Avaya Contact Center Select Advanced Administration

Release 7.0.3
Issue 02.05
July 2018

© 2015-2018, Avaya Inc.
All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. 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 CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License type(s)

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

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER’S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, 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, Hosted Service(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.

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

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction

Purpose

This guide describes the advanced configuration tasks that administrators of the Avaya Contact Center Select server can perform.

Intended audience

This guide is for personnel who perform management tasks on the Avaya Contact Center Select server.

Related resources

Avaya Contact Center Select Documentation

The following table lists the documents related to Avaya Contact Center Select. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Use this document to:	Audience
Overview		
Avaya Contact Center Select Solution Description	This document provides a technical description of Avaya Contact Center Select. It describes the product features, specifications, licensing, and interoperability with other supported products.	Customers and sales, services, and support personnel
Avaya Contact Center Select Documentation Catalog	This document describes available Avaya Contact Center Select documentation resources and indicates the type of information in each document.	Customers and sales, services, and support personnel

Table continues…

Title	Use this document to:	Audience
Contact Center Performance Management Data Dictionary	This document contains reference tables that describe the statistics and data in the historical and real-time reports generated in Contact Center.	System administrators and contact center supervisors
Implementing		
Deploying Avaya Contact Center Select DVD	This document contains information about Avaya Contact Center Select DVD installation, initial configuration, and verification. This document contains information about maintaining and troubleshooting the Avaya Contact Center Select server.	Implementation personnel
Deploying Avaya Contact Center Select Software Appliance	This document contains information about Avaya Contact Center Select Software Appliance (VMware) preparation, deployment, initial configuration, and verification. This document contains information about maintaining and troubleshooting the software appliance.	Implementation personnel
Deploying Avaya Contact Center Select Hardware Appliance	This document contains information about Avaya Contact Center Select Hardware Appliance (physical server) installation, initial configuration, and verification. This document contains information about maintaining and troubleshooting the hardware appliance.	Implementation personnel
Avaya Contact Center Select Business Continuity	This document contains information about deploying Avaya Contact Center Select Business Continuity.	Implementation personnel
Upgrading and patching Avaya Contact Center Select	This document contains information about upgrading and patching Avaya Contact Center Select.	Implementation personnel and system administrators
Administering		
Administering Avaya Contact Center Select	This document contains information and procedures to configure the users, skillsets, and contact center configuration data. This document contains information about creating Avaya Contact Center Select real-time and historical reports.	System administrators and contact center supervisors
Avaya Contact Center Select Advanced Administration	This document contains information about managing the Avaya Contact Center Select server, licensing, and multimedia configuration.	System administrators

Table continues…

Title	Use this document to:	Audience
Using Contact Center Orchestration Designer	This document contains information and procedures to configure script and flow applications in Contact Center Orchestration Designer.	System administrators
Maintaining		
Contact Center Event Codes	This document contains a list of errors in the Contact Center suite and recommendations to resolve them. This document is a Microsoft Excel spreadsheet.	System administrators and support personnel
Using		
Using Agent Desktop for Avaya Contact Center Select	This document provides information and procedures for agents who use the Agent Desktop application to accept, manage, and close contacts of all media types in Contact Center.	Contact center agents and supervisors
Using the Contact Center Agent Browser application	This document provides information and procedures for agents who use the Agent Browser application to log on to Contact Center and perform basic tasks.	Contact center agents

Finding documents on the Avaya Support website

Procedure

1. Navigate to http://support.avaya.com/.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
7. Click **Enter**.

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

  Note:

  Videos are not available for all products.

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: Changes in this release

The following sections describe the new features and changes in Avaya Contact Center Select Release 7.0 advanced administration.

Features

New features in the Release 7.0 base build

See the following sections for information about feature changes in the Release 7.0 base:

- Contact Center services secured by default on page 20

New features in Release 7.0 Feature Pack 1

See the following sections for information about feature changes in Release 7.0 Feature Pack 1:

- Instant Messaging feature supports Microsoft Skype for Business 2015 on page 20
- Provision of adding a friendly name for a web chat agent on page 20
- Server Message Block signing enabled on Windows Server 2012 on page 21
- Support for Avaya WebLM centralized licensing on page 21
- Support for the Open Queue Open Interface on page 21
- Whisper Coaching on page 21

New features in Release 7.0 Feature Pack 2

See the following sections for information about new features added by Feature Pack 2:

- Increased CCMM customer contact ratio on page 21
- Offline Security Store on page 22
- REST API integration on page 22

New features in Release 7.0 Feature Pack 3

See the following sections for information about new features added by Feature Pack 3:

- Ability to store email attachments in the database on page 22
- Contact Center database encryption on page 22
- Data Management - customer privacy on page 22
- REST API Enhancements on page 23

- Security Manager support for chained certifcates on page 23

Contact Center services secured by default

Contact Center includes a number of services and connections that you can secure using Transport Layer Security (TLS). By default, Contact Center installs commonly used Web services and CTI connections with security enabled. This feature includes enhancements to the Contact Center Certificate Management tool to make it easier to manage server and root certificates.

On a new Contact Center install, the following connections and services use TLS by default:

- Contact Center Manager Administration (CCMA)
- Contact Center Multimedia (CCMM) Administration
- Agent Desktop
- Multimedia Services
- Orchestration Designer
- Outbound Campaign Management Tool
- Contact Center Web Services
- Communication Control Toolkit (CCT) Web Administration

Turn off Contact Center security after installation and initial configuration, to quickly configure Avaya Contact Center Select (ACCS) and test a first call. If you want to use TLS security, you can then create a new security store containing a signed server certificate and root certificate from your Certificate Authority (CA).

Instant Messaging feature supports Microsoft Skype for Business 2015

From Release 7.0 Feature Pack 1, the Contact Center Instant Messaging feature integrates with Microsoft Skype for Business 2015. Integration and operation is identical with releases of Microsoft Lync already supported in the Contact Center 7.0 base release.

Provision of adding a friendly name for a web chat agent

From Release 7.0 Feature Pack 1, Contact Center administrators can add a friendly name or nickname for a web chat agent. If administrators configure the Friendly Name label, the nickname of the web chat agent is displayed in agents’ responses to web chat messages. Administrators can also choose that the friendly name is displayed in welcome messages.

Server Message Block signing enabled on Windows Server 2012

From Release 7.0 Feature Pack 1, both the Contact Center DVD and the Release Pack installer modify the Windows Server 2012 local group policy to enable Server Message Block (SMB) signing. SMB signing places a digital tag into each server message block, which helps prevent man-in-the-middle attacks on network file sharing.

If you do not want to use SMB signing, you can disable it by modifying the Windows Server 2012 local group policy.

Support for Avaya WebLM centralized licensing

From Release 7.0 Feature Pack 1, Avaya Contact Center Select (ACCS) supports Avaya WebLM centralized licensing in an ACCS Powered solution. This enables licensing multiple Avaya Contact Center Select servers from a single Avaya WebLM server.

Support for the Open Queue Open Interface

From Release 7.0 Feature Pack 1, Avaya Contact Center Select (ACCS) supports the Open Queue Open Interface.

The Open Queue Open Interface delivers existing Open Queue functions to third-party applications that use a Web service. Third-party applications can add and remove contacts of a specific type in Contact Center.

Whisper Coaching

From Release 7.0 Feature Pack 1, SIP-enabled Contact Centers extend the Supervisor Observe feature to include Whisper Coaching. Using Whisper Coaching, a supervisor can talk to an agent on a skillset call with a customer, without being heard by the customer. In the coaching mode, a supervisor can hear everything that is said on the call. However, the advice that the supervisor provides is audible only to the agent.

Whisper Coaching improves agent training and performance because supervisors can coach the agent by whispering advice to the agent.

Increased CCMM customer contact ratio

From Release 7.0 Feature Pack 2, the customer to contact ratio in Contact Center Multimedia (CCMM) has been increased to 1:1000 (or 1 customer record per 1000 contacts).

Offline Security Store

From Release 7.0 Feature Pack 2, you can create an offline store using Security Manager. This allows you to minimize downtime if you want to replace your current security store. When your offline store is created, you can swap between the active store and the offline store. You can make the offline store the active store at any point using Security Manager. You must stop Contact Center services before making the offline store active.

REST API integration

From Release 7.0 Feature Pack 2, Contact Center allows you to invoke REST API in a Contact Center workflow. REST (Representational state transfer) provides efficient scalable services for web communications.

A Contact Center workflow can request data using scripting commands, and the workflow uses the TfeRestService to request and retrieve data from the REST API.

Ability to store email attachments in the database

From Release 7.0 Feature Pack 3, there is an option to save new email attachments in the MULTIMEDIA database instead of on the file system. You can configure this option using the Multimedia Administration utility.

Contact Center database encryption

From Release 7.0 Feature Pack 3, you can encrypt and decrypt the Contact Center database using Security Manager. To encrypt the database, you must create and activate an encryption key and use it to encode the files in the Contact Center Caché database.

Data Management - customer privacy

From Release 7.0 Feature Pack 3, you can use the Multimedia Data Management utility to act on privacy requests from contact center customers. For example, if a customer exercises their right to access information or their right to be forgotten, you can use the Multimedia Data Management utility to satisfy these requests.

REST API Enhancements

From Release 7.0 Feature Pack 3, the Contact Center REST API supports GET, POST, PUT, or DELETE request methods. Using the TFE REST Configurator, you can now add environments which enable the use of environment variables in REST requests.

Contact Center workflows now support the CONVERT and JSON GET ELEMENT command.

Security Manager support for chained certifcates

From Release 7.0 Feature Pack 3, Security Manager supports importing chained certificates.

Other changes

Other changes in Release 7.0 Feature Pack 1

See the following sections for information about other changes in Feature Pack 1:

- Automated backup of new security store on page 23
- Contact Center implements Transport Layer Security version 1.2 by default on page 23
- File extension restrictions for attachments on page 24
- Multimedia account passwords must meet minimum complexity criteria on page 24
- Removal of the default Agent Desktop Dashboard password on page 25

Automated backup of new security store

From Release 7.0 Feature Pack 1, Contact Center automatically backs up a new security store when you create it. This allows you to recover from situations where the store is damaged or deleted before you make a manual backup of the store.

Contact Center implements Transport Layer Security version 1.2 by default

From Release 7.0 Feature Pack 1, Contact Center implements Transport Layer Security (TLS) version 1.2 as the default minimum version negotiated for secure communications. This is to avoid security vulnerabilities that exist in TLS 1.0.

Before migrating to Release 7.0 Feature Pack 1, ensure that the browsers you use for CCMA or Element Manager are configured to use TLS 1.2.

For backward compatibility and inter-operation with third-party or custom applications connecting to Contact Center, Administrators can set lower versions of TLS on certain communication channels. When a lower version of TLS is available, Contact Center still negotiates the highest level of TLS that the other application can support.

Before migrating from a previous Release, or before applying Feature Pack 1 to a Release 7.0 solution, check third-party or custom applications that connected securely to Contact Center, to understand whether you need to change the Contact Center TLS versions.

If you apply Feature Pack 1 to an existing Release 7.0 installation, Contact Center does not apply this change, and retains your Release 7.0 TLS configuration.

File extension restrictions for attachments

From Release 7.0 Feature Pack 1, Contact Center administrators can use the Contact Center Multimedia (CCMM) Administration utility to configure the supported list of file extensions that agents can attach to emails. When agents add a file attachment to an email, Agent Desktop displays the configured list of file attachment extensions in the Open dialog box. If the attachment type is not in the configured list, Agent Desktop displays a warning message and does not attach the file to the email.

Multimedia account passwords must meet minimum complexity criteria

From Release 7.0 Feature Pack 1, Contact Center requires multimedia accounts to meet the minimum password complexity criteria. If you are an agent or supervisor who handles multimedia contacts, Agent Desktop forces you to change your password if you log on using the default password or your password that does not meet the minimum password complexity criteria.

Passwords must fulfill the following complexity criteria:

- Must be between 8 to 20 characters
- Must contain a number
- Must contain at least one uppercase letter and at least one lowercase letter
- Must not contain spaces
- Must not contain any of these characters: \ & : < > |

Agents can change the multimedia account password using the **Preferences** tab in the User Preferences screen. Administrators also can change multimedia account passwords using the Multimedia Administration utility.

Removal of the default Agent Desktop Dashboard password

From Release 7.0 Feature Pack 1, Contact Center has removed the default password that was required to access Agent Desktop Dashboard. You can collect and upload log files or videos to the Contact Center server without entering a password.

Chapter 3: Contact Center Multimedia fundamentals

Use the Contact Center Multimedia (CCMM) Administration utility to allow Contact Center to accept a variety of contact types and route them to agents. The contact types that an agent can handle are determined by the skillsets to which the agent is assigned.

Contact types routed using Avaya Contact Center Select include the following:

- voice contacts
- email messages
- Short Message Service (SMS) text messages
- faxed documents
- scanned documents
- voice mail messages
- outbound contacts
- Web communications contacts

Contact Center License Manager licenses each contact type. You must have the appropriate license in your contact center to enable routing for each contact type.

Important:

To start the CCMM Administration utility, you must first log on to Contact Center Manager Administration (CCMA). You must log on to CCMA from a Web browser on the Avaya Contact Center Select server to access the CCMM Administration utility.

Email contact type

Use email messages to communicate with clients by using an email provider such as Microsoft Exchange. The following figure shows the life cycle of an email contact from the time it is received by the email server until it is routed to an agent.

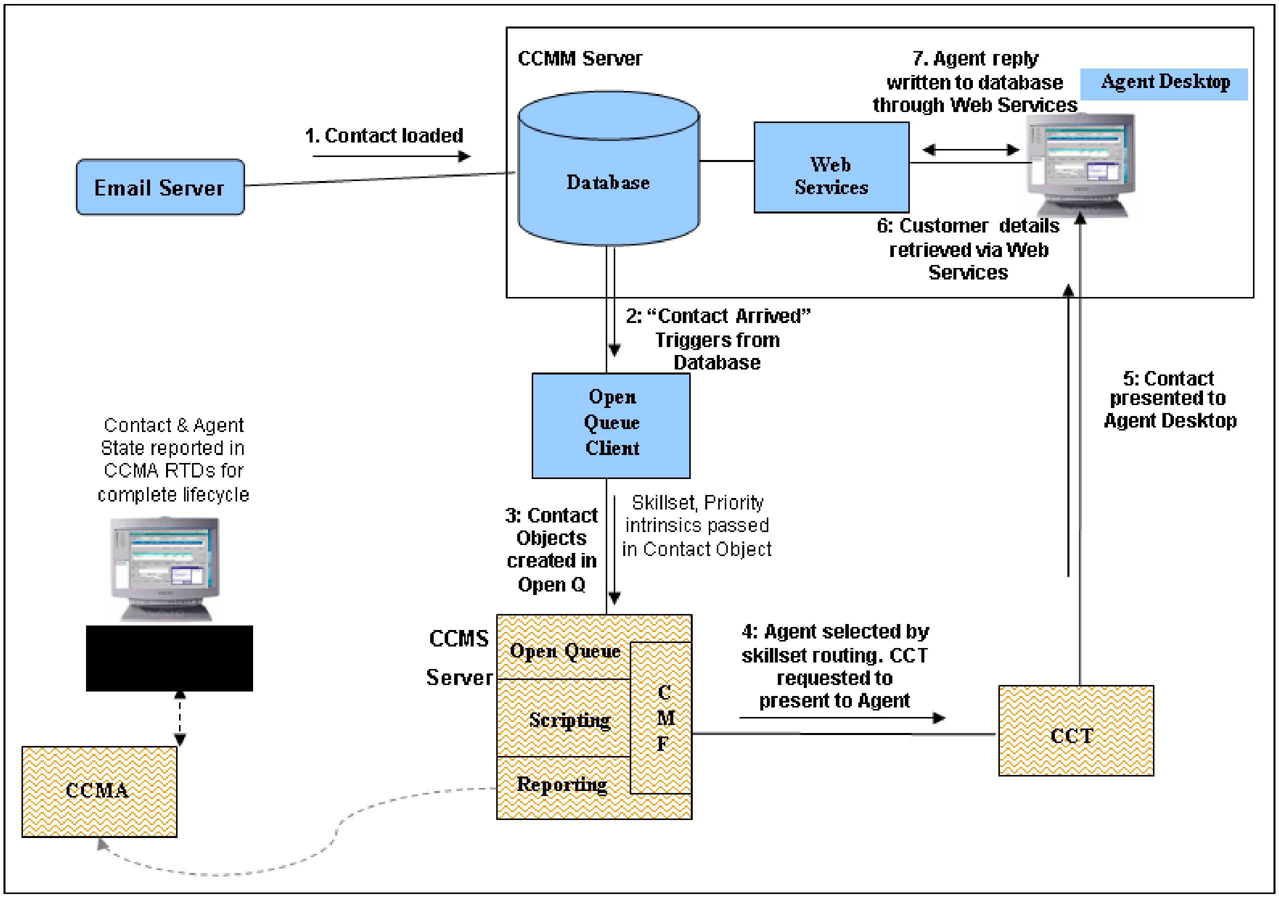

CCMM Server
7. Agent reply written to database through Web Services
Agent Desktop
1. Contact loaded
Email Server
Database
Web Services
6: Customer details retrieved via Web Services
2: "Contact Arrived" Triggers from Database
5: Contact presented to Agent Desktop
Open Queue Client
Contact & Agent State reported in CCMA RTDs for complete lifecycle
3: Contact Objects created in Open Q
Skillset, Priority intrinsics passed in Contact Object
CCMS Server
Open Queue
Scripting
Reporting
C M F
4: Agent selected by skillset routing. CCT requested to present to Agent
CCT
CCMA

Figure 1: Email contact life cycle

You can route email contacts by using rule groups based on specific information you configure for the contacts. The Email Manager routes incoming contacts based on the address where the contact is received, the text is in the email message, or who sent it. The email message is assigned to a skillset with a priority and then to an agent who can handle the contact based on the received criteria.

The email contact type has several components:

- Email rule groups on page 28
- Recipient mailboxes on page 29
- Inbound email settings on page 29

You must configure email settings for email messages leaving your contact center as a campaign or in response to customer email messages.

- Outbound email settings on page 29
- Character encoding for outgoing email messages on page 29

You can configure the email message contact type for international languages, see Asian email on page 30.

You can view real-time traffic reports for your email messages. Configure the date and time for which you want to review the email traffic in your contact center. See Email traffic reports on page 30.

You can enable the Extended Email Capacity feature if you require the email backlog capacity to be more than 20 000. The Extended Email Capacity feature increases the email backlog capacity to 100 000 contacts. For more information, see Extended Email Capacity on page 31.

You can configure the Supervisor Email Approval feature so that supervisors can approve email messages before they reach the customers.

Note:

The approval process applies to email contacts only and does not apply to other contact types such as Fax, Scanned Documents, and SMS.

Based on your quality assurance requirements, regulatory requirements or agent training requirements, some or all of the email messages can be sent for supervisor approval. You can configure email messages targeted for supervisor approval on a per skillset basis or per agent basis. For more information, see Supervisor approval of email messages on page 32.

Agents handle email messages using Agent Desktop. For more information about Agent Desktop, see Agent Desktop on page 33.

Email rule groups

Rules determine how a multimedia contact is routed based on information about the email message (input) and configurations in your contact center.

A basic rule considers the first recipient address of the contact and can assign a skillset. You can further enhance the routing by searching for specific keywords in the body of an email or by looking at who sent the message.

Rule groups are collections of rules that evaluate the incoming email and route the contact according to the best match or the first match.

You can also enhance the routing by selecting additional output details for your contact center, such as automatic responses.

By default, one rule group is supplied that contains the default rule for routing an email contact to a specific skillset with a priority.

For example, a magazine advertises an investment strategy. Customers can learn more about the investment by sending an email with “Good Investing” in the subject line to a specific address. Create a rule to search incoming email messages for “Good Investing.” If the email subject line contains this subject line, then a brochure is sent to the customer. No interaction from an agent is required. The rule group “investments” is applied to the recipient mailbox at which the email message is received.

Recipient mailboxes

Contact Center Multimedia polls specific recipient mailboxes on the email server based on a list of mailboxes defined in the Multimedia Administrator recipients list. The email retrieved from these mailboxes is routed based on defined rules applied to either a mail store or an alias. You must ensure that enabled email addresses configured in your Email Manager are already configured on your corporate email server.

The recipient mailbox has a default rule group assigned to handle the email messages, but you can assign a custom rule group to the recipient.

Recipient mailboxes also receive messages from other contact types. Voice Mail contacts attach a .wav file. Faxes and scanned documents attach a .tiff file to an email message handled by the Email Manager. An SMS text message also uses the Email Manager to route text messages.

Inbound email settings

Perform this optional configuration if you are licensed for email contacts.

You can configure the following optional email settings:

- how frequently you scan the email server for new messages
- the location in which to store attachments
- the text searched when you use keywords for rules

Outbound email settings

Configure outgoing email mailbox settings to identify who responds to the email message from the customer. For outgoing email, you can change the character encoding of the message to display the email message with the correct characters.

The response can contain the email address to which the customer sent the original email message or a general corporate email address configured for each skillset. Agent-initiated messages are always sent from an email address associated with a skillset.

Email messages must be relayed through the email server, not forwarded to another party if you manage email messages on behalf of an external source. Sending email messages preserves the original To address that is used for email rule administration and outgoing email addresses.

Character encoding for outgoing email messages

The Contact Center Multimedia Email Manager replies to an email message using the same characters as the inbound email. For example, if an email arrives to the contact center with Latin-1 encoding, the reply from the Agent Desktop or the automatic response is sent in Latin-1. The customer email client can understand the format of the message sent from the contact center.

If the customer sends an email message in English and receives either an agent response or an automatic response in another character set, you cannot tell if the customer email client can decode the new character set. Avaya recommends that if you use an automatic response, you use rules to search for words in the expected languages (for example, Japanese or English) to ensure that the response sent matches the language of the inbound email.

If the original email is encoded with the Latin-1 character set (ISO-8859-1), you can choose to reply in Latin-9 character set (ISO-8859-15) to provide support for the Euro Currency Symbol. The Euro Currency Symbol is not included in the Latin-1 character set, instead, it is represented by a question mark (?). Not all recipients understand the Latin-9 character set, and the reply email can be perceived as a blank email. Avaya recommends that only contact centers in Europe use Latin-9 encoding.

Asian email

Internationalized domain names (IDN) can include characters from East Asian languages. Using characters from East Asian languages is dangerous because this can be used by phishing sites. Phishing is a way of attempting to acquire information such as names, passwords, and credit card details by misrepresenting a malicious website as a legitimate website.

Phishing email messages contain links to malicious websites that look similar to legitimate business websites. For example, the IDN of a phishing site can achieve this by replacing Latin 1 characters with East Asian characters that are visually similar or identical.

The World Wide Web Consortium uses punycode to implement IDNs. Punycode is an ASCII equivalent to the domain name. Normally, the client (Web browser or email client) accepts the IDN in native characters and converts it to punycode; for example, xn--jp-cd2fp15c@xn--fsq.com. The receiving client identifies the sender as being a punycode string and interprets the native characters.

Contact Center Multimedia supports IDNs. You or a customer can enter a punycode email address. The receiving client can render the native characters.

Email traffic reports

Reports appear in the CCMM Administration utility to show the current status of the email traffic. The following reports appear when you select E-mail in the left column of the Multimedia Administrator application. You can choose the report date and the skillsets represented in all displayed real-time reports.

- E-mail (New Vs. Closed) shows the number of contacts in a new and closed state against the time for the selected date and skillsets. You can use this report to monitor the incoming and closing rate for email and to determine if the traffic levels are adequately managed. The number of new contacts is defined as those with an arrival time since midnight on the selected date. The number of closed contacts is defined as those with a close time since midnight on the selected date.

- E-mail Progress shows the number of contacts in a new or closed state on a defined date to determine the traffic levels for that date.
- E-mail Closed Contacts Queue Time shows the average time an email contact spends in the queue while the contact center is open. The queue time is defined as the time between when the contact arrives in the contact center and the time the contact is presented to an agent less the time that the contact center is closed. This report shows only closed contacts for the selected date, and reflects only a partial summary of the service level achieved for the date.

Extended Email Capacity

The Extended Email Capacity feature increases the email backlog capacity to 100 000 contacts. Contact centers that have large email volumes can use the Extended Email Capacity feature to pull email messages that are present in the CCMM database. Agents can then view email contacts in the CCMM database and search or extract these contacts, while on a voice call with a customer.

The Email Scheduler Service is a Contact Center Multimedia (CCMM) service that monitors the Real-time Statistics Multicast (RSM) stream and multimedia database for skillset statistics corresponding to email skillsets. This service gathers the following information:

- The skillsets in service.
- The number of available agents. The CCMM database provides the number of in-service agents.
- The number of queued contacts. RSM provides information about the Calls Waiting statistics.

The Email Scheduler Service uses this information to ensure that sufficient contacts are queued on each skillset.

Note:

Generally, the system queues two contacts per logged in agent on a skillset. However, in certain circumstances the actual amount of contacts queued can be more.

By default, the Extended Email Capacity feature is disabled. If you require the email backlog capacity to be more than 20 000, you must enable this feature.

If the Extended Email Capacity feature is disabled, Email Manager performs nightly checks on the number of email messages that have a New status in the multimedia database. If the number of email messages that have the New status is more than 10 000 in a standalone CCMM configuration and 3 000 in a co-resident configuration, Email Manager sends an email to the administrator to enable the Extended Email Capacity feature. You can configure the distribution list for this email in the Multimedia Dashboard. Email Manager uses the address assigned to the EM_Default_Skillset as the From Address. If you do not configure this address, Email Manager sends the notification to a dummy address, which triggers a delivery failure notification. The delivery failure notification then routes to an agent. The text of the email is set up as a prepared response with a default System Message.

On the Multimedia Dashboard, you can see whether the Extended Email Capacity feature is enabled. If the Extended Email Capacity feature is disabled, and the number of New email contacts in the CCMM database is more than 2 000, the dashboard displays a warning in amber. If the number of New email contacts in the CCMM database is more than 3 000, the dashboard displays a warning in red.

Supervisor approval of email messages

Before an email message reaches a customer, supervisors can approve or reject email messages that agents send to customers.

The approval process applies only to email contacts. The approval process does not apply to other contact types such as Fax, Scanned Documents, and SMS.

Configuration of Supervisor approval of email messages

Based on your requirements, the system can send some or all of the email messages to supervisors for approval before the system sends the email messages to a customer.

Quality assurance or Regulatory requirements: You can configure contacts that the system sends to supervisors for approval on a per skillset basis, which means that a percentage (0-100) of email messages sent from a skillset requires approval from supervisors. For more information, see Configuring supervisor approval for email messages on a per skillset basis on page 116.

❗ **Important:**

> For approval of agent email messages, you must configure an approval skillset to which the system sends the agent email messages.

Agent training: You can also configure contacts that the system sends to supervisors for approval on a per agent basis, which means that a percentage (0-100) of the email messages sent by particular agents require approval from supervisors.

For example, you can configure that 100% of the email messages that new agents send require approval from supervisors and 50% of the email messages that agents who have been in the contact center for over six months send require approval from supervisors. For more information, see Configuring supervisor approval for email messages on a per agent basis on page 51.

Agents can pull contacts for approval. You must restrict this by configuring skillset partitions. For more information, see Configuring agent access to contacts on page 52.

Agents cannot request approval of email messages. You cannot configure keywords to trigger the approval process.

You can configure up to five levels of approval from supervisors before email messages reach customers. The system sends email messages through a hierarchy of supervisors before the system grants the final approval.

You can also configure the system to automatically reject email messages from all skillsets based on keyword groups. For more information, see Configuring auto-rejection of email messages from all skillsets that use approval hierarchy on page 118.

Flow of email messages through Agent Desktop

Agent Desktop handles the flow of email messages as follows:

- When an agent sends an email message, the system marks the email message for approval and returns the email message to a predetermined skillset in the queue for approval.

  Supervisors who review the email message that the agent sends to the customer must be assigned to the approval skillset.

  Agents can belong to the skillset that approves email messages. Therefore, you must configure the approval process in a way that restricts agents from approving email messages.
- If the supervisor approves the email message, the system marks the email message to be sent to the customer or returns the email message to the queue if the email message requires further approval. If the email message requires further approval, the system targets the email message to the next approval skillset in the hierarchy.
- If the supervisor rejects the email message, the system marks the email message as rejected and returns the email message to the queue targeted to the previous skillset. The email message flows through the rejection hierarchy till the email message reaches the originator for redrafting. The supervisor must add review comments so that the originator can redraft the email message.

  Only the originator of the email message can edit or redraft the email message. Supervisors at all levels can only add review comments.

The system does not move email messages through the approval hierarchy in the following situations:

- You delete a skillset that is part of the supervisor approval chain and the contact is already in queue waiting for that skillset to come into service
- You delete the original agent and a supervisor rejects the email message
- You delete the supervisor who must approve the email message

In order to handle such contacts, agents must use Agent Desktop to pull contacts.

Agent Desktop

Agents use Agent Desktop to process email contacts. When an email message arrives at the contact center, it is routed to Agent Desktop, and agents can perform the following activities:

- Accept or reject an email message.
- Review and update customer information.
- Create a reply.
- Transfer the contact to an agent, skillset, or expert.
- Select a prepared response to send to the customer contact.
- Select an activity code to record the result of the customer contact.

SMS text messages, faxes, scanned documents, and voice mail attachments

The Short Message Service (SMS) text message is a standard communications protocol for the exchange of short text messages between mobile phone devices. SMS messages are forwarded by an SMS gateway to an email address.

A fax (short for facsimile) is a document sent over a phone line. Faxes are forwarded by a fax server to an email address as a .tiff attachment.

A scanned document is an electronic version of a printed page or document. Scanned documents are forwarded by a document imaging server to an email address as a .tiff attachment.

A voice mail is a spoken message including a message on an answering machine. Voice mail messages are forwarded by a voice mail server to an email address as a .wav attachment.

For each type of contact, you can configure the routing of the specified contact and assign a priority to the contact. See Mailbox configuration on page 34.

You can view traffic report summaries for each type of contact. See Traffic reports on page 35.

Use the Agent Desktop to open and reply to SMS, faxes, scanned documents, and voice mail contacts. See Agent Desktop on page 35.

For the previously listed contact types, the Email Manager retrieves the message or attachment and queues it to the default or defined skillset with the assigned priority. For faxes and voice mail attachments, the Email Manager permits the caller ID be extracted to facilitate replies or callbacks.

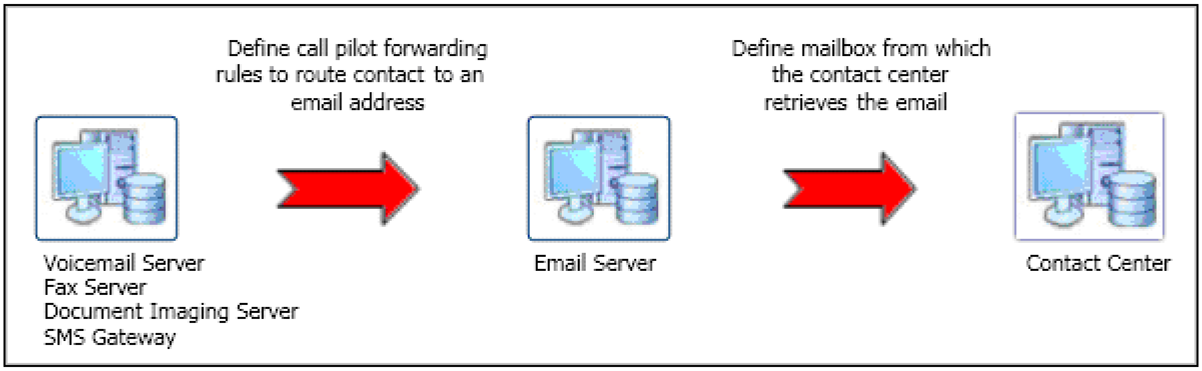

Define call pilot forwarding rules to route contact to an email address
Define mailbox from which the contact center retrieves the email
Voicemail Server
Fax Server
Document Imaging Server
SMS Gateway
Email Server
Contact Center

Figure 2: Contacts attached to email cycle

Mailbox configuration

You can configure the following properties for the contacts:

- POP3 or IMAP Server (for receiving email messages)
- recipient mailbox
- password for access to the mailbox

- skillset and priority
- sender address, either full sender address or Calling Line ID (CLID)
- reply address for skillset
- SMTP Server (for sending email messages)
- sending mailbox

Traffic reports

Reports appear in the CCMM Administration utility to show the current status of the contact type traffic. The following reports appear when you select the contact type in the left column of the Multimedia Administrator application. You can choose the report date and the skillsets represented in all displayed real-time reports.

- The New Vs. Closed report shows the number of contacts in a new and closed state against the time for the selected date and skillsets. You can use this report to monitor the incoming and closing rate for contacts of a particular type and to determine if the traffic levels are adequately managed. The number of new contacts is defined as those with an arrival time since midnight on the selected date. The number of closed contacts is defined as those with a close time since midnight on that date.
- The Progress report shows the number of contacts in a new or closed state on a defined date to determine the traffic levels for the selected date.
- The Closed Contacts Queue Time report shows the average time a contact spends in the queue while the contact center is open. The queue time is defined as the time between when the contact arrives in the contact center and the time the contact is presented to an agent less the time that the contact center is closed. This report shows only closed contacts for the selected date, and reflects only a partial summary of the service level achieved for the date.

Agent Desktop

Agents use Agent Desktop to process SMS, faxes, scanned documents, and voice mail contacts. When one of these contacts arrives at the contact center, CCMM routes it to a skillset, and agents can perform the following activities:

- Accept or reject the contact.
- Review and update customer information.
- Create a reply.
- Select a prepared response to send to the customer.
- Select a activity code to record the result of the customer contact.

Outbound contact type

The outbound contact type is an outgoing call made by agents to customers for sales or marketing.

The following figure shows how outbound contacts interact with Contact Center Manager Administration, Contact Center Multimedia, and Contact Center Manager Server.

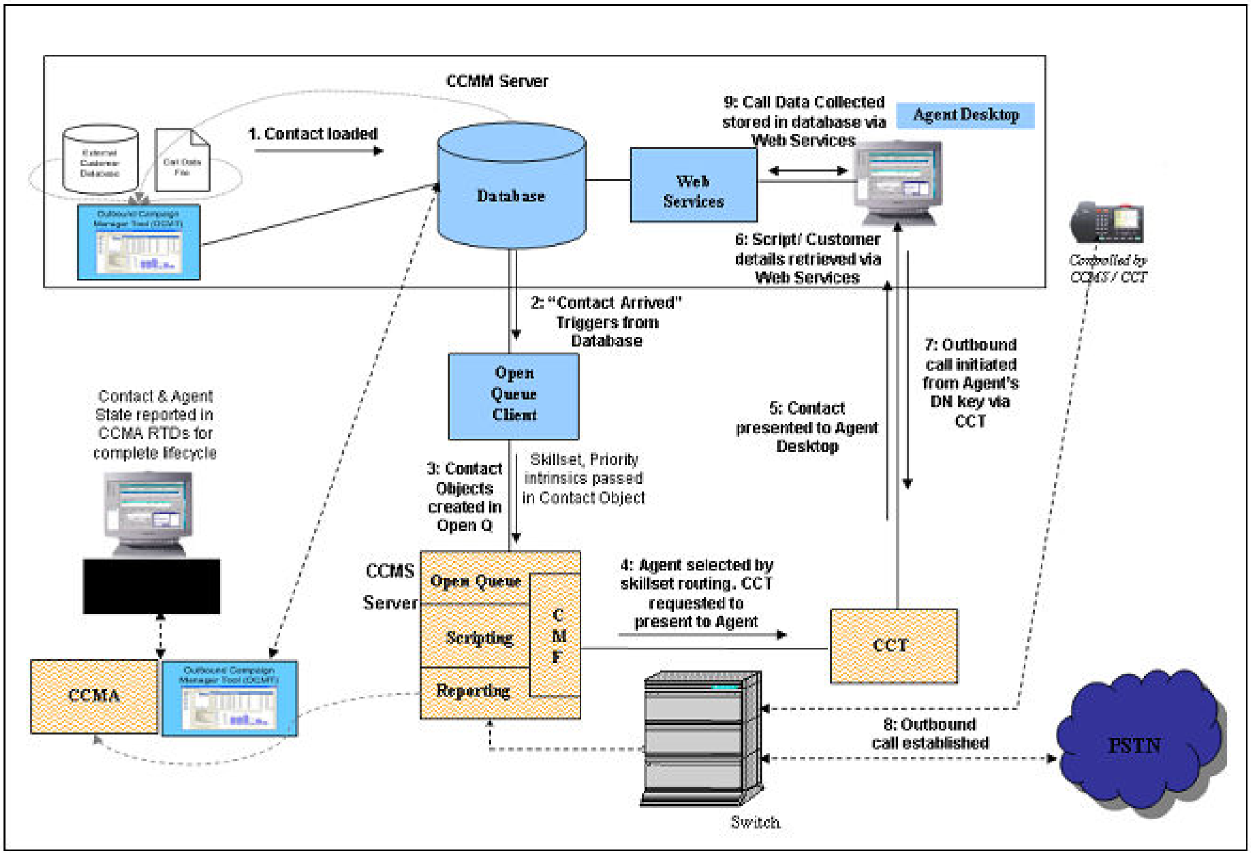

CCMM Server
External Customer Database
Call Data File
1. Contact loaded
Outbound Campaign Manager Tool (OCMT)
Database
Web Services
9: Call Data Collected stored in database via Web Services
Agent Desktop
6: Script/ Customer details retrieved via Web Services
Controlled by CCMS / CCT
2: "Contact Arrived" Triggers from Database
Open Queue Client
7: Outbound call initiated from Agent's DN key via CCT
5: Contact presented to Agent Desktop
Contact & Agent State reported in CCMA RTDs for complete lifecycle
3: Contact Objects created in Open Q
Skillset, Priority intrinsics passed in Contact Object
CCMS Server
Open Queue
Scripting
Reporting
CMF
4: Agent selected by skillset routing. CCT requested to present to Agent
CCT
CCMA
Outbound Campaign Manager Tool (OCMT)
8: Outbound call established
PSTN
Switch

Figure 3: Outbound contact type routing

Contact Center Outbound consists of several components:

- Outbound Campaign Management Tool on page 37
- Campaign Scheduler on page 37
- Agent Desktop on page 38
- Contact Center Manager Administration on page 38

Outbound Campaign Management Tool

Use the Outbound Campaign Management Tool in Contact Center Manager Administration to create, modify, and monitor outbound campaigns.

A contact center administrator or supervisor can use the Outbound Campaign Management Tool to create and monitor outbound campaigns. The Outbound Campaign Management Tool provides the following main functions:

- Define a campaign.
- Import call data.
- Create disposition codes.
- Review outbound call data.
- Create and preview optional agent scripts.
- Review campaign progress.

Campaign Scheduler

This Contact Center Multimedia server component determines when to queue contacts to the Contact Center Manager Server. The Campaign Scheduler monitors the status of each campaign and performs the following actions:

- Assigns the campaign status to running and queues contacts to Contact Center Manager Server when the campaign start time or daily start time occurs.
- Assigns the campaign status to nonrunning and removes contacts from Contact Center Manager Server when the daily end time occurs.
- Assigns the campaign status to expired and removes contacts from Contact Center Manager Server when the daily end time occurs.
- Assigns the campaign status to completed when all contacts are processed.

The Campaign Scheduler queues outbound contacts at the rate required to maintain 5 outbound contacts waiting for each logged in agent on each outbound skillset.

The Campaign Scheduler also queues rescheduled outbound contacts falling due within the next 15 minutes. Therefore the Real Time Display (RTD) for the skillset can show more than 5 times the number of staffed agents, depending on rescheduled outbound contacts falling due within the next 15 minute period.

The RTD can display less than 5 times the number of staffed agents, where there are not enough outbound contacts, which fall within the configured dialing hours based on customer time zone, waiting in outbound campaigns.

Agent Desktop

Agents use Agent Desktop to process outbound contacts. When a campaign runs, outbound contacts are routed to Agent Desktop, and agents can perform the following activities:

- Accept or reject an outbound contact.
- Review and update customer information.
- Make the outbound voice call.
- Follow an agent script and record customers answers and comments.
- Select a disposition code to record the result of the call.

Contact Center Manager Administration

Use Real-Time Reporting and Historical Reporting in Contact Center Manager Administration to create and run real-time and historical reports for outbound contacts.

Real-Time Reporting displays real-time and up-to-date statistics information regarding a campaign, such as the number of waiting contacts, the number of answered contacts, or the average answer delay.

Web services

The Open Queue Open Interface delivers existing Open Queue functions to third-party applications that use a Web service. Third-party applications can add and remove contacts of a specific type in Contact Center.

For more information, see the SDK documentation.

Chapter 4: General configuration

The Contact Center Multimedia server supports multimedia contacts. To manage the multimedia contacts, you must configure general administrator settings and global routing options.

Configuring Internet Explorer

About this task

Configure Internet Explorer to access Contact Center Manager Administration.

Install Microsoft Internet Explorer 10.0 or 11.0 (32 bit version only). Contact Center Manager Administration supports only the 32 bit version of Microsoft Internet Explorer.

Note:

You must run Internet Explorer in compatibility mode for Contact Center Manager Administration.

Procedure

1. Start Internet Explorer.
2. Click the **Tools** icon and select **Internet Options**.
3. In the **Internet Options** dialog box, click the **Security** tab.
4. Click the **Trusted Sites** icon.
5. Click **Custom Level**.
6. In the **Security Settings** dialog box for trusted sites, under the **.NET Framework-reliant components** heading, select **Enable** for the following:
    - **Run components not signed with Authenticode**
    - **Run components signed with Authenticode**
7. Under the **ActiveX controls and plug-ins** heading, select **Enable** for the following:
    - **Automatic prompting for ActiveX controls**
    - **Run ActiveX Controls and plug-ins**
    - **Script ActiveX Controls marked safe for scripting**

8. Under the **Downloads** heading, select **Enable** for the following:
    - **Automatic prompting for file downloads**
    - **File download**
9. Under the **Miscellaneous** heading, for **Allow script-initiated windows without size or position constraints**, select **Enable**.
10. Under the **Miscellaneous** heading, for **Allow websites to open windows without address or status bars**, select **Enable**.
11. Under **Reset custom settings**, from the **Reset to:** list select **Medium-low**.
12. Click **Reset**.
13. On the Warning dialog box, click **Yes**.
14. Click **OK**.
15. If you enabled ActiveX options, when a message appears asking you to confirm your choice, click **Yes**.
16. Click the **Trusted Sites** icon.
17. Click **Sites**.
18. In the **Trusted sites** dialog box, clear the **Require server verification {https:} for all sites in this zone** check box.
19. In the **Add this Web site to the zone** box, type the server name (not the IP address) for your Avaya Contact Center Select server.
20. Click **Add**.
21. Click **Close** to return to the **Internet Options** dialog box.
22. Click the **Privacy** tab.
23. In the **Pop-up Blocker** section, select the **Block pop-ups** check box.
24. Click **Settings**.
25. In the **Pop-up Blocker Settings** dialog box, in the **Address of website to allow** box, type the Avaya Contact Center Select server URL.

    The default URL is `https://`*`<server name>`* OR if you turned off Web Services security, type `http://`*`<server name>`*, where <*server name*> is the name of the Avaya Contact Center Select server.
26. Click **Add**.
27. Click **Close**.
28. In the **Internet Options** dialog box, click the **Advanced** tab.
29. Under **Browsing**, clear the **Reuse windows for launching shortcuts** check box.
30. Click **OK** to exit the **Internet Options** dialog box.
31. Restart Internet Explorer to activate your changes.

Starting the CCMM Administration utility

Before you begin

- Configure Internet Explorer.

About this task

Use the CCMM Administration utility to commission and maintain multimedia resources. To start the CCMM Administration utility, you must first log on to Contact Center Manager Administration.

Procedure

1. Start Internet Explorer.
2. In the Address box, type the URL of the Contact Center server. For example, type `https://<server name>`, OR if you turned off Web Services security, type `http://<server name>`, where <*server name*> is the computer name of the Contact Center server.
3. Press **Enter**.
4. In the main logon window, in the **User ID** box, type an administrator user name.
5. In the **Password** box, type the password.
6. Click **Log In**.
7. On the Launchpad, click **Multimedia**.
8. In the left pane, select the CCMM server to administer.

   The system displays the Multimedia Administration screen in the right pane.
9. Select **Install prerequisite software**.
10. Click **Launch Multimedia Client**.
11. On the **File Download** box, click **Run**.

    Important:

    If you see an **Application Run Security Warning** or a **SmartScreen Filter** warning message, confirm the **Publisher** is Avaya or that you are launching from a trusted link, before continuing to run the utility.

    The prerequisite software takes some time to install. After the install, the CCMM Administration utility appears.

Configuring the reporting credentials

About this task

Configure the password for the mmReport user. The mmReport user is configured in the Multimedia database to pass data and reporting information to Contact Center Manager Administration to generate real-time and historical reports, and integrated reporting.

If you change the password in the Contact Center Multimedia Administrator application, you must update the Contact Center Multimedia password in Contact Center Manager Administration.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **General Administration**.
3. Click **General Settings**.
4. In the Reporting Credentials section, under **Reporting Account Password Reset**, select the account ID for the reporting. The default account is mmReport.
5. Click **Set Password** to use the default password. The default password is assigned to new agents.

   OR

   Type the new password in the **New Password** and **Confirm Password** boxes.

   The password must fulfill the following complexity criteria:

   - Must be between 8 to 20 characters
   - Must contain a number
   - Must contain at least one uppercase letter and at least one lowercase letter
   - Must not contain spaces
   - Must not contain any of these characters: \ & : < > |
6. Click **Save**.

Adding administrators

About this task

Add administrators for the Contact Center Multimedia server to control access to configuration components in your contact center. For example, one administrator account can provide access to configure the predictive support tool or some Web services.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.

2. In the left pane, click **General Administration**.
3. Click **Administrator Settings**.
4. Click **New**.
5. In the **General Identification Details** section, type the last name, the first name, and the user name of the Administrator.
6. In the **Contact Details** section, add information about how to contact the Administrator, such as the phone number, fax number, and email address.
7. In the **Password** section type and confirm your password.

   The password must fulfill the following complexity criteria:

   - Must be between 8 to 20 characters
   - Must contain a number
   - Must contain at least one uppercase letter and at least one lowercase letter
   - Must not contain spaces
   - Must not contain any of these characters: \ & : < > |
8. Click **Save**.

Removing administrators

About this task

Remove an administrator account that you no longer require in your contact center.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **General Administration**.
3. Click **Administrator Settings**.
4. Select the administrator account to remove.
5. Click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the decision.

Configuring office hours

Before you begin

- Know the office hours of the contact center.

About this task

Configure the days and hours that your contact center is open each week.

Configuring the office hours is important to determine accurate queued time for contacts that can have a delayed response such as email, voice mail, SMS, scanned documents, and faxes. For example, if a contact is received on Friday and processed on Monday and you configure the office hours to show the contact center is closed over the weekend, the queue time for the contact only includes the time the contact center is open.

You can use the office hour calendar in email rules to determine the skillset to which to route the contact. The email rules can send a specific response if the office is closed.

The office hour calendar uses sliders to indicate closed times for your contact center. The Start Closed Period slider is a blue triangle (◢). The End Closed Period slider is a red triangle (◤). Each closed period is shown in red with a Start Closed Period and End Closed Period at the beginning and end of the closed office hours.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **General Administration**.
3. Click **Office hours**.
4. Under **Template**, type the name of a calendar to configure.
5. Configure holidays for the office hour template.
6. Beside a day of the week, click ⊞.
7. For the day you select, move the Start Closed Period ◢ and End Closed Period ◤ sliders to define a period when the contact center is closed.

   Open hours for the contact center are shown by the green bars. Closed hours are in red.
8. Repeat step 6 on page 44 and step 7 on page 44 for every day of the week.
9. Click **Save**.

Configuring holidays

Before you begin

- Identify the closed days of the contact center.

About this task

Configure the days and times that your contact center is open for holidays.

Configuring the office hours is important to determine accurate service levels for contacts that can have a delayed response such as email, voice mail, SMS, scanned documents, and faxes. For example, if a contact is received on a holiday, the queue time for the contact includes only the time the contact center is open.

You can use the office hour calendar in email rules to determine the skillset to which to route the contact.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **General Administration**.
3. Click **Office hours**.
4. Under **Template**, type the name of a calendar to configure.
5. In the holiday box, under **Name**, type the name of a public holiday.
6. Select the **Holiday Date** for the holiday and specify the time for the holiday. You can choose from **All Day** or a specify **Start time** and **End time**.
7. Click **Save**.

Applying office hours

Before you begin

- Create a calendar template with office hours or holidays. See Configuring office hours on page 44 or Configuring holidays on page 44.

About this task

Apply a designated calendar showing open and closed hours of the contact center controlled by the Contact Center Multimedia server.

The designated calendar is used in email settings for the contact center.

You can respond to email messages by selecting the office hours calendar to send automatic messages to incoming email contacts. You can select which rule group to apply the global office hours to. For more information, see Creating or changing rules on page 110.

You can also configure a calendar for each skillset in your contact center. For more information about configuring office hours for a skillset, see Configuring skillsets for email on page 92.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.

2. In the left pane, click **E-mail**.
3. In the left pane, click **General Settings**.
4. Under **Office Hours**, select the **Out of office hours treatment is enabled** check box to automatically send an out-of-office type message to the customer when the contact center is closed.
5. Select the calendar you want to use to determine the business hours for your contact center.
6. Select the automatic response for the out of office hours notice.
7. Click **Save**.

Viewing real-time traffic reports by contact

About this task

For email, voice mail, fax, SMS, and scanned documents, you can view traffic reports for each contact type.

The reports appear in the Contact Center Multimedia Administration utility to show the current traffic status. The following reports appear when you select View Reports in the left column of the Contact Center Multimedia application. You can choose the report date and the skillsets represented in all displayed real-time reports.

- The New Vs. Closed report shows the number of contacts in a new and closed state against the time for the selected date and skillsets.
- The Progress report shows the number of contacts in a new or closed state on a defined date to determine the traffic levels for that date.
- The Closed Contacts Queue Time report shows the average time a contact spends in queue while the contact center is open.

You can change the time for the displayed traffic reports. See Configuring the displayed date for traffic reports on page 47.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select a media type that supports the traffic report views (**Text Messaging (SMS)**, **E-mail**, **Fax**, **Scanned Documents**, and **Voice Mail**).
3. Click **View Reports**.

Configuring the displayed date for traffic reports

About this task

For email, voice mail, fax, SMS, and scanned documents, you can view traffic reports for each contact type.

You can choose a date and specify the skillsets for each media type for the current reports.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. Select a media type that supports the traffic report views (**Text Messaging (SMS)**, **E-mail**, **Fax**, **Scanned Documents**, and **Voice Mail**).
3. Click **View Reports**.
4. In the bottom left corner of the report view, in the **Report Date** list, select the date for which to view the traffic for your contact center.
5. To display all skillsets, select the **Select All Skillsets** check box.

   OR

   Specify the skillsets to view. The skillsets must be valid for the contact type you review.
6. Click **Update**.

Configuring a Directory LDAP server

About this task

The Lightweight Directory Access Protocol (LDAP) server contains databases of customer addresses and other information to use when handling email contacts in the Agent Desktop. Agents can select recipients from the Directory LDAP list when composing an email message.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **General Administration**.
3. Click **Server Settings**.
4. Select the **Directory LDAP Server**.
5. Click **Edit**.
6. Select **Anonymous Logon** to enable the administrator to log on to the LDAP server without having to supply a username or domain.
7. Select **Enable Address Book Retrieval** to enable the directory lookup.

8. In the **User** field, type the user name for the administrator on the LDAP server in the format domain name\user name.
9. In the **Password** field, type the password for the administrator on the LDAP server.
10. In the **Polling Interval** field, type the polling interval, in hours, for the interval between polls for the email server lookup.
11. In the **Search Base** field, specify the preciseness of the LDAP search. For example, in a large enterprise of tens of thousands of people, it is not advisable to search for all users. In such a case, use a more restrictive search base, such as search for names in the local workgroup.
12. Click **Edit Server** to change the properties of the Directory LDAP server.
13. In the **Server Name** field, type the server name for the email server that you use to get email addresses. The default port number for the LDAP server is 389.
14. In the **Server Port** box, type the port number for the server.
15. Select **Use TLS** if you want Agent Desktop to communicate securely with the Directory LDAP server. The server specified must support TLS.
16. Click **Save**.
17. Click **Test** to test the connection to the LDAP server.
18. Click **Save**.

Configuring a Phonebook LDAP server

Before you begin

- Configure the Directory LDAP server. See Configuring an LDAP server on page 47.

  Important:

  To retrieve contacts from the LDAP server, ensure you select the **Enable Address Book Retrieval** check box.

- Ensure that the Contact Center LDAP Phone Book check box on the Multimedia, Agent Desktop Configuration, and Advanced Settings page is enabled.

About this task

Configuring a Phonebook LDAP server provides agents with a list of contacts during a voice call or while working on an email contact.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Agent Desktop Configuration**.

3. On the Agent Desktop General Settings screen, click **Advanced**.
4. On the Advanced Settings screen, enable **Contact Center LDAP Phone Book**.
5. Click **Save**.
6. Click **Yes**.
7. Click **OK**.
8. In the left pane, select **General Administration**.
9. Click **Server Settings**.
10. Click **New**.
11. In the **Server Type** list, select the **Phonebook LDAP Server** option.
12. In the **User** field, type the user name for the administrator on the Phonebook LDAP server in the format domain name\user name.
13. In the **Password** field, type the password for the administrator on the Phonebook LDAP server.
14. In the **Polling Interval** box, type the polling interval, in hours, for the interval between polls for the email server lookup.
15. In the **Search Base** field, specify the precision of the Phonebook LDAP search.

    For example, in a large enterprise of tens of thousands of people, it is not advisable to search for all users. In such a case, use a more restrictive search base, such as search for names in the local workgroup.
16. Click **Edit Server** to change the properties of the Phonebook LDAP server.
17. In the **Server Name** box, type the server name.
18. In the **Server Port** box, type the port number for the server.
19. Select **Use TLS** if you want Agent Desktop to communicate securely with the Phonebook LDAP server. The server specified must support TLS.
20. Click **Save**.
21. Click **Test** to test the user name, password, and search base, by connecting to the configured server to retrieve contacts.
22. Click **Save**.

Chapter 5: Agent Desktop configuration

The Contact Center Multimedia Administrator application includes settings that you use to configure properties for Agent Desktop. These settings allow agents to access database information and work with contacts.

Perform the procedures in this chapter to configure the Agent Desktop settings.

Adding a friendly name for a web chat agent

About this task

From Release 7.0 Feature Pack 1, Contact Center administrators can add a friendly name or nickname for a web chat agent.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **General Administration**.
3. Click **Agent Settings**.
4. In Edit Single Agent Settings, in the **Friendly name** field, type the friendly name for the web chat agent.

   The rules for the friendly name are similar to the rules for first name, which are as follows:

   - Can have a maximum of 30 characters
   - Can have white spaces
   - Cannot have the following characters: "!""#$%&*+/:;<=>?@[\]^`{|}~"
5. Click **Save**.

Next steps

Administrators must also choose the label that gets displayed in agents' responses to text chat messages with the contact. Administrators can also choose that the friendly name is displayed in welcome messages. For more information, see Configuring welcome messages and text chat labels on page 132.

Controlling access to email message text

About this task

Agents, by default, cannot edit text in an email message. You can either enable particular agents or enable all agents to delete text from email messages that enter the contact center.

For example, select this feature so agents can delete credit card information from an email message to protect confidential customer information.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **General Administration**.
3. Click **Agent Settings.**
4. Select the **Enable E-mail Text Deletion For All Agents** check box, to enable all agents to delete text from email messages.

   OR

   Click the agent, and under **Delete Enabled**, click the **Yes** option, to enable that agent to delete text from email messages.
5. Click **Save**.

Configuring supervisor approval for email messages on a per agent basis

About this task

Supervisors can approve email messages before the email messages reach the customers.

Note:

The approval process applies to email contacts only. The approval process does not apply to other contact types such as Fax, Scanned Documents, and SMS.

The approver of the email messages is the supervisor assigned to the approval skillset of the contacts that the agent handles.

Note:

Agents can pull contacts for approval. Restrict agents from pulling contacts for approval by configuring skillset partitions. For more information see, Configuring agent access to contacts on page 52.

You can configure the system to send email messages to supervisors for their approval on a per agent basis or per skillset basis. For more information, see Supervisor approval of email messages on page 32 and Configuring supervisor approval for email messages on a per skillset basis on page 116.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **General Administration**.
3. Click **Agent Settings**.
4. From the right pane, select an agent.
5. Under Edit Agent Settings in the **Email Approval Ratio** field, type the percentage of email messages that require supervisor approval for the agent.

   The approval ratio must be whole numbers ranging from 0 to 100.
6. Click **Save**.

Configuring agent access to contacts

About this task

Agents, by default, see all contacts in the contact center. You can restrict the access to show agents only the contacts assigned to the agent's skillsets. You can also apply these restrictions for multimedia contact transfers. Partitioning changes do not take effect until after an agent logs out and logs in again.

Note:

This procedure does not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **General Settings**.
4. Under **Agent Skillset Partitioning**, select **Enable Partitioning**.
5. If you want to apply partitioning rules when an agent transfers a multimedia contact, select **Apply Partitioning to Transfers**.
6. Click **Save**.

Creating or changing custom fields in Agent Desktop

About this task

You can add a custom field to the Agent Desktop for multimedia contacts that pertains to your contact center. For example, if your customers subscribe to a magazine, you can view information about each customer's subscription expiry date.

The value entered by the contact center agent for each customer appears in the custom field, the same as any other customer-entered information such as email address or phone numbers.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **Resources**.
4. In the first blank row under **Current Custom Fields**, type the name of a custom field.

   OR

   Click on an existing field to change the label.
5. Press **Tab** to save your changes.

Deleting a custom field in Agent Desktop

About this task

Delete a custom field from the Agent Desktop when it is not required.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **Resources**.
4. Under **Current Custom Fields**, select a custom field.
5. Press **Delete** on your keyboard.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the decision.

Configuring the active contact timer

About this task

Configure the maximum amount of time that you want a multimedia contact to remain open on a desktop. The active contact timer does not apply to Outbound or Web communications contacts.

When this time expires, the contact remains open for a maximum of an hour more than the maximum open duration set in CCMM Administration. Agent Desktop force closes the contact when the additional hour expires. Agent Desktop warns the user when the contact has 60 minutes, 30 minutes, and 5 minutes left before force closing the contact.

The default time in the Contact Center Multimedia configuration is 1 hour (60 minutes).

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **General Settings**.
4. In the **Maximum Open Duration** box, type the maximum amount of time you want multimedia contacts to remain active.

   The minimum is 10 minutes and the maximum is 12 hours.
5. Click **Save**.

Configuring the callback timer

About this task

Configure the callback timer as a range of minutes to days for the system to wait before reoffering a pending contact to agents. An agent can delay the contact or place the contact into pending state because they are waiting for additional information to complete the contact.

The callback timer can be 2 minutes to 200 days (about 6 months). The default range provides the limits to which the you configure the callback time. The actual time value appears by default in the Agent Desktop application when the agent reschedules the contact.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **General Settings**.
4. Under **Callback Time**, type a number of minutes in the **Minimum Time** box.
5. Under **Callback Time**, type a maximum number of days in the **Maximum Time** box.

6. Click **Save**.

Configuring the callback trunk access

About this task

Configure the callback trunk access to ensure that you can create a callback to the customer you work with. Callback trunk access enables you to schedule callbacks with customers who requested callbacks.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **General Settings**.
4. Under **Callback Trunk Access**, type the trunk access number in the **Trunk Access Code** box.
5. Click **Save**.

Specifying the attachment size

About this task

Specify the maximum size of the attachments that an agent can attach to an email message.

Important:

The maximum file size set for attachments also applies to inline attachments.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **General Settings**.
4. Under **Attachment Upload Size**, in the **Maximum Size** box, type the maximum number of kilobytes for a file.
5. Click **Save**.

Configuring Agent Desktop behavior

About this task

You can configure Agent Desktop to alert the agent when a new contact arrives. The alert can be one or more of the following methods:

- Bring Agent Desktop to the front.
- Give focus to Agent Desktop.

Important:

Changes you make to Agent Desktop configuration take effect only when agents restart Agent Desktop.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **General Settings**.
4. Under **New Contact Presentation**, select the check boxes that describe the presentation.

   Choose **Bring to front** or **Give focus**.
5. Click **Save**.

Variable definitions

Name	Description
New Contact Presentation	The method in which contacts are presented: • Bring to front: The Agent Desktop moves to the front upon arrival of a new contact. If Bring to front is disabled while Give focus is enabled, the Agent Desktop makes a warning sound and the toolbar flashes, but it is not brought to the front. • Give focus: The Agent Desktop window is the active window when it moves to the front. The Bring to Front check box must be selected for the Give Focus check box to be enabled.

Configuring Web statistics

About this task

Configure Web statistics, so that agents and supervisors can use Agent Desktop to view real-time statistics for call handling, skillset data, and state information on Agent Desktop.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Agent Desktop Configuration**.
3. Select **General Settings**.
4. Under **Web Statistics**, select **Enabled**.
5. Click **Save**.

Configuring Web reporting

About this task

Enable Web reporting so that Contact Center reports on peer-to-peer Instant Messaging (IM). If an agent initiates an IM while active on a Contact Center contact, Contact Center reports on this activity.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Agent Desktop Configuration**.
3. Select **General Settings**.
4. Under **Web Reporting**, select **Enabled**.
5. Click **Save**.

Creating or changing a closed reason

About this task

Indicate a reason for closing a contact.

If one or more closed reasons are configured, then the agent must choose a closed reason to close the contact; otherwise, the agent need select no reason.

You can choose a default closed reason for each type of contact. See Configuring default closed reasons on page 58.

You can also assign a default closed reason to each contact type. The default reason is selected in the Agent Desktop application. The agent can choose another closed reason when closing a contact.

Important:

You cannot modify a default closed reason code.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **Resources**.
4. Under **Closed Reason**, type a name for the **Closed Reason**.
5. Under the **Type** box, select **All** or the type of contact for each closed reason.
6. Press **Tab** to save your changes.

Configuring default closed reasons

Before you begin

- Create a closed reason. See Creating or changing a closed reason on page 57.

About this task

You can specify a default closed reason for each contact type (email, fax, SMS, Web communications, scanned document, and voice mail) in the contact center. A contact is automatically assigned the default closed reason code unless an agent changes it when the contact is closed.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **Default Closed Reasons**.
4. In the **E-mail** drop-down box, select the configured closed reason to apply to email message contacts by default.
5. In the **Fax** drop-down box, select the configured closed reason to apply to email message contacts by default.

6. In the **SMS** drop-down box, select the configured closed reason to apply to SMS message contacts by default.
7. In the **Web Comms** drop-down box, select the configured closed reason to apply to Web communications contacts by default.
8. In the **Scanned Doc** drop-down box, select the configured closed reason to apply to scanned documents contacts by default.
9. In the **Voice Mail** drop-down box, select the configured closed reason to apply to voice mail contacts by default.
10. Click **Save**.

Deleting a closed reason

About this task

Delete a closed reason if you do not want the reason to appear in the Agent Desktop application. You cannot delete a default closed reason code.

Important:

You can delete only one row at a time.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **Resources**.
4. Select a closed reason from the list.
5. Press **Delete** on your keyboard.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the decision.

Configuring Shortcut keys for Agent Desktop

About this task

You can configure shortcut keys that agents can use in Agent Desktop. Agents can use shortcut keys to perform common tasks in Agent Desktop more efficiently.

In the CCMM Administration utility, you can map shortcut keys to a list of activities that agents perform on Agent Desktop. The default keys are already specified in the CCMM Administration utility. However, you can choose to change the default keys as you see fit for operational reasons.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **Shortcut Keys**.

   The system displays the list of shortcut keys, which are mapped to specific activities that agents perform on Agent Desktop.
4. Update the shortcut keys as required.

   Shortcut keys have the format of Ctrl + (Optional) additional modifier + an alphanumeric character.

   The (Optional) additional modifier is either Shift or Alt. The alphanumeric character is in the range [A-Z] or [0–9].

   For example, the shortcut key for Login / Logout is Ctrl + Shift + L.

   Note:

   If you select **NONE** in the additional modifier field and **NONE** in the alphanumeric field of a shortcut key for a task, then the shortcut key for that task is disabled. This means that agents cannot use the shortcut key to perform this task on Agent Desktop.

   For example, if we select **CTRL** + **NONE** + **NONE** for Login / Logout, then the shortcut key for Login / Logout is disabled. The agents cannot use shortcut keys to login to or logout from Agent Desktop.
5. Click **Save**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the change.

Configuring Basic Screen Pops

About this task

Use the Basic Screenpop page to configure application shortcuts and intrinsics. Agent Desktop starts these applications when Agent Desktop displays an alert (Launch State: Alerting) for a work item or when an agent accepts a work item (Launch State: Active). When the agent opens the contact, the system displays the intrinsics for an open contact in Agent Desktop.

You can select one intrinsic that Contact Center sends as a parameter to the configured basic screen pop applications.

By default, the screen pop intrinsics list includes the standard intrinsics present on any call that Contact Center handles. You can add any other intrinsic to this list, and select the intrinsic. The intrinsic must already exist as a variable in Orchestration Designer, and must be populated so that the screen pop can use the intrinsic.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **Basic Screenpops**.
4. Click the **General settings** tab.

   The settings under the Global Screenpop settings and the Basic Screenpop settings sections are applicable to both Basic and Advanced screen pops. However, you can override the Basic Screenpop settings when you configure Advanced screen pops. For more information, see Configuring Advanced Screen pops on page 65.
5. Select the **Allow Agents select Screen Pop(s)** check box to allow agents to choose the applications the agents require while using Agent Desktop.
6. Select the **Auto Expand AAAD on Work Item Answer** check box to expand the Agent Desktop application when an agent responds to a work item.
7. Select the **Launch Screen Pop on Incoming Personal Calls** check box to open screen pops during personal calls.
8. Select the **Launch Screen Pop on Outgoing Personal Calls** check box to open screen pops during personal outbound calls.
9. Select the **Launch Screenpop on Consultation received** check box to automatically open screen pops on the consulted agent’s desktop after a contact consult or transfer starts.
10. Select the **Launch Screenpop on Consultation initiating** check box to automatically open screen pops on the Agent Desktop of the agent who initiates the consult. The screen pop appears when the consult is initiated.
11. Select the **Close Screenpop when Consult/Transfer is Completed** to automatically close screen pops after a contact consult or transfer is complete.
12. Select the **Display Screenpops when Observe** check box to automatically open screen pops after a voice or Web Communications contact is observed.
13. Select the **Launch Screen Pop in a tab inside AAAD** check box to open the screen pop application within Agent Desktop.

    Only Web-based applications can open within Agent Desktop.
14. Select the **Auto Close Screenpop tab(s) on Work Item Release** check box to automatically close the screen pop tab on the Agent Desktop when an agent releases a contact.

15. From the **Launch State** drop-down list, select the event to open Basic screen pops. You can select one of the following:

    - **Active**: The screen pop application opens when an agent answers a contact.
    - **Alerting**: The screen pop application opens when Agent Desktop displays an alert for a work item.

    Note:

    You can configure a maximum of 20 basic screen pops. However, you can configure up to five screen pops only to open on Agent Desktop for each event.

16. Click the **General Intrinsics** tab.

17. Under **Screen Pop Intrinsics**, configure the intrinsics used to display data to the agent.

    You can configure only one intrinsic to “force launch”. This intrinsic is used for all Basic screen pops.

    Note:

    For consults or transfers, Contact Center provides the Skillset intrinsic only on Email and Web Communications contacts, and not on Voice contacts.

18. Click **Add** to add more intrinsics.

    Note:

    The name of the intrinsic you add in the Multimedia Administration utility must match the corresponding variable name in Orchestration Designer. The names are case-sensitive.

19. Click **Contact Screen Pop Intrinsics** to set different intrinsics for the configured contact types.

    You can select only one intrinsic for each contact type.

20. Click **Personal Call Screen Pop Intrinsics** to assign **Inbound** and **Outbound** intrinsics.

21. Click the **Basic Screenpop (Shortcuts)** tab.

    Use the **Basic Screenpop (Shortcuts)** tab to configure Basic screen pops. Basic screen pops consist of four parts:

    - **Name**: The **Name** field contains the name of the screen pop.
    - **Path**: The **Path** field contains the command that Agent Desktop uses to open the screen pop.
    - **Always on screenpop** check box: The **Always on screenpop** check box defines the basic screen pop shortcuts that are launched as screen pops. Agent Desktop can launch only five screen pop shortcuts.
    - **Event**: The **Event** field reflects the launch state that you set in the **General settings** tab. The **Event** field cannot be edited.

22. **(Optional)** Click **Add** to add more applications.

23. Select the **Always on screenpop** check box to choose the applications that open on client computers when Agent Desktop displays the screen pop.

    Text applications such as Notepad, or search engines such as Google can open automatically. You can add other applications, but you must ensure that the applications are installed on all clients.
24. Click the **Basic Filters (Launch Types)** tab.
25. Under the **Filter screenpops by Contact Types** list, select the contact types. All Basic screen pops open based on the selected contact types.
26. Click **Save**.

