Avaya Aura™ Contact Center

SIP Commissioning

NN44400-511

Document status: Standard
Document issue: 02.05
Document date: 12 November 2010
Product release: Release 6.0/6.1
Job function: Configuration
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/ 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

New in this release 5
Features 5
Avaya Aura™ Unified Communications Platform support 5
SIP-enabled Contact Center features 5
SIP Hotdesking 6
Supported contact types 6
SIP-enabled Contact Center feature limitations 7
Introduction 9
Introduction to SIP 9
SIP-enabled contact center using the Avaya Aura™ Unified Communications Platform 9
SIP-enabled contact center using Avaya CS 1000 13
CDNs and SIP Route Points 14
Networking Routing Service 15
TDM-based contact center 15
Avaya Communication Server 1000 configuration 19
Adding SIP endpoints for Contact Center Manager Server 21
Adding SIP Routing Entry for Contact Center Manager Server 22
Configuring the Signaling Server for SIP CTI (Remote Call Control) 23
Configuring the Call Server for SIP CTI (Remote Call Control) 24
Configuring Agent DN with SIP CTI (RCC) on the Call Server 24
Office Communications Server configuration 27
Ensuring that OCS supports TCP SIP Transport connection type 28
Adding Contact Center Manager Server as an authorized host 29
Adding a static route from OCS to Contact Center Manager Server 30
Contact Center Manager Server configuration 31
Adding the Contact Center Manager Server to Contact Center Manager Administration 33
Adding route points for voice and instant messages 33
Adding media servers 34
Adding media servers to the required services 35
Adding agents to the contact center 36
Adding a TFE script 38
CCMS certificate management 41
Creating a certificate store using Certificate Manager 42
Generating a Certificate Signing Request file 44
Signing a Certificate Signing Request file 45
Adding a certificate file to the certificate store 47
Removing a certificate file from the certificate store 49
Examining a certificate file in the certificate store 49
Media Application Server configuration 51
Logging onto MAS Element Manager 54
Adding the CCSM service license 55
Confirming the CCSM packaged application locale 55
Adding Contact Center Manager Server as a trusted node 56
Adding a media content namespace 57

Uploading a batch zip file 58
Adding a media content group 59
Uploading a music media file 59
Uploading a treatment media file 61
Configuring MAS settings for SIP-enabled contact center 61
Configuring MAS for locale-specific tones 63
Communication Control Toolkit configuration 65
Configuring the licensing for CCT 67
Configuring the deployment type for CCT 68
Confirming that the CCT services start 70
Adding the CCT Server in CCMA 71
Adding agents in CCMA 71
Verifying CCT using Reference Client 72
Agent Desktop deployment 75
Deploying Agent Desktop for the first time 76
Logging on to the Agent Desktop 76
Configuring CCMM user name and password and OCS account details 77
Launching the Agent Desktop after initial installation 78
Avaya Aura™ Hotdesking 79
Logging on to an Avaya Aura™ station 79
CS 1000 Hotdesking configuration 81
Logging on to Virtual Office remotely 81
Logging off of Virtual Office 82
SIP-enabled contact center testing 83
Verifying correct operation 83

New in this release

The following sections detail what is new in *Avaya Aura™ Contact Center SIP Commissioning* (NN44400-511) for Release 6.0/6.1.

Navigation

- Features (page 5)

Features

See the following sections for information about feature changes:

- Avaya Aura™ Unified Communications Platform support (page 5)
- SIP-enabled Contact Center features (page 5)
- SIP Hotdesking (page 6)
- Supported contact types (page 6)
- SIP-enabled Contact Center feature limitations (page 7)

Avaya Aura™ Unified Communications Platform support

Avaya Aura™ Contact Center supports integration with the Avaya Aura™ Unified Communications platform. This integration gives Avaya Aura™ Contact Center access to and control of the Avaya Aura™ Unified Communications solution and phones. The Avaya Aura™ Unified Communications platform benefits by accessing Contact Center skill-based routing, call treatments, reporting, and the graphical Service Creation Environment.

Avaya Aura™ Contact Center, when integrated with an Avaya Aura™ Unified Communications platform, supports only the Avaya 9600 Series IP Deskphone.

The following documents include content on Avaya Aura™ Unified Communications Platform support and integration:

- *Avaya Aura™ Contact Center Planning and Engineering* (NN44400-210)
- *Avaya Aura™ Contact Center Configuration – Avaya Aura™ Unified Communications Platform Integration* (NN44400-521)

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
- Music on hold for transfers

SIP Hotdesking

In a SIP-enabled contact center, hotdesking is the practice of an agent being able to sit at any desk and use whatever devices are configured there to do their job.

You configure agent details, phone number, and logon credentials using Contact Center Manager Administration (CCMA). A contact center agent can log on to any Avaya Aura™ Agent Desktop using their credentials and all contacts to the agent are then presented to that Agent Desktop. Independently of agent configuration in CCMA, you must configure the contact center PABX to route phone calls to hotdesking agents.

Avaya Aura™ Contact Center supports agent hotdesking on the following PABX switches:

- The Avaya Aura™ Unified Communications platform
- Avaya Communication Server 1000 (CS 1000)

For more information on configuring hotdesking in an Avaya Aura™ Unified Communications platform based contact center, see Avaya Aura™ Hotdesking (page 79).

For more information on configuring hotdesking in an Avaya Communication Server 1000 based contact center, see CS 1000 Hotdesking configuration (page 81).

Supported contact types

SIP-enabled contact centers with a Contact Center Multimedia server support the following new contact types:

- Fax messages
- Scanned Document messages
- SMS Text messages
- Voice mail messages

SIP-enabled contact centers with a Contact Center Multimedia server support the following complete list of contact types:

- Voice contacts
- E-mail messages
- Instant Message, supported only on a Microsoft Office Communications Server (OCS) SIP system
- Web Communications

- Fax messages
- Scanned Document messages
- SMS Text messages
- Voice mail messages

SIP-enabled Contact Center feature limitations

SIP-enabled Contact Centers have the following limitations:

- Call Forward (CFW) is not supported. CFW must be disabled on Agent phones. Call Forward is not supported on Agent phones. Call Forward All Calls and Call Forward No Answer are not supported. The Call Presentation Class of Service settings may be used to direct calls back to the application.
- Each Avaya Communication Server 1000 Agent phone supports a single key.
- Emergency key is not supported.
- Trunk information in Historical Reports is not supported.
- Host Enhanced Routing is not supported.
- The "Let call ring" Presentation class is not supported.
- The Instant Messaging CDN alias and number must be configured the same.

Introduction

This document introduces SIP-enabled contact centers and describes the steps to configure a SIP-enabled Avaya Aura™ Contact Center.

Avaya Aura™ Contact Center supports SIP-enabled contact centers based on the following PABX switches:

- Avaya Aura™ Unified Communications platform
- Avaya Communication Server 1000 (CS 1000)

This section introduces SIP, and describes how to integrate Avaya Aura™ Contact Center with the Avaya Aura™ Unified Communications platform or an Avaya CS 1000 to build a SIP-enabled contact center. This section also compares traditional TDM-based contact centers to SIP-enabled contact centers to assist sites converting from legacy TDM installations.

- Introduction to SIP (page 9)
- SIP-enabled contact center using the Avaya Aura™ Unified Communications Platform (page 9)
- SIP-enabled contact center using Avaya CS 1000 (page 13)
- TDM-based contact center (page 15)

SIP-enabled contact centers with a Contact Center Multimedia server can support multimedia contact types such as e-mail. SIP-enabled contact centers with a Microsoft Office Communications Server (OCS) can also support Instant Messaging.

Introduction to SIP

Session Initiation Protocol (SIP) is a signaling protocol widely used to control multimedia communication sessions such as voice and video calls over Internet Protocol (IP). SIP works in the application layer of the Open Systems Interconnection (OSI) communications model. SIP can establish multimedia sessions or Internet telephony calls, and modify, or terminate them. SIP is designed to be independent of the underlying transport layer. It is a text-based protocol, incorporating many elements of the Hypertext Transfer Protocol (HTTP) and the Simple Mail Transfer Protocol (SMTP) for direct inspection by administrators.

SIP-enabled contact center using the Avaya Aura™ Unified Communications Platform

Avaya Aura™ Contact Center uses industry-standard SIP and CSTA (TR/87 over SIP) interfaces to communicate with the outside world. The Avaya Aura™ Unified Communications platform supports these SIP-enabled interfaces.

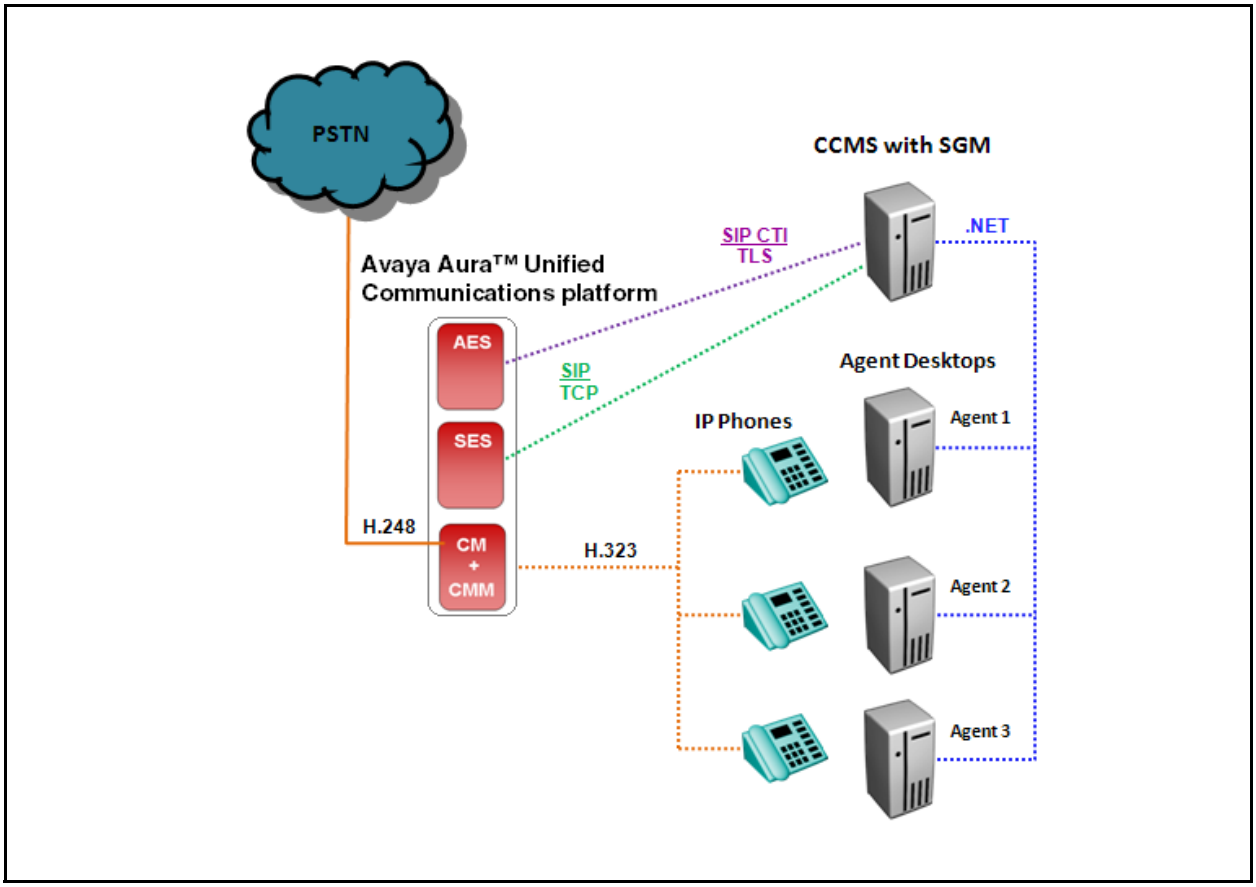
Integrating Contact Center with the Avaya Aura™ Unified Communications platform using SIP infrastructure supports multi-nodal communication between customers and contact center agents. This integration gives Contact Center access to and control of Avaya Aura™ phones. Avaya Aura™ benefits from Contact Center skill-based routing, call treatments, reporting, and the graphical Service Creation Environment. Avaya Aura™ Agent Desktop supports Avaya Aura™ phones and continues to support voice, e-mail, and Web chat contact types.

You must configure the following Avaya Aura™ Unified Communications platform components to work with Contact Center:

- Avaya Aura™ Communication Manager (CM)
- Avaya Aura™ SIP Enablement Services (SES)
- Avaya Aura™ Application Enablement Services (AES)

Avaya Aura™ System Platform is a real-time virtualization technology that enables unmodified versions of Avaya Communication Manager, SIP Enablement Services, and Application Enablement Services to be deployed on a single server. The following diagram shows a typical SIP-enabled contact center based on an Avaya Aura™ Unified Communications platform.

SIP-enabled contact center using the Avaya Aura™ Unified Communications platform



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

Integrating Avaya Aura™ Contact Center with the Avaya Aura Communication Manage using SIP infrastructure supports multi-nodal communication between customers and contact center agents. This integration gives Contact Center access to and control of Avaya Aura™ stations (phones).

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

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

Avaya Aura™ Application Enablement Services (AES) are a set of enhanced telephony APIs, protocols, and Web services. These applications support access to the call processing, media, and administrative features available in Communication Manager. They enable off-the-shelf and custom integration with communications and business applications such as Microsoft Office Communicator, as well as a broad range of Call Center, Call Recording, and Click-to-Dial applications.

