you are prompted to do so.

--End--

Starting the Contact Center

The System Control and Monitor Utility (SCMU) enables the administrator to start and stop the contact center applications, for example CCMS and CCT. This procedure describes how to start the contact center.

Procedure steps

- | Step | Action |
|------|---|
| 1 | Click Start, All Programs, Avaya, Contact Center, Common Utilities, System Control and Monitor Utility . |
| 2 | On the Contact Center tab click Start Contact Center . |
| 3 | Click Yes . |
| 4 | Select the CCMS and CCT tab to view the started services. |
| 5 | Select Close |

Attention: If a CCMS monitored service is stopped using the SCMU utility or the Windows Service Control Manager, the CCMS Service monitor cannot restart the service and will not trigger a switchover. This rule permits the administrator to stop a service for maintenance.

--End--

Shutting down the Contact Center

The System Control and Monitor Utility (SCMU) enables the administrator to start and stop the contact center applications, for example CCMS and CCT. This procedure describes how to stop the contact center.

Procedure steps

Step	Action
1	Click Start, All Programs, Avaya, Contact Center, Common Utilities, System Control and Monitor Utility .
2	On the Contact Center tab, click Shutdown Contact Center .
3	Click Yes .
4	Select the CCMS and CCT tab to view the stopped services.
5	Select Close .

--End--

Integrated Reporting commissioning

This section describes how to commission Integrated Reporting.

Contact Center Manager Server (CCMS) has an integrated reporting capability for Multimedia (CCMM) and Media Application Server (MAS) statistics.

You can configure CCMS to collect and store MAS and CCMM statistical contact data in the CCMS database. You must select the CCMS Contact Summary Reporting (CSR) feature to enable Integrated Reporting.

The MAS database location, username and password may be entered in the CCMS Database Maintenance utility, allowing CCMS to collect MAS statistical data every 15 minutes and store it in the CCMS database.

The Contact Center Multimedia database location, username and password may be entered in the CCMS Database Maintenance utility, allowing CCMS to access CCMM statistical data directly without storing it in the CCMS database.

For front-end IVR scenarios, MAS assigns a unique number to each call. MAS passes this unique call number to the CCMS Open Networking web service, as the call is transferred to the CCMS. The CCMS then uses this unique call number to match the MAS part of the call with the CCMS part of the same call and generate meaningful call flow statistics. The CCMS Open Networking Web Service must be enabled for this procedure to work. For MAS treatment scenarios, the call arrives first on CCMS, which assigns it a unique number. When the call is treated by MAS, this unique number is extracted by the MAS application using CTI, and stored in the reporting data for this part of the call. The Open Networking Web service is not required for the MAS treatment scenario. Contact Summary Reporting must be enabled on the CCMS to collect these CSR statistics.

The MAS uses a Landing Pad, a CDN controlled by the CCMS, to transfer the call to the Contact Center.

Prerequisites for Integrated Reporting commissioning

- Read the *Avaya Aura™ Contact Center Planning and Engineering* (NN44400-210).
- Complete the *Avaya Aura™ Contact Center Installation Checklist* (NN44400-310).
- Install the Contact Center Manager Server software.
- Install the other Avaya Aura™ Contact Center components on your server.
- The system clock time must be the same on both the CCMS and MAS server. The time zones can be different, if for example the MAS server is in