Configuring Advanced screen pop applications

About this task

When configuring an Advanced screen pop, you must select an application that you want Agent Desktop to open. This procedure outlines the steps for configuring an Advanced application.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **Advanced Screenpops**.

   The system displays the Advanced Screenpop Settings page.
4. Click the **Advanced Applications** tab.

   The system displays the Applications grid that contains the existing applications.
5. Click **New** to create a new application.

   The system displays the Create/Edit Application section at the bottom of the page.
6. Type the name of the application in the **Name** field.
7. Type the location of the application in the **Path** field.

   The path information can contain parameters.

   Note:

   You can assign a maximum of five parameters to each application.
8. To prevent mistakes when you type a parameter, click the **Insert Parameter** button to insert a parameter within a path.
9. Click **Save**.

   The system displays the new application under the Applications grid.

Configuring Advanced screen pop filters

About this task

When you are configuring Advanced screen pops, you can optionally select a filter for that Advanced screen pop. A filter defines additional conditions that must be met before an Advanced screen pop opens. These conditions match the contact intrinsic values with the predefined values. This procedure outlines the steps for configuring an Advanced filter.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **Advanced Screenpops**.

   The system displays the Advanced Screenpop Settings page.
4. Click the **Advanced Filters** tab.

   The system displays the Filters grid that contains the existing filters.
5. Click **New** to create a new filter.

   The system displays the Create/Edit Filter section at the bottom of the page.
6. Type the name of the filter in the **Name** field.
7. From the **Intrinsic Type** field, select an intrinsic whose value is compared against a set of applicable values.

   Note:

   The method of defining these applicable values depends on the intrinsic type you select. If you select an intrinsic of type Skillset, CDN, or DNIS, you must select the applicable values from a list. Otherwise, you must type an instrinsic value to match against the applicable values in a text box under the Intrinsic Values section and click **Add >**.

   Agent Desktop opens screen pops based on the intrinsic type.
8. From the **Contact Types** list , select the contact types to which the filter is applicable.

   Note:

   If you select the intrinsic type as Skillset, the list of applicable values to compare against changes according to the contact types selected or deselected.
9. If you select an intrinsic of type Skillset, CDN, or DNIS, select the applicable values from the list of values the system displays under the Intrinsic Values section.

   Or

   Type an instrinsic value to match against the applicable values in a text box under the Intrinsic Values section and click **Add >**.

Contact Center Manager Server (CCMS) retrieves the intrinsic values if the intrinsic types are Skillset, CDN, and DNIS. You must correctly configure the intrinsic values in CCMS for this functionality to work.

Note:

If you add an intrinsic, the intrinsic must already exist as a variable in Orchestration Designer and must be populated so that the screenpop can use the intrinsic.

10. Click **Save**.

    The system displays the new filter under the Filters grid.

Configuring Advanced Screen pops

About this task

Use Advanced Screen pops to configure individual screen pops to open on specific intrinsic triggers and filters. Advanced Screen pops provide administrators with greater range and flexibility with respect to conditions and triggers for opening a particular screen pop. However, administrators must configure the screen pop application to open based on one intrinsic. For example, configure a Web page (application) to open when you receive a contact with skillset EM_Ramdom_Skillset (intrinsic).

A maximum of five screen pops can launch on Agent Desktop for each event. The order of opening the screen pops is as follows:

1. All Basic Screen pops that match the configured contact type, event, and intrinsic.
2. Advanced Screen pops that match the configured contact type, event, and filter. Advanced Screen pops open in an ascending order based on the screen pops configured on the Advanced Screenpop Settings page.

Note:

The Advanced Screenpops wizard displays the Screenpop Summary section at the bottom of each screen. Screenpop Summary summarizes the actions that a user performs to configure a screen pop. You can use Screenpop Summary as a reference when you are configuring screen pops.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **Advanced Screenpops**.

   The system displays the Advanced Screenpop Settings page.
4. Click the **Advanced Screenpops** tab.

The system displays the Advanced Screenpops grid that contains the existing screen pops. Select a screen pop and then click the up arrow (**^**) button or the down arrow (**v**) button to change the order of the screen pops. This affects the order in which the screen pops are evaluated for launch.

5. Click **New** to create a new screen pop.

   The system displays Step 1 of 7 — Name page of the New Screenpop wizard.

6. Type the name of the screen pop in the **Screenpop Name** field.

   Screen pop names must be unique.

7. Click **Next**.

   The system displays Step 2 of 7 — Contact Types page of the New Screenpop wizard.

8. From the **Contact Types** list, select the contact types. The screen pop opens based on the selected contact types.

9. Click **Next**.

   The system displays Step 3 of 7 — Launch Event page of the New Screenpop wizard.

10. From the **Launch Event** drop-down list, select the event to open the screen pop. You can select one of the following:

    - **Active**: The screen pop application opens when an agent answers a contact.
    - **Alerting**: The screen pop application opens when Agent Desktop displays an alert for a work item.

    Note:

    A maximum of five screen pops can launch on Agent Desktop for each event.

11. Click **Next**.

    The system displays Step 4 of 7 — Application page of the New Screenpop wizard.

12. From the **Application Name** drop-down list, select the application that opens on client computers when Agent Desktop displays the screen pop.

    Or

    Click the Add (**+**) icon to add a new screen pop application. For more information, see Configuring Advanced screen pop applications on page 63.

    Or

    Select an existing application from the drop-down list and click **Edit** to edit an existing screen pop application.

    Note:

    Editing an existing application is supported only when the application is not in use.

Text applications such as Notepad, or search engines such as Google can start automatically. You can add other applications, but you must ensure that the applications are installed on all clients.

13. Click **Next**.

    The system displays Step 5 of 7 — Customise Application page of the New Screenpop wizard.

14. From the **Parameter** drop-down list, select a parameter that is present in the path.

    The number of parameters depends on the number of placeholders configured in the application on page Step 4 of 7 — Application.

    Note:

    You can set up to a maximum of five parameters for each screen pop application.

15. From the **Intrinsic** drop-down list, select an intrinsic value that replaces the parameter placeholder at runtime.

16. Click **Set**.

    The system displays the parameter and the corresponding intrinsic value under the Parameters section.

    Note:

    You must assign intrinsic values for all parameters present in the path.

17. Click **Next**.

    The system displays Step 6 of 7 — Filter page of the New Screenpop wizard.

18. **(Optional)** From the **Filter** drop-down list, select the filter for the screen pop.

    Or

    Click the Add (**+**) to add a new filter. For more information, see Configuring Advanced screen pop filters on page 64.

    Click **Edit** to edit an existing filter.

    Note:

    If you select a filter, Agent Desktop displays the screen pop only if matched conditions between the filter and the created screen pop are met.

    Only the filters containing all the contact types that you select from the **Contact Types** list on page Step 2 of 7 — Contact Types are available.

    If you select an existing filter, the system displays the filter conditions under the Selected Filter Conditions section. The Selected Filter Conditions section displays the intrinsic name and the corresponding values under the Match Values section.

19. Click **Next**.

The system displays Step 7 of 7 — Presentation Options page of the New Screenpop wizard.

The presentation options are set to the global settings that you configured for Basic screen pops. However, for Advanced screen pops you can change these settings for each screen pop. For more information about global settings, see Configuring Basic Screen Pops on page 60.

20. Select the **Launch Screen Pop in a tab inside AAAD** check box to open the screen pop application within Agent Desktop.

    Only Web-based applications can open within Agent Desktop.

21. Select the **Auto Close Screen Pop tab(s) on Work Item Release** check box to automatically close the screen pop tab on Agent Desktop once an agent releases a contact.
22. Click **Finish**.

    The system displays the Saved dialog box.

23. Click **OK**.

    The system displays the new screen pop under the Advanced Screenpops grid.

Enabling Customer History on Voice Contacts

Before you begin

- Use the administration tool on a Contact Center Multimedia server in order to configure customer history on voice contacts.
- Enable Contact Summary Data generation in Contact Center Manager Administration, to ensure that individual contact history data is created in the Contact Center Manager Server database.

About this task

You can search for customer history based on the calling line ID for voice contacts.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **User Settings**.
4. Select **True** in the **Display Customer History on Voice Contact** list, to display customer history for voice contacts in Agent Desktop.

5. In the **Voice Contact Identifier for Customer History** list, select the parameter to lookup the CCMM database that contains customer history for the originator of the incoming voice call.
6. Select **True** in the **Display Voice Calls in Customer History** list to display previous voice calls for the originator of the current active contact in Agent Desktop. Enable this setting to lookup the Contact Center Manager Server database for Voice Contact history.

   ! **Important:**

   Ensure that you have entered the port number that is used by the Agent Desktop to connect to the Contact Center Manager Server in the Voice History Port box in the Multimedia, Agent Desktop Configuration, and Advanced Settings page for retrieving the voice history information.
7. Click **Save**.

Restricting file extensions for attachments

About this task

You can use the CCMM Administration utility to configure the supported list of file extensions that agents can attach to emails.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **General Administration**.
3. Click **Agent Settings**.
4. Click **User Settings**.
5. To configure file extensions, perform one of the following:
   a. To add a new extension, type the file extension in the **Supported attachment file extensions** field and click **Add**.

      You must add the file extension in the description with the appropriate file extensions format. Each file extension must be separated by a semicolon (;).

      For example, if you want to add Word documents as a supported file extension, type `Word documents (*.doc;*.docx)`.

   b. To remove a file extension, select the file extension from the **Current supported file extensions** field and click **Remove**.
6. Click **Save**.

Configuring Advanced Settings

About this task

You can specify advanced configuration settings for Agent Desktop.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Agent Desktop Configuration**.
3. Click **General Settings**.
4. On the General Settings screen, click **Advanced**.
5. Update the required settings.
6. Click **Save**.

Variable definitions

Name	Description
Platform	The type of platform that your contact center uses. Select **SIP**.
Switch Type	The type of switch that you use in your contact center for voice contacts. Select **IP Office**.
IM Provider	If you use peer-to-peer Instant Messaging (IM) with any supported Microsoft instant messaging server in your solution, select **Lync 2010 / Lync 2013**. Otherwise, select **None**.
IM Consult Reporting on Voice Contacts	Enable or disable the reporting of IM or Multimedia consults by agents on voice contacts.
Agent Web Statistics	Enable Agent Web Statistics on Agent Desktop, so that agents and supervisors can use Agent Desktop to view statistics for call handling, skillset data, and state information on Agent Desktop.
Voice History Port	Enter the port number on CCMS that Agent Desktop connects to for retrieving the voice history information. Voice history information contains details of previous voice calls to the Contact Center from the dialed number of the currently active contact.

Table continues…

Name	Description
	Note: The default port is 443 with the security feature on which is the default value. In case you have disabled the security feature, the default port is 80. You cannot change the value of the port.
Number of Simultaneous Web Comms Observe/Barge-in Contacts	Enter the maximum number of Web Communications contacts that a supervisor can observe or barge-in on simultaneously.
Web Comms Observe/Barge-in Refresh Rate	Enter the time, in seconds, at which the multimedia intrinsics and chat summary refreshes for each Web Communications contact in the **Supervisor Observe: Contact** list on Agent Desktop.
Number of Messages to Display in Web Comms Observe/Barge-in Summary	Enter the number of messages to display in the chat summary for the selected Web Communications contact in the **Supervisor Observe: Contact** list on Agent Desktop. Agent Desktop displays the newest messages first in the list. For example, if this value is 5 and a supervisor selects a Web Communications contact containing 6 messages, then the summary displays messages from 2 to 6.
Contact Center LDAP Phone Book	Enable the Contact Center LDAP Phonebook to provide agents with a list of other agents, whom they can consult, during a voice call or an email contact.
Contact Types That Can Be Observed	Select the contact types that agent supervisors can observe. You can select **Web Communications**.
IM Logging	Select the **IM Logging** check box so that Agent Desktop log files capture log messages for the Microsoft instant messaging server.
Web Stats Logging	Select the **Web Stats Logging** check box so that Agent Desktop log files capture log messages relating to the Web Statistics feature. **Note:** **Web Stats Logging** generates logging inside Agent Desktop only.
Web Comms Logging	Select the **Web Comms Logging** check box so that Agent Desktop log files capture log messages for the Web Communications server. **Note:** **Web Comms Logging** generates logging inside Agent Desktop only.

Table continues…

Name	Description
CCT Logging Level	Select the logging level that Agent Desktop log files capture for CCT. You can choose from the following: • **Off** • **Verbose** ✱ **Note:** **CCT Logging Level** generates logging inside Agent Desktop only.
Enable Reason Code Logging	Select the **Enable Reason Code Logging** check box so that Agent Desktop log files capture log messages for reason codes that agents enter during a contact. ✱ **Note:** **Enable Reason Code Logging** generates logging inside Agent Desktop only.
Enable Advanced Audio Controls for Softphone	Select the **Enable Advanced Audio Controls for Softphone** check box to allow an agent to control Receive Gain and Transmit Gain, which allows agents to change the audio level of the incoming and outgoing speech path when Agent Desktop is in the My Computer mode.
LDAP Phonebook Unique Key	Enter the LDAP attribute that Agent Desktop uses to uniquely identify any entries that agents search for in the LDAP server. The default value is objectGUID, which is the default Microsoft Active Directory unique identifier.
LDAP Phonebook Display Name	Enter the LDAP attribute that Agent Desktop uses as the primary display field in Phonebook.
Barge-in Wait Time	Enter the time in seconds between a Supervisor initiating an observe and having the ability to initiate a barge-in on the same contact. The default value is 5 seconds.
Supervisor Observe window refresh delay	Enter the time in seconds between an agent answering a new contact and the supervisor control refreshing to display this contact. The default value is 1 second.
Replace + with trunk access code	Select the **Replace + with trunk access code** check box so that Agent Desktop Phonebook adds a trunk access code before dialing any number. Therefore, agents do not need to manually add a leading digit to call externally or forward a call using Phonebook.

Table continues…

Name	Description
	By default, **Replace + with trunk access code** is selected.
Auto Sign On to CCMM	Select the **Auto Sign On to CCMM** check box so that agents do not need to login separately to CCMM when logging on to Agent Desktop.

Configuring User Settings

About this task

The User Settings page contains configuration settings that you can customize for the Agent Desktop.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Agent Desktop Configuration**.
3. Click **User Settings**.
4. Update the required settings.
5. Click **Save**.

Variable definitions

Name	Description
Open Queue Contact Processing	Select the **Open Queue Contact Processing** check box to use Contact Center Multimedia to route multimedia contacts to agents by using the existing scripting and skillset routing features available for calls. You must install and license the Open Queue feature for Agent Desktop and configure Open Queue on the Contact Center server.
Display Customer History on Voice Contact	Select the **Display Customer History on Voice Contact** check box to display customer history for voice contacts on Agent Desktop. Contact Center Multimedia searches for customer history of previous contacts based on the calling line ID for voice contacts.

Table continues…

Name	Description
Display Customer History on Personal Calls	Select the **Display Customer History on Personal Calls** check box to display customer history for voice contacts on personal calls on Agent Desktop.
Voice Contact Identifier for Customer History	Select either **AD_CLID** or **SIP_FROM_ADDRESS** to look up the Contact Center Multimedia database that contains customer history for the originator of the incoming voice call. In order to search the database you must also enable the Voice Contact Search parameter.
Encoding Page of CCT Attached Data	Select the value that determines the decode Code Page used to convert the Binary Attached Data stream to a String contact types for the configured intrinsics. This is used to retrieve the Skillset Name. The system supports the following cases: • The default encoding, that is, the encoding specified in the regional settings for the computer executing this method • little-endian Unicode (UTF-16LE) • big-endian Unicode (UTF-16BE) • Windows operating system (windows-1252) • UTF-7 • UTF-8 • ASCII • Latin1 • GB18030 (Chinese Simplified) • CodePage Name • 1200 “UTF-16LE”, “utf-16”, “ucs-2”, “unicode”, or “ISO-10646-UCS-2” • 1201 “UTF-16BE” or “unicodeFFFE” • 1252 “windows-1252” • 65000 “utf-7”, “csUnicode11UTF7”, “unicode-1-1-utf-7”, “unicode-2-0-utf-7”, “x-unicode-1-1-utf-7”, or “x-unicode-2-0-utf-7” • 65001 “utf-8”, “unicode-1-1-utf-8”, “unicode-2-0-utf-8”, “x-unicode-1-1-utf-8”, or “x-unicode-2-0-utf-8” • 20127 “us-ascii”, “us”, “ascii”, “ANSI_X3.4-1968”, “ANSI_X3.4-1986”, “cp367”, “csASCII”, “IBM367”, “iso-ir-6”, “ISO646-US”, or “ISO_646.irv:1991”

Table continues…

Name	Description
	• 54936 “GB18030”
Attachment Upload Timeout	Enter the time in seconds after which the Communication Control Toolkit server session expires during uploading an attachment.
Suppress Browser Script Errors	Select the **Suppress Browser Script Errors** check box to suppress browser script errors.
Display Not Ready Reason Text Only	Select the **Display Not Ready Reason Text Only** check box to display only not ready reason text.
Display Voice Calls in Customer History	Select the **Display Voice Calls in Customer History** check box to display previous voice calls for the originator of the current active contact in Agent Desktop. Enable this setting to lookup the Contact Center Manager Server database for Voice Contact history. Enable **Contact Summary Data generation** in Contact Center Manager Administration, to ensure that individual contact history data is created in the Contact Center Manager Server database.
Number of Personal IM's Allowed To Go Ready	Enter the maximum number of open IM's an individual agent is allowed before the agent is not allowed to go ready. The number of personal IM's an agent is allowed open on Agent Desktop at one time cannot exceed the number configured in this field.
Audible Alert Setting	Select the type of alert Agent Desktop plays when contacts are presented to agents. There are four options: • NONE. No alert is played. • BEEP. The agents internal sound card is played as the alert. • WAV. A .wav audio file is played as the alert. • BOTH. Both the WAV and BEEP settings work.
Play Alert on Voice	Select the **Play Alert on Voice** check box to ensure an alert is played when voice contacts are presented to agents.
Play Alert on CCMM	Select the **Play Alert on CCMM** check box to ensure an alert is played when multimedia contacts are presented to agents.
Source of WAV	Select **MM**. This determines that the .wav file played is a CCMM .wav file.
Display Caller's Friendly Name	Select the **Display Caller's Friendly Name** check box to enable a friendly name display on Agent

Table continues…

Name	Description
	Desktop for DN calls. When this is enabled, when one contact center agent receives a call from another contact center agent, the name of the calling agent (as configured in CCMA) displays on the Agent Desktop of the called agent. **Note:** Both agents must be configured in CCMA for the friendly name to be displayed on Agent Desktop.
Highlight DN Call During Transfer	This setting determines which leg of the call has focus on Agent Desktop during a supervised transfer — the original customer leg or the DN leg to the transfer party. Select **Highlight DN Call During Transfer** to focus the DN leg to the transfer party on Agent Desktop during a supervised transfer.
Put Call on Hold During Transfer for the Phonebook	Select the **Put Call on Hold During Transfer for the Phonebook** check box to place the customer call on hold when an agent initiates a call transfer, using the Phonebook on Agent Desktop.
Observe Agent Initiated Contact Center Calls	Select the **Observe Agent Initiated Contact Center Calls** check box to allow agent-supervisors to use the Observe function to listen in on an agent-initiated voice contact.
Taskbar Alert on New WebComms Message	Select the **Taskbar Alert on New WebComms Message** check box to configure a taskbar alert, when a new web communication message arrives, on the Agent Desktop.
Clear Previous Phone Number	Select the **Clear Previous Phone Number** check box to clear the number of the previous voice contact present on Agent Desktop.
Clear Previous E-mail Address	Select the **Clear Previous E-mail Address** check box to clear the email address of the previous email contact present on Agent Desktop.
Maximum Number of Agent Initiated E-mails	Enter the maximum number of email messages an agent can initiate. **Note:** By default, the maximum number of email messages that an agent can initiate is 5.
Web Comms/IM Tab Blink Duration	Enter the time, in seconds, for which the Web Communications Tab must blink on Agent Desktop.

Table continues…

Name	Description
	Note: By default, the Web Communications tab blinks for 5 seconds on Agent Desktop.
Web Stats Ticker Duration	Enter the time, in seconds, for which the Web Statistics ticker displays for each skillset. **Note:** By default, the Web Statistics ticker displays for 10 seconds for each skillset on Agent Desktop.
Display Agent Login Duration	Select the **Display Agent Login Duration** check box to display the time that the agent is logged into Agent Desktop.
Show CCMM Contact ID in Workitem	Select the **Show CCMM Contact ID in Workitem** check box to display the Contact ID for multimedia contacts for the Work Item present on Agent Desktop.
Close IM Popout Window Automatically When Session Has Ended	Select the **Close IM Popout Window Automatically When Session Has Ended** check box to close the IM popout window automatically when the agent completes the IM contact on Agent Desktop. **Note:** **Close IM Popout Window Automatically When Session Has Ended** is applicable only to contact centers that have IM enabled and by default this check box is selected in the CCMM Administration utility.
Decline Personal IM Automatically When Agent Busy On Contact	Select the **Decline Personal IM Automatically When Agent Busy On Contact** check box to refuse personal IM messages automatically when the agent is busy with a contact on Agent Desktop. **Note:** **Decline Personal IM Automatically When Agent Busy On Contact** is applicable only to contact centers that have IM enabled and by default this check box is selected in the CCMM Administration utility.
Maximum Number of E-mail Recipients	Enter the maximum number of people to whom an agent can send an email message.

Table continues…

Name	Description
	Note: By default, the maximum number of people to whom an agent can send an email message is 30.
Force Send Emails	Select the **Force Send Emails** check box to provide agents with the option to override an email address validation failure and send an email message even when the system detects an invalid email address.
Mandatory Comments for Email Approval	Select the **Mandatory Comments for Email Approval** check box to make review comments mandatory when supervisors approve or reject an email message.
Pull Contact On Same Skillset Only	Select the **Pull Contact On Same Skillset Only** check box so that agents can pull contacts only from the skillsets that the agents are currently assigned to.
Show All Email Skillsets	Select the **Show All Email Skillsets** check box so that agents can see all the skillsets configured in Contact Center when they are initiating an outgoing email. If you do not select the **Show All Email Skillsets** check box, agents see only the email skillsets to which they are currently assigned.
Web Stats Refresh Interval	Enter the time in seconds after which the Web Statistics information refreshes. **Note:** By default, the Web Statistics information refreshes every 60 seconds.
Web Stats Exception Limit	Enter the number of Contact Center Web Statistics (CCWS) connection exceptions allowed before the system disables the statistics feature. **Note:** If you enter zero in the **Web Stats Exception Limit** field, the statistics feature is never disabled.
Number of Rings on Voice Alert	Enter the number of times the agent phone rings when a voice contact alerts on Agent Desktop. **Note:** By default, the agent phone rings 5 times when a voice contact alerts on Agent Desktop.

Table continues…

Name	Description
Number of Alert Tones for Multimedia Contacts	Enter the number of alert tones that can be defined for Multimedia contacts. **Note:** By default, 5 alert tones can be defined for Multimedia contacts.
Maximum Roster Size	Enter the maximum number of IM contacts that agents can add to the **My Contacts** list in Agent Desktop. By default, 150 contacts are defined.
Force Logout Delay	Enter the time, in seconds, the system displays the `You've Been Logged Out` alert before shutting down Agent Desktop, after a supervisor remotely logs an agent out of Contact Center from the Contact Center Manager Administration (CCMA) user interface. **Note:** By default, the system displays the `You've Been Logged Out` alert for 60 seconds.
Display System Defined Contact Center Codes	Select the **Display System Defined Contact Center Codes** check box so that Agent Desktop displays system-defined Not Ready Reason Codes and After Call Work Item codes.
Contact Center Code Display Preference	Select how Agent Desktop displays Contact Center codes. You can choose from the following: • Code. Agent Desktop displays Contact Center codes based on the code number. • Text. Agent Desktop displays Contact Center codes based on the code text. • Both. Agent Desktop displays Contact Center codes based on both the code number and the code text. **Note:** You can select **Contact Center Code Display Preference** only if you select the **Display System Defined Contact Center Codes** check box.
Enable Keyboard Shortcuts	Select the **Enable Keyboard Shortcuts** check box so that shortcut keys are enabled in Agent Desktop, and agents can use shortcut keys to perform common tasks on Agent Desktop.

Table continues…

Name	Description
	Note: By default, **Enable Keyboard Shortcuts** is selected in the CCMM Administration utility.
Allow Custom Contacts	Select the **Allow Custom Contacts** check box so that agents can add custom contacts to Phonebook in Agent Desktop. Custom contacts are personal contacts of the agents and are not present in the LDAP directory.
Maximum Number of Custom Contacts	Enter the maximum number of custom contacts that agents can add to Phonebook in Agent Desktop.
Log Call History	Select the **Log Call History** check box so that calls made by agents are logged. Agents can view the call history in the **Call History** tab of Phonebook in Agent Desktop.
Allow Erasing of Call History	Select the **Allow Erasing of Call History** check box so that agents can erase the call history from the **Call History** tab of Phonebook in Agent Desktop.
Append Selected Auto Phrase to Existing Text	Select the **Append Selected Auto Phrase to Existing Text** check box so that agents can add an automatic phrase to an existing chat message or email message.
Allow Agent Desktop Panel Swap	Select the **Allow Agent Desktop Panel Swap** check box so that agents can move the **Left Pane** of Agent Desktop to the right side of Agent Desktop and vice-versa.
Autostart Quality of Service Window Service	Select the **Autostart Quality of Service Window Service** check box so that the Quality of Service (QoS) service automatically starts. **Note:** This is only applicable to Avaya Aura® environments, where embedded softphone is used in My Computer mode.
Enable AAAD System Tray Icon	Select the **Enable AAAD System Tray Icon** check box so that agents can add the **Avaya Aura Agent Desktop** system tray icon to the Windows system tray.
Enable AAAD Dashboard	Select the **Enable AAAD Dashboard** check box so that agents can collect and upload log files or videos to the CCMM server. Agents can also use the Dashboard to check the connectivity of Agent Desktop with the Contact Center servers.

Table continues…

Name	Description
	Note: By default, **Enable AAAD Dashboard** is selected in the CCMM Administration utility.
Prompt User for Login Details	Select the **Prompt User for Login Details** check box to automatically prompt agents to enter their credentials when Agent Desktop opens. If you do not select **Prompt User for Login Details** Agent Desktop tries to log in the agent using the current windows user credentials. If this login fails, Agent Desktop prompts the user to enter a set of credentials.
Disallow Duplicate Login	Select the **Disallow Duplicate Login** check box to prevent Agent Desktop from opening if the specified user ID is already logged into Contact Center from a different location.
Enable AAAD Preference Retention	Select the **Enable AAAD Preference Retention** check box to retain agent preferences when agents log back on to Agent Desktop after previously logging out.
Enable Localization	Select the **Enable Localization** check box to enable localization of Agent Desktop when a supported locale is detected on the client computer.
Default Not Ready Reason Code when Rejecting a Contact	Enter the default Not Ready Reason code that the system sends when an agent is forced into the Not Ready state after rejecting a contact. If the **Default Not Ready Reason Code when Rejecting a Contact** field is blank the agent is forced into the Not Ready state with a Reject Contact Default Code (000).
Default Not Ready Reason Code when Pulling a Contact	Enter the default Not Ready Reason code that the system sends when an agent is forced into the Not Ready state after pulling a contact. If the **Default Not Ready Reason Code when Pulling a Contact** field is blank the agent is forced into the Not Ready state with a Pull Mode Default Code (0000).
Default Not Ready Reason Code After Max Open Duration	Enter the default Not Ready Reason code that the system sends when an agent is forced into the Not Ready state when a contact is open for longer than the **Maximum Open Duration** and the contact is recycled. The CCMM Administration utility does not allow the **Default Not Ready Reason Code After Max Open**

Table continues…

Name	Description
	Duration field to be left blank. By default, the agent is forced into the Not Ready state with a MaxOpen Default Code (000).
Home Page Enabled	Select the **Home Page Enabled** check box so that Agent Desktop displays the **Home Page** button on the Agent Desktop toolbar. Agents can use the **Home Page** button to reopen the Agent Desktop home page. The Agent Desktop home page displays a screen pop that contains a Web URL that you configure to open when an agent starts Agent Desktop.
Home Page URL	Type the web URL of the Agent Desktop home page. The home page displays a screen pop that contains this web page when an agent starts Agent Desktop.
Home Page Name	Type the name of the home page that Agent Desktop displays when an agent starts Agent Desktop.
Close Multiple Contacts	Select the type of user that can close multiple contacts simultaneously from search results. You can select one of the following options: • Supervisor. Select **Supervisor** to allow supervisors to close multiple contacts. • Agent. Select **Agent** to allow agents to close multiple contacts. This is the default option. • None. Select **None** so that no user has the permission to close multiple contacts.
Maximum Number of Calls to Log	Enter the maximum number of calls for which the call history is logged. Agents view the call history in the **Call History** tab of Phonebook in Agent Desktop.
Maximum Number of Speed Dials	Enter the maximum number of contacts that agents can add to their speed dial list in Phonebook.
Maximum Number of Favorites	Enter the maximum number of contacts that agents can add as favorites in Phonebook.
Contact Lookup Priority	Enter the order by which the system performs the caller name lookup. You can select one of the following options: • Custom contacts. Select **Custom contacts** so that the system performs caller name lookup from within the agent's Custom Contacts.

Table continues…

Name	Description
	• LDAP contacts. Select **LDAP contacts** so that the system performs caller name lookup from within LDAP contacts. • Intrinsics / Call property. Select **Intrinsics/Call property** so that the system performs caller name lookup by using the name taken from either an intrinsic property or a property on the call object. When a name matches the number on the incoming call, Agent Desktop displays that name on the user interface.
Insert Line Break Before Auto Response	Select the **Insert Line Break Before Auto Response** check box to add a blank line before the auto response is sent to the customer.
Display Agent Time in Not Ready State	Select the **Display Agent Time in Not Ready State** check box to display a timer on Agent Desktop that displays the duration the agent is in the Not Ready state.
Display Softphone Out Of Service Message on Start-up	Select the **Display Softphone Out Of Service Message on Start-up** check box to display a message box alerting agents that the CTI Link to the softphone is out of service while starting Agent Desktop in applicable configurations. The system also displays a message box to alert the agent that the softphone is now in service, after agents log using My Computer mode.
Show Original Action When Pulling MM Contact	Select the **Show Original Action When Pulling MM Contact** check box so that Agent Desktop displays the original action when pulling a contact. If you do not select the **Show Original Action When Pulling MM Contact** check box then Agent Desktop displays the most recent action when pulling a contact. An example of an original action is an email message that is sent by a customer. The most recent action is an agent's reply to the original email message.
Pop Up Notification – Closes After Time	Select the **Pop Up Notification – Closes After Time** check box so that the pop-up messages related to Teleworker Status on Agent Desktop disappear automatically after a certain configured time.

Table continues…

Name	Description
Pop Up Notification – Display Time	Enter the length of time, in milliseconds, that the Teleworker Status pop-up messages stay visible on Agent Desktop.
Teleworker Recovery Button – Click Delay	Enter the time in milliseconds that sets the Click Delay time. The Click Delay time limits how quickly Agent Desktop registers clicks to the Teleworker Recovery Button. When agents click on the Teleworker Recovery Button on Agent Desktop, Contact Center attempts to reinitiate the nail-up call.
Bring AAAD to Front when Max Open Duration Exceeded	Select the **Bring AAAD to Front when Max Open Duration Exceeded** check box to automatically bring Agent Desktop to the front of the desktop when a contact is open for longer than the configured Maximum Open Duration.
Display Disposition Codes Names	Select the **Display Disposition Codes Names** check box so that Agent Desktop uses the **DisplayName** field to display disposition codes. By default, Agent Desktop uses the **Name** field to display disposition codes. Outbound Campaign Management Tool uses the **DisplayName** field to display disposition codes.
Show Web Comms System Prompts	Select the **Show Web Comms System Prompts** check box to display a message when an agent pushes a page to a customer. This message precedes the page push URL.
Use call attached data for skillset information	Select the **Use call attached data for skillset information** check box to display call attached data instead of the skillset intrinsic on contacts in Agent Desktop for AML-based contact centers.
Notify an Agent if a Contact is being Observed/ Barged-In On	Select the **Notify an Agent if a Contact is being Observed/Barged-In On** check box, so that Agent Desktop displays an icon on a work item when a supervisor/agent observes, whisper coaches, or barges-in on a call.
Display Observable Contacts of Logged Out Agents	Select the **Display Observable Contacts of Logged Out Agents** check box to allow supervisor/ agents to see non-skillset calls of agents who are logged out of Agent Desktop. Supervisor/agents can see agent calls only where the agent uses CCT to log on to the desk phone.
Display Supervisor Observe Color Coding	Select the **Display Supervisor Observe Color Coding** check box, so that Agent Desktop uses color coding on the **Supervisor Observe** dialog to

Table continues…

Name	Description
	distinguish between skillset, non-skillset, observed, barged-in, and whisper coached calls and contacts.
Suppress OS softphone not supported popup	Select the **Suppress OS softphone not supported popup** check box to suppress a warning message that the softphone process is not supported on the Operating System on which Agent Desktop is running. By default, the **Suppress OS softphone not supported popup** option is not selected.
Enable one click copy of caller line ID	Select the **Enable one click copy of caller line ID** check box to allow agents to use the **Copy CLID** button on the Agent Desktop toolbar to copy the Calling Line Identification (CLID) number of a customer to the clipboard. Agent Desktop displays the name of the caller using the contacts directory integration.
Maximum signature image file size	Enter a number that specifies the maximum file size for images that agents can add when creating a signature in Agent Desktop. Administrators can specify a value between 1 and 50 KB.
Maximum Number of Images Allowed Per Signature	Enter a number that specifies the maximum number of images that agents can add when creating a signature in Agent Desktop. Administrators can specify a value between 0 and 3. The default value is 3.
Maximum number of characters Per Email Signature	Enter a number that specifies the maximum number of characters that agents can add when creating a signature in Agent Desktop. Administrators can specify a value between 0 and 2000. The default value is 2000.
Force all agents to use a not ready reason code when going not ready	Select the **Force all agents to use a not ready reason code when going not ready** check box to force agents and supervisor/agents to enter a Not Ready reason code when changing their status to Not Ready.
Display Previous Login Time	Select the **Display Previous Login Time** check box so that Agent Desktop displays the previous login time for the currently logged in agent. The login time displayed is the time of the Contact Center server and not the local time of the agent.
Show agent comments for external transfer	Select the **Show agent comments for external transfer** check box so that agent comments are added to an email that is transferred externally. By default, the **Show agent comments for external transfer** option is not selected.

Table continues…

Name	Description
Put Call on Hold During Transfer/Conference for the Enter Value	Select the **Put Call on Hold During Transfer/ Conference for the Enter Value** check box to place the customer call on hold when an agent initiates a call transfer or conference by entering the number in Agent Desktop.
Critical level of free Virtual Memory in MB	Enter the minimum amount of free RAM in MB that must be present on a client PC. If the free RAM drops below the level specified, Agent Desktop displays a warning message. By default, the minimum amount of free RAM is set at 250 MB.
Enable Unsupported Client OS	Select the **Enable Unsupported Client OS** check box to support Agent Desktop on Citrix and is required for desktop virtualization.
Supported attachment file extensions	Configure the supported file extensions that agents can attach to emails in the **Supported attachment file extensions** field. For information on configuring the supported file extensions, see Restricting file extensions for attachments on page 69.
POM Custom fields sort order	Select the type of sorting that Agent Desktop performs on the custom fields for POM contacts. There are three options: • NO SORT: Agent Desktop displays the custom fields for POM contacts in the same order as received from the POM server. This is the default option. • ASC.: Agent Desktop displays the custom fields for POM contacts in an ascending order. • DESC.: Agent Desktop displays the custom fields for POM contacts in an descending order.

Configuring IIS to support MDB database file attachments in email messages

About this task

Configure Internet Information Services (IIS) to support Microsoft Access MDB files as attachments in Agent Desktop email messages. By default, IIS filters MDB file attachments.

Procedure

1. Log on to the CCMM server with administrative privileges.
2. On the **Desktop**, select **Administrative Tools**.

3. Select **Internet Information Services (IIS) Manager**.
4. In the left pane, navigate to the **Default Web Site**.
5. In the middle pane, in the **IIS** section, select **Request Filtering**.
6. From the **File Name Extensions** list, right-click **.mdb** and select **Remove**.
7. On the **Confirm Remove** message box, click **Yes**.
8. From the main **Internet Information Services (IIS) Manager** menu, select **File** > **Exit**.

Chapter 6: Email configuration

This chapter describes how to set up your contact center with the optional configurations for routing email contacts to fulfill your customer requirements.

When you commission your contact center, you configure the email server, a default email skillset, and a default recipient with at least one rule group. The default settings ensure email messages go only to an agent with the ability to handle email messages. You can customize your contact center with additional skillsets, rule groups and email servers.

To further enhance your customer service, you can configure routing tools to use in rule groups. Use keyword groups and sender groups to decide how to route contacts. Configure which skillset and priority the email contact is assigned to based on the input for routing contacts. Use automatic suggestions for the agent to reply quickly to an email or automatic responses to send a reply to the customer without agent interaction. You can close the contact immediately after the automatic response. This chapter describes how to configure all optional routing tools.

You can configure outbound email settings, such as which skillset to use as a reply address and a list of email addresses that must not receive automatic responses. For each skillset you use to route contacts, you can have a signature with your corporate branding or special information based on the skillset.

Other types of contacts generate email messages that are routed using the inbound and outbound email options.

Reports appear in the Contact Center Multimedia Administration utility to show the current status of the email traffic. The following reports appear when you select email and View Reports in the left column of the Contact Center Multimedia application. You can choose the report date and the skillsets represented in all displayed real-time reports.

- Email (New Vs. Closed) shows the number of contacts in a new and closed state against the time for the selected date and skillsets.
- Email Progress shows the number of contacts in a new or closed state on a defined date to determine the traffic levels for that date.
- Email Closed Contacts Queue Time shows the average time an email contact spends in queue while the contact center is open.

You can configure general email settings to minimize space and format special characters for other languages.

Configuring the email server names

About this task

Configure the email server names to identify the inbound server (POP3 or IMAP) for email messages received by the contact center and the outbound server (SMTP) for email messages sent by the contact center.

If you configured the email servers during installation and the names of the inbound and outbound email servers remain unchanged, you can skip this procedure.

You can configure secondary inbound and outbound email servers. If a primary email server fails, the email retrieved during the failure is duplicated in the Multimedia database when you restore the primary server.

Avaya recommends that you use POP3 as the inbound protocol to receive email messages.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **General Administration**.
3. Click **Server Settings**.
4. Under Edit Current Servers select **Inbound Mail Server**.
5. Click **Edit**.
6. In the **Primary Hostname** field, type the name of the server that receives email messages.
7. In the **Inbound Protocol** field, select the protocol that is used for receiving email messages. You can choose one of the following:
    - **IMAP**
    - **POP3**
8. In the **Encryption** field, select the security protocol that is used for receiving email messages. You can choose one of the following:
    - **Clear Text** (Default)
    - **TLS**
    - **STARTTLS**
9. In the **Port Number** field, type the port number for the email server.
10. If you have a backup email server, in the **Secondary Hostname** field, provide a host name for the backup server.
11. Click **Save**.
12. Under Edit Current Servers, select **Outbound SMTP Server**.
13. Click **Edit**.
14. In the **Primary Hostname** field, type the name of the server that sends email messages.

15. In the **SMTP Authentication** field, select the SMTP authentication, if required, for your outbound email server.
16. In the **Encryption** field, select the security protocol that is used for sending email messages. You can choose one of the following:
    - **Clear Text** (Default)
    - **TLS**
    - **STARTTLS**
17. In the **Port Number** field, type the port number for the email server.
18. If you have a backup email server, in the **Secondary Hostname** field, provide a host name for the backup server.
19. Click **Save**.

Variable definitions

Name	Description
Port Number	Port number for the email server.
Primary Hostname	The name of the server that receives email messages.
Secondary Hostname	Name of a secondary email server, if one is available in your contact center.

Adding an email server

About this task

Add or update the email server for your Contact Center Multimedia server so you can poll multiple email servers in your contact center for email messages to be routed. You can retrieve email messages for the contact center only if you are licensed to use the email feature.

If you select TLS or STARTTLS as the encryption type for incoming or outgoing mail, you must add a valid certificate on the Contact Center Multimedia server. For more information, see Adding a certificate for use with TLS email connections on page 124.

Avaya recommends that you use POP3 as the inbound protocol to receive email messages.

❗ **Important:**

Contact Center Multimedia supports adding a maximum of five POP3 or IMAP servers as inbound email servers and five SMTP servers as outbound email servers. You can have a mix of email servers that have POP3 or IMAP protocols for receiving email messages and SMTP protocol for sending email message with a mix of TLS, STARTTLS, and no security channels.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **General Administration**.
3. Click **Server Settings**.
4. Under Edit Current Servers, click **New**.
5. Select **Inbound Mail Server** to add a new inbound email server.
6. In the **Primary Hostname** field, type the name of the server that receives email messages.
7. In the **Inbound Protocol** field, select the protocol that is used for receiving email messages. You can choose one of the following:
    - **IMAP**
    - **POP3**
8. In the **Encryption** field, select the security protocol that is used for receiving email messages. You can choose one of the following:
    - **Clear Text** (Default)
    - **TLS**
    - **STARTTLS**
9. In the **Port Number** field, type the port number for the email server.
10. If you have a backup email server, in the **Secondary Hostname** field, provide a host name for the backup server.
11. Click **Save**.
12. Under Edit Current Servers, click **New**.
13. Select **Outbound SMTP Server** to add a new outbound email server.
14. Click **Edit**.
15. In the **Primary Hostname** field, type the name of the server that sends email messages.
16. In the **SMTP Authentication** field, select the SMTP authentication, if required, for your outbound email server.
17. In the **Encryption** field, select the security protocol that is used for sending email messages. You can choose one of the following:
    - **Clear Text** (Default)
    - **TLS**
    - **STARTTLS**
18. In the **Port Number** field, type the port number for the email server.
19. If you have a backup email server, in the **Secondary Hostname** field, provide a host name for the backup server.

20. Click **Save**.

Deleting an email server

About this task

Delete an email server or other nonessential server if the server is no longer required.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **General Administration**.
3. Click **Server Settings**.
4. Select the sever to delete.
5. Click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion.

Configuring skillsets for email

Before you begin

- If required, configure an office hour template. See Configuring office hours on page 44 and Configuring holidays on page 44.

About this task

Configure a route point for each skillset, to use the skillsets in rules. A route point is a location on the open queue that enables incoming calls to be queued and run through a script on the Contact Center Manager Server.

An automatic signature is text automatically added at the bottom of an outgoing message. For example, you can encourage customers to visit your customer support website by adding the URL and other promotional information to every message. You can also use the automatic signature to add disclaimer text to messages.

You can also apply an office hours template for your skillset. If agents in a different time zone or different department have a different set of office hours, you can apply an office hour template that is different from the global office hours schedule configured in general email settings to this skillset.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **General Administration**.
3. Click **Skillset Settings**.
4. Select a skillset for which to assign a route point.
5. Click **Edit**.
6. From the **Route Point** list, select the route point to assign to the skillset.
7. Under **Office Hours**, choose an office hour template that gives the office hours particular to the selected skillset.
8. If applicable, in the **Auto Signature** box, type the signature to assign to the skillset.
9. Click **Save**.

Creating or changing a recipient mailbox

Before you begin

- Ensure that any enabled email address you want to configure in the Email Manager is already configured on your corporate email server.

About this task

Create a recipient email box to ensure that at least one email box is configured for your contact center. You must configure one recipient to commission the server. You can create additional mailboxes to have the Contact Center Manager Server poll a mailbox on the email server and handle contacts based on the recipient address.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **Recipient Addresses**.
4. Click **New**.

   OR

   Select a recipient address, and click **Edit**.
5. If you select **New**, select **Mail Store** from the **Mailbox Type** list.
6. Under Mailbox Details, in the **Mailbox** box, type the SMTP mailbox name.
7. In the **Domain** field, type the domain for your email server.

8. In the **Display Name** field, type the name to appear in the email From address.
9. In the **Password** field, type the password for the mailbox.

   Important:

   When you change a password on the email server, you must update this password in the Multimedia Administration Tool.
10. In the **Confirm Password** field, type the same password you typed in the Password box.
11. In the **Inbound (POP3) Server** field, select the host name of your POP3 or IMAP server along with the respective security protocol.
12. In the **Inbound Mail Threshold** field, type the maximum number of email messages to be retrieved from the mailbox every scan interval.

    You can enter a different value for this variable for each mailbox.
13. In the **Outbound SMTP Server** field, select the host name of your SMTP server.
14. In the **Rule Group** field, select the name of the Rule Group to assign to the recipient mailbox.
15. Click **Save**.

Variable definitions

Name	Description
Display Name	The name to appear in the email From address. For example, Sales Department.
Domain	The domain name for the email server.
Mailbox	The name of a mailbox on the email server. If the Contact Center Multimedia server is in the same domain as the email server, in the Mailbox Name box, type the address, and in the E-mail Domain box, type the domain name. If the Contact Center Multimedia server is not in the same domain as the email server, and you are using Windows 2000, in the Mailbox Name box, type the address in the format domain\user. If the Contact Center Multimedia server is not in the same domain as the email server, and you use a version of Windows later than Windows 2000, in the Mailbox Name box, type the address in the format user@domain.

Table continues…

Name	Description
	❗ **Important:** Mailbox names are case-sensitive. You must type the mailbox name exactly as it appears on your server.
Username	The username used to access the mailbox on the email server.
Password and Confirm	The password used to access the mailbox on the email server. Type the password in the Confirm box to ensure accuracy. Contact Center Multimedia supports a maximum mailbox password length of 100 characters.
Inbound Mail Threshold	The maximum number of email messages to be retrieved from the mailbox every scan interval. You can enter a different value for this variable for each mailbox. The default value is 10.
Rule Group	The name of the rule group that applies to this recipient mailbox. Configure rule group properties in the Contact Center Multimedia Administrator.
Inbound (POP3 or IMAP) Server	The name of the email server, either POP3 or IMAP, that handles email messages coming into the contact center.
Outbound (SMTP) Server	The name of the email server that delivers email messages that leave the contact center.

Creating or changing an alias for a recipient mailbox

Before you begin

- Ensure that any enabled email address you want to configure in the Email Manager is already configured on your corporate email server.
- Configure a mail store recipient mailbox. See Creating or changing a recipient mailbox on page 93.

About this task

Create an alias, or another name, for the recipient email box.

For example, the mailbox general@magscripts.com can have the aliases carz@magsubscriptions.com and planez@magsubscriptions.com. Email messages addressed to either alias are forwarded to the general@magscripts.com mailbox. The Email Manager routes the email messages according to the alias-based rules.

Aliases can be useful to filter email messages. For example, you can define an alias for a short promotional period after which email messages that arrive at that alias are discarded.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **Recipient Addresses**.
4. Click **New**.

   OR

   Select the alias and click **Edit**.
5. In the **Mailbox Type** list, select **Alias**.
6. Under **Mailbox Details**, in the **Mailbox** box, type the SMTP mailbox name.
7. In the **Domain** box, type the domain for your email server.
8. In the **Display Name** box, type the name of the alias set up on the email server.
9. In the **Rule Group** box, select the name of the Rule Group to assign to the alias for the recipient mailbox.
10. In the **Outbound SMTP Server** box, ensure that the host name of your SMTP server appears.
11. Select the **Use alternative username for SMTP Authentication** check box if you configure an inbox as an alias.

    If SMTP authentication is enabled on your email server, and you use aliases, log on to the SMTP server with a different user name.
12. In the **Username** box, type the username of the mail store recipient address.
13. In the **Password** box, type the password of the mail store recipient address.

    Important:

    When you change a password of the mail store recipient address on the email server, you must update this password in the Multimedia Administration Tool.
14. In the **Confirm Password** box, type the same password you typed in the Password box.
15. Click **Save**.

Variable definitions

Name	Description
Alias	An alias is an address that forwards all email messages it receives to another email account.
Display Name	The name to appear in the email From address.

Table continues…

Name	Description
	For example, Sales Department.
Domain	The domain name for the email server.
Mailbox	The name of a mailbox on the email server. If the Contact Center Multimedia server is in the same domain as the email server, in the Mailbox Name box, type the address, and in the E-mail Domain box, type the domain name. If the Contact Center Multimedia server is not in the same domain as the email server, and you are using Windows 2000, in the Mailbox Name box, type the address in the format domain\user. If the Contact Center Multimedia server is not in the same domain as the email server, and you use a version of Windows later than Windows 2000, in the Mailbox Name box, type the address in the format user@domain. **Important:** Mailbox names are case-sensitive. You must type the mailbox name exactly as it appears on your server.
Username	The username used to access the mailbox on the email server.
Password and Confirm	The password used to access the mailbox on the email server. Type the password in the Confirm box to ensure accuracy. Contact Center Multimedia supports a maximum mailbox password length of 100 characters.
Rule Group	The name of the rule group that applies to this recipient mailbox. Configure rule group properties in Contact Center Multimedia Administrator.
Outbound (SMTP) Server	The name of the email server that delivers email messages that leave the contact center.

Deleting a recipient mailbox

Before you begin

- Before you delete a mailbox, you must ensure that no email messages are sent to the inbox and no aliases are directed to that mailbox.
- Avaya recommends that you archive all contacts associated with a recipient before you delete the recipient.

About this task

Delete a recipient mailbox from your system if you no longer require it to monitor email. Removing extra mailboxes saves space in your database.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **Recipient Addresses**.
4. Select the address from the recipient list that you want to delete.
5. Click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion of the recipient mailbox.

Updating the system default rule

Before you begin

- Ensure that you know the default settings for the system delivery failure rule:
  - use the email default skillset, EM_Default_Skillset
  - use no automatic response
  - assign priority 3
- Use caution when you change the properties of the system default rule:
  - If you change the properties of the rule, you affect the behavior of the system default rule, which affects all recipient mailboxes.
  - If you delete the skillset associated with the default rule, EM_Default_Skillset is used.
  - If you delete EM_Default_Skillset, the system stops processing email messages.
- Configure the route points for the skillset you assign to the system default rule. For more information, see Configuring skillsets for email on page 92.

About this task

Update the system default rule to ensure that an email arriving at each configured recipient mailbox is assigned a skillset and can be routed.

When you create a recipient mailbox, the system default rule is copied as the last regular rule into the list of rules for the recipient mailbox.

The automatic signature is text appended to each email message sent from the contact center in addition to the agent message. The text in the automatic signature contains corporate disclaimer information and must be in fixed-width font. The automatic signature appears in an email message after any personal signature, which is configured in the Agent Desktop application.

The system default rule is used in every rule group configured in Contact Center Multimedia.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **System Rules**.
4. Under **System Default Rule**, from the **Skillset** list, select a skillset name.
5. To change the automatic response settings, under **Auto Responses**, select another automatic response from the list.
6. To change the priority, under **Priority**, select a different priority for the contact.
7. Click **Save**.

Variable definitions

Name	Description
Skillset	A label applied to a set of skills, capabilities, or knowledge that an agent requires to respond to a request. The skillsets are retrieved from the Contact Center Manager Server database. You must select a route point for a skillset used to route contacts.
Auto Response	A message sent to a customer with no agent interaction. An automatic response can be an intelligent response, such as a sales promotion flyer, or an acknowledgement, such as, “Thank you for your email. We will respond to you within three days.”
Priority	The priority given to a request for a skillset agent. The lower the priority number, the greater the priority. The values of the priorities range from 1 to 10. For example, a call with priority 1 is handled before a call with priority 10.

Updating the system delivery failure rule

Before you begin

- Ensure that you are licensed to handle email messages.

- Ensure that you know the default settings for the system delivery failure rule:
    - use the email default skillset, EM_Default _Skillset
    - use keyword group delivery failure keywords
    - assign priority 10 (lowest)
- Use caution when you change the properties of the system default rule:
    - If you change the properties of the rule, you affect the behavior of the system default rule, which affects all recipient mailboxes.
    - If you delete the skillset associated with the default rule, EM_Default_Skillset is used.
    - If you delete EM_Default_Skillset, the system stops processing email messages.
- Configure the route point for the skillset you plan to assign to the system delivery failure rule. See Configuring skillsets for email on page 92.

About this task

Update the system delivery failure rule to ensure that any email message that contains particular phrases such as undeliverable, returned mail, unknown recipient, delivery failure, or delivery report is deleted and not assigned to an agent.

When you create a recipient mailbox, the system delivery failure rule is copied as the first regular rule into the list of rules for the recipient mailbox.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **System Rules**.
4. Under **System Delivery Failure** Rule, from the **Skillset** list, select a skillset name.
5. To change the keyword group, under **Keyword Group**, select an existing keyword group from the list.
6. To change the priority, under **Priority**, select a different priority for the contact.
7. Select the **Will close contact** check box to have the rule to close the contact.
8. Click **Save**.

Variable definitions

Name	Description
Skillset	A label applied to a set of skills, capabilities, or knowledge that an agent requires to respond to a request. The skillsets are retrieved from the Contact Center Manager Server database. You must select

Table continues…

Name	Description
	a route point for a skillset used to route outbound contacts.
Keyword group	A list of words that you can search in an email message. Keyword groups associate keywords and expressions considered important by the contact center to be handled in a particular way.
Priority	The priority given to a request for a skillset agent. The lower the priority number, the greater the priority. The values of the priorities range from 1 to 10. For example, a call with priority 1 is handled before a call with priority 10.
Will close contact	Select the check box to close the email contact after the system delivery failure rule determines that the contact is not appropriate for the contact center. Clear the check box to leave the email contact open for review.

Creating or changing a keyword group

About this task

You must assign at least one keyword to a keyword group before you can save the keyword group.

The keyword search in an email message is not case-sensitive. For example, if you add the word John, the Email Manager also matches JOHN and john.

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

You can specify a spelling accuracy in the keyword group.

Keyword groups support only asterisks (*) and question marks (?) as wildcard characters. The asterisk (*) represents multiple characters. For example, t* specifies a list of all the words that start with t. The question mark (?) represents a single character. For example, p?t specifies all three letter words that start with p and end with t.

A keyword does not support the following characters: +-!(){}[]^"~:\&&||#$@€/><,.‘;=%£&¬|`'“. If you use any of these characters in your keywords, you receive an error message stating that the keyword contains invalid characters.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **Keyword Groups**.

4. Click **New** or **Edit**.
5. Under **Keyword Group**, in the **Group Name** box, type a unique name for the keyword group.
6. In the **Keyword** box, type a word or a group of words related to the keyword group you create.
7. Optional: To allow close misspellings of the word, select the **Allow spelling inaccuracies** check box.

   The system displays the following levels of accuracy:

   - **Low (greater than 70% accuracy)**
   - **Medium (greater than 80% accuracy)**
   - **High (greater than 90% accuracy)**
8. Optional: Select the required level of accuracy.
9. Click **>**.

   The keyword or expression is added to the list, and the keyword group is created.
10. Repeat step 6 on page 102 through step 9 on page 102 to add more keywords to the list.
11. Click **Save**.

Variable definitions

Name	Description
Name	Name of the keyword group. The name must be unique and less than 64 characters.
Keyword	A word, or string of characters, used to search the email message for particular text to determine the routing of the contact. A maximum of 50 keywords can be in each keyword group.
Allow spelling inaccuracies	Select the check box to allow small inaccuracies in spelling of words. Specify to allow a spelling inaccuracy of 70%, 80%, or 90% in the keyword list. For example, to allow charles, charlie, and charley in the search for the keyword charlie, you can select a low (70%) degree of accuracy because 2 of the 7 characters or 71% of the characters are correct. Inaccuracies of 80% or 90% do not allow the error.

Deleting a keyword from a keyword group

About this task

Remove a keyword from a keyword group. The remaining keywords and phrases in the keyword group remain active for rules.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **Keyword Groups**.
4. Select a keyword group from the **Keyword Groups** list.
5. Click **Edit**.
6. In the **Keywords in Group** list, select the keyword.
7. Click **Remove**.

   The system displays a Warning dialog box.
8. Click **Yes** to confirm the deletion.
9. Click **Save**.

Deleting a keyword group

About this task

Delete a keyword group. After you remove the keyword group, you cannot use it in any rule. In certain scenarios, rules that use the deleted keyword group do not route the contact as expected.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **Keyword Groups**.
4. Select a keyword group from the **Keyword Groups** list.
5. Click **Delete**.
6. Click **Delete**.

   The system displays a Warning dialog box.
7. Click **Yes** to confirm the deletion.

Creating or changing prepared responses

About this task

There are three types of prepared responses; auto response, chat history header, and auto suggestion.

You can use automatic responses to automatically send responses to a sender without agent intervention. Chat history headers provide email headers for sending chat history to a customer. Suggested responses give agents template text for common responses, which they can review and edit and send as a response. The body of a prepared response is limited to 3900 characters. This limit includes hidden characters such as HTML tags.

You must add a suggested response to a rule group, to make it available to agents on Agent Desktop. To send prepared chat history headers, you must configure a header on each WC skillset.

Prepared responses support both standard and inline attachments. You can add inline attachments such as company logos to the responses. You can include only images as inline attachments. The formats supported are .gif, .bmp, .jpg, and .png.

Agents can also place inline attachments (only as images) in email messages.

Inline attachments display complete information within the body of the email. This makes the information easily accessible to customers, even without explicitly opening the attachment. For example, adding a company logo, as an inline image, increases brand awareness.

Examples of prepared responses include the following:

- provide the customer with their Web logon ID and password (password reminder automatic response)
- inform a customer if your office is closed (out-of-office automatic response)
- acknowledge the receipt of an email contact (automatic response, or an automatic acknowledgement)
- include standard content on a web chat history email
- provide specific information in response to rule inputs (suggested response)

Configuring prepared responses for a rule is optional.

You can create categories for the prepared responses. The categories enhance the ability of the agent to search through the prepared responses on Agent Desktop.

A password reminder and an out-of-hours automatic response are configured by default. You cannot delete the default automatic responses.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **Prepared Responses**.
4. In the **Prepared Responses** table, click **New Response**.

   OR

In the **Prepared Responses** table, select a response, for editing that particular prepared response.

5. In the **Name** box, type or edit the name of the prepared response.
6. In the **Type** box, select the type of response.
7. In the **Subject** box, type or edit the subject of the response email message.
8. In the **Body** box, type or edit the message to include in the response.

   Use the formatting bar described below to apply formats to your email message.
9. **(Optional)** Click the **Image** icon to add images or inline images to the response.

   The system displays the Insert Image dialog box.
10. **(Optional)** Beside the **Attachment** box, click **Add** to add attachments to the response.

    The system displays the Attachment dialog box.
11. **(Optional)** Choose a category for the prepared response to make it easier for agents to navigate on Agent Desktop.
12. Click **Save**.

Variable definitions

Name	Description
Name	The name of the automatic response. The name must be unique.
Type	The type of prepared response. Auto-Response is a reply that Contact Center Multimedia can send automatically when it receives an email message. Chat History Header provides common headers for Web Chat history emails. You must configure this response on each WC skillset for which you want to use this response. Auto-Suggest is a template that agents can use to provide common responses to customers. You must add a suggested response to a rule group, to make it available to agents.
Subject	The subject of the prepared response used as an email message.
Body	The body of the prepared response. The body is limited to 3900 characters. The body can include attachments, formatting, and variables for a customer. To access the variables for the content,

Table continues…

Name	Description
	insert a placeholder by right-clicking the content and selecting the placeholder from the menu.
Categories	The category for the prepared response. Specifying the category makes it easier for agents to find automatic suggestions on Agent Desktop.
Attachments	The attachment is stored on the Contact Center Multimedia server for later use.
Image	Inline images are seen directly within the message body. The inline image file size limit is the same as the current limit set for attachments in Agent Desktop.
Browse	Available only when you select Image. Browse to locate the inline image that you want to include in the email.
Image Address (URL)	Type the url for the inline image that you want to include in the email.
Alternate text	Type the alternative text for the image. Alternate text is what the customer views if their email client cannot display the image.
Align	Select the alignment of the image. The options are inline, left, and right.
Border	Inserts a border around the image. For example, enter 2 to add a double-sized border around the image.
Margin	Inserts a margin around the image.
Insert Image	Insert the inline image.
Cancel	Exit the Inline Attachments fields.

Deleting prepared responses

About this task

Delete the prepared responses that are no longer used by agents in your contact center.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **Prepared Responses**.
4. Select an existing prepared response.

5. Click **Delete Response**.
6. Click **Yes** to confirm the deletion.

Removing attachments from prepared responses

About this task

Remove attachments from a prepared response. The attachment file is stored on the Contact Center Multimedia server for later use.

To remove inline attachments, select the attachment and delete it from the body of the email.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left column, click **E-mail**.
3. Click **Prepared Responses**.
4. Select the prepared response from which you want to remove an attachment.
5. Select the attachment to delete.
6. Beside the **Attachments** box, click **Delete**.

   The system displays a Warning dialog box.
7. Click **Yes** to confirm the deletion.
8. Click **Save**.

Promoting suggested responses

About this task

You can configure prepared responses for agents in the contact center. An agent can use a suggested response during the contact. Contact Center Multimedia tracks the number of times the suggestion is used. If one suggestion is used often, it is considered a strong reply, and then you can promote the suggestion to an automatic response.

Promoting the suggested responses ensures that the customer receives a correct response because the agent checks it. The agent can make small changes to the suggestion until it is acceptable to run as an automatic response.

You can promote the suggested responses to an automatic response based on the following criteria:

- rules where the suggestion is assigned

- number of contacts in the past 30, 60, 90 or 120 days
- list of all suggestions that are used by agents
- number of times the suggestion is used
- percent of total contacts where the suggestion is applied by agents

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **Auto-Suggest Promotion**.
4. Under **Rules**, select the rule for which to promote the suggestion.
5. In the **Number of Contacts in past** box, choose the length of time for which to see the contacts for the selected rule.
6. Under **Auto Suggestions**, review the list of suggested answers.
7. Select the suggestion to promote.
8. If you want to close the contacts with automatic suggestion, select the **Will Close Contacts** box.
9. Click **Promote**.

Creating or changing a sender group

About this task

You must place any sender addresses that you want to track in a sender group. You can use sender groups to route important sender email addresses to particular skillsets.

Using a sender group in a rule is optional.

Sender groups support asterisks (*) as wildcard characters when they are placed in the email address.

Avaya recommends that you have a maximum of 20 sender email addresses in one sender group.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **Sender Groups**.
4. Click **New** or **Edit**.
5. In the **Name** box type a unique name of the sender group.

6. In the **Email Address** box, type an email address.
7. If you know the user is in the contact database, start typing an email address, and then click **Look up email**.

   Email addresses that match the characters appear in the list.
8. Click **Add** to insert the email address you looked up, or click **Add Freeform** to add your typed email address to the sender group.

   This text box supports unicode language.
9. Repeat step 5 on page 108 through step 8 on page 109 to add sender addresses to this sender group.
10. Click **Save**.

Variable definitions

Name	Description
Name	The unique name for the sender group. The name must be less than 64 characters.
Email Address	The email address to add to the sender group.
Addresses in Group	A list of addresses in a group that are reviewed when the system applies a sender group to a rule. You can specify only 50 addresses for each group.

Deleting a sender group

Before you begin

- You must have a sender group. See Creating or changing a sender group on page 108.

About this task

Delete a sender group from your contact center if it is not required in the contact center.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **Sender Groups**.
4. Select the Sender Group you want to remove.
5. Click **Delete**.

The system displays a Warning dialog box.

6. Click **Yes** to confirm the deletion.

Deleting a sender from a sender group

About this task

Remove a sender address from a sender group if it is no longer required. The remaining addresses in the sender group remain active for rules.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **Sender Groups**.
4. Select a sender group from the list.
5. Click **Edit**.
6. Under **Addresses in Group** box, select the email address from the list.
7. Click **Remove**.

   The system displays a Warning dialog box.
8. Click **Yes** to confirm the deletion.
9. Click **Save**.

Creating or changing rules

Before you begin

- If you plan to use office hours for routing email messages, configure your office hours. See Configuring office hours on page 44.
- Configure at least one email skillset. See Configuring skillsets for email on page 92.
- Create keyword groups, if required. See Creating or changing a keyword group on page 101.
- Configure prepared responses (automatic responses or suggestions), if required for the rule. See Creating or changing prepared responses on page 104.

About this task

Create or change a rule to route your email contacts.

A rule is a mechanism for routing email contacts. In your contact center, you receive email messages from the customer, as well as other contacts that are routed using the rules including SMS, Fax, scanned documents, and voice mail.

You can create a rule with one or more of the following routing options:

- determine when the email was received (office hours)
- determine who sent the email (sender groups)
- look for specific characters, words or phrases (keywords)

Rules can send an automatic response to a customer and thus requires no interaction by an agent.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **Rule Groups**.
4. Click **New** or select an existing Rule Group and click **Edit**.
5. Under **Rules**, click the plus sign (+) button.

   OR

   Select an existing rule.
6. Under **Current Search Criteria**, click **New** and choose the criterion to add to the rule.
7. Select the criterion from the **Add New Criterion** drop-down box

   You can choose between **Keyword Match** and **Sender Group**.
8. Click **Go**.
9. Configure the keyword match or sender group to use.
10. Repeat step 5 on page 111 to step 7 on page 111 to select a maximum of five criteria for the rule.
11. Click **OK**.
12. Under **Current Search Criteria**, choose the weightage for each criterion.

    The total weightage must add up to 100 percent.
13. Under **Current Search Criteria Summary**, click the blue text to view the details of each criterion you configure.
14. Click **Next**.
15. To select an automatic response for the rule, under **Available Auto-Responses**, select the configured automatic response, and then click **>**.
16. To select automatic suggestions for the rule, under **Available Auto-Suggests**, select the automatic suggestion you want to include, and then click **>**.

To remove a suggestion, select the suggestion, and then click **<** to remove it from the rule list.

17. Click **Next**.
18. In the General Settings area, in the **Name** box, type a name for the rule.
19. In the **Priority** box, select the priority to assign to the contact.
20. In the **Skillset** box, select the skillset to apply for the rule.
21. If you want to apply the office hours to the email message, click **Will use Office hours**.
22. To close the contact, click **Will Close Contact**.
23. Click **Save**.

Variable definitions

Name	Description
Current Search Criteria	Select the criterion to configure for the rule. Choose Keyword Match to select a keyword group that contains phrases or words to search. Choose Sender Group to select an email address from which the email message is received. Choose a maximum of five criteria for each rule. **Note:** If you select multiple keyword groups that include an 'AND' statement, CCMM detects matches only if all keywords are found in either the subject or body of the email message. CCMM detects no match if some keywords are included in the body and some keywords are included in the subject.
Available Auto Responses	Select the automatic response that you can choose for the rule group. You can choose only one automatic response. Automatic responses under Available Auto Responses show what you can choose. The Automatic responses in the right column show the configuration for this rule.
Available Auto Suggests	Select the automatic suggestions that you can choose for the rule group. You can choose up to five automatic suggestions for future automatic suggestion promotion.

Table continues…

Name	Description
	Automatic suggestions under Available Auto Suggestions show what you can select. The automatic suggestions in the right column show the configuration for this rule.
Name	The name of the rule. The name must be unique and less than 64 characters.
Skillset	Select the name of the skillset to route contacts.
Priority	The priority given to a request for a skillset agent. The lower the priority number, the greater the priority. The values of the priorities range from 1 to 10.
Will use office hours	Select the check box to use the office hours calendar to determine whether the contact center is open or closed.
Will close contact	Select the check box to close the contact when the rule is applied to the contact.
Call Open Interface web service	Select the check box to call a Web service.
Web Service	Select the Web service associated with the rule.

Enabling a rule

About this task

Rules can be enabled within a rule group.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **Rule Groups**.
4. Select a disabled rule.
5. Under **Rules**, click the check mark (√) button.
6. Click **Save**.

Disabling a rule

About this task

Rules can be disabled within a rule group. You can disable the rule functionality without deleting the rule.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **Rule Groups**.
4. Select an enabled rule.
5. Under **Rules**, click the cross (**X**) button.
6. Click **Save**.

Deleting a rule

Before you begin

- Create a rule.

About this task

Permanently delete a rule. After you delete the rule, you cannot use the rule for routing email messages.

You cannot delete the Default Rule.

If you permanently delete a rule, existing contacts for the rule can no longer be archived by rule and any Contacts by Rule reports no longer work. Avaya recommends that you archive all contacts associated with a rule before you delete the rule.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **Rule Groups**.
4. Under **Rules**, select the name of the rule to delete.
5. Click the minus sign (**—**) button.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion.

7. Click **Save**.

Creating or changing rule groups

About this task

Create rule groups to apply to the recipient mailboxes and aliases in your contact center.

A rule is a mechanism to route contacts based on who sent the email (sender groups), to apply treatments based on the time a contact was received (office hours), or to route the contact based on words or phrases (keywords). A rule can also send an automatic response and require no interaction by an agent.

A rule group is an ordered collection of rules that are reviewed and compared to the incoming email in a particular order. Contacts that best match or first match the rule are assigned to the skillset based on the rule that routes the contact. The rule group contains the default rule which routes the contact if no other rule in the rule group matches the email message.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **Rule Groups**.
4. Click **New**.
5. In the **Name** box, type the name of the new rule group.