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

You can obtain a root certificate from your Certificate Authority. A root certificate is an unsigned public key that identifies the Root Certificate Authority (CA). Add the root certificate to the AES server and then use it to generate a Certificate Signing Request (CSR). Send the CSR and the Common Name (CN) of the AES server to your CA. The CA verifies the identity of the request and issues a signed certificate (a private key) for use by the AES server.

You must apply the root certificate and the signed client certificate from your Certificate Authority to the AES server. If using the same Certificate Authority on the Avaya Aura™ Contact Center then you can apply the same root certificate to Contact Center. The Contact Center, like the AES server, must then generate a Certificate Signing Request (CSR) and get it signed by a Certificate Authority before it can establish a secure TLS SIP link. The AES and Contact Center can then communicate securely using a TLS SIP connection.

In an Avaya Aura™ Contact Center and Avaya Aura™ Unified Communications platform integration, Microsoft Office Communications Server (OCS) is not supported. Therefore, in this environment Instant Messaging and Presence are not supported.

For more information about configuring an Avaya Aura™ Unified Communications platform based contact center, see *Avaya Aura™ Contact Center Configuration – Avaya Aura™ Unified Communications Platform Integration* (NN44400-521).

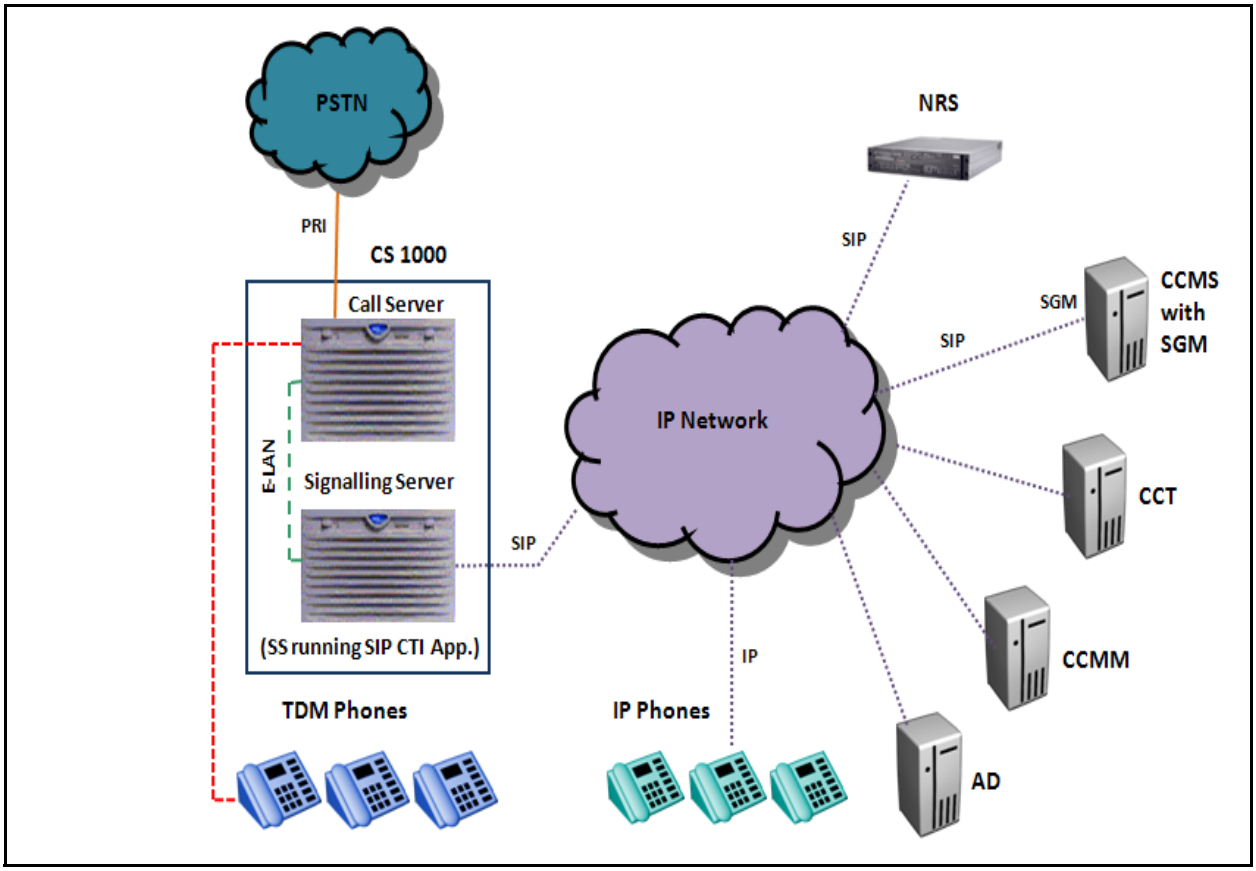
SIP-enabled contact center using Avaya CS 1000

Avaya Communication Server 1000 (CS 1000) uses an additional server, called a Signaling Server (SS) to handle SIP signaling. The Signaling Server connects to the Call Server via a local ELAN. The Signaling Server converts traditional signals like PRI DCHs into new interfaces such as SIP trunks and SIP CTI (TR87/CSTA). The SS has two network interfaces to support this functionality, one connecting to the ELAN and the other connecting to the TLAN/IP network.

CCMS uses a SIP Gateway Manager (SGM) component to support SIP. SGM is a CCMS component that communicates with the outside world using the SIP protocol. The CCMS SGM is a stand-alone SIP element that can receive and process IP calls without help from an Avaya Communication Server 1000. The CCMS SGM is the call processor in the contact center.

A SIP CTI application on the Signaling Server (SS) looks like a TAPI application from a CS point of view. The SIP CTI application acquires and controls phones, and uses an ELAN configuration in the same way as any TAPI application would. The SIP CTI application communicates via SIP, with CSTA (TR87) on the IP side. The following diagram shows a typical SIP-enabled contact center based on an Avaya Communication Server 1000.

SIP-enabled contact center using Avaya CS 1000



SIP-enabled contact centers do not need an ACD, CDN, or ACD phones on the Avaya Communication Server 1000. Calls can originate anywhere in the SIP network. In smaller deployments, calls typically enter via a PRI link into the Avaya Communication Server 1000. The Avaya Communication Server 1000 uses DSP to convert TDM calls into IP and tandems these IP calls for processing to the SIP-enabled contact center. When incoming PSTN trunk calls need to be processed by the SIP-enabled contact center, the Avaya Communication Server 1000 SS converts them from TDM into IP and tandems them onto the SIP-enabled contact center.

Avaya standard dialing plans incorporate the SIP-enabled contact center into the overall dialing plan setup.

CDNs and SIP Route Points

In a legacy TDM contact center, a CDN and associated Agents are configured on the Avaya Communication Server 1000 Call Server. When the CCMS starts up, it acquires the CDN (associated agents) using the TDM link into the Avaya Communication Server 1000.

In a SIP-enabled contact center, the CDN (called a Route Point in SIP) is not on the Avaya Communication Server 1000, so nothing is acquired. The CCMS SIP Gateway Manager (SGM) emulates and controls SIP Route Points configured in CCMA.

Networking Routing Service

Networking Routing Service (NRS) is a software application running on Avaya Communication Server 1000 Signaling Server or on a stand-alone Commercial Off The Shelf (COTS) server.

Two types of NRS are available: SIP Redirect Server (SRS), and SIP Proxy Server (SPS).

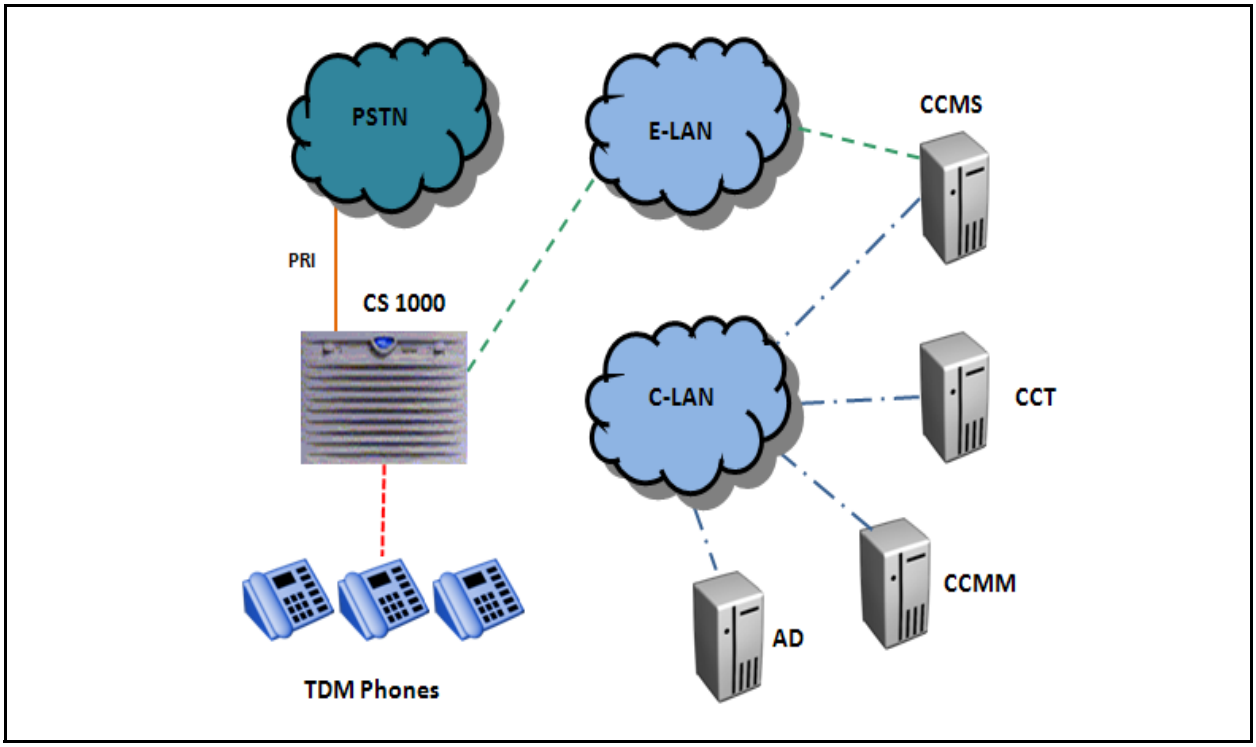
The NRS provides routing services to SIP compliant devices. The Avaya Communication Server 1000 needs an NRS to route calls to the SIP-enabled contact center. The SIP-enabled contact center (CCMS SGM) can route voice calls to contact center agents via the NRS.

SIP-enabled contact center is installed in an environment that supports Converged Office. Although Converged Office is not mandatory, the Office Communications Server and the Avaya Communication Server 1000 must be able to support it, as a SIP-enabled contact center employs the same interfaces, such as SIP trunking (TCP) and SIP Computer Telephony Integration (CTI) for Remote Call Control (RCC).

TDM-based contact center

Avaya Communication Server 1000 uses a Call Server (CS) to handle traditional Time-Division Multiplex (TDM) telephony. Traditional TDM-based phones connect directly to this Call Server. In TDM-based contact centers the Contact Center Manager Server (CCMS) controls the Avaya Communication Server 1000 contact center calls by controlling a Controlled Directory Number (CDN). The CCMS communicates with the Avaya Communication Server 1000 Call Server over an embedded network (ELAN). Each CCMS requires a dedicated Avaya Communication Server 1000 to handle contact center calls. Using a CCMS to control contact center calls ensures CCMS can support skill-based routing, call treatments, and reporting. The following diagram shows a typical TDM-based contact center.

TDM-based contact center



Prerequisites

- Ensure you have the most recent documentation. Documentation is available on the Avaya Web site at www.avaya.com/support.
- Read *Avaya Aura™ Contact Center Fundamentals* (NN44400-110).
- Read *Avaya Aura™ Contact Center Planning and Engineering* (NN44400-210).
- Read *Avaya Aura™ Contact Center Configuration – Avaya Aura™ Unified Communications Platform Integration* (NN44400-521).
- Install the Office Communications Server. For more information, see your Microsoft documentation.
- Install and commission the following Contact Center components required for SIP-enabled contact center:
  - Contact Center Manager Server
  - Contact Center License Manager
  - Contact Center Manager Server Utility
  - Contact Center Manager Administration
  - Media Application Server
  - Communication Control Toolkit

— Contact Center Multimedia

For more information about installing and commissioning Contact Center components, see *Avaya Aura™ Contact Center Installation* (NN44400-311) and *Avaya Aura™ Contact Center Commissioning* (NN44400-312).

Navigation

- Avaya Communication Server 1000 configuration (page 19)
- Office Communications Server configuration (page 27)
- Contact Center Manager Server configuration (page 31)
- CCMS certificate management (page 41)
- Media Application Server configuration (page 51)
- Communication Control Toolkit configuration (page 65)
- Agent Desktop deployment (page 75)
- SIP-enabled contact center testing (page 83)

Avaya Communication Server 1000 configuration

This section describes how to configure the Avaya Communication Server 1000 for a SIP-enabled contact center.

This section also describes how to configure the Avaya Communication Server 1000 to continue processing calls if the SIP-enabled contact center is taken off line for maintenance, or in the unlikely event of an outage.