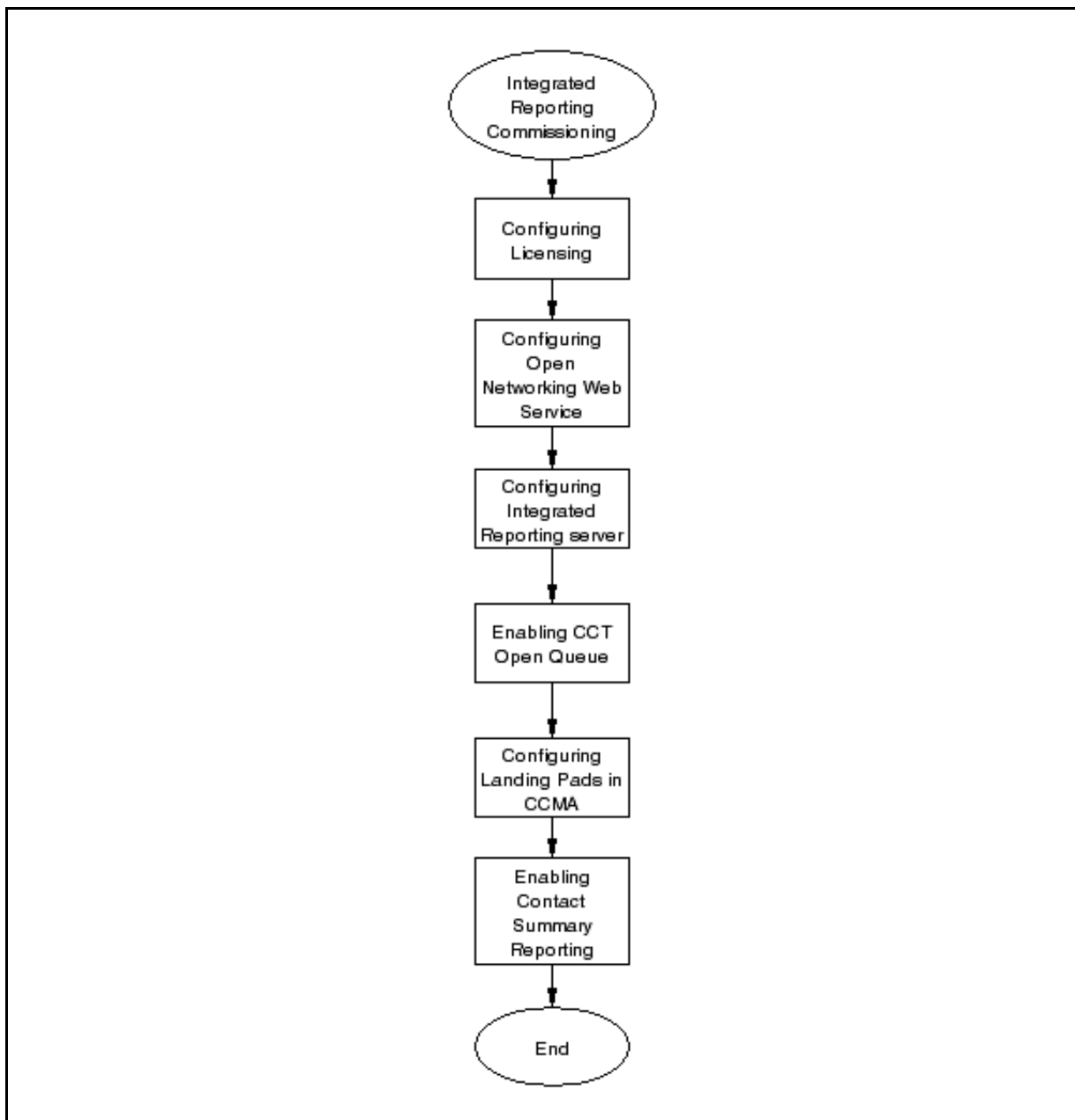
Eastern time zone and CCMS is in the GMT time zone, the system clock time must be the same on both servers. CCMS already obtains the time from the Avaya Communication Server 1000, therefore all Contact Center servers have the same clock. To ensure that the system clock time on the CCMS and the MAS servers are synchronized configure the system so that they both obtain their times from the same external clock source. This is achieved as follows:

- Configure the MAS Network Time Protocol (NTP) service as a client of an external time source clock.
- Configure the Avaya Communication Server 1000 time service as a client of the same external time source clock as used for MAS.
- Contact Center collects data from only one MAS. If the Contact Center interacts with multiple MAS servers on a Cluster, create the replication account for Integrated Reporting on the Active or Secondary with appropriate Session Detail Record (SDR) replication settings. Integrated Reporting supports only one cluster. If more than one cluster is configured, only one of them can be designated as the Integrated Reporting cluster.

Commissioning Integrated Reporting

This task flow shows you the sequence of procedures you perform to configure Integrated Reporting. To link to any task, go to [Navigation for commissioning Integrated Reporting \(page 212\)](#).