   OR

   In the **Rule Groups** list, select the rule group to change.
6. Select the **Matching Type** for the rule group.
7. To add a new rule to the group, click the plus sign (**+**) button.
8. To remove a rule from the group, click the minus sign (**—**) button.
9. Configure the new rule using the input criteria, responses, and general settings.
10. To change the order of the rules in the group, select the rule, and then click the up arrow (**^**) button and down arrow (**v**) button to change the order of the rules.
11. Click **Save**.

Variable definitions

Name	Description
Matching Type	Choose the matching type. For Best match, the system checks all rules in the rule group and routes the email message according to the rule with the highest percentage match. For First match, the system checks one rule at a time, in the order of the rule group and routes the email message according to the rule that matches first.
Name	Name of the rule group. The name of the rule group must be unique and less than 64 characters.

Configuring supervisor approval for email messages on a per skillset basis

Before you begin

If you want to use keyword groups to reject email messages automatically, configure keyword groups. See Creating or changing a keyword group on page 101.

About this task

Supervisors can approve email messages before the email messages reach the customers.

Note:

The approval process applies to email contacts only and does not apply to other contact types such as Fax, Scanned Documents, and SMS.

You can configure Contact Center to send email messages to supervisors for approval on a per skillset basis or per agent basis.

You can configure up to five levels of supervisor approval before Contact Center sends the email messages to the customer. Contact Center offers the email message to a hierarchy of supervisors before the final approval is granted.

Note:

Under the following conditions, a contact can get held up in the approval process:

- an administrator deletes a skillset that is part of the supervisor approval chain and the contact is already in queue waiting for that skillset to come into service
- an administrator deletes the original agent and a supervisor rejects the email message
- an administrator deletes the supervisor who needs to approve the email message

In such situations, an agent must pull the contact using Agent Desktop.

For more information, see Supervisor approval of email messages on page 32 and Configuring supervisor approval for email messages on a per agent basis on page 51.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **Supervisor Approvals**.
4. Select a skillset under Supervisor Approvals.
5. Click **Edit**.
6. From the drop-down list, under Approval Hierarchy, select the skillset for which you need supervisors to approve email messages.

   You can configure an approval hierarchy of up to five unique approval skillsets. You cannot configure a skillset to be approved by itself.

   Note:

   Agents can belong to the skillset that approves email messages. Therefore, you must configure the approval process in a way that restricts agents from approving email messages.
7. From the drop-down list, under Rejection Flow, select the rejection hierarchy for each approval level. You can select one of the following:
   - **Reject to original skillset**
   - Reject to current approval level –1. This hierarchy is the default setting. For example, **Reject to approval level 1**.

   You must configure a rejection hierarchy for each approval level. The rejection hierarchy controls the flow of email messages through the levels of approval skillsets for a rejected email message. For example, you can decide to automatically send all rejected email messages, at any level, back to the originator.
8. In the **Approval Ratio** field, type the percentage of email messages that require supervisor approval for that skillset.

   The approval ratio must be whole numbers ranging from 0 to 100.
9. **(Optional)** From the **Auto-Rejection Keyword Group** drop-down list, select a keyword group based on which the system automatically rejects the email messages for that skillset.
10. **(Optional)** To create a new keyword group, click the plus (**+**) button next to the **Auto-Rejection Keyword Group** drop-down list. The system uses the new keyword group to automatically reject email messages for that skillset.
11. Click **Save**.

Next steps

Optionally, you can configure Contact Center to auto-reject contacts on all the skillsets configured for supervisor approvals, based on a single keyword group. For more information, see Configuring auto-rejection of email messages from all skillsets that use approval hierarchy on page 118.

Configuring auto-rejection of email messages from all skillsets that use approval hierarchy

Before you begin

- Configure your keyword groups. See Creating or changing a keyword group on page 101.
- Configure supervisor approval on one or more skillsets.

About this task

If you have set up supervisor approval of email messages, you can configure Contact Center to use a keyword group to automatically reject email messages from all the skillsets that use approval hierarchy.

For example, you can configure a keyword group named Abusive, and then add a list of abusive words to the group. For all skillsets that use approval hierarchy, Contact Center automatically rejects email messages that contain words listed in the Abusive keyword group. This configuration does not affect skillsets that do not have an approval hierarchy.

Note:

Auto-rejection of email messages applies to the first approval level prior to the first review by a supervisor. After a supervisor reviews an email message, auto-rejection of email messages is not applicable.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **Supervisor Approvals**.
4. Under Global Settings, in the **Auto-Rejection Keyword Group For All Skillsets** drop-down list, select a keyword group based on which Contact Center rejects email messages automatically.
5. Review the list of skillsets, and ensure that the skillsets to which you want the auto-rejection keyword group to apply have an approval hierarchy.
6. Click **Save**.

Configuring the email settings

About this task

Configure the following email settings for email messages entering and leaving your designated contact center mailboxes:

- how frequently you scan the email server for new messages
- the location in which attachments are stored
- automatic numbering of email messages
- which text is searched when you use keywords for rules

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

Procedure

1. Open the Multimedia Administration utility.
2. In the left pane, click **E-mail**.
3. Click **General Settings**.
4. To change the attachment file location from the file system to the database, select **Store in the database**.
5. To change the attachment file locations on the file system, under **Attachment Files**, type the new paths for the inbound and outbound URL and shared folders into the fields provided.
6. To configure a mailbox scan interval, under **Mailbox Scan Interval**, in the **Interval** box, type the time in minutes.
7. To include the customer ID or contact ID in a number for the outgoing email message numbering, under **Message Properties**, select the **Customer ID** check box, the **Contact ID** check box, or both.
8. To include the email message body in the keyword search, select the **Include email body in keyword search** check box.
9. Click **Save**.

Variable definitions

Name	Description
Interval	The interval between mailbox scans to check for new incoming email messages. You can specify minutes and seconds between each scan.

Table continues…

Name	Description
Store in the database	Select the check box to save new attachments in the MULTIMEDIA database instead of on the file system.
Inbound Url	The uniform resource locator (URL) that shows the location of the inbound email attachments. When Web Services security is on, use https as the URL prefix. If you have turned off Web Services security, use http as the URL prefix.
Inbound Share	The path of the shared folder on the Contact Center Multimedia server in which the inbound email attachments are stored.
Outbound Url	The uniform resource locator (URL) that shows the location of the outbound email attachments. When Web Services security is on, use https as the URL prefix. If you have turned off Web Services security, use http as the URL prefix.
Outbound Share	The path of the shared folder on the Contact Center Multimedia server in which the outbound email attachments are stored.
Autonumber outgoing email	Select the check box to number the email message automatically with either the customer ID, the contact ID, or both. The number appears in the subject of the message for identification.
Include email body in keyword search	Select the check box to enable a keyword search in both the subject and the body of the email message.
Search for first characters	Specify the number of characters in the content of the body of the email message that you search for keywords if you enabled the keyword search in the body of the email message.

Changing the character encoding for outgoing and incoming email

Before you begin

- Avaya recommends that only contact centers in Europe use Latin-9 encoding.

About this task

Change the character encoding of outgoing email to reply to an email message by using the same character set as the inbound email. For example, if an email arrives at the contact center with

Latin-1 encoding, the reply from the Agent Desktop or the automatic response is sent in Latin-1. The customer email client can understand the format of the message sent from the contact center.

Use Latin-9 to provide support for the Euro currency symbol, as this character is not included in the Latin-1 character set. Outgoing email messages encoded in Latin-1 that include the Euro symbol, deliver the symbol as a question mark. However, not all recipient clients understand Latin-9 and can receive what is perceived as a blank email message. Therefore, Avaya recommends that contact centers in Europe use the option for Latin-9 encoding while contact centers outside Europe avoid it.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **General Settings**.
4. In the **Encoding for agent initiated emails** list, select the type of character encoding to use.
5. To use Latin-9 encoding for replies, under **Customer Replies**, select the **Reply to Latin 1 as Latin 9** check box.
6. Click **Save**.
7. On the Contact Center Multimedia server, on the **Start** screen click **Administrative Tools** > **Services**.
8. Right-click **CCMM Email Manager.**
9. Click **Restart**.
10. Close the Services window.

Selecting the outgoing email address

Before you begin

- Configure the email mailbox from which to send outbound email messages. See Creating or changing a recipient mailbox on page 93.

About this task

You can send email messages from the email address to which the original message was sent or from a general email address in the contact center.

You can choose the response email address based on a skillset.

Note:

This procedure does not apply to automatic responses. Contact Center sends all automatic responses from the email address that the incoming email message was sent to.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **Outgoing E-mail**.
4. On the **Skillset to Mailbox Mappings** tab, select a skillset.
5. Click **Edit**.
6. In the **Address** box, select the address from which you want email messages sent from this skillset.
7. To send customer responses from an address specified for the skillset, click **Send both Agent-Initiated Contacts and Customer Responses from this e-mail address**.
8. To send customer responses from the address that the customer used, click **Respond to Customer Contacts with the Recipient address of the original e-mail, and send Agent-Initiated Contacts from this address**.
9. Click **Save**.

Barring email addresses

About this task

Configure Contact Center Multimedia to block certain email addresses. When you bar an email address, automatic replies, and agent email messages are not sent to the barred address.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **Outgoing E-mail**.
4. Click the **Barred Outgoing Addresses** tab.
5. Click **New**.

   OR

   Select an existing barred email address, and then click **Edit**.
6. In the **Address** box, type the email address to block.
7. Click **Save**.

   The address appears in the list of Barred Addresses.

Deleting a barred email address

Before you begin

- Ensure that removing a barred address does not violate local governing for do-not-call lists.

About this task

Remove a blocked email address from the barred email address list.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **Outgoing E-mail**.
4. Click the **Barred Outgoing Addresses** tab.
5. Select a barred email address from the list provided.
6. Click **Delete**.

   The system displays a Warning dialog box.
7. Click **Yes** to confirm the deletion.

Configuring Microsoft Exchange for sending outgoing email

Before you begin

- Ensure that you use Microsoft Exchange on your email server.

About this task

Configure Microsoft Exchange to send outgoing email messages from Agent Desktop.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **General Administration**.
3. Click **Server Settings**.
4. Select **Outbound Mail Server (SMTP)**.
5. Click **Edit**.
6. Under **Advanced SMTP Authentication**, select **Base 64 Encoded Authentication**.
7. Click **Save**.

8. Close the Contact Center Manager Administration window.
9. Log on to the Microsoft Exchange server.
10. Open the Exchange Management Console.
11. Click **Server Configuration** > **Hub Transport** > **Receive Connectors Tab**.
12. Right-click **Default <Servername>** and select **Properties**.
13. Click the **Authentication** tab.
14. Disable all authentication options except for the following:
    - Basic Authentication
    - Exchange Server Authentication
    - Integrated Windows Authentication
15. Click **OK**.
16. If you are using Microsoft Exchange 2007, close the Exchange Management Console and skip the remainder of this procedure.
17. Click **Server Configuration** > **Client Access**.
18. Click the **POP3 and IMAP4** tab.
19. Right-click **POP3** and select **Properties**.
20. Click the **Authentication** tab.
21. Under **Logon Method**, select **Plain text logon (Basic authentication). No TLS connection is required for the client to authenticate to the server**.
22. Click **OK**.
23. Close the Exchange Management Console.
24. On your Microsoft Exchange server, click **Start** > **Administrative Tools** > **Services**.
25. In the **Services** window, right-click the **Microsoft Exchange POP3** icon and select **Restart**.
26. Close the **Services** window.

Adding a certificate for use with TLS email connections

Before you begin

- Avaya recommends that you use a false connection on the fallback. If you assign fallback to false, a secure connection cannot be established and the operation fails. If you assign the fallback to true, during a failure the connection is insecure.

About this task

Enable Transport Layer Security (TLS) on the Email Manager. Contact Center Multimedia supports TLS to protect data traveling between the email server and the Contact Center Multimedia server.

Although SMTP is secure, when email traverses the Internet, it becomes insecure. Implementations of secure SMTP vary as does the port number. For more information, see the documentation for your email server.

The following error can occur:

```
EmailManager.log file javax.net.ssl.SSLHandshakeException: Could not
find trusted certificate.
```

This message indicates that the target mail server TLS certificate was signed with a certificate from a signing authority that is not trusted, or that you are using a test certificate and must enable SMTP Authentication on your email server.

Note:

> Contact Center supports monitored mailboxes distributed across several email servers.

Use the Java keytool to enable trust for a signing authorities certificate. By default, Java applicationTLS implementations automatically trust many of the major certificate authorities such as Verisign or Thawte.

Procedure

1. Copy the certificate file into the following directory:

   `C:\Program Files (x86)\Zulu\zulu-8-jre\lib\security`

2. On the **Desktop** screen, click **Start** > **Command Prompt**.

3. Use the following CD command to change to the Java security certificates directory:

   ```
   CD “C:\Program Files (x86)\Zulu\zulu-8-jre\lib\security”
   ```

4. Enter the following command:

   ```
   keytool -importcert -alias <mycacert> -file <mycacert>.cer -keystore cacerts
   ```

   Where <*mycacert*> is the name of your certificate file.

5. After the Java keytool prompts you for a keystore password, enter the default installation password for the JRE trust keystore, `changeit`.

   After the Java keytool prints the certificate details, the Java keytool prompts you to trust this certificate.

6. Type `yes`, and then press `Enter` to update the keystore.

   The file appears, similar to the following example:

   ```
   Owner: OU=For VeriSign authorized testing only. No
   assurances (C)VS1997, OU=www.verisign.com/repository/
   TestCPS Incorp. By Ref. Liab. LTD., O=“VeriSign, Inc”
   Issuer: OU=For VeriSign authorized testing only. No
   assurances (C)VS1997, OU=www.verisign.com/repository/
   TestCPS Incorp. By Ref. Liab. LTD., O=“VeriSign, Inc”
   Serial number: 52a9f424da674c9daf4f537852abef6e
   ```

```
Valid from: Sun Jun 07 01:00:00 BST 1998 until: Wed Jun
07 00:59:59 BST 2006
Certificate fingerprints:
MD5:
40:06:53:11:FD:B3:3E:88:0A:6F:7D:D1:4E:22:91:87
SHA1:
93:71:C9:EE:57:09:92:5D:0A:8E:FA:02:0B:E2:F5:E6:98:6C:6
0:DE
Trust this certificate? [no]: y
Certificate was added to keystore
```

7. Enter the keystore password `changeit`.
8. Restart the **Email Manager** service.
9. To change the default password for security reasons, type the following command and enter a new password:

   ```
   keytool -storepasswd -new changeit -keystore
   C:\Program Files (x86)\Zulu\zulu-8-jre\lib\security\cacerts
   ```

Enabling SMTP Authentication on your email server

About this task

Enable SMTP authentication for Microsoft Exchange Server. SMTP Authentication is a mechanism to restrict non-authenticated clients from sending email messages outside your organization. Agents who want to send external email messages must provide their logon credentials to the email server before their email is relayed. Failure to authenticate leads to an immediate message from the email server indicating that sending the email is prohibited or a later non-delivery report email. Organizations generally implement SMTP authentication to prevent SPAM messages from being relayed through the networks. For more information, see the Microsoft Knowledge Base article Q197869.

SMTP authentication varies among email servers.

Procedure

1. Log on to the **Microsoft Exchange Server** with domain administrative privileges.
2. Start the **Microsoft Exchange Administrator** program.
3. On the **Configuration** branch, double-click **Internet Mail Service**.
4. On the **Routing** tab, click **Routing Restrictions**.
5. Ensure you select the **Only Hosts and Clients who successfully authenticate** check box.
6. Restart the **Microsoft Exchange Internet Mail Service**.

Determining if SMTP Authentication is enabled

About this task

Use Telnet to verify whether the server response to the SMTP commands is enabled on an email server.

After a successful logon, you can send an email message using the MAIL, RCPT, and DATA commands.

Procedure

1. Start Telnet and connect to the IP Address or host name of the mail server. Connect using the well-known port for SMTP (Port 25). Ensure that your Telnet application is enabling a local echo.

   The following message appears:

   ```
   220 SERVERNAME.DOMAIN.COM ESMTP Server (Microsoft
   Exchange
   Internet Mail Service 5.5.2650.21) ready
   ```

2. Type `HELO`.
3. Try to send an email message to an external address using the MAIL command:

   ```
   MAIL FROM: anymailbox
   250 OK - mail from <anymailbox>
   ```

4. Specify recipients using the RCPT command.

   If SMTP Authentication is enabled, you see the following message:

   ```
   RCPT TO: anyone@externaladdress.com
   550 Relaying is prohibited
   ```

   Otherwise, you receive the following message:

   ```
   RCPT TO: anyone@externaladdress.com
   250 OK - Recipient <anyone@externaladdress.com>
   ```

5. If you find that SMTP Authentication is not enabled, you can continue to send an email message using the DATA command:

   ```
   DATA
   354 Send data. End with CRLF.CRLF
   ```

6. Conclude the email message by typing `<ENTER> . <ENTER>`

   The email message is sent.

   `250 OK`

7. If the SMTP Authentication is enabled, you must reconnect to your email server.

8. Enter the EHLO command after you reconnect:

```
EHLO
250-SERVERNAME.DOMAIN.COM Hello [LocalMachineName]
250-XEXCH50
250-HELP
250-ETRN
250-DSN
250-SIZE 0
250-AUTH LOGIN
250 AUTH=LOGIN
```

9. Type the AUTH LOGIN command:

```
AUTH LOGIN
334 VXNlcm5hbWU6
```

10. Type your user name encoded using Base64.

    A base64 encoded prompt for password appears:

```
AUTH LOGIN
334 VXNlcm5hbWU6
dGVzdA==
334 UGFzc3dvcmQ6
dGVzdA==
235 LOGIN authentication successful
```

Important:

dGVzdA== represents the word *test* when base64-encoded. The responses shown here are examples. Use the base64 representation of your user name and password that is specific to your email mailbox account.

11. Confirm the user name and password.

Enabling Extended Email Capacity

Before you begin

Ensure that you configure your multicast IP address.

About this task

The Extended Email Capacity feature increases the email backlog capacity to 100 000. Enable the Extended Email Capacity feature if you want to increase the email backlog capacity to more than 20 000.

While enabling the Extended Email Capacity feature, you can select the order in which the system queues the contacts, either by priority or by age.

Note:

After you enable the Extended Email Capacity feature, you can disable this feature only if the number of contacts in the Open or Waiting status is less than the Maximum Open Contacts Threshold. The Maximum Open Contacts Threshold is 3 000.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **General Settings**.
4. Click **Advanced**.

   The system displays the Advanced Email Configuration dialog box.
5. Select the **Enable Extended E-mail Capacity** check box.
6. In the **E-mail Queue Preference** field, select the order in which the system queues the contacts. You can queue the contacts in one of the following ways:
   - **By priority first, then age**
   - **By age first, then priority**
7. Click **Save**.

Disabling Extended Email Capacity

About this task

You can disable the Extended Email Capacity feature only if the number of contacts in the Open or Waiting status is less than the Maximum Open Contacts Threshold, which is 3 000.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **E-mail**.
3. Click **General Settings**.
4. Click **Advanced**.

   The system displays the Advanced Email Configuration dialog box.
5. Clear the **Enable Extended E-mail Capacity** check box.
6. Click **Save**.

Chapter 7: Web communications configuration

The Contact Center Multimedia server supports text-based conversations between the customer and the agent by using Web communications text chat. When customers initiate a Web communications contact, a list of skillsets determines the appropriate topic for the contact.

Before making any Web communications contacts, you must ensure the Web communications server is configured.

To personalize the Web communications contacts, you can configure welcome messages for all contacts, and specialized messages for each skillset. You can also place labels in the text-based conversation to identify the text written by the customer and agent. You can also send a copy of the transcript of the Web communication contact to the customer when the contact is complete.

Timers control the length of time for alerts to indicate when the agent or customer stops responding in the Web communication contact.

To assist agents with Web communications contacts, you can use automatic phrases to configure text for agents to automatically insert in the text-based conversation. You can also configure page push URLs, a predefined URL that is commonly sent to customers. The automatic phrases and page push URLs save the agent typing time when communicating with the customer.

The Web on hold URLs creates a list of Web pages that are sent to the customer's desktop while they wait for an agent to respond to their initial contact.

A Web on hold comfort group creates a list of messages that are sent to the customer's desktop, while the customer waits for an agent to respond, for a specified period of time to their initial contact, on a Web communications skillset.

A Web communications comfort group creates a list of messages that are sent to the customer's desktop while they wait for an agent to respond, for a specified period of time, either to their initial contact or during the communication, on a Web communications skillset.

An agent-supervisor can observe or participate in any currently active agent-customer Web communications chat session, provided the agent is under the supervision of that particular agent-supervisor. Agent-supervisors using Agent Desktop can see a display of all such applicable Web communications and Voice contacts currently active. This display also flags any Web communications contacts where certain intrinsic values exceed the defined threshold.

Prerequisites for Web communications configuration

Procedure

Ensure that you have a license for Web communications.

Assigning a development Web server name

Before you begin

- Know the name of your development Web server and the production Web server.

About this task

Configure the external Web server name to identify the external Web server for Web contacts received by the contact center.

If you configured the external Web server during installation, and the name of the server remains the same, you can skip this procedure. If you move your external website from a test computer to the production server, you must configure the external Web server name.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **General Administration**.
3. Click **Server Settings**.
4. In the **Server Settings** dialog box, select **External Web Server** and click **New**.
5. In the **Server Name** box, type the name of the external Web server where you plan to install the sample Web customer interface and develop your custom website.
6. In the **Server Port** box, type the port number for the external Web server you use to develop your custom website.
7. Click **Save**.

Variable definitions

Name	Description
Server Name	The name of the external Web server on which you plan to install the sample Web customer interface and develop your custom website.
Server Port	The port number for the external Web server for your custom website.

Configuring welcome messages and text chat labels

About this task

The welcome messages and text chat labels for a Web communications contacts have a welcome message for customers who initiate the contact, and labels for the agent and customers in the text conversation.

Configure a default welcome message that appears for all skillsets and welcome messages that apply for a single skillset. One welcome message appears for the customer. If the welcome message for the skillset appears, the global welcome message does not. The customer chooses the skillset when they initiate the contact.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Web Comms**.
3. Click **Resources**.
4. In the **Default Welcome Message** box, type the message to appear at the beginning of every contact. The maximum size for this message is 255 characters.
5. In the **Agent Label** list, select the label to appear at the beginning of the agent contact list.

   In the first box, choose from a list of automatic text such as Friendly Name, First Name, Last Name, or both First Name and Last Name. Use the second box to type custom text.
6. In the **Customer Label** box, type the text to appear at the beginning of the customer responses in the contact.

   Note:

   Customer Label is supported up to version xampp-win32-1.7.2 only.
7. To create a customer welcome message for a specific skillset, under **Custom Welcome Messages**, select a skillset.
8. Under **Welcome Message**, type the welcome message for the skillset.
9. Click **Save**.

Variable definitions

Name	Description
Agent Label	The label that appears beside the text typed for the agent. Select one of the following items: • First Name: The first name of the agent appears at the beginning of the agent responses in the contact (for example, Robert). • First Name, Last Name: The first and last name of the agent appear at the beginning of the agent responses in the contact (for example, Robert Smith). • Last Name, First Name: The last name of the agent, followed by the first name of the agent appears at the beginning of the agent responses in the contact (for example, Smith, Robert). • Friendly Name: The friendly name or nickname of the agent appears at the beginning of the agent responses in the contact (for example, Rob). The first name of the agent is the default value for Friendly Name. For example, if you have entered the first name of the agent as Fred in Contact Center Manager Administration, the default Friendly Name is set as Fred. You can modify the Friendly name using Contact Center Multimedia. While upgrading to Contact Center 7.0.1, the default value is applied to any existing agents. The default values is also applied to any new agents who are added to the system after the upgrade. You can also type custom text to appear at the beginning of the agent responses. The maximum size of the label is 255 characters.
Customer Label	The text to appear at the beginning of the customer responses in the contact. The maximum size of the Customer Label is 255 characters.

Configuring Web communications agent timers

About this task

Configure the contact timers for Web communications conversations in your Contact Center.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Web Comms**.
3. Click **Config**.
4. In the **Keep Alive Time** box, type the interval in minutes and seconds between heartbeat pulses that verify whether both ends of the Web communications contact are open.
5. In the **Message Refresh** box, type the refresh time for the Agent Desktop.
6. In the **Desirable Response (Customer awaiting Agent)** box, type the threshold for the agent to respond.
7. In the **Desirable Response (Agent awaiting Customer)** box, type the threshold for the customer to respond.
8. In the **Consult Request Timeout** box, type the length of time in seconds that a consultation is requested before it times out.
9. Select the **Force Idle Customer Check** check box so that the Agent Desktop alerts agents when a customer has not replied in a Web communications session, for a predefined period. The Agent Desktop also brings that web chat contact to the front.
10. In the **Force Idle Customer Check Timeout** box, type the time after which the Agent Desktop considers a customer in a web chat session idle, if a customer has not responded in a Web communications session.
11. Click **Save**.

Variable definitions

Name	Description
Message Refresh	The refresh time for the Agent Desktop.
Keep Alive Time	The interval in minutes and seconds between heartbeat pulses that verify whether both ends of the Web communication contact are open.
Desirable Response (Agent awaiting Customer)	The time after which the conversation indicator on the Agent Desktop changes color to indicate that the desirable time for an agent response is exceeded.
Desirable Response (Customer awaiting Agent)	The time after which the conversation indicator on the Agent Desktop changes color to indicate that the desirable time for a customer response is exceeded.
Consult Request Timeout	The time after which the consult request expires.

Table continues…

Name	Description
Force Idle Customer Check	Select this check box to enable Agent Desktop to alert agents when a customer has not replied in a Web communications session, for a predefined period. The Agent Desktop also brings that web chat contact to the front.
Force Idle Customer Check Timer	The time after which the Agent Desktop considers a customer in a web chat session idle, if a customer has not responded in a Web communications session.

Saving Web communications chat session details

About this task

Configure the details you want to save for each Web communications chat session in your contact center.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Web Comms**.
3. Click **Config**.
4. Select the **Save Timestamp on Chat Message** check box to enable the saving of a timestamp with each chat message sent in a chat session.
5. Select the **Save Chat History** check box to enable the saving of chat session history. When enabled, the entire history of a chat session is saved.
6. Click **Save**.

Configuring the Web communications chat session limits

About this task

Configure limits for Web communications chat sessions. These limits restrict the number of concurrent sessions and scheduled callbacks that a customer can have. Setting these limits reduces the possibility of Denial of Service attacks through the Web communications interface.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Web Comms**.
3. Click **Config**.
4. In the **Concurrent Chats Limit per Customer** box, type the maximum number of concurrent chat sessions each customer can create. Type a value between 1 and 10. The default value is 3, which is the value that Avaya recommends.
5. In the **Requested Call-backs Limit per Customer** box, type the maximum number of scheduled Web communication callbacks each customer can have. Type a value between 1 and 10. The default value is 3, which is the value that Avaya recommends.
6. Click **Save**.

Configuring customer notification log

Before you begin

- Configure an outgoing email address to use to send the log file to the customer.

About this task

Configure the customer notification log information to prepare to send an email to the customer of the written conversation.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Web Comms**.
3. Click **Config**.
4. Under **Chat Conversation**, select **E-mail Chat Log to Customer**.
5. Click **Save**.

Enabling Web Communications transfer to a skillset

About this task

Configure the Web Communications (WC) transfer to a skillset feature to allow agents to transfer a WC contact to a skillset.

Note:

If you want to transfer a Web Communications contact, your contact center must be licensed to use the Multiplicity feature.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Web Comms**.
3. Click **Config**.
4. Select the **Enable Transfer To Skillset** checkbox.
5. Click **Save**.

Creating automatic phrases

About this task

Configure automatic phrases by skillset. You can create a list of commonly used phrases for agents to insert into their Web communications contacts instead of typing individual responses.

You can select a single automatic phrase for all skillsets. If you choose all skillsets, the automatic phrase applies to all skillsets for Web communications and instant message contacts.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Web Comms**.
3. Click **Auto Phrases**.
4. Under **Edit Auto Phrases**, select the skillset to add new phrases.

   OR

   Click **All Skillsets** to apply an automatic phrase for all skillsets.
5. Click **Edit**.
6. In the **Previously Configured Auto Phrase** box, review the phrase to decide whether you want to change it or to use it for other skillsets.

   Important:

   If you select All Skillsets, the Previously Configured Auto Phrase box is unavailable.
7. In the **Name** box, type a name to represent this automatic phrase.
8. In the **Phrase Text** box, type the text that is commonly used for the contacts based on the selected skillset.

9. Click **Add**.
10. Click **Save**.

Deleting an automatic phrase

About this task

Delete the automatic phrase to remove it from the list of automatic phrases available to the agents in the Agent Desktop.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Web Comms**.
3. Click **Auto Phrases**.
4. Under **Edit Auto Phrases**, select the skillset from which you want to remove the phrases.

   OR

   Select **All Skillsets** to remove phrases for use with all skillsets.
5. Click **Edit**.
6. In the **Phrases in Group** box, select the automatic phrase to delete.
7. Click **Remove**.

   The system displays a Warning dialog box.
8. Click **Yes** to confirm the decision.
9. Click **Save**.

Creating a page push URL

About this task

In the Agent Desktop, the agent can choose from a list of Web pages for the skillset assigned to the Web communication contact.

Create the Web pages that appear the Agent Desktop. Ensure that the name of the page push URL is descriptive to assist agents in using the Agent Desktop.

You can configure maximum 50 URLs.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Web Comms**.
3. Click **Page Push Urls**.
4. Under **Edit Page Push URLs**, select the skillset to add new URLs.

   OR

   Select **All Skillsets**.
5. Click **Edit**.
6. In the **URL** box, type the URL for the website to add to the list that appears in the Agent Desktop.
7. In the **Description** box, type a description for the page push URL that describes the URL that the agent can push.
8. Click **Add**.
9. Click **Save**.

Deleting a page push URL

About this task

Delete a page push URL to remove it from the list of pages the agent can push to customers during a Web communications contact.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Web Comms**.
3. Click **Page Push Urls**.
4. Under **Edit Page Push URLs**, select the skillset to change the URLs.

   OR

   Select **All Skillsets**.
5. Click **Edit**.
6. In the **URLs in Group** box, select the URL to delete.
7. Click **Remove**.

   The system displays a Warning dialog box.

8. Click **Yes** to confirm the decision.
9. Click **Save**.

Creating Web On Hold URLs groups

About this task

Web On Hold URL groups is a sequence of URLs presented automatically to a customer's Web browser while the customer waits for an agent in the Web communications. You can define the time that each URL appears on the customer's Web browser.

Web On Hold URLs can include multimedia formats, such as video clips (Quick Time) or audio files (MPEG3). However, the customer browser must be able to play these formats. Customers are responsible for the plug-ins needed to run multimedia files.

You can add up to 50 URLs to a Web-on-hold group, but Avaya recommends that you use no more than 25 URLs in each Web-on-hold group.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Web Comms**.
3. Click **Web On Hold**.
4. Click the **On Hold URLs** tab.
5. Click **New**
6. In the **Tag** box, type a name for the new Web On Hold group.
7. In the **Description** box, type a description for the Web On Hold URL.
8. In the **Hold Time** box, type the number of seconds to display each URL in the customer's browser.
9. In the **URL** box, type the URL to display on the customer's Web browser.
10. Click **Add**.
11. Repeat step 6 on page 140 to step 11 on page 140 to add all URLs to the current Web on hold group.
12. Click **Save**.

Deleting a URL from a Web On Hold URL group

About this task

Delete a URL from a Web on hold URL group if the URL is not available.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Web Comms**.
3. Click **Web On Hold**.
4. Click the **On Hold Urls** tab.
5. Click **Edit**.
6. Under **Edit Web On Hold URL Group** dialog box, in the **URLs in Group** box, select the URL to delete.
7. Click **Remove**.

   The system displays a Warning dialog box.
8. Click **Yes** to confirm the decision.
9. Click **Save**.

Deleting a Web On Hold URLs group

About this task

Delete a Web-on-hold URLs group to avoid displaying the Web pages to the customer during Web communications contacts.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Web Comms**.
3. Click **Web On Hold**.
4. Click the **On Hold Urls** tab.
5. Select the **Group** to delete.
6. Click **Delete**.

   The system displays a Warning dialog box.
7. Click **Yes** to confirm the deletion.

Creating Web On Hold comfort groups

Before you begin

- Add the Web on hold comfort group to the Web communications skillset. For more information adding comfort groups to a Web communications skillset, see Configuring Web On Hold comfort groups for a Web communications skillset on page 147.

About this task

A Web on hold comfort group consists of a list of sequential messages that are sent to the customer's desktop, while the customer waits for an agent to respond, for a specified period of time to their initial contact, on a Web communications skillset. You can also add variables to the Web on hold message text for a customer.

You can set the time for which messages display on the customer's desktop.

✱ **Note:**

Avaya recommends that you use no more than five messages in each Web on hold comfort group and one Web on hold comfort group for each Web communications skillset.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Web Comms**.
3. Click **Web On Hold**.
4. Click the **On Hold Comforts Group** tab.
5. Under **Comfort Group**, click **New**.
6. In the **Name** box, type a name for a new Web on hold comfort group.
7. In the **Delay** box, type the number of seconds to display each comfort message in the customer's desktop.
8. In the **Message** box, type the comfort message.
9. Optional: To insert a placeholder for accessing variables for the message, right-click in the **Message** box and select the placeholder from the menu.
10. Click **Add**.
11. Repeat step 9 and step 10 to add messages to the current Web on hold comfort group.
12. Under **Group Messages**, use the arrow keys to configure the sequence of messages.
13. Click **Save**.

Changing the sequence of messages in a Web On Hold comfort group

Before you begin

- Set up a Web on hold comfort group that is associated with Web communications skillset.

About this task

Follow this procedure to change the sequence in which comfort messages in a Web on hold comfort group appear to customers.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Web Comms**.
3. Click **Web On Hold**.
4. Click the **On Hold Comfort Groups** tab.
5. Under **Comfort Group**, select the comfort group to change.
6. Click **Edit**.
7. Under **Group Messages**, use the arrow keys to configure the sequence of messages.
8. Click **Save**.

Deleting a message from a Web On Hold comfort group

Before you begin

- Set up a Web on hold comfort group that is associated with Web communications skillset.

About this task

Follow this procedure to delete a comfort message from a Web on hold comfort group, if you do not want to use a specific message in the comfort group.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Web Comms**.
3. Click **Web On Hold**.
4. Click the **On Hold Comfort Groups** tab.
5. Under **Comfort Group**, select the **Group** that contains the **Message** to delete.

6. Click **Edit**.
7. Under **Group Messages**, select the **Message** to delete.
8. Under **Edit Group**, click **Remove**.

   The system displays a Warning dialog box.
9. Click **Yes** to confirm the decision.
10. Click **Save**.

Deleting a Web On Hold comfort group

Before you begin

- Set up a Web on hold comfort group that is associated with Web communications skillset.
- Ensure that the Web on hold comfort group is unlinked from any other skillset before it is removed.

About this task

Follow this procedure to delete a Web on hold comfort group if you do not want to use a specific comfort group.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Web Comms**.
3. Click **Web On Hold**.
4. Click the **On Hold Comfort Groups** tab.
5. Under **Comfort Group**, select the **Group** to delete.
6. Click **Delete**.

   The system displays a Warning dialog box.
7. Click **Yes** to confirm the deletion.

Creating Web communications comfort groups

Before you begin

- Add the Web communications comfort group to the Web communications skillset. For more information adding Web communications comfort groups to a Web communications skillset, see Configuring Web communications comfort groups for a Web communications skillset on page 149.

About this task

A Web communications comfort group consists of a list of sequential messages that are sent to the customer's desktop while they wait for an agent to respond, for a specified period of time, either to their initial contact or during the communication, on a Web communications skillset. You can also add variables to the Web communications message text for a customer.

You can set the time for which messages display on the customer’s desktop.

Note:

Avaya recommends that you use no more than five messages in each Web communications comfort group and one Web communications comfort group for each Web communications skillset.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Web Comms**.
3. Click **Comfort Messages**.
4. Under **Comfort Group**, click **New**.
5. In the **Name** box, type a name for a comfort group.
6. In the **Delay** box, type the number of seconds to display each comfort message in the customer's desktop.
7. In the **Message** box, type the comfort message.
8. Optional: To insert a placeholder for accessing variables for the message, right-click in the **Message** box and select the placeholder from the menu.
9. Click **Add**.
10. Repeat step 8 on page 145 and step 9 on page 145 to add messages to the current Web communications comfort group.
11. Under **Group Messages**, use the arrow keys to configure the sequence of messages.
12. Click **Save**.

Changing the sequence of messages in a Web communications comfort group

Before you begin

- Set up a Web communications comfort group that is associated with Web communications skillset.

About this task

Follow this procedure to change the sequence in which comfort messages in a Web communications comfort group appear to customers.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Web Comms**.
3. Click **Comfort Messages**.
4. Under **Comfort Group**, select the comfort group to change.
5. Click **Edit**.
6. Under **Group Messages**, use the arrow keys to configure the sequence of messages.
7. Click **Save**.

Deleting a message from a Web communications comfort group

Before you begin

- Set up a Web communications comfort group that is associated with Web communications skillset.

About this task

Follow this procedure to delete a comfort message from a Web communications comfort group, if you do not want to use that message in a Web communications comfort group.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Web Comms**.
3. Click **Comfort Messages**.
4. Under **Comfort Group**, select the **Group** that contains the **Message** to delete.
5. Click **Edit**.
6. Under **Group Messages**, select the **Message** to delete.
7. Under **Edit Group**, click **Remove**.

   The system displays a Warning dialog box.
8. Click **Yes** to confirm the decision.

9. Click **Save**.

Deleting a Web communications comfort group

Before you begin

- Set up a Web communications comfort group that is associated with Web communications skillset.
- Ensure that the Web communications comfort group is unlinked from any other skillset before it is removed.

About this task

Follow this procedure to delete a Web communications comfort group if you do not want to use that comfort group.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Web Comms**.
3. Click **Comfort Messages**.
4. Under **Comfort Group**, select the **Group** to delete.
5. Click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion.

Configuring Web On Hold comfort groups for a Web communications skillset

Before you begin

- Set up the Web On Hold comfort group.

About this task

You must configure a Web On Hold comfort group on a Web communications skillset to automatically send messages to the customer's desktop. These messages are sent to the customer while they wait for an agent to respond, for a specified period of time to their initial contact, on a Web communication skillset.

For more information on Web On Hold comfort groups, see Creating Web On Hold comfort groups on page 142.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **General Administration**.
3. Click **Skillset Settings**.
4. In the **Skillset Settings** dialog box, select the skillset for which to assign a Web On Hold comfort group. The skillset must have the prefix WC for Web communications.
5. Under the **Edit Skillset** dialog box, in the **On Hold Group** list, select the group to assign to the Web communications skillset.
6. Click **Save**.

Removing a Web On Hold comfort group for a Web communications skillset

Before you begin

- The Web On Hold comfort group must be associated with the Web communications skillset.

About this task

You can remove a Web On Hold comfort group from a Web communications skillset, if the group has been deleted or if you do not want to use a specific Web On Hold comfort group.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **General Administration**.
3. Click **Skillset Settings**.
4. Under the **Edit Skillset** dialog box, in the **On Hold Group** list, select the group that you want to remove and click **Unlink Group**.
5. When the warning message asking you to confirm unlinking the Web On Hold comfort group appears, click **Yes**.

Configuring Web communications comfort groups for a Web communications skillset

Before you begin

- Set up the Web On Hold comfort group.

About this task

You must configure a Web communications comfort group on a Web communications skillset to automatically send messages to the customer's desktop. These messages are sent to the customer while they wait for an agent to respond, for a specified period of time, either to their initial contact, or during the communication, on a Web Communications skillset.

For more information on Web communications comfort groups, see Creating Web communications comfort groups on page 144.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **General Administration**.
3. Click **Skillset Settings**.
4. In the **Skillset Settings** dialog box, select the skillset for which to assign a Web communications comfort group. The skillset must have the prefix WC for Web communications.
5. Under the **Edit Skillset** dialog box, in the **Comfort Group** list, select the group to assign to the Web communications skillset.
6. Click **Save**.

Removing a Web communications comfort group from a Web communications skillset

Before you begin

- The Web communications comfort group must be associated with the Web communications skillset.

About this task

You can remove a Web communications comfort group from a Web communications skillset, if the group has been deleted or if you do not want to use a specific Web communications comfort group.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **General Administration**.
3. Click **Skillset Settings**.
4. Under the **Edit Skillset** dialog box, in the **Comfort Group** list, select the group that you want to remove and click **Unlink Group**.
5. When the warning message asking you to confirm unlinking the Web communications comfort group appears, click **Yes**.

Configuring intrinsics for agent-supervisor observe and barge-in

About this task

An agent-supervisor can observe or barge-into any active incoming agent-customer Web Communications chat session of all agents under the supervision of the agent-supervisor. Agent Desktop displays active incoming Web Communications contacts and Voice contacts to agent-supervisors.

Agent Desktop flags any Web Communications contacts where certain intrinsic values exceed the defined threshold.

Using the Multimedia Administration utility, you can set the threshold values for intrinsics. Some of the intrinsics are:

- Conversation Length (seconds)
- Seconds since last message out
- Seconds since last message in
- Number of Agent Messages
- Unanswered Messages

Using the Multimedia Administration utility, you can assign a priority from 1 to 5, 1 being the highest priority, to each of the intrinsics. The system uses the threshold and priority values assigned to sequence the Web Communications contacts in a list. Contacts which require urgent attention appear at the top of this list.

Important:

Each intrinsic type has a unique priority level. For example, Conversation Length and Customer Idle Time intrinsics cannot have the same priority level.

If the value set for the intrinsics exceeds the defined threshold, the system flags the contact as requiring attention. If the system flags more than one contact, then these contacts are sequenced based on a weightage. The system calculates this weightage using the priority of the intrinsic with exceeded thresholds. A higher weightage is given to intrinsics that have a higher priority.

For example, if contact A has exceeded the threshold for intrinsics of priority 1 and 2, and contact B has exceeded the threshold for intrinsics of priority 1 and 3, then contact A appears above contact B in the list.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Web Comms**.
3. Click **Intrinsic Settings**.
4. Under **Intrinsic Data**, type a number of seconds or type a number in the **Threshold** box.
5. Under **Intrinsic Data**, select a number, from 1 to 5, in the **Priority** drop-down box.

   Each intrinsic type has to have a unique priority level.
6. Click **Save**.

Chapter 8: Outbound configuration

To create, monitor, and add data to an outbound campaign, use the Outbound Campaign Management Tool.

You must use the Multimedia Administration tool to configure how contacts are routed to a contact type using a skillset. Complete all other configuration for previewed outbound campaigns in the Outbound Configuration Management Tool. For more information, see *Administering Avaya Contact Center Select*.

Prerequisites for Outbound configuration

Procedure

- Ensure that you are licensed for Outbound contacts in your contact center.
- Ensure that the Moving Window Skillset Multicast Rate is five seconds or greater. Configure the Moving Window Skillset Multicast Rate using the CCMS Multicast Address and Port Configuration tool.
- Ensure that the route points (CDN) are configured in Contact Center Manager Administration.

Configuring a route point for an Outbound skillset

About this task

Configure a route point for an outbound skillset to route outbound contacts to a particular direction. Skillsets are used to assign the contacts to agents.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **General Administration**.
3. Click **Skillset Settings**.
4. In the **Skillset Settings** dialog box, select the skillset for which to assign a route point.

   The skillset must have the prefix OB for outbound.

5. Under the **Edit Skillset** dialog box, in the **Route Point** list, select the route point to assign to the outbound skillset.
6. Click **Save**.

Variable definitions

Name	Description
Route point	A location in the open queue that enables incoming contacts to queue and run through a script on the Contact Center Manager Server.

Chapter 9: Voice mail configuration

This chapter contains the configuration steps for the voice mail recipient mailbox and routing voice mail contacts.

In the contact center, the recipient mailboxes are polled for incoming voice mail messages. A voice mail server forwards voice mail messages to an email address. The Contact Center Multimedia Email Manager retrieves the voice mail (.wav) attachment and queues it to the appropriate skillset with an assigned priority. The caller ID is extracted to facilitate callbacks to the customer.

Reports appear in the Contact Center Multimedia Administration utility to show the current status of the voice mail traffic. The following reports appear when you select Voice Mail and View Reports in the left column of the Contact Center Multimedia application. You can choose the report date and the skillsets represented in all displayed real-time reports.

- The Voice Mail (New Vs. Closed) report shows the number of contacts in a new and closed state against the time for the selected date and skillsets.
- The Voice Mail Progress report shows the number of contacts in a new or closed state on a defined date to determine the traffic levels for that date.
- The Voice Mail Closed Contacts Queue Time report shows the average time a voice mail contact spends in queue while the contact center is open.

Prerequisites for voice mail configuration

Procedure

Ensure that you are licensed for email contacts.

Configuring a route point for a voice mail skillset

About this task

Configure a route point for a voice mail skillset to route voice mail contacts to a particular agent. Skillsets are used to assign contacts to agents.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **General Administration**.
3. Click **Skillset Settings**.
4. In the **Skillset Settings** dialog box, select the skillset to assign a route point.

   The skillset must have the prefix VM.
5. Under the **Edit Skillset** dialog box, in the **Route Point** list, select the route point to assign to the voice mail skillset.
6. Click **Save**.

Variable definitions

Name	Description
Route point	A location in the open queue that enables incoming contacts to queue and run through a script on the Contact Center Manager Server.

Adding a voice mail server

About this task

Add the voice mail server for your Contact Center Multimedia server as per your requirement.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Voice Mail**.
3. Click **Mailbox Configuration**.
4. Click **Voice Mail Server** (image).
5. In the Voice Mail Server Configuration window, click **Add**.
6. In the **Voice Mail Server Hostname** box, type the name of the new server.
7. In the **Type** box, select the type of server.
8. Click **Save**.

Updating a voice mail server

About this task

Update the voice mail server for your Contact Center Multimedia server as per your requirement.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Voice Mail**.
3. Click **Mailbox Configuration**.
4. Click **Voice Mail Server** (image).
5. In the Voice Mail Server Configuration window, click **Edit**.
6. Change the properties of your Voice Mail server, as required.
7. Click **Save**.

Deleting a voice mail server

About this task

Delete the voice mail server for your Contact Center Multimedia server if it is no longer required.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Voice Mail**.
3. Click **Mailbox Configuration**.
4. Click **Voice Mail Server** (image).
5. In the Voice Mail Server Configuration window, select the server that you want to and click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the server deletion.
7. Click **Close**.

Adding a voice mail mailbox

Before you begin

- Configure a skillset for a voice mail contact.

Important:

You must configure the voice mail server, the email server, and a recipient mailbox in Contact Center to receive voice mail messages in the contact center.

About this task

Add a voice mail mailbox to the multimedia configuration for receiving voice mail messages as .wav attachments.

Also, choose the skillset for the mailbox so that the voice mail message is routed to the agent who has the best skills to handle the specific contact.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Voice Mail**.
3. Click **Mailbox Configuration**.
4. Click **Add**.
5. On the **Mailbox** tab, in the **Inbound Server** field, select the host name of your POP3 or IMAP server along with the respective security protocol.
6. In the **Outbound Server** field, select the host name of your SMTP server.
7. In the **Mailbox** field, type the mailbox name.
8. In the **Domain** field, type the mailbox domain.
9. In the **Password** and **Confirm** boxes, type and retype the password to access the mailbox.
10. In the **Skillset** field, choose a configured skillset for routing the voice mail contacts.
11. In the **Contact Priority** field, choose a priority for voice mail contacts received in this mailbox.
12. Click the **Sender Address** tab.
13. Select **Use full sender address** or **Parse sender address for CLID**.
14. If you select **Parse sender address for CLID**, then in the **Leading Characters to Remove** field, type the characters that you must not dial when making the outgoing callback.
15. Click **Save**.

Variable definitions

Name	Description
Inbound Server	The host name of the email server that handles email messages that enter the contact center.
Outbound Server	The host name of the email server that delivers email messages that leave the contact center.
Mailbox	Name of the mailbox on the email server that is polled for new incoming email messages.
Domain	The domain name for the email server.
Password	The password used to access the mailbox on the email server. Type the password in the Confirm Password box to ensure accuracy. Contact Center Multimedia supports a maximum mailbox password length of 100 characters.
Skillset	A label applied to a set of skills, capabilities, or knowledge that an agent requires to respond to a request. The skillsets are retrieved from the Contact Center Manager Server database. You must select a route point for a skillset used to route voice mail contacts.
Priority	The priority given to a request for a skillset agent. The lower the priority number, the greater the priority. The values of the priorities range from 1 to 6. For example, a call with priority 1 is handled before a call with priority 6.
Sender address	Select Use full sender address or Parse the address for the Calling Line identification (CLID) to save for future contacts. The address in the format you select is stored with the contact for future communication with the customer.
Leading characters to remove	If you select a Calling Line Identification (CLID) to add the customer’s phone number into the contact information, type any leading characters or trunk numbers to remove from the current number.

Updating a voice mail mailbox

Before you begin

- Add a voice mail mailbox.

About this task

Update the properties of the voice mail mailbox, as per your requirements.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Voice Mail**.
3. Click **Mailbox Configuration**.
4. Select the mailbox to be edited.
5. Click **Edit**.
6. Update the mailbox settings as required.
7. Click **Save**.

Deleting a voice mail mailbox

Before you begin

- Add a voice mail mailbox.

About this task

Delete a voice mail mailbox, if it is no longer required.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Voice Mail**.
3. Click **Mailbox Configuration**.
4. Select the mailbox to be deleted.
5. Click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion.

Updating the voice mail system default rule

Before you begin

- Ensure that you know the default settings for the system delivery failure rule:
  - use the voice mail default skillset, VM_Default_Skillset
  - use no automatic response
  - assign priority 3
- Use caution when you change the properties of the system default rule:
  - If you change the properties of the rule, you affect the behavior of the system default rule, which affects all recipient mailboxes.
  - If you delete the skillset associated with the default rule, VM_Default_Skillset is used.
- Configure the route points for the skillset you assign to the system default rule. For more information, see Configuring a route point for a voice mail skillset on page 154.

About this task

Update the voice mail system default rule to ensure that email messages received with voice mail attachments are routed to an agent if no other rule associated to the recipient mailbox routes the email message.

The system default rule is used in every rule group configured in Contact Center Multimedia.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Voice Mail**.
3. Click **Default Rules**.
4. Under **System Default Rule**, from the **Skillset** list, select a skillset name to assign to the contact.
5. Under **System Default Rule**, from the **Priority** list, select the priority to assign to the contact.
6. Click **Save**.

Variable definitions

Name	Description
Skillset	A label applied to a set of skills, capabilities, or knowledge that an agent requires to respond to a request. The skillsets are retrieved from the Contact

Table continues…

Name	Description
	Center Manager Server database. You must select a route point for a skillset used to route contacts.
Priority	The priority given to a request for a skillset agent. The lower the priority number, the greater the priority. The values of the priorities range from 1 to 10. For example, a call with priority 1 is handled before a call with priority 10.

Updating the voice mail system delivery failure rule

Before you begin

- Ensure that you are licensed to handle email messages.
- Ensure that you know the default settings for the system delivery failure rule:
  - use the voice mail default skillset, VM_Default _Skillset
  - use keyword group delivery failure keywords
  - assign priority 10 (lowest)
- Use caution when you change the properties of the system default rule:
  - If you change the properties of the rule, you affect the behavior of the system default rule, which affects all recipient mailboxes.
  - If you delete the skillset associated with the default rule, VM_Default_Skillset is used.
- Configure the route point for the skillset you plan to assign to the system delivery failure rule. See Configuring a route point for a voice mail skillset on page 154.

About this task

Update the voice mail system delivery failure rule to ensure that any email message that contains particular phrases such as undeliverable, returned mail, unknown recipient, delivery failure, or delivery report is deleted and not assigned to an agent.

When you create a recipient mailbox, the system delivery failure rule is copied as the first regular rule into list of rules for the recipient mailbox.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Voice Mail**.
3. Under **System Delivery Failure Rule**, from the **Skillset** list, select a skillset name to assign to the contact.
4. To change the keyword group, select the keyword group which contains the delivery failure keywords from the **Keyword Group** list under the **System Delivery Failure Rule**.

5. To change the priority, under **Priority**, select the priority to assign to the contact from the **Priority** list under the **System Delivery Failure Rule**.
6. To close contacts matching the delivery failure keywords, select the **Will close contact** check box.
7. Click **Save**.

Variable definitions

Name	Description
Skillset	A label applied to a set of skills, capabilities, or knowledge that an agent requires to respond to a request. The skillsets are retrieved from the Contact Center Manager Server database. You must select a route point for a skillset used to route outbound contacts.
Keyword group	A list of words that you can search in an email message. Keyword groups associate keywords and expressions considered important by the contact center to be handled in a particular way.
Priority	The priority given to a request for a skillset agent. The lower the priority number, the greater the priority. The values of the priorities range from 1 to 10. For example, a call with priority 1 is handled before a call with priority 10.
Will close contact	Select the check box to close the email contact after the system delivery failure rule determines that the contact is not appropriate for the contact center. Clear the check box to leave the email contact open for review.

Chapter 10: Scanned document configuration

This chapter contains the configuration steps for the recipient mailbox that receives scanned documents.

In the contact center, the recipient mailboxes are polled for incoming scanned documents. A server forwards scanned documents to an email address. The Contact Center Multimedia Email Manager retrieves the scanned document as an attachment (.tiff) and queues it to the appropriate skillset with an assigned priority.

Reports appear in the Contact Center Multimedia Administration utility to show the current status of the contact type traffic. The following reports appear when you select Scanned Documents and View Reports in the left column of the Contact Center Multimedia application. You can choose the report date and the skillsets represented in all displayed real time reports.

- The Scanned Document (New Vs. Closed) report shows the number of contacts in a new and closed state against the time for the selected date and skillsets.
- The Scanned Document Progress report shows the number of contacts in a new or closed state on a defined date to determine the traffic levels for that date.
- The Scanned Document Closed Contacts Queue Time report shows the average time a contact spends in queue while the contact center is open.

Prerequisites for scanned document configuration

Procedure

Ensure that you are licensed for email contacts.

Configuring a route point for a scanned document skillset

About this task

Configure a route point for a scanned document skillset to route the contact to a particular agent. Skillsets are used to assign the contacts to agents.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **General Administration**.
3. Click **Skillset Settings**.
4. In the **Skillset Settings** dialog box, select the skillset to assign a route point.

   The skillset must have the prefix SD.
5. Under the **Edit Skillset** dialog box, in the **Route Point** list, select the route point to assign to the scanned document skillset.
6. Click **Save**.

Variable definitions

Name	Description
Route point	A location in the open queue that enables incoming contacts to queue and run through a script on the Contact Center Manager Server.

Adding a document imaging server

About this task

Add the document imaging server for your Contact Center Multimedia server as per your requirement.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Scanned Documents**.
3. Click **Mailbox Configuration**.
4. Click **Document Imaging Server** (image).
5. In the Document Imaging Server Configuration window, click **Add**.
6. In the **Document Server Hostname** box, type the name of the new server.
7. In the **Type** box, select the type of server.
8. Click **Save**.

Updating a document imaging server

About this task

Update the document imaging server for your Contact Center Multimedia server as per your requirement.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Scanned Documents**.
3. Click **Mailbox Configuration**.
4. Click **Document Imaging Server** (image).
5. In the Document Server Configuration window, select the server you are updating and click **Edit**.
6. Change the properties of your document imaging server.
7. Click **Save**.

Deleting a document imaging server

About this task

Delete the document imaging server for your Contact Center Multimedia server if it is no longer required.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Scanned Documents**.
3. Click **Mailbox Configuration**.
4. Click **Document Imaging Server**.
5. In the Document Server Configuration window, select the server that you want to and click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion.
7. Click **Close**.

Adding a scanned document mailbox

Before you begin

- Configure a skillset for a scanned document.

About this task

Add a scanned document mailbox to the multimedia configuration for receiving scanned documents as .tiff attachments.

Also, choose the skillset for the mailbox so that the scanned document is routed to the agent who has the optimal skillset to handle the specific contact.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Scanned Document**.
3. Click **Mailbox Configuration**.
4. Click **Add**.
5. On the **Mailbox** tab, in the **Inbound Server** field, select the host name of your POP3 or IMAP server along with the respective security protocol.
6. In the **Outbound Server** field, select the host name of your SMTP server.
7. In the **Mailbox** field, type the mailbox name.
8. In the **Domain** field, type the mailbox domain.
9. In the **Password** and **Confirm** fields, type and retype the password to access the mailbox.
10. In the **Skillset** field, choose a configured skillset for routing the contact.
11. In the **Contact Priority** field, choose a priority for contacts received in this mailbox.
12. Click **Save**.

Variable definitions

Name	Description
Inbound Server	The host name of the email server that handles email messages entering the contact center.
Outbound Server	The host name of the email server that delivers email messages that leave the contact center.
Mailbox	Name of the mailbox on the email server that is polled for new incoming email messages.
Domain	The domain name for the email server.

Table continues…

Name	Description
Password	The password used to access the mailbox on the email server. Type the password in the Confirm box to ensure accuracy. Contact Center Multimedia supports a maximum mailbox password length of 100 characters.
Skillset	A label applied to a set of skills, capabilities, or knowledge that an agent requires to respond to a request. The skillsets are retrieved from the Contact Center Manager Server database. You must select a route point for a skillset used to route contacts.
Priority	The priority given to a request for a skillset agent. The lower the priority number, the greater the priority. The values of the priorities range from 1 to 6. For example, a call with priority 1 is handled before a call with priority 6.

Updating a scanned document mailbox

Before you begin

- Add a scanned document mailbox.

About this task

Update the properties of the scanned document mailbox, as per your requirements.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Scanned Document**.
3. Click **Mailbox Configuration**.
4. Select the mailbox to be edited.
5. Click **Edit**.
6. Update the mailbox settings as required.
7. Click **Save**.

Deleting a scanned document mailbox

Before you begin

- Add a scanned document mailbox.

  Important:

  A scanned document mailbox cannot be deleted if it is currently assigned to a skillset

About this task

Delete a scanned document mailbox, if it is no longer required.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Scanned Document**.
3. Click **Mailbox Configuration**.
4. Select the mailbox to be deleted.
5. Click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion.

Configuring a scanned document reply mailbox

About this task

Configure the reply information to the scanned document received by your contact center.

Configure the outgoing mailbox properties with a signature related to the skillset for replying to scanned document.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Scanned Document**.
3. Click **Reply Configuration**.
4. Under **Skillsets**, select a scanned document skillset for the mailbox configuration.
5. Under **Mailbox**, select a configured mailbox.

   OR

   Click **New** to create a new mailbox.

OR

Click **Edit** to edit an existing mailbox.

6. In the **SMTP Server** box, select the SMTP server to use for outgoing email messages.
7. In the **Mailbox** box, specify the new mailbox or change the name of the existing mailbox.
8. In the **Domain** box, type the email server domain.
9. In the **Password** and **Confirm** boxes, type and retype the email server password.
10. To use a different user name for the SMTP authentication, select the **Use Alternative username for SMTP Authentication** check box.
11. In the **Username** box, type the alternative user name.
12. Click **Save**.

Variable definitions

Name	Description
SMTP Server	The name of the email server that handles email messages leaving the contact center.
Mailbox	Name of the mailbox on the email server polled for email messages.
Domain	The domain name for the email server.
Password	The password used to access the mailbox on the email server. Type the password in the Confirm box to ensure accuracy. Contact Center Multimedia supports a maximum mailbox password length of 100 characters.
Use Alternative username for SMTP Authentication	If SMTP authentication is required for your outbound email server, select the user name for the authentication.

Deleting a scanned document reply mailbox

About this task

Delete a scanned document reply mailbox, if it is no longer required.

Important:

A scanned document reply mailbox cannot be deleted if it is currently assigned to a skillset.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Scanned Document**.
3. Click **Reply Configuration**.
4. Select the mailbox to be deleted.
5. Click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion.

Updating the scanned documents system default rule

Before you begin

- Ensure that you know the default settings for the system delivery failure rule:
  - use the scanned documents default skillset, SD_Default_Skillset
  - use no automatic response
  - assign priority 3
- Use caution when you change the properties of the system default rule:
  - If you change the properties of the rule, you affect the behavior of the system default rule, which affects all recipient mailboxes.
  - If you delete the skillset associated with the default rule, SD_Default_Skillset is used.
- Configure the route points for the skillset you assign to the system default rule. For more information, see Configuring a route point for a scanned document skillset on page 163.

About this task

Update the scanned documents system default rule to ensure that email messages received with scanned document attachments are routed to an agent if no other rule associated to the recipient mailbox routes the email message.

The system default rule is used in every rule group configured in Contact Center Multimedia.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Scanned Documents**.
3. Click **Default Rules**.
4. Under **System Default Rule**, from the **Skillset** list, select a skillset name to assign to the contact.

5. Under **System Default Rule**, from the **Priority** list, select the priority to assign to the contact.
6. Click **Save**.

Updating the scanned documents system delivery failure rule

Before you begin

- Ensure that you are licensed to handle email messages.
- Ensure that you know the default settings for the system delivery failure rule:
  - use the scanned documents default skillset, SD_Default _Skillset
  - use keyword group delivery failure keywords
  - assign priority 10 (lowest)
- Use caution when you change the properties of the system default rule:
  - If you change the properties of the rule, you affect the behavior of the system default rule, which affects all recipient mailboxes.
  - If you delete the skillset associated with the default rule, SD_Default_Skillset is used.
- Configure the route point for the skillset you plan to assign to the system delivery failure rule. See Configuring a route point for a scanned document skillset on page 163.

About this task

Update the scanned documents system delivery failure rule to ensure that any email message that contains particular phrases such as undeliverable, returned mail, unknown recipient, delivery failure, or delivery report is deleted and not assigned to an agent.

When you create a recipient mailbox, the system delivery failure rule is copied as the first regular rule into list of rules for the recipient mailbox.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Scanned Documents**.
3. Under **System Delivery Failure Rule**, from the **Skillset** list, select a skillset name to assign to the contact.
4. To change the keyword group, select the keyword group which contains the delivery failure keywords from the **Keyword Group** list under the **System Delivery Failure Rule**.
5. To change the priority, under **Priority**, select the priority to assign to the contact from the **Priority** list under the **System Delivery Failure Rule**.
6. To close contacts matching the delivery failure keywords, select the **Will close contact** check box.

7. Click **Save**.

Chapter 11: Fax configuration

This chapter contains the configuration steps for the fax recipient mailbox.

In the contact center, the recipient mailboxes are polled for incoming fax messages. A fax server forwards messages to an email address. The Contact Center Multimedia Email Manager retrieves the fax attachment (.tiff) and queues it to the appropriate skillset with an assigned priority. The caller ID is extracted to facilitate callbacks to the customer.

Reports appear in the Contact Center Multimedia Administration utility to show the current status of the fax traffic. The following reports appear when you select Fax and View Reports in the left column of the Contact Center Multimedia application. You can choose the report date and the skillsets represented in all displayed real-time reports.

- The Fax (New Vs. Closed) report shows the number of contacts in a new and closed state against the time for the selected date and skillsets.
- The Fax Progress report shows the number of contacts in a new or closed state on a defined date to determine the traffic levels for that date.
- The Fax Closed Contacts Queue Time report shows the average time a contact spends in queue while the contact center is open.

Prerequisites for fax configuration

Procedure

Ensure that you are licensed for email contacts.

Configuring a route point for a fax skillset

About this task

Configure a route point for a fax skillset to route fax contacts to a particular agent. Skillsets are used to assign the contacts to agents.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.

2. In the left pane, select **General Administration**.
3. Click **Skillset Settings**.
4. In the **Skillset Settings** dialog box, select the skillset to assign a route point.

   The skillset must have the prefix FX.
5. Under the **Edit Skillset** dialog box, in the **Route Point** list, select the route point to assign to the fax skillset.
6. Click **Save**.

Variable definitions

Name	Description
Route point	A location in the open queue that enables incoming contacts to queue and run through a script on the Contact Center Manager Server.

Adding a fax server

About this task

Add the fax server for your Contact Center Multimedia server as per your requirement.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Fax**.
3. Click **Mailbox Configuration**.
4. Click **Fax Server** (image).
5. In the Fax Server Configuration window, click **Add**.
6. In the **Fax Server Hostname** box, type the name of the new server.
7. In the **Type** box, select the type of server.
8. Click **Save**.

Updating a fax server

About this task

Update the fax server for your Contact Center Multimedia server as per your requirement.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Fax**.
3. Click **Mailbox Configuration**.
4. Click **Fax Server** (image).
5. In the Fax Server Configuration window, click **Edit**.
6. Change the properties of your fax server.
7. Click **Save**.

Deleting a fax server

About this task

Delete the fax server for your Contact Center Multimedia server if it is no longer required.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Fax**.
3. Click **Mailbox Configuration**.
4. Click **Fax Server**.
5. In the Fax Server Configuration window, select the server that you want to and click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion.
7. Click **Close**.

Adding a fax mailbox

Before you begin

- Configure a skillset for a fax contact.

About this task

Add a fax mailbox to the multimedia configuration for receiving fax messages as .tiff attachments.

Also, choose the skillset for the mailbox so that the fax message is routed to the agent who has the optimal skillset to handle the specific contact.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Fax**.
3. Click **Mailbox Configuration**.
4. Click **Add**.
5. On the **Mailbox** tab, in the **Inbound Server** field, select the host name of your POP3 or IMAP server along with the respective security protocol.
6. In the **Outbound Server** field, select the host name of your SMTP server.
7. In the **Mailbox** field, type the mailbox name.
8. In the **Domain** field, type the mailbox domain.
9. In the **Password** and **Confirm** fields, type and retype the password to access the mailbox.
10. In the **Skillset** field, choose a configured skillset for routing the contacts.
11. In the **Contact Priority** field, choose a priority for contacts received in this mailbox.
12. Click the **Sender Address** tab.
13. Select **Use full sender address** or **Parse sender address for CLID**.
14. If you select **Parse sender address for CLID**, in the **Leading Characters to Remove** field, type the characters that you must not dial when making the outgoing callback.
15. Click **Save**.

Variable definitions

Name	Description
Inbound Server	The host name of the email server that handles email messages entering the contact center.

Table continues…

Name	Description
Outbound Server	The host name of the email server that delivers email messages that leave the contact center.
Mailbox	Name of the mailbox on the email server that is polled for new incoming email messages.
Domain	The domain name for the email server.
Password	The password used to access the mailbox on the email server. Type the password in the Confirm box to ensure accuracy. Contact Center Multimedia supports a maximum mailbox password length of 100 characters.
Skillset	A label applied to a set of skills, capabilities, or knowledge that an agent requires to respond to a request. The skillsets are retrieved from the Contact Center Manager Server database. You must select a route point for a skillset used to route contacts.
Priority	The priority given to a request for a skillset agent. The lower the priority number, the greater the priority. The values of the priorities range from 1 to 6. For example, a call with priority 1 is handled before a call with priority 6.
Sender address	Select Use full sender address or Parse the address for the Calling Line identification (CLID) to save for future contacts. The address in the format you select is stored with the contact for future communication with the customer.
Leading characters to remove	If you select a Calling Line Identification (CLID) to add the customer's phone number into the contact information, type any leading characters or trunk numbers to remove from the current number.

Updating a fax mailbox

Before you begin

- Add a fax mailbox.

About this task

Update the properties of the fax mailbox, as per your requirements.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.

2. In the left pane, select **Fax**.
3. Click **Mailbox Configuration**.
4. Select the mailbox to be edited.
5. Click **Edit**.
6. Update the mailbox settings as required
7. Click **Save**.

Deleting a fax mailbox

Before you begin

- Add a fax mailbox.

❗ **Important:**

A fax mailbox cannot be deleted if it is currently assigned to a skillset.

About this task

Delete a fax mailbox, if it is no longer required.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Fax**.
3. Click **Mailbox Configuration**.
4. Select the mailbox to be deleted.
5. Click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion.

Configuring a fax reply mailbox

About this task

Configure the reply information for the fax message received by your contact center.

Configure the outgoing mailbox properties with a signature related to the skillset for replying to fax messages.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Fax**.
3. Click **Reply Configuration**.
4. Under **Skillsets**, select a fax skillset for the mailbox configuration.
5. Under **Mailbox**, select a configured mailbox.

   OR

   Click **New** to create a new mailbox.

   OR

   Click **Edit** to edit an existing mailbox.
6. In the **SMTP Server** box, select the SMTP server to use for outgoing email messages.
7. In the **Mailbox** box, specify the new mailbox or change the name of the existing mailbox.
8. In the **Domain** box, type the email server domain.
9. In the **Password** and **Confirm** boxes, type the email server password.
10. To use a different user name for the SMTP authentication, select the **Use Alternative username for SMTP Authentication** check box.
11. In the **Username** box, type the alternative user name.
12. Click **Save**.

Variable definitions

Name	Description
SMTP Server	The name of the email server that handles email messages leaving the contact center.
Mailbox	Name of the mailbox on the email server polled for email messages.
Domain	The domain name for the email server.
Password	The password used to access the mailbox on the email server. Type the password in the Confirm box to ensure accuracy. Contact Center Multimedia supports a maximum mailbox password length of 100 characters.
Use Alternative username for SMTP Authentication	If SMTP authentication is required for your outbound email server, select the user name for the authentication.

Deleting a fax reply mailbox

About this task

Delete a fax reply mailbox, if it is no longer required.

Important:

A fax reply mailbox cannot be deleted if it is currently assigned to a skillset.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Fax**.
3. Click **Reply Configuration**.
4. Select the mailbox to be deleted.
5. Click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion.