Prerequisites to Avaya Communication Server 1000 configuration

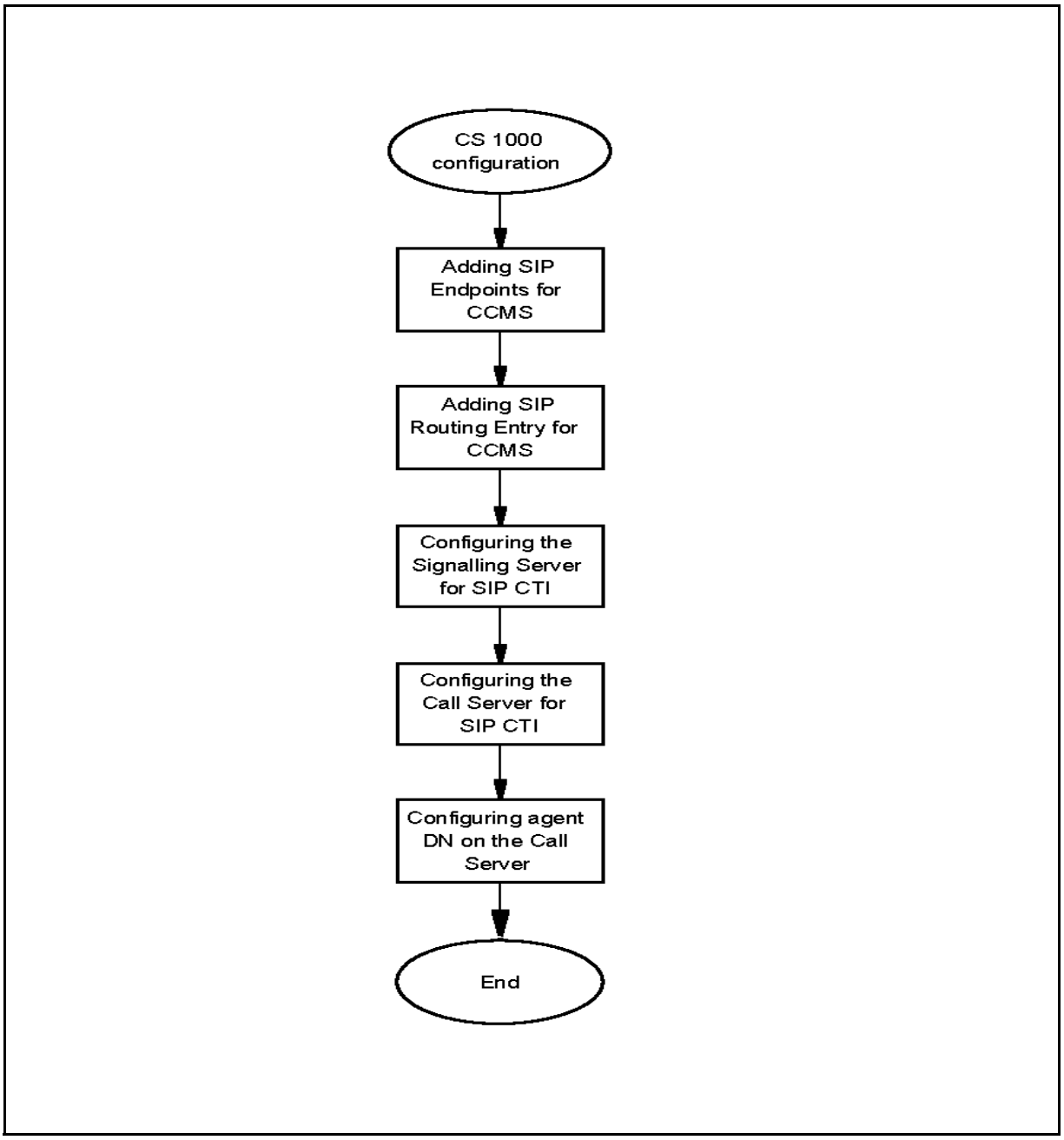
- You should be familiar with IP Telephony, including SIP Trunking and TR87 CTI on the Avaya Communication Server 1000.
- Engineer the Avaya Communication Server 1000 system so it can support SIP, in particular DSP hardware resources to support TDM/IP transcoding. Incoming PSTN calls require one DSP for each call. Agents with TDM phones will each require another DSP. For more information, see *Communication Server 1000M Large System Planning and Engineering* (NN43021-220) and *Communication Server 1000E Planning and Engineering* (NN43041-220).
- Obtain suitable licenses and packages for SIP trunking, T87A Class of Service (CLS), and SIP CTI services.
- Configure SIP trunking and SIP CTI in the same way you configure Converged Office. For more information, see *Converged Office Fundamentals — Microsoft Office Communications Server 2007* (NN43001-121).
- Configure a dialing plan (CDP or UDP) using Element Manager or Avaya Communication Server 1000 overlays. A dialing plan is required to route calls from the Avaya Communication Server 1000 towards the SIP-enabled Contact Center Manager Server. Typically, this configuration occurs through the SIP trunk towards the Network Routing Service (NRS).

Avaya Communication Server 1000 configuration procedures

This task flow shows the sequence of procedures you perform to configure the Avaya Communication Server 1000 for a SIP-enabled contact center.

To link to any task, go to Avaya Communication Server 1000 configuration navigation (page 21).

Avaya Communication Server 1000 configuration procedures



Avaya Communication Server 1000 configuration navigation

- Adding SIP endpoints for Contact Center Manager Server (page 21)
- Adding SIP Routing Entry for Contact Center Manager Server (page 22)
- Configuring the Signaling Server for SIP CTI (Remote Call Control) (page 23)
- Configuring the Call Server for SIP CTI (Remote Call Control) (page 24)
- Configuring Agent DN with SIP CTI (RCC) on the Call Server (page 24)

Adding SIP endpoints for Contact Center Manager Server

Add Contact Center Manager Server as a static endpoint to the Network Routing Services (NRS). Then the routing entries are added, because dynamic registration is not yet supported. Routing entries enable the NRS decide, based on received REQUEST URIs, when to forward calls to the new Contact Center Manager Server endpoint.

Various types of Network Routing Services are available for the Avaya Communication Server 1000, such as SIP Redirect Server (SRS) or SIP Proxy Server (SPS).

Procedure steps

Step	Action
1	Log on to the NRS.
2	In the navigation pane, expand the **Numbering Plan** option.
3	Click **Endpoints**, **Gateway Endpoints**.
4	Under Managing, click **Standby database**.
5	In the **Limit results to Domain**, select the appropriate domain from the **All service domains** list.
6	In the **Limit results to Domain**, select the appropriate domain from the **All L1 domains** list.
7	In the **Limit results to Domain**, select the appropriate domain from the **All L0 domains** drop-down list. The new Endpoint is added to this domain and the Add button is enabled.
8	Click **Add**.
9	In the **End point name** box, type the name of the Contact Center Manager Server.
10	In the **Description** box**,** type a descriptive name for the CCMS in your Contact Center.

11 In the **Endpoint authentication enabled** list, select **Authentication off**.

12 Scroll down to find the Static endpoint address field.

13 In the **Static endpoint address** box, type the IP address of the Contact Center Manager Server.

14 From the **SIP support** list, select Static **SIP** endpoint.

15 Select **TCP transport enabled.** (UDP may also be selected, TLS is not yet supported).

16 Click **Save**.

17 In the left pane, click **System, Database**.

18 Click **Cut over**.

19 Click **Commit**.

--End--

Adding SIP Routing Entry for Contact Center Manager Server

Routing entries ensure the NRS can decide when to forward calls to the Contact Center Manager Server endpoint.

This procedure outlines how to add a SIP Routing Entry for Contact Center Manager Server on the NRS.

Prerequisites

- Know the dialling plan entry.

Procedure steps

Step	Action
1	Log on to the NRS.
2	In the navigation pane, expand the **Numbering Plan** option.
3	Click **Routes**, **Gateway Endpoint**.
4	Under **Managing** click on the **Standby database**.
5	In the **Limit results to Domain,** select the appropriate domain from the **All service domains** list.
6	In the **Limit results to Domain**, select the appropriate domain from the **All L1 domains** list.
7	In the **Limit results to Domain**, select the appropriate domain from the **All L0 domains** list.
8	Click **Add**.

9	In the **DN type** list, select the appropriate Dial Plan.
10	In the **DN prefix** box, type the required prefix to integrate your Contact Center solution into your Dial Plan.
11	Enter a **Route cost** to support least-cost routing, usually 1.
12	Click **Save**.
13	In the left pane, click **System, Database**.
14	Click **Cut over**.
15	Click **Commit**.

--End--

Configuring the Signaling Server for SIP CTI (Remote Call Control)

You can use SIP CTI to control and monitor an Avaya Communication Server 1000 DN, if that DN has the TR87 class of service (CLS) and key 0 or 1 has AST applied.

This procedure outlines configuring the SIP Signaling Server for SIP CTI (Remote Call Control) and enabling the SIP CTI services configuration.

Prerequisites

- The Signaling Server must be reset for the following changes to take effect.

Procedure steps

Step	Action
1	Log on to Element Manager of the Signaling Server.
2	In the left pane, click **System**, **IP Network**, **Nodes: Servers, Media Cards**.
3	Click **Edit**.
4	In the right pane, expand the **SIP CTI Services** heading.
5	Select the **Service Enabled** check box.
6	Clear the **Support TLS Endpoints Only** check box.
7	Under **CTI Settings,** from the **Maximum Associations per DN** list, select the maximum number of associations for each DN. Avaya recommends that you configure this value as 2 or greater.
8	Click **Save and Transfer**.

--End--

Configuring the Call Server for SIP CTI (Remote Call Control)

The following example demonstrates how to configure the Call Server for SIP CTI remote call control. This procedure uses an example from a Release 5.0 CP-PM system.

This procedure outlines how to add a new elan and vas for SIP CTI using Avaya Communication Server 1000 overlay 17.

Procedure steps

Step	Action	
1	>ld 17	
	REQ chg	
	TYPE adan	
	ADAN new elan **36**	**<- Must be over 35 because it is virtual**
	CTYP elan	
	DES elan	
	LCTL	
	...	
	ADAN DATA SAVED	
	ADAN	
	...	
	REQ chg	
	TYPE vas	
	VAS new	
	VSID **36**	
	ELAN **36**	
	SECU yes	
	INTL	
	MCNT	
	VSID	
	VAS	

--End--

Configuring Agent DN with SIP CTI (RCC) on the Call Server

This procedure outlines how to configure agent DN with SIP CTI remote call control on the Call Server. This procedure uses an example from a Release 5.0 CP-PM system.
SIP CTI is used to control and monitor an Avaya Communication Server 1000 DN with T87A CLS, specified with key 0 or 1 via the AST prompt.

Prerequisites

- Create Agent DNs with T87A class of service (CLS) and AST key.

Procedure steps

Step	Action
1	Configure the Call Server as shown in the following example:

```
>ld 11

REQ: new
TYPE: 2004p1
TN   160 0 15 29
DES 2004p1
CUST 0
NUID
......
SFLT
CAC_MFC
CLS t87a              <- Use t87a Class of Service for SIP
HUNT
SCI
PLEV
DANI
AST 1                 <- May also be 0
IAPG
ITNA
MLWU_LANG
MLNG
DNDR
KEY 00 scr 50509      <- Key zero is SCR
MARP
CPND
VMB
KEY
```

--End--

Office Communications Server configuration

This section describes how to configure the Microsoft Office Communications Server (OCS) 2007.

For OCS environments with multiple OCS Enterprise Edition pools or Standard Edition Front End (FE) servers, you must configure these settings for each pool or FE server. A static route configured on one pool or one FE server is not visible to other pools or FE servers in the domain.

For federated users to access the SIP-enabled contact center where OCS edge servers and OCS directors are employed, apply this configuration to the OCS directors as well.

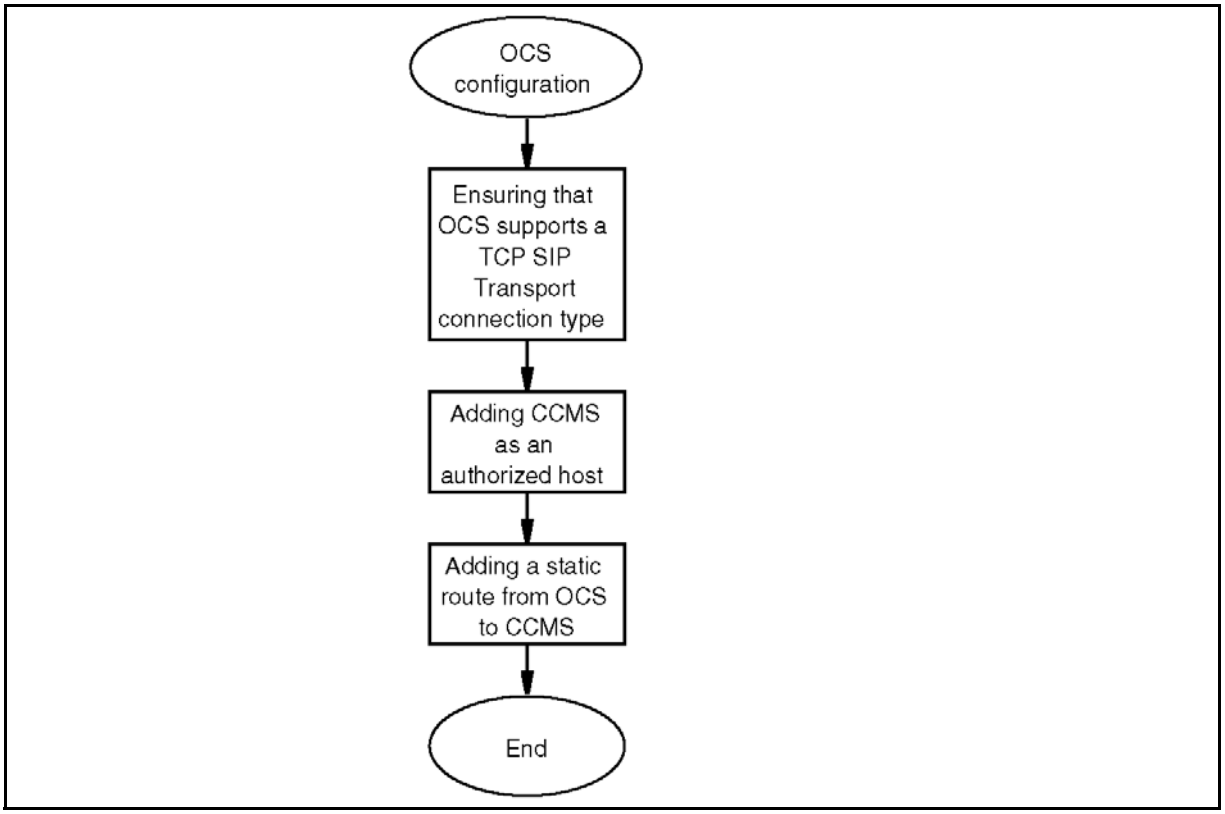
For nonfederated instant messaging, the static route matching URI can be any string. For federated IM, the wildcard must be the same as the service domain or the domain that is federated with third-party organizations.