Integrated Reporting commissioning procedures



Navigation for commissioning Integrated Reporting

- [Configuring Licensing \(page 212\)](#)
- [Configuring Open Networking Web Service \(page 213\)](#)
- [Configuring Integrated Reporting Server \(page 214\)](#)
- [Enabling Communication Control Toolkit Open Queue \(page 216\)](#)
- [Configuring Landing Pads \(page 217\)](#)
- [Enabling Contact Summary Reporting \(page 220\)](#)

Job aid: Timing

The estimated time to commission Integrated Reporting is 1 hour.

Configuring Licensing

Use this procedure to configure licensing to enable the Open Networking feature.

Prerequisites

- Install the Open Queue feature.
- The Universal Networking feature is available with an Enterprise license.

Attention: You must restart your server at the end of this procedure.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Server.
2	Click Start, All Programs, Avaya, Contact Center, Manager Server, Server Configuration .
3	Click the Licensing tab.
4	From the CCMS Optional Packages list, select Networking, Universal Networking .
5	Select Open Queue . Enable this option even if Open Queue is not otherwise being used.
6	Select Open Interfaces Universal Networking .

- 7 Click **OK**.
- 8 Click **Yes** to restart the server.

--End--

Procedure job aid

After you restart Contact Center Manager Server, Open Queue is enabled.

Configuring Open Networking Web Service

Use this procedure to configure the Open Networking Web service.

Prerequisites

- Know how to stop and restart the core CCMS services.
- Ensure that a valid SOA license is available.
- The Open Networking Web service is available only if the customer purchased the Universal Networking feature, and selected the enable SOA option on the CCMS order.
- If enabling TLS, understand Certificate Authorities, certificate signing requests, and certificates.
- A Certificate Authority is also required to generate the certificates.

Attention: You must restart your server after you perform this procedure.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Server.
2	Click Start, All Programs, Avaya, Contact Center, Manager Server, Server Configuration .
3	In the left pane of the Server Configuration console, click WS Open Interfaces .
4	Select the SOA Enabled check box.
5	Ensure the Host contains the host name of the server.
6	In Ports , type an available port number for which the services are available for access.
7	In the Session Timeout box, select the value of the timeout duration in minutes.
8	To publish services under TLS (HTTPS), select the TLS Encryption check box. To publish services under HTTP, clear the TLS Encryption check box.

- 9 Click **Apply All**.
- 10 Click **OK**.
- 11 Select **Exit** to save your changes.
- 12 Stop and restart the core Contact Center Manager Server services.

--End--

Variable definitions

Parameter	Value
Host	The host name of the server, not the IP address.
Ports	The port number on which the OpenQueue and OpenNetwork Interfaces are published. This port and the following three consecutive port numbers are used to access the Web services from the external applications. All four port numbers must be available.
Session Timeout	The time in minutes that a session is valid after a user logs on. The session times out if it is inactive for the specified duration. The default is 120 minutes.
TLS Encryption	To publish services under TLS (HTTPS), mark the TLS Encryption check box. To publish services under HTTP, clear the TLS Encryption check box.

Procedure job aid

Once enabled, the WSDL for the Open Networking web service is available at:

`http://<CCMS HostName>:9080/SOAOL/services/OpenNetworking?wsdl`

Configuring Integrated Reporting Server

Add Media Application Server (MAS) and Contact Center Multimedia (CCMM) as Integrated Reporting Servers using the CCMS Database Maintenance Utility. The CCMS Database Maintenance Utility - Integrated Reporting Server supports one CCMM server and one MAS server.

Use the CCMS Database Maintenance utility to configure one MAS and one CCMM server to enable integrated reporting for MAS Contact Summary Report (CSR) statistics and MM CSR statistics.