Updating the fax system default rule

Before you begin

- Ensure that you know the default settings for the system delivery failure rule:
  - use the fax default skillset, FX_Default_Skillset
  - use no automatic response
  - assign priority 3
- Use caution when you change the properties of the system default rule:
  - If you change the properties of the rule, you affect the behavior of the system default rule, which affects all recipient mailboxes.
  - If you delete the skillset associated with the default rule, FX_Default_Skillset is used.
- Configure the route points for the skillset you assign to the system default rule. For more information, see Configuring a route point for a fax skillset on page 173.

About this task

Update the fax system default rule to ensure that email messages received with fax attachments are routed to an agent if no other rule associated to the recipient mailbox routes the email message.

The system default rule is used in every rule group configured in Contact Center Multimedia.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Fax**.
3. Click **Default Rules**.
4. Under **System Default Rule**, from the **Skillset** list, select a skillset name to assign to the contact.
5. Under **System Default Rule**, from the **Priority** list, select the priority to assign to the contact.
6. Click **Save**.

Updating the fax system delivery failure rule

Before you begin

- Ensure that you are licensed to handle email messages.
- Ensure that you know the default settings for the system delivery failure rule:
  - use the fax default skillset, FX_Default _Skillset
  - use keyword group delivery failure keywords
  - assign priority 10 (lowest)
- Use caution when you change the properties of the system default rule:
  - If you change the properties of the rule, you affect the behavior of the system default rule, which affects all recipient mailboxes.
  - If you delete the skillset associated with the default rule, FX_Default_Skillset is used.
- Configure the route point for the skillset you plan to assign to the system delivery failure rule. See Configuring a route point for a fax skillset on page 173.

About this task

Update the fax system delivery failure rule to ensure that any email message that contains particular phrases such as undeliverable, returned mail, unknown recipient, delivery failure, or delivery report is deleted and not assigned to an agent.

When you create a recipient mailbox, the system delivery failure rule is copied as the first regular rule into list of rules for the recipient mailbox.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Fax**.

3. Under **System Delivery Failure Rule**, from the **Skillset** list, select a skillset name to assign to the contact.
4. To change the keyword group, select the keyword group which contains the delivery failure keywords from the **Keyword Group** list under the **System Delivery Failure Rule**.
5. To change the priority, under **Priority**, select the priority to assign to the contact from the **Priority** list under the **System Delivery Failure Rule**.
6. To close contacts matching the delivery failure keywords, select the **Will close contact** check box.
7. Click **Save**.

Chapter 12: Short Message Service configuration

This chapter contains the configuration steps for the SMS recipient mailbox.

In the contact center, the recipient mailboxes are polled for incoming Short Message Service (SMS) messages. A server forwards the SMS messages to an email address. The Contact Center Multimedia Email Manager retrieves the text of the SMS and queues it to the appropriate skillset with an assigned priority. The caller ID is extracted to facilitate callbacks to the customer.

Reports appear in the Contact Center Multimedia Administration utility to show the current traffic status. The following reports appear when you select Text Messages (SMS) and View Reports in the left column of the Contact Center Multimedia application. You can choose the report date and the skillsets represented in all displayed real-time reports.

- The SMS (New Vs. Closed) report shows the number of contacts in a new and closed state against the time for the selected date and skillsets.
- The SMS Progress report shows the number of contacts in a new or closed state on a defined date to determine the traffic levels for that date.
- The SMS Closed Contacts Queue Time report shows the average time a contact spends in queue while the contact center is open.

Prerequisites for SMS configuration

Procedure

Ensure that you are licensed for email contacts.

Configuring a route point for an SMS skillset

About this task

Configure a route point for an SMS skillset to route SMS contacts to an agent. Skillsets are used to assign the contacts to agents.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **General Administration**.
3. Click **Skillset Settings**.
4. In the **Skillset Settings** dialog box, select the skillset to assign a route point.

   The skillset must have the prefix SM.
5. Under the **Edit Skillset** dialog box, in the **Route Point** list, select the route point to assign to the SMS skillset.
6. Click **Save**.

Variable definitions

Name	Description
Route point	A location in the open queue that enables incoming contacts to queue and run through a script on the Contact Center Manager Server.

Adding an SMS Gateway

About this task

Add the SMS server for your Contact Center Multimedia server as per your requirement.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Text Messaging (SMS)**.
3. Click **Mailbox Configuration**.
4. Click **SMS Gateway** (image).
5. In the SMS Gateway Configuration window, click **Add**.
6. In the **SMS Gateway** box, type the name of the new server.
7. Click **Save**.

Updating an SMS Gateway

About this task

Update the SMS server for your Contact Center Multimedia server as per your requirement.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Text Messaging (SMS)**.
3. Click **Mailbox Configuration**.
4. Click **SMS Gateway** (image).
5. In the SMS Gateway Configuration window, click **Edit**.
6. Change the properties of your SMS server.
7. Click **Save**.

Deleting an SMS Gateway

About this task

Delete the SMS server for your Contact Center Multimedia server if it is no longer required.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Text Messaging (SMS)**.
3. Click **Mailbox Configuration**.
4. Click **SMS Gateway** (image).
5. In the SMS Gateway Configuration window, select the SMS gateway you are deleting and click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion.
7. Click **Close**.

Adding a SMS mailbox

Before you begin

- Configure a skillset for a SMS contact.

About this task

Add a SMS mailbox to the multimedia configuration for receiving SMS messages in an email message.

Also, choose the skillset for the mailbox so that the SMS message is routed to the agent who has the optimal skillset to handle the specific contact.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Text Messaging (SMS)**.
3. Click **Mailbox Configuration**.
4. Click **Add**.
5. On the **Mailbox** tab, in the **Inbound Server** field, select the host name of your POP3 or IMAP server along with the respective security protocol.
6. In the **Outbound Server** field, select the host name of your SMTP server.
7. In the **Mailbox** field, type the mailbox name.
8. In the **Domain** field, type the mailbox domain.
9. In the **Password** and **Confirm** fields, type and retype the password to access the mailbox.
10. In the **Skillset** field, choose a configured skillset for routing the contacts.
11. In the **Contact Priority** field, choose a priority for contacts received in this mailbox.
12. Click the **Sender Address** tab.
13. Select **Use full sender address** or **Parse sender address for CLID**.
14. If you select **Parse sender address for CLID**, in the **Leading Characters to Remove** field, type the characters that you must not dial when making the outgoing callback.
15. Click **Save**.

Variable definitions

Name	Description
Inbound Server	The host name of the email server that handles email messages entering the contact center.

Table continues…

Name	Description
Outbound Server	The host name of the email server that delivers email messages that leave the contact center.
Mailbox	Name of the mailbox on the email server that is polled for new incoming email messages.
Domain	The domain name for the email server.
Password	The password used to access the mailbox on the email server. Type the password in the Confirm Password box to ensure accuracy. Contact Center Multimedia supports a maximum mailbox password length of 100 characters.
Skillset	A label applied to a set of skills, capabilities, or knowledge that an agent requires to respond to a request. The skillsets are retrieved from the Contact Center Manager Server database. You must select a route point for a skillset used to route SMS contacts.
Priority	The priority given to a request for a skillset agent. The lower the priority number, the greater the priority. The values of the priorities range from 1 to 6. For example, a call with priority 1 is handled before a call with priority 6.
Sender address	Select Use full sender address or Parse the address for the Calling Line identification (CLID) to save for future contacts. The address in the format you select is stored with the contact for future communication with the customer.
Leading characters to remove	If you select Calling Line Identification (CLID) to add the customer’s phone number into the contact information, type any leading characters or trunk numbers to remove from the current number.

Updating an SMS mailbox

Before you begin

- Add an SMS mailbox.

About this task

Update the properties of the SMS mailbox, as per your requirements.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Text Messaging (SMS)**.
3. Click **Mailbox Configuration**.
4. Select the mailbox to be edited.
5. Click **Edit**.
6. Update the mailbox settings as required.
7. Click **Save**.

Deleting an SMS mailbox

Before you begin

- Add an SMS mailbox.

Important:

An SMS mailbox cannot be deleted if it is currently assigned to a skillset.

About this task

Delete an SMS mailbox, if it is no longer required.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Text Messaging (SMS)**.
3. Click **Mailbox Configuration**.
4. Select the mailbox to be deleted.
5. Click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion.

Configuring an SMS reply mailbox

About this task

Configure the reply information for the SMS message received by your contact center.

Configure the outgoing mailbox properties with a signature related to the skillset for replying to an SMS.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Text Messaging (SMS)**.
3. Click **Reply Configuration**.
4. Under **Skillsets**, select a fax skillset for the mailbox configuration.
5. Under **Mailbox**, select a configured mailbox.

   OR

   Click **New** to create a new mailbox.

   OR

   Click **Edit** to edit an existing mailbox.
6. In the **SMTP Server** box, select the SMTP server to use for outgoing email messages.
7. In the **Mailbox** box, specify the new mailbox or change the name of the existing mailbox.
8. In the **Domain** box, type the email server domain.
9. In the **Password** and **Confirm** boxes, type the email server password.
10. To use a different user name for the SMTP authentication, select the **Use Alternative username for SMTP Authentication** check box.
11. In the **Username** box, type the alternative user name.
12. Click **Save**.

Variable definitions

Name	Description
SMTP Server	The name of the email server that handles email messages leaving the contact center.
Mailbox	Name of the mailbox on the email server polled for email messages.
Domain	The domain name for the email server.
Password	The password used to access the mailbox on the email server. Type the password in the Confirm Password box to ensure accuracy. Contact Center Multimedia supports a maximum mailbox password length of 100 characters.

Table continues…

Name	Description
Use Alternative username for SMTP Authentication	If SMTP authentication is required for your outbound email server, select the user name for the authentication.

Deleting an SMS reply mailbox

About this task

Delete an SMS reply mailbox, if it is no longer required.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, select **Text Messaging (SMS)**.
3. Click **Reply Configuration**.
4. Select the mailbox to be deleted.
5. Click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion.

Updating the SMS system default rule

Before you begin

- Ensure that you know the default settings for the system delivery failure rule:
  - use the SMS default skillset, SM_Default_Skillset
  - use no automatic response
  - assign priority 3
- Use caution when you change the properties of the system default rule:
  - If you change the properties of the rule, you affect the behavior of the system default rule, which affects all recipient mailboxes.
  - If you delete the skillset associated with the default rule, SM_Default_Skillset is used.
- Configure the route points for the skillset you assign to the system default rule. For more information, see Configuring a route point for an SMS skillset on page 183.

About this task

Update the SMS system default rule to ensure that email messages received with SMS text are routed to an agent if no other rule associated to the recipient mailbox routes the email message.

The system default rule is used in every rule group configured in Contact Center Multimedia.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Text Messaging (SMS)**.
3. Click **Default Rules**.
4. Under **System Default Rule**, from the **Skillset** list, select a skillset name to assign to the contact.
5. Under **System Default Rule**, from the **Priority** list, select the priority to assign to the contact.
6. Click **Save**.

Updating the SMS system delivery failure rule

Before you begin

- Ensure that you are licensed to handle email messages.
- Ensure that you know the default settings for the system delivery failure rule:
  - use the SMS default skillset, SM_Default _Skillset
  - use keyword group delivery failure keywords
  - assign priority 10 (lowest)
- Use caution when you change the properties of the system default rule:
  - If you change the properties of the rule, you affect the behavior of the system default rule, which affects all recipient mailboxes.
  - If you delete the skillset associated with the default rule, SM_Default_Skillset is used.
- Configure the route point for the skillset you plan to assign to the system delivery failure rule. See Configuring a route point for an SMS skillset on page 183.

About this task

Update the SMS system delivery failure rule to ensure that any email message that contains particular phrases such as undeliverable, returned mail, unknown recipient, delivery failure, or delivery report is deleted, and not assigned to an agent.

When you create a recipient mailbox, the system delivery failure rule is copied as the first regular rule into list of rules for the recipient mailbox.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 41.
2. In the left pane, click **Text Messaging (SMS)**.
3. Under **System Delivery Failure Rule**, from the **Skillset** list, select a skillset name to assign to the contact.
4. To change the keyword group, select the keyword group which contains the delivery failure keywords from the **Keyword Group** list under the **System Delivery Failure Rule**.
5. To change the priority, under **Priority**, select the priority to assign to the contact from the **Priority** list under the **System Delivery Failure Rule**.
6. To close contacts matching the delivery failure keywords, select the **Will close contact** check box.
7. Click **Save**.

Chapter 13: Data Management - cleanup and purging

Use the procedures in this chapter to set up the cleanup rules and tasks to remove closed contacts from the active Multimedia database.

Avaya Contact Center Select includes a Multimedia Offline database, a background synchronization task, and cleanup and purge tools. The background synchronization task automatically updates contacts from the active Multimedia database to the Offline database. You create rules and schedules to clean up the active Multimedia database by removing closed contacts from it, while leaving them in the Offline database. This keeps the active database small and efficient, while also allowing for historical reporting across all the contacts in both the active and the Multimedia Offline databases

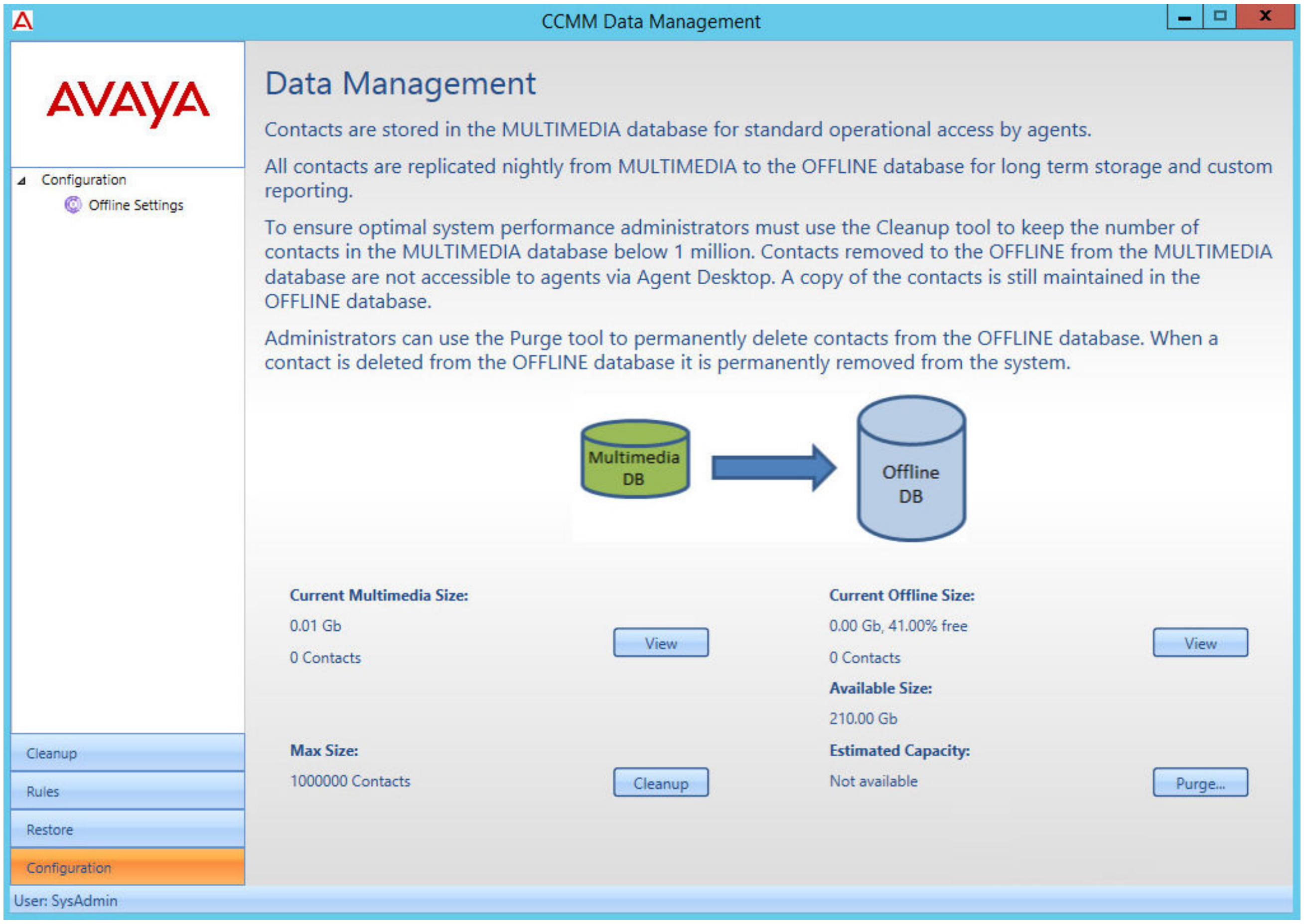
You can configure the Offline database to purge contacts over a specific age. You specify the age at which ACCS purges closed contacts. ACCS runs a purge task every day, and purges contacts that meet the age criteria. You cannot recover a purged contact other than by restoring a backed-up Offline database.

Database sizing and limits

The active Multimedia database supports a maximum of 1,000,000 contacts. You must regularly cleanup contacts from the active Multimedia database to stay below this limit. The maximum size of the Offline database is 70% of the database drive size. For example, if the Multimedia database drive size is 200 Gb, then the maximum size of the Offline database is 140 Gb. If the Offline database fills up, you can either increase the Multimedia database disk space, or change the Offline database purge interval.

To prevent service interruption, updates to the Offline database stop when the database drive size is 70% full and the Offline database has less than 5% free space. Updates continue after you purge contacts, or if space is freed or added to the drive.

You can check the current sizes of the databases in the CCMM Data Management tool.



Data Management

Contacts are stored in the MULTIMEDIA database for standard operational access by agents.

All contacts are replicated nightly from MULTIMEDIA to the OFFLINE database for long term storage and custom reporting.

To ensure optimal system performance administrators must use the Cleanup tool to keep the number of contacts in the MULTIMEDIA database below 1 million. Contacts removed to the OFFLINE from the MULTIMEDIA database are not accessible to agents via Agent Desktop. A copy of the contacts is still maintained in the OFFLINE database.

Administrators can use the Purge tool to permanently delete contacts from the OFFLINE database. When a contact is deleted from the OFFLINE database it is permanently removed from the system.

Current Multimedia Size:
0.01 Gb
0 Contacts

Max Size:
1000000 Contacts

Current Offline Size:
0.00 Gb, 41.00% free
0 Contacts

Available Size:
210.00 Gb

Estimated Capacity:
Not available

Figure 4: Data Management Configuration screen

When the current size of the Offline database grows to 75% of the maximum size, CCMM logs this event to the log file. When the current size of the Offline database grows above 90% of the maximum size, CCMM logs events to the event viewer. If the current size of the Offline database exceeds 95%, CCMM stops automatically synchronizing contacts from the Multimedia database, and prevents you from running manual or scheduled archives.

You can purge contacts from the Offline database to reduce the database size. You specify the age at which ACCS purges closed contacts. ACCS runs a purge task every day, and purges contacts that meet the age criteria. You cannot recover a purged contact other than by restoring a backed-up Offline database.

Cleanup rules

You create a cleanup rule to select contacts for a scheduled cleanup task. Cleanup rules apply to the Multimedia database only. Cleanup rules select contacts based on the number of days they have been in a Closed state, and any one of the following criteria:

- outbound campaign
- email rule
- contact skillset

- closed reason
- contact customer

In addition, there are four system cleanup rules:

- **Anonymous web customers with no contacts**: This rule clears anonymous customers that a Web Chat application can create, if it allows customers to start a web chat anonymously.
- **Customers with no contacts**: This rule clears customer records with no contacts, which can occur on systems upgraded from an earlier release.
- **All contacts more than 1 year old**: This rule clears all contacts that are more than 1 year old.
- **All contacts more than 5 years old**: This rule clears all contacts that are more than 5 years old.

You cannot modify these rules. They allow you to clear customer records with no contacts that occur in exceptional circumstances. Run scheduled tasks with these rules periodically to clear unwanted customer records from the active database.

Each scheduled cleanup task uses a rule, so you must create a rule before you can create a scheduled task.

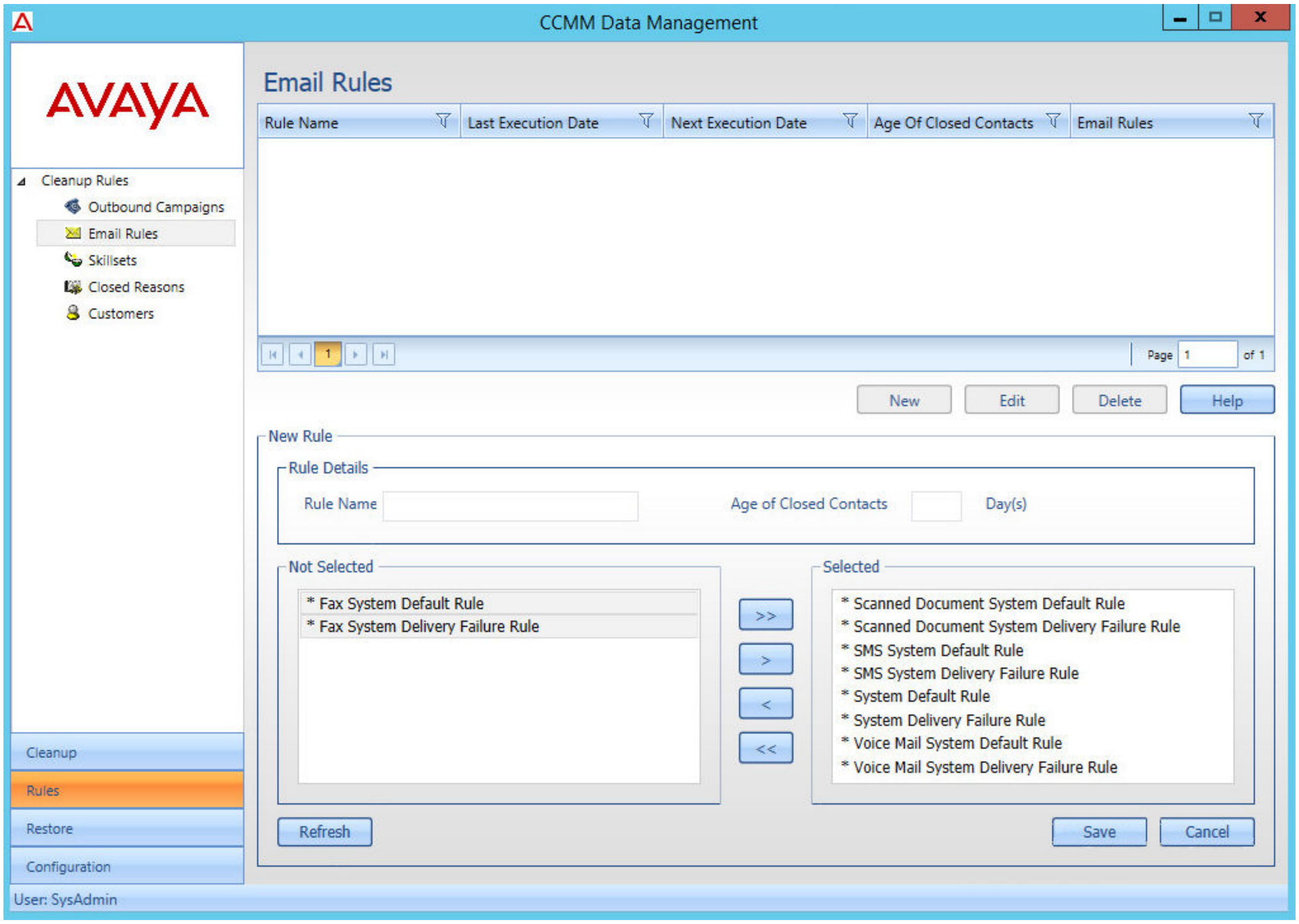


Figure 5: The Multimedia Data Management utility rules interface

Scheduled tasks

You create scheduled cleanup tasks to clear contacts from the active Multimedia database. A scheduled task uses a single cleanup rule to select the contacts to clear. Scheduled tasks clear only closed contacts that were already copied to the Multimedia Offline database. If a contact was not previously copied to the Multimedia Offline database, the scheduled task copies it and then clears it.

The following figure shows the interface that you use to create scheduled cleanups of the active Multimedia database.

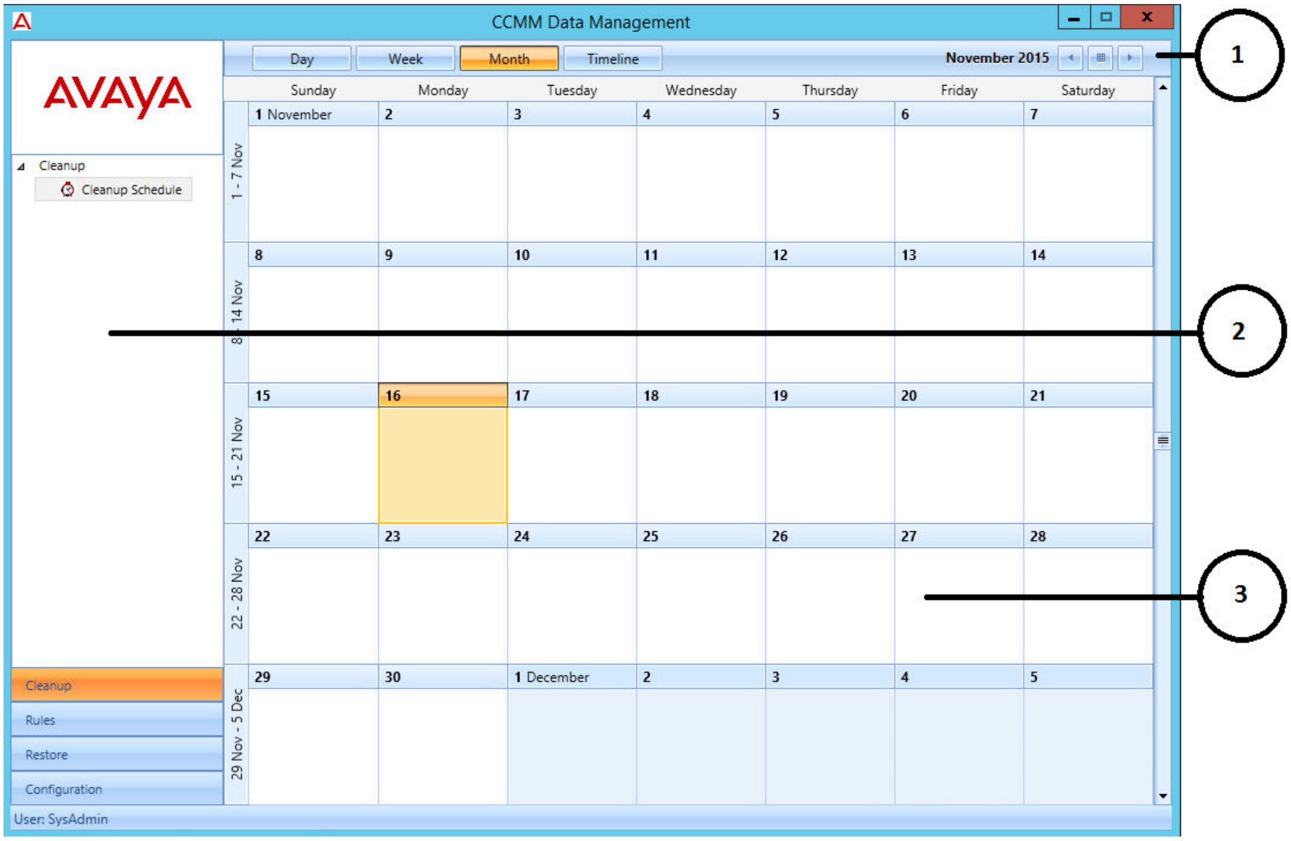


Figure 6: The Multimedia Archive Administration tool scheduling interface

The illustrated interface shows three work areas:

1	The Top Bar.
2	The Navigation Pane.
3	The Scheduled Task Calendar.

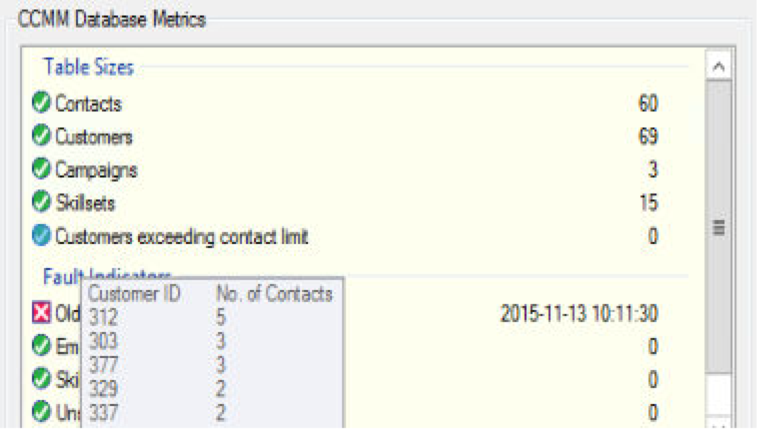
Restoring contacts

You can restore the contacts cleared by a scheduled cleanup task.

Using the Multimedia Dashboard metrics to identify data to purge

You can use the Multimedia Dashboard metrics to identify data to clean up. The CCMM Database Metrics section shows alerts when the metrics exceed normal thresholds. If you place your mouse over the alerting metric, the Dashboard displays a tooltip with details of the database values causing the alert. For example, if the database has one or more customers with over 1000 contacts, the tooltip displays:

- the customer IDs
- number of contacts for the customer



CCMM Database Metrics

Table Sizes

✓ Contacts	60
✓ Customers	69
✓ Campaigns	3
✓ Skillsets	15
✓ Customers exceeding contact limit	0

Fault Indicators

☒ Old	2015-11-13 10:11:30
✓ Em	0
✓ Ski	0
✓ Un	0

Customer ID	No. of Contacts
312	5
303	3
377	3
329	2
337	2

Figure 7: Example of a dashboard tooltip identifying the number of contacts customers have

Starting the Multimedia Data Management utility

Before you begin

- Log on to the Contact Center server.

About this task

Start the Multimedia Data Management utility to configure your cleanup rules and scheduled tasks.

Procedure

On the **Apps** screen, in the **Avaya** section, select **Data Management**.

Creating an Outbound Campaigns cleanup rule

Before you begin

- Log on to the Contact Center server.
- Start the Multimedia Data Management utility.

About this task

Create a cleanup rule to select closed contacts in the MULTIMEDIA database, based on the outbound campaign that closed the contact. You can use this rule in a scheduled cleanup task to clear these contacts from the MULTIMEDIA database. There are two criteria you can use to select contacts by outbound campaign:

- The number of days the contact has been in a Closed state.
- The outbound campaign that created and closed the contact.

Procedure

1. In the Data Management utility, select **Rules**.
2. Select **Outbound Campaigns**.
3. In the **Outbound Campaigns** screen, click **New**.
4. In the **Rule Name** field, enter a descriptive name for this rule.
5. In the **Age of Closed Contacts** field, type the number of days that a contact must be Closed to match this rule.
6. If you want to remove the campaign from the Outbound Campaign Management Tools (OCMT) Campaign List, select **Delete Campaign**.

   OCMT removes the campaign from the Campaign List when a cleanup task has removed all the campaign contacts and the campaign is Expired, Cancelled, or Completed.
7. For each campaign you want to add to the rule:
   a. In the **Not Selected** field, select an outbound campaign.
   b. Click the right-arrow button to move the outbound campaign to the **Selected** field.
8. For each campaign you want to remove from the rule:
   a. In the **Selected** field, select an outbound campaign.
   b. Click the left-arrow button to move the outbound campaign to the **Not Selected** field.
9. Click **Save**.

Next steps

Create a new scheduled task to use this rule to clear closed contacts from the MULTIMEDIA database.

Creating an Email Rules cleanup rule

Before you begin

- Log on to the Contact Center server.
- Start the Multimedia Data Management utility.

About this task

Create a cleanup rule to select closed email contacts in the MULTIMEDIA database. You can use this rule in a scheduled cleanup task to clear these contacts from the database. There are two criteria you can use to select email contacts:

- The number of days the contact has been in a Closed state.
- The email rule that the incoming email matched when Contact Center created the contact.

Procedure

1. In the Data Management utility, select **Rules**.
2. Select **Email Rules**.
3. In the **Email Rules** screen, click **New**.
4. In the **Rule Name** field, enter a descriptive name for this rule.
5. In the **Age of Closed Contacts** field, type the number of days that a contact must be Closed to match this rule.
6. For each email rule you want to add to the cleanup rule:
    a. In the **Not Selected** field, select an email rule.
    b. Click the right-arrow button to move the email rule to the **Selected** field.
7. For each email rule you want to remove from the rule:
    a. In the **Selected** field, select an email rule.
    b. Click the left-arrow button to move the email rule to the **Not Selected** field.
8. Click **Save**.

Next steps

Create a new scheduled task to use this rule to clear closed contacts from the MULTIMEDIA database.

Creating a Skillsets cleanup rule

Before you begin

- Log on to the Contact Center server.
- Start the Multimedia Data Management utility.

About this task

Create a cleanup rule to select closed contacts in the MULTIMEDIA database, based on the contact skillset. You can use this rule in a scheduled cleanup task to clear these contacts from the database. There are two criteria you can use to select contacts by skillset:

- The number of days the contact has been in a Closed state.

- The contact skillset.

Procedure

1. In the Data Management utility, select **Rules**.
2. Select **Skillsets**.
3. In the **Skillset Rules** screen, click **New**.
4. In the **Rule Name** field, enter a descriptive name for this rule.
5. In the **Age of Closed Contacts** field, type the number of days that a contact must be Closed to match this rule.
6. For each skillset you want to add to the cleanup rule:
    a. In the **Not Selected** field, select a skillset.
    b. Click the right-arrow button to move the skillset to the **Selected** field.
7. For each skillset you want to remove from the rule:
    a. In the **Selected** field, select a skillset.
    b. Click the left-arrow button to move the skillset to the **Not Selected** field.
8. Click **Save**.

Next steps

Create a new scheduled task to use this rule to clear closed contacts from the MULTIMEDIA database.

Creating a Closed Reason cleanup rule

Before you begin

- Log on to the Contact Center server.
- Start the Multimedia Data Management utility.

About this task

Create a cleanup rule to select closed contacts in the MULTIMEDIA database, based on the closed reason. You can use this rule in a scheduled cleanup task to clear these contacts from the database. There are two criteria you can use to select contacts by closed reason:

- The number of days the contact has been in a Closed state.
- The closed reason code an agent applied to the contact.

Procedure

1. In the Data Management utility, select **Rules**.
2. Select **Closed Reason**.

3. In the **Closed Reason Rules** screen, click **New**.
4. In the **Rule Name** field, enter a descriptive name for this rule.
5. In the **Age of Closed Contacts** field, type the number of days that a contact must be Closed to match this rule.
6. For each closed reason you want to add to the cleanup rule:
    a. In the **Not Selected** field, select a closed reason.
    b. Click the right-arrow button to move the closed reason to the **Selected** field.
7. For each closed reason you want to remove from the rule:
    a. In the **Selected** field, select a closed reason.
    b. Click the left-arrow button to move the closed reason to the **Not Selected** field.
8. Click **Save**.

Next steps

Create a new scheduled task to use this rule to clear closed contacts from the MULTIMEDIA database.

Creating a Customers cleanup rule

Before you begin

- Log on to the Contact Center server.
- Start the Multimedia Data Management utility.

About this task

Create a cleanup rule to select closed contacts in the MULTIMEDIA database, based on the contact customer. You can use this rule in a scheduled cleanup task to clear these contacts from the database. There are two criteria you can use to select contacts by customer:

- The number of days the contact has been in a Closed state.
- The contact customer.

Note:

The search function returns and displays the customer First and Last name. Different customers might share the same First and Last names. Therefore the results of the search function can be identical for different customer’s IDs.

Procedure

1. In the Data Management utility, select **Rules**.
2. Select **Customers**.
3. In the **Customer Rules** screen, click **New**.

4. In the **Rule Name** field, enter a descriptive name for this rule.
5. In the **Age of Closed Contacts** field, type the number of days that a contact must be Closed to match this rule.
6. For each customer you want to add to the cleanup rule:
    a. In the **Customer Search** field, select the search key for the customer, either **ID** or **E-mail**.
    b. In the **Equal To** field, type the ID or email address of the customer that you want to add to the rule.
    c. Click **Search**.
    d. Select the customer that the search function returns.
    e. Click the right-arrow button to move the customer to the **Selected** field.
7. For each customer you want to remove from the rule:
    a. In the **Selected** field, select a customer.
    b. Click the left-arrow button to move the customer to the **Not Selected** field.
8. Click **Save**.

Next steps

Create a new scheduled task to use this rule to clear closed contacts from the MULTIMEDIA database.

Creating a new scheduled cleanup task

Before you begin

- Log on to the Contact Center server.
- Start the Multimedia Data Management utility.
- Create a new rule to select the contacts you want to clear.

About this task

Create a scheduled cleanup task to clear contacts from the MULTIMEDIA contact database. A scheduled task uses a single cleanup rule to select the contacts to clear. Scheduled tasks clear only closed contacts that were already copied to the OFFLINE database. If a contact was not previously copied to the OFFLINE database, the scheduled task copies it before clearing it.

You can select only a single rule for each scheduled task. You can choose to run a scheduled task once, weekly, or monthly. If you select to run a scheduled task weekly or monthly, you can optionally set an end date after which the scheduled task does not run.

The Cleanup Schedule interface shows a calendar, in a similar manner to many graphical scheduling tools. You can change the calendar to use Week, Month, or Timeline views.

Procedure

1. In the Data Management utility, select **Cleanup**.
2. Select **Cleanup Schedule**.
3. In the schedule calendar, select the date on which you want to schedule a cleanup task. You can use the **Day**, **Week**, **Month**, **Timeline**, **Back**, **Calendar**, and **Forward** controls in the Top Bar to browse to a date if it is not currently visible.
4. Double click the date on which you want to create the scheduled task.

   Contact Center displays the **Schedule Cleanup** window.
5. In the **Name** field, enter a display name for this scheduled task.
6. In the **Description** field, enter a description of what this scheduled task does.
7. In the **Select Type** field, select the type of cleanup rule for this scheduled task.
8. In the **Select Rule** field, select an existing cleanup rule that the scheduled task uses to identify contacts to clear.
9. In the **Schedule** section, select the frequency with which you want this task to run; either **Run Once**, **Weekly**, or **Monthly**.
10. If you selected **Run Once**:

    In the **Start Date** fields, select the date and time on which you want the task to run.
11. If you selected **Weekly**:
    a. In the **Start Date** fields, select the first date and time on which you want the task to run.
    b. Select the days of the week on which you want the task to run.
    c. If you want this scheduled task to stop running after a date in the future, select **End on** and select a date after which this task does not run.
12. If you selected **Monthly**:
    a. In the **Start Date** fields, select the first date and time on which you want the task to run.
    b. In the **Day** field, enter the day of the month on which you want the task to run.
    c. In the **of every** field, enter the frequency of this monthly task.

       For example, enter 1 to run the task every month, enter 2 to run the task every second month, or enter 12 to run the task once a year.
    d. If you want this scheduled task to stop running after a date in the future, select **End on** and select a date after which this task does not run.
13. Click **Save**.

Enabling OFFLINE database purging

Before you begin

- Log on to the Contact Center server.
- Start the Multimedia Data Management utility.

About this task

Enable OFFLINE database purging to permanently remove closed contacts from the OFFLINE database. Choose the length of time that closed contacts can remain in the OFFLINE database before Contact Center purges them. Contact Center runs the purge task every day, and deletes contacts that have been closed for the duration you configure. Avaya recommends that you do not configure purging unless the OFFLINE database approaches maximum usage.

Important:

When Contact Center purges a contact from the OFFLINE database, you cannot recover the contact except by retrieving it from a backed-up OFFLINE database. Ensure the duration you configure to retain contacts is consistent with your local legislative and corporate data retention requirements.

Procedure

1. In the Data Management utility, select **Configuration**.
2. Click **Purge**.
3. On the **Purge Settings** dialog, select **Enable Data Purge**.
4. In the **Keep Offline records (months)** field, type the number of months a contact must be closed for Contact Center to purge it from the OFFLINE database.

   Ensure the value you enter is consistent with your local legislative and corporate data retention requirements.
5. Click **Save**.
6. On the **CCMM Data Management** dialog, click **Yes**.
7. On the **Purge Settings** dialog, click **Close**.

Restoring an archive from a previous Release

Before you begin

- The archive from the previous Release must be in the original archive location.

About this task

You can restore Multimedia database archives from the previous Release if you need to recover old contacts to work with them. Use the legacy Multimedia Archive/Restore Utility to restore the contacts. Reopen the contacts you want to work with, and then cleanup the rest of the contacts so that Contact Center moves them to the OFFLINE database.

Procedure

1. Run the legacy Multimedia RestoreArchive executable `D:\Avaya\Contact Center\Multimedia Server\Server Applications\ARCHIVE RESTORE\ArchiveRestore.exe`.
2. Click **Restore**.
3. In the **Restore** pane, select the archive you want to restore.
4. Click **Restore**.
5. When the restore completes, exit the Archive/Restore Utility.
6. Use Agent Desktop to search for and reopen the contacts that you want to work with, so that they remain in the MULTIMEDIA database.
7. On the **Apps** screen, in the **Avaya** section, select **Data Management**.
8. Create a new cleanup rule to clear the restored contacts from the active database. The configuration of this rule depends on the contacts that you restored.
9. Click **Cleanup Schedule**.
10. Create a scheduled task with the new cleanup rule to clear the restored contacts from the MULTIMEDIA database.

Restoring contacts cleared by a scheduled task

Before you begin

- Log on to the Contact Center server.
- Start the Multimedia Data Management utility.

About this task

Follow this procedure to restore the contacts cleared by a scheduled cleanup task. When you restore a scheduled task, Contact Center restores all the cleared contacts to the MULTIMEDIA database.

If you need to restore contacts previously cleared by a scheduled task, check to ensure that an existing scheduled task does not clear the contacts the next time it runs. For example, re-open the contacts, cancel the scheduled task that originally cleared them, or change the cleanup rule that the contacts matched.

The Cleanup History list shows all previously-completed scheduled tasks that cleared contacts. It provides the following information for each task:

- The task name.
- The execution date of the task.
- The number of contacts that the task cleared from the MULTIMEDIA database.
- The number of customers whose contacts the task cleared from the database.

- The number of campaigns for which the task cleared contacts from the database (only for tasks with an Outbound rule).
- The restore status of the task.

Note:

Avaya recommends running one cleanup task at a time. Where more than one cleanup task is run a contact might be included in each cleanup. Restoring any of the cleanups successfully moves the contact into the active database.

Procedure

1. In the Data Management utility, select **Restore**.
2. In the navigation pane, select **Restore**.
3. In the **Cleanup History** screen, review the list of completed scheduled cleanup tasks.
4. Select the scheduled task that cleared the contacts that you want to restore.
5. Click **Restore**.
6. On the **CCMM Cleanup Restore** window, click **Yes**.

   Contact Center schedules a task to restore the contacts, and shows the start time in the **Restore Status** field. When the restore task starts, the **Restore Status** field shows the task progress.

Chapter 14: Data Management - customer privacy

The Multimedia Data Management utility includes a Customer Privacy tab that allows you to act on privacy requests from contact center customers. The following customer privacy requests can be addressed using the Multimedia Data Management utility:

- If a customer exercises their right to access information, you can provide customers with information stored about them in the MULTIMEDIA and OFFLINE databases. You can save this information in an XML file, which can be modified before you provide it to the customer. The file contains all relevant customer information.
- If a customer exercises the right to be forgotten, you can delete their history records from the MULTIMEDIA and OFFLINE databases. In High Availability solutions, the records are also deleted from standby and RGN servers.

  Note:

  To prevent deletion of contacts not yet handled by agents, a customer’s history records can be fully deleted only when all of their contacts are in a closed status. For example, a customer with contacts in new or open status cannot not be deleted.

Generating a customer information file

About this task

If you receive a customer information request, use the Multimedia Data Management utility to generate customer information in an XML file. You can then modify this file if required, before you provide it to the customer.

The Multimedia Data Management utility retrieves the customer information from the MULTIMEDIA and OFFLINE databases.

You can search for customers based on Customer ID or email address.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Data Management**.
2. In the Data Management utility, select **Privacy**.
3. Select **Information Request**.

4. Under **Customer Search**, from the drop-down list, select **ID** or **E-mail**.
5. In the **Equal To** box, type the customer's ID or email address and click **Search**.
6. Select the customer and click **Save As**.
7. Navigate to the folder where you want to save the XML file.
8. In the **File name** box, type a name for the file and click **Save**.
9. After the file saves, click **OK** on the dialog box confirming the file location.

   ✱ **Note:**

   The time it takes to generate the file depends on the size of the customer record.

Next steps

Modify the file if required before providing it to the customer.

Deleting customer history

About this task

If you receive a customer right to be forgotten request, use the Multimedia Data Management utility to delete customer history records from the MULTIMEDIA and OFFLINE databases.

You can search for customers based on Customer ID or email address.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Data Management**.
2. In the Data Management utility, select **Privacy**.
3. Select **Delete Request**.
4. Under **Customer Search**, from the drop-down list, select **ID** or **E-mail**.
5. In the **Equal To** box, type the customer's ID or email address and click **Search**.
6. Select the customer and click **Delete**.
7. Click **Yes** to confirm that you want to delete the customer history record.

Chapter 15: Orchestration Designer example flow applications

This chapter describes how to create three example flow applications using Orchestration Designer (OD) that provide either estimated wait time or position in queue information to customers, or provide customers with the option to leave a voice mail if all agents are busy. These flow applications use Avaya Contact Center Select default sample data; you can use these example flows in your contact center.

This chapter also provides a brief description of how to install and use OD. You can use OD to create and manage flow applications to route contacts to an appropriate queue in the contact center. For more detailed information about Orchestration Designer and using Orchestration Designer in your contact center, see *Using Contact Center Orchestration Designer*.

Installing Orchestration Designer

About this task

Install the Orchestration Designer client to manage Contact Center applications.

Procedure

1. Log on to the Contact Center Manager Administration as an administrator.

   Contact Center Manager Administration (CCMA) displays the date and time of your last login and also the number of failed login attempts before a successful login.

2. From the Launchapd, click **Scripting**.
3. Click **Orchestration Designer** > **Launch Orchestration Designer**.
4. When prompted to download Orchestration Designer, click **OK**.
5. In the File Download - Security Warning message dialog box, click **Run**.
6. In the Installation Welcome window, click **Next**.
7. In the Customer Information window, type a **User Name** and **Organization Name** in the appropriate boxes.
8. Under **Install this application for**, select the option for your installation.
9. Click **Next**.

10. In the Destination Folder window, select the installation folder for Orchestration Designer.
11. Click **Next**.
12. In the Ready to Install the Program window, click **Install**.
13. After the installation is complete, click **Finish**.

Opening Orchestration Designer

About this task

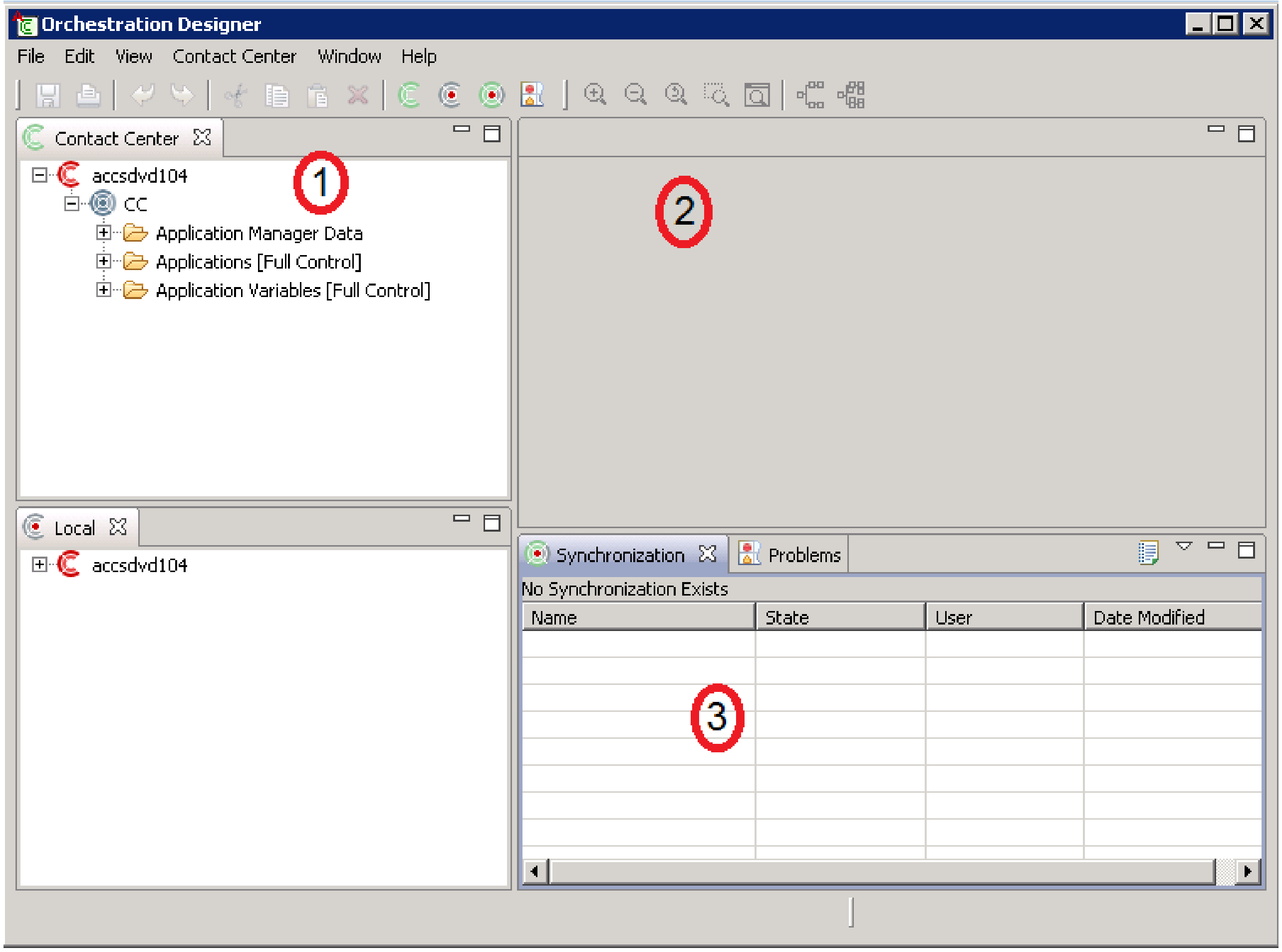
Open Orchestration Designer to configure the routing in your contact center.

Procedure

1. Log on to Contact Center Manager Administration as an administrator.
2. From the Launchpad, click **Scripting**.
3. Click **Orchestration Designer** > **Launch Orchestration Designer**.

Procedure job aid

The following figure shows Orchestration Designer for Contact Center. Each part of the window contains a label that describes what appears in the panel.



No Synchronization Exists

Name	State	User	Date Modified

Figure 8: Orchestration Designer for Contact Center

1	Contact Center view: The Contact Center view of Orchestration Designer shows all applications, application variables, and application management data currently configured in your Contact Center.
2	Application editor view: The Application editor is the main tool to create or modify the default applications. It provides the canvas on which to place the blocks.
3	Synchronization view: The Synchronization view shows the difference between the objects in the Local view and the Contact Center view for the Contact Center Manager Server.

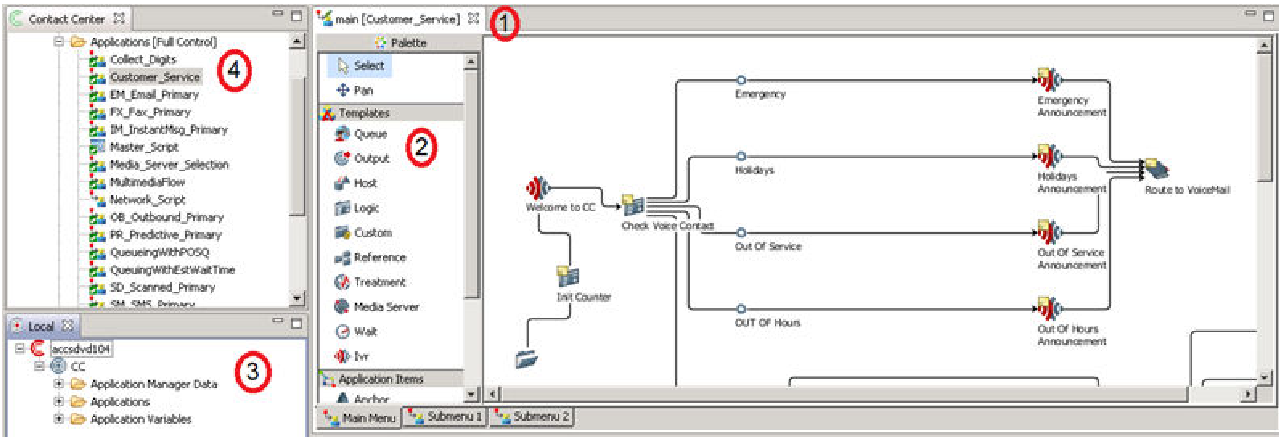


Figure 9: Orchestration Designer tabs

1	View tabs: The tabs located across the top of the Application editor represent main pages and block editors for the flow applications on which you work.
2	Palette bar: The icons represent blocks that you can use to build your Contact Center applications. The blocks you see depend on the switch you use in your Contact Center.
3	Local view: The Local view provides a user work space on a desktop to work with copies of the variables and applications.
4	Application Manager Data folder contains a list of all the agents, skillsets, CDNs, and DNISs. Applications folder contains a list of all the applications in the system. Applications are used to control how contacts are routed through the Contact Center and the treatment each contact receives. Applications Variables contains a list of all the variables in the system. Variables are used to change the nature of a flow at run time without changing the application.

You can also start Orchestration Designer from the **Apps** screen.

If you start Orchestration Designer from the **Apps** screen, you can create and work with applications and variable data in a local version of Orchestration Designer without affecting the working contact center.

The local version of Orchestration Designer allows you to perform the following tasks:

- Access all information without restrictions by access classes.
- Perform updates without affecting your Contact Center applications.
- Create applications using Orchestration Designer before the rest of the Contact Center software is installed.

By default, the Local and Problems views appear in your Orchestration Designer window. The top right corner is reserved for the script or flow application editor.

If you start Orchestration Designer from the Contact Center Manager Administration application, there are no partition restrictions. You log on to Contact Center Manager Administration as an administrator and work with blocks and variables in Orchestration Designer as an administrator.

Only one instance of Orchestration Designer can run at a time.

View name	Description
Contact Center view	The Contact Center view shows all of the applications, variables, and application management data that are currently inactive or active in your Contact Center. You can make minor changes to applications in the Contact Center view. However, Avaya recommends that you work on a copy of the application in the Local view to make significant changes.
Local view	The Local view shows all of the applications, variables, application management data, and intrinsics saved on the local machine. You need not be connected to a Contact Center Manager Administration or to the network to work with this data. You can upload applications to the Contact Center view after you finish your modifications.
Synchronization view	The Synchronization view shows the differences between all objects stored on the Contact Center Manager Server (Contact Center view) and the objects stored on the Local client (Local view) after you use the Synchronization command.
Problems view	The Problems view shows the errors in the current application. You can use the problems view to determine where the problem is, and determine the reason for the problem.

Configuring a flow application to provide estimated wait time information

About this task

Create a new graphical flow application in Orchestration Designer that provides an estimated wait time to customers if a particular skillset is busy or out of service. This example uses Avaya Contact Center Select default sample data such as:

- The *SimpleQueueing* application template as a starting point.
- The *Skill1* skillset.
- The *Sample_Music* Route, number 511. This corresponds to the default Sample_Music content group in CCMA Prompt Management, which includes two sample music files.

This example flow application uses custom media files, uploaded to the en_us content group using CCMA Prompt Management:

Prompt name	Prompt transcript	Sample flow application using this prompt
holdtime	“The estimated hold time is currently”	QueuingWithEstWaitTime
seconds	“seconds”	QueuingWithEstWaitTime

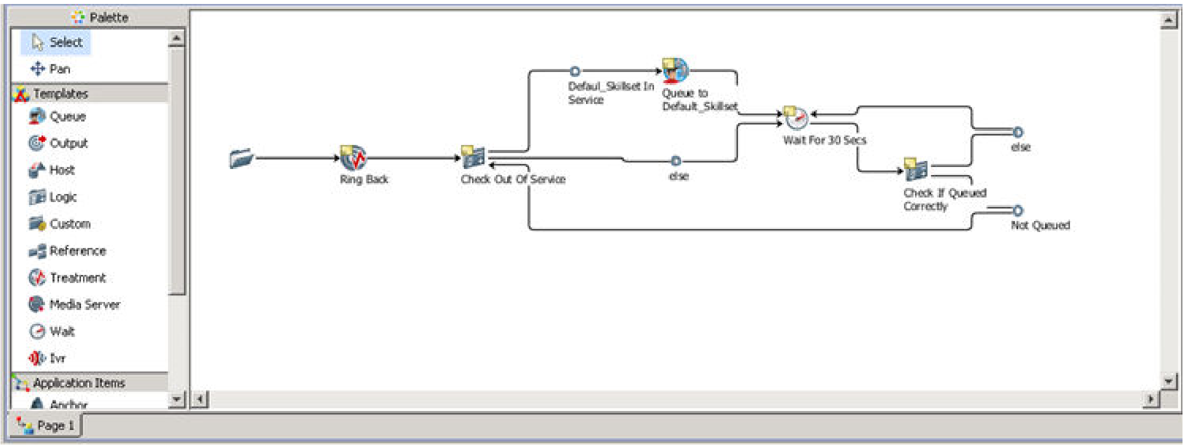
Table continues…

Prompt name	Prompt transcript	Sample flow application using this prompt
Note: These prompts are not available in Avaya Contact Center Select by default. You must supply these custom media files. Upload custom media files using CCMA Prompt Management. You must upload the .WAV files encoded as Linear 16-bit PCM, 8KHz Mono with a sampling rate of 128kbits/sec. For more information about how to upload media files using Prompt Management, see *Administering Avaya Contact Center Select*.		

Procedure

1. Launch Orchestration Designer.
2. In the **Contact Center** pane, expand the CCMA name. The CCMA name matches the host name of the Avaya Contact Center Select server.
3. Expand **CC**.
4. Right-click **Applications [Full Control]**, and select **New** > **Application**.
5. In the **New Contact Center Application** dialog box, select **Create in Contact Center**.
6. In the **Application Name** box, type the name of your new flow application. For this example, the name is QueuingWithEstWaitTime.
7. For **Application Type**, select **Graphical Flow**.
8. From the **Application Template** list, select **SimpleQueuing**.
9. Click **Finish**.

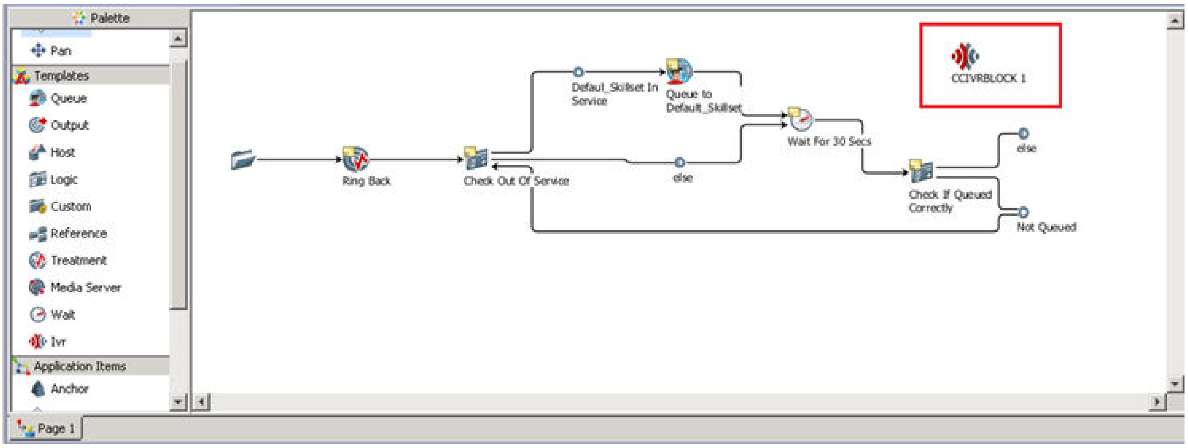
   The Flow Editor opens the new flow based on the SimpleQueuing template.



10. Select the **else** condition icon that appears to the right of the **Wait For 30 Secs** block icon.
11. Right-click on the **Wait For 30 Secs** block icon and select **(Dis)Connect**.
12. From the palette bar, select the **IVR** block icon.

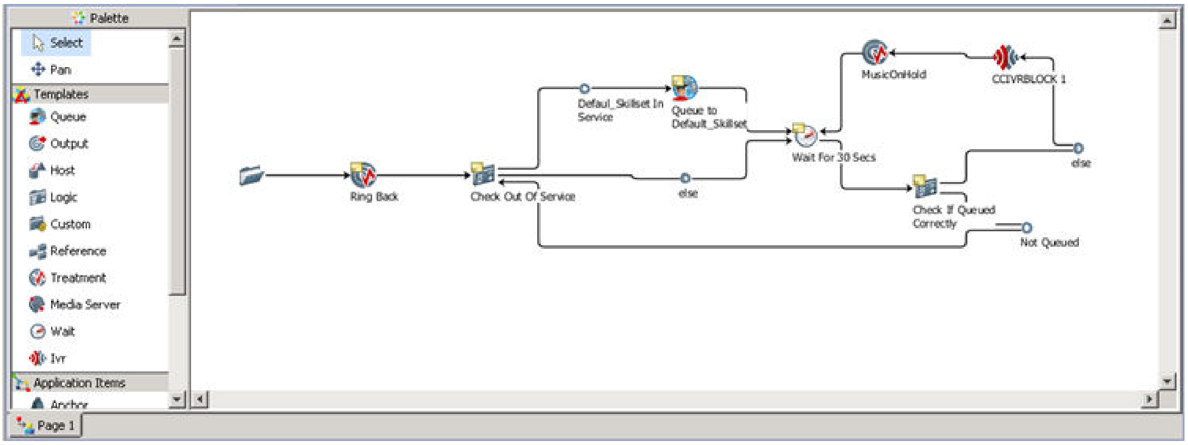
13. Click the **main [QueuingWithEstWaitTime]** panel.

    The CCIVRBLOCK icon appears in the Main Flow Editor. Reposition the icon if needed.
14. Select the **else** condition icon that appears to the right of the **Wait For 30 Secs** block icon.
15. Right-click on the **CCIVRBLOCK** icon and select **(Dis)Connect**.

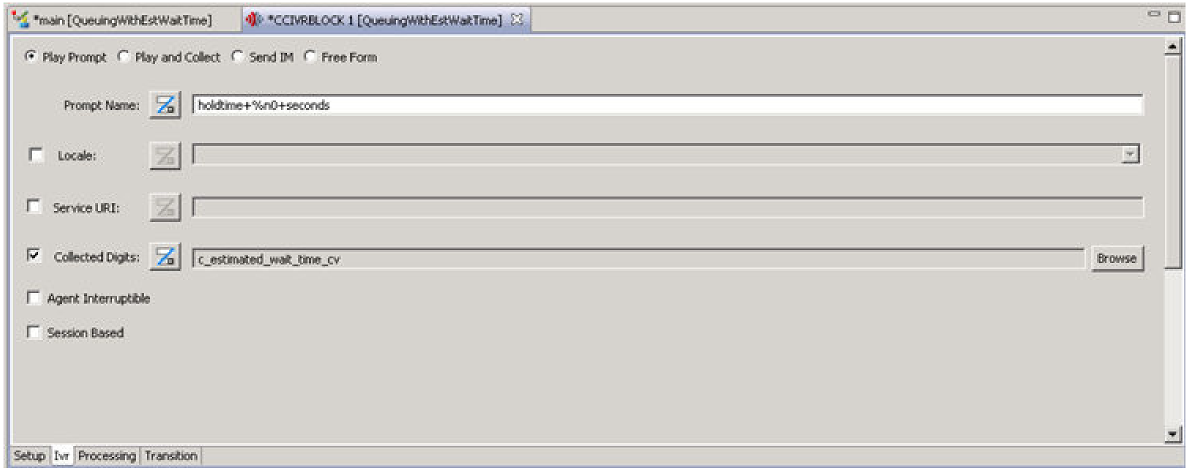


16. From the palette bar, select the **Treatment** block icon.
17. Click the **main [QueuingWithEstWaitTime]** panel.

    The CCTREATMENTBLOCK icon appears in the Main Flow Editor. Reposition the icon if needed.
18. Right-click on the **CCTREATMENTBLOCK** icon and select **Rename**.
19. In the **Name** box, type `MusicOnHold` and click **OK**.
20. Select the **CCIVRBLOCK** icon.
21. Right-click on the **MusicOnHold** icon and select **(Dis)Connect**.
22. Select the **MusicOnHold** icon.
23. Right-click on the **Wait for 30 Secs** icon and select **(Dis)Connect**.



24. Double-click the **CCIVRBLOCK** icon.
25. In the **Prompt Name** box, type `<MediaFileName1>+%n0+<MediaFileName2>`. For example, type holdtime+%n0+seconds.
26. Select the **Collected Digits** check box and click **Browse**.
27. In the **Chooser** dialog box, expand **Application Variables** > **INTEGER**.
28. Select **c_estimated_wait_time_cv** and click **OK**.


*main [QueuingWithEstWaitTime]
*CCIVRBLOCK 1 [QueuingWithEstWaitTime]
Browse
Setup
Ivr
Processing
Transition

● Play Prompt ○ Play and Collect ○ Send IM ○ Free Form

Prompt Name: holdtime+%n0+seconds

□ Locale:

□ Service URI:

☑ Collected Digits: c_estimated_wait_time_cv

□ Agent Interruptible

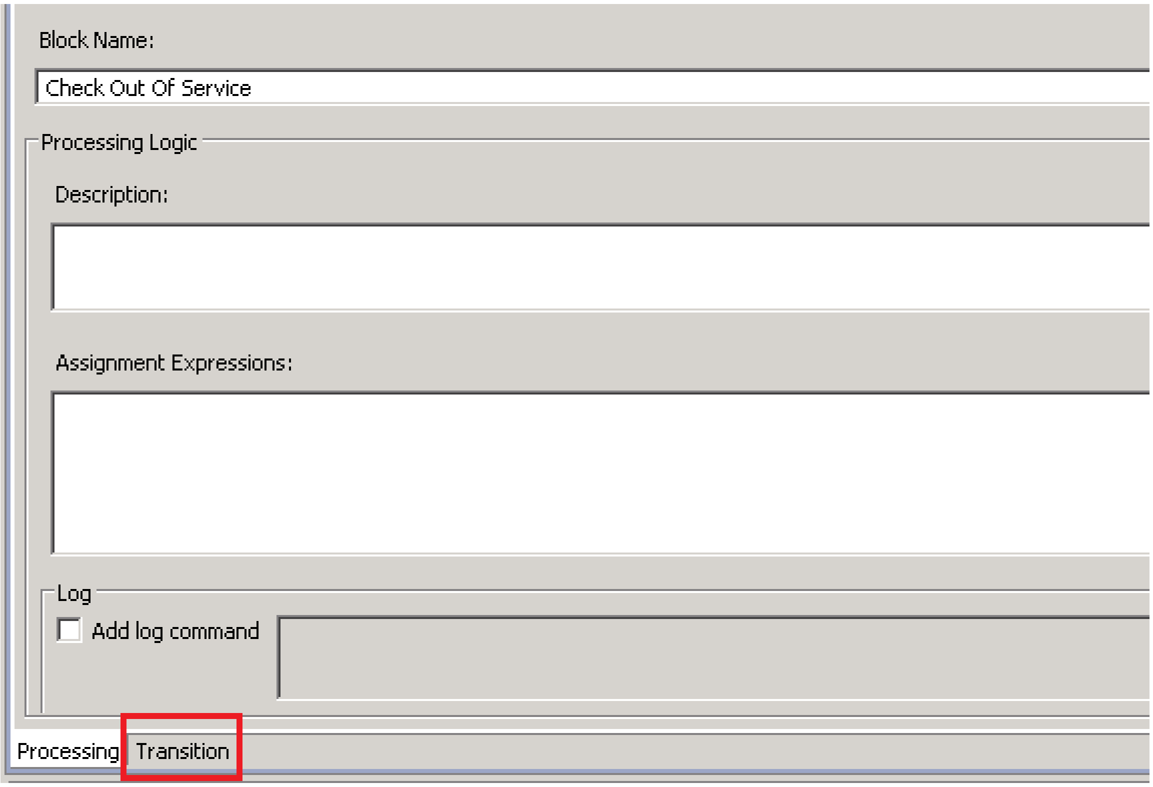
□ Session Based

29. Close the **CCIVRBLOCK** tab.
30. Double-click the **MusicOnHold** treatment icon.
31. Under **Treatment Options**, select **Music**.
32. In the **Music Route** box, type 511.

    Note:

    This number corresponds to the Avaya Contact Center Select default Sample_Music route configured in CCMA.