Attention: In an Avaya Aura™ Contact Center and Avaya Aura™ Unified Communications platform integration, Microsoft Office Communications Server (OCS) is not supported. Therefore, in this environment Instant Messaging and Presence are not supported.

Office Communications Server configuration procedures

This task flow shows you the sequence of procedures you perform to configure the Office Communications Server. To link to any task, go to Office Communications Server configuration navigation (page 28).

Office Communications Server configuration procedures



Office Communications Server configuration navigation

- Ensuring that OCS supports TCP SIP Transport connection type (page 28)
- Adding Contact Center Manager Server as an authorized host (page 29)
- Adding a static route from OCS to Contact Center Manager Server (page 30)

Ensuring that OCS supports TCP SIP Transport connection type

Ensure that OCS supports TCP SIP Transport connection type to enable OCS to communicate with SIP-enabled contact center.

Procedure steps

Step	Action
1	Open the Microsoft Office Communications Server 2007 console snap-in.
2	Expand the tree.
3	Click the SIP Contact Center OCS server.

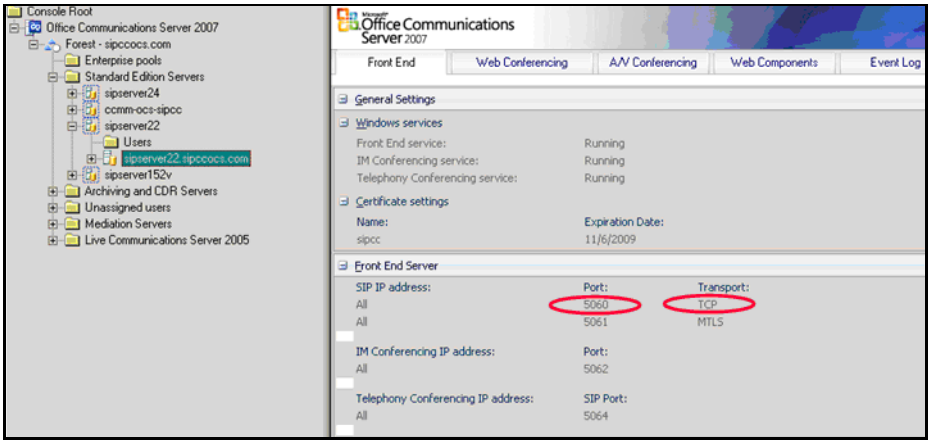
4 In the **Front End Server** section, ensure that **5060** appears under **Port** and the **TCP** appears under **Transport**.

--End--

Procedure job aid

The following figure shows an Office Communications Server configured for TCP SIP Transport type.

OCS 2007



Adding Contact Center Manager Server as an authorized host

Add the Contact Center Manager Server as an authorized host on the Office Communications Server to enable communication between the two.

Procedure steps

Step	Action
1	Open the Microsoft Office Communications Server 2007 console snap-in.
2	Expand the tree.
3	Click the **Front Ends** folder.
4	Right-click the OCS server, and then select **Properties**.
5	On the **Front End Properties** dialog box, click the **Host Authorization** tab.
6	Click **Add**.
7	On the **Add Authorized Host** dialog box, select **IP address** and type the IP address of the Contact Center Manager Server.
8	Under **Settings**, select **Throttle As Server** and **Treat As Authenticated**.
9	Click **OK**.

Step	Action
10	On the **Front End Properties** dialog box, click **OK**.

--End--

Adding a static route from OCS to Contact Center Manager Server

Add a static route from OCS to Contact Center Manager Server to enable communication between the two servers.

When you add Contact Center Manager Server as a trusted node in an OCS pool, add each Front End server to the trusted list as well. This is required for instant messages that originate from Contact Center Manager Server to be routable by the Front End servers internal to the pool.

Procedure steps

Step	Action
1	Open the Microsoft Office Communications Server 2007 console snap-in.
2	Expand the tree.
3	Click the **Front Ends** folder.
4	Right-click the OCS server, and then select **Properties**.
5	On the **Front Ends Properties** dialog box, click the **Routing** tab.
6	Click **Add**.
7	On the **Add Static Route** dialog box, under **Matching URI**, in the **Domain** box, type the name for the domain. For nonfederated instant messaging, the static route matching URI can be any string. For federated IM, the wildcard can be the same only as the service domain or the domain that is federated with third-party organizations.
8	Under **Next Hop**, select **IP address** and type the IP address of the Contact Center Manager Server.
9	From the **Transport** list, select **TCP**.
10	In the **Port** box, type the port number.
11	Click **OK**.
12	On the **Front Ends Properties** dialog box, click **OK**.

--End--

Contact Center Manager Server configuration

This section describes how to configure Contact Center Manager Server in a SIP-enabled contact center. Perform these tasks using Contact Center Manager Administration. For information about configuring the CCMS TLS certification, see CCMS certificate management (page 41).

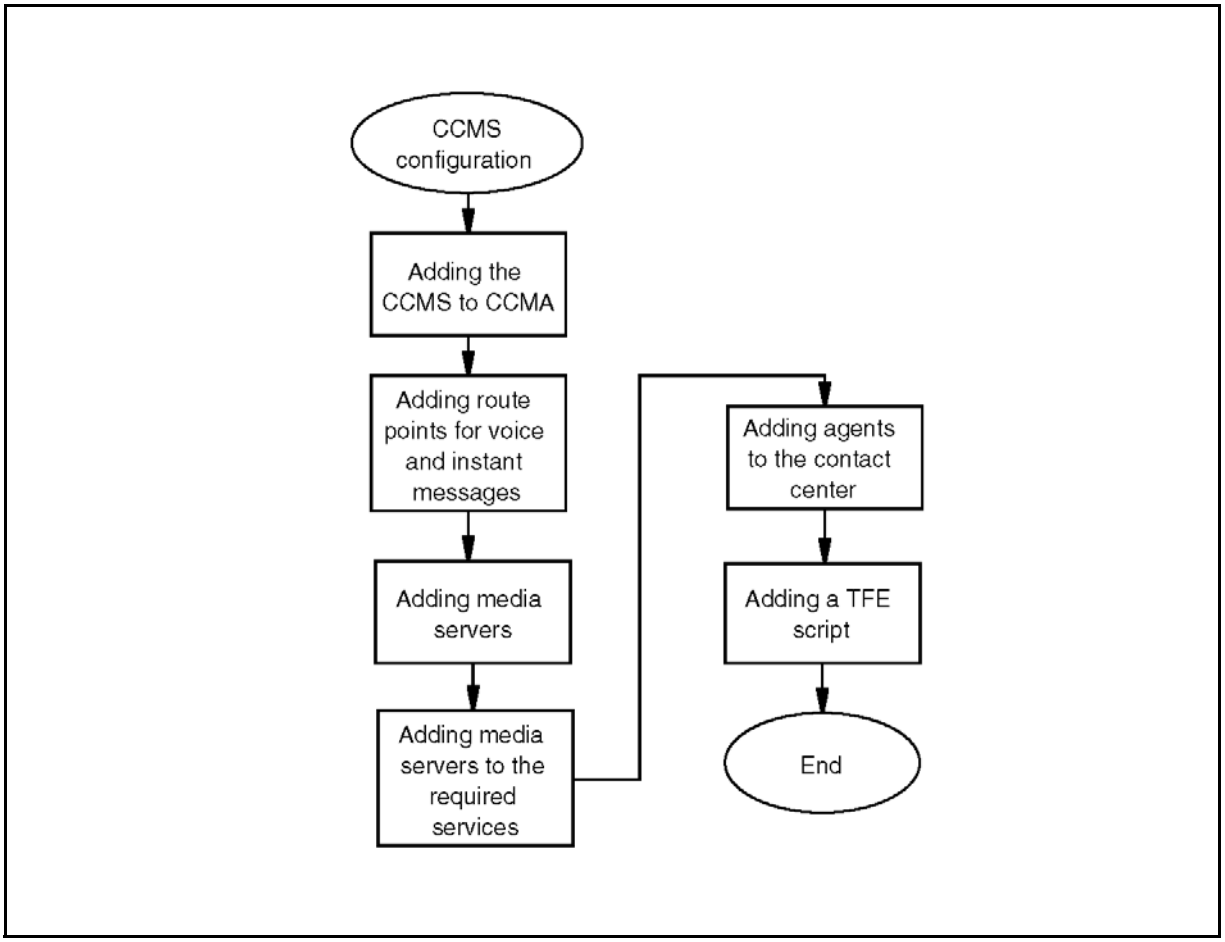
Prerequisites to Contact Center Manager Server configuration

- Install Contact Center Manager Server and Contact Center Manager Administration. For more information, see *Avaya Aura™ Contact Center Installation* (NN44400-311).

Contact Center Manager Server configuration procedures

This task flow shows you the sequence of procedures you perform to configure Contact Center Manager Server. To link to any task, go to Contact Center Manager Server configuration procedures navigation (page 32).

CCMS configuration procedures



Contact Center Manager Server configuration procedures navigation

- Adding the Contact Center Manager Server to Contact Center Manager Administration (page 33)
- Adding route points for voice and instant messages (page 33)
- Adding media servers (page 34)
- Adding media servers to the required services (page 35)
- Adding agents to the contact center (page 36)
- Adding a TFE script (page 38)

Adding the Contact Center Manager Server to Contact Center Manager Administration

Add the Contact Center Manager Server to Contact Center Manager Administration to enable communication within your contact center.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration with administrative privileges.
2	On the **Launchpad**, click **Configuration**.
3	From the menu, choose **Server**, **Add Server**.
4	In the **Server Name** box, type the computer name of the Contact Center Manager Server.
5	Press **Tab**. *The Contact Center Manager Server IP automatically appears in the IP Address box.*
6	In the **Display Name** box, type the name of the Contact Center Manager Server as you want it to appear in the system tree of Contact Center Administration. 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.
7	In the **Login ID** box, type the Login ID for the Contact Center Manager Server. The Login ID corresponds to a user account created using the Contact Center Manager Server Utility.
8	In the **Password** box, type the password for the Contact Center Manager Server.
9	From the **Type** list, select **CCMS**.
10	Click **Submit**.

--End--

Adding route points for voice and instant messages

Add route points for voice and instant message (IM) contacts

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration with administrative privileges.

2 On the **Launchpad**, click **Configuration**.

3 In the left pane, click the plus sign (+) next to the SIP-enabled Contact Center Manager Server to which you want to add the route point.

4 Select the **CDNs (Route Points)** folder.

5 On the **CDNs (Route Points)** window, in the **Name** box, type the name of the route point.

6 In the **Number** box, type the number for the route point.

7 In the **URI** box, type the value for the Uniform Resource Indicator (URI) of the route point on the SIP server.

8 From the **Call Type** list, select **Local**.

9 Select the **Acquired** check box.

10 Click any other row of the table to add and acquire the Route Point.

--End--

Variable definitions

Variable	Definition
Name	A name that describes the route point, type, or function (for example, IM_sales for an IM route point that handles sales).
Number	The number used internally by the SIP-enabled contact center that is inherited from TDM-based contact centers and appears in the TFE scripts as a CDN.
URI	The URI the SIP-enabled contact center accepts for processing by the SIP-enabled contact center. INVITEs received that do not match these URI are rejected. Avaya recommends that you use lowercase letters for URIs.
Type	Local or network. You must enable the networking option to use the Route Point for network calls.
Acquired	Select this check box to indicate to the system to acquire and process calls using this URI.

Adding media servers

Add media servers to Contact Center Manager Server using Contact Center Manager Administration.

Avaya Aura™ Contact Center uses Media Application Server media processing capabilities to support conferencing, announcements and dialogs. Each MAS in a contact center is configured in Contact Center Manager Administration as a Media Server and assigned to handle conference, announcement or/and dialogs media services.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration with administrator privileges.
2	On the **Launchpad,** click **Configuration**.
3	In the left pane, click the plus (+) sign next to the SIP-enabled Contact Center Manager Server.
4	From the list of configuration items for the Contact Center Manager Server, select **Media Servers**.
5	On the **Media Servers** window, in the **Server Name** box, type a name for the media server.
6	In the **IP Address** box, type the IP address of the MAS media server.
7	In the **Port Number** box, type the port number.

Attention: The port number must match the MAS port number. The default is 5060, your MAS might be set at 5070 for example, if MAS is co-resident with CCMS.

8	Ensure that the value for **Transport** is **TCP** or **UDP**.
9	Click **Refresh Status**.
10	On the **Save Changes** message box, click **Yes**.
11	Repeat step 1 to step 10 for each MAS media server to add.