Prerequisites

- If integrating CCMS with MAS, the MAS database replication userID account and password must be setup on the MAS Server using Element Manager. This account and password are needed by CCMS to access the MAS reporting server to collect statistics for Integrated Reporting. This account is set up using the MAS Element Manager under - Replication Account.
- Contact Center collects data from only one MAS. If the Contact Center interacts with multiple MAS servers on a Cluster, this replication account should be created on the Active or Secondary with appropriate SDR replication settings. Integrated Reporting only supports one cluster. If more than one cluster is configured, only one of them can be designated as the Integrated Reporting cluster.
- If integrating with CCMM, use the CCMM mmReport account and its password. These are set up during the CCMM installation.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Server.
2	Click Start, All Programs, Avaya, Contact Center, Database Utilities, Database Maintenance .
3	In the Database Maintenance dialog box, in the left pane, click Integrated Reporting Server .
4	In the right pane, click Create to add a new row to the Server table.
5	From the Type list, select the type ICP or MULTIMEDIA from the list. This automatically populates the Port & Database Name columns.
6	In the Display Name box, type the MAS server name, or the CCMM server as it will appear in reports.
7	In the IP box, type the IP address of the MAS or CCMM server.
8	In the Username box, type the MAS database replication account username, or the CCMM mmReport user name.
9	In the Password box, type the MAS database replication account password, or the CCMM mmReport password.
10	Click OK .
11	Click Exit .

--End--

Variable definitions

Parameter	Value
Type	ICP or MULTIMEDIA, as appropriate. If the server type is MAS select the ICP option.
Display Name	The MAS or CCMM server name as it will appear in reports.
IP	The IP address of the MAS or CCMM server.
Port	Automatically filled in.
Database Name	Automatically filled in.
Username	The MAS replication account user name. Or the CCMM mmReport account name.
Password	The MAS replication account password Or the CCMM mmReport account password.

Enabling Communication Control Toolkit Open Queue

Enable Open Queue functionality on stand alone Communication Control Toolkit (CCT). If CCT is co-resident with CCMS, enable Open Queue on CCMS, see [Enabling Open Queue \(page 24\)](#).

Prerequisites

- Open Queue must be enabled on the CCMS.
- Know how to stop and restart the core Communication Control Toolkit services.

Procedure steps

Step	Action
1	Log on to the Communication Control Toolkit server.
2	Click Start, All Programs, Avaya, Contact Center, Communication Control Toolkit, CCT Console .
3	In the left pane of the CCT console, expand Communication Control Toolkit .
4	Expand Server Configuration .
5	Select Deployment Type .
6	In the Deployment Type dialog box, select your deployment option for Communication Control Toolkit.
7	In the CCMS Server Hostname box, type the name of the Contact Center Manager Server.

- 8 In the Actions pane on the right, select **Apply changes**.
- 9 Stop and restart the core Communication Control Toolkit services.

--End--

Configuring Landing Pads

Use this procedure to configure Landing Pads using CCMA.

Avaya recommends that you configure multiple Landing Pads to ensure proper capacity and scalability. The Open Networking Web service distributes load across all configured Landing Pads.

Although you can configure both CDNs and DNISs as Landing Pads, the Integrated Reporting feature is available when you use CDN Landing Pads only. For more information about Landing Pads, see *Avaya Aura™ Contact Center Server Administration* (NN44400-610).

For more information on configuring Landing Pads see *Avaya Aura™ Contact Center Manager Administration – Client Administration* (NN44400-611).

Prerequisites

- The selected CDN must be configured on the switch.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration.
2	On the CCMA web page, select Configuration .
3	In the left pane, double-click the Contact Center Manager Server on which to add the Landing Pad CDN (Route Point).
4	Select the CDNs (Route Points) folder.
5	In the CDNs (Route Points) window, select the Landing Pads tab.
6	In Name box, type a name for the CDN (Route Point) Landing Pad.
7	In the Number box, type the number for the CDN (Route Point) Landing Pad. This number must match the number configured on the switch.
8	For SIP Contact Centers, you must configure the Landing Pad URI. In the URI box, type the value for the Universal Resource Indicator (URI) of the CDN (Route Point) on the SIP server.
9	Click any other row in the grid to add the CDN (Route Point) Landing Pad. Not Acquired appears in the Status column.
10	Select the Acquired check box for the CDN (Route Point) Landing Pad.