33. Close the **MusicOnHold** tab.
34. Optionally, double-click the **Wait for 30 Secs** wait block.
    a. Under **Block Name**, type a new name for the wait block. For example, type `Wait for 10 Secs`.
    b. In the **Duration (secs)** box, type `10`.
    c. Close the **Wait for 30 Secs** tab.
35. Double-click the **Check Out Of Service** icon.
36. Click the **Transition** tab.

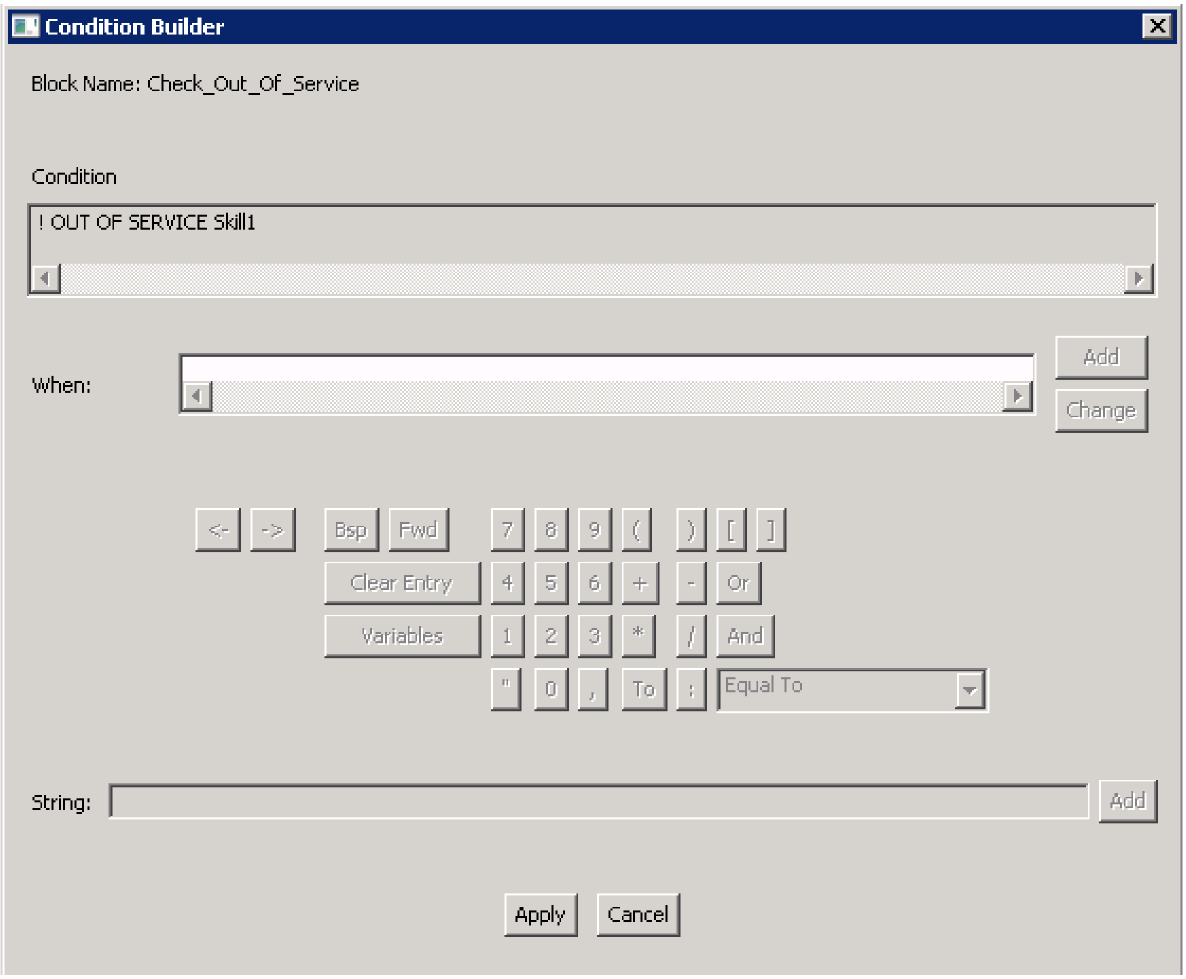


Block Name:

Check Out Of Service

37. Click the **Default_Skillset In Service** tab.
38. Under **Conditional Expression**, click **Edit**.
39. Under **Condition**, select **! OUT OF SERVICE Default_Skillset**.

    ! OUT OF SERVICE Default_Skillset appears in the **When** box.
40. Click **Clear Entry**.
41. From the **Not** drop-down list, select **Not**. Ensure “!” appears in the **When** box after you select **Not**.
42. Click **Variables**.
43. On the **Chooser** dialog, expand **Intrinsics** > **Skillset**.
44. Select **OUT OF SERVICE** and click **OK**.
45. Click **Variables**.
46. On the **Chooser** dialog, expand **Application Manager Data** > **Skillsets** > **Local**.
47. From the list of skillsets, select a voice skillset. For example, select Skill1.
48. Click **OK**.
49. Click **Change**.



Condition Builder

Block Name: Check_Out_Of_Service

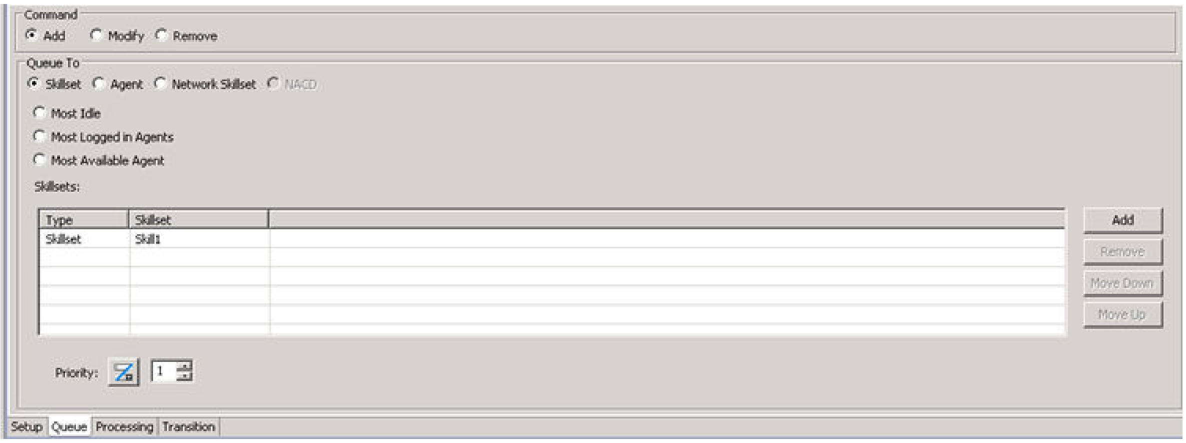
Condition

! OUT OF SERVICE Skill1

When:

String:

50. Click **Apply**.
51. Close the **Check Out Of Service** tab.
52. Double-click the **Queue to Default_Skillset** icon.
53. Under **Skillsets**, click **Add**.
54. Expand **Application Manager Data** > **Local Skillsets**.
55. From the list of skillsets, select a voice skillset. For example, select Skill1.
56. Click **OK**.
57. To remove a skillset from the list, for example Default_Skillset, select the skillset and click **Remove**.



Command: ● Add

Queue To: ● Skillset

Skillsets:

Type	Skillset
Skillset	Skill1

Priority: 1

58. Close the **Queue to Default_Skillset** tab.
59. Right-click the **Queue to Default_Skillset** icon and click **Rename**.
60. In the **Name** box, type `Queue to Skill1` and click **OK**.
61. Close the **QueuingWithEstWaitTime** flow application.
62. On the **Save Resource** box, click **Yes** to save the application.
63. On the **Confirm** box, click **OK** to activate the application.
64. In the **Contact Center** view, double-click on **Master_Script**.
65. Under **Configured Routes** in the right pane, expand **CDN**.
66. Select **SampleCDN** and click **Edit**.
67. In the Application Chooser, under Valid Applications, select the **QueuingWithEstWaitTime** flow application.
68. Click **OK**.

    Calls to the SampleCDN (Route Point) are routed to the QueuingWithEstWaitTime flow application for treatment and queueing to the appropriate agent skillset queue (for example, the Skill1 skillset). If the skillset is busy or out of service for any reason, customers that call the sample Route Point hear a recording that provides an estimate wait time for their call to be answered by an agent.
69. Close **Contact_Router**.
70. On the **Save Resource** box, click **Yes**.
71. On the **Confirm** box, click **OK** to activate the Master_Script.

Configuring a flow application to provide position in queue information

About this task

Create a new graphical flow application in Orchestration Designer that provides position in queue information to customers if a particular skillset is busy or out of service. This example uses Avaya Contact Center Select default sample data such as:

- The *SimpleQueueing* application template as a starting point.
- The *Skill1* skillset.
- The *Sample_Music* Route, number 511. This corresponds to the default Sample_Music content group in CCMA Prompt Management, which includes two sample music files.

This example flow application uses custom media files, uploaded to the en_us content group using CCMA Prompt Management:

Prompt name	Prompt transcript	Sample flow application using this prompt
PosInQueue	"Thank you for holding. You are currently number"	QueuingWithPOSQ
InQueue	"in the queue. Please wait for the next available agent"	QueuingWithPOSQ

Note:

These prompts are not available in Avaya Contact Center Select by default. You must supply these custom media files.

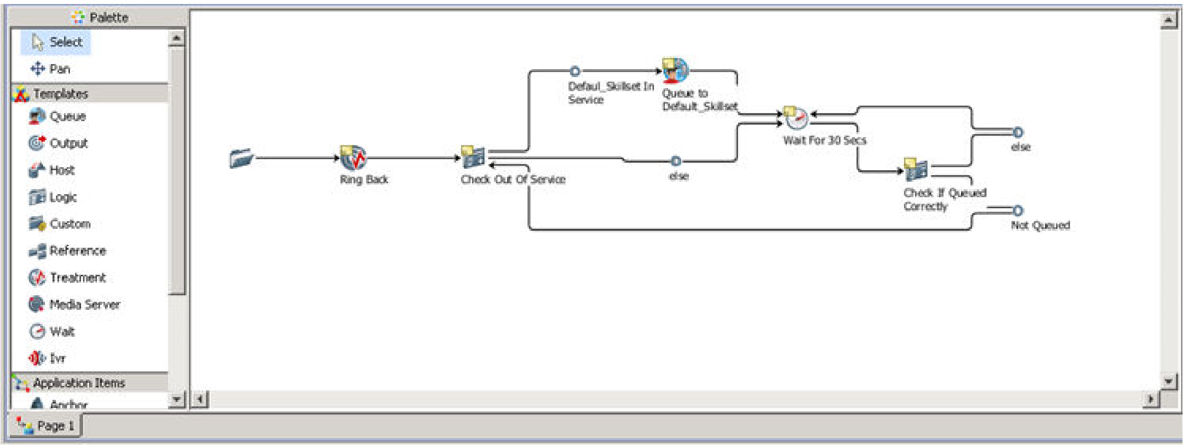
Upload custom media files using CCMA Prompt Management. You must upload the .WAV files encoded as Linear 16-bit PCM, 8KHz Mono with a sampling rate of 128kbits/sec. For more information about how to upload media files using Prompt Management, see *Administering Avaya Contact Center Select*.

Procedure

1. Launch Orchestration Designer.
2. In the **Contact Center** pane, expand the CCMA name. The CCMA name matches the host name of the Avaya Contact Center Select server.
3. Expand **CC**.
4. Right-click **Applications [Full Control]**, and select **New** > **Application**.
5. In the **New Contact Center Application** dialog box, select **Create in Contact Center**.
6. In the **Application Name** box, type the name of your new flow application. For this example, the name is QueuingWithPOSQ.
7. For **Application Type**, select **Graphical Flow**.
8. From the **Application Template** list, select **SimpleQueuing**.

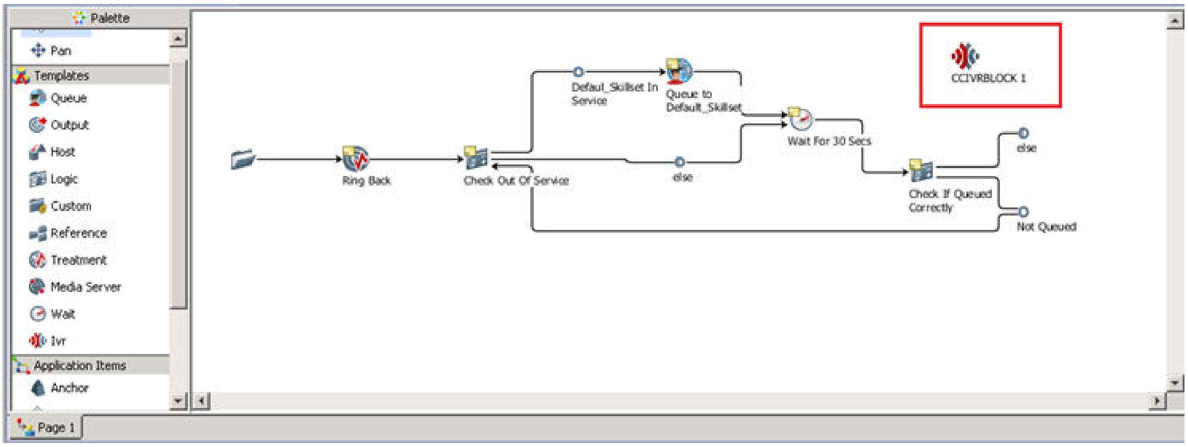
9. Click **Finish**.

   The Flow Editor opens the new flow based on the SimpleQueuing template.



10. Select the **else** condition icon that appears to the right of the **Wait For 30 Secs** block icon.
11. Right-click on the **Wait For 30 Secs** block icon and select **(Dis)Connect**.
12. From the palette bar, select the **IVR** block icon.
13. Click the **main [QueuingWithPOSQ]** panel.

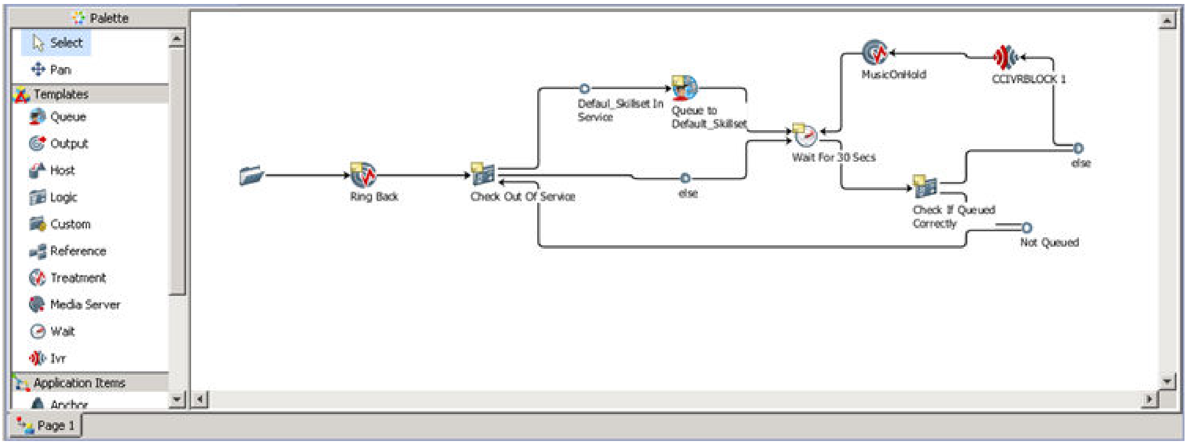
    The CCIVRBLOCK icon appears in the Main Flow Editor. Reposition the icon if needed.
14. Select the **else** condition icon that appears to the right of the **Wait For 30 Secs** block icon.
15. Right-click on the **CCIVRBLOCK** icon and select **(Dis)Connect**.



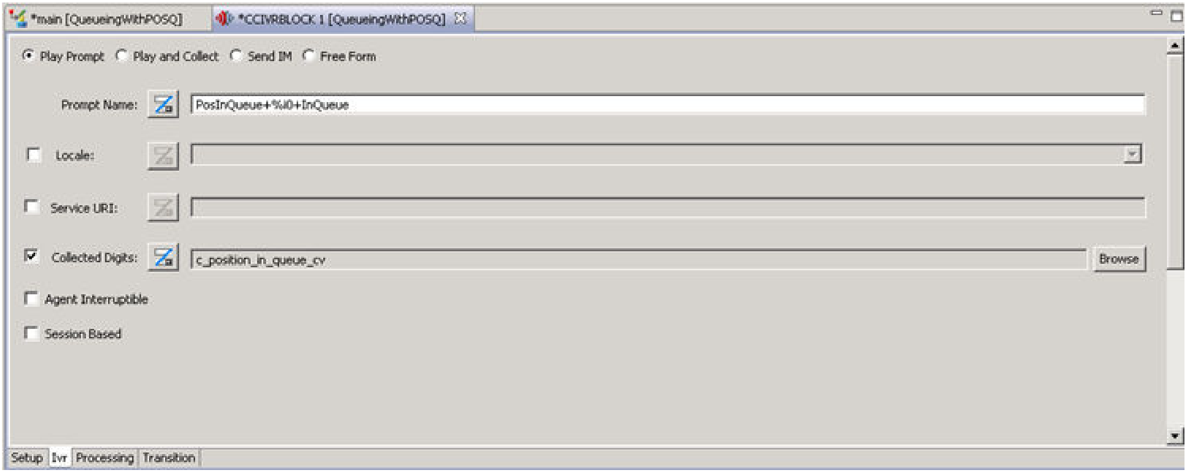
16. From the palette bar, select the **Treatment** block icon.
17. Click the **main [QueuingWithPOSQ]** panel.

    The CCTREATMENTBLOCK icon appears in the Main Flow Editor. Reposition the icon if needed.
18. Right-click on the **CCTREATMENTBLOCK** icon and select **Rename**.

19. In the **Name** box, type `MusicOnHold` and click **OK**.
20. Select the **CCIVRBLOCK** icon.
21. Right-click on the **MusicOnHold** icon and select **(Dis)Connect**.
22. Select the **MusicOnHold** icon.
23. Right-click on the **Wait for 30 Secs** icon and select **(Dis)Connect**.



24. Double-click the **CCIVRBLOCK** icon.
25. In the **Prompt Name** box, type `<MediaFileName1>+%i0+<MediaFileName2>`. For example, type PosInQueue+%i0+InQueue.
26. Select the **Collected Digits** check box and click **Browse**.
27. In the **Chooser** dialog box, expand **Application Variables** > **INTEGER**.
28. Select **c_position_in_queue_cv** and click **OK**.



● Play Prompt ○ Play and Collect ○ Send IM ○ Free Form

Prompt Name: PosInQueue+%i0+InQueue

□ Locale:

□ Service URI:

☑ Collected Digits: c_position_in_queue_cv

□ Agent Interruptible

□ Session Based

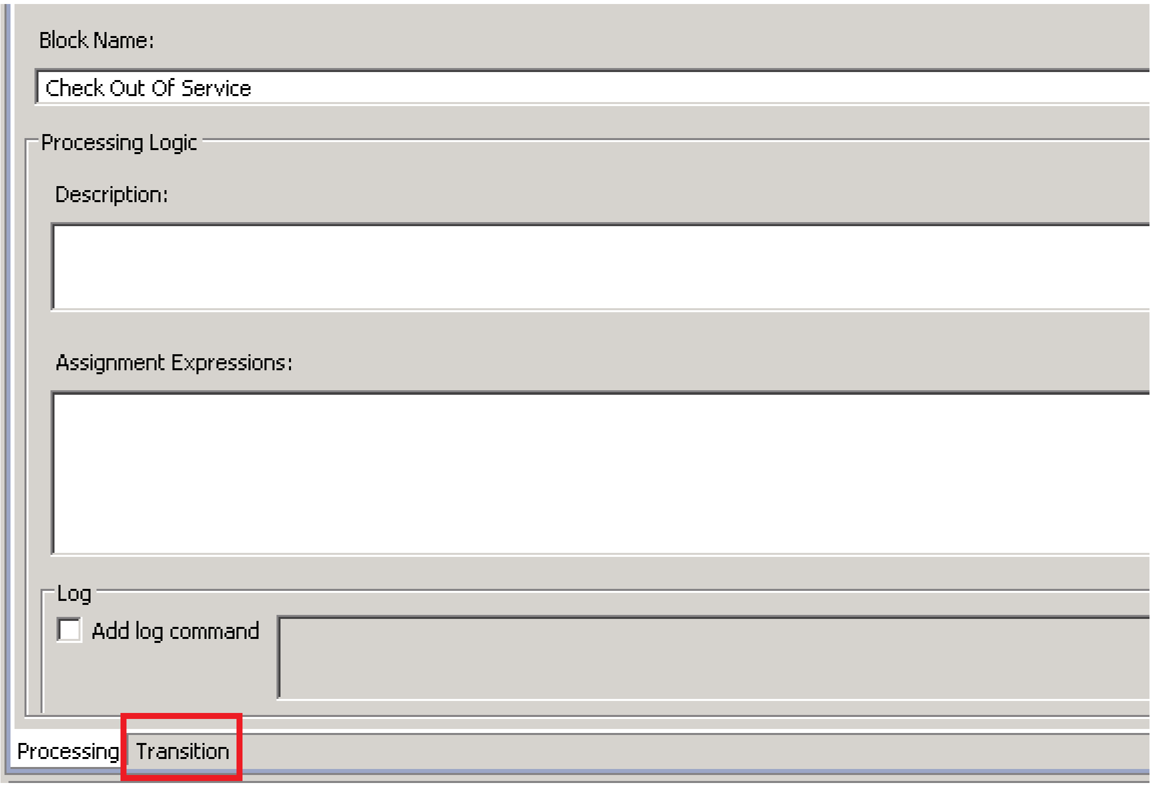
29. Close the **CCIVRBLOCK** tab.
30. Double-click the **MusicOnHold** treatment icon.
31. Under **Treatment Options**, select **Music**.

32. In the **Music Route** box, type 511.

    Note:

    This number corresponds to the Avaya Contact Center Select default Sample_Music route configured in CCMA.

33. Close the **MusicOnHold** tab.
34. Optionally, double-click the **Wait for 30 Secs** wait block.
    a. Under **Block Name**, type a new name for the wait block. For example, type `Wait for 10 Secs`.
    b. In the **Duration (secs)** box, type `10`.
    c. Close the **Wait for 30 Secs** tab.
35. Double-click the **Check Out Of Service** icon.
36. Click the **Transition** tab.



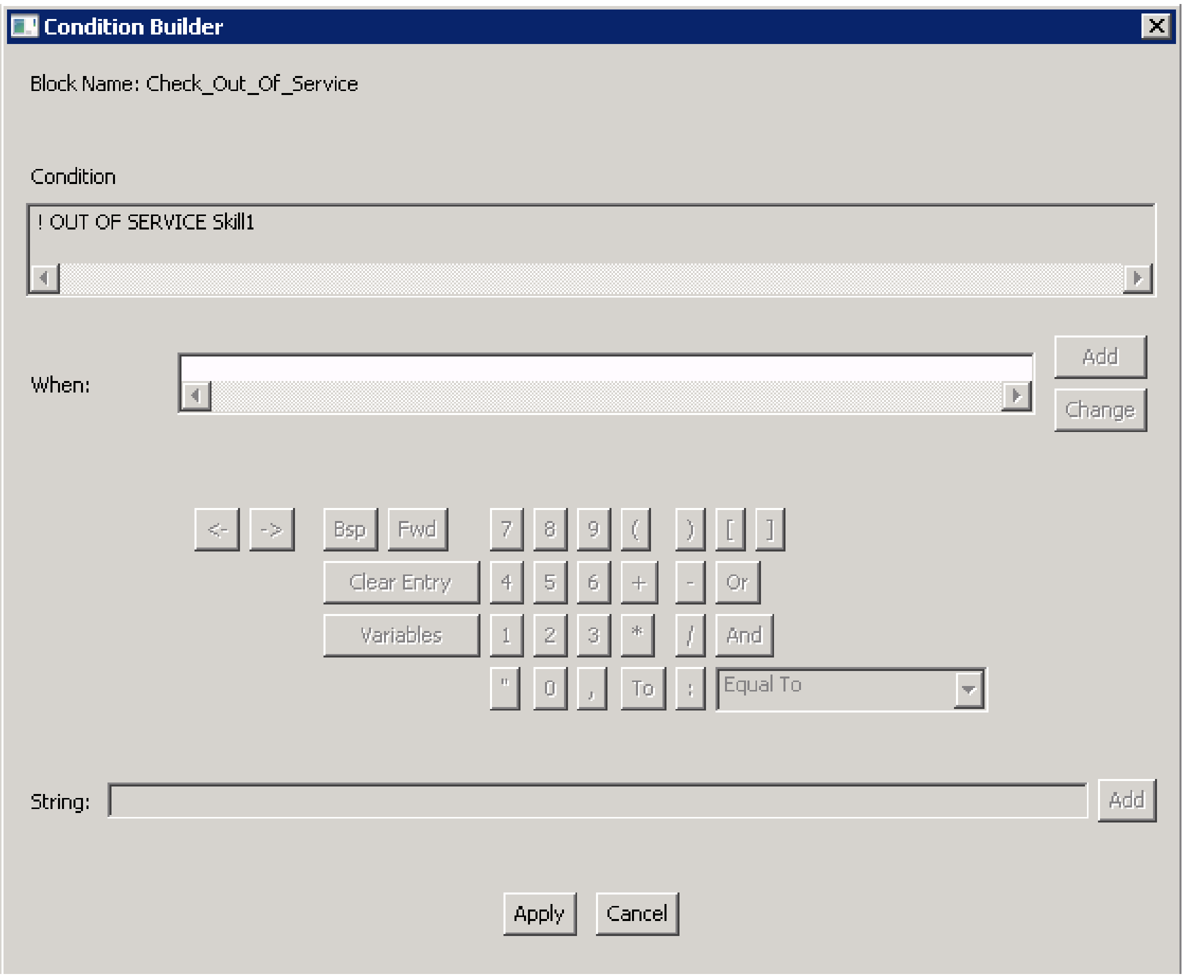
Block Name:

Check Out Of Service

37. Click the **Default_Skillset In Service** tab.
38. Under **Conditional Expression**, click **Edit**.
39. Under **Condition**, select **! OUT OF SERVICE Default_Skillset**.

    ! OUT OF SERVICE Default_Skillset appears in the **When** box.
40. Click **Clear Entry**.

41. From the **Not** drop-down list, select **Not**. Ensure “!” appears in the **When** box after you select **Not**.
42. Click **Variables**.
43. On the **Chooser** dialog, expand **Intrinsics** > **Skillset**.
44. Select **OUT OF SERVICE** and click **OK**.
45. Click **Variables**.
46. On the **Chooser** dialog, expand **Application Manager Data** > **Skillsets** > **Local**.
47. From the list of skillsets, select a voice skillset. For example, select Skill1.
48. Click **OK**.
49. Click **Change**.



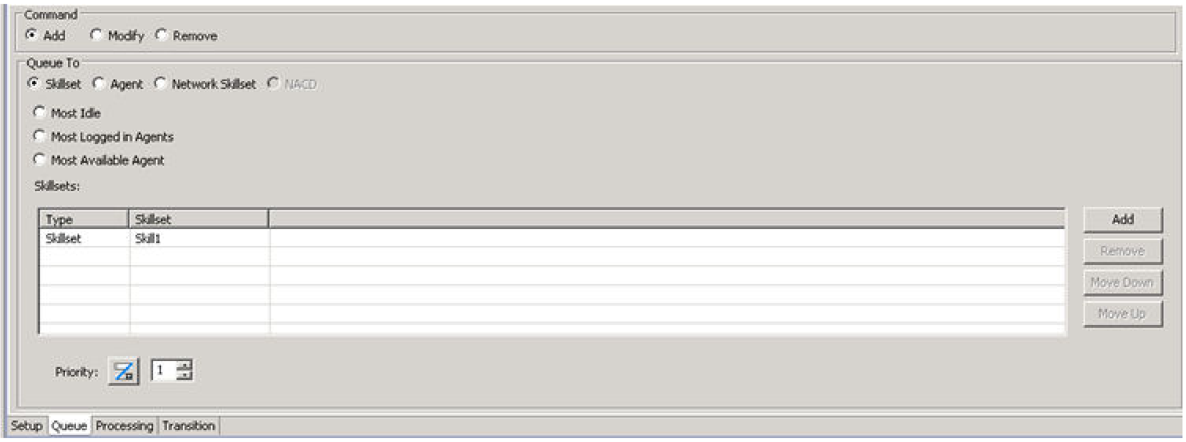
Block Name: Check_Out_Of_Service

Condition

! OUT OF SERVICE Skill1

50. Click **Apply**.
51. Close the **Check Out Of Service** tab.
52. Double-click the **Queue to Default_Skillset** icon.

53. Under **Skillsets**, click **Add**.
54. Expand **Application Manager Data** > **Local Skillsets**.
55. From the list of skillsets, select a voice skillset. For example, select Skill1.
56. Click **OK**.
57. To remove a skillset from the list, for example Default_Skillset, select the skillset and click **Remove**.



Command
● Add ○ Modify ○ Remove

Queue To
● Skillset ○ Agent ○ Network Skillset ○ NACD

○ Most Idle
○ Most Logged in Agents
○ Most Available Agent

Skillsets:

Type	Skillset
Skillset	Skill1

Priority: 1

58. Close the **Queue to Default_Skillset** tab.
59. Right-click the **Queue to Default_Skillset** icon and click **Rename**.
60. In the **Name** box, type `Queue to Skill1` and click **OK**.
61. Close the **QueuingWithPOSQ** flow application.
62. On the **Save Resource** box, click **Yes** to save the application.
63. On the **Confirm** box, click **OK** to activate the application.
64. In the **Contact Center** view, double-click on **Master_Script**.
65. Under **Configured Routes** in the right pane, expand **CDN**.
66. Select **SampleCDN** and click **Edit**.
67. In the Application Chooser, under Valid Applications, select the **QueuingWithPOSQ** flow application.
68. Click **OK**.

    Calls to the SampleCDN (Route Point) are routed to the QueuingWithPOSQ flow application for treatment and queueing to the appropriate agent skillset queue (for example, the Skill1 skillset). If the skillset is busy or out of service for any reason, customers that call the sample Route Point hear a recording that provides position in queue information.
69. Close **Contact_Router**.
70. On the **Save Resource** box, click **Yes**.

71. On the **Confirm** box, click **OK** to activate the Master_Script.

Configuring a flow application to provide a queuing customer with the option to leave a voice mail

About this task

Create a new graphical flow application in Orchestration Designer that allows a customer to leave a voice mail if all agents are busy. This example uses Avaya Contact Center Select default sample data such as:

- The *SimpleQueueing* application template as a starting point.
- The *Skill1* skillset.
- The *InvalidEntry_CS* script variable. This variable corresponds to the InvalidEntry_CS prompt that informs customers that they have inputted an invalid entry.
- The *Voicemail_gv* script variable. This variable corresponds to a Voicemail Pro DN number. The default value of Voicemail_gv is the value entered in the Ignition Wizard configuration utility at install time. You can change the DN number for the Voicemail_gv script variable using the Scripting component in CCMA.

This example flow application uses a custom media file, uploaded to the en_us content group using CCMA Prompt Management:

Prompt name	Prompt transcript	Sample flow application using this prompt
VoiceMailOption	“We are sorry for this delay. If you wish, press 1 now to be routed to our voice mail system to leave a message for one of our experts, or press 2 to remain queuing.”	LeaveVoiceMail

Note:

This prompt is not available in Avaya Contact Center Select by default. You must supply this custom media file.

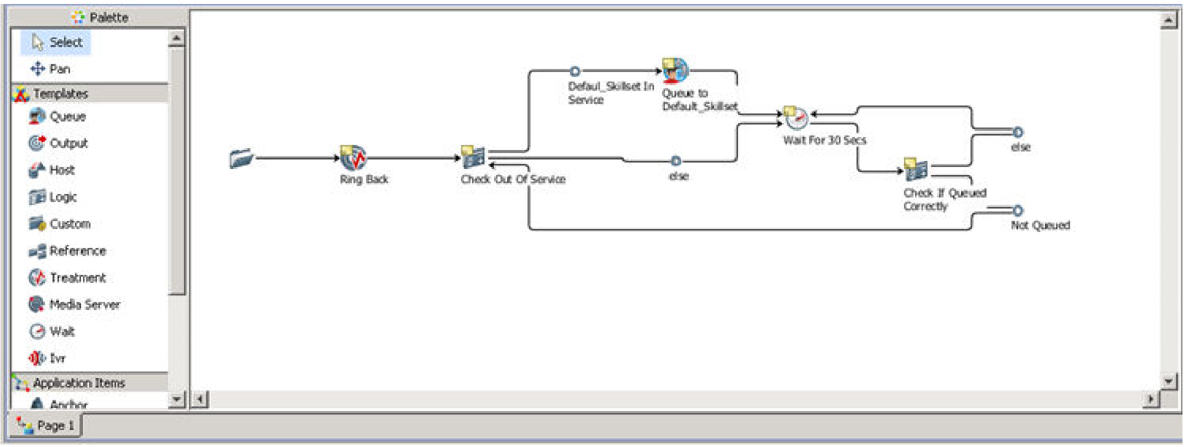
Upload custom media files using CCMA Prompt Management. You must upload the .WAV files encoded as Linear 16-bit PCM, 8KHz Mono with a sampling rate of 128kbits/sec. For more information about how to upload media files using Prompt Management, see *Administering Avaya Contact Center Select*.

Procedure

1. Launch Orchestration Designer.
2. In the **Contact Center** pane, expand the CCMA name. The CCMA name matches the host name of the Avaya Contact Center Select server.
3. Expand **CC**.

4. Right-click **Applications [Full Control]**, and select **New** > **Application**.
5. In the **New Contact Center Application** dialog box, select **Create in Contact Center**.
6. In the **Application Name** box, type the name of your new flow application. For this example, the name is LeaveVoiceMail.
7. For **Application Type**, select **Graphical Flow**.
8. From the **Application Template** list, select **SimpleQueuing**.
9. Click **Finish**.

   The Flow Editor opens the new flow based on the SimpleQueuing template.

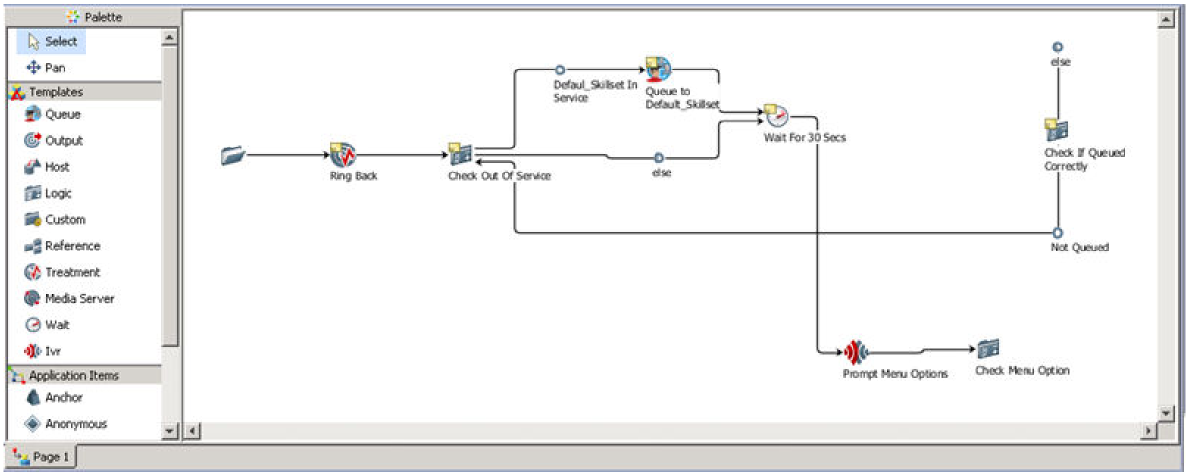
   

10. Select the **else** condition icon that appears to the right of the **Wait For 30 Secs** block icon.
11. Right-click on the **Wait For 30 Secs** block icon and select **(Dis)Connect**.
12. Select the **Wait For 30 Secs** block icon.
13. Right-click on the **Check If Queued Correctly** block icon and select **(Dis)Connect**.
14. From the palette bar, select the **IVR** block icon.
15. Click the **main [LeaveVoiceMail]** panel.

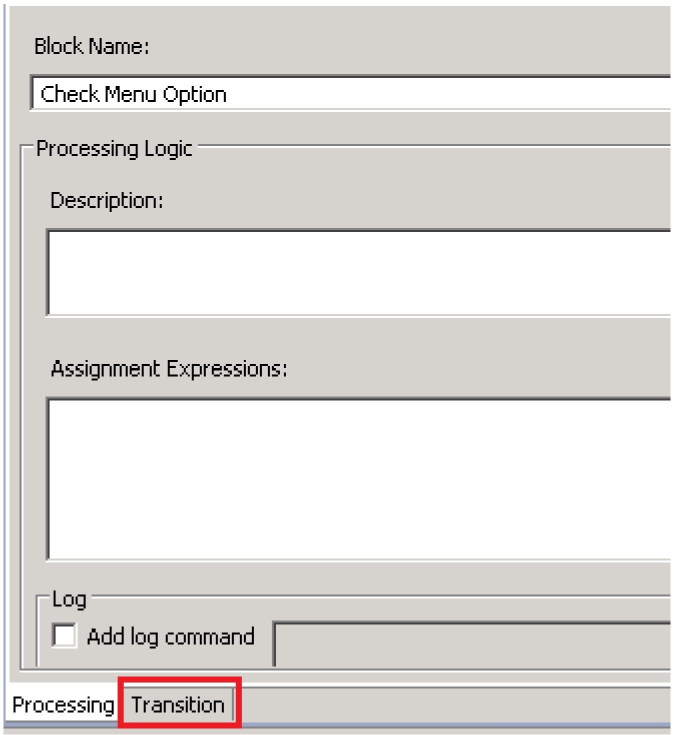
    The CCIVRBLOCK icon appears in the Main Flow Editor. Reposition the icon if needed.
16. Right-click on the **CCIVRBLOCK** icon and select **Rename**.
17. In the **Name** box, type `Prompt Menu Options` and click **OK**.
18. Select the **Wait For 30 Secs** block icon.
19. Right-click on the **Prompt Menu Options** icon and select **(Dis)Connect**.
20. From the palette bar, select the **Logic** block icon.
21. Click the **main [LeaveVoiceMail]** panel.

    The CCLOGICBLOCK icon appears in the Main Flow Editor. Reposition the icon if needed.
22. Right-click on the **CCLOGICBLOCK** icon and select **Rename**.

23. In the **Name** box, type `Check Menu Option` and click **OK**.
24. Select the **Prompt Menu Options** block icon.
25. Right-click on the **Check Menu Option** icon and select **(Dis)Connect**.



26. Double-click on the **Check Menu Option** icon.
    a. Click the **Transition** tab.



Block Name:

Check Menu Option

Processing Logic

Description:

Assignment Expressions:

Log

□ Add log command

Processing | Transition

    b. Click **Add Transition**.
    c. Select the **tran** tab.

d. In the **Description** box, type a description. For example, type “`If the customer enters 1, route the contact to IP Office Voice Mail. Otherwise the contact remains queuing.`”

e. Under **Conditional Expression**, click **Edit**.

f. In the **Condition Builder**, click **Variables**.

g. In the **Chooser** box, expand **Application Variables** > **STRING**.

h. Select **im_str** and click **OK**.

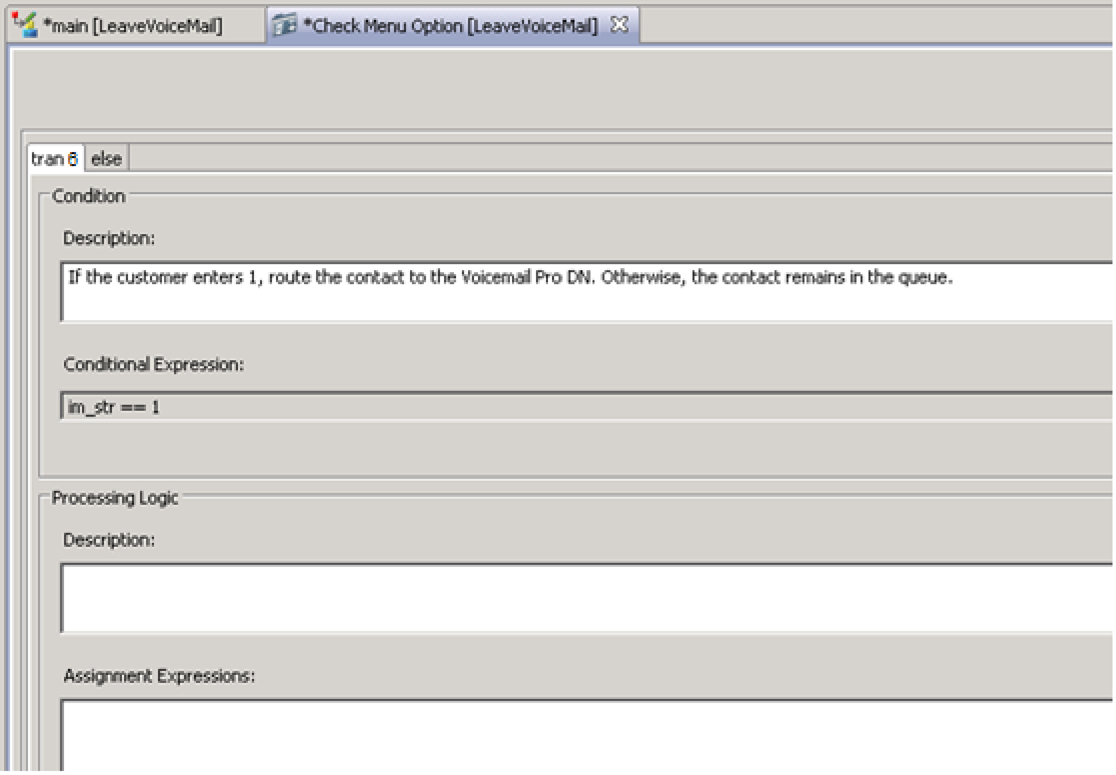
i. From the drop-down list, select **Equal To**.

   Ensure that “im_str ==” appears in the **When** box you select **Equal To**.

j. In the **String** box, type `1` and click **Add**.

k. To the right of the **When** box, click **Add**.

l. Click **Apply**.



Description:

If the customer enters 1, route the contact to the Voicemail Pro DN. Otherwise, the contact remains in the queue.

Conditional Expression:

im_str == 1

Description:

m. Click **Add Transition**.

n. Select the newly created **tran** tab.

o. In the **Description** box, type a description. For example, type “`If the customer enters 2, continue queuing.`”

p. Under **Conditional Expression**, click **Edit**.

q. In the **Condition Builder**, click **Variables**.

r. In the **Chooser** box, expand **Application Variables** > **STRING**.

s. Select **im_str** and click **OK**.

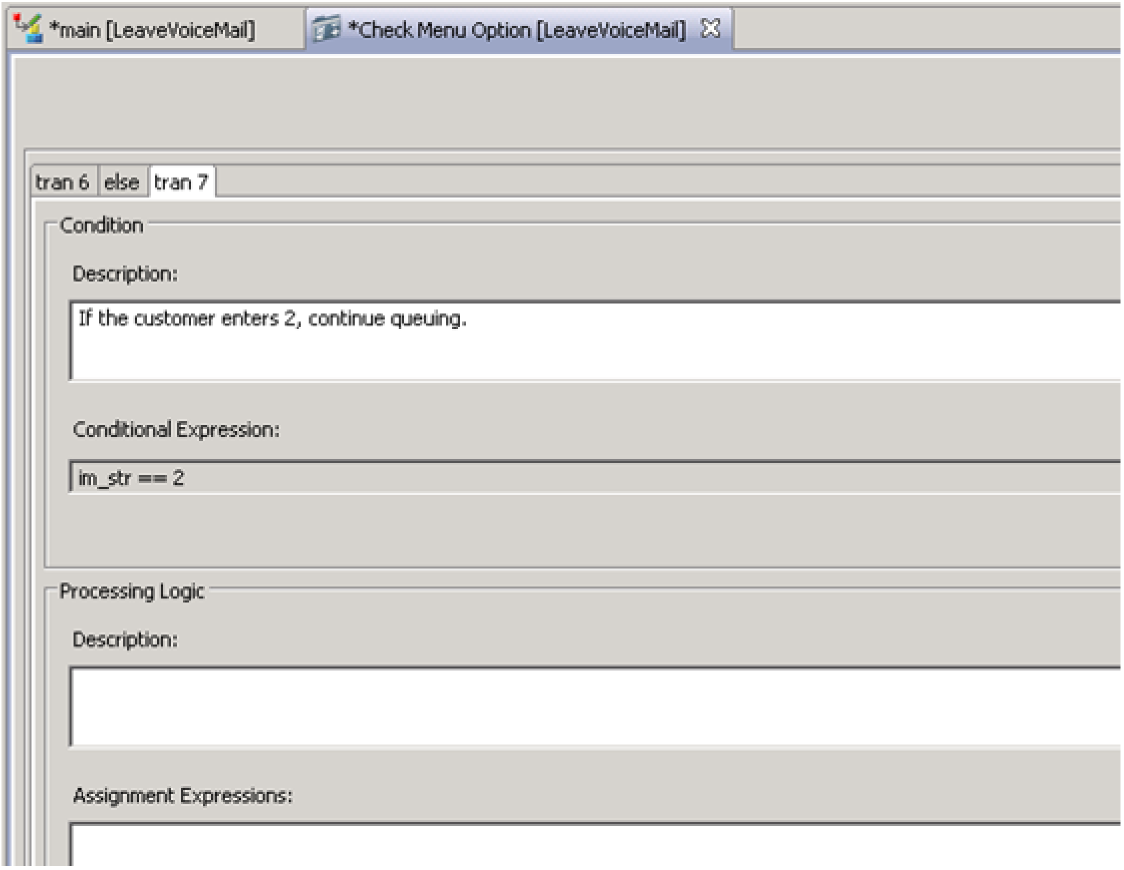
t. From the drop-down list, select **Equal To**.

   Ensure that “im_str ==” appears in the **When** box you select **Equal To**.

u. In the **String** box, type `2` and click **Add**.

v. To the right of the **When** box, click **Add**.

w. Click **Apply**.



If the customer enters 2, continue queuing.

im_str == 2

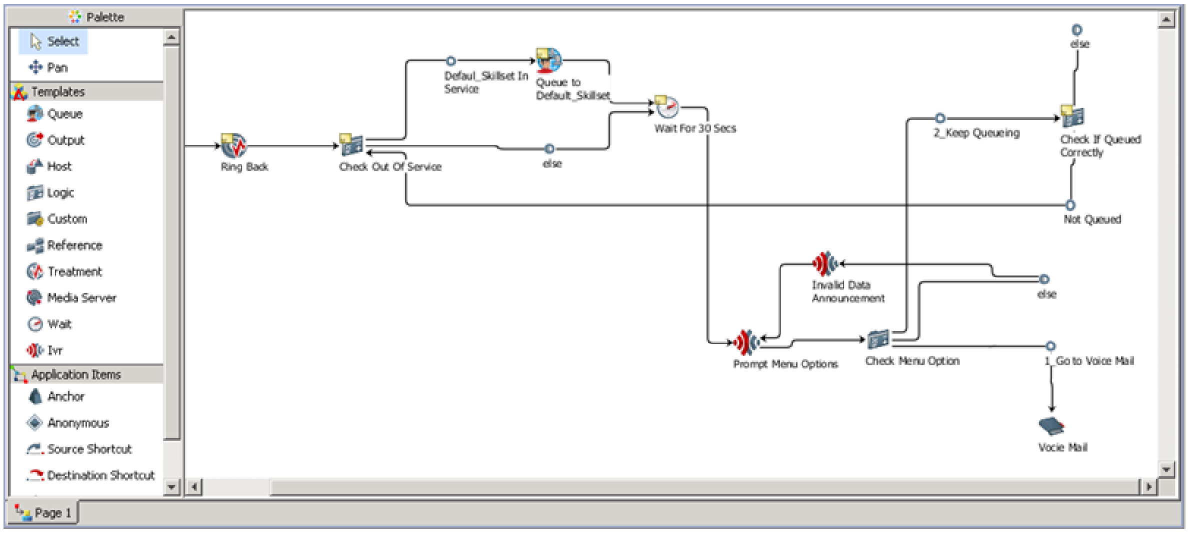
x. Close the **Check Menu Option** tab.

27. Right-click on the **tran** icon with the conditional expression of “im_str == 1” and select **Rename**.
28. In the **Name** box, type `1_Go to Voice Mail` and click **OK**.
29. Right-click on the **tran** icon with the conditional expression of “im_str == 2” and select **Rename**.
30. In the **Name** box, type `2_Keep Queueing` and click **OK**.

31. Select the **2_Keep Queueing** icon.
32. Right-click on the **Check If Queued Correctly** icon and select **(Dis)Connect**.
33. From the palette bar, select the **Finish** block icon.
34. Click the **main [LeaveVoiceMail]** panel.

    The CCFINISHBLOCK icon appears in the Main Flow Editor. Reposition the icon if needed.
35. Right-click on the **CCFINISHBLOCK** icon and select **Rename**.
36. In the **Name** box, type `Voice Mail` and click **OK**.
37. Select the **1_Go to Voicemail** icon.
38. Right-click on the **Voice Mail** icon and select **(Dis)Connect**.
39. From the palette bar, select the **Ivr** block icon.
40. Click the **main [LeaveVoiceMail]** panel.

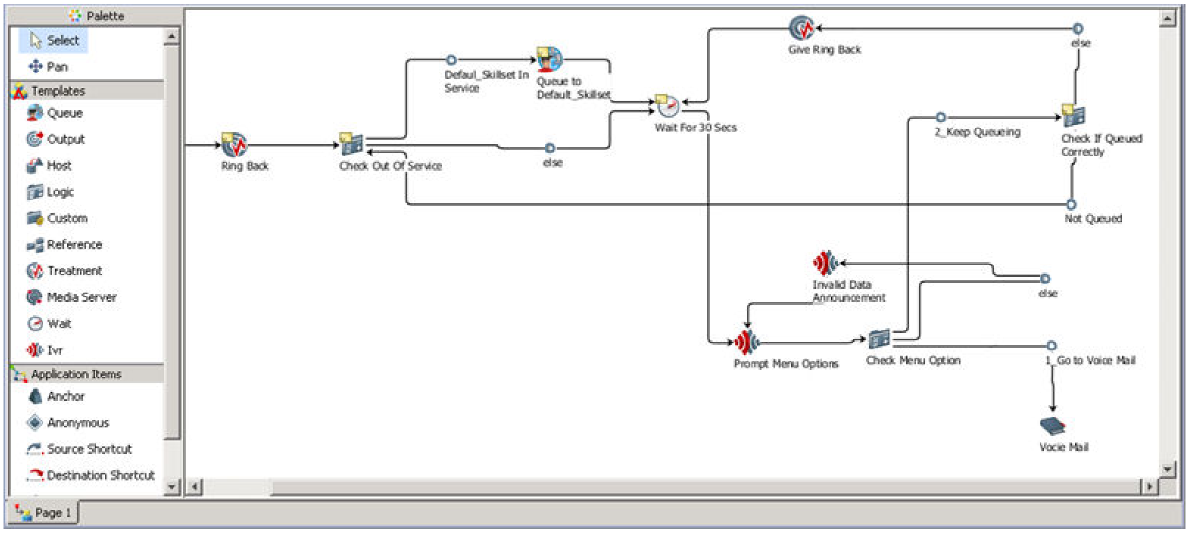
    The CCIVRBLOCK icon appears in the Main Flow Editor. Reposition the icon if needed.
41. Right-click on the **CCIVRBLOCK** icon and select **Rename**.
42. In the **Name** box, type `Invalid Data Announcement` and click **OK**.
43. Select the Check Menu Option **else** icon.
44. Right-click on the **Invalid Data Announcement** icon and select **(Dis)Connect**.
45. Select the **Invalid Data Announcement** icon.
46. Right-click on the **Prompt Menu Options** icon and select **(Dis)Connect**.



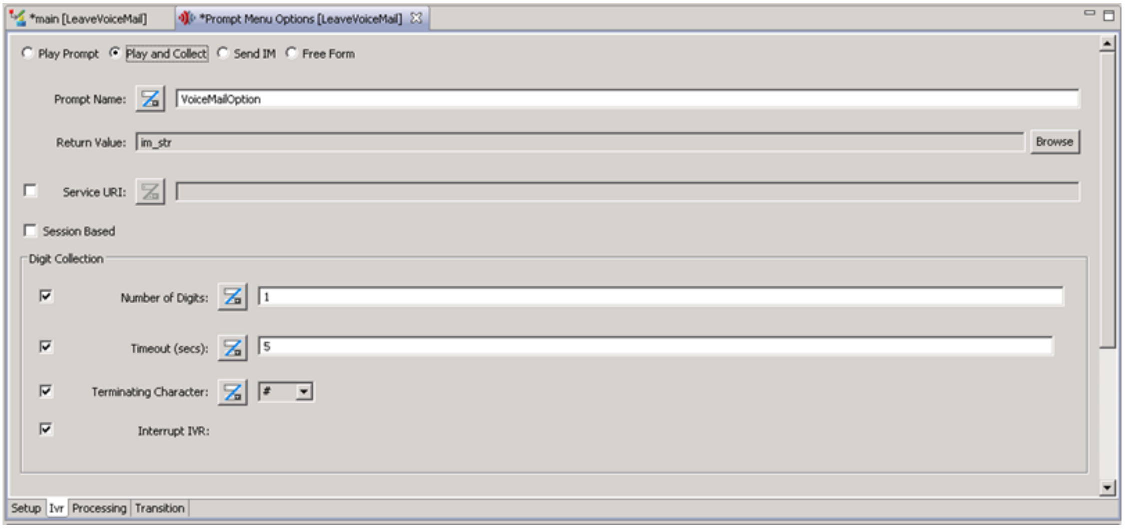
47. From the palette bar, select the **Treatment** block icon.
48. Click the **main [LeaveVoiceMail]** panel.

    The CCTREATMENTBLOCK icon appears in the Main Flow Editor. Reposition the icon if needed.

49. Right-click on the **CCTREATMENTBLOCK** icon and select **Rename**.
50. In the **Name** box, type `Give Ring Back` and click **OK**.
51. Select the Check If Queued Correctly **else** condition icon.
52. Right-click on the **Give Ring Back** icon and select **(Dis)Connect**.
53. Select the **Give Ring Back** icon.
54. Right-click on the **Wait For 30 Secs** icon and select **(Dis)Connect**.



55. Double-click the **Prompt Menu Options** icon.
    a. On the **Ivr** tab, select **Play and Collect**.
    b. In the **Prompt Name** box, type the name of your custom media file. For example, type `VoiceMailOption`.
    c. Under **Return Value**, click **Browse**.
    d. In the **Chooser** dialog box, expand **Application Variables** > **STRING**.
    e. Select **im_str** and click **OK**.
    f. Under **Digit Collection**, select all check boxes.
    g. In the **Number of Digits** box, type 1.
    h. In the **Timeout (secs)** box, type 5.



*main [LeaveVoiceMail] | *Prompt Menu Options [LeaveVoiceMail]

○ Play Prompt ● Play and Collect ○ Send IM ○ Free Form

Prompt Name: VoiceMailOption

Return Value: im_str

□ Service URI:

□ Session Based

Digit Collection

☑ Number of Digits: 1

☑ Timeout (secs): 5

☑ Terminating Character: #

☑ Interrupt IVR:

i. Close the **Prompt Menu Options** tab.

56. Double-click the **Voice Mail** icon.

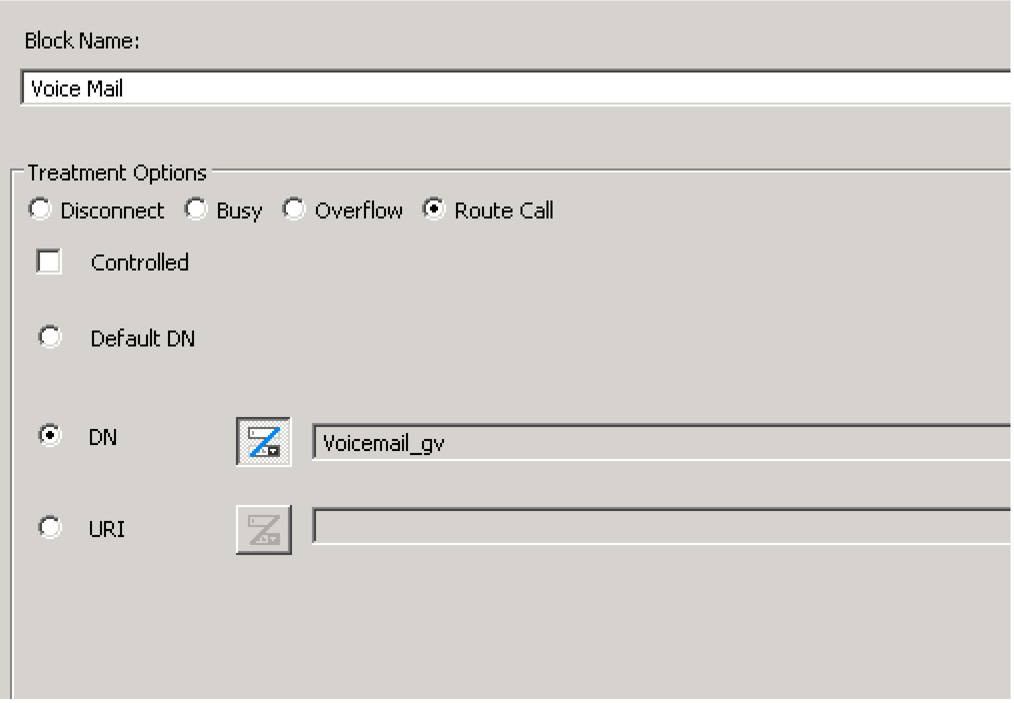
a. Under **Treatment Options**, select **Route Call**.

b. Select the **DN** option and click the icon ( ).

c. Click **Browse**.

d. In the **Chooser** dialog box, expand **Application Variables** > **DN**.

e. Select **Voicemail_gv** and click **OK**.



Block Name: Voice Mail

Treatment Options

○ Disconnect ○ Busy ○ Overflow ● Route Call

□ Controlled

○ Default DN

● DN Voicemail_gv

○ URI

f. Close the **Voice Mail** tab.

57. Double-click the **Invalid Data Announcement** icon.

    a. On the **Ivr** tab, select **Play Prompt**.

    b. Select the Prompt Name icon ( ) and click **Browse**.

    c. In the **Chooser** dialog box, expand **Application Variables** > **STRING**.

    d. Select **InvalidEntry_CS** and click **OK**.

    e. Close the **Invalid Data Announcement** tab.

58. Double-click the **Give Ring Back** icon.

    a. In the **Minimum Duration (secs)** box, type 2.

    b. Close the **Give Ring Back** tab.

59. Optionally, double-click the **Wait for 30 Secs** wait block.

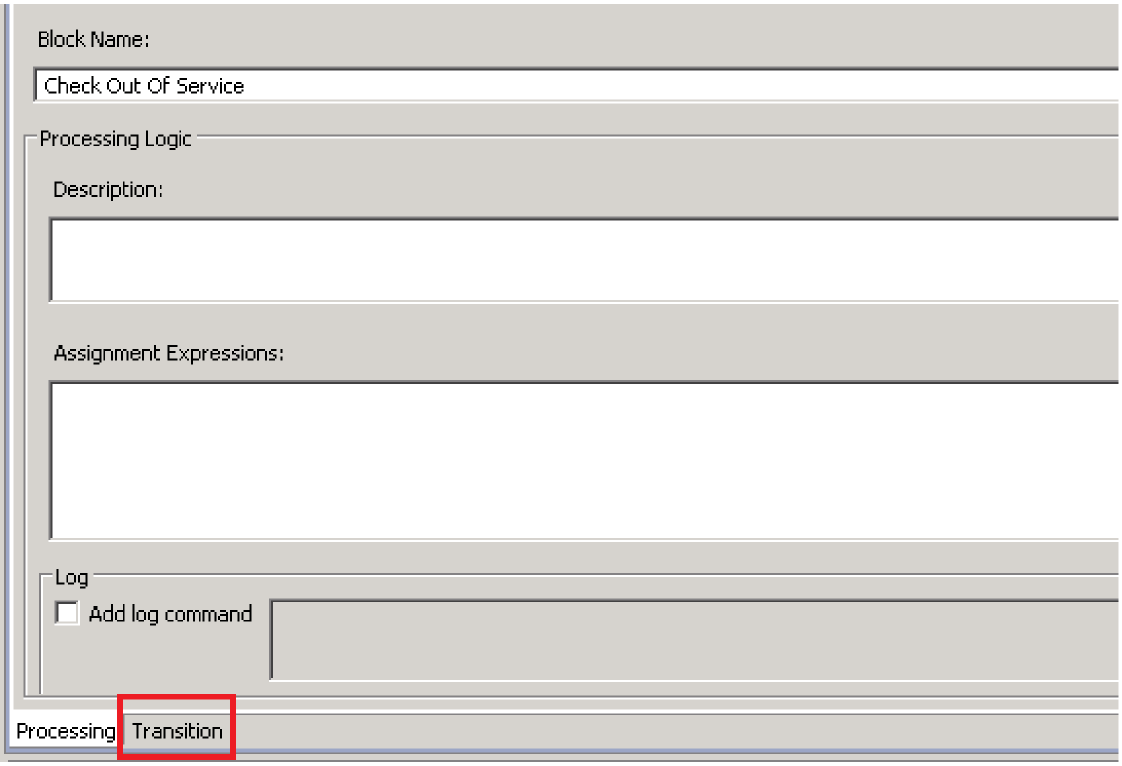
    a. Under **Block Name**, type a new name for the wait block. For example, type `Wait for 20 Secs`.

    b. In the **Duration (secs)** box, type `20`.

    c. Close the **Wait for 30 Secs** tab.

60. Double-click the **Check Out Of Service** icon.

    a. Click the **Transition** tab.



Block Name:

Check Out Of Service

Processing Logic

Description:

Assignment Expressions:

Log

☐ Add log command

b. Click the **Default_Skillset In Service** tab.

c. Under **Conditional Expression**, click **Edit**.

d. Under **Condition**, select **! OUT OF SERVICE Default_Skillset**.

   ! OUT OF SERVICE Default_Skillset appears in the **When** box.

e. Click **Clear Entry**.

f. From the **Not** drop-down list, select **Not**. Ensure “!” appears in the **When** box after you select **Not**.

g. Click **Variables**.

h. On the **Chooser** dialog, expand **Intrinsics** > **Skillset**.

i. Select **OUT OF SERVICE** and click **OK**.

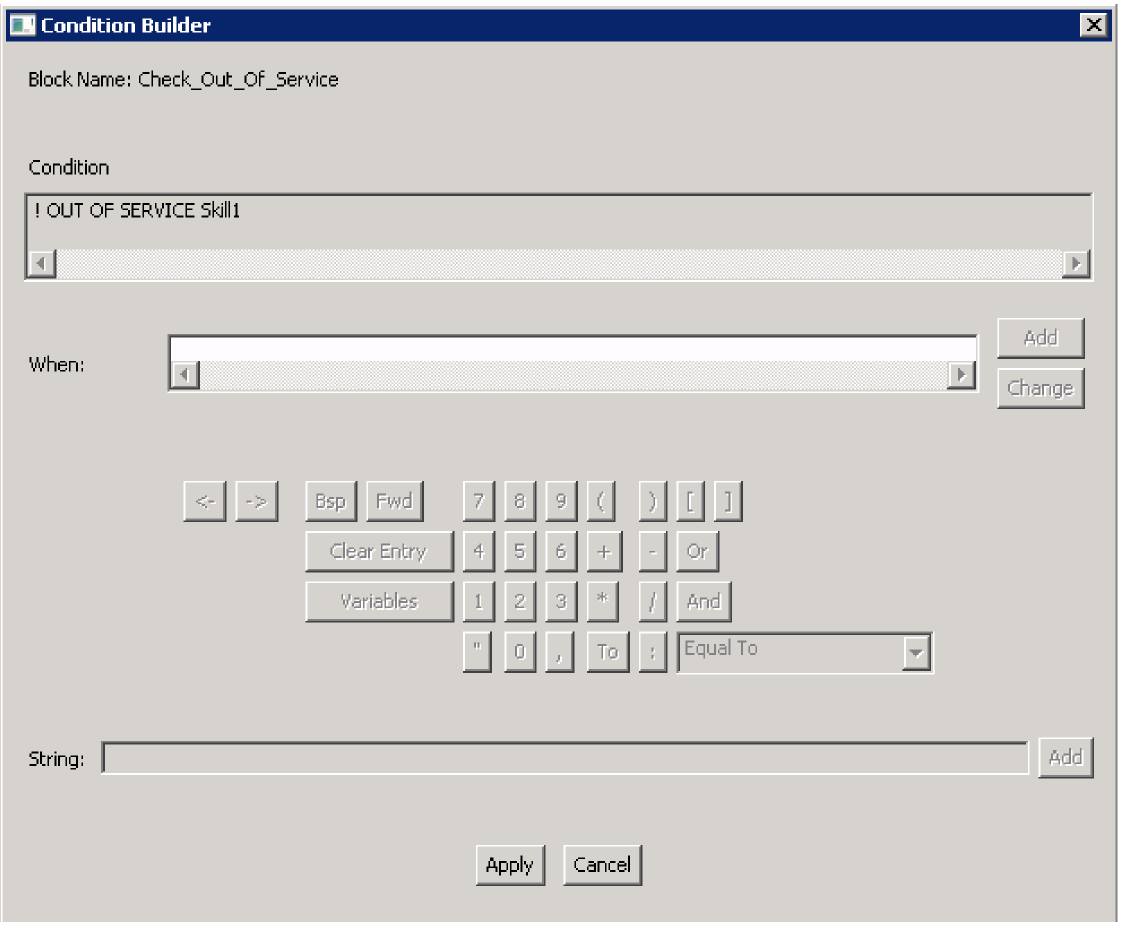
j. Click **Variables**.

k. On the **Chooser** dialog, expand **Application Manager Data** > **Skillsets** > **Local**.

l. From the list of skillsets, select a voice skillset. For example, select Skill1.

m. Click **OK**.

n. Click **Change**.



Condition Builder

Block Name: Check_Out_Of_Service

Condition

! OUT OF SERVICE Skill1

When:

String:

   o. Click **Apply**.

   p. Close the **Check Out Of Service** tab.

61. Double-click the **Queue to Default_Skillset** icon.

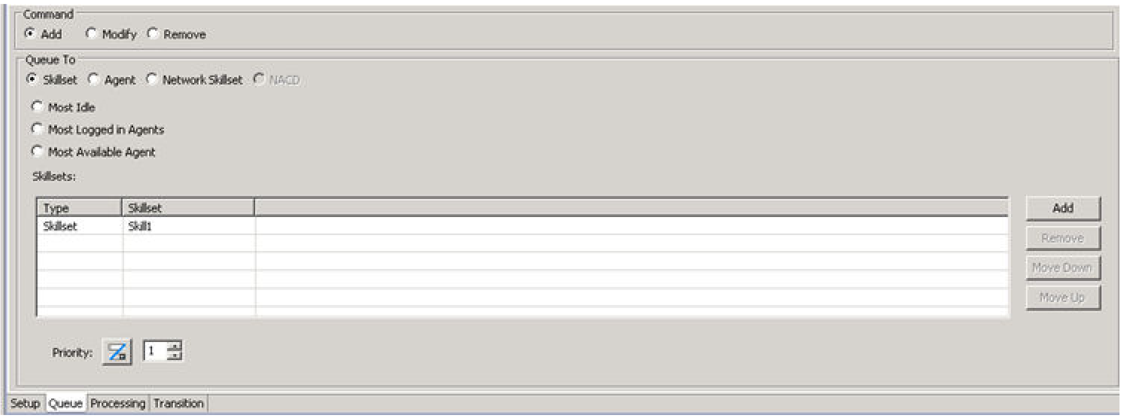
   a. Under **Skillsets**, click **Add**.

   b. Expand **Application Manager Data** > **Local Skillsets**.

   c. From the list of skillsets, select a voice skillset. For example, select Skill1.

   d. Click **OK**.

   e. To remove a skillset from the list, for example Default_Skillset, select the skillset and click **Remove**.



Command

● Add ○ Modify ○ Remove

Queue To

● Skillset ○ Agent ○ Network Skillset ○ NACD

○ Most Idle

○ Most Logged in Agents

○ Most Available Agent

Skillsets:

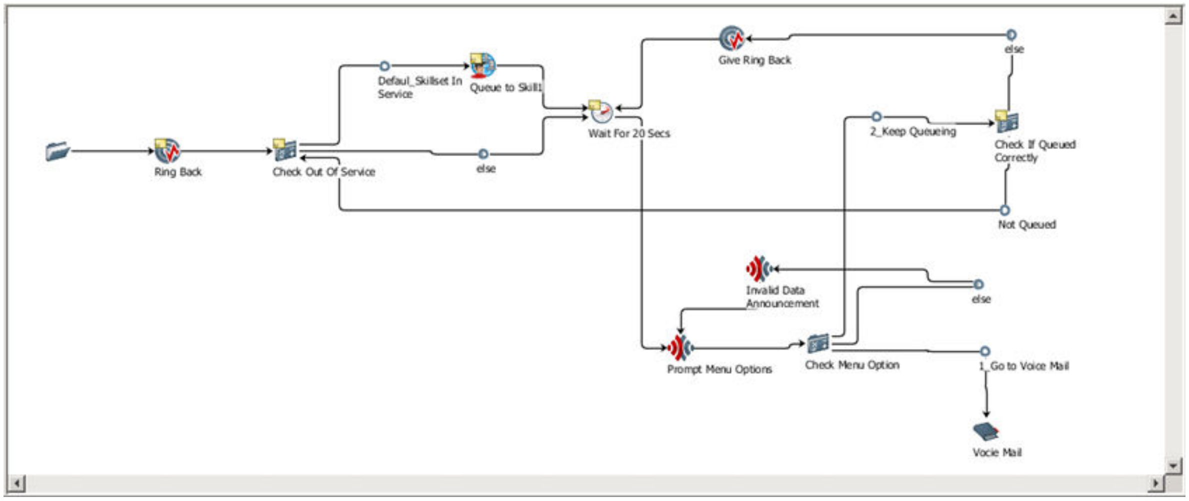
Type	Skillset
Skillset	Skill1

Priority: 1

   f. Close the **Queue to Default_Skillset** tab.