--End--

Adding media servers to the required services

Each SIP-enabled contact center requires at least one Media Application Server (MAS) to supply the following services:

- Announcements (ANNC)
- Conferences (CONF)
- Interactive Voice Response (IVR) dialog (DIALOG)

Avaya Aura™ Contact Center uses Media Application Server media processing capabilities to support conferencing, announcements and dialogs. Each MAS in a contact center is configured in Contact Center Manager Administration as a Media Server and assigned to handle conference, announcement or/and dialogs media services.

You must assign a MAS media server for each announcement, conferencing and dialog service.

Prerequisites

- Add the media servers to Contact Center Manager Server. See Adding media servers (page 34).

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration.
2	On the **Launchpad,** click **Configuration**.
3	In the left pane, click the plus sign (+) next to the SIP-enabled Contact Center Manager Server.
4	From the list of configuration items for the Contact Center Manager Server, select **Media Services and Routes**.
5	Ensure that each of the following Contact Center services is associated with at least one MAS: • **ANNC** • **DIALOG** • **CONF**
6	Select **ANNC**.
7	Select the **Media Application Server**.
8	Select the arrow key.
9	Click **Submit**.
10	Repeat step 6 to step 9 for each service required.

--End--

Adding agents to the contact center

Add agents to the contact center. Assign the agents to skillsets and associate each with a primary supervisor.

Prerequisites

- Ensure that you have the appropriate access class to access and work in this window.
- Configure skillsets, contact types, and call presentation types in Contact Center Manager Administration. For more information, see *Avaya Aura™ Contact Center Manager Administration – Client Administration* (NN44400-611).

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration with administrator privileges.
2	On the **Launchpad**, click **Contact Center Management**.
3	In the left pane, click the Contact Center Manager Server to which you want to add the agent.
4	From the menu, choose **Add**, **Agent**.
5	In the **New Agent Details** window, enter the following mandatory information about the agent: • First Name • Last Name • Login ID • Primary Supervisor • Call Presentation • Threshold • Voice URI • IM URI
6	Enter any optional information about the agent (for example, Title, Department, or Comments).
7	If **Open Queue** is enabled on the Contact Center Manager Server, click the **Contact Types** heading to expand the branch.
8	Select the check box beside each **Contact Type** to assign to the agent (for example, Voice, IM).
9	Click the **Skillsets** heading to expand the branch.
10	In the **Skillsets** area, click **List All** to list all skillsets configured on the server.
11	From the **Priority** list for each skillset to assign to the agent, select the priority level or select **Standby** to place the agent in standby mode for this skillset.
12	If you have administrator privileges, you can add this new agent to the partitions assigned to the agent's supervisor (instead of doing so in Access and Partition Management). Click the **Partitions** heading.

The list of partitions configured on the server appears.

13 Select the check boxes beside the partitions to which to add the new agent.

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

--End--

Variable definitions

Variable	Definition
Call Presentation	The call presentation class to assign to this agent
First Name	The first name of the agent
Last Name	The last name of the agent
Login ID	The number that the agent enters to log on to the phone
Primary Supervisor	The agent's supervisor
Voice URI	The SIP address of the TR87-controlled terminal dedicated to this agent, in the format sip:agent. If using an Avaya Aura SES, use Extension@SIPdomain. Where SIPdomain is the CCMS Local SIP Subscriber Domain name. For example; sip:4400@avaya1.com If using an Avaya CS 1000, use DN@SIPdomain. Where SIPdomain is the CCMS Local SIP Subscriber Domain name. For example: sip:3280@avaya2.com
IM URI	The agent's SIP address as configured on the OCS (for example, sip:johndoe@sipccocs.com) Note: OCS is not supported in an Avaya Aura™ Unified Communications platform integration.
Threshold	The threshold class to assign to this agent

Adding a TFE script

Add a TFE script to provide treatment for contacts.

Procedure steps

Step **Action**

1 Use the Service Creation Environment (SCE) application to add a TFE script. For more information, see *Avaya Aura™ Contact Center Configuration – Service Creation Environment Application Development* (NN44400-510).

--End--

CCMS certificate management

In a SIP-enabled contact center, the Contact Center Manager Server (CCMS) enables secure communication between the Media Application Server (MAS) and the PABX platform. Avaya Aura™ Contact Center uses industry-standard SIP and CSTA (TR/87 over SIP) interfaces to communicate with the outside world. The Avaya Aura™ Unified Communications platform supports these SIP-enabled interfaces.

The SIP CTI link between CCMS and Avaya Aura™ Application Enablement Services (AES) uses the Transport Layer Security (TLS) protocol to provide secure communication. TLS uses signed security certificates to secure the link between the CCMS and the AES. The CCMS Certificate Manager can request and store these signed security certificates. CCMS Certificate Manager generates certificate signing requests (CSR). Certificate Authorities use the certificate signing requests to create a signed certificate. The Certificate Authority also supplies a root certificate. The the CCMS Certificate Manager stores signed and root certificates.

A signed certificate must be signed by a Certificate Authority, CCMS Certificate Manager does not sign certificates.

This section describes how to configure Contact Center Manager Server to communicate securely with Avaya Aura™ Application Enablement Services using a TLS SIP connection.

Attention: In a SIP-enabled contact center using an Avaya Aura™ Unified Communications platform and High Availability resiliency, the active and standby CCMS servers must both have TLS certificates in place to communicate securely with the Avaya Aura™ Unified Communications platform and to support High Availability switch-over.

For more information about configuring the Avaya Aura™ Unified Communications platform end of this secure TLS — SIP CTI link, see *Avaya Aura™ Contact Center Configuration – Avaya Aura™ Unified Communications Platform Integration* (NN44400-521).

Prerequisites

- Install Contact Center Manager Server. See *Avaya Aura™ Contact Center Installation* (NN44400-311).
- Commission Contact Center Manager Server. See *Avaya Aura™ Contact Center Commissioning* (NN44400-312).

Navigation

- Creating a certificate store using Certificate Manager (page 42)
- Generating a Certificate Signing Request file (page 44)
- Signing a Certificate Signing Request file (page 45)
- Adding a certificate file to the certificate store (page 47)
- Removing a certificate file from the certificate store (page 49)
- Examining a certificate file in the certificate store (page 49)

Creating a certificate store using Certificate Manager

The Certificate Manager creates a store that holds the private keys, signed certificates, and Certificate Authority root certificates. Create the certificate store after you install CCMS. The certificate store is password protected.

Procedure steps

Step	Action
1	Log on to the server where you want to create the certificate store.
2	Click **Start**, **All Programs**, **Avaya, Contact Center, Common Utilities**.
3	Select **Certificate Manager**.
4	In the **Certificate Manager** window, from the **Create Certificates for** list, select **SIP**.
5	In the **Certificate Store** tab, in the **Full Computer Name (FQDN) box,** type the full FQDN of the server that the certificate store is on.

Attention: The FQDN must be the full machine name of the server that the Certificate Store resides on. The FQDN name is case-sensitive.

6	In the **Name of Organizational unit** box, type the name of the department or division within the company.
7	In the **Name of Organization** box, type the company name.
8	In the **City or Locality** box, type the name of the city or district in which the contact center is located.
9	In the **State or Province** box, type the state or province in which the contact center is located.
10	In the **Two Letter Country Code** box, type the country code in which the contact center is located.
11	In the **Certificate Store password** box, type a password to access the certificate store.

12 In the **Confirm Store password** box, type a password to access the certificate store.

13 To change the password, type the password, and click **Change Password**.

14 Select **Create Store**, the private key is created. This private key is used in the private-public key encryption.

Certificate Manager automatically displays the Certificate Request tab, showing the newly created Certificate Signing Request file contents.

15 Select **Close**.

Attention: When the store has been created, the next time you start the Certificate Manager it will prompt you for a password. You must enter the correct password to access Certificate Manager features and the certificate store. If you enter an incorrect password, the Certificate Manager will start, but a no password detected message will appear if you try to access the certificate store.

--End--

Variable definitions

Variable	Value
Full Computer Name (FQDN)	The host name and parent domain which fully qualifies the computer where the certificate store is to be created. The FQDN name is case sensitive. The Certificate Manager auto-populates the FQDN field by reading the name from the operating system. You can modify this field if required. Example FQDN format: computerX.DomainY.com
Name of Organizational unit	The department or division within a company.
Name of Organization	The company name.
City or Locality	The city or district in which the system is located.
State or Province	The state or province in which the system is located.
Two Letter Country Code	The country code in which the system is located.
Certificate Store password	Choose a password to access the certificate store. The password fields have been pre-populated with a default password “__avaya” (double underscore followed by name). Avaya recommends that you change this password.

Generating a Certificate Signing Request file

The Certificate Manager automatically generates Certificate Signing Requests (CSR) when you create the store. The Certificate Manager—Certificate Request tab displays the name, location, and contents of the Certificate Signing Request (CSR) file on the server. You can e-mail this CSR file to a Certificate Authority or use your own Certificate Authority to get a signed security certificate. Contact Center uses the signed security certificate to configure a trust relationship between it and the Avaya Aura™ Application Enablement Services (AES).

If the Certificate Signing Request (CSR) is not signed straight away, the next time you log on to the Certificate Manager the CSR file will still be present and the Signing Request Status field show the CSR status as Pending. When the CSR is signed and placed into the certificate store via the Add Certificate Tab this status will change to Signed status to indicate that this CSR has been signed.

Attention: When creating certificates for Contact Center and Avaya Aura™ Unified Communications platform integration and connectivity you must use a custom certificate template. This custom certificate template is based on a Web Template but with the addition of Client and Server Authentication. For more information on creating this template, see *Avaya* Aura™ *Application Enablement Services Implementation Guide for MS LCS 2005 or MS OCS 2007* (02-601893).

Prerequisites

- Speak with your System Administrator to identify a Certificate Authority.
- Save both signed and root certificates as Distinguished Encoding Rules (DER) format using the custom AES template.

Procedure steps

Step	Action
1	Log on to server containing the store.
2	Choose **Start**, **All Programs**, **Avaya, Contact Center, Common Utilities**.
3	Select **Certificate Manager**.
4	Select **Certificate Request** tab.
5	Check the status of the Certificate Signing Request (CSR). If **Signing Request Status** is set to **Pending,** have the CSR signed by a Certificate Authority.
6	Select **Close**.

Attention: After you perform this procedure, the certificate must be signed by a Certificate Authority. Contact your System Administrator for the preferred method of processing the signed certificate request file to obtain a signed certificate. When you receive the signed certificate, save it on the server containing the Certificate Store.

--End--

Variable definitions

Variable	Value
Certificate Store Status	Indicates if the Certificate Store is created.
Signing Request Status	Indicates if the generated Certificate Signing Request that appears is signed and added back into the store. Pending: Certificate Manager is waiting for a signed certificate to be added back into the store Signed: Certificate Manager added the certificate signed by a specific Certificate Authority into the store.
File Location	Location of the Certificate Signing Request file.
Contents	Displays the contents of the Certificate Signing Request file. You can copy this directly from the field and have it signed.

Signing a Certificate Signing Request file

Certificate Signing Request (CSR) files generated by the Certificate Manager must be signed by a trusted Certificate Authority (CA) before they can be used to establish a secure communication channel with Avaya Aura™ Application Enablement Services (AES).

You can choose from many third-party Certificate Authorities. You can also promote a windows server to be a private certificate authority, but this private CA is not trusted by other companies and is trusted inside that organization sphere of influence only.

Attention: When you create certificates for Contact Center and Avaya Aura™ Unified Communications platform integration and connectivity, you must use a custom certificate template. This custom certificate template is based on a Web Template but with the addition of Client and Server Authentication. For more information about creating this template, see *Avaya* Aura™ *Application Enablement Services Implementation Guide for MS LCS 2005 or MS OCS 2007*.

This procedure is an example of using a private Certificate Authority to sign a Certificate Signing Request (CSR) file.

Prerequisites

- In the example used in this procedure, you must have your own Certificate Authority to sign Certificate Signing Request (CSR) files.
- You must have created an Avaya Aura custom certificate template.
- Copy the contents of your CSR file into your Windows clipboard.

Procedure steps

Step	Action
1	In your browser, type in <http:\\CAserverName\certsrv>, where <CAserverName> is the name of your private Certificate Authority server.
2	To access the CA server Web site, type the administrator user name and password.
3	From the **options** shown, select **Request a Certificate, Advanced Certificate Request.**
4	Select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.**
5	Copy the contents of the CSR file generated earlier into the **Saved Request** box.
6	Select the custom certificate template.
7	Click **Submit**.
8	Under **Encoding Method**, select **DER.**
9	Select the **Download certificate** link.
10	Save the file to your server, with the name **certnew.cer.**
11	This is now a signed certificate. Place this back on the server for which it is assigned.

--End--

Adding a certificate file to the certificate store

The Certificate Manager can add both signed certificates and Certificate Authority root certificates to the certificate store. There are two options when adding signed and root certificates.

Automatically adding certificates
You can select a folder that contains signed and root certificates. Certificate Manager accesses this folder and automatically determines which are signed certificates and which are root certificate and then adds them to the certificate store accordingly.

Manually adding certificates
For manually added certificates, you can browse for individual signed and root CA certificates and add them to the certificate store, one at a time. Certificate Manager checks the certificates and does not add signed certificates as root CA certificates.

Attention: Signed certificates must be in DER format. Root Certificate Authority certificates must be in Base64 format.

Prerequisites

- Save the certificate files on your certificate store computer.

Procedure steps

Step	Action
1	Log on to server containing the certificate store.
2	Click **Start**, **All Programs**, **Avaya, Contact Center, Common Utilities**.
3	Select **Certificate Manager**.
4	In **Store Access,** type the certificate store password.
5	Click **OK**.
6	In the **Certificate Manager** window, in the **Create Certificates for** list, select **SIP**.
7	Select **Add Certificate** tab.
8	Select the method to add certificates. Select **Add Certificates Automatically,** and skip to step 9. OR Select **Add Certificates Manually,** and skip to step 13.