Integrated Reporting commissioning

- 11 Click any other row of the table to acquire the CDN (Route Point) Landing Pad.
- 12 Click **Refresh Status** to view the current status

--End--

Variable definitions

Variable	Value
Name	The name of the CDN (Route Point) as you want it to appear in reports. Valid value: 30-character maximum (no special characters)
Number	The number assigned to the CDN (Route Point). The number passed to the switch in requests to acquire or deacquire the CDN (Route Point). This number must match the number configured at the switch. Attention: You cannot change a saved CDN (Route Point) number. You must delete the CDN and then recreate it. Valid values: 7-digit maximum.
URI	URI box (only present for SIP connected contact centers). The Universal Resource Identifier (URI) of the CDN (Route Point) on the Media Application Server. The URI must equate to the fully qualified SIP address for the CDN (Route Point). Valid values: maximum 255 characters, including numbers, English characters, forward slash (/), backslash (\), question mark (?), ampersand (&), period (.), at symbol (@), underscore (_) and hyphen (-). This field is mandatory. You cannot modify the URI of a saved CDN (Route Point). The URI must be unique to URIs currently assigned to other CDNs, DNISSs, or agents.
Acquired	Attention: You must configure the CDN (Route Point) on the switch and add it on Contact Center Manager Server before you can acquire it. Select the Acquired check box to acquire or deacquire the CDN (Route Point) and then click Refresh Status to refresh the Status column. If the acquisition is successful, Acquired appears in the Status column. When you successfully deacquire the CDN (Route Point), Not Acquired appears in the Status column.
Status	The Status column displays the acquisition status of the CDN (Route Point) or Open Queue CDN (Route Point).

Enabling Contact Summary Reporting

Contact Summary Reporting (CSR) must be enabled on the CCMS server for the Integrated Reporting to be enabled. Integrated Reporting then returns the statistical data for MAS CSR and CCMM CSR.

You must enable the Contact Summary Reporting using CCMA – Configuration component under Historical Statistics node.

For more information, see Configuring Historical statistics in *Avaya Aura™ Contact Center Manager Administration – Client Administration* (NN44400-611).

Procedure steps

- | Step | Action |
|------|---|
| 1 | Log in to Contact Center Manager Administration. |
| 2 | On the CCMA web page, select Configuration . |
| 3 | In the left pane, double-click the server on which to configure Historical Statistics. |
| 4 | Select the Historical Statistics folder. |
| 5 | In the right-pane, select the Collect the following statistics table. |
| 6 | For each statistic type, in the Collect column, select the check box beside the statistics to collect, or clear the check box beside the statistics not to collect. |
| 7 | In the Collect the following statistics table, select the Contact Summary check box. |
| 8 | Scroll down and select the Duration table. |
| 9 | For each type of statistic, enter the amount of time the statistic is stored on the server. |
| 10 | In the Duration table, enter 1 or more days as appropriate for Contact Summary (days) . |
| 11 | Click Submit to save your changes. |

--End--

Contact Center Manager Server Web service configuration

A series of SOAP-based Open Interfaces is provided to third-party software structures so that you can enable communications for your applications based on the SOA architecture.

The Open Queue Open Interface provides existing OpenQ functions to third-party applications using a Web service. In a controlled fashion, third-party applications can add and remove contacts of a specific type in Avaya Aura™ Contact Center.

The Open Networking Open Interface enables a third-party application to transfer a call between nodes in a network along with any data associated with the call. The third-party applications can reserve a Landing Pad on the target node to enable the call to be transferred with data attached. The Web services also provide the functionality to cancel the reservation of a Landing Pad to free it for other calls transferred across the network.

The open interface applications are optional.

For more details, see the SDK documentation.

Navigation

- [Generating a Certificate Signing Request \(page 221\)](#)
- [Importing the CSR-Related Certificates \(page 222\)](#)
- [Configuring SOA OpenQueue and OpenNetworking Web Services \(page 223\)](#)
- [Removing Certificate Configuration \(page 226\)](#)

Generating a Certificate Signing Request

Generate a Certificate Signing Request (CSR) to configure certificates and enable the Web services over the Transport Layer Security.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Server.

- 2 Click **Start, All Programs, Avaya, Contact Center, Manager Server, Server Configuration**.
- 3 In the left pane of the Server Configuration console, click **WS Open Interfaces**.
- 4 Select the **TLS Encryption** check box.
- 5 Ensure the **Host** box contains the host name of the server.
- 6 In the **Password** box, type a password that contains at least six characters.
- 7 Click **Apply All**.
The CSR appears in the CSR box. Use the CSR file to apply to a Certificate Authority (CA) to buy a certificate and import the certificate to the service using the configuration application.
- 8 Click **OK**.