62. Right-click the **Queue to Default_Skillset** icon and click **Rename**.

63. In the **Name** box, type `Queue to Skill1` and click **OK**.



64. Close the **LeaveVoiceMail** flow application.

65. On the **Save Resource** box, click **Yes** to save the application.

66. On the **Confirm** box, click **OK** to activate the application.
67. In the **Contact Center** view, double-click on **Master_Script**.
68. Under **Configured Routes** in the right pane, expand **CDN**.
69. Select **SampleCDN** and click **Edit**.
70. In the Application Chooser, under Valid Applications, select the **LeaveVoiceMail** flow application.
71. Click **OK**.

    Calls to the SampleCDN (Route Point) are routed to the LeaveVoiceMail flow application for treatment and queueing to the appropriate agent skillset queue (for example, the Skill1 skillset). If the skillset is busy or out of service for any reason, customers that call the sample Route Point have an option to leave a voice mail or to continue waiting for an agent.
72. Close **Contact_Router**.
73. On the **Save Resource** box, click **Yes**.
74. On the **Confirm** box, click **OK** to activate the Master_Script.

Next steps

Before you use the flow application in your contact center, ensure that the flow works correctly by performing the following:

- Take the Skill1 skillset out of service.
- Place a test call to the SampleCDN.
- Verify that after hearing ringback for 20 seconds, you hear the “VoiceMailOption” prompt.
- Verify that if you press 1 after hearing the prompt, you can leave a voice mail message.
- Verify that if you press 2 after hearing the prompt, you continue hearing ringback and the prompt plays every 20 seconds thereafter.
- Verify that if you press a key other than 1 or 2, or if you do not press any key, you hear the Invalid Entry prompt.

Chapter 16: Avaya Contact Center Select Server Configuration

This chapter describes how to change the configuration properties for the Avaya Contact Center Select software on your server. Configure the Avaya Contact Center Select server using Server Configuration. Use the Server Configuration utility to modify the data entered during the initial configuration of the Avaya Contact Center Select server. You can change the local settings, licensing, and network settings information.

Changing the local settings configuration

About this task

Change the local configuration settings of the Avaya Contact Center Select server, if you need to change the names and IP addresses required for Contact Center to run.

Procedure

1. Log on to the Avaya Contact Center Select server.
2. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.
3. In the **Server Configuration** dialog box, click the **Local Settings** tab.
4. Update the local settings.
5. Click **Apply All**.
6. Click **Exit**.
7. If prompted, restart the server.

Variable definitions

Name	Description
Customer Name	The designated contact person at the company that uses Contact Center software.

Table continues…

Name	Description
Company Name	The name of the company that uses the Contact Center software.
CLAN subnet IP Address	The IP address of the Contact Center server.
Site Name	The site name for the Contact Center. The site name must not contain spaces or non alphabetical characters except for hyphen (-) and underscore (_). The first character must be a letter. The site name must be unique and can consist of any combination of 6 to 15 characters.
Real-Time Statistics Multicast IP Address	The RSM IP address of the server to associate with sending real-time data. The IP address must be 224.0.1.0 to 239.255.255.255. The default is 234.5.6.10.

Changing the licensed features configuration

About this task

Change the licensing configuration of the Avaya Contact Center Select to update the licensing details.

You can use this application to enable or disable Avaya Contact Center Select licensed features, including Open Queue.

Procedure

1. Log on to the Avaya Contact Center Select server.
2. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.
3. In the **Server Configuration** dialog box, click the **Licensing** tab.
4. Update the licensing details.
5. Click **Apply All.**
6. Click **OK**.
7. Click **Exit**.
8. If prompted, restart the server.

Variable definitions

Name	Description
CCMS Package	The installation package indicates the licenses that you purchased with Contact Center: • Nodal Enterprise: The base package for Contact Center.
Optional Packages	You must choose the package you purchased. Packaged features includes: • Web Based Statistics: Use Agent Web Statistics on Agent Desktop, so that agents and supervisors can use Agent Desktop to view real-time statistics for call handling, skillset data, and state information on Agent Desktop. • Multiplicity: Use Multiplicity to ensure an agent can handle multiple concurrent contacts. At any one time an agent can be active on a voice and multimedia contact; only one of these can be active, the others automatically are on hold. • Open Queue: Use Contact Center Multimedia to route multimedia contacts to agents by using the existing scripting and skillset routing features available for calls. • Open Interfaces Open Queue—The Web services are a series of Open Interfaces provided to third parties to enable application communication based on the SOA architecture. The Web services ensure customers can discover the functions offered by each Web service using the WSDL provided. • Off Site Agent: This feature allows agents to log on to Agent Desktop in Other Phone mode. This allows agents to handle skillset calls regardless of location.

Changing the IP Office network data

About this task

Change the IP Office network data after you install Avaya Contact Center Select to enable communication with the IP Office platform.

Important:

Changes to the IP Office network data sometimes requires restarting Avaya Contact Center Select.

Procedure

1. Log on to the Avaya Contact Center Select server.
2. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.
3. In the **Server Configuration** dialog box, under **SIP**, click the **Network Settings** tab.
4. Update the **IP Office Settings** details.
5. Click **Apply All**.
6. Click **OK**.
7. Click **Exit**.
8. If prompted, restart the server.

Variable definitions

Name	Description
IP Office Address	The IP address of the IP Office server.
Voice Proxy Server — Port	The server listening port. The default port is 5060.
IP Office System Password	The system password for your IP Office server. Ask your IP Office Administrator for the System Password. If this password changes on the IP Office server, you must update the password in Server Configuration.

Changing the Local Subscriber data

About this task

Change the local subscriber data after you install Avaya Contact Center Select to enable communication with other network elements.

Important:

Changes to the Local Subscriber data sometimes requires restarting Avaya Contact Center Select.

Procedure

1. Log on to the Avaya Contact Center Select server.
2. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.

3. In the **Server Configuration** dialog box, under **SIP**, click the **Local Subscriber** tab.
4. Update the SIP Local Subscriber details.
5. Click **Apply All**.
6. Click **OK**.
7. Click **Exit**.
8. If prompted, restart the server.

Variable definitions

Name	Description
Domain Name	The SIP domain name of Avaya Contact Center Select. This domain name must match the IP Office SIP domain name.
MS Locale	Locale (including language and dialects) of the system environment.
Local Listening Ports	The SIP Communication protocol accepted by the system for incoming calls. • TCP/UDP Port default is 5060. • TLS Port default is 5061.
SIP Line Extension Number	The IP Office SIP User Extension Number used to register Avaya Contact Center Select.
Password	The password of the IP Office SIP User Extension Number used to register Avaya Contact Center Select.

Chapter 17: REST API configuration

Contact Center allows you to invoke REST API in a Contact Center workflow. REST (Representational state transfer) provides efficient scalable services for web communications.

A Contact Center workflow can request data using scripting commands, and the workflow uses the TfeRestService to request and retrieve data from the REST API.

The Contact Center workflows pass JSON (JavaScript Object Notation) data to the TfeRestService, which identifies the REST API to invoke and populates the REST API parameters. The data returned from the API is reconfigured into a JSON object and then passed back to the workflow. Contact Center supports generic REST API exposed as a URL end-point and query string parameters.

For more information about creating and configuring Contact Center workflows for REST API integration, see *Using Contact Center Orchestration Designer*.

TFE REST Configurator

Contact Center provides an application to configure and test REST API calls. The TFE REST Configurator allows you to configure your REST API end-point and parameters, and to test your configuration. If you receive a successful response after you send the test request, you can then save your configuration to the database. You can use the application to create GET, POST, PUT, or DELETE requests.

You can also add environments using the TFE REST Configurator. Environments enable the use of environment variables. An environment variable is shared across all requests associated with the environment. For example, a service defines a security access token that must be included in the header of all requests for that service. Contact Center provides a default environment named ‘No environment’. You cannot delete this environment. When you create a new request it is automatically associated with the default environment, unless you select an alternative environment that you previously created. The TfeRestService replaces any environment variables in the request with the variable value that you set when creating the environment.

REST API security

Using the TFE REST Configurator, you can configure the following authorization protocols:

- No Auth
- Basic Auth
- OAuth 2.0

Adding a new environment

About this task

Add environments using the TFE REST Configurator. Environments enable the use of environment variables.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **REST Configurator**.
2. In the TFE REST Configurator application, click the Environment settings icon.
3. On the **Environment** window, click the **New environment** icon.
4. In the **Key** and **Value** boxes, type the key and value of the environment variable.
5. Click **Add**.

Creating and testing REST requests

Before you begin

- Ensure that you have all the required REST API end-point and security details, if required.
- Add an environment if required.

About this task

Use the TFE REST Configurator to configure your REST API end-point and parameters, and to test and save your configuration. The TFE REST Configurator supports GET, POST, PUT, or DELETE request methods.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **REST Configurator**.
2. In the TFE REST Configurator application, click the new request icon.
3. From the environment drop-down list, select an environment if required.

   Note:

   The default environment is automatically selected.
4. If security details are required to test the REST API end-point, click the **Authorisation** tab. If security is not required, skip to step 7.
5. Select **Basic Auth** or **OAuth 2.0**.
6. If you select **Basic Auth**:
   a. In the **Username** box, type the user name for the REST API end-point.
   b. In the **Password** box, type the password.

7. If you select **OAuth 2.0**:
    a. To create a new access token, click **New token**. If an access token already exists, skip to step 6h.
    b. On the **Access Token** window, In the **Token Name** box, type a name for the token.
    c. In the **Access Token URL** box, type the URL to access the security token for your end-point.
    d. In the **Client ID** box, type the client ID that identifies the end-point.
    e. In the **Client Secret** box, type the OAuth 2.0 client secret generated for the end-point.
    f. From the **Client Authentication** list, select the authentication method as required for your end-point.
    g. Click **Request**.
    h. From the **Available tokens** list, select the previously created access token.
8. From the request method drop-down list, select the request method for the new request. Select GET, POST, PUT, or DELETE.
9. In the **Please enter request** box, type the request URL.
10. Click the **Parameters** tab to add parameters to the request, if required.
11. In the **Key** and **Value** boxes, type the key value pair to test. You can add multiple key value pairs.
12. Click the **Headers** tab to add header data to the request, if required.
13. In the **Key** and **Value** boxes, type the key value pair of header data to test. You can add multiple key value pairs. The key-value pairs are JSON encoded.
14. Click the **Body** tab to add body data to the request, if required.
15. In the **Key** and **Value** boxes, type the key value pair of body data to test. You can add multiple key value pairs. The key-value pairs are JSON encoded.
16. Click **Execute**.

    The result of the request appears in the **Response** panel.
17. If the request was successful, click the Save icon to add the REST request to the database.
18. On the **Warning** box, click **Continue**.
19. On the **Success** box, click **OK**.

    The REST request appears in the **REST Services** list.

    ! Important:

    Note the ID of your saved REST requests. The ID is required when you configure your scripts for REST API integration.

Updating a REST request

About this task

Use the TFE REST Configurator to update your saved REST requests.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **REST Configurator**.
2. From the **REST Services** list, select the request to update.
3. Modify the request.
4. Click **Execute** to test the updated request.

   The result of the request appears in the **Response** panel.
5. If the request was successful, click the Update icon to add the REST request to the database.
6. On the **Warning** box, click **Continue**.
7. On the **Success** box, click **OK**.

   The updated REST request appears in the **REST Services** list.

Deleting a REST request

About this task

Use the TFE REST Configurator to delete your saved REST requests from the database.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **REST Configurator**.
2. From the **REST Services** list, select the request to delete.
3. Click the Delete icon.
4. On the **Warning** box, click **Continue**.
5. On the **Success** box, click **OK**.

   The REST request is removed from the **REST Services** list.

Updating an environment

About this task

Update an environment using the TFE REST Configurator.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **REST Configurator**.
2. In the TFE REST Configurator application, click the Environment settings icon.
3. On the **Environment** window, select the environment to edit and click the **Edit environment** icon.
4. In the **Key** and **Value** boxes, edit the values as required.
5. Click **Update**.

Deleting an environment

About this task

Delete an environment using the TFE REST Configurator.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **REST Configurator**.
2. In the TFE REST Configurator application, click the Environment settings icon.
3. On the **Environment** window, select the environment to delete and click the **Delete environment** icon.
4. On the **Warning** box, click **Continue**.

   The environment is deleted.

Chapter 18: Avaya Contact Center Select routine maintenance

This chapter describes how to maintain the Avaya Contact Center Select software and server. You must maintain Avaya Contact Center Select to protect against data loss and to ensure that you are using the most recent software.

The Avaya Aura® Media Server software appliance does not support *root* account access, therefore it has distinct routine maintenance instructions. When maintaining the Avaya Aura® Media Server software appliance, use the procedures specific to the software appliance. You use the Avaya Aura® Media Server Open Virtual Appliance (OVA) file to create a VMware-based Avaya Aura® Media Server software appliance.

Database maintenance

Perform an immediate backup of the Avaya Contact Center Select databases to save the current data. It is important to complete this procedure after you complete your installation or when any significant change occurs in the database, so that you can restore the database easily. Perform backups during low traffic periods. Avaya Contact Center Select services are not shut down during backups. Back up the databases to a secure network location. Schedule regular backups of the Avaya Contact Center Select databases to ensure resiliency against media failure or data loss. You can also restore the database content to your server using the Database Maintenance utility.

Avaya Contact Center Select logs a warning message when a there has not been a scheduled or manual backup for a specified number of days. You can configure the number of days before Avaya Contact Center Select logs the warning. The default is seven days. The Database Maintenance Utility also displays the time that has elapsed since the last backup.

Backing up the Contact Center databases

About this task

Perform an immediate backup of the Contact Center server databases to save the current data. Perform a scheduled backup to maintain snapshots of data for emergency purposes. For more information about scheduled backups, see Scheduling a backup of the Contact Center server databases on page 252.

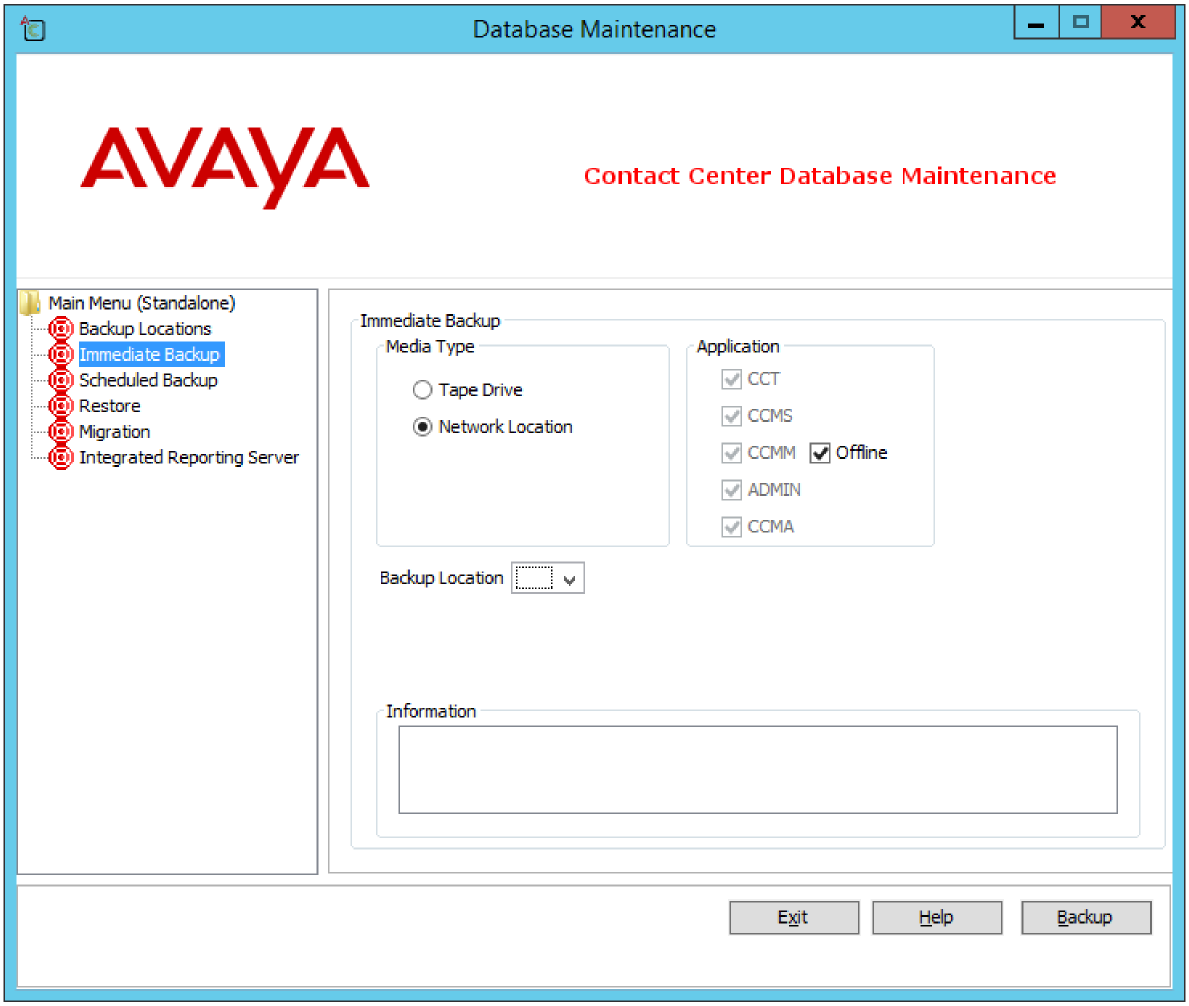
It is important to complete this procedure after you complete your installation or when any significant change occurs in the database, so that you can restore the database easily if required.

Perform backups during low traffic volume periods.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Database Maintenance**.
2. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
3. In the right pane, click **Create**.
4. From the **Drive Letter** list, select the network drive on which to store the Contact Center database.
5. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name \Folder\Backup Location.
6. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
7. In the **Password** box, type the user password.
8. Click **Save**.

9. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Immediate Backup**.



Database Maintenance

AVAYA

Contact Center Database Maintenance

Main Menu (Standalone)
- Backup Locations
- Immediate Backup
- Scheduled Backup
- Restore
- Migration
- Integrated Reporting Server

Immediate Backup

Media Type
- ○ Tape Drive
- ● Network Location

Application
- ☑ CCT
- ☑ CCMS
- ☑ CCMM ☑ Offline
- ☑ ADMIN
- ☑ CCMA

Backup Location

Information

10. In the **Media Type** section, select **Network Location**.
11. From the **Backup Location** list, select the network drive on which to store the backup.
12. Click **Backup**.
13. Click **Yes**, to continue with the backup.

    The database is backed-up.
14. Click **Exit**.

Configuring the overdue backup notification

About this task

Avaya Contact Center Select logs a warning message when there has not been a scheduled or manual backup for a specified number of days. Configure the number of days after which Avaya Contact Center Select logs a warning that a backup is overdue.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Database Maintenance**.
2. In the Database Maintenance dialog box, click **Backup Locations**.
3. In the right pane, in the **Number of days without a backup before notification** box, type the number of days after which Avaya Contact Center Select logs a warning that a backup is overdue.

   You can set the notification period from 1 day to 999 days. The default value is seven days.
4. Click **Save**.

Creating a backup location for scheduled backups

Before you begin

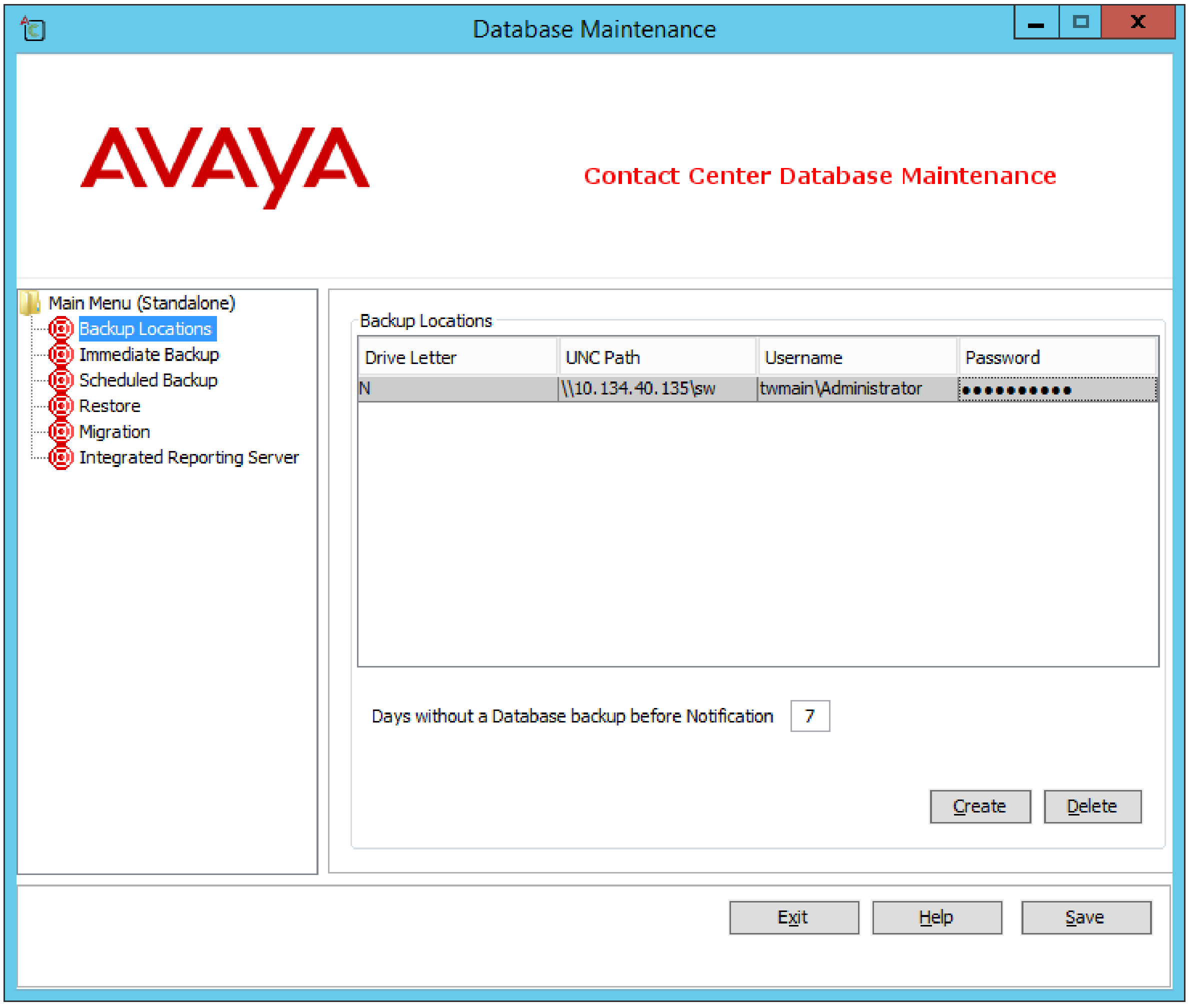
- Ensure that you log on with a user account with full permissions to access the location where you store the database backups.

About this task

Create a backup location on your network with the correct access permissions to ensure that you have a designated location for the scheduled backups.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Database Maintenance**.
2. In the Database Maintenance dialog box, click **Backup Locations**.
3. In the right pane, click **Create**.
4. From the **Drive Letter** list, select a drive letter.
5. In the **UNC Path** text box, type the location to which to back up the database.
6. In the **Username** box, type the user name used to log on to the server specified in the UNC Path box in the format Computer Name\Account Name.
7. In the **Password** box, type the Windows password.
8. Click **Save**.



Drive Letter	UNC Path	Username	Password
N	\\10.134.40.135\sw	twmain\Administrator	●●●●●●●●●●●

Days without a Database backup before Notification 7

Scheduling a backup of the Contact Center server databases

Before you begin

- Create a backup location. For more information, see Creating a backup location for scheduled backups on page 251.

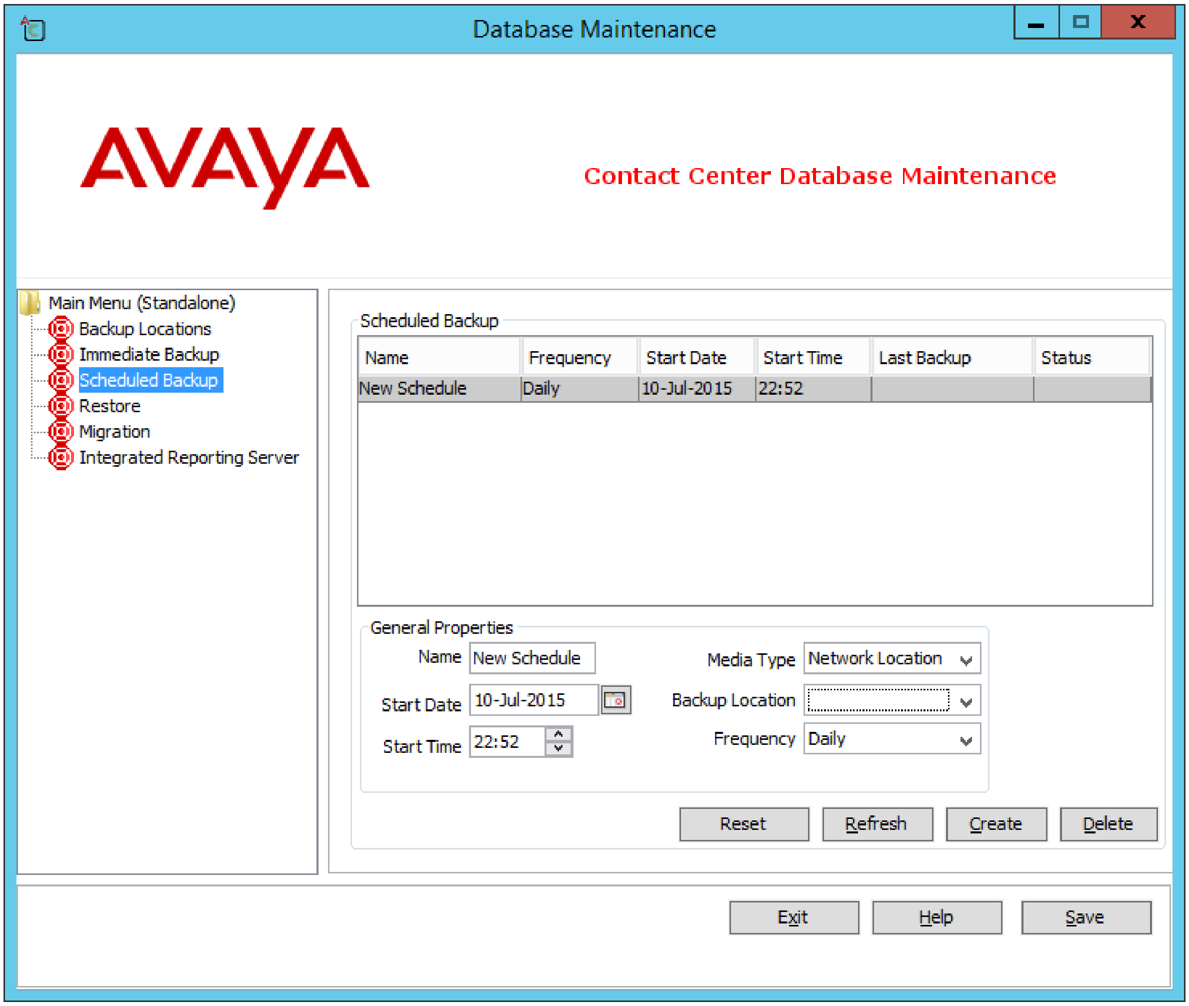
About this task

Schedule a backup of the Contact Center server databases to save the data regularly. Perform a scheduled backup to maintain snapshots of data for emergency purposes.

Perform backups during low traffic volume periods.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Database Maintenance**.
2. In the Database Maintenance dialog box, in the left pane, click **Scheduled Backup**.



Name	Frequency	Start Date	Start Time	Last Backup	Status
New Schedule	Daily	10-Jul-2015	22:52		

Name: New Schedule
Start Date: 10-Jul-2015
Start Time: 22:52
Media Type: Network Location
Backup Location:
Frequency: Daily

3. In the right pane, click **Create**.
4. Under **General Properties**, in the **Name** box, type a name for the scheduled backup.
5. From the **Media Type** list, select **Network Location**.
6. In the **Start Date** box, type the date on which to begin scheduled backups.

   OR

   Click the calendar icon and select a date on which to begin scheduled backups.
7. In the **Start Time** box, select the time to start the backup.
8. From the **Backup Location** list, select a drive to store the backup.
9. From the **Frequency** list, select the frequency of the backup.

10. Click **Save**.
11. Click **Exit** to close the Database Maintenance utility.

Restoring the Avaya Contact Center Select Release 7.0 databases

Before you begin

- Back up the old databases.
- Map a drive to the database backups.

About this task

Restore the Avaya Contact Center Select Release 7.0 databases. After you complete this procedure, you must restart your server.

! **Important:**

You must complete this procedure to ensure all databases are restored at the same time.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Database Maintenance**.
2. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
3. In the Backup Locations pane, click **Create**.
4. Select the Drive Letter, UNC path, user name, and password to specify the network location where you stored the server database backup.
5. Click **OK**.
6. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Restore**.
7. In the **Media Type** section, select **Network Location**.
8. In the **Application** section, select **CCT**, **CCMS**, **CCMM**, **ADMIN**, and **CCMA**.
9. In the **Restore contents** section, select **Data** and **Offline**.
10. From the **Backup Location** list, select the network drive containing the backed up Avaya Contact Center Select server databases.
11. Click **Restore**.
12. Use the **Progress information** field to monitor the progress of the restoration.
13. On the **Database Maintenance** message box, click **OK**.

    Wait for the restore to complete.

14. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.
15. In the Server Configuration dialog box, click **Apply All**.
16. Restart the server.

Logging on to Avaya Aura® Media Server Element Manager

Before you begin

- Obtain a valid user name and password to access Avaya Aura® Media Server Element Manager.

About this task

Log on to the Avaya Aura® Media Server Element Manager as an administrator to configure Avaya Aura® Media Server.

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

Procedure

1. On the Avaya Contact Center Select server, start a Web browser. In the address box, type https://SERVER_IP_ADDRESS:8443/em, where SERVER_IP_ADDRESS is the IP address of the Avaya Aura® Media Server.
2. In the **User ID** box, type the Avaya Aura® Media Server User ID log on account name. The default Element Manager User ID account name is *cust*.
3. In the **Password** box, type the Avaya Aura® Media Server Element Manager password. The default Element Manager password is the *cust* password.
4. Click **Log in**.

Creating a backup destination for Avaya Aura® Media Server

Before you begin

- Configure the destination ftp server and check that it is operational. If you plan to use the default backup location for Avaya Aura® Media Server backups, do not configure an ftp server.
- Ensure that you have the address or host name, ftp account details, and path for the backup server.

About this task

Create a location to store backups. You can specify an ftp server to which you can send backups from Avaya Aura® Media Server Element Manager.

You can configure any number of remote backup destinations. When performing remote backup destinations, Element Manager (EM) uploads the backup files to the specified File Transfer Protocol (FTP) server and then deletes the duplicate backup files from the Avaya Aura® Media Server server. To perform a backup and restore, you must have permission to upload files to the remote backup destination.

You can accept the default backup location to save the Avaya Aura® Media Server backup on the local server. Avaya Aura® Media Server stores the backups in:

- For Linux: `$MASHOME/platdata/EAM/`
- For Windows: `%MASHOME%\platdata\EAM`

Procedure

1. Log on to Avaya Aura® Media Server Element Manager.
2. Expand **Tools** > **Backup and Restore** > **Backup Destinations**.
3. On the Backup Destinations page, click **Add**.
4. In the **Destination Name** field, type a unique name for the backup destination.
5. In the **Host Name** field, type the host name of the destination server.
6. In the **User Name** field, type the ftp user name.
7. In the **Password** field, type the ftp password.
8. In the **Destination Path** field, type the path on the backup location to specify where the backup function writes the backup files.
9. Optionally, click **Test** to test your connection.
10. Click **Save**.

Backing up the Avaya Aura® Media Server database

Before you begin

- Configure the destination ftp server and check that it is operational.
- Ensure that you have the address or host name, ftp account details, and path for the backup server.

About this task

Create a location to store backups. You can specify an ftp server to which you can send Avaya Aura® Media Server Element Manager backups. Backup the Avaya Aura® Media Server data so you can restore it on the new server.

Procedure

1. Log on to Avaya Aura® Media Server Element Manager.
2. Expand **Tools** > **Backup and Restore** > **Backup Tasks**.
3. On the Backup Tasks window, click **Add**.
4. On the Add New Backup Task window, in the **Backup Task Name** box, type a name for this backup.
5. Select **System Configuration**.
6. Select **Application Content**.
7. Choose the backup destination that you created for the migration.
8. Select **Manually, as needed**.
9. Click **Save**.
10. In the Backup Tasks window, select the backup task you created.
11. Click **Run Now**.

    The Confirm Backup window appears, showing the backup task name details about the backup.
12. Click **Confirm**.

    The History Log Window appears. When the backup is complete, the backup details appear in the list.

Recovering a scheduled backup

Before you begin

- Ensure that you view the event in Windows Event Viewer and address the reason why the scheduled backup failed.

About this task

Recover a scheduled backup if an error occurs while the backup is running. A scheduled backup failure can occur for several reasons, for example, if the backup location is not available or if there is not enough space to save the backup file. If an error occurs, the scheduled backup stops running and an event is created. To view the event, use Windows Event Viewer.

Procedure

1. Log on to the Avaya Contact Center Select server.
2. On the **Apps** screen, in the **Avaya** section, select **Database Maintenance**.
3. In the Database Maintenance dialog box, in the left pane, click **Scheduled Backup**.
4. Click the name of the scheduled backup you want to recover.

5. Click **Reset**.
6. Click **OK**.

   To run the schedule next time the error is cleared and the scheduled backup is recovered.

Restoring the Avaya Aura® Media Server database

Before you begin

Copy the backup zip files to the new Avaya Aura® Media Server server. The backup file names derive from the name that you entered in Element Manager for the backup task.

About this task

Restore the Avaya Aura® Media Server database backup data.

Procedure

1. Log on to Avaya Aura® Media Server Element Manager.
2. Expand **Tools** > **Backup and Restore** > **Restore**.
3. On the Restore window, from the **Restore Source** list, select **Upload Backup Files**.
4. Click **Browse**.
5. Select the Avaya Aura® Media Server backup that you want to restore.
6. Click **Upload Files**.
7. On the **Confirm Restore** page, review the information and click **Confirm** to proceed with the restore.
8. Restart the server.

Backing up the Avaya Aura® Media Server software appliance database

About this task

Backup the Avaya Aura® Media Server software appliance database. The Avaya Aura® Media Server software appliance (OVA) does not support root access. Use this procedure to backup data on an Avaya Aura® Media Server software appliance.

Procedure

1. Log on to Avaya Aura® Media Server Element Manager.
2. Navigate to **Tools** > **Backup and Restore** > **Backup Tasks**.

3. Create or select an existing backup task that includes System Configuration and Application Content backup types.
4. Click **Run Now**.
5. To monitor the Backup and Restore History Log, navigate to **Tools** > **Backup and Restore** > **History Log**.

   After the backup is complete, the log shows a completed backup task entry.
6. If you are using an FTP or SFTP backup destination, ensure that the backup files are saved to their required location.

   There is one file for each backup type for a total of two backup files.
7. If you are using a local backup destination and about to perform an upgrade or redeploy of the Avaya Aura® Media Server appliance, you must move the backup files to a safe location by performing the following steps:
   a. Log in to a Linux shell using the customer *cust* account.
   b. Change to the public directory by using the `cdpub` alias or the following command:

      ```
      cd /opt/avaya/app/pub
      ```
   c. List the backups available on the local system by using the following command:

      ```
      bkupFile -list
      ```
   d. Move the recent configuration and application data backups from the local backup storage to the current directory by using the following commands:

      ```
      bkupFile -retrieve SystemConfiguration_backup.zip
      ```

      ```
      bkupFile -retrieve ApplicationContent_backup.zip
      ```
   e. Save both backup files in a safe location by using the sftp file transfer tool, or another similar tool, to transfer the files off the server.
   f. After you confirm the files are safely saved, you can delete the backup files from the current directory to free disk space.

Uploading a backup file to an Avaya Aura® Media Server software appliance

About this task

Upload a backup file to an Avaya Aura® Media Server software appliance (OVA). The Avaya Aura® Media Server software appliance (OVA) does not support root access. Use this procedure to upload data to a default backup folder on an Avaya Aura® Media Server software appliance.

The default backup folder: `$MASHOME/platdata/EAM/Backups`

Procedure

1. Log on to Avaya Aura® Media Server Element Manager.
2. Navigate to **Tools** > **Backup and Restore** > **Restore**.
3. On the **Restore** page, in the **Restore Source** drop-down list, select **Upload Backup Files**.
4. Click **Browse** to select the backup files.

   You can upload a System Configuration and Application Content backup at the same time.
5. On the **Confirm Restore** page, click **Confirm** to proceed with the upload.

   Important:

   Restoring a backup archive might impact running applications. After you click Confirm, the system invokes the restore task. Then Element Manager and Avaya Aura® Media Server close the connections to all users until the system completes the restoration.

Restoring data from the local folder on an Avaya Aura® Media Server software appliance

Before you begin

Upload a backup file to the Avaya Aura® Media Server software appliance.

About this task

Restore an Avaya Aura® Media Server OVA database from a default backup folder. The Avaya Aura® Media Server software appliance (OVA) does not support root access. Use this procedure to restore data to an Avaya Aura® Media Server software appliance.

The default backup folder: `$MASHOME/platdata/EAM/Backups`

Procedure

1. Log on to Avaya Aura® Media Server Element Manager.
2. Navigate to **Tools** > **Backup and Restore** > **Restore**.
3. On the **Restore** page, in the **Restore Source** drop-down list, select **Default Backup Destination**.
4. In the **Restore Task List**, select the backups from the list which you want to use for the restore.

   Important:

   To ensure that the application data is restored to the configured location, restore the system configuration data before restoring the application data.
5. Click **Restore Now**.

6. On the **Confirm Restore** page, click **Confirm** to proceed with the restore.

   ❗ **Important:**

   Restoring a backup archive might impact running applications. After you click Confirm, the system invokes the restore task. Then Element Manager and Avaya Aura® Media Server close the connections to all users until the system completes the restoration.

Chapter 19: Simple Network Management Protocol administration

Windows provides a Simple Network Management Protocol (SNMP) agent, which runs as a service on each Contact Center server. Contact Center servers use this service to forward events to a Network Management System (NMS) on your network. Contact Center automatically installs the Windows SNMP Service.

For more information about event codes and a list of recommended events to forward, see *Contact Center Event Codes*.

This chapter describes how to configure the Simple Network Management Protocol for your contact center.

Configuring Windows SNMP Service

About this task

Configure Windows Simple Network Management Protocol (SNMP) service on each Contact Center server to forward events to a Network Management System (NMS) on your network.

Procedure

1. Log on to the Contact Center server as Administrator.
2. On the **Start** screen, click **Administrative Tools** > **Services**.
3. In the Services window, select the **SNMP Service**.
4. Click **Action** > **Properties**.
5. In the SNMP Service Properties window, click the **Traps** tab.
6. If no community name is defined, in the **Community name** box, type `public`.
7. Click **Add to list**.
8. Click **Add** to add the IP address of the NMS to which the server sends traps.
9. In the SNMP Service Configuration window, type the IP address of the NMS.
10. Click **Add**.
11. In the SNMP Service Properties window, click **Add**.

12. In the Services window, right-click the **SNMP Trap** Service, and select **Start**.
13. Close the Services window.

Selecting CCMS events to be forwarded

About this task

Contact Center Manager Server uses SNMPFilterCnfg.exe to forward all Contact Center Manager Server related events (these events fall between the range 44900 to 51400).

Procedure

1. Using Windows Explorer, browse to the folder **D:\Avaya\Contact Center\Manager Server \bin**, and double-click **SNMPFilterCnfg.exe**.
2. In the **Level of Filtering** box, select the types of events that you want to forward to the Network Management System (NMS).

   Important:

   All event types that appear and the type that you select are also forwarded. For example, if you select Major, then all Unknown, Critical, and Major events are forwarded.
3. Click **OK**.

Selecting CCMA, LM, CCT, and CCMM events to be forwarded

About this task

Contact Center Manager Administration, License Manager, Communication Control Toolkit, and Contact Center Multimedia use the Windows Server 2012 R2 Event to Trap Translator (evntwin.exe) to select the events to be forwarded to the Network Management System (NMS).

When you are selecting events to forward, not all event sources populate the event descriptions. For some event sources the Event to Trap Translator shows event codes and descriptions, and for others it shows event codes.

Avaya provides a SNMP Trap Configuration File (.cnf) that is aligned with the *Contact Center Event Codes* document. Download the Contact Center Release 7.0 SNMP Trap Configuration File from the Avaya Support website at http://support.avaya.com. The file is available in the Contact Center software download Service Pack section. You can load this SNMP Trap Configuration file into the Event to Trap Translator on the Contact Center server.

In addition to the recommended SNMP Traps, you can add additional event codes to be forwarded to the NMS.

For more information about event codes, event source names, and a list of recommended events to forward, see *Contact Center Event Codes*.

Procedure

1. Download the Contact Center Release 7.0 SNMP Trap Configuration file (.cnf) from the Avaya Support website at http://support.avaya.com. The file is available in the Contact Center software download Service Pack section. Copy the .cnf file to the Contact Center server.
2. On the Contact Center server, open a command window and navigate to the location of the downloaded .cnf file.
3. Use the Windows `evntcmd` utility to load the SNMP Trap Configuration file.

   ```
   evntcmd -v 10 <SNMP Trap Configuration file name.cnf>
   ```

   For example:

   ```
   evntcmd -v 10 ACC_7_0_0_0_SNMP_Trap_File_ver1_0.cnf
   ```
4. On the **Desktop** screen, right-click the Windows icon and select **Run**.
5. In the **Run** text box, type `C:\Windows\System32\evntwin.exe`.
6. On the **Event to Trap Translator**, under **Configuration type**, select **Custom**.

   Ensure the recommended event traps from the *Contact Center Event Codes* document are listed.

   Important:

   Contact Center and related event sources are listed under several categories, including Application and System. License Manager events are listed under the NGEN event source.
7. Click **OK** to save the settings.
8. You can add additional event codes to be forwarded to the NMS.
   a. Click **Edit**.
   b. Under Event sources, click the folder for the event source you require.

      Important:

      Contact Center and related event sources are listed under several categories, including Application and System. License Manager events are listed under the NGEN event source.
   c. From the list of events, double-click the event you want to convert to an SNMP trap.
   d. On the **Properties** window, click **OK** if no change is required to generate the trap.
   e. Repeat these sub-steps for each event that you want added to the list of events to be translated into SNMP traps.
9. Close the Event to Trap Translator window.

Configuring the NMS

About this task

After you configure the server, you must configure the Network Management System (NMS) to receive and interpret traps (including identification to the NMS, and the origin and format of the Contact Center traps).

Load or compile the Contact Center Manager Server Management Information Block (MIB) files in the NMS. The following Contact Center Manager Server MIB files describe the format of the traps generated by Contact Center Manager Server:

- NB-FLT.mib - This is an SMNP v1 MIB that supports RFCs 1115,1212,1213 & 1215. This MIB describes the format of the traps that are sent from Contact Center Manager Server.
- RR-AACCDB.mib - This is an SNMP v2 MIB that supports RFCs 2578, 2579, & 2580. This MIB describes the format of the traps that are sent from the Contact Center Cache Database component.

You can use these files on the NMS system.

- The NB-FLT.mib file is available on the Contact Center Manager Server server, in the `D:\Avaya\Contact Center\Manager Server\data` folder.
- The RR-AACCDB.mib file is available on the Contact Center Manager Server server, in the `D:\Avaya\Contact Center\Common Components\Cache` folder.

Procedure

For more information about configuring your NMS, see your NMS documentation.

Chapter 20: Licensing administration

The Contact Center License Manager (LM) controls the licensing for Avaya Contact Center Select. Contact Center License Manager provides central control and administration of application licensing for all of the elements of Avaya Contact Center Select.

If Contact Center is not able to communicate with Contact Center License Manager it continues to function for a period of time. This is called a grace period. If the grace period expires, Contact Center shuts down and locks. You cannot restart Contact Center without resetting the grace period.

> ❗ **Important:**
>
> Avaya Aura® Media Server does not support the grace period. In a Hardware Appliance deployment of Avaya Contact Center Select, if the licensing services stop, Avaya Aura® Media Server stops and Contact Center ceases processing voice contacts.

This chapter describes how to configure Contact Center License Manager for your contact center.

Resetting the grace period

Before you begin

- You must apply separate unlock codes for the CCMS Control Service and the ASM Service. Repeat this procedure for each service.
- Obtain a Grace Period Unlock Code from Product Support.

About this task

If Contact Center is not able to communicate with Contact Center License Manager, normal operation of the Contact Center Manager Server continues for a period of time called a grace period.

If the grace period expires, Contact Center shuts down and locks. You cannot restart Contact Center without resetting the grace period.

When a communication error occurs, an event is fired to the Server Utility. The Server Utility records the details, the time elapsed in the Grace Period and a Grace Period Lock Code. These details must be sent to Product Support to obtain a Grace Period Unlock Code. Use this Grace Period Unlock Code to unlock the server and continue working.

Procedure

1. Log on to the Contact Center server.

2. From the Event Viewer, make a copy of the lock code and send this code to Product Support.
3. On the **Apps** screen, in the **Avaya** section, select **License Grace Period Reset**.
4. Enter the unlock code you received from Product Support.
5. Click **Apply**.
6. Click **Exit**.
7. Restart Contact Center.

Updating the license file

About this task

Update the license file to upgrade or expand your Avaya Contact Center Select solution.

If you are using a remote Avaya WebLM server, see the Avaya WebLM documentation for instructions on applying your updated license file on the Avaya WebLM server.

Procedure

1. Log on to the Avaya Contact Center Select server.
2. On the **Apps** screen, in the **Avaya** section, select **License Manager Configuration**.
3. Select the **Configuration** tab.
4. From the **License Type** list, select the type of license you are using.
5. Click **Browse** to navigate the file system and locate the new license file.
6. Click **Open**.
7. Click **Apply**.
8. On the dialog, click **Yes** to restart Contact Center License Manager.
9. Click **Close** to close the window.

Changing the licensing information for Contact Center

Before you begin

- Shut down the Contact Center services on the server.
- Plan to restart the server at the end of this procedure.

About this task

Change the license manager package information on the Avaya Contact Center Select server if you purchased additional features.

Procedure

1. Log on to the Avaya Contact Center Select server.
2. On the **Apps** screen, in the **Avaya** section, select **System Control and Monitor Utility**.
3. Click the **Contact Center** tab.
4. Click **Shut down Contact Center**.

   Contact Center shuts down.
5. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.
6. Click **Licensing**.
7. Under **License Manager Package**, change the **Package** and **Features** information to reflect your new licensed options.
8. Click **Apply All**.
9. Click **Yes** to restart the server.

Configuring a remote Avaya WebLM server

About this task

Configure Contact Center License Manager to use a remote Avaya WebLM server without centralized licensing. Contact Center License Manager can obtain licenses from a remote Avaya WebLM server, and then use these licenses to control Avaya Contact Center Select licensed features.

Refer to the Avaya WebLM documentation for instructions on applying your updated license file on the remote Avaya WebLM server.

Procedure

1. Log on to the Avaya Contact Center Select server.
2. On the **Apps** screen, in the **Avaya** section, select **License Manager Configuration**.
3. Select the **Configuration** tab.
4. From the **License Type** list, select the **Remote WebLM license**.
5. In the **WebLM IP or Fully Qualified Domain Name** box, type the IP address or FQDN host name of the remote Avaya WebLM server.
6. Click **Apply**.
7. On the dialog, click **Yes** to restart Contact Center License Manager.
8. Click **Close** to close the window.

Configuring Avaya WebLM centralized licensing

About this task

Configure Contact Center License Manager to use Avaya WebLM centralized licensing in an Avaya Contact Center Select Powered solution. Contact Center License Manager can share licenses from an Avaya WebLM server with centralized licensing, and use these licenses to control ACCS licensed features.

Refer to the Avaya WebLM documentation for instructions on applying your updated license file on the remote Avaya WebLM server.

Procedure

1. Log on to the Avaya Contact Center Select server.
2. On the **Apps** screen, in the **Avaya** section, select **License Manager Configuration**.
3. Click **Configuration**.
4. From the **License Type** list, select **Remote WebLM**.
5. Select **Centralized Licensing**.
6. In the **WebLM IP or Fully Qualified Domain Name** box, type the IP address or FQDN host name of the Avaya WebLM server.
7. In the **CLID** box, type the Centralized License ID (CLID) for this ACCS server.
8. Click **Apply**.
9. On the dialog, click **Yes** to restart Contact Center License Manager.
10. Click **Close** to close the window.

Chapter 21: Dialed number identification services configuration

This section describes the configuration you must perform on IP Office to support dialed number identification service (DNIS) on Avaya Contact Center Select.

DNIS is an optional service that Avaya Contact Center Select uses to identify the phone number dialed by the incoming caller. Avaya Contact Center Select uses direct dial-in (DDI) information it receives from IP Office to route calls to appropriate skillsets or agents based on DNIS numbers.

You must also configure DNIS numbers in Contact Center Manager Administration. For more information about configuring DNIS numbers in Contact Center Manager Administration, see *Administering Avaya Contact Center Select*.

Configuring DNIS on IP Office

About this task

A dialed number identification service (DNIS) is an optional service that Avaya Contact Center Select uses to identify the phone number dialed by the incoming caller. Avaya Contact Center Select uses direct dial-in (DDI) information it receives from IP Office to route calls to appropriate skillsets or agents based on DNIS numbers.

To configure DNIS for Avaya Contact Center Select, you must configure an Incoming Call Route number on IP Office that corresponds to an Avaya Contact Center Select DNIS number. You must then add an IP Office short code as a destination for the Incoming Call Route. Each IP Office short code is mapped to an Avaya Contact Center Select CDN (Route Point) number. You can assign multiple DNIS numbers (Incoming Call Routes) to a single Contact Center Route Point number or multiple Contact Center Route Point numbers.

Procedure

1. Using IP Office Manager, select the IP Office server in the **Configuration** pane.
2. In the **Configuration** pane, under the **Solution** node, right-click on **Incoming Call Route** and select **New**.
3. In the right pane, from the **Bearer Capability List** select **Any Voice**.
4. In the **Line Group ID** box, type the Line Group ID number.
5. In the **Incoming Number** box, type the DNIS number.

6. Click the **Destinations** tab.
7. From the **Destination** list, select the IP Office short code you want to assign the DNIS number to.
8. Click **OK**.

Chapter 22: Secure SIP and CTI communication configuration

This section describes how to configure secure SIP and CTI communication between Avaya Contact Center Select (ACCS) and IP Office (IPO).

ACCS uses SIP and custom CTI interfaces to communicate with IPO.

IPO supports Transport Layer Security (TLS) communication for the SIP and CTI connections with ACCS .

TLS is a public key encryption cryptographic protocol that helps secure a communications channel from danger or loss, and thus helps provide privacy and safety. With public key cryptography, two keys are created, one public and one private.

Certificate Authorities (CA) issue and manage server certificates in software security systems that use public key technologies, such as telecoms systems that use Transport Layer Security (TLS) communication.

When you get a signed server certificate and a corresponding root certificate from a CA, you install the certificates on the server system that requested the certificate, for example IP Office. You then install the root certificate into the Trusted Store of the client system(s), for example ACCS. This allows the client systems to request secure communications with the server systems.

Both ACCS and IPO can request secure communications of the other. Therefore, you must generate a Certificate Signing Request (CSR) and get a signed server certificate from a CA on both ACCS and IPO. Both ACCS and IPO must have a root certificate to match the server certificates. When these are in place, IP Office and ACCS can communicate securely using TLS SIP and TLS CTI connections.

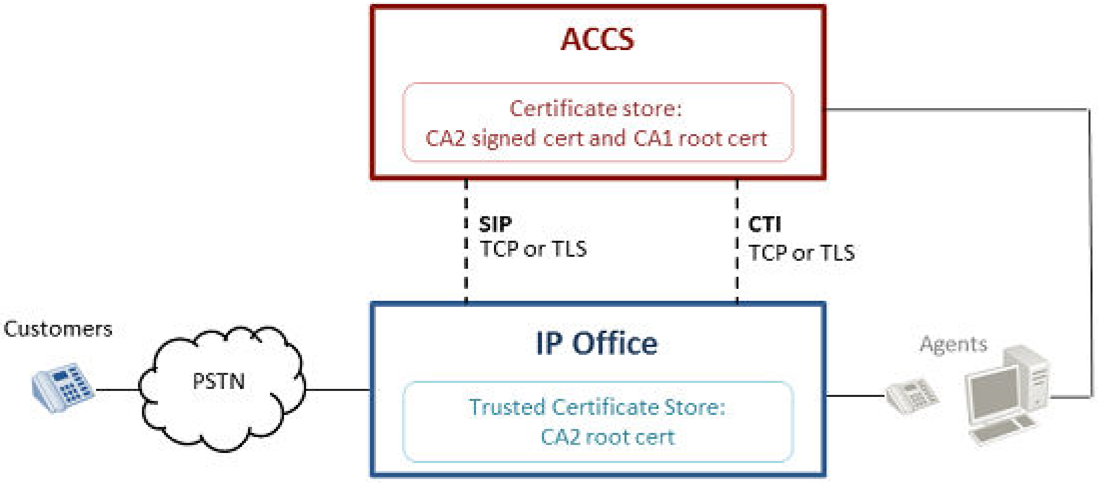


Figure 10: ACCS and IPO secure SIP communication configuration using Certificate Authority

For example, if your IP Office uses Certificate Authority “CA1”, and if ACCS uses a Certificate Authority “CA2”, then:

- The ACCS *Security Store* contains a server certificate supplied and signed by the ACCS Certificate Authority (CA2) and the IP Office Certificate Authority (CA1) root certificate.
- The IP Office *Trusted Security Store* contains the ACCS Certificate Authority (CA2) root certificate.
- IP Office and ACCS can use the same Certificate Authority. Therefore, “CA1” and “CA2” can be the same Certificate Authority.

A server certificate must be signed by a CA; ACCS Security Manager does not sign certificates. Avaya recommends that you use third-party CA or your organization’s Certificate Authority to sign your server certificates.

Certificate Authority deployments vary depending on IT infrastructure and security requirements. You can use either a third party CA, or configure your own CA within your IT infrastructure.

The SIP and CTI links between Avaya Contact Center Select and IP Office use the Transport Layer Security (TLS) protocol to provide secure communication. TLS uses signed security certificates to secure the link between the Avaya Contact Center Select and the IP Office.

The Avaya Contact Center Select Security Manager can request and store these signed security certificates. The ACCS Security Manager generates a Certificate Signing Request (CSR) file. A Certificate Authority uses this Certificate Signing Request file to create a signed certificate. ACCS Security Manager then imports and stores Certificate Authority supplied root certificates and signed certificates.

In ACCS solutions using IP Office and ACCS Business Continuity resiliency, the active and standby Avaya Contact Center Select servers can both have TLS certificates in place to communicate securely with the IP Office server and to support Business Continuity switchover.

Secure SIP and CTI Communication configuration procedures

This task flow shows you the sequence of procedures you perform to configure secure SIP communication between Avaya Contact Center Select and IP Office.

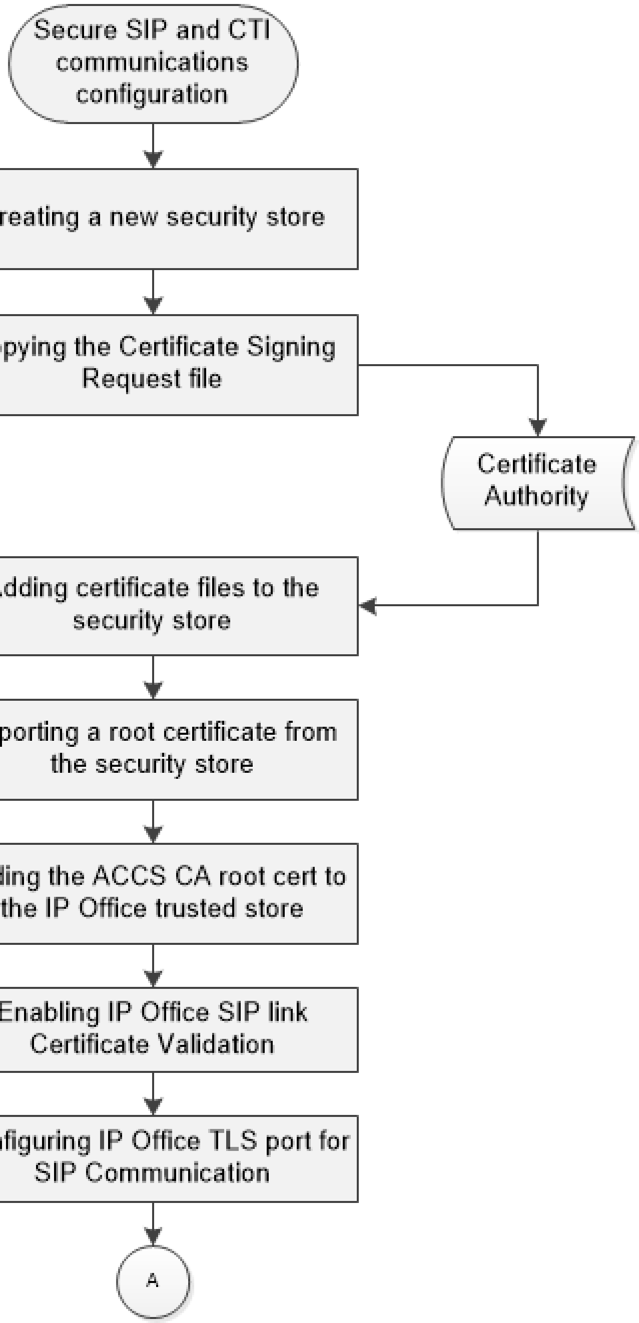

Secure SIP and CTI communications configuration
Creating a new security store
Copying the Certificate Signing Request file
Certificate Authority
Adding certificate files to the security store
Exporting a root certificate from the security store
Adding the ACCS CA root cert to the IP Office trusted store
Enabling IP Office SIP link Certificate Validation
Configuring IP Office TLS port for SIP Communication
A

Figure 11: Configuring secure SIP and CTI communication between ACCS and IPO

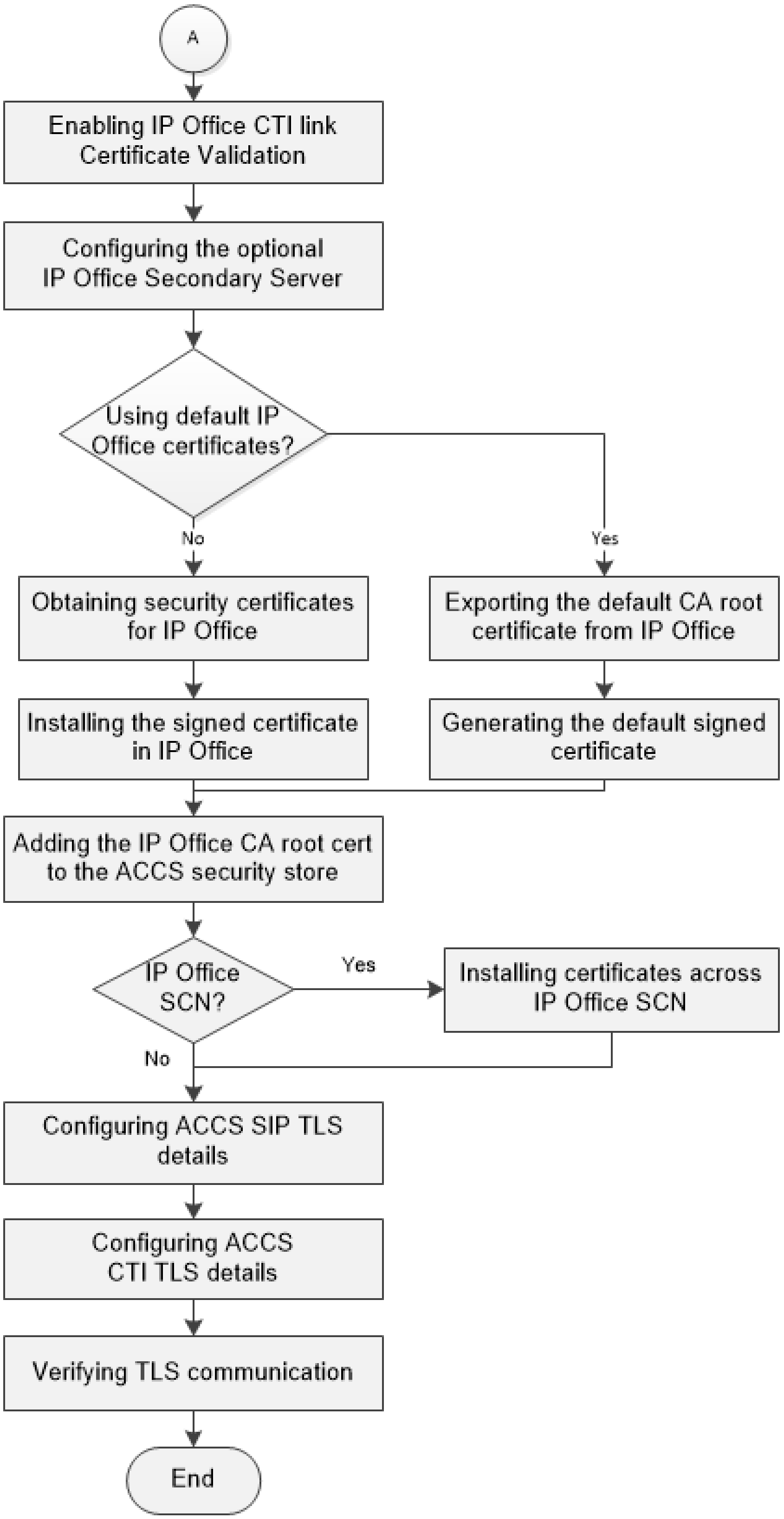

A
Enabling IP Office CTI link Certificate Validation
Configuring the optional IP Office Secondary Server
Using default IP Office certificates?
No
Yes
Obtaining security certificates for IP Office
Exporting the default CA root certificate from IP Office
Installing the signed certificate in IP Office
Generating the default signed certificate
Adding the IP Office CA root cert to the ACCS security store
IP Office SCN?
Yes
Installing certificates across IP Office SCN
No
Configuring ACCS SIP TLS details
Configuring ACCS CTI TLS details
Verifying TLS communication
End

Figure 12: Configuring secure SIP and CTI communication between ACCS and IPO continued

Creating a new security store

About this task

The Security Manager uses a store to hold Certificate Authority root certificates and signed certificates. Create the security store if you plan to use a Certificate Authority and generate signed certificates.

The default encryption setting is SHA2 with a key size of 2048. For backward compatibility, you can choose SHA1 or a key size 1024. However, neither SHA1 nor 1024 provide the industry-recommended level of encryption. If you select one of these values, Contact Center displays a warning message.

If you created a security store at install time using the Ignition Wizard, skip this procedure.

Procedure

1. Log on to the Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. In the **Security Manager** window, select the **Security Store** tab.
4. In the **Security Store** tab, in the **Full Computer Name (FQDN)** box, type the full FQDN of the server on which you are creating the security store.

   ❗ **Important:**

   The FQDN must be the full machine name of the server that the Security Store resides on. The FQDN name is case-sensitive.
5. In the **Name of Organizational unit** box, type the name of the department or division within the company.
6. In the **Name of Organization** box, type the company name.
7. In the **City or Locality** box, type the name of the city or district in which the contact center is located.
8. In the **State or Province** box, type the state or province in which the contact center is located.
9. In the **Two Letter Country Code** box, type the country code in which the contact center is located.
10. In the **Security Store password** box, type a password for accessing the new security store.
11. In the **Confirm Store password** box, confirm the password for accessing the new security store.

    ❗ **Important:**

    Ensure you remember this password, because you will need it the next time you log on to Security Manager. If you forget the password, you will not be able to access Security Manager.

12. If you want to change the encryption setting, select the required encryption settings from the **Encryption Algorithm** and **Key Size** drop-down lists.

    The default value for **Encryption Algorithm** is SHA2 and the default value for **Key Size** is 2048.

    Contact Center displays a warning message if you select SHA1 or 1024. Contact Center includes these values for backward-compatibility only, because these settings do not meet the industry-recommended level of encryption.

13. Click **Create Store**.

    Contact Center creates the private key required for private-public key encryption.

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

    Contact Center automatically backs up the new security store to the folder `D:\Avaya\Contact Center\autoBackUpCertStore`. Do not overwrite or delete this backup location.

14. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Next steps

Send the Certificate Signing Request file to the Certificate Authority, and receive a signed server certificate, so that you can import the server certificate to the security store.

Copying the Certificate Signing Request file

Before you begin

- Speak with your System Administrator to identify a Certificate Authority.

About this task

Security Manager automatically generates a Certificate Signing Request (CSR) when it creates a new security store. The Security Manager—Certificate Request tab displays the name, location, and contents of the Certificate Signing Request (CSR) file on the server. A Certificate Authority uses this Certificate Signing Request (CSR) file to generate a signed server certificate. Contact Center uses the signed server certificate to establish secure communication links with IP Office, the Agent Browser application, and Web Services clients.

Until you add a signed server certificate, the Signing Request Status field shows the CSR status as Pending. When the CSR is signed, and you add it to the security store using the “Add Certificate Tab”, the status changes to “Signed” to indicate that this CSR has been signed.

Procedure

1. Log on to the Contact Center server containing the security store.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.

3. Select the **Certificate Request** tab.
4. Check the **Signing Request Status** value. If this value is **Pending**, you must have the CSR signed by a Certificate Authority.
5. Note the location of the Certificate Signing Request file from **File location**.
6. Select **Logout**.
7. Copy the Certificate Signing Request file from the directory referenced in **File location**, to send to a Certificate Authority.
8. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Next steps

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. Send the Certificate Signing Request file to a Certificate Authority and receive a signed server certificate and root certificate to import into the security store.

Adding certificate files to the security store

Before you begin

- Use the CSR file from the Contact Center Security Manager to obtain a Certificate Authority (CA) signed server certificate and root certificate.
- Save the certificate files on the Contact Center server.

About this task

Contact Center Security Manager can add both CA root certificates and signed server certificates to the security store. Contact Center requires a signed server certificate and a corresponding CA root certificate to communicate using secure services.

There are two options when adding CA root and signed server certificates.

Automatically adding certificates :

You can select a folder that contains signed server and root certificates. Security Manager accesses this folder and automatically determines which are server certificates and which are root certificates and then adds them to the security store accordingly.

Important:

Security Manager attempts to import all files and certificates it finds in the certificate folder. Ensure that the certificate folder contains only CA root certificates and server certificates.

Manually adding certificates :

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

Procedure

1. Log on to the Contact Center server containing the security store.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. On the **Store Access** dialog, type the security store password.
4. Click **OK**.
5. In the Security Manager window, select the **Add Certificate** tab.
6. To add certificates automatically:
    a. Click **Browse**.
    b. On the Select Directory dialog, browse to the directory where you saved the certificate files, and click **Select Directory**.

       Security Manager displays the certificates in the **Certificates** field.
    c. Click **Add all Certificates**.
7. To add certificates manually:
    a. Select **Add Certificates Manually**.
    b. To manually add a CA root certificate, click **Browse**.
    c. Browse to the CA root certificate, and click **Select File**.
    d. Click **Add CA Certificate**.
    e. To manually add a server certificate, click **Browse**.
    f. Browse to the CA signed server certificate, and click **Select File**.
    g. Click **Add Signed Certificate**.

Exporting a root certificate from the security store

About this task

Export the CA root certificate from the Contact Center security store so that clients using secured services can trust the server public key for encryption. Avaya recommends that you always export the root certificate from the security store, so that it is consistent with the current server certificate.

Before you begin

- Add a server certificate and root certificate to the security store.

Procedure

1. Log on to the Contact Center server containing the store.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. On the **Store Access** dialog, type the security store password, and click **OK**.

4. In the Security Manager window, select the **Store Maintenance** tab.
5. In the **Root Certificates** field, select the root certificate that you want to export.
6. Click **Export**.
7. On the Select Directory To Export To dialog, select or create a directory to which you want to export the root certificate.
8. Click **Export To**.