9 Click **Browse**, and navigate to the directory that contains the certificates.

10 Select the directory.

11 Click **Add all Certificates.**

12 Skip to step 16.

13 In the **Add Root Certificate** or **Add Signed Certificate** section as appropriate, click **Browse**, and navigate to the required certificate.

14 To manually add a root certificate**,** click **Add CA Certificate**.

15 To manually add a signed certificate**,** click **Add Signed Certificate**.

16 Select **Close**.

--End--

Variable definitions

Variable	Value
Certificate Store password	Password to access the certificate store.
Add Certificates Automatically	Certificate Manager automatically determines which certificates are signed and which are root certificate and then adds them to the certificate store accordingly.
Select folder	The folder from which Certificate Manager automatically loads certificates.
Add Certificates Manually	Manually add certificates, one at a time.
Add Root Certificate	The name and location of the root certificate. Root Certificate Authority certificates must be in Base64 format.
Add Signed Certificate	The name and location of the signed certificate. Signed certificates must be in DER format.

Procedure job aid

The same root certificate must be applied to the Avaya Aura™ Unified Communications platform so that CCMS can communicate securely with it using TLS. For more information about configuring Avaya Aura™ Unified Communications platform certificates, see *Avaya Aura™ Contact Center Configuration – Avaya Aura™ Unified Communications Platform Integration* (NN44400-521).

Removing a certificate file from the certificate store

You can remove the certificates added to the store manager by using the Store Maintenance tab of the Certificate Manager.

Prerequisites

- Save the certificate files on your certificate store computer.

Procedure steps

Step	Action
1	Log on to server containing the store.
2	Click **Start**, **All Programs**, **Avaya, Contact Center, Common Utilities**.
3	Select **Certificate Manager**.
4	In **Store Access,** type the certificate store password.
5	Click **OK**.
6	In the **Certificate Manager** window, in the **Create Certificates for** list, select **SIP**.
7	Select the **Store Maintenance** tab.
8	In **Certificates,** Certificate Manager lists all certificates in the store.
9	Select the certificate to remove.
10	Select **Remove**, to remove the selected certificate from the store.
11	Select **Close**.

--End--

Variable definitions

Variable	Value
Certificate Store password	Password to access the certificate store.
Certificates	List of certificates saved in the store.

Examining a certificate file in the certificate store

View the certificates in the store using the Certificate Manager Display Certificates tab.

Prerequisites

- The certificate store must contain one of more certificate.

Procedure steps

Step	Action
1	Log on to server containing the store.
2	Click **Start**, **All Programs**, **Avaya, Contact Center, Common Utilities**.
3	Select **Certificate Manager**.
4	In **Store Access,** enter the certificate store password.
5	Click **OK**.
6	In the **Certificate Manager** window, in the **Create Certificates for** list, select **SIP**.
7	Select the **Display Certificates** tab.
8	Select **List,** to list all stored certificates in the store.
9	Select a certificate. *The details of the certificate are displayed.*
10	Select **Close**.

--End--

Variable definitions

Variable	Value
Certificate Store password	Password to access the certificate store.
Select Certificate	List of certificates saved in the store.
Certificate Detail	Display details of the certificate.

Media Application Server configuration

This section describes how to configure Media Application Server (MAS) for a SIP-enabled contact center.

Avaya Aura™ Contact Center uses the media processing capabilities of the Contact Center Services for MAS (CCSM) component to support conferencing, announcements and dialogs in SIP-enabled contact centers.

- Conference–This service creates a MAS conference and anchors customer calls, announcements, and agent calls to the MAS conference.
- Announcement–This service plays treatments (ringback, announcements) into a MAS conference.
- Dialog–This service plays and collects DTMF digits entered in the MAS conference.

Each MAS in a contact center is configured in Contact Center Manager Administration as a Media Server and assigned to handle conference, announcement or/and dialogs media services.

In SIP-enabled contact centers MAS provides default media for standard ringback and busy tones. Contact Center uses these default tones with SIP-based phone calls. Additional media for recorded announcements (RAN) and music on-hold must be provisioned in order for MAS to provide meaningful media to the customer. When adding this additional media, the Media Content Name in MAS must match the Local SIP Subscriber Domain Name in Contact Center Manager Server–Server Configuration.

In MAS Element Manager (EM), you can organize media into content namespaces and content groups. Use content namespaces to divide media into logical containers. Use content groups to subdivide the media in a content namespace into logical groups. The following example shows the structure of a typical content namespace (sipaacc.com) with four content groups, one locale specific (en_us) and three other content groups for music.

Example of media content namespace structure:

```
sipaacc.com          <= media content namespace
        | en_us      <= locale specific media content group (announcements)
        | folk       <= non-locale specific media content group (folk music)
        | pop        <= non-locale specific media content group (pop music)
        | rock       <= non-locale specific media content group (rock music)
```

MAS requires licenses for the CCSM conference, announcement, and dialog features. When installed co-resident with Contact Center Manager Server MAS uses the Contact Center License Manager, otherwise MAS uses the MAS License Server.

A SIP-enabled Contact Center solution must contain one or more MAS server. Each MAS server in a SIP-enabled Contact Center solution must be licensed and configured to provide media services.

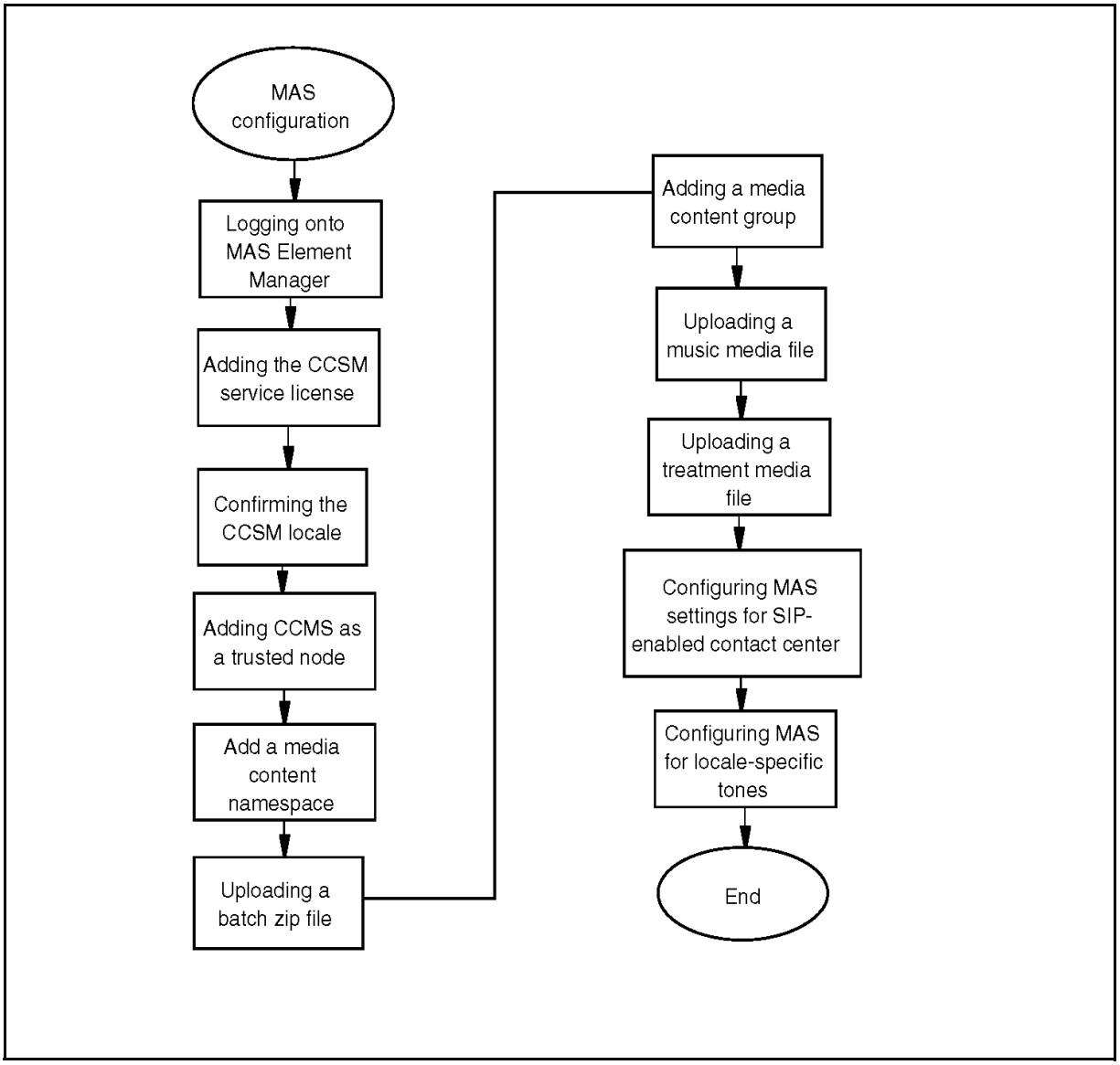
Prerequisites for MAS configuration

- Install MAS. For more information, see *Avaya Aura™ Contact Center Installation* (NN44400-311).
- Obtain a SIP-enabled contact center MAS license.

MAS configuration procedures

This task flow shows you the sequence of procedures you perform to configure the MAS. To link to any task, go to MAS configuration navigation (page 53).

MAS configuration procedures



MAS configuration navigation

- Logging onto MAS Element Manager (page 54)
- Adding the CCSM service license (page 55)
- Confirming the CCSM packaged application locale (page 55)
- Adding Contact Center Manager Server as a trusted node (page 56)
- Adding a media content namespace (page 57)
- Uploading a batch zip file (page 58)
- Adding a media content group (page 59)

- Uploading a music media file (page 59)
- Uploading a treatment media file (page 61)
- Configuring MAS settings for SIP-enabled contact center (page 61)
- Configuring MAS for locale-specific tones (page 63)

Logging onto MAS Element Manager

Log onto the MAS Element Manager as an administrator to configure MAS to support SIP-enabled contact centers.

Element Manager (EM) is a web-based administration tool that facilitates the Operation, Administration, and Maintenance (OAM) of Multimedia Application Server (MAS). A SIP-enabled Contact Center solution must contain one or more MAS server. Each MAS server in the Contact Center solution must be licensed and configured to provide media services.

Prerequisites

- Obtain a valid user name and password to access MAS Element Manager.

Procedure steps

Step	Action
1	On the MAS server desktop, double-click the **Element Manager** shortcut.
2	In the **User ID** box, type the MAS User ID log on account name. The default Element Manager User ID account name is the MAS server administrator account name.
3	In the **Password** box, type the MAS Element Manager password. The default Element Manager password is the administrator password for the MAS server.
4	Click **Log in**.

--End--

Procedure job aid

On each MAS server, the default URL to access Element Manager is:

```
https://localhost:8443/em
```

Adding the CCSM service license

MAS requires licenses for the Contact Center Services for MAS (CCSM) conference, announcement, and dialog features.

When installed co-resident with Contact Center Manager Server, MAS uses the Contact Center License Manager and the license server on MAS is disabled.

When not co-resident with Contact Center Manager Server, MAS uses the MAS License Server and the Contact Center Services for MAS (CCSM) licenses must be applied using the MAS Element Manager. When MAS is not co-resident with Contact Center Manager Server, add a license for the Contact Center Services for MAS (CCSM) services to enable contact center services on MAS.

Prerequisites

- Obtain a valid user name and password to access MAS Element Manager.
- Obtain valid license keys for the features you will use. For example, obtain MAS SIP Announcements, MAS SIP Conference, and MAS SIP Dialog license keys.

Procedure steps

Step	Action
1	Log on to Element Manager.
2	In the navigation pane, click **Licensing**, **General Settings**.
3	On the **General Settings** page, under **Licensing**, select **Use License Server**.
4	In the **Add License Keys** box, type the MAS SIP Announcements, SIP Conference, and SIP Dialog license keys.
5	Click **Validate**.
6	Click **Save**.

--End--

Confirming the CCSM packaged application locale

Avaya Aura™ Contact Center uses the media processing capabilities of the MAS Contact Center Services for MAS (CCSM) component to support conferencing, announcements and dialogs in a SIP-enabled contact center. CCSM installs a MAS Packaged Application which delivers conferencing, announcements and dialogs features on the MAS server. These features are locale specific.

For example, if the Local SIP Subscriber MS Locale in Contact Center Manager Server–Server Configuration is set to en_gb, then all CCSM packaged applications locale specific announcements and tones must also use this same locale.

Confirm the locale of the core CCSM Packaged Applications to ensure a SIP-enabled contact center receives the correct tones and announcements.

Procedure steps

Step	Action
1	Log on to Element Manager.
2	In the navigation pane, click **Applications**, **Packaged Applications**, **Contact Center**.
3	On the **Announcements** page, confirm the **Default Locale**, matches **Local SIP Subscriber MS Locale** in Contact Center Manager Server–**Server Configuration**.
4	On the **Conference** page, confirm the **Default Locale**, matches **Local SIP Subscriber MS Locale** in Contact Center Manager Server–**Server Configuration**.
5	On the **Dialog** page, confirm the **Default Locale**, matches **Local SIP Subscriber MS Locale** in Contact Center Manager Server–**Server Configuration**.

--End--

Adding Contact Center Manager Server as a trusted node

Add the Contact Center Manager Server as a trusted node to MAS using Element Manager to allow Contact Center Manager Server to interact with MAS.

This procedure is not required when MAS is installed co-resident with Contact Center Manager Server.