--End--

Variable definitions

Variable	Value
TLS (Transport Layer Security)	Protocol that allows secure communication between applications across a network.

Procedure job aid

Certificate Authorities (CA) include the following components:

- Verisign
- Thawte
- Create your own

Importing the CSR-Related Certificates

Import the CSR-Related Certificates to the SOA configuration after you receive the certificates to enable services over the Transport Layer Security.

Prerequisites

- Ensure you generate a CSR certificate. For more information, see [Generating a Certificate Signing Request \(page 221\)](#).
- Ensure you apply to a Certificate Authority (CA) for a certificate.

Procedure steps

- | Step | Action |
|------|--|
| 1 | Log on to the Contact Center Manager Server. |

- 2 Click **Start, All Programs, Avaya, Contact Center, Manager Server, Server Configuration**.
- 3 In the left pane of the Server Configuration console, click **WS Open Interfaces**.
- 4 In the **Generate Certificate Signing Request Password** box, type a password.
- 5 In the **Alias** box, type an alias to identify the CA certificate, such as SomeCAPublicCert1.
- 6 In the **Trusted Certificate Authority CA Cert** box, click **Browse**, and then select the CA public certificate.
- 7 In the **CSR Response Certificate CSR Cert** box, click **Browse**, and then select the certificate.
- 8 Click **Apply All**.
- 9 Click **OK**.

--End--

Configuring SOA OpenQueue and OpenNetworking Web Services

Configure and enable the SOA OpenQueue and OpenNetworking Web Services to configure other applications that can add contacts to the open queue for routing, remove contacts from the open queue, and move contacts between nodes in a network.

Prerequisites

- Know how to stop and restart the core CCMS services.
- Install and commission Contact Center Manager Server. See *Avaya Aura™ Contact Center Installation* (NN44400-311) and *Avaya Aura™ Contact Center Commissioning* (NN44400-312).
- Ensure that the Contact Center License Manager is licensed to provide SOA OpenQueue and OpenNetworking Web Services.
- Ensure OpenQ and OpenNetworking Web Services and the CCT Web Services do not use the same port on the server. Change the OpenQ and OpenNetworking services port value from 9080 to 9070 in the Web services section of server configuration.
- If you enable TLS, understand Certificate Authorities, certificate signing requests, and certificates. A Certificate Authority is also required to generate the certificates. Configure the SOA Configuration of Certificates using the procedure in [Generating a Certificate Signing Request \(page 221\)](#).

Procedure steps

- | Step | Action |
|------|---|
| 1 | Log on to the Contact Center Manager Server. |
| 2 | Click Start, All Programs, Avaya, Contact Center, Manager Server, Server Configuration . |
| 3 | In the left pane of the Server Configuration console, click WS Open Interfaces . |
| 4 | Select the SOA ENABLED check box. |
| 5 | Ensure the Host box contains the host name of the server. |
| 6 | In the Ports box, type an available port number for which the services are available for access. |
| 7 | In the Session Timeout box, select the value of the timeout duration in minutes. |
| 8 | To publish services under TLS (HTTPS), select the TLS Encryption check box. To publish services under HTTP, clear the TLS Encryption check box. |
| 9 | In the User Password field, type the new password for the OpenWsUser account. |
| 10 | Click Apply All . |
| 11 | Click OK . |
| 12 | Stop and restart the core Contact Center Manager Server services. |
| 13 | Verify that the services are available by viewing the following on the host: http://localhost:9090 . |

--End--

Variable definitions

Variable	Value
Host	The host name of the server, not the IP address.
Ports	The port number on which the OpenQueue and OpenNetwork Interfaces are published. This port and the following three consecutive port numbers are used to access the Web services from the external applications. All four port numbers must be available.
Session Timeout	The time in minutes that a session is valid after a user logs on. The session times out if it is inactive for the specified duration. The default is 120 minutes.
TLS Encryption	To publish services under TLS (HTTPS), select the TLS Encryption check box. To publish services under HTTP, clear the TLS Encryption check box.

Removing Certificate Configuration

Remove certificate configuration to delete all imported certificates and any outstanding CSR files.