   Security Manager exports two files to the directory. For most clients, use the Security Certificate file. Use the PEM file for Avaya Aura® MS and any client that supports only PEM format.

Next steps

Apply the root certificate to all ACCS clients.

Import the PEM format root certificate to Avaya Aura® MS.

Adding the ACCS CA root certificate to the IP Office trusted store

Before you begin

- For more information about configuring IP Office, refer to IP Office Manager online help and documentation.

About this task

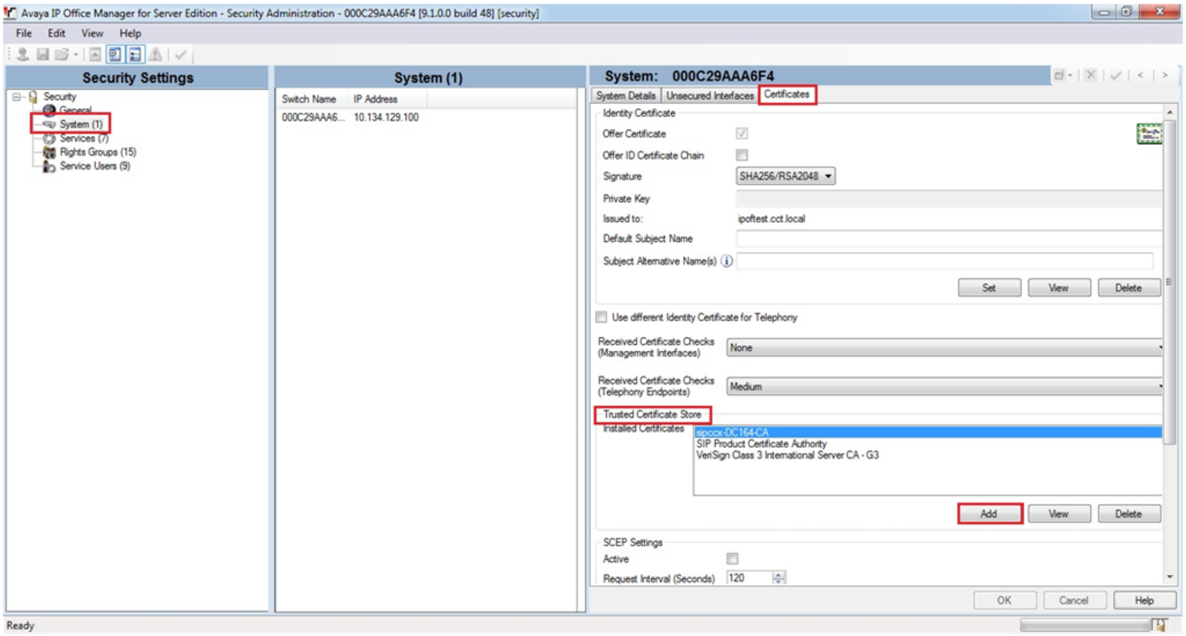
Add the Avaya Contact Center Select Certificate Authority root certificate to the IP Office trusted store.

The security store contains a set of trusted certificates used to evaluate received client certificates. You can install up to 25 X.509v3 certificates.

For more information about the types of certificates supported by IP Office, refer to the IP Office and IP Office Manager documentation.

Procedure

1. Using IP Office Manager, select **File** > **Advanced** > **Security Settings** > **System** > **Certificates**.
2. In the **Trusted Security Store** section, click **Add**.
3. Locate and add the Avaya Contact Center Select Certificate Authority root certificate.



Avaya IP Office Manager for Server Edition - Security Administration - 000C29AAA6F4 [9.1.0.0 build 48] [security]

Security Settings

- Security
  - General
  - System (1)
  - Services (7)
  - Rights Groups (15)
  - Service Users (9)

System (1)

Switch Name	IP Address
000C29AAA6...	10.134.129.100

System: 000C29AAA6F4

System Details | Unsecured Interfaces | Certificates

Identity Certificate

Offer Certificate ☑

Offer ID Certificate Chain □

Signature: SHA256/RSA2048

Private Key

Issued to: ipoftest.cct.local

Default Subject Name

Subject Alternative Name(s)

□ Use different Identity Certificate for Telephony

Received Certificate Checks (Management Interfaces): None

Received Certificate Checks (Telephony Endpoints): Medium

Trusted Certificate Store

Installed Certificates:
sipccx-DC164-CA
SIP Product Certificate Authority
VeriSign Class 3 International Server CA - G3

SCEP Settings

Active □

Request Interval (Seconds): 120

4. Click **OK**.
5. Select **File** > **Save Security Settings**.

Enabling IP Office SIP link certificate validation

Before you begin

- For more information about configuring IP Office, refer to IP Office Manager online help and documentation.

About this task

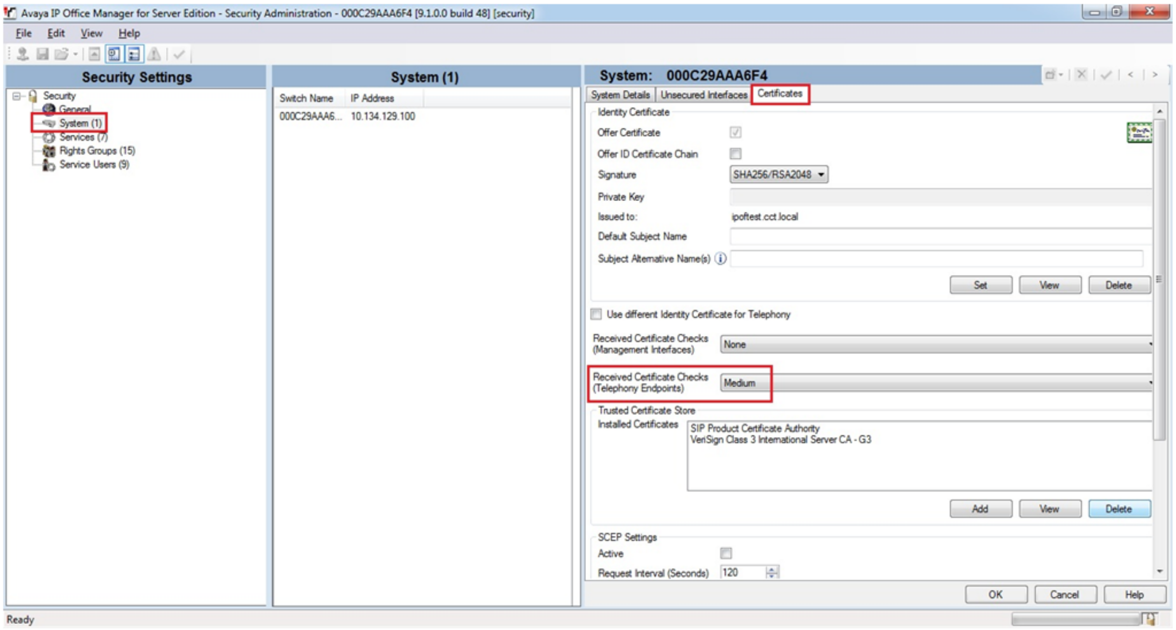
Enable IP Office SIP link certificate validation. When using TLS as the transport protocol for the SIP link, certificate validation must be enabled in IP Office. This configures IP Office to verify that the ACCS certificate is trusted and permits an ACCS TLS SIP connection with IP Office.

Note:

This configuration item is not unique to Avaya Contact Center Select and might have possible impacts on other endpoints configured to use TLS with IP Office.

Procedure

1. Using IP Office Manager, select **File** > **Advanced** > **Security Settings** > **System** > **Certificates**.
2. From the **Received Certificate Checks (Telephony Endpoints)** list, select **Medium**.



Switch Name	IP Address
000C29AAA6...	10.134.129.100

Identity Certificate

Offer Certificate ☑

Offer ID Certificate Chain ☐

Signature SHA256/RSA2048

Private Key

Issued to: ipoftest.cct.local

Default Subject Name

Subject Alternative Name(s)

☐ Use different Identity Certificate for Telephony

Received Certificate Checks (Management Interfaces) None

Received Certificate Checks (Telephony Endpoints) Medium

Trusted Certificate Store

Installed Certificates
SIP Product Certificate Authority
VeriSign Class 3 International Server CA - G3

SCEP Settings

Active ☐

Request Interval (Seconds) 120

3. Click **OK**.
4. Select **File** > **Save Security Settings**.

Configuring the IP Office TLS port for SIP communication

Before you begin

- For more information about configuring IP Office, refer to IP Office Manager online help and documentation.

About this task

Configure the IP Office TLS port used for SIP communication.

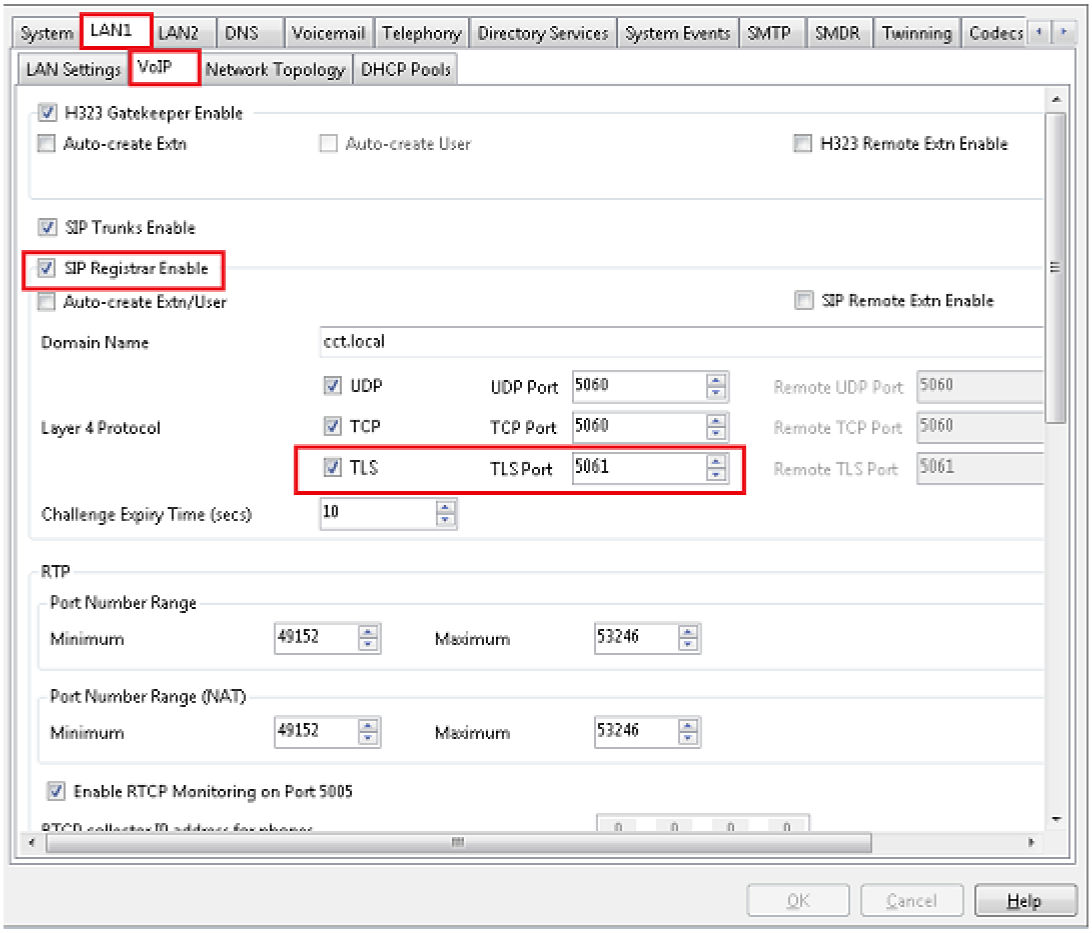
Note:

This configuration item is not unique to Avaya Contact Center Select and might have possible impacts on other endpoints configured to use TLS with IP Office.

Procedure

1. Using IP Office Manager, select the IP Office server in the **Configuration** pane.
2. In the **Configuration** pane, under the IP Office server, select **System**.
3. Select **LAN1** > **VoIP**.
4. In the **SIP Registrar** section, in the **Layer 4 Protocol** area, select **TLS**.

5. Record the TLS Port number. This port number must match the Avaya Contact Center Select TLS port number.



☑ H323 Gatekeeper Enable

□ Auto-create Extn □ Auto-create User □ H323 Remote Extn Enable

☑ SIP Trunks Enable

☑ SIP Registrar Enable

□ Auto-create Extn/User □ SIP Remote Extn Enable

Domain Name: cct.local

Layer 4 Protocol:
☑ UDP UDP Port 5060 Remote UDP Port 5060
☑ TCP TCP Port 5060 Remote TCP Port 5060
☑ TLS TLS Port 5061 Remote TLS Port 5061

Challenge Expiry Time (secs): 10

RTP

Port Number Range: Minimum 49152 Maximum 53246

Port Number Range (NAT): Minimum 49152 Maximum 53246

☑ Enable RTCP Monitoring on Port 5005

RTCP collector IP address for phones: 0 . 0 . 0 . 0

6. Click **OK**.

7. Select **File** > **Save Security Settings**.

Enabling IP Office CTI link certificate validation

Before you begin

- For more information about configuring IP Office, refer to IP Office Manager online help and documentation.

About this task

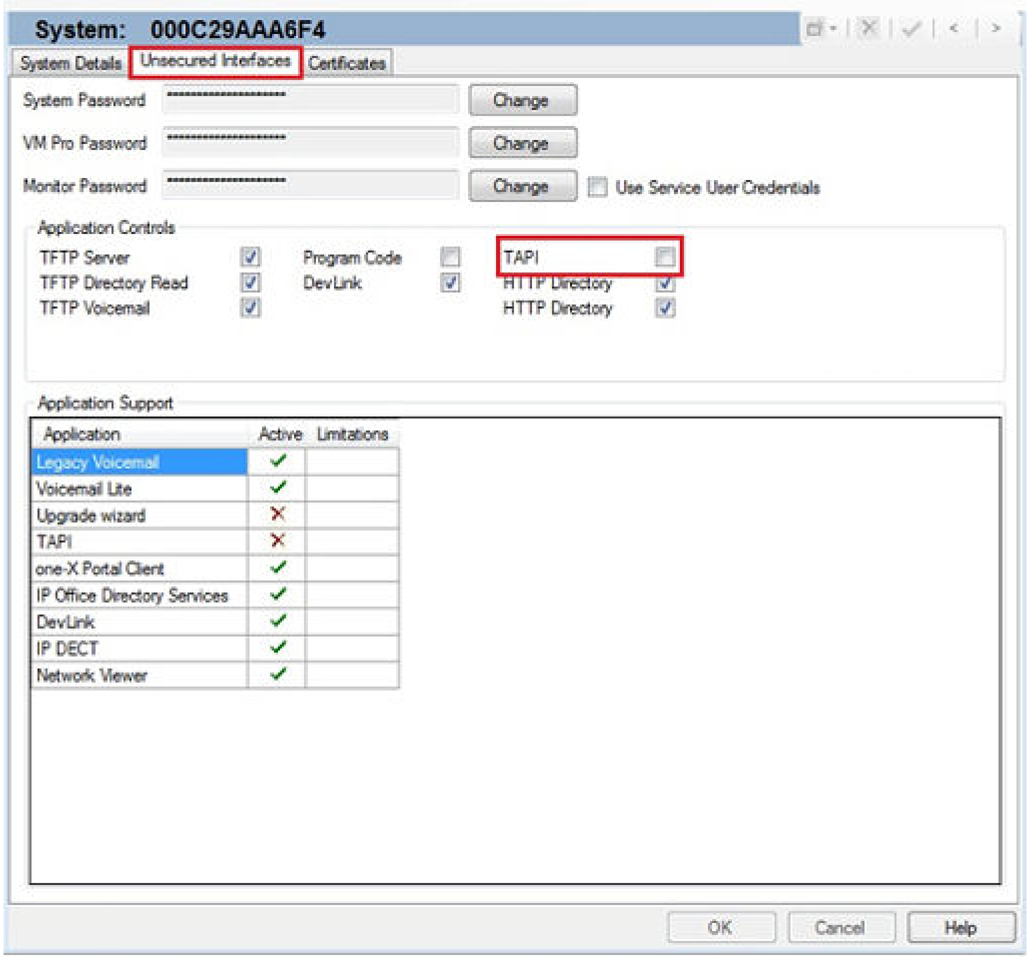
Enable the IP Office CTI link certificate validation. When using TLS as the transport protocol for the CTI link, certificate validation must be enabled in IP Office. This configures IP Office to verify that the Avaya Contact Center Select certificate is trusted and permits an Avaya Contact Center Select TLS CTI connection with IP Office.

Note:

This configuration item is not unique to the Avaya Contact Center Select CTI connection to IP Office. Turning on CTI certificate validation on the Avaya Contact Center Select TAPID link also turns on certificate validation for the TAPI SCN links in an IP Office SCN. For more information, see Installing certificates across IP Office SCN on page 292.

Procedure

1. Using IP Office Manager, select **File** > **Advanced** > **Security Settings** > **System** > **Unsecured Interfaces**.
2. In the **Application Controls** section, clear the **TAPI** check box.



System: 000C29AAA6F4

System Password ******************** Change

VM Pro Password ******************** Change

Monitor Password ******************** Change □ Use Service User Credentials

Application Controls

TFTP Server ☑

TFTP Directory Read ☑

TFTP Voicemail ☑

Program Code □

DevLink ☑

TAPI □

HTTP Directory ☑

HTTP Directory ☑

Application Support

Application	Active	Limitations
Legacy Voicemail	✓	
Voicemail Lite	✓	
Upgrade wizard	✗	
TAPI	✗	
one-X Portal Client	✓	
IP Office Directory Services	✓	
DevLink	✓	
IP DECT	✓	
Network Viewer	✓	

3. Click **OK**.
4. Select **File** > **Save Security Settings**.

Configuring the optional IP Office Secondary Server

Before you begin

- Configure secure TLS communication for the IP Office Primary Server.
- For more information about configuring IP Office, refer to IP Office Manager online help and documentation.

About this task

If your Avaya Contact Center Select solution uses an IP Office Secondary Server, configure TLS communication between Avaya Contact Center Select and the Secondary Server.

Procedure

1. Add the ACCS Certificate Authority root certificate to the IP Office Secondary Server. For more information, see Adding the ACCS CA root certificate to the IP Office trusted store on page 281.
2. Ensure the IP Office Secondary Server uses the a TLS port number that matches ACCS. For more information, see Configuring IP Office TLS port for SIP Communication on page 283.
3. Configure the IP Office Secondary Server to support TLS certificates. For more information, see Enabling IP Office CTI link Received Certificate Checks on page 284.

Exporting the default CA root certificate from IP Office

Before you begin

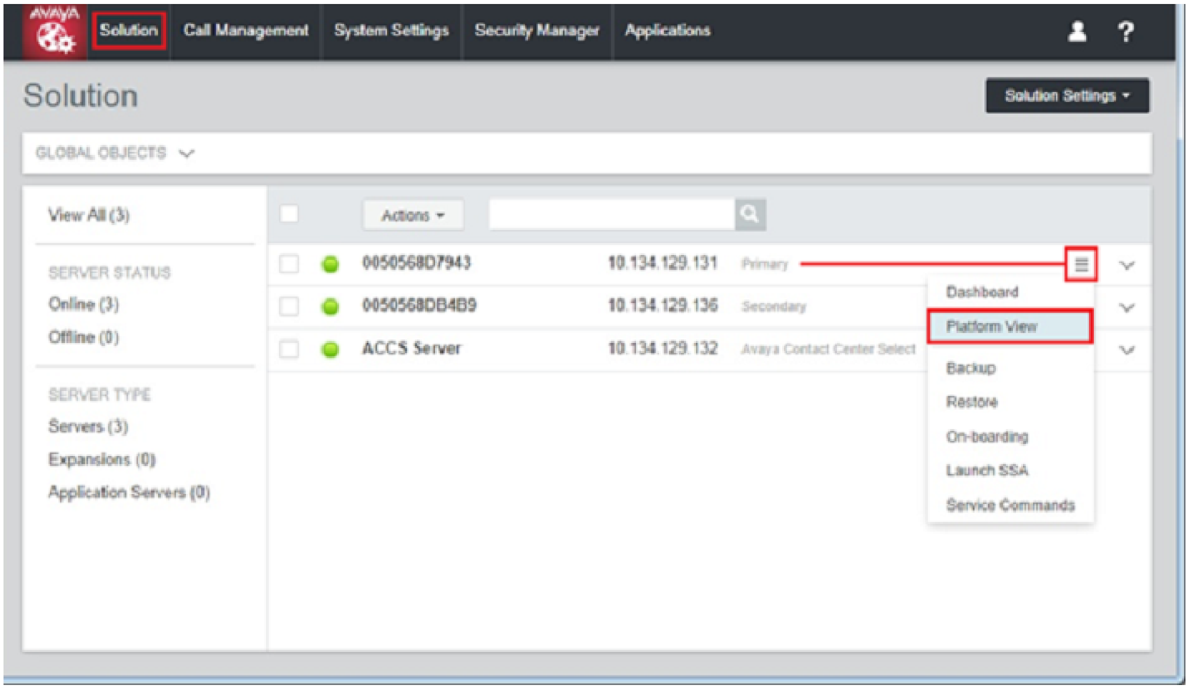
- For more information about configuring IP Office, refer to IP Office Manager online help and documentation.

About this task

Export the default Certificate Authority (CA) root certificate from IP Office.

Procedure

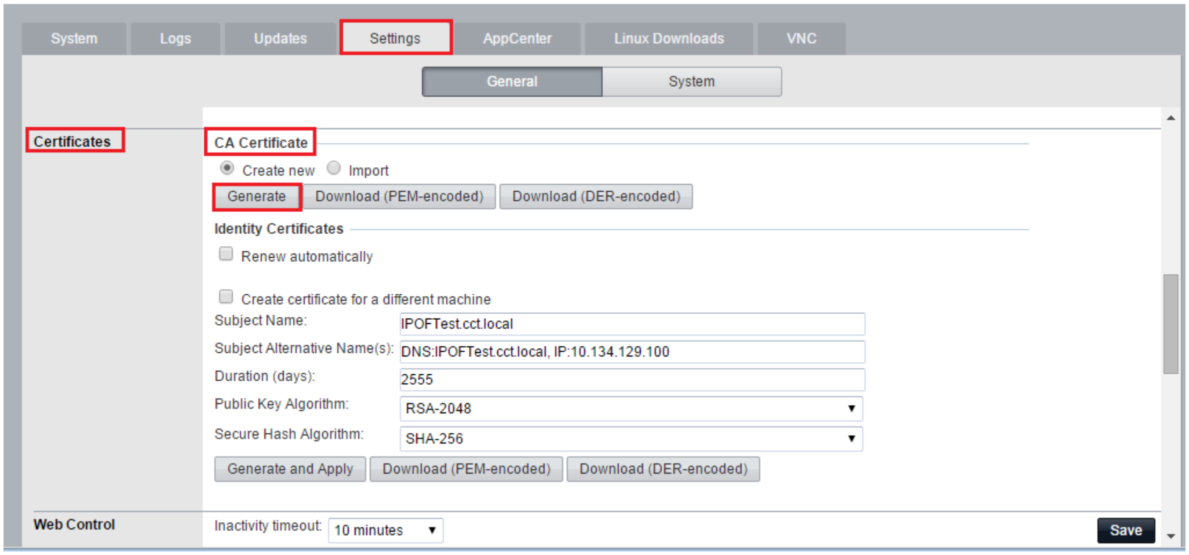
1. Log on to IP Office Web Manager.
2. From **Solution** view, locate the IP Office node that you are configuring, click the **Settings** icon on the right hand side and select **Platform View**.



●	0050568D7943	10.134.129.131	Primary
●	0050568DB4B9	10.134.129.136	Secondary
●	ACCS Server	10.134.129.132	Avaya Contact Center Select

3. Select **Settings** > **General**.
4. Scroll down to the **Certificates** section.
5. In the **CA Certificate** section, click **Download (DER-encoded)** and save the file to a secure location.

   If on clicking **Download (DER0-encoded)** you are shown an error page then it is possible that there is no Certificate Authority configured. If you see an error message, click **Generate** to create a new default CA, and then click **Download (DER-encoded)**.



● Create new ○ Import

□ Renew automatically

□ Create certificate for a different machine

Subject Name: IPOFTest.cct.local

Subject Alternative Name(s): DNS:IPOFTest.cct.local, IP:10.134.129.100

Duration (days): 2555

Public Key Algorithm: RSA-2048

Secure Hash Algorithm: SHA-256

Inactivity timeout: 10 minutes

Next steps

Install this exported IP Office CA root certificate in the Avaya Contact Center Select security store.

Generating the default signed certificate

Before you begin

- For more information about configuring IP Office, refer to the IP Office Manager online help and documentation.

About this task

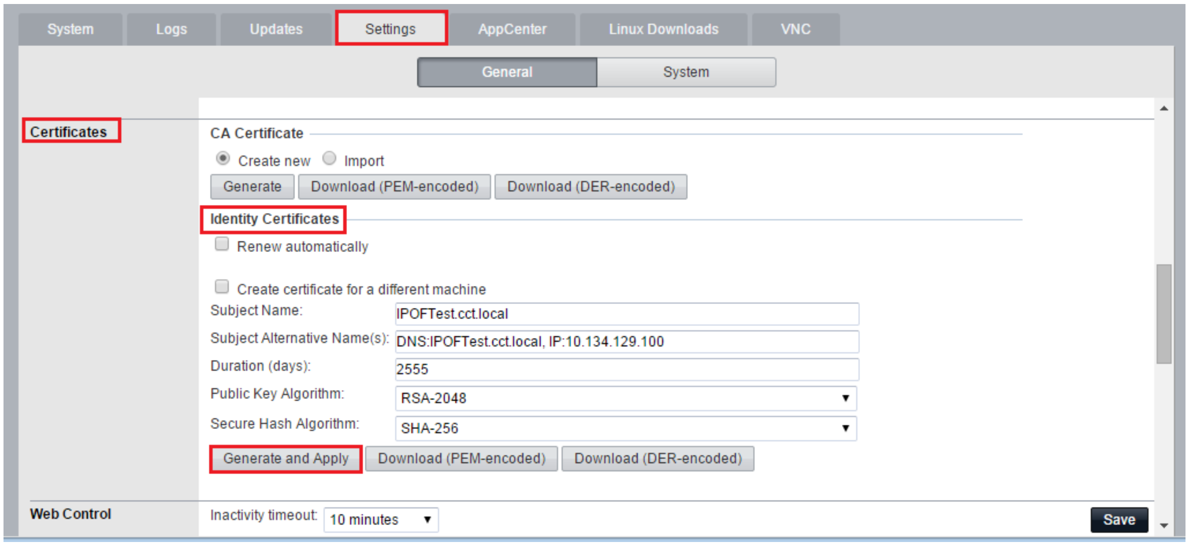
Generate the default signed certificate for IP Office.

When IP Office starts up for the first time, or whenever the identity certificate is deleted, a new identity certificate is created at startup time. This certificate, created at startup time, is not compatible with the TLS communication links on Avaya Contact Center Select. You must create a new identity certificate for IP Office which is compatible with Avaya Contact Center Select.

Procedure

1. Log on to IP Office Web Manager.
2. From the **Solution** view, locate the IP Office node that you are configuring, click the **Settings** icon on the right hand side and select **Platform** View.
3. Select **Settings** > **General**.
4. Scroll to the **Certificates** section.
5. In the **Identity Certificate** section, click **Generate and Apply** to set a new identity certificate for IP Office.

   Note: This is necessary only if a new identity certificate has not yet been applied to IP Office.



CA Certificate

● Create new ○ Import

Identity Certificates

□ Renew automatically

□ Create certificate for a different machine

Subject Name: IPOFTest.cct.local

Subject Alternative Name(s): DNS:IPOFTest.cct.local, IP:10.134.129.100

Duration (days): 2555

Public Key Algorithm: RSA-2048

Secure Hash Algorithm: SHA-256

Inactivity timeout: 10 minutes

Obtaining security certificates for IP Office

About this task

Obtain security certificates for IP Office.

Procedure

Obtain a Certificate Authority root certificate and signed server certificate from your IP Office or corporate Security Prime.

Installing the signed certificate in IP Office

Before you begin

- Obtain security certificates for IP Office.
- For more information about configuring IP Office, refer to IP Office Manager online help and documentation.

About this task

Install the signed certificate in IP Office. When a signed certificate has been generated and the corresponding Certificate Authority (CA) root certificate received from the CA that signed the certificate, then install the signed certificate in IP Office. The CA root certificate is not installed in IP Office. The CA root certificate is installed in the ACCS security store so that ACCS can validate the IP Office signed certificate.

Note:

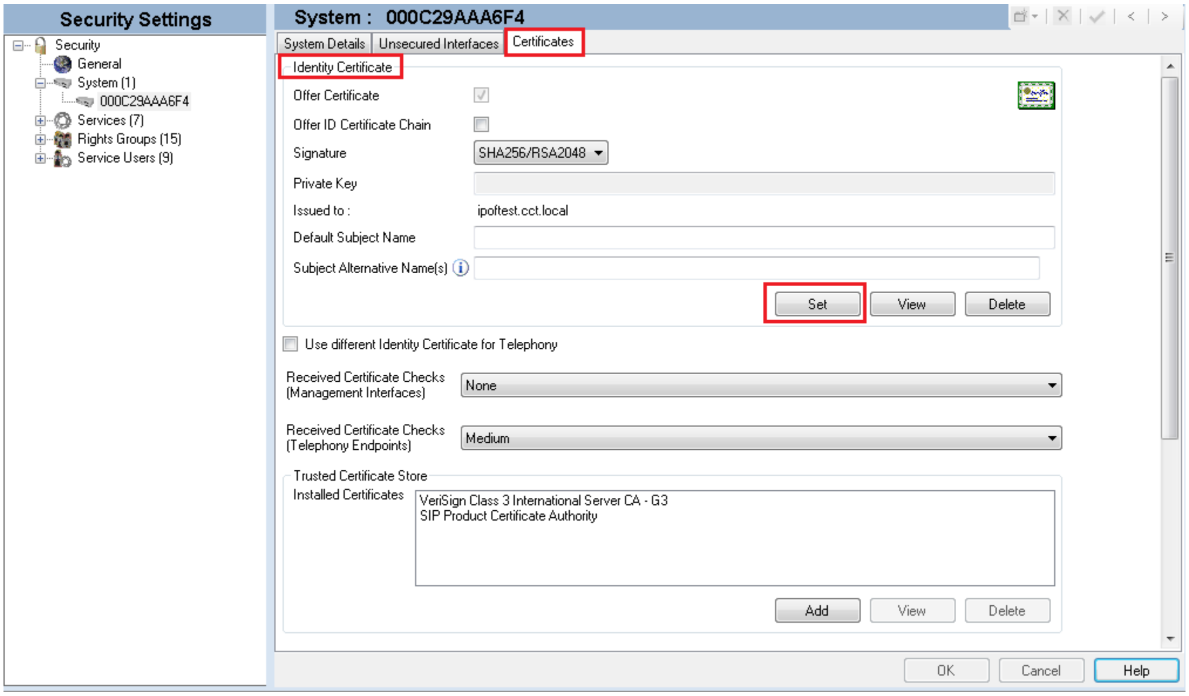
This configuration item is not unique to Avaya Contact Center Select and might have possible impacts on other Management Interfaces and/or Telephony endpoints configured to use TLS with IP Office.

The Identity Certificate is an X.509v3 certificate that identifies the system to a connecting client device such as Avaya Contact Center Select. This certificate is offered in the TLS exchange when the system is acting as a TLS server, which occurs when accessing a secured service.

You can use different certificates for the SIP and CTI link in IP Office. The SIP link falls under the category of Telephony Endpoints while the CTI link falls under the category of Management Interfaces.

Procedure

1. Using IP Office Manager, select **File** > **Advanced** > **Security Settings** > **System** > **Certificates**.
2. In the **Identity Certificate** section, click **Set**.
3. Locate and add the IP Office signed certificate.



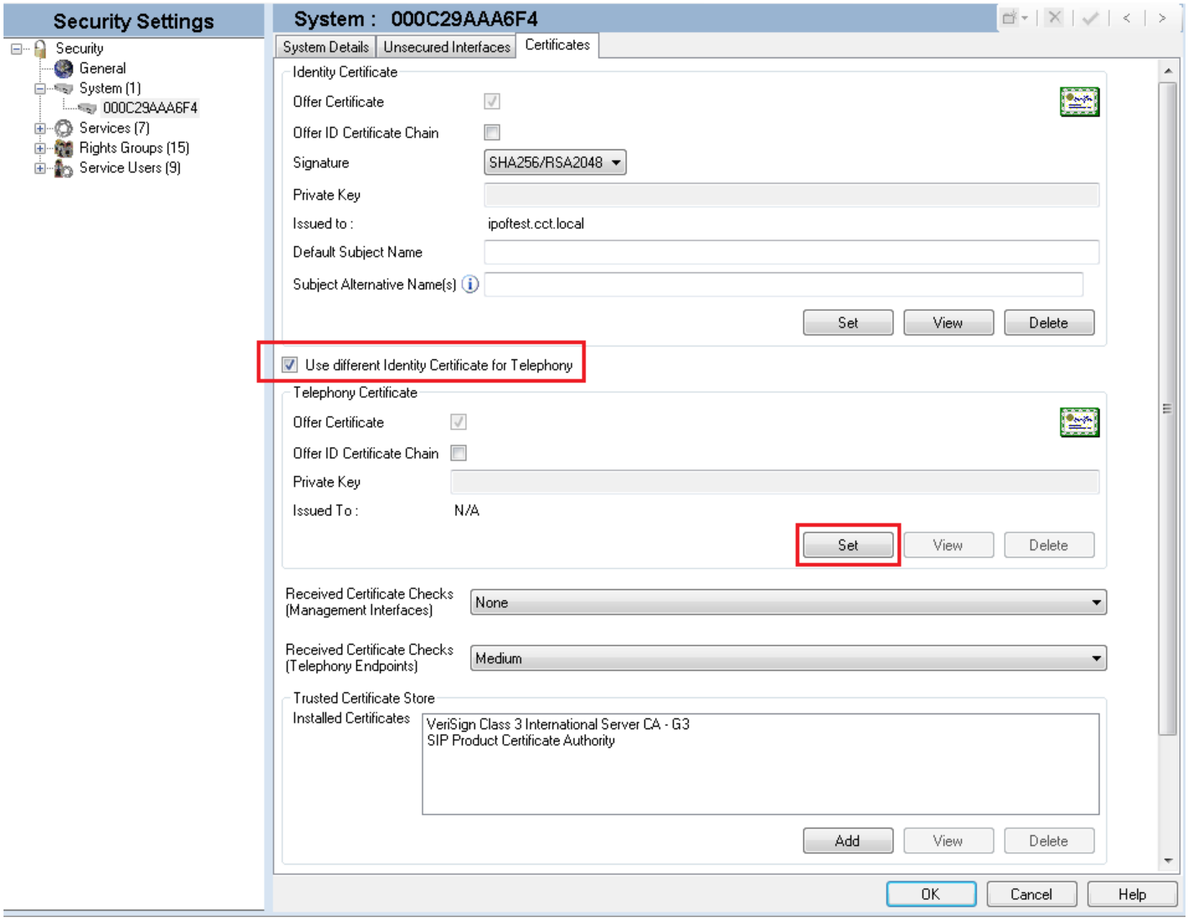
Offer Certificate ☑
Offer ID Certificate Chain □
Signature: SHA256/RSA2048
Private Key
Issued to : ipoftest.cct.local
Default Subject Name
Subject Alternative Name(s)

□ Use different Identity Certificate for Telephony

Received Certificate Checks (Management Interfaces): None
Received Certificate Checks (Telephony Endpoints): Medium

Installed Certificates:
VeriSign Class 3 International Server CA - G3
SIP Product Certificate Authority

4. If you want to use a different signed certificate for the SIP link, click **Use different Identity Certificate for Telephony**.
5. In the **Telephony Certificate** section, click **Set**.
6. Locate and add the IP Office signed certificate to be used for the SIP link.



System : 000C29AAA6F4

Identity Certificate

Offer Certificate ☑

Offer ID Certificate Chain □

Signature: SHA256/RSA2048

Private Key

Issued to : ipoftest.cct.local

Default Subject Name

Subject Alternative Name(s)

☑ Use different Identity Certificate for Telephony

Telephony Certificate

Offer Certificate ☑

Offer ID Certificate Chain □

Private Key

Issued To : N/A

Received Certificate Checks (Management Interfaces): None

Received Certificate Checks (Telephony Endpoints): Medium

Trusted Certificate Store

Installed Certificates:
VeriSign Class 3 International Server CA - G3
SIP Product Certificate Authority

7. Click **OK**.
8. Select **File** > **Save Security Settings**.

Adding the IP Office CA root certificate to the ACCS security store

Before you begin

- Obtain an IP Office Certificate Authority (CA) root certificate. If you are using a custom certificate, see Obtaining security certificates for IP Office on page 289. If you are using the default IPO certificate, see Exporting the default CA root certificate from IP Office on page 286.
- Save the certificate file on the Avaya Contact Center Select (ACCS) server.
- For more information about configuring IP Office (IPO), refer to IP Office Manager online help and documentation.

About this task

Add the IP Office CA root certificate to the ACCS security store so that ACCS can request secure communication with IPO.

Note:

If you used a different CA to generate the signed certificate for the SIP link, you must add that CA root certificate here also.

Procedure

1. Log on to server containing the security store.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. Select **Security Manager**.
4. On the **Store Access** dialog, type the security store password.
5. Click **OK**.
6. In the Security Manager window, select the **Add Certificate** tab.
7. Select **Add Certificates Manually**.
8. To manually add a CA root certificate, click **Browse**.
9. Browse to the IPO CA root certificate, and click **Select File**.
10. Click **Add CA Certificate**.
11. Click **Close**.

Installing certificates across IP Office SCN

Before you begin

- For more information about configuring IP Office, refer to IP Office Manager online help and documentation.
- For more information about configuring an IP Office Small Community Network, refer to IP Office Web Manager online help and documentation.

About this task

A Small Community Network (SCN) is a system of networked IP Office telephone systems that can, among other features, share extension numbers and user names. Each IP Office SCN supports a single connected Avaya Contact Center Select.

If you configure TLS certificate checking for the TAPID CTI link between Avaya Contact Center Select and an IP Office server in an SCN, you must also configure certificate checking for all TAPI links in that SCN. This includes the TAPI SCN links between IP Office nodes in an IP Office SCN environment.

The default certificate generated by each node is not generated from a single root. They are generated from a local Certificate Authority (CA) root on each node and the local CA root certs are not installed in the Trusted Store of any other node on the SCN. So by default the TAPI SCN links might not pass TLS authentication once certificate checking is enabled. To overcome this potential issue you must configure and install signed certificates and CA root certificates across all nodes in the SCN. The procedure describes two methods of doing this.

Procedure

1. **Method 1**: This method is applicable if you are using custom certificates for IP Office. Generate a signed certificate for each node in the SCN from a single CA, deploy the signed certificates to each IP Office node and install the common CA root certificate to the Trusted Store of all nodes in the network. For each IP Office node in the SCN:

    a. Obtain a security certificate and install the signed certificate in IP Office. For more information, see Obtaining security certificates for IP Office on page 289.

    b. Install the certificate on the IP Office node. For more information, see Installing the signed certificate in IP Office on page 289.

    c. Install the CA root certificate that was used to sign the certificate in step (a) in the Trusted Store of the IP Office node. For more information, see Adding the ACCS CA root certificate to the IP Office trusted store on page 281.

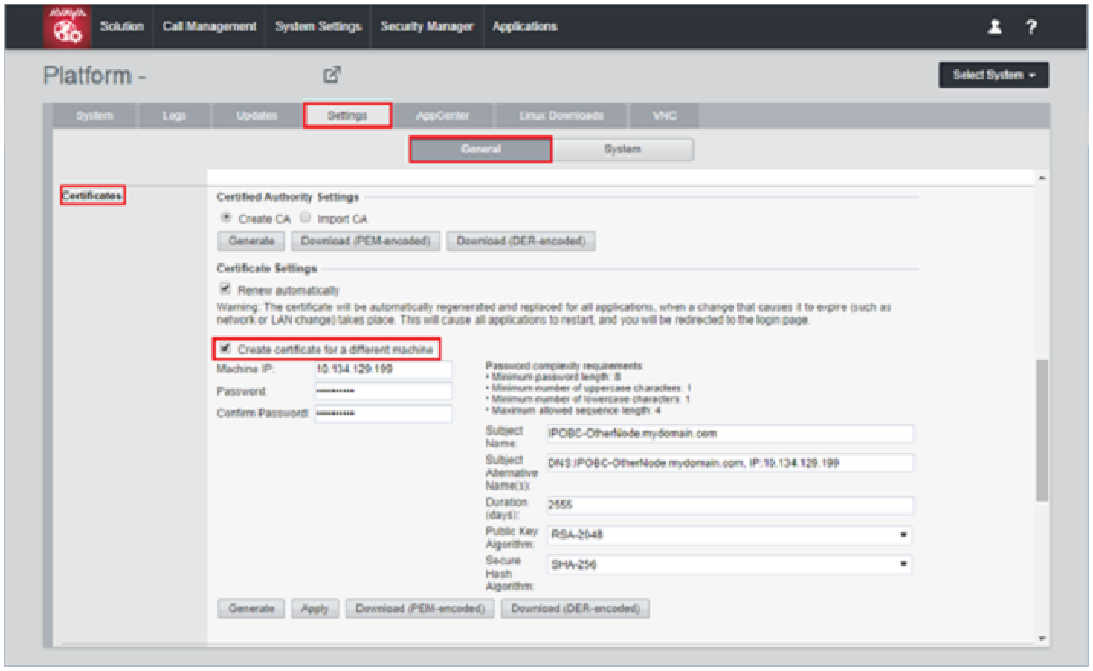
2. **Method 2**: You can use one of the IP Office nodes as the CA server to generate the signed certificates and provide the common CA root certificate. For each IP Office node in the SCN:

    a. Generate a security certificate using IP Office Web Manager. Use the same Web Manager instance to generate all certificates, this ensures a common CA root certificate is used for all certificates.

        - i. Log on to IP Office Web Manager.
        - ii. From **Solution** view, find the IP Office node you are configuring, click the **Settings** icon on the right hand side and select **Platform View**.
        - iii. Select **Settings** > **General** and scroll to the **Certificates** section.
        - iv. Select **Create certificate for a different machine**.
        - v. In the **Machine IP** box, enter the IP address of the IP Office node that the certificate is being generated for.
        - vi. In the **Password** box, enter a password. This password is required later when importing the certificate on the IP Office node. The password must adhere to the password complexity requirements as specified on the **Certificates** user interface.
        - vii. In the **Subject Name** box, enter the FQDN or hostname of the IP Office node that the certificate is being generated for.
        - viii. In the **Subject Alternate Name(s)** box, enter the a string in the following format: “DNS: “ + FQDN (or hostname) + “, IP: ” + ip address.

          For example: “DNS: myserver.mycompany.com, IP: 10.134.120.130”
        - ix. In the **Duration** box, enter the number of days after which the certificate expires.

- x. From the **Public Key Algorithm** list, select **RSA-2048**.
- xi. From the **Secure Hash Algorithm** list, select **SHA-256**.



Certified Authority Settings

● Create CA ○ Import CA

Certificate Settings

☑ Renew automatically

Warning: The certificate will be automatically regenerated and replaced for all applications, when a change that causes it to expire (such as network or LAN change) takes place. This will cause all applications to restart, and you will be redirected to the login page.

☑ Create certificate for a different machine

Machine IP: 10.134.129.199

Password: ••••••••••

Confirm Password: ••••••••••

Password complexity requirements:
• Minimum password length: 8
• Minimum number of uppercase characters: 1
• Minimum number of lowercase characters: 1
• Maximum allowed sequence length: 4

Subject Name: IPOBC-OtherNode.mydomain.com

Subject Alternative Name(s): DNS:IPOBC-OtherNode.mydomain.com, IP:10.134.129.199

Duration (days): 2555

Public Key Algorithm: RSA-2048

Secure Hash Algorithm: SHA-256

- xii. Click **Generate**.
- xiii. On the message box, click on the link and save the certificate with a **.p12** extension.

b. Install this signed certificate on the IP Office node that the certificate was generated for. For more information, see Installing the signed certificate in IP Office on page 289.

c. Export the common CA root certificate. For more information, see Exporting the default CA root certificate from IP Office on page 286.

d. Install the common CA root certificate in the trusted store of the same IP Office node as step (b). For more information, see Adding the ACCS CA root certificate to the IP Office trusted store on page 281.

Configuring Avaya Contact Center Select SIP TLS details

Before you begin

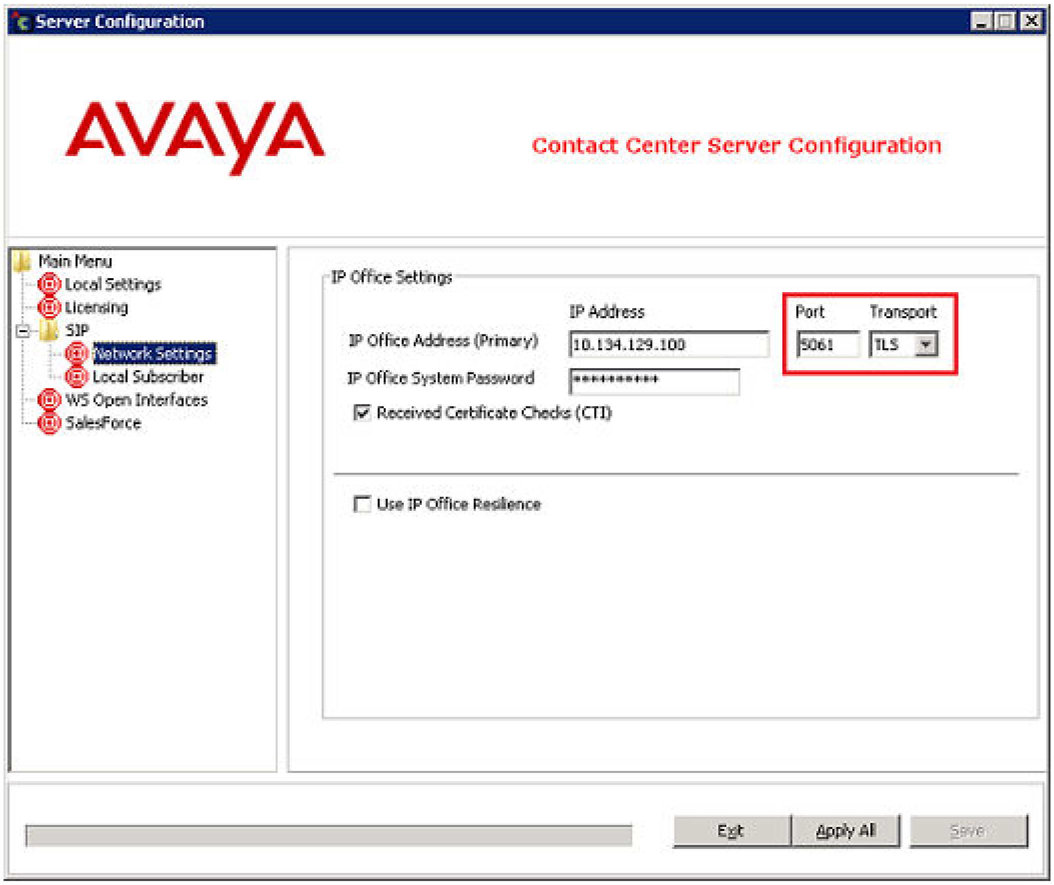
- Know the TLS port number used by IP Office. For more information, see Configuring IP Office TLS port for SIP Communication on page 283.

About this task

Configure Avaya Contact Center Select SIP TLS details.

Procedure

1. Log on to the Avaya Contact Center Select active server.
2. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.
3. In the **Server Configuration** dialog box, under **SIP**, click the **Network Settings** tab.
4. From the **Transport** list, select **TLS**.
5. In the **Port** number box, ensure the configured port number is the same as the TLS port number configured in IP Office.



IP Office Settings

	IP Address	Port	Transport
IP Office Address (Primary)	10.134.129.100	5061	TLS
IP Office System Password	**********		

☑ Received Certificate Checks (CTI)

□ Use IP Office Resilience

6. If your solution has an IP Office Secondary Server, enable **Use IP Office Resilience** and select TLS transport for it and configure the TLS port number to match the IP Office Secondary Server.
7. Click **Apply All**.
8. Click **OK**.

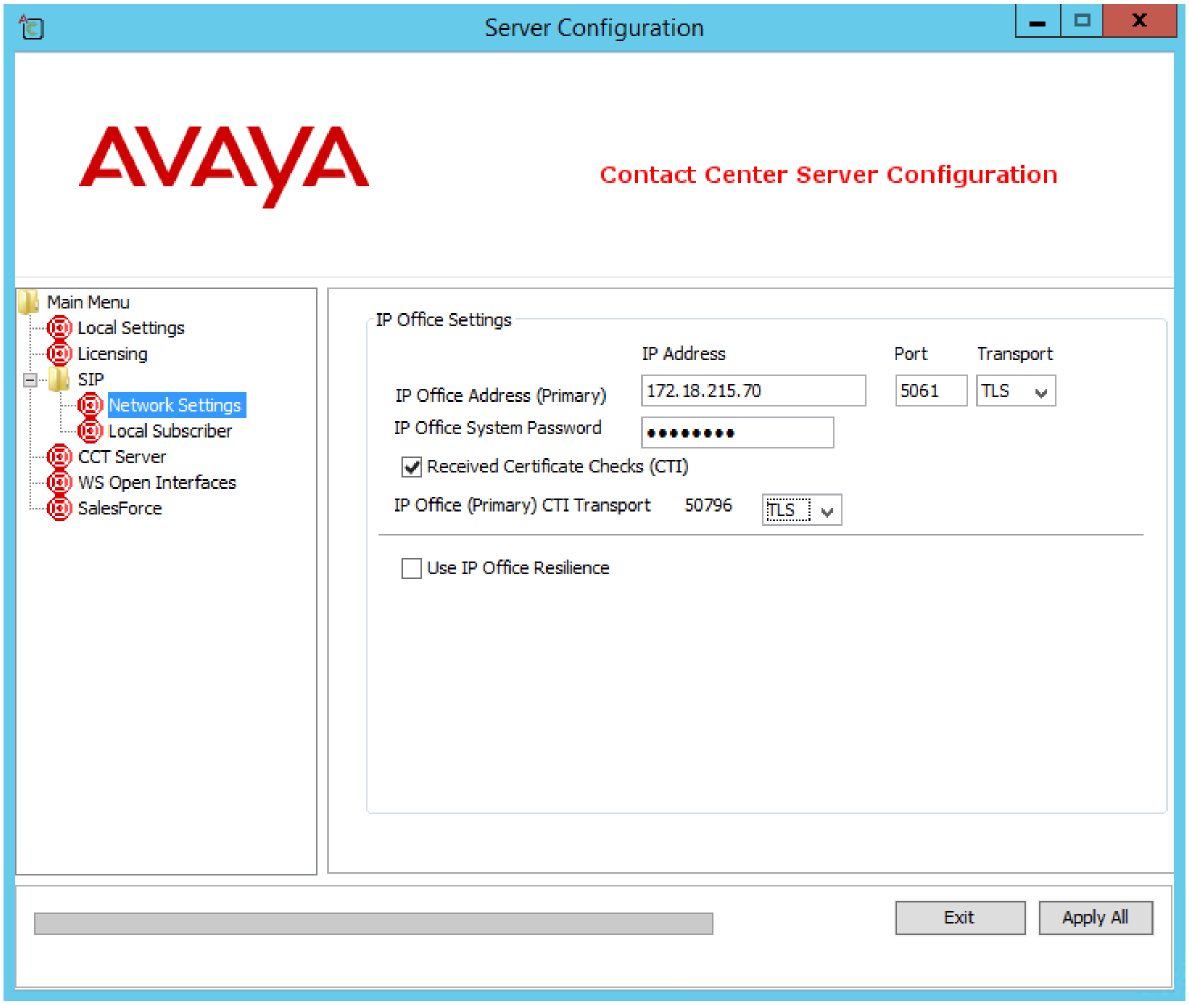
Configuring Avaya Contact Center Select CTI TLS details

About this task

Configure Avaya Contact Center Select to use TLS CTI communication with IP Office, and to support certificates for TLS communication. Avaya Contact Center Select supports both TCP and TLS CTI communication with IP Office.

Procedure

1. Log on to the Avaya Contact Center Select server.
2. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.
3. In the **Server Configuration** dialog box, under **SIP**, click the **Network Settings** tab.
4. Select **Received Certificate Check (CTI)**.
5. From the **IP Office (Primary) CTI Transport** drop-down list, ensure that **TLS** is selected.



IP Office Settings

	IP Address	Port	Transport
IP Office Address (Primary)	172.18.215.70	5061	TLS
IP Office System Password	••••••••		

☑ Received Certificate Checks (CTI)

IP Office (Primary) CTI Transport 50796 TLS

☐ Use IP Office Resilience

6. If your solution has an IP Office Secondary Server, enable **Use IP Office Resilience** and in the IP Office Secondary Server section, select **Received Certificate Check (CTI)** and ensure that **TLS** is selected from the **IP Office (Primary) CTI Transport** drop-down list.
7. Click **Apply All**.
8. Click **OK**.
9. Click **Exit**.

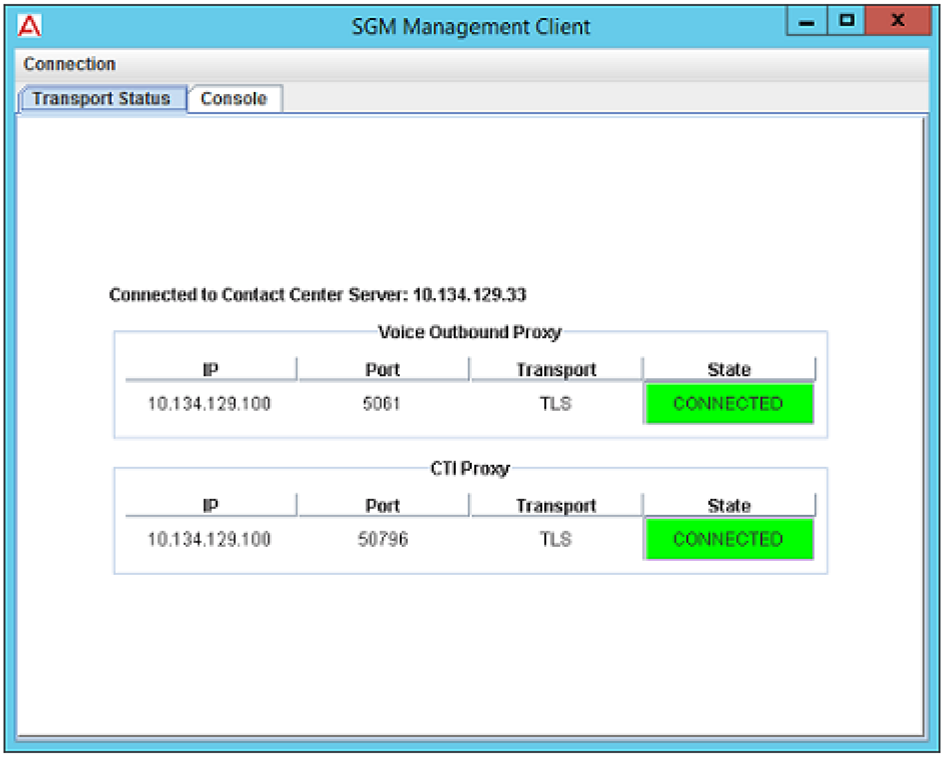
Verifying TLS communication

About this task

Verify the TLS communication between Avaya Contact Center Select and IP Office.

Procedure

1. Log on to the Avaya Contact Center Select server.
2. On the **Apps** screen, in the **Avaya** section, select **SIP Gateway Management Client**.
3. Select the **Transport Status** tab.



Connected to Contact Center Server: 10.134.129.33

Voice Outbound Proxy

IP	Port	Transport	State
10.134.129.100	5061	TLS	CONNECTED

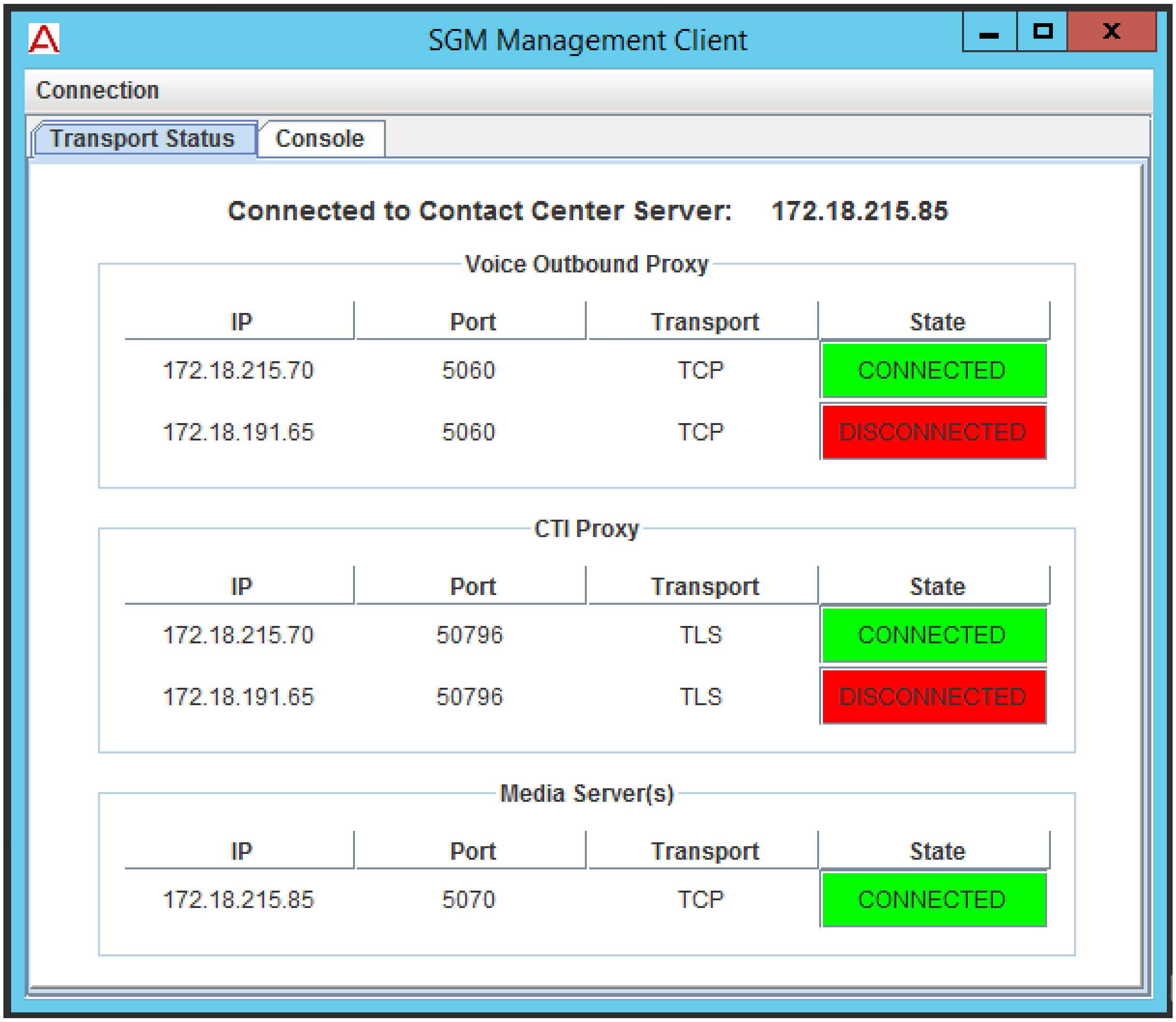
CTI Proxy

IP	Port	Transport	State
10.134.129.100	50796	TLS	CONNECTED

4. Verify that the **Voice Outbound Proxy** link **Transport** setting is **TLS** and that the link status is **CONNECTED**.

5. Verify that the **CTI Proxy** link **Transport** setting is **TLS** and that the link status is **CONNECTED**.

6. If your solution uses an IP Office Secondary Server, verify that the links to the Secondary Server use TLS. Avaya Contact Center Select connects to one IP Office at a time, so only one set of links can be **CONNECTED** at a time.



Connected to Contact Center Server: 172.18.215.85

Voice Outbound Proxy

IP	Port	Transport	State
172.18.215.70	5060	TCP	CONNECTED
172.18.191.65	5060	TCP	DISCONNECTED

CTI Proxy

IP	Port	Transport	State
172.18.215.70	50796	TLS	CONNECTED
172.18.191.65	50796	TLS	DISCONNECTED

Media Server(s)

IP	Port	Transport	State
172.18.215.85	5070	TCP	CONNECTED

Chapter 23: Administering security

Avaya Contact Center Select (ACCS) includes a number of services and connections that you can secure using Transport Layer Security (TLS). You can use the Ignition Wizard to create a security store, generate a Certificate Signing Request (CSR) and import a Certificate Authority root certificate. Use the procedures in this chapter to administer Web Services security, including turning on security, backing up the security store, and modifying the security store inspection tasks.

The following Web services use the security store to implement HTTPS:

- Contact Center Manager Administration (CCMA)
- Contact Center Multimedia (CCMM) Administration
- Agent Desktop
- Multimedia Services
- Orchestration Designer
- Outbound Campaign Management Tool
- Agent Browser application

ACCS security store

ACCS includes a security store for securing both SIP communications and Web services. When you configure the ACCS security store for SIP communications, it is ready for securing Web services.

The ACCS security store includes a server certificate and root certificate. ACCS also uses the Internet Information Services (IIS) security store for some services.

Security Manager

Security Manager provides an interface for managing the security certificates in the ACCS security store and the IIS security store. ACCS supports the management of the IIS security store only through Security Manager: do not use IIS functions to manage the IIS security store on a ACCS server. Security Manager supports importing chained certificates, and places these certificates in the security store for distribution across the solution.

Supported TLS versions

Contact Center defaults to using only TLS 1.2 for secured services and connections. For backward compatibility, Contact Center supports Administrators changing the minimum TLS version that Contact Center can negotiate with other systems. This is to inter-operate with legacy systems that do not support TLS 1.2. You can set minimum TLS versions separately for the following connections:

- SIP signaling
- CCMA and CCMM administration

- Event Broker Web service (this setting also sets the minimum TLS version used for Web Statistics)

If you change the CCMA and CCMM administration setting, the configuration applies the Windows Server 2012 TLS settings, and affects all applications on the server that use Windows Server 2012 secure communications technology.

When the Contact Center configuration is for a TLS version lower than 1.2, Contact Center still attempts to negotiate the highest (and most secure) version first, before stepping down to a lower (and less secure) version.

Avaya recommends that you maintain the TLS version settings at the highest possible TLS version, and that you change these settings only when it is certain that parts of your overall contact center solution do not work with the higher TLS version.

ACCS Business Continuity

In a Business Continuity (BC) system, the security stores must use Subject Alternative Names (SANs). Include a SAN for the Managed name and the server name. This ensures clients connecting to ACCS using the managed name do not get warnings that the signed certificate name does not match the server name.

Certificate Authority root certificates

When a client initiates a secure connection with a server, it must have a root certificate from the CA that provided the server signed certificate. If the client does not have a matching root certificate, it does not complete the connection. If the client has a root certificate from a CA, it can trust any server certificate signed by that CA.

To secure the ACCS Web services, you must export the root certificate from Security Manager, and import it into all the ACCS clients (CCMA clients and Agent Desktop computers).

Avaya recommends that you use a single CA to sign all the certificates in your contact center. This greatly simplifies the deployment process, because you need to distribute only a single root certificate to all the clients. If you want to use different CAs to sign certificates for your different servers, you must copy the root certificate from each CA to all the clients in your contact center.

For some Web services, servers can act as clients of other servers. Therefore you must ensure that all servers also have the required CA root certificate(s).

Offline Store

You can create an offline store using Security Manager, which minimizes downtime if you want to replace your current security store. When your offline store is created, you can swap between the active store and the offline store. You can make the offline store the active store at any point using Security Manager. You must stop Contact Center services before making the offline store active.

Security Store notifications

Security certificates contain an expiration date and they are not valid after this date. If the security certificates used by ACCS expire, the contact center loses call control and stops functioning.

Security Manager provides a security store inspection utility to help you monitor and maintain valid security certificates. You can use Security Manager to schedule a security store inspection task. Security Manager adds the scheduled task to the underlying Windows Task Scheduler. The scheduled task runs the security store inspection utility once a week. The inspection utility checks the status of the security certificates in the ACCS security store. If any of the security certificates are due to expire within a month, the inspection utility sends a notification email to the contact center administrator. The contact center administrator must then refresh the security certificates.

Security Manager provides the notification email; it cannot renew expired security certificates. For uninterrupted contact center functionality, if you receive an email about upcoming certificate expiration dates, you must renew the security certificates before they expire.

Security Manager uses the Microsoft Windows Task Scheduler to schedule the weekly security store inspection. You must ensure that there is a Microsoft Windows user account that has the necessary privileges from which Security Manager can schedule a task on Windows Task Scheduler. You can use the Windows administrator account that you used to install ACCS to add a task to Windows Task Scheduler.

Security Manager uses a specified Simple Mail Transport Protocol (SMTP) server to send the notification emails to the administrator's email address. ACCS does not provide this SMTP server. You must provision this SMTP server and ensure that the ACCS server can communicate with it at all times. ACCS does not support Secure Sockets Layer (SSL) connectivity to this SMTP server.

Server Message Block signing on Windows Server 2012

Both the Contact Center DVD and the Release Pack installer modify the Windows Server 2012 local group policy to enable Server Message Block (SMB) signing. SMB signing places a digital "tag" into each server message block, which helps prevent man-in-the-middle attacks on network file sharing.

If you do not want to use SMB signing, you can disable it by modifying the Windows Server 2012 local group policy.

Exporting a root certificate from the security store

About this task

Export the CA root certificate from the Contact Center security store so that clients using secured services can trust the server public key for encryption. Avaya recommends that you always export the root certificate from the security store, so that it is consistent with the current server certificate.

Before you begin

- Add a server certificate and root certificate to the security store.

Procedure

1. Log on to the Contact Center server containing the store.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. On the **Store Access** dialog, type the security store password, and click **OK**.
4. In the Security Manager window, select the **Store Maintenance** tab.
5. In the **Root Certificates** field, select the root certificate that you want to export.
6. Click **Export**.
7. On the Select Directory To Export To dialog, select or create a directory to which you want to export the root certificate.

8. Click **Export To**.

   Security Manager exports two files to the directory. For most clients, use the Security Certificate file. Use the PEM file for Avaya Aura® MS and any client that supports only PEM format.

Next steps

Apply the root certificate to all ACCS clients.

Import the PEM format root certificate to Avaya Aura® MS.

Applying the root certificate to a Contact Center client

About this task

Copy the root certificate exported from the Contact Center security store to the Contact Center clients and servers that use secure services. If you have a large number of clients, you can use automated methods to distribute and apply the root certificates. For example, you can use a Group Policy to distribute root certificates to clients using supported Microsoft Windows operating systems.

This procedure shows how to manually apply a root certificate on a Microsoft Windows operating system.

Before you begin

- Add a signed certificate and root certificate to the security store.
- Export the root certificate from the security store.

Procedure

1. On the client operating system Desktop, click **Start** > **Run**.
2. Type `MMC`, and click **OK**.
3. Select Click **File** > **Add/Remove Snap In**.
4. From the **Available snap ins** list, select **Certificates**, and click **Add**.
5. On the Certificates Snap in dialog, select **Computer account**, and click **Next**.
6. Click **Finish**.
7. On the Add or Remove Snap-ins dialog, click **OK**.
8. In the console root, expand **Certificates (Local Computer)** and then expand **Trusted Root Certification Authorities**.
9. Right-click the **Certificates** folder.
10. Select **All Tasks** > **Import**.
11. On the Certificate Import Wizard dialog, click **Next**.
12. Click **Browse**, and browse to the location where you copied the root certificate file.

13. Select the root certificate file and click **Open**.
14. On the Certificate Import Wizard dialog, click **Next**.
15. Click **Next**.
16. When the Certificate Import Wizard finishes importing the certificate, click **Finish**.

Importing the Contact Center root certificate into Avaya Aura® MS

Before you begin

- Export the root certificate from the Contact Center security store.

About this task

Import the Contact Center root certificate into the Avaya Aura® MS trust store to support Transport Layer Security (TLS) communications.

Procedure

1. Log on to Avaya Aura® MS Element Manager.
2. Navigate to **EM** > **Security** > **Certificate Management** > **Trust Store**.
3. Click **Import**.
4. In the **Trust friendly name** field, type a friendly name for the CA root certificate.
5. Click **Browse**.
6. Select the root certificate file that you exported from the Contact Center security store.
7. Click **Save**.

Creating an offline store

Before you begin

- Ensure that a security store already exists.

About this task

Create an offline security store if you want to replace the existing active security store, and minimize downtime. The procedure to create an offline store is the same as creating an active security store.

Security Manager uses a store to hold Certificate Authority root certificates and signed certificates. Create the security store if you plan to use a Certificate Authority and generate signed certificates.