Prerequisites

- Obtain a valid user name and password to access MAS Element Manager.

Procedure steps

Step	Action
1	Log on to Element Manager.
2	In the navigation pane, click **System Configuration**, **Signaling Protocols**, **SIP**.
3	Click **Nodes and Routes**.

4 Click the **Trusted Nodes** link.

5 Click **Add**.

6 On the **Add SIP Trusted Node** page, in the **Host or Server Address** box, type the IP address of the Contact Center Manager Server.

7 Click **Save**.

--End--

Adding a media content namespace

In MAS Element Manager (EM), you can organize media into content namespaces and content groups. Use content namespaces to divide media into logical containers. Use content groups to subdivide the media in a content namespace into logical groups.

Prerequisites

- Create the media files for a content namespace on your local system.

Attention: You must name the root directory the same as the content namespace name.

Procedure steps

Step	Action
1	Log on to Element Manager.
2	In the navigation pane, click **Tools**, **Media Management**.
3	On the **Media Management** page, under **Content Namespace**, click **Add**.
4	In the **Name** box, type the name for the content namespace. A unique name for the namespace. The name cannot begin with the at (@) symbol. The name must be less than 128 characters and must not contain spaces.

Attention: This media content namespace is used by Avaya Aura™ Contact Center to access media services. This media content namespace must match the Local SIP Subscriber Domain Name in Contact Center Manager Server–Server Configuration.

5 Click **Save**.

6 On the **Provision Media** page, in the left pane, click the namespace to identify the specific namespace that you want to manage.

--End--

Uploading a batch zip file

Upload a batch zip file to provision media for MAS. You can then use the media to provide call treatments, such as announcements or music-on-hold.

You can initially provision a content namespace by using one .zip file for the whole content namespace or by creating one content group at a time. After the media file is uploaded, Element Manager (EM) displays it in a tree view. The root of the tree is the content namespace and individual content groups appear below it with + or - icons before their names. EM displays the namespace, and the content groups in the left pane, and the media files contained in the selected content group in the right pane. The media file list includes the file name, content type, and size of the file; the time initially created; the time last modified; and the version information. You can browse content namespaces and add, rename, or delete content groups.

To provision a single media file, see Uploading a treatment media file (page 61).

Prerequisites

- Add content namespaces. For more information about adding content namespaces, see Adding a media content namespace (page 57).
- Create the media files for a content namespace on your local system. The media files must be in the required file structure. Then zip the media files.

Attention: You must name the root directory the same as the content namespace name.

Procedure steps

Step	Action
1	Log on to Element Manager.
2	In the navigation pane, click **Tools**, **Media Management**.
3	On the **Media Management** page, select the check box next to the content namespace to which you want to add the media.
4	Click **Browse**.
5	On the **Provision Media** page, right-click the content namespace and select **Batch File Provision** on the shortcut menu.
6	On the **Batch File Provision** dialog box, click **Browse**, and then navigate to the zip file to upload.
7	Click **Always overwrite file with the same name**. **OR** Click **Do not overwrite files with the same name**.
8	Click **Upload**.

--End--

Adding a media content group

In MAS Element Manager (EM), you can organize media into content namespaces and content groups. Use content namespaces to divide media into logical containers. Use content groups to subdivide a content namespace into logical groups such as locale specific folders for announcements, or logical groups for non-locale specific media such as folk, pop, and rock music.

Add a content group to subdivide the media in a content namespace into logical groups.

Prerequisites

- Create the media content namespaces. For more information about adding content namespaces, see Adding a media content namespace (page 57).

Attention: You must name the root directory the same as the content namespace name.

Procedure steps

Step	Action
1	Log on to Element Manager.
2	In the navigation pane, click **Tools**, **Media Management**.
3	On the **Provision Media** page, in the left pane, click the namespace to identify the specific namespace in which you want to add a content group.
4	Click **Add Content Group**.
5	In the **New Content Group** dialog box, in the **Name** field, type a name for the new content group.
6	Click **Save**.

--End--

Uploading a music media file

Upload a music file to provision music for the MAS. The music file is used to provide music-on-hold. Music media files are not locale specific. Typically music media are stored in non-locale specific folk, rock or pop content groups.

Prerequisites

- Add a content namespace. For more information about adding a content namespaces, see Adding a media content namespace (page 57).
- Add a content group. For more information about adding a content group, see Adding a media content group (page 59).
- Configure and acquire a route for music/recorded announcement on the CCMS using the Configuration page of CCMA. This route name must match the 'content group' described in the steps below. For more information, see *Avaya Aura™ Contact Center Manager Administration – Client Administration* (NN44400-611).
- Add or edit a script to provide music using the SCE tool. This Route Number should match the Route Number entered in the Configuration page of CCMA. For more information, see *Avaya Aura™ Contact Center Configuration – Service Creation Environment Application Development* (NN44400-510).

Procedure steps

Step	Action
1	Log on to Element Manager.
2	In the navigation pane, click **Tools**, **Media Management.**
3	On the **Media Management** page, select the check box next to the content namespace to which you want to add music.

Attention: This Media Content Namespace is used by Avaya Aura™ Contact Center to access media services. This Media Content Namespace must match the Local SIP Subscriber Domain Name in Contact Center Manager Server–Server Configuration.

4	Click **Browse**.
5	On the **Provision Media** page, select the content group to which you want to add a music file. Typically music media are stored in folk, rock or pop content groups.
6	Click **Add Media**.
7	In the **Add Media** dialog box, click **Browse** and navigate to the music file on the server.
8	Click **Upload.**

--End--

Uploading a treatment media file

Upload a media file to provide call treatments, such as announcements. Treatment media files are locale specific and must be stored in locale specific content groups such as en_us.

Prerequisites

- Add a content namespace. For more information about adding a content namespace, see Adding a media content namespace (page 57).
- Add a content group. For more information about adding a content group, see Adding a media content group (page 59).

Procedure steps

Step	Action
1	Log on to Element Manager.
2	In the navigation pane, click **Tools**, **Media Management**.
3	On the **Media Management** page, select the check box next to the content namespace to which you want to add media.

Attention: This Media Content Namespace is used by Avaya Aura™ Contact Center to access media services. This Media Content Namespace must match the Local SIP Subscriber Domain Name in Contact Center Manager Server–Server Configuration.

4	Click **Browse**.
5	On the **Provision Media** page, select the content group to which you want to add a media file. Treatment media files are locale specific and must be stored in locale specific content groups such as en_us.
6	Click **Add Media**.
7	In the **Add Media** dialog box, click **Browse** and navigate to the media file on the server.
8	Click **Upload**.

--End--

Configuring MAS settings for SIP-enabled contact center

Configure the MAS settings to ensure MAS can provide the optimal service for the Contact Center application.

Procedure steps

Step	Action
1	Log on to Element Manager.

2 In the navigation pane, click **System Configuration**, **Media Processing**, **Media Security**.

3 On the **Media Security** page, from the **Security Policy** list, select **Security Disabled**.

4 Click **Save**.

5 In the navigation pane, click **System Configuration**, **Engineering Parameters**.

6 On the **Engineering Parameters** page, in the **Number Of Media Processing Units** box, type **1500**.

7 Click **Save**.

8 In the navigation pane, click **System Configuration**, **Media Processing**, **Video Codecs**.

9 On the **Video Codecs** page, remove all codecs.

10 Click **Save**.

11 In the navigation pane, click **System Configuration**, **Media Processing**, **Audio Codecs**.

12 On the **Audio Codecs** page, ensure that the codecs you want to support appear in the **Enabled** list.

13 Click **Save**.

14 In the navigation pane, **System Configuration**, **Media Processing**, **Digit Relay (DTMF)**.

15 On the **Digit Relay (DTMF)** page, enable **RFC2833.**

16 On the **Digit Relay (DTMF)** page, enable **INFO digits**. INFO digits must be enabled after enabling RFC2833, RFC2833 must appear first on the list.

17 Click **Save**.

18 In the navigation pane, click **System Configuration**, **Media**, **General Settings**.

19 On the **General Settings** page, clear the **QoS Monitoring** check box.

20 Click **Save**.

21 In the navigation pane, click **System Configuration**, **Signaling Protocols**, **SIP**, **General Settings**.

22 On the **General Settings** page, clear the **Enforce SIP Route Configuration** check box.

23 Click **Save**.

--End--

Configuring MAS for locale-specific tones

Each MAS installation has a set of locale-specific tones. The default tones set is United States English (en_us). The following table lists the set of installed standard locale-specific tones.

MAS locale specific tones

Tones	Language/country
de_at	German (Austria)
de_ch	German (Switzerland)
de_de	German (Germany)
en_au	English (Australia)
en_gb	English (United Kingdom)
en_ie	English (Ireland)
en_us	English (United States)
es_es	Spanish (Spain)
fr_be	French (Belgium)
fr_ch	French (Switzerland)
fr_fr	French (France)
it_it	Italian (Italy)
ja_jp	Japanese (Japan)
ko_kr	Korean (South Korea)
nl_nl	Dutch (Netherlands)
pt_br	Portuguese (Brazil)
pt_pt	Portuguese (Portugal)
sv_se	Swedish (Sweden)
zh_cn	Chinese (China)

Use this procedure to create new locale-specific tones, custom ringtones or busy tones.

Procedure steps

Step	Action
1	To update an existing locale, navigate to the locale folder on the MAS server and go to step 3.

2 To provision a new locale, create a locale folder in the MAS. You can use the en_us folder as a template: copy and rename the folder structure to the desired locale.

3 Replace ringback.wav, overflow.wav and busy.wav files in this new folder with your custom ringback.wav, overflow.wav and busy.wav files.

4 Restart the **MAS service** using the Restart option in the Element Status window.

--End--

Procedure job aid

The standard set of MAS locale-specific tones are installed in following folder:

".\MAS\Multimedia_Applications\MAS\platdata\Announcements\contactcenter\default\"

Communication Control Toolkit configuration

Use the procedures in this section to commission Communication Control Toolkit (CCT) in a SIP-enabled contact center.

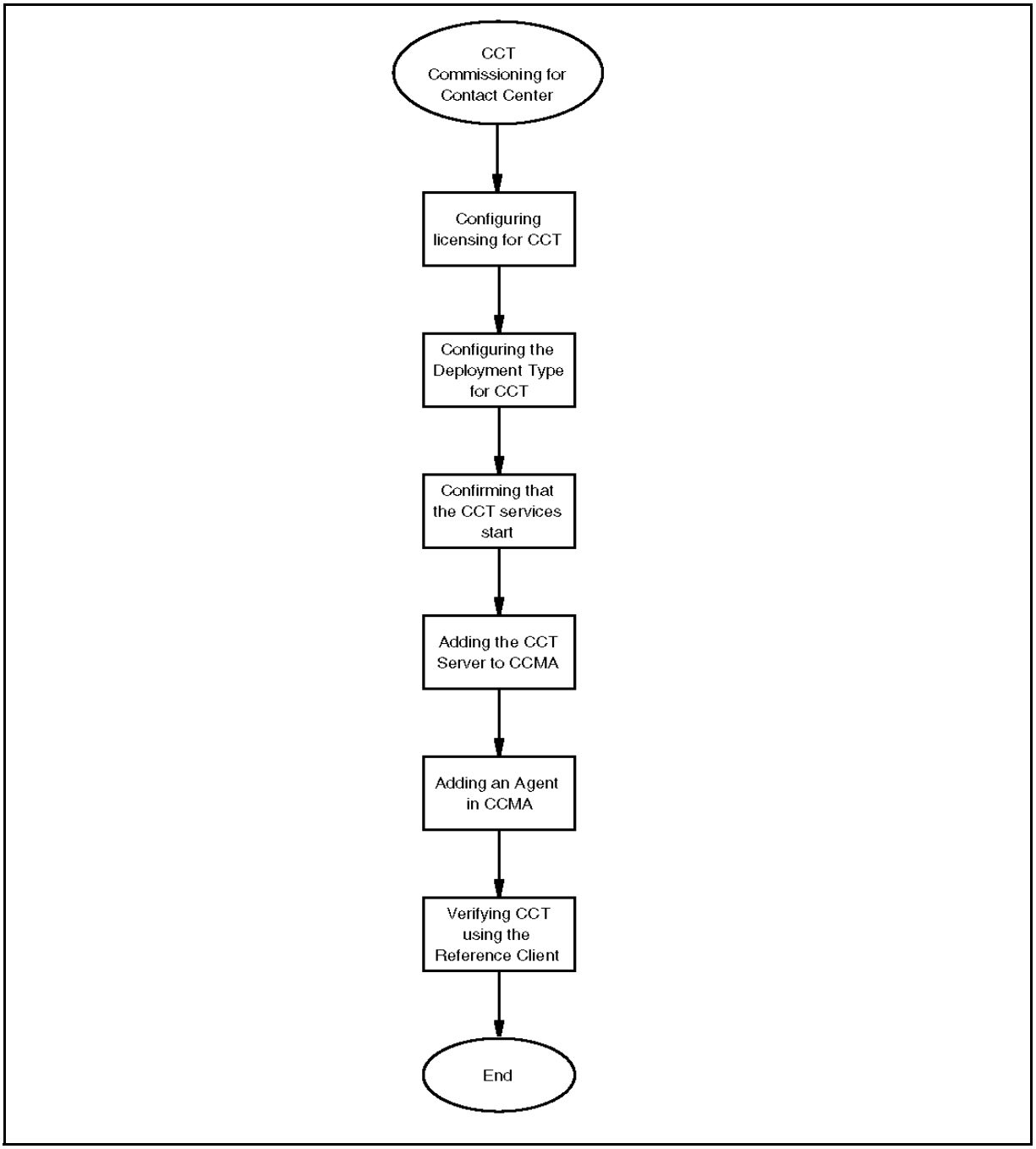
Prerequisites for Communication Control Toolkit configuration

- Install Contact Center Manager Server and Contact Center Manager Administration in the contact center. See *Avaya Aura™ Contact Center Installation* (NN44400-311).
- Commission Contact Center Manager Server and Contact Center Manager Administration. See *Avaya Aura™ Contact Center Commissioning* (NN44400-312).
- Install Communication Control Toolkit server software in your contact center. See *Avaya Aura™ Contact Center Installation* (NN44400-311).