Prerequisites

- Clear the TLS Security check box.
- Ensure the certificates are configured. For more information, see [Generating a Certificate Signing Request \(page 221\)](#).

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Server.
2	Click Start, All Programs, Avaya, Contact Center, Manager Server, Server Configuration .
3	In the left pane of the Server Configuration console, click WS Open Interfaces .
4	Select the SOA Enabled check box.
5	Select the Remove Certificates check box.
6	Click Apply All , and then OK .
7	In the confirmation dialog box, click Yes .
8	Click OK .

--End--

Communication Control Toolkit Web service configuration

A series of SOAP-based Open Interfaces is provided to third-party software structures so that you can enable communications for your applications based on the SOA architecture.

The CCT Open Interfaces is a development environment that offers functionality similar to the CCT SDK but with the flexibility to choose your own development environment.

You can use these services to re-create Agent tools within your own applications or to access call control functionality for Avaya Aura™ Contact Center from any business process.

The open interface applications are optional.

For more details, see the SDK documentation.

Navigation

- [Configuring SIP Call Recording \(page 228\)](#)
- [Generating a Certificate Signing Request \(page 229\)](#)
- [Importing CSR-related Certificates \(page 230\)](#)
- [Configuring SOA CCT Web Services \(page 231\)](#)
- [Removing Certificate Configuration \(page 232\)](#)

Configuring SIP Call Recording

Configure the SIP Call Recording user account. This SIP Call Recording user account is a special user that is only used by the Call Recording server to connect to Communication Control Toolkit, and only using the OI interface.

Avaya recommend that the SIP Call Recording user account is a Windows domain user account, although no restriction is in place to prevent the selection of a local Windows Security Account Manager (SAM) account.

Procedure steps

- | Step | Action |
|------|--|
| 1 | Log on to the Communication Control Toolkit server. |
| 2 | Click Start, All Programs, Avaya, Contact Center, Communication Control Toolkit, CCT Console . |
| 3 | In the left pane of the CCT console, Expand Communication Control Toolkit . |
| 4 | Expand Server Configuration . |
| 5 | Select CCT Web Services . |
| 6 | Select the Enable CCT Web Services check box in the right pane. |
| 7 | Under SOA Configuration , select the Enable SIP Call Recording check box. |
| 8 | Click Browse Users . |
| 9 | On the Browse Users dialog, in the Location list, select the location of the Windows account you plan to use as the SIP Call Recording user account. |
| 10 | In the Search Type list, select All Users . |
| 11 | Click Search . |
| 12 | From the list of users, select the user that you plan to use as the SIP Call Recording user account. |
| 13 | Click OK . |

--End--

Generating a Certificate Signing Request

Generate a Certificate Signing Request (CSR) to configure certificates and enable services over the Transport Security Layer (TLS).

An application can use CSR to apply to a Certificate Authority (CA) for a certificate. The host name and password is used to generate the CSR. The password is saved in an encrypted format.

After the CSR file is generated and it is available to present to a Certificate Authority to obtain a corresponding certificate.

Procedure steps

Step	Action
1	Log on to the Communication Control Toolkit server.
2	Click Start, All Programs, Avaya, Contact Center, Communication Control Toolkit, CCT Console .
3	In the left pane of the CCT console, Expand Communication Control Toolkit .
4	Expand Server Configuration .
5	Select CCT Web Services .
6	Select the Enable CCT Web Services check box in the right pane.
7	Select the TLS Security check box.
8	Ensure the Host Name box contains the host name of the server.
9	Click Generate CSR .
10	In the Location box, type the location of the company.
11	In the Company Name box, type the name of your company.
12	In the Password box, type a password that contains at least six characters.
13	Click Generate .
14	Click OK .

Attention: After you generate a CSR, import Trusted Certificate Authority (CA) for a certificate and import CSR Response Certificate then Apply Changes. These three steps are required to enable services over the TLS.

--End--

Variable definitions

Variable	Value
TLS (Transport Layer Security)	Protocol for secure communication between applications across a network.

Importing CSR-related Certificates

After you receive the certificate, import the CSR-related certificates to the SOA configuration to enable services over the TLS.

Prerequisites

- Ensure you generate a CSR certificate. For more information, see [Generating a Certificate Signing Request \(page 229\)](#).
- Ensure you apply to a Certificate Authority (CA) for a certificate.