Communication Control Toolkit configuration

This task flow shows you the sequence of procedures you perform to commission the Communication Control Toolkit in a SIP-enabled contact center environment. To link to any task, go to Communication Control Toolkit configuration navigation (page 66).

Communication Control Toolkit configuration procedures



Communication Control Toolkit configuration navigation

- Configuring the licensing for CCT (page 67)
- Configuring the deployment type for CCT (page 68)
- Confirming that the CCT services start (page 70)

- Adding the CCT Server in CCMA (page 71)
- Adding agents in CCMA (page 71)
- Verifying CCT using Reference Client (page 72)

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.

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 Contact Center 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 Contact Center License Manager is installed.

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

The CCT deployment type configuration option is disabled when CCT is installed co-resident with CCMS. If CCT is installed co-resident with CCMS, then CCT must use that 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. See *Avaya Aura™ Contact Center Commissioning* (NN44400-312).
- Know how to stop and restart the CCT services. See *Avaya Aura™ Contact Center Commissioning* (NN44400-312).

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.

Confirming that the CCT services start

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

Procedure steps

Step	Action
1	Click **Start, 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 **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

Adding the CCT Server in CCMA

To administer the CCT server from the CCMA client application, add the CCT server to CCMA then associate it with a CCMS server. This is a brief summary of the procedure. For more details, see *Avaya Aura™ Contact Center Manager Administration – Client Administration* (NN44400-611).

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.

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--

Adding agents in CCMA

Create SIP agents using CCMA and associate them with contact center windows users. This is a brief summary of the procedure. For more details, see *Avaya Aura™ Contact Center Manager Administration – Client Administration* (NN44400-611).

Prerequisites

- Ensure all required windows users are created on the domain.
- Add CCT server to CCMA configuration, see Adding the CCT Server in CCMA (page 71).
- 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 windows domain 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 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 and is not to be deployed for production contact center use.

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, enter the details of a user, enter 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--

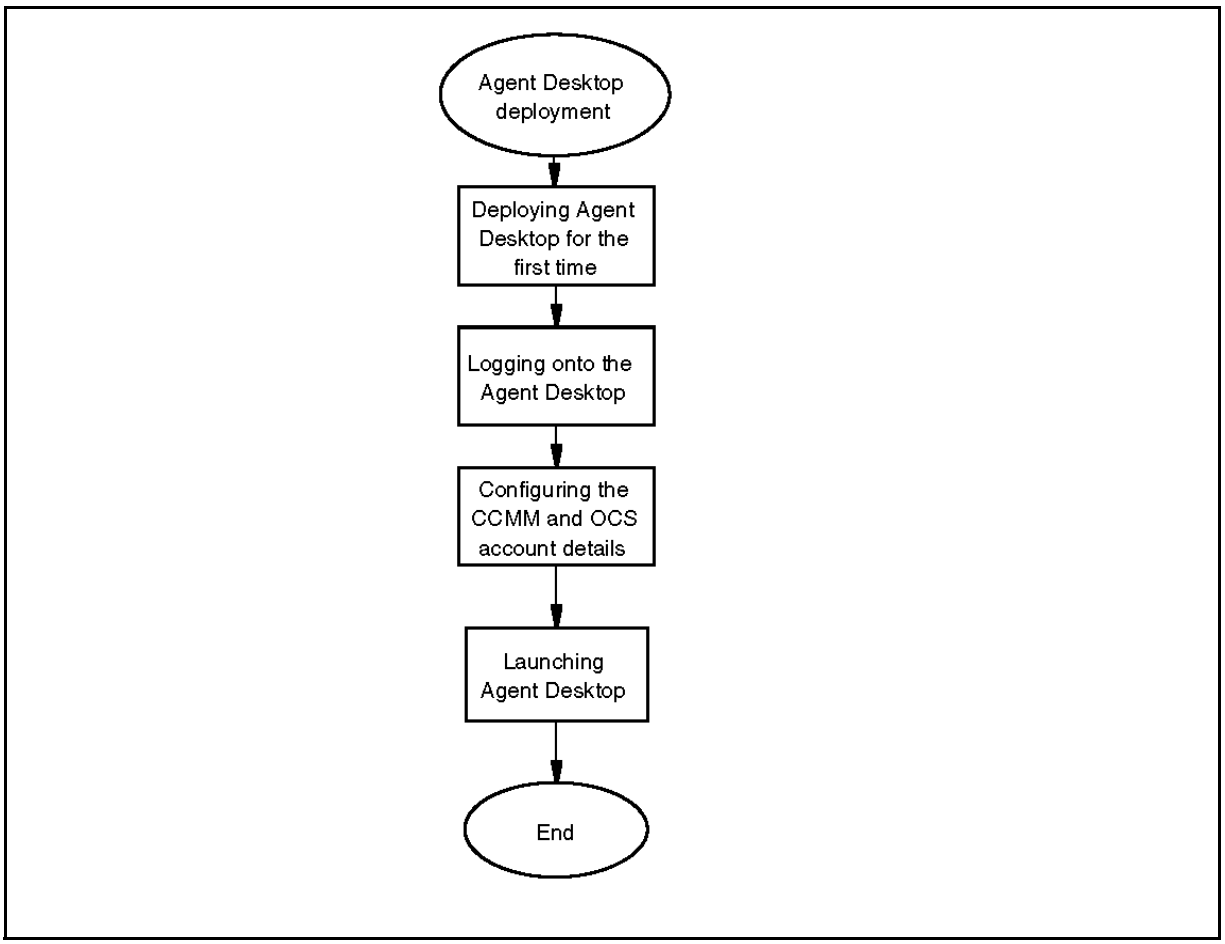
Agent Desktop deployment

This section describes how to install and configure Avaya Aura™ Agent Desktop in a SIP-enabled contact center.

Agent Desktop deployment procedures

This task flow shows the sequence of procedures you perform to configure the agent desktop for SIP-enabled contact center. To link to any task, go to Agent Desktop deployment navigation (page 75).

Agent Desktop deployment procedures



Agent Desktop deployment navigation

- Deploying Agent Desktop for the first time (page 76)
- Logging on to the Agent Desktop (page 76)

- Configuring CCMM user name and password and OCS account details (page 77)
- Launching the Agent Desktop after initial installation (page 78)

Deploying Agent Desktop for the first time

Deploy Agent Desktop for the first time to install the Agent Desktop on a client PC. When you install Agent Desktop for the first time, Agent Desktop will install the .NET 3.0 Framework and Visual C++ Runtime Libraries.

Prerequisites

- Ensure your client PCs meet all requirements as described in *Avaya Aura™ Contact Center Planning and Engineering* (NN44400-210).
- Know the fully qualified domain name (FQDN) of the Contact Center Multimedia server.
- Log on to the client PC with local administrator rights. These rights are required to install the .NET Framework and Visual C++ Runtime Library packages.

Procedure steps

Step	Action
1	On the client PC, start Internet Explorer.
2	In the address bar, type **http://<ccmm_server>/agentdesktop**, where <ccmm_server> is the FQDN of the Contact Center Multimedia server.
3	On the Agent Desktop page, click **Install Prerequisites**.
4	After the installation of the prerequisites is complete, click **Launch** Agent Desktop.

--End--

Logging on to the Agent Desktop

Log on to the Agent Desktop to connect to Communication Control Toolkit.

Prerequisites

- Install Agent Desktop on the client PC. See Deploying Agent Desktop for the first time (page 76).

Procedure steps

Step	Action
1	Start the Agent Desktop. *If the client PC is logged on using an agent's credentials, single sign-on (SSO) logs Agent Desktop into Communication Control Toolkit automatically.* *If the agent PC is not logged on, the CCT Connection Failure message box appears.*
2	On the **CCT Connection Failure** message box, click **Retry**.
3	On the **User Credentials** dialog box, in the **User ID** box, type the agent's user ID.
4	In the **Password** box, type the agent's password.
5	In the **Domain** box, type the domain name.
6	Click **OK**.

--End--

Configuring CCMM user name and password and OCS account details

Configure the CCMM user name and password and OCS account details to enable instant messaging and presence on the Agent Desktop.

Attention: In an Avaya Aura™ Contact Center and Avaya Aura™ Unified Communications platform integration, Microsoft Office Communications Server (OCS) is not supported. Therefore, in this environment Instant Messaging and Presence are not supported.

Prerequisites

- Log on to Agent Desktop. See Logging on to the Agent Desktop (page 76).

Procedure steps

Step	Action
1	On the **Enter Login Details** dialog box, in the **Multimedia account info** section, in the **ID** box, type the ID of the agent as configured on the Contact Center Multimedia server.
2	In the **Password** box, type the password for the agent as configured on the Contact Center Multimedia server.
3	In the **OCS** section, in the **Sign-in name** box, type the sign-in name for the agent.

4 In the **Password** box, type the password for the agent.

5 In the **Domain** box, type the Contact Center SIP domain (for example, sipserver.com).

6 In the **Uri** box, type the SIP URI for the agent as configured in Contact Center Manager Administration.

7 In the **Connection Settings** section, in the **Server name or IP** box, type the name or IP address of the OCS.

8 In **Connect using**, select **TCP**.

9 Click **Save this profile**.

The agent is now logged on and can use Agent Desktop to control the phone for DN calls. After the agent clicks Not Ready, the agent can receive contacts from Contact Center Manager Server.

--End--

Launching the Agent Desktop after initial installation

Launch the Agent Desktop to log on and receive contacts.

Prerequisites

- Install the Agent Desktop on the client PC. See Deploying Agent Desktop for the first time (page 76).

Procedure steps

Step	Action
1	Click **Start**, **All Programs**, **Avaya**, Agent Desktop.

--End--

Avaya Aura™ Hotdesking

This section outlines hotdesking in an Avaya Aura™ Unified Communications platform based contact center.

The Avaya Aura™ Communication Manager allows any agent to use their own credentials (extension number and password) to log on to any designated station. The Communication Manager then registers that station with the agent's extension number and the agent can receive their calls on that station's phone.

Navigation

- Logging on to an Avaya Aura™ station (page 79)

Logging on to an Avaya Aura™ station

Log on to an Avaya Aura™ station to receive your phone calls.

Procedure steps

Step	Action
1	On the Avaya Aura™ deskphone, press the **Menu** button.
2	Scroll down to the **Login** option.
3	Enter your extension number and password credentials.

--End--

CS 1000 Hotdesking configuration

This section outlines how to configure an Avaya Communication Server 1000 based and SIP-enabled contact center to support agent hotdesking using Virtual Office.

The Avaya Communication Server 1000 Virtual Office feature allows agents to log on to any designated phone and use their individual phone configurations at that phone. Phone calls to the agent are then routed to the phone where the agent is logged on.

For more information on configuring Avaya Communication Server 1000 Virtual Office, see *Avaya Communication Server 1000 Telephones and Consoles Fundamentals* (NN43001-567).

Navigation

- Logging on to Virtual Office remotely (page 81)
- Logging off of Virtual Office (page 82)

Logging on to Virtual Office remotely

Log on to Virtual Office remotely to use the features of your home office IT phone.

Prerequisites

- Apply packages 382 and 387 to your Avaya Communication Server 1000.
- On the Avaya Communication Server 1000, Station Control Password Length (SCPL) must be configured in LD 15 to enable the Station Control Password (SCPW) prompt.
- On the Avaya Communication Server 1000, the remote IP phone must have an Station Control Password (SCPW) configured in LD 11.
- The Remote Call Server must have the Virtual Office User Allowed (VOUA) Class of Service (CLS) configured in LD 11.
- The Host Call Server must have the Virtual Office Login Allowed (VOLA) Class of Service (CLS) configured in LD 11.
- You must have a working IP peer configuration and know how to dial the remote phone from the host phone.

Procedure steps

Step	Action
1	On the phone, click the **Applications** button.
2	From the menu, select **Virtual Office**.
3	At the **Enter User ID** prompt, enter the diallable DN of the target remote phone.
4	At the **Enter Password** prompt, enter the SCPW of the target remote phone. *If successful, the host phone resets and comes back online with the features of the remote IP phone, including the DN, autodial numbers, feature keys, and voice mail indication and access.*

--End--

Logging off of Virtual Office

Log off from Virtual Office to remove the features transferred to the phone when you logged on.

Procedure steps

Step	Action
1	From the **Options** menu, select **Virtual Office Logout**. *After you log off, the features that were transferred to that phone are removed.*

--End--

SIP-enabled contact center testing

This section describes how to test the SIP-enabled contact center to verify correct operation.

Navigation

- Verifying correct operation (page 83)

Verifying correct operation

Verify correct operation to ensure your SIP-enabled contact center is correctly configured.

Procedure steps

Step	Action
1	Ensure an agent phone is online.
2	Log the agent on.
3	Start the Agent Desktop.
4	Direct a voice call towards the system.
5	Ensure that the call is treated correctly as specified by the TFE script (for example, Ringback, Music on Hold, or IVR) and that the call is routed to the agent.
6	If your contact center supports Instant Messaging, direct an instant message (IM) towards the system.
7	Ensure the IM is treated correctly as specified by the TFE script (for example, automated IM prompts, IM IVR, URL push) and is routed to the agent.

--End--