Procedure steps

- | Step | Action |
|------|---|
| 1 | Log on to the Communication Control Toolkit. |
| 2 | Click Start, All Programs, Avaya, Contact Center, Communication Control Toolkit, CCT Console . |
| 3 | In the left pane of the CCT console, expand Communication Control Toolkit . |
| 4 | Expand Server Configuration . |
| 5 | Select CCT Web Services . |
| 6 | Select the Enable CCT Web Services check box. |
| 7 | Select the TLS Security check box. |
| 8 | In the CA Alias box, type an alias to identify the CA certificate, such as SomeCAPublicCert1. |
| 9 | Click Import Trusted CA Certificate to select the CA public certificate. |
| 10 | Click Import Certificate to select the certificate. |
| 11 | Click Apply Changes , and then click OK . |

--End--

Configuring SOA CCT Web Services

Configure and enable the SOA CCT Web Services.

Prerequisites

- Understand the network requirements for your installation of Communication Control Toolkit (co-resident, stand-alone, or multimedia).
- Know how to stop and restart the core Communication Control Toolkit services.
- Install and commission Contact Center Manager Server. See *Avaya Aura™ Contact Center Installation* (NN44400-311) and *Avaya Aura™ Contact Center Commissioning* (NN44400-312).
- Ensure that a valid SOA license is available.
- If you enable TLS, understand Certificate Authorities, certificate signing requests, and certificates. A Certificate Authority is required to generate the certificates. Configure the SOA Configuration of Certificates using the procedure in [Generating a Certificate Signing Request \(page 229\)](#).

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Server.
2	Click Start, All Programs, Avaya, Contact Center, Communication Control Toolkit, CCT Console .
3	In the left pane of the CCT console, expand Communication Control Toolkit .
4	Expand Server Configuration .
5	Select CCT Web Services .
6	Select the Enable CCT Web Services check box.
7	Ensure the Host Name box contains the host name of the server.
8	In the Ports box, type an available port number where the services are available for access.
9	In the Domain Authentication Server box, type the fully qualified domain name of the active directory server that any domain users are to be authenticated against.
10	Select the required Domain Authentication Method .
11	In the Session Timeout box, select the value of the timeout duration in minutes.
12	To publish services under TLS (HTTPS), select the TLS Security check box. To publish services under HTTP, clear the TLS Security check box.
13	Click Apply .
14	Click OK .

- 15 Stop and restart the core Communication Control Toolkit services.
- 16 Verify that the services are available by viewing the following on the host:
<http://localhost:9090>.

--End--

Variable definitions

Variable	Value
Authentication Server	The name of the active directory server that domain users must be authenticated against. The name must be in the format host.domain. For example, myDomainServer.myDomain.com.
Domain Authentication Method	The Domain Authentication Method: Simple or Digest-MD5 specifies if LDAP authentication requests to the Authentication Server is in digest or plain text format. Digest authentication works only with an Active Directory server if the user details are stored with reverse encryption enabled.
Host	The host name of the server, not the IP address.
Port	The port number on which the SOA CCT Interfaces are published. This port, along with the following three consecutive port numbers are used to access the Web services from the external applications. All four port numbers must be available.
Session Timeout	The amount of time in minutes that a session is valid after a user logs on The session times out if it is inactive for the specified duration. The default is 120 minutes.
TLS	To publish services under TLS (HTTPS), select the TLS check box. To publish services under HTTP, clear the TLS check box.

Removing Certificate Configuration

Remove certificate configuration to delete all imported certificates and any outstanding CSR files.

Prerequisites

- Clear the TLS Security check box.

- Ensure the certificates are generated. For more information, see [Generating a Certificate Signing Request \(page 229\)](#).

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Server.
2	Click Start, All Programs, Avaya, Contact Center, Communication Control Toolkit, CCT Console .
3	In the left pane of the CCT console, expand Communication Control Toolkit .
4	Expand Server Configuration .
5	Select CCT Web Services .
6	Select the Enabled CCT Web Services check box.
7	Click Reset TLS Encryption Configuration .
8	In the confirmation dialog box, click Yes , and then click Confirm .
9	Click OK .

--End--