The default encryption setting is SHA2 with a key size of 2048. For backward compatibility, you can choose SHA1 or a key size 1024. However, neither SHA1 nor 1024 provide the industry-recommended level of encryption. If you select one of these values, Contact Center displays a warning message.

You cannot make any security configuration changes in Security Manager while you are viewing the offline store.

Procedure

1. Log on to the Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. In the **Security Manager** window, click **Store Commands** > **Create Offline Store**.
4. In the **Security Store** tab, in the **Full Computer Name (FQDN)** box, type the full FQDN of the server on which you are creating the security store.

   Important:

   The FQDN must be the full machine name of the server that the Security Store resides on. The FQDN name is case-sensitive.
5. In the **Name of Organizational unit** box, type the name of the department or division within the company.
6. In the **Name of Organization** box, type the company name.
7. In the **City or Locality** box, type the name of the city or district in which the contact center is located.
8. In the **State or Province** box, type the state or province in which the contact center is located.
9. In the **Two Letter Country Code** box, type the country code in which the contact center is located.
10. In the **Security Store password** box, type a password for accessing the new security store.
11. In the **Confirm Store password** box, confirm the password for accessing the new security store.

    Important:

    Ensure you remember this password, because you will need it the next time you log on to Security Manager. If you forget the password, you will not be able to access Security Manager.
12. If you want to change the encryption setting, select the required encryption settings from the **Encryption Algorithm** and **Key Size** drop-down lists.

    The default value for **Encryption Algorithm** is SHA256 and the default value for **Key Size** is 2048.

Contact Center displays a warning message if you select SHA1 or 1024. Contact Center includes these values for backward-compatibility only, because these settings do not meet the industry-recommended level of encryption.

13. Click **Create Store**.

    Contact Center creates the private key required for private-public key encryption.

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

    Contact Center automatically backs up the new security store to the folder `D:\Avaya\Contact Center\OfflineAutoBackUpCertStore`. Do not overwrite or delete this backup location.

14. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Switching between the active and offline security stores

About this task

When an active and offline security store exist, you can view either store without any impact to Contact Center operation. Security Manager displays a message indicating which store you are currently viewing. You cannot make configuration changes to the offline security store.

Before you begin

- Ensure that an active and offline security store already exist.

Procedure

1. Log on to the Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. In the **Security Manager** window, click **Store Commands** > **View**.

   Depending on which store you are currently viewing, you can choose to view the other security store. Security Manager displays a message indicating which store you are currently viewing.

Making an offline store active

About this task

When the offline security store is ready to be placed into production, you can activate the offline store using Security Manager.

Note:

You must restart the Contact Center server after activating the offline store.

Before you begin

- Ensure that an active and offline security store already exist.
- Stop Contact Center services.

Procedure

1. Log on to the Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. In the **Security Manager** window, click **Store Commands** > **View** > **Offline Store**.
4. In the **Security Manager** window, click the **Make Active** button.
5. Click **Confirm** to apply the new security settings and activate the offline store.

   A message appears under **Store Status** to indicate that the Make Active operation was successful. The offline security store is now the new active security store. The old active security store is now the offline store.
6. Restart the Contact Center server.

Next steps

After restarting the Contact Center server, verify the configuration settings for the new active security store using the **Security Configuration** tab in Security Manager.

Turning on Web Services security

About this task

Turn on Web Services security if you want to use HTTPS security for management and agent operations.

Before you begin

- Read the security section of *Avaya Contact Center Select Solution Description*.
- Create a new security store and import the signed server certificate and root certificate from the CA.
- Export the CA root certificate from the security store, and apply it to all the CCMA and Agent Desktop clients in the contact center.

Procedure

1. Log on to the server as a local administrator.

Important:

If you log on to the server as a domain administrator, this procedure does not complete successfully.

2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. On the Store Access dialog, type the password for the security store, and click **OK**.
4. On the Security Manager screen, select the **Security Configuration** tab.
5. Click **Security On**.
6. Click **Apply**.
7. On the Security Change Confirmation dialog, click **Confirm**.
8. Click **Log Out**.

Next steps

Configure the IPO data synchronization user account to match the Web Services security settings. For more information, see Changing the data synchronization user account to match Web Services security settings on page 308.

Instruct all users in the contact center to use `https` instead of `http` when connecting to the server from CCMA clients or Agent Desktop.

Configuring the minimum TLS version

About this task

Configure minimum TLS versions that Contact Center can negotiate for secure connections. This enables third-party and legacy systems that do not support TLS 1.2 to communicate securely with Contact Center. If you do not change these settings, Contact Center uses only TLS 1.2, and does not connect to systems that support only lower versions of TLS.

You can set minimum TLS versions separately for the following communications:

- SIP and CTI signaling
- CCMA and CCMM administration
- Event Broker Web service
- Web statistics (this setting also sets the minimum TLS version used for Web Statistics)

Before you begin

- Read the security section of *Avaya Contact Center Select Solution Description*.
- Create a new security store and import the signed server certificate and root certificate from the CA.

Procedure

1. Log on to the server as a local administrator.

> **Important:**
>
> If you log on to the server as a domain administrator, this procedure does not complete successfully.

2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. On the Store Access dialog, type the password for the security store, and click **OK**.
4. On the Security Manager screen, select the **Security Configuration** tab.
5. In the **SIP and CTI Signalling Level** box, select the lowest version of TLS for SIP and CTI signaling communication.

   In addition to the SIP signaling level, this also controls the TLS protocol version used for the TAPID CTI link between Avaya Contact Center Select and IP Office.
6. In the **CCMA — Multimedia Web Service Level** box, select the lowest version of TLS for CCMA and Multimedia Web service communication.

   This changes the setting for IIS, and for Windows Server 2012 generally.
7. In the **Event Broker Web Service Level** box, select the lowest version of TLS for Event Broker Web Service communication.
8. Click **Apply**.
9. Click **Log Out**.

Changing the data synchronization user account to match Web Services security settings

About this task

Change the configuration of the data synchronization user account to match the Web Services security configuration. If you turn on Web Services security, the URL prefix must be https, and if you turn off Web Services security it must be http.

Procedure

1. Using IP Office Manager, select the IP Office server in the **Configuration** pane.
2. In the **Configuration** pane, under the IP Office server, select **System**.
3. Select the **Contact Center** tab.
4. In the **CCMA Address** box, type the address of the Avaya Contact Center Select server.

   If you turned on Web Services security, type `https://<ACCS server IP Address>`.

   If you turned off Web Services security, type `http://<ACCS server IP Address>`.
5. Click **OK**.

Turning off Web Services security

About this task

Turn off Web Services security if you want to stop using the feature.

Before you begin

- Read the security section of *Avaya Contact Center Select Solution Description*.

Procedure

1. Log on to the server as a local administrator.

   ❗ **Important:**

   If you log on to the server as a domain administrator, this procedure does not complete successfully.

2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. On the Store Access dialog, type the password for the default security store, and click **OK**.
4. On the Security Manager screen, select the **Security Configuration** tab.
5. Click **Security Off**.
6. Click **Apply**.
7. On the Security Change Confirmation dialog, click **Confirm**.
8. Click **Log Out**.

Next steps

Configure the IPO data synchronization user account to match the Web Services security settings. For more information, see Changing the data synchronization user account to match Web Services security settings on page 308.

Instruct all users in the contact center to use `http` instead of `https` when connecting to the server from CCMA clients or Agent Desktop.

Scheduling a security store inspection task

Before you begin

- Configure the SMTP server and email account details.

About this task

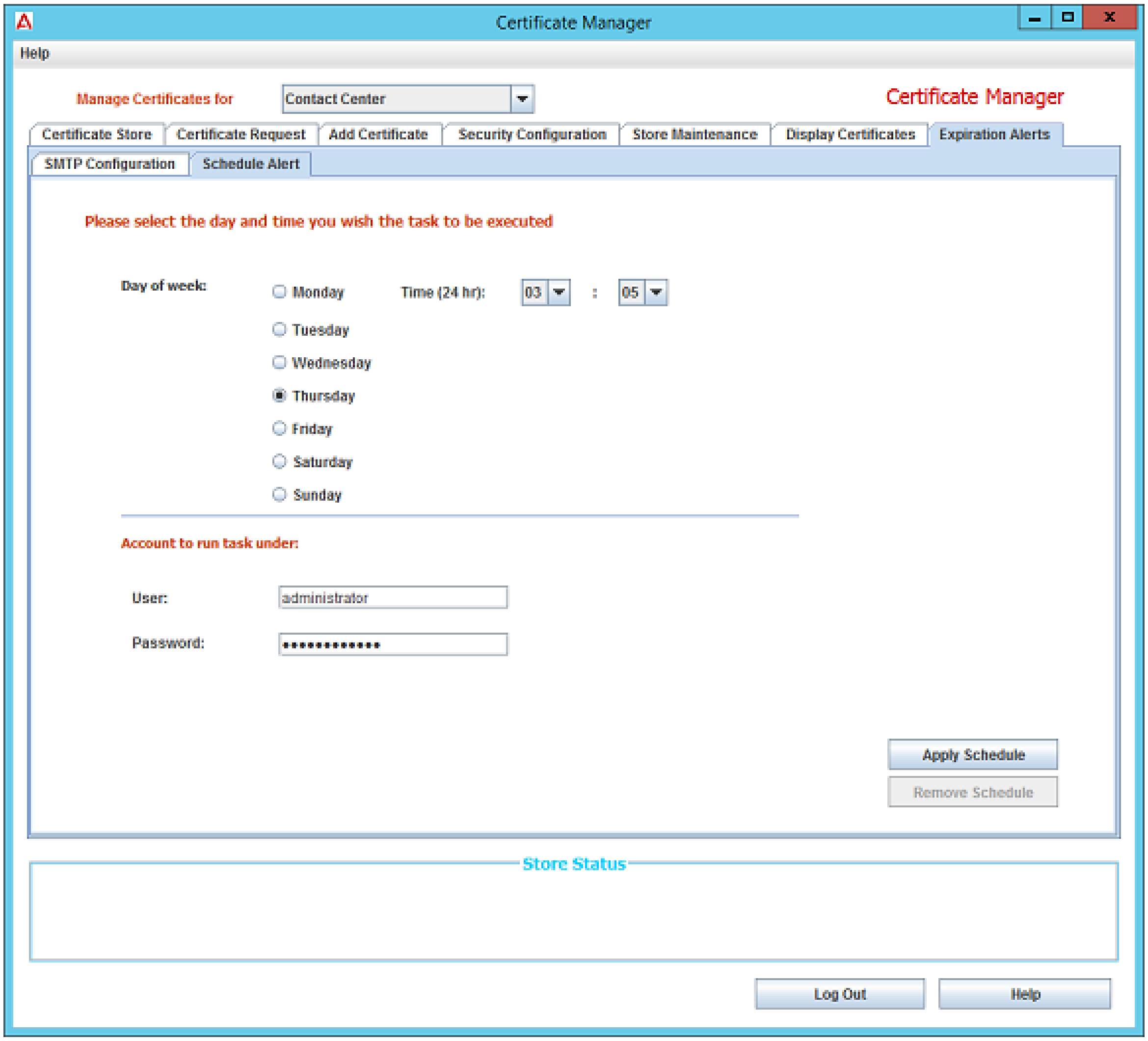
Schedule a security store inspection task. Security Manager adds the scheduled task to the underlying Windows Task Scheduler. The scheduled task runs the security store inspection utility once a week. You can select the time and day of the week that the security store inspection task runs during the week.

Procedure

1. Log on to the Avaya Contact Center Select Security Manager.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. Select **Expiration Alerts** > **Schedule Alerts**.
4. To enable the weekly inspection task, select **Schedule alerts**.
5. From the **Day of week** list, select the day on which to schedule the weekly inspection task.
6. In the **Time (24 hr)** section, enter the time of day on which to schedule the weekly inspection task. Use twenty four hour format time.
7. In the **User** box, enter the name of a Windows user account that has the privileges necessary to access the Windows Task scheduler and schedule the task.
8. In the **Password** box, enter the password of the Windows user account that has the privileges necessary to access the Windows Task scheduler and schedule the task.
9. Click **Apply Schedule**.

   Security Manager schedules this task on the underlying Microsoft Windows Task Scheduler. After successfully scheduling the task, the name on the **Apply Schedule** button changes to **Modify Schedule** and the button is disabled. To enable the **Modify Schedule** button, select a new time. You can then update the scheduled task time by clicking **Modify Schedule**.

   Example of a scheduled task:



Manage Certificates for: Contact Center

Please select the day and time you wish the task to be executed

Day of week:

○ Monday
○ Tuesday
○ Wednesday
● Thursday
○ Friday
○ Saturday
○ Sunday

Time (24 hr): 03 : 05

Account to run task under:

User: administrator

Password: ••••••••••••

Configuring SMTP server details

Before you begin

- Provision, configure, and maintain a Simple Mail Transport Protocol (SMTP) server. Contact Center Security Manager supports Microsoft Exchange Server.
- Know the authentication logon account and password details for the SMTP server.
- Ensure that the Contact Center server can access the SMTP server at all times.
- On the SMTP server, configure an email address for the contact center administrator. Security Manager sends the notification emails to this address. Ensure the contact center administrator monitors this email address.
- On the SMTP server, configure an email address for Avaya Contact Center Select Security Manager. Security Manager can then use this email address to send notification emails.

About this task

Configure the details of the SMTP server and accounts used to send the Security Manager status report email.

Procedure

1. On the **Security Manager** screen, select the **Expiration Alerts** tab.
2. Select **SMTP Configuration**.
3. From the **Outgoing e-mail server (SMTP)** list, select **IP** or **Address**. The Contact Center server must be able to communicate with the SMTP server by IP address or SMTP address.
4. In the **Outgoing e-mail server (SMTP)** box, enter the IP address or SMTP address of the SMTP server.
5. In the **Port number** box, enter the TCP port number for the SMTP server. The default port number is 25.
6. In the **Sender e-mail address** box, enter the email address to be used by Security Manager to send notification emails. Ensure this email address is registered with the SMTP server.
7. In the **Recipient e-mail address** box, enter the email address to which Security Manager is to send the notification emails. Ensure this email address is registered with the SMTP server. This is typically the contact center administrator's email address. You must monitor this email address for notifications about the status of Contact Center security certificates.
8. If your SMTP server requires authentication, select **SMTP server requires authentication**. If your SMTP server does not require authentication, clear this check box.
9. In the **User name** box, enter the user account name used to authenticate with the SMTP server.
10. In the **Password** box, enter the password of the user account used to authenticate with the SMTP server.
11. Click **Save Configuration**.

Modifying a scheduled security store inspection task

Before you begin

- Configure the scheduled task.

About this task

Modify the time of day for an existing scheduled task. For an existing scheduled task, you can change only the time of day; you cannot change the day of week for an existing scheduled task.

This is an optional procedure.

Procedure

1. Log on to the Avaya Contact Center Select Security Manager.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. In **Store Access**, type the certificate store password.
4. Click **OK**.
5. Select **Expiration Alerts** > **Schedule Alerts**.
6. In the **Time (24 hr)** section, enter the new time of the day on which to schedule the security store inspection task. Use twenty four hour format time.
7. In the **User** box, enter the name of a Windows user account that has the privileges necessary to access the Windows Task scheduler and schedule a task.
8. In the **Password** box, enter the password of the Windows user account that has the privileges necessary to access the Windows Task scheduler and schedule the task.
9. Click **Modify Schedule**.

   Security Manager then schedules this task to run at the new time of day on the underlying Microsoft Windows Task Scheduler.

Verifying the scheduled security store inspection task

Before you begin

- Configure the scheduled task.

About this task

Verify that the Windows Task Scheduler lists the Security Manager scheduled inspection task. Do not modify the scheduled task in Task Scheduler. Use only Security Manager to modify the scheduled inspection task.

Procedure

1. Log on to the Contact Center server.
2. On the **Start** screen, under **Administrative Tools**, click **Task Scheduler**.
3. In the left pane, click **Task Scheduler Library**.
4. In the middle pane, confirm that there is a task named **aaccSentinel**.
5. Confirm that the task **Status** is **Ready**.
6. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Removing a scheduled security store inspection task

Before you begin

- Configure the scheduled task.

About this task

Remove the Security Manager activated scheduled task from the Windows Task Scheduler. If you delete the scheduled security store inspection task, Security Manager no longer sends notification emails when Security Manager security certificates are due to expire. You must then manually monitor the status and expiration dates of the security certificates.

Procedure

1. Log on to the Avaya Contact Center Select Security Manager.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. In **Store Access**, type the certificate store password.
4. Click **OK**.
5. Select **Expiration Alerts** > **Schedule Alerts**.
6. Click **Remove Schedule**.

Examining a certificate file in the security store

Before you begin

- The security store must contain one or more certificate.

About this task

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

Procedure

1. Log on to the server containing the store.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. In **Store Access**, enter the security store password.
4. Click **OK**.
5. Select the **Display Certificates** tab.
6. Select **List**, to list all stored certificates in the store.
7. Select a certificate.

   The details of the certificate are displayed.
8. Select **Close**.

Removing a certificate file from the security store

About this task

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

Procedure

1. Log on to the server containing the store.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. In **Store Access**, type the security store password.
4. Click **OK**.
5. In the **Security Manager** window, Select the **Store Maintenance** tab.
6. Under **Signed and Root Certificates that reside in the store**, Security Manager lists all certificates in the store.
7. To delete a signed certificate, click **Delete Signed Cert** and click **OK**.
8. To delete a root certificate, select the certificate to remove from the **Root Certificates** list and click **Delete**.

Disabling Server Message Block signing in the server local group policy

About this task

Both the Contact Center DVD and the Release Pack installer modify the Windows Server 2012 local group policy to enable Server Message Block (SMB) signing. SMB signing places a digital “tag” into each server message block, which helps prevent man-in-the-middle attacks on network file sharing.

If you do not want to use SMB signing, follow this procedure to disable it by modifying the Windows Server 2012 local group policy.

Procedure

1. Log on to the Contact Center server as Administrator.
2. On the **Desktop** screen, right-click **Start** and select **Run**.
3. In the **Run** text box, type `gpedit.msc`.
4. Click **OK**.
5. On the Local Group Policy Editor window, in the left pane, select **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options**.

6. In the Name column, right-click **Microsoft network client: Digitally sign communications (always)**, and select **Properties**.
7. On the Microsoft network client: Digitally sign communications (always) dialog, select **Disable**.
8. In the Name column, right-click **Microsoft network server: Digitally sign communications (always)**, and select **Properties**.
9. On the Microsoft network server: Digitally sign communications (always) dialog, select **Disable**.

Backing up the security store

About this task

Back up the security store for restoring the server or before creating a new security store. Keeping a backup of the security store allows you to restore Security Manager if there is a failure with the current store.

Important:

Record the password for this security store. If you restore this backup, you will need the security store password to log on to Security Manager.

Before you begin

- Read the security section of *Avaya Contact Center Select Solution Description*.

Procedure

1. Log on to the Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. On the Store Access dialog, type the security store password, and click **OK**.
4. On the Security Manager screen, select the **Store Maintenance** tab.
5. Under **Backup and Restore Security Store**, click **Browse**.
6. On the Select Directory dialog, browse to the folder where you want to back up the security store.
7. Click **Select Directory**.
8. On the Store Maintenance screen, click **Backup**.

   Security Manager displays the result of the backup and updates the **Last Backup** section.

Deleting the security store

About this task

Delete an existing security store when it is no longer required. You can delete an active or an offline security store.

Procedure

1. Use the System Control and Monitor Utility to stop all Avaya Contact Center Select services.

    a. On the **Apps** screen, in the **Avaya** section, select **System Control and Monitor Utility**.

    b. Click the **Contact Center** tab.

    c. Click **Shut down Contact Center**.

2. On the Security Manager screen, select the **Security Store** tab.
3. Click **Delete Store**.
4. On the Security Manager — Delete Store Confirmation dialog, click **Delete Store**.

    Security Manager deletes the store and updates the **Store Status** to “NOT CREATED”.

5. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Chapter 24: Database encryption administration

This chapter describes the steps you need to perform to encrypt the Contact Center database. Using Security Manager, you can create and activate an encryption key and use it to encode the files in the Contact Center Caché database.

⚠ **Caution:**

> You must back up the encryption key, and the encryption key credentials. If you lose the encryption key or its credentials, they are not retrievable. This can result in loss of service.

You can also use Security Manager to decrypt the Contact Center database.

❗ **Important:**

> You must perform Contact Center database encryption or decryption during a scheduled maintenance window.

Business Continuity

In a Business Continuity (BC) solution, you must use the same encryption key on all Contact Center servers in the solution. Contact Center supports BC solutions where the Active server database is encrypted and the Standby server database is not encrypted, and vice versa. Database shadowing remains operational regardless of the encryption status of the Contact Center database. This allows you to minimize downtime while you implement database encryption in your solution. If you want to encrypt the databases in a BC solution, you can use the following procedure to minimize downtime:

1. Stop all Contact Center services on the standby server system (Server B).
2. Encrypt the standby server database (Server B).
3. Start the standby server B. Ensure that you synchronize the data between the servers.
4. Run a manual switchover, the current standby Server B becomes an active server. Server B is now running and processing contacts.
5. Stop all Contact Center services on Server A.
6. Encrypt the new standby server database (Server A). You must use the same encryption key as you used to encrypt Server B.
7. Backup all the contact center databases on the active server, Server B.
8. Restore all the active Server B contact center database backups onto Server A.
9. Configure Business Continuity on the standby Server A.
10. Configure standby Server A for your contact center.

11. Start the standby Server A. Ensure that data is synchronized between the servers.
12. Run a manual switchover if required, the current standby Server A becomes an active server. Server A is now running and processing contacts.

Upgrades

Before you upgrade your Contact Center solution, you must ensure that all databases are not encrypted.

Creating and activating an encryption key

About this task

Create and activate an encryption key and use it to encode the files in the Contact Center Caché database.

Procedure

1. Log on to the Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. On the Store Access dialog, type the security store password, and click **OK**.
4. On the Security Manager screen, select the **Database Encryption** tab.
5. Under **Credentials**, in the **User Name** box, type the user name for the new encryption key.
6. In the **Password** box, type the password for the new encryption key.

   Note:

   Passwords must be between 8 and 20 characters in length, and include at least one number, at least one uppercase letter, at least one lowercase letter, and no spaces. Passwords must not contain any of the following characters: **& " : > |**.
7. Under **Create/Select and Activate Key**, click **Browse**.
8. Browse to the folder where you want to save the encryption key.
9. In the **File Name** box, type a name for the key and click **Save File**.
10. Click **Create and/or Activate Key**.
11. On the **Confirm Password** dialog box, type the encryption key password and click **OK**.

    The **Output** pane shows the progress of the task.

Next steps

Caution:

You must back up the encryption key, and the encryption key credentials. If you lose the encryption key or its credentials, they are not retrievable. This can result in loss of service.

Encrypting the Contact Center database

About this task

Encrypt the Contact Center database during a scheduled maintenance window to ensure that sensitive data is secure.

Before you begin

- Create an encryption key, and ensure that the location of the key is accessible from the Contact Center server.
- Stop Contact Center services.

Procedure

1. Log on to the Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. On the Store Access dialog, type the security store password, and click **OK**.
4. On the Security Manager screen, select the **Database Encryption** tab.
5. Under **Credentials**, in the **User Name** box, type the user name for the encryption key.
6. In the **Password** box, type the password for the encryption key.

   Note:

   Passwords must be between 8 and 20 characters in length, and include at least one number, at least one uppercase letter, at least one lowercase letter, and no spaces. Passwords must not contain any of the following characters: **& " : > |**.
7. Under **Encrypt/Decrypt Database**, if the **Key Location** box is not already populated with the encryption key location, click **Browse**.
8. In the **Select Key File** window, navigate to the location of the encryption key.
9. Select the encryption key file and click **Select File**.
10. Click **Encrypt**.

    The **Output** pane shows the progress of the task. The amount of time this task takes depends on the size of the Contact Center database.

Next steps

When the encryption is complete, start Contact Center services.

Decrypting the Contact Center database

About this task

Decrypt the Contact Center database during a scheduled maintenance window. Before you upgrade Contact Center software, you must decrypt the database.

Before you begin

- Ensure that the location of the encryption key is accessible from the Contact Center server.
- Stop Contact Center services.

Procedure

1. Log on to the Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. On the Store Access dialog, type the security store password, and click **OK**.
4. On the Security Manager screen, select the **Database Encryption** tab.
5. Under **Credentials**, in the **User Name** box, type the user name for the encryption key.
6. In the **Password** box, type the password for the encryption key.
7. Under **Encrypt/Decrypt Database**, click **Browse**.
8. In the **Select Key File** window, navigate to the location of the encryption key.
9. Select the encryption key file and click **Select File**.
10. Click **Decrypt**.

    The **Output** pane shows the progress of the task. The amount of time this task takes depends on the size of the Contact Center database.

Next steps

When the decryption is complete, start Contact Center services.

Chapter 25: Agent Desktop client software installation using Remote Desktop Services

This chapter describes how to use Remote Desktop Services on a Windows Server 2012 R2 server to host and publish Agent Desktop.

Agent Desktop client software installation using Remote Desktop Services prerequisites

Procedure

- Install the required Contact Center server software.
- Install and commission one or more Agent Desktop clients to confirm Agent Desktop functionality.
- Deploy and integrate Windows Server 2012 Remote Desktop Services servers in your solution. Deploy a RD Connection Broker, a RD Web Access, and a RD Session Host co-resident or standalone.
- Install Agent Desktop software on the RD Session Host server, using the Agent Desktop MSI installation package. Ensure that you disable the softphone option. For more information about installing Agent Desktop using MSI installation package, see the ACCS Deployment guide that applies to your solution:
  - *Deploying Avaya Contact Center Select DVD*
  - *Deploying Avaya Contact Center Select Software Appliance*
  - *Deploying Avaya Contact Center Select Hardware Appliance*
- Review the Agent Desktop client requirements for deployment using Remote Desktop Services. See *Avaya Contact Center Select Solution Description*.

Publishing Agent Desktop client software using Remote Desktop Services

About this task

Remote Desktop Services, formerly known as Terminal Services, allows a server to host multiple simultaneous client sessions. In the Remote Desktop Services (RDS) environment, an application runs entirely on the Remote Desktop Session Host (RD Session Host) server. The RDS client performs no local processing of application software.

Follow the procedure below to publish Agent Desktop client software using Remote Desktop Services.

Procedure

1. Configure CCMM to support Agent Desktop on a Windows 2012 R2 operating system:
    a. Log on to CCMA.
    b. On the Launchpad, click **Multimedia**.
    c. In the left pane, select the server to which you want to log on.
    d. Click **Launch Multimedia Client**.
    e. In the left column, select **Agent Desktop Configuration**.
    f. Click **User Settings**.
    g. Select **Suppress OS not supported popup**.
    h. Click **Save**.
2. Log on to the RDS Session Host server with administrative privileges.
3. Using the **Server Manager – Remote Desktop Services** utility, select **Collections** > **QuickSessioncollection**.
4. In the **REMOTEAPP PROGRAMS** section, from the **TASKS** drop-down list, select **Publish RemoteApp Programs**.
5. From the **RemoteApp Programs** list, select **Avaya Agent Desktop 7.0**.
6. Click **Next**.
7. Click **Publish**.
8. From the **REMOTEAPP PROGRAMS** list, right-click **Agent Desktop** and select **Properties**.
9. Configure the agent, user, and user group accounts to access the Agent Desktop RemoteApp.
10. Log on to an agent client computer.
11. Use Internet Explorer to access the RD Web Access Interface. For example, access the RD Web Access Interface using the following URL:

    ```
    https://<RDS Server FQDN>/RDWeb
    ```

12. On the **Work Resources** page, enter the Windows domain account details for the agent and click **Sign in**.

    The web interface lists the RemoteApps available to the agent.

13. In the **Current folder** section, double-click **Agent Desktop**.
14. Log on to Agent Desktop and Go Ready.
15. Verify that the Agent Desktop RemoteApp can handle routed customer calls, and continue to verify the features your solution requires.

Next steps

Using the Server Manager Performance and Best Practice Analyzer, continue to monitor all the resources of the RDS host servers, focusing on CPU, memory, and disk drive resources. Capture the initial CPU and memory usage as baseline performance metrics.

Chapter 26: Publishing ACCS client software in a Citrix deployment

This chapter describes how to configure and publish Avaya Contact Center Select software applications in a Citrix deployment.

Prerequisites

Procedure

- Install Avaya Contact Center Select.
- Ensure that you have administrative privileges on the client computer.
- Install one of the supported operating systems on the client computer. The supported operating systems are as follows:
  - Windows 7 (32-bit and 64-bit)
  - Windows 8.1
  - Windows 10
- Install Internet Explorer Release 10.0 or 11.0.
- Optionally, depending on your solution, create the Citrix users allowed to run the published Avaya Contact Center Select applications.

Configuring the client OS setting for Citrix deployments

About this task

Configure Contact Center Multimedia to support Agent Desktop in Citrix deployments.

Procedure

1. Log on to Contact Center Manager Administration with administrator privileges.
2. On the Launchpad, click **Multimedia**.
3. In the left pane, select the server to which you want to log on.

4. Click **Launch Multimedia Client**.
5. In the left column, select **Agent Desktop Configuration**.
6. Click **User Settings**.
7. Select **Enable Unsupported Client OS**.
8. Click **Save**.

Publishing Agent Desktop client software on a Citrix server

Before you begin

- Install Agent Desktop on the Avaya Contact Center Select server.
- Copy the Agent Desktop client folder from the Avaya Contact Center Select server to a location on the Citrix server. The folder is located on the server at: `D:\Avaya\Contact Center\Multimedia Server\Agent Desktop\client`

About this task

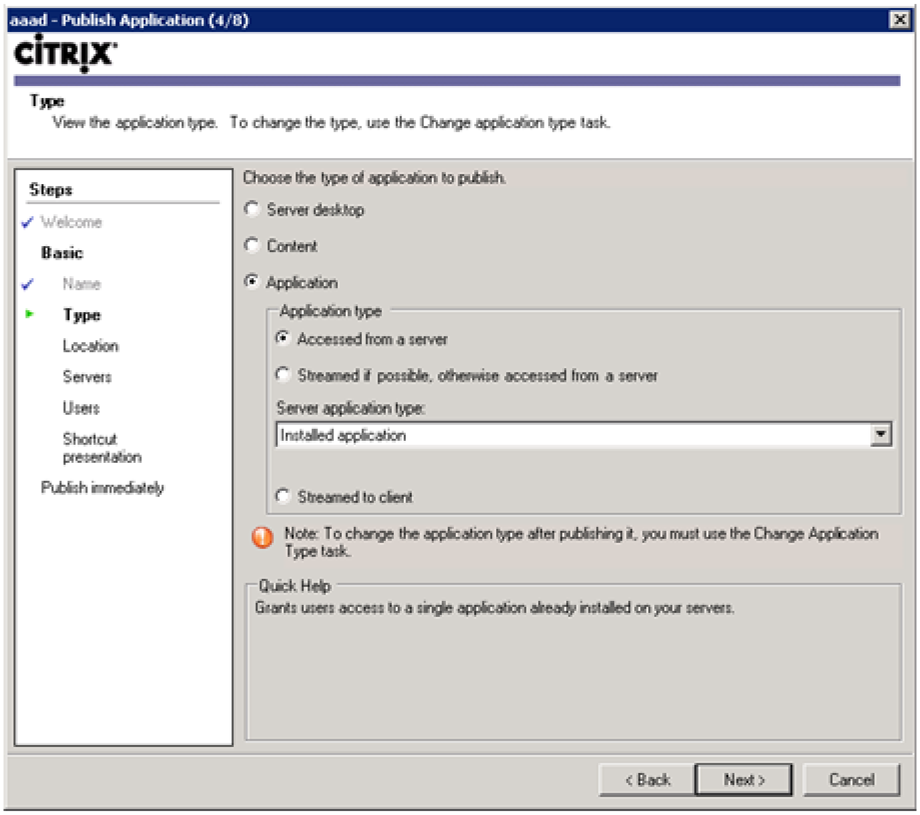
You can launch Agent Desktop client software on a client computer using a Citrix server. You must configure your Citrix server to publish Agent Desktop as a published application before you can launch Agent Desktop software on client computers. Publish Agent Desktop client software on a Citrix Server by following the procedure below.

Note:

The following example uses Citrix XenApp 6.5.

Procedure

1. On your Citrix server, open Citrix AppCenter.
2. In the left pane, right-click **Applications** and click **Publish Application**.
3. On the **Name** window, in the **Display name** box, type a name for the new published application. For example, type `Agent Desktop`.
4. In the **Application description** box, type a description for the new published application.
5. Click **Next**.
6. On the **Type** window, under **Application type**, select **Accessed from a server**.



aaad - Publish Application (4/8)

Type

View the application type. To change the type, use the Change application type task.

Steps

- ✓ Welcome
- Basic
  - ✓ Name
  - ▸ Type
  - Location
  - Servers
  - Users
  - Shortcut presentation
- Publish immediately

Choose the type of application to publish.

○ Server desktop

○ Content

● Application

Application type

● Accessed from a server

○ Streamed if possible, otherwise accessed from a server

Server application type: Installed application

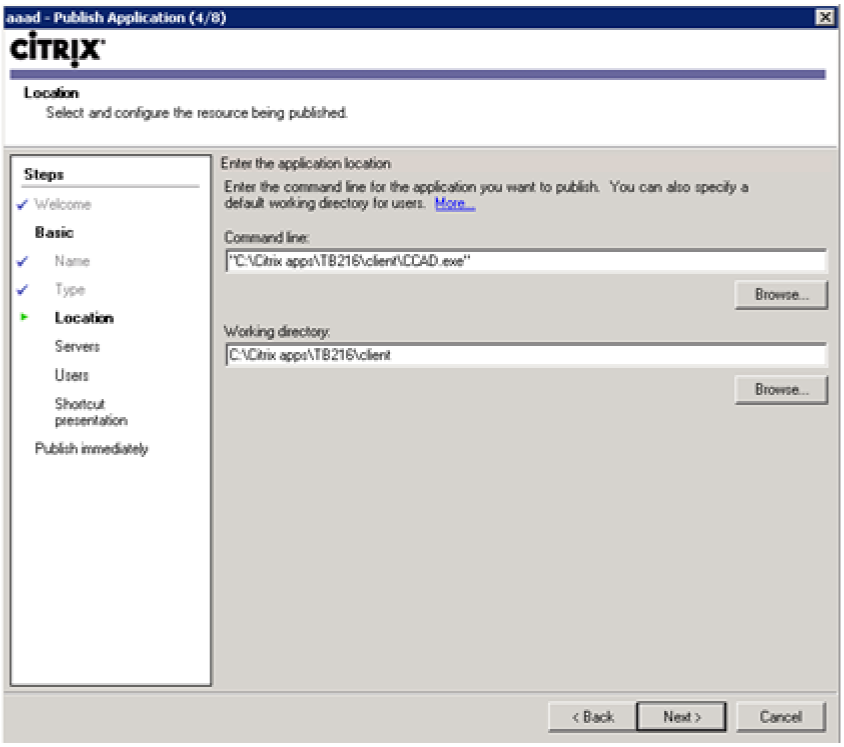
○ Streamed to client

Note: To change the application type after publishing it, you must use the Change Application Type task.

Quick Help

Grants users access to a single application already installed on your servers.

7. Click **Next**.
8. On the **Location** window, click **Browse**.
9. Navigate to the location on the Citrix server where the Agent Desktop client folder is stored.
10. Select the CCAD.exe file and click **OK**.



aaad - Publish Application (4/8)

Location

Select and configure the resource being published.

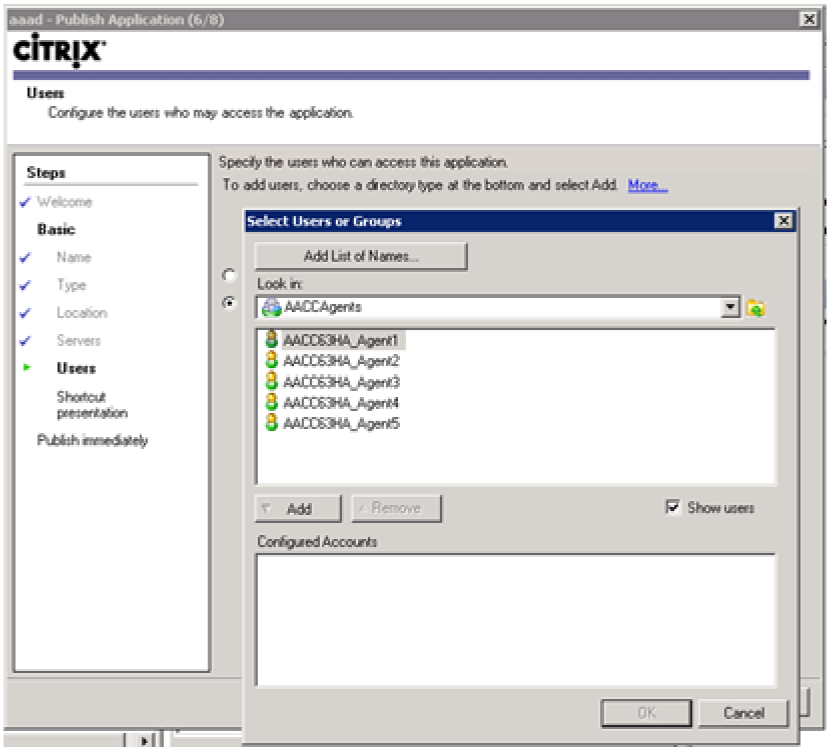
Enter the application location

Enter the command line for the application you want to publish. You can also specify a default working directory for users.

Command line: "C:\Citrix apps\TB216\client\CCAD.exe"

Working directory: C:\Citrix apps\TB216\client

11. Click **Next**.
12. On the **Servers** window, click **Add**.
13. On the **Select Servers** dialog box, select the Citrix server used to run the Agent Desktop application and click **Add**.
14. Click **OK**.
15. Click **Next**.
16. On the **Users** window, click **Add**.
17. On the **Select Users or Groups** dialog box, select the users allowed to run the published application. For example, select your Contact Center agents and click **Add**.



aaad - Publish Application (6/8)

Users

Configure the users who may access the application.

Steps

✓ Welcome

Basic

✓ Name

✓ Type

✓ Location

✓ Servers

▸ Users

Shortcut presentation

Publish immediately

Specify the users who can access this application.

To add users, choose a directory type at the bottom and select Add. More...

Select Users or Groups

Look in: AACCAgents

AACC63HA_Agent1

AACC63HA_Agent2

AACC63HA_Agent3

AACC63HA_Agent4

AACC63HA_Agent5

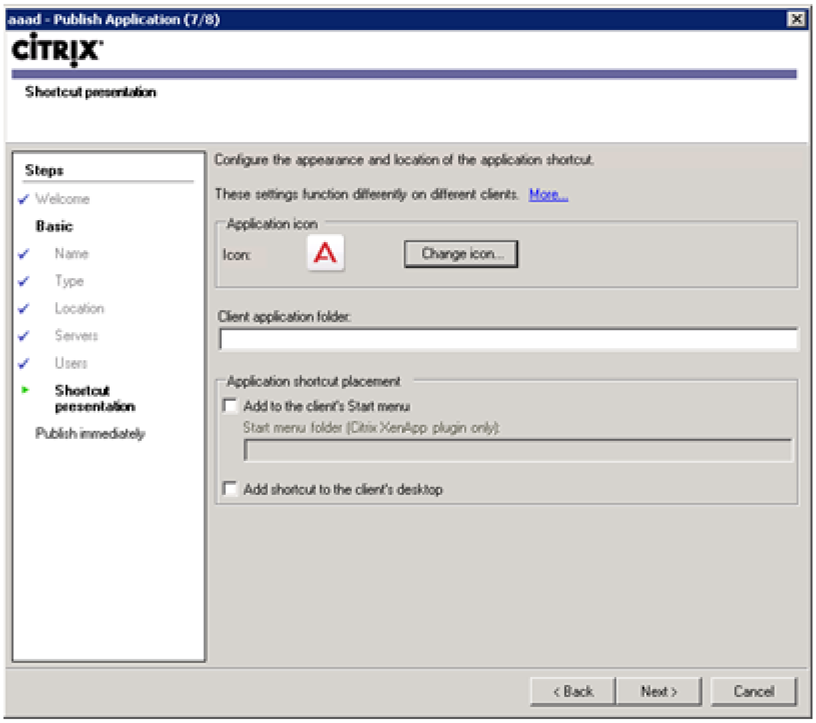
☑ Show users

Configured Accounts

18. Click **OK**.
19. Click **Next**.
20. On the **Shortcut presentation** window you can select from a number of shortcut options on the browser.

Note:

The Agent Desktop icon appears by default as an icon. You can also choose to create a client application folder on each client computer that contains all published applications, or add shortcuts to the client computer’s Start menu or desktop.



Shortcut presentation

Configure the appearance and location of the application shortcut.

These settings function differently on different clients. More...

Application icon

Icon:

Client application folder:

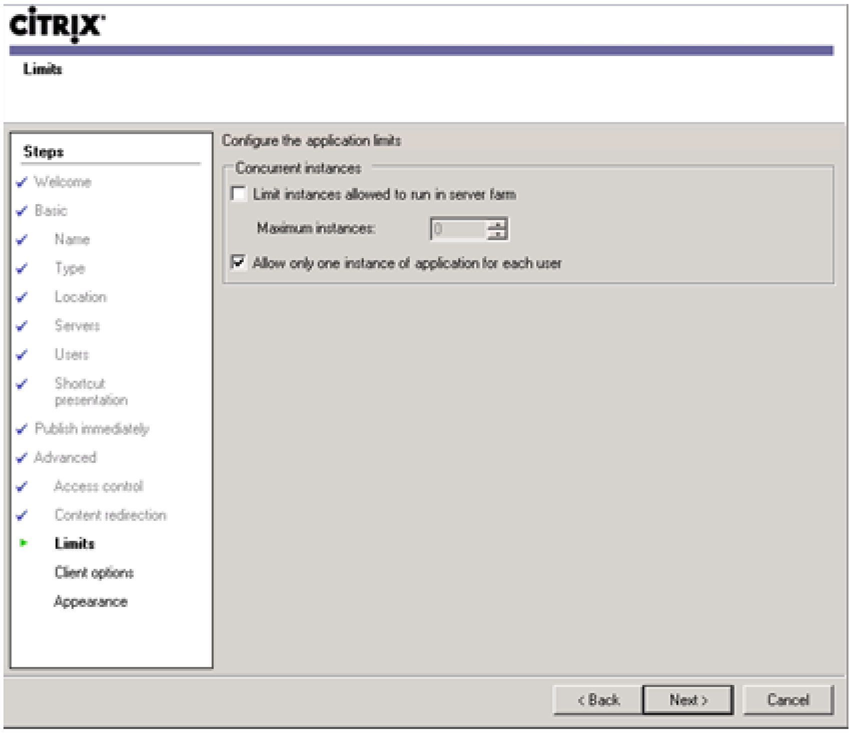
Application shortcut placement

□ Add to the client's Start menu

Start menu folder (Citrix XenApp plugin only):

□ Add shortcut to the client's desktop

21. Click **Next**.
22. On the **Publish immediately** window, select **Configure advanced application settings now** and click **Next**.
23. Continue clicking **Next** until the **Limits** window appears.
24. Select **Allow only one instance of application for each user**.



Limits

Configure the application limits

Concurrent instances

□ Limit instances allowed to run in server farm

Maximum instances: 0

☑ Allow only one instance of application for each user

25. Click **Next**.
26. Click **Finish**.
27. On the client computer, agents can now launch Agent Desktop using one of the configured shortcuts.

Publishing Contact Center Manager Administration on a Citrix server as content

Before you begin

- Install Avaya Contact Center Select.

About this task

You can access the Contact Center Manager Administration application on a client computer using a Citrix server. You must configure your Citrix server to publish CCMA as published content.

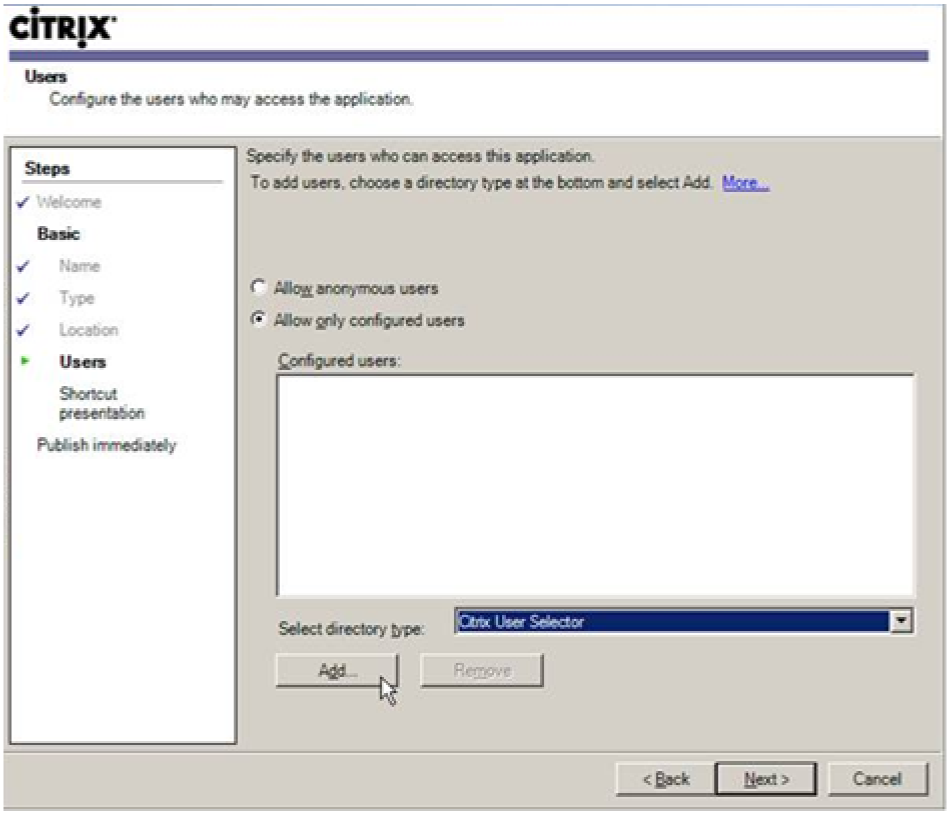
Procedure

1. On your Citrix server, open Citrix AppCenter.
2. In the left pane, right-click **Applications** and click **Publish Application**.
3. On the **Name** window, in the **Display name** box, type a name for the new published application. For example, type `ccma`.

4. In the **Application description** box, type a description for the new published application.
5. Click **Next**.
6. On the **Type** window, under **Choose the type of application to publish**, select **Content**.
7. Click **Next**.
8. On the **Location** window, type the Contact Center Manager Administration URL. For example, type

   ```
   http://<server name>
   ```

   where <server name> is the name of the Avaya Contact Center Select server.
9. Click **Next**.
10. On the **Users** window, select **Allow only configured users**.
11. Select **Citrix User Selector** as the **directory type**.
12. Click **Add**.



Users

Configure the users who may access the application.

Specify the users who can access this application.

To add users, choose a directory type at the bottom and select Add. More...

○ Allow anonymous users

● Allow only configured users

Configured users:

Select directory type: Citrix User Selector

13. On the **Select Users or Groups** dialog box, select the users allowed to run the published application. For example, select your Contact Center administrators and click **Add**.
14. Click **OK**.
15. Click **Next**.

16. Click **Next**.
17. Click **Finish**.
18. On the client computer, authorized users can now access CCMA using the Citrix client.

Publishing Contact Center Manager Administration on a Citrix server as an installed application

Before you begin

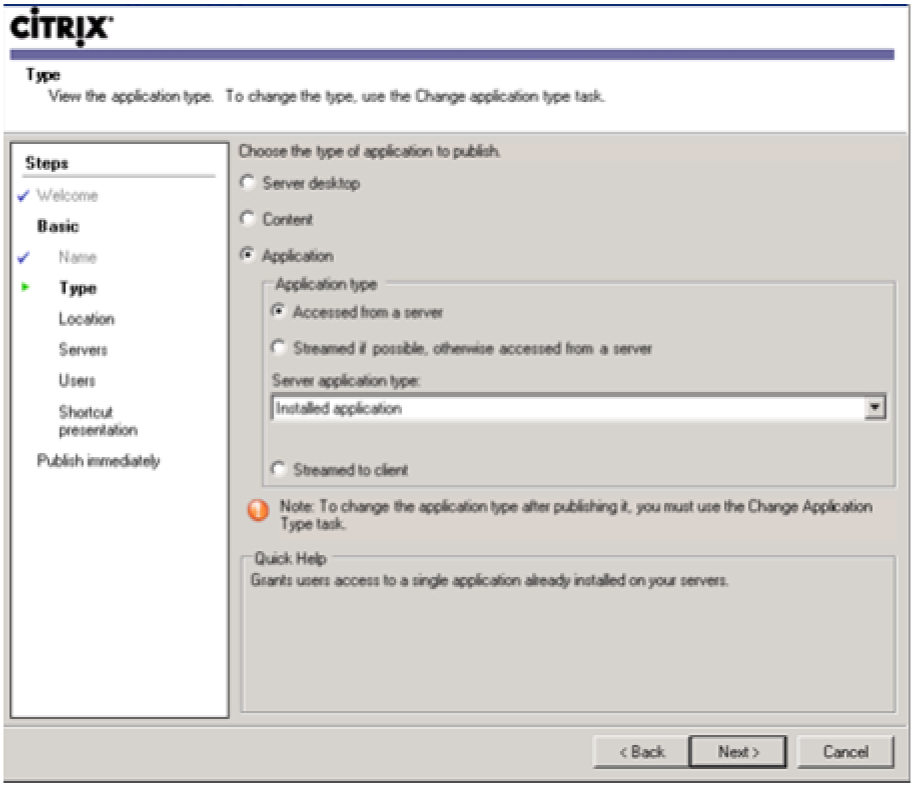
- Install Avaya Contact Center Select.

About this task

You can access the Contact Center Manager Administration application on a client computer using a Citrix server. You must configure your Citrix server to publish CCMA as an installed application.

Procedure

1. On your Citrix server, open Citrix AppCenter.
2. In the left pane, right-click **Applications** and click **Publish Application**.
3. On the **Name** window, in the **Display name** box, type a name for the new published application. For example, type `ccma`.
4. In the **Application description** box, type a description for the new published application.
5. Click **Next**.
6. On the **Type** window, under **Choose the type of application to publish**, select **Application**.
7. Under **Application Type**, select **Accessed from a server**.



Type

View the application type. To change the type, use the Change application type task.

Choose the type of application to publish.

○ Server desktop

○ Content

● Application

Application type

● Accessed from a server

○ Streamed if possible, otherwise accessed from a server

Server application type: Installed application

○ Streamed to client

Note: To change the application type after publishing it, you must use the Change Application Type task.

Quick Help

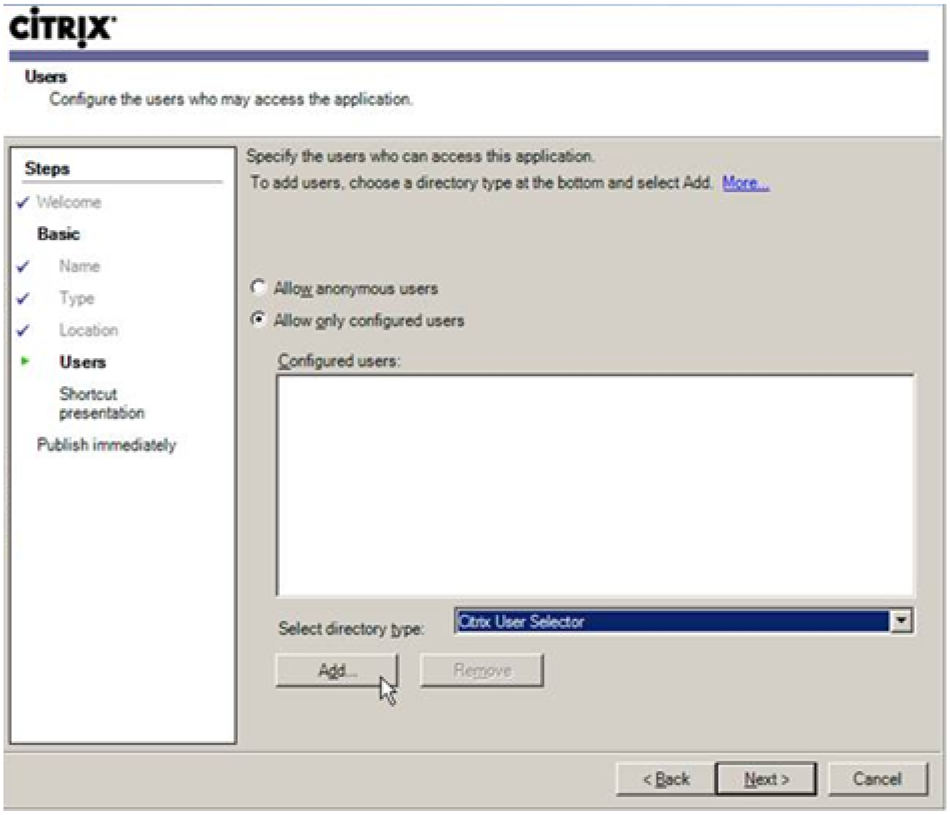
Grants users access to a single application already installed on your servers.

8. Click **Next**.
9. On the **Location** window, click **Browse**.
10. Navigate to the location on the Citrix server of the Internet Explorer executable. For example, navigate to `C:\Program Files (x86)\Internet Explorer\iexplore.exe`.
11. Ensure the location appears within quotation marks, and type the Contact Center Manager Administration URL after the location. For example, type

    ```
    "C:\Program Files (x86)\Internet Explorer\iexplore.exe" http://<server name>
    ```

    where <server name> is the name of the Avaya Contact Center Select server.
12. Click **Next**.
13. On the **Servers** window, click **Add**.
14. On the **Select Servers** dialog box, select the Citrix server used to run the CCMA application and click **Add**.
15. Click **OK**.
16. Click **Next**.
17. Click **Next**.
18. On the **Users** window, select **Allow only configured users**.

19. Select **Citrix User Selector** as the **directory type**.
20. Click **Add**.



Users

Configure the users who may access the application.

Specify the users who can access this application.

To add users, choose a directory type at the bottom and select Add. More...

○ Allow anonymous users

● Allow only configured users

Configured users:

Select directory type: Citrix User Selector

21. On the **Select Users or Groups** dialog box, select the users allowed to run the published application. For example, select your Contact Center administrators and click **Add**.
22. Click **OK**.
23. Click **Next**.
24. Click **Next**.
25. Click **Finish**.
26. On the client computer, authorized users can now access CCMA using the Citrix client.

Installing the ActiveX Controls on the Citrix server

Before you begin

- Configure the Web browser to enable initialize and script ActiveX Controls not marked as safe. See Configuring Internet Explorer on page 39.

About this task

Install the ActiveX Controls.msi file on the Citrix server.

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

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

Procedure

1. Read the Avaya Contact Center Select Release Notes to obtain the location of the latest ActiveX Controls.msi file for your Avaya Contact Center Select release.
2. Log on to the Citrix server with administrator privileges.
3. Copy the ActiveX Controls.msi file to a location on the Citrix server.
4. In the location of the the ActiveX Controls.msi file on the Citrix server, double-click **ActiveX Controls.msi** to begin the installation.
5. Click **Next**.
6. Select a **Destination Folder** or accept the default installation folder.
7. Click **Next**.
8. In the **Ready to Install the Program** window, click **Install**.
9. Click **Finish**.

Chapter 27: Language support fundamentals

This chapter provides background information for Language support. If you want to use English across all platforms, you can ignore this chapter.

Contact Center Multimedia (CCMM) and Contact Center Manager Administration (CCMA) support the following languages:

- English
- French (FR)
- German (DE)
- Japanese (JA)
- Russian (RU)
- Simplified Chinese (Zh-CN)
- Latin American Spanish (ES)
- Brazilian Portuguese (PT-BR)
- Italian (IT)
- Korean (KO)

The following table lists the compatibility between the CCMA language and the Operating System (OS) language family. You can enable only compatible languages on the Contact Center server.

OS language	FR	DE	ES	PT-BR	IT	Zh-CN	JA	RU	KO
English	Yes	Yes	Yes	Yes	Yes	No	No	No	No
Any 1 Latin language	Yes	Yes	Yes	Yes	Yes	No	No	No	No
Simplified Chinese	No	No	No	No	No	Yes	No	No	No
Japanese	No	No	No	No	No	No	Yes	No	No
Russian	No	No	No	No	No	No	No	Yes	No
Korean	No	No	No	No	No	No	No	No	Yes

You use the Contact Center Manager Administration Language Settings utility to enable additional languages. Access the Language Settings utility from the CCMA Configuration screen. The English language is always enabled and you cannot disable it. The Language Settings utility displays the current server code page for the Contact Center server.

A code page is an internal table that the operating system uses to map symbols (letters, numerals, and punctuation characters) to a number. Different code pages provide support for the character sets used in different languages. Code pages have a number for reference; for example, code page 932 represents the Japanese character set, and code page 950 represents the Chinese character set. In a Contact Center solution, on an English Contact Center server, the Server Code Page is 1252. On a Contact Center server with Japanese, the Server Code Page is 932.

Install the most recent Service Pack and patches to enable the localized languages in the CCMA Language Settings utility. A Service Pack contains all supported languages. For CCMA, you can enable only languages that are appropriate to the local operating system of the server. For example, you can enable the simplified Chinese language on a simplified Chinese OS, but you cannot enable German on a simplified Chinese OS. The client computers operating systems must be of the same language family as the associated server. You can enable multiple languages from the same language family on a single server.

If you enable a language in the Language Settings utility, users see the localized CCMA screens in the preferred language that is set in their client browser. For example, if you enable Spanish in the Language Settings utility, and if Spanish is the preferred language in Internet Explorer on the CCMA client computer, then CCMA appears in Spanish in the CCMA client browser.

For some languages, translations can be different from the terms usually used in your region:

- French: The translation attempts to find terms that are acceptable to both Canadian and European French speakers.
- Latin American (LA) Spanish: The translation attempts to find terms that are acceptable to both Latin American and European Spanish speakers.

Read the Contact Center Service Pack Release Notes for further information. The Service Pack Release Notes contain the most recent information about language support.

Note:

If the server code page changes, you can still change previously enabled languages. You must disable the languages that are not supported.

Language levels

Contact Center Multimedia and Contact Center Manager Administration support two levels of language environment:

- international environment
- international and local environment

International environment

In the international environment, the graphical user interface, the online Help, and all reports are in English. However, you can enter user information that contains non-ASCII characters (such as agent and supervisor names). Also, you can manage date and time formats from a different regional time zone.

International and local environment

In the combined international and local environment, the graphical user interface, the online Help, and many reports are translated into one of the following supported languages: French, German, Japanese, Italian, Korean, Russian, Simplified Chinese, LA Spanish, and Brazilian Portuguese. Also, you can enter user information that contains non-ASCII characters and you can use date and time formats from a different regional time zone. For details of the reports that are translated for a particular language, see the Contact Center Service Pack Release Notes.

In this environment, you must install the most recent Service Pack on the Contact Center servers. See the Service Pack Release Notes for further information.

Language family compatibility

For Contact Center Manager Administration to function properly, the language family of the operating systems must be compatible across all platforms in the network. If the language versions of the operating systems on the Contact Center Manager Server, Contact Center Multimedia, Contact Center Manager Administration server, and the client PC belong to the same language family, the platforms can coexist on the same network. This compatibility is useful if your contact center supports multiple languages.

The character sets for English are included in all language families. Contact Center Multimedia and Contact Center Manager Administration recognize the following language families:

- Latin-1
- Japanese
- Russian
- Simplified Chinese
- Korean

Latin-1 includes all Western European languages that use the Latin-1 character set. French, German, Italian, LA Spanish, and Brazilian Portuguese belong to the Latin-1 language family. Agents in the contact center can view Contact Center Manager Administration and Contact Center Multimedia in English, French, German, LA Spanish, Italian, or Brazilian Portuguese. For Latin-1 language family and server compatibility, see the Contact Center Localization Release Notes for further information.

If you use the Japanese language family, users in the same contact center can view Contact Center Manager Administration and Contact Center Multimedia in English or Japanese. If you use the Simplified Chinese language family, users in the same contact center can view Contact Center Manager Administration and Contact Center Multimedia in English or Simplified Chinese. If you use the Russian language family, users in the same contact center can view Contact Center Manager Administration and Contact Center Multimedia in English or Russian.

Configuring the operating system language

About this task

Perform the following procedure to configure a new language for the Contact Center server operating system. You must perform this procedure to ensure that Contact Center operates correctly when using a new operating system language.

Before you begin

- Download and install the language pack for the language you want to configure on the operating system. Refer to Microsoft documentation for information about language packs.

Procedure

1. Log on to the Contact Center server.
2. On the **Start** screen, click **Control Panel**.
3. In the Control Panel, click **Clock, Language, and Region**.
4. Click **Language**.
5. Click **Add a language**.
6. From the list of languages, select a language and click **Open**.
7. If required, from the list of regional variants, select the regional variant of the language and click **Add**.
8. On the Language window, select the newly added language and click **Move up**.
9. Click **Advanced settings**.
10. Under **Override for Windows display language**, from the drop-down list, select the newly added language.
11. Under **Override for default input method**, from the drop-down list, select the newly added language.
12. Click **Save**.
13. On the **Change display language** dialog box, click **Log off later**.
14. On the Language window, in the left pane, click **Change date, time, or number formats**.
15. On the Region window, select the **Administrative** tab.
16. Click **Copy settings**.
17. On the Welcome screen and new user accounts settings window, select the **Welcome screen and system accounts** check box and the **New user accounts** check box.

18. Click **OK**.
19. Restart the Contact Center server.

Setting the system locale

About this task

Ensure that the Contact Center server system locale matches the operating system language. If the system locale does not match the operating system language, you cannot enable a localized language in Contact Center Manager Administration (CCMA).

Procedure

1. Log on to the Contact Center server.
2. On the **Start** screen, click **Control Panel**.
3. In the Control Panel, click **Clock, Language, and Region**.
4. On the Clock, Language, and Region window, click **Region**.
5. On the Region window, select the **Administrative** tab.
6. Click **Change system locale**.
7. On the Region Settings window, in the **Current system locale** field, select a locale that matches the operating system language.
8. Click **OK**.
9. On the Region window, click **OK**.

Enabling a localized language

Before you begin

- Check that the system locale matches the operating system language setting. For information about setting the system locale, see Setting the system locale on page 341.
- Read the Contact Center Service Pack Release Notes for more information. The Release Notes contain the most recent information about language support.
- Ensure that Contact Center is working before installing the Service Pack.
- Using the Release Pack Installer (RPI) and Avaya Contact Center Update Manager, apply the most recent Service Pack and patches.

About this task

Enable a language using the Contact Center Manager Administration (CCMA) Language Settings utility so that CCMA administrators and users see the localized CCMA screens in their client browsers.

Procedure

1. Log on to the Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Manager Administration Configuration**.
3. In the Avaya Applications Configuration window, in the right pane, click **Language Settings**.
4. In the Language Settings window, select the required CCMA localized language from the list, and select **Enabled** for that language.
5. Click **Save**.

Accessing the CCMA Web client using a localized language

Before you begin

- Install the most recent Service Pack on the Contact Center server, and enable the required language.

About this task

Access the Contact Center Manager Administration (CCMA) Web client from a Web Browser on an English OS client computer using a localized language. For example, access the CCMA Web client from a Web Browser on an English OS client computer, but using the French language and screens with CCMA. This enables French speaking CCMA administrators and users with an English OS client computer to access and use CCMA with a French language user interface.

If French is enabled in the Language Settings utility, and if French is the preferred language in Internet Explorer on the CCMA client computer, then CCMA appears in French in the CCMA client Internet Explorer browser display.

Procedure

1. From an English client computer, start Internet Explorer.
2. In Internet Explorer, click **Tools** > **Internet Options**.
3. Click **Languages**.
4. Click **Add**.
5. From the list of languages, click the appropriate language. For example, select **French (France) [fr-FR]**.
6. Click **OK**.
7. On the Language Preferences window, use the **Move up** button to move the language you want to use to the top of the **Languages** list.

8. Click **OK** to close the Language Preferences window.
9. Click **OK** to close the Internet Options window.
10. In the **Address** box, type the URL of the server. For example, type `https://<server name>`, OR if you turned off Contact Center security, type `http://<server name>`, where *<server name>* is the computer name of the Contact Center server.

    ❗ **Important:**

    You must log on using the Contact Center server name. Do not use the server IP address.

    The CCMA screens display in French.

Chapter 28: Common procedures

This chapter describes the common procedures that you perform to administer your Avaya Contact Center Select software.

Starting or stopping Contact Center applications

About this task

Use the System Control and Monitor Utility to start and stop all of the applications in Contact Center.

Procedure

1. Log on to the Avaya Contact Center Select server.
2. On the **Apps** screen, in the **Avaya** section, select **System Control and Monitor Utility**.
3. Click the **Contact Center** tab.
4. Select the check box for each application to start or stop on the server.
5. To start the selected applications, click **Start Contact Center**.

   OR

   To stop the selected applications, click **Shut down Contact Center**.

Appendix A: Server name or IP address change - hardware appliance or DVD install

This Appendix describes the procedures you must perform to change the name or IP address of the Avaya Contact Center Select hardware appliance or an Avaya Contact Center Select server. You must perform a server name or IP address change during a Contact Center maintenance window.

❗ **Important:**

Avaya Contact Center Select does not support changing the server name or IP address of servers configured for Business Continuity. Avaya recommends that you configure the final production name of the Avaya Contact Center Select servers before configuring Business Continuity.

Avaya Contact Center Select server name change

Change the name of the Avaya Contact Center Select server. You must also change the server name of Avaya Aura® Media Server. The new host name of the server must meet the specifications of the server names in the Contact Center suite.

Security considerations

If you change the name of a secured Contact Center server, Avaya recommends that you create a new security store with a server certificate that matches the new server name.

Each server certificate has a name, which normally derives from the server Fully Qualified Domain Name (FQDN). If a server certificate name does not match the name of the website or web service to which a client connects, the client generates a warning. Normally on a GUI, a user can bypass the warning and continue. If the client is a service on another system, it does not handle and bypass the warning unless coded to do so.

If you change the server name and do not change the server certificate, users always see warnings when they connect to Contact Center web services.

Solutions that require server certificates

- Solutions that use TLS security for the CTI link to IP Office.

- Solutions using the Agent Browser application. These always use TLS security for the Agent Browser application client.
- Solutions on which you enabled Web Services security.
- Solutions using Secure Real Time Protocol for voice traffic.

Preparing a server certificate before changing the server name

If you use an external Certificate Authority (CA), it can sometimes take an extended period to receive a signed server certificate after submitting your Certificate Signing Request (CSR) to the CA. To minimize the time elapsed for a server name change, you can create a CSR and request and receive a new server certificate before changing the server name. The following high-level procedures outline how to create a new CSR to send to the CA.

Important:

> If the CA you use to sign the new server certificate is different to the CA you used to sign the old server certificate, you must also distribute a new root certificate to all the relevant clients and servers after changing the server name and applying the new server certificate.

To create a new CSR in the Contact Center security store using Security Manager:

- Schedule a maintenance window for this task, because you must stop the Contact Center services.
- In Security Manager, back up the Contact Center security store.
- Delete the existing security store.
- Create a new security store, specifying the planned new server name as the common name for the certificate.
- Copy the CSR content from the new security store, to send to the CA to request a server certificate.
- Restore the Contact Center security store that you backed up.

You can now use the CSR you generated to request a server certificate from a CA. When the CA provides the new server certificate, you can schedule the Contact Center server name change.

In Avaya Aura® Media Server, you can create a new CSR at any time without stopping the server or impacting the existing certificates. Create a new CSR to request a new server certificate from a CA. When the CA provides the new server certificate, you can schedule the server name change.

Avaya Contact Center Select server name change prerequisites

Procedure

- Ensure that the new server name is unique.
- Ensure that the new server name is from 6 to 15 characters and that the first character is alphabetical.
- Ensure that the new server name contains no underscores (_), spaces ( ), or punctuation.

Turning off Web Services security

About this task

Turn off Web Services security before you rename the server. If Web Services security is not enabled on your contact center, you can skip this procedure.

Procedure

1. Log on to the Contact Center server as a local administrator.

   ❗ **Important:**

   If you log on to the server as a domain administrator, this procedure does not complete successfully.

2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. On the Store Access dialog, type the password for the security store, and click **OK**.
4. On the Security Manager screen, select the **Security Configuration** tab.
5. Click **Security Off**.
6. Click **Apply**.
7. On the Security Change Confirmation dialog, click **Confirm**.
8. Click **Log Out**.
9. Restart the Contact Center server.

Stopping Avaya Contact Center Select

About this task

You must stop the Avaya Contact Center Select system before changing the server name or IP address.

Procedure

1. Log on to the Avaya Contact Center Select server.
2. On the Windows System Tray, right-click on the System Management and Monitoring Component (SMMC) system tray icon, and select **Stop System**.

   Avaya Contact Center Select services begin shutting down. When all services are shut down, the SMMC icon in the Windows System Tray changes to the stopped state.

Changing the server name in the operating system

About this task

Change the server name of the Avaya Contact Center Select server operating system to reflect the new name of the server.

Procedure

1. Log on to the Avaya Contact Center Select server as an administrator.
2. On the **Start** screen, click **Control Panel**.
3. Click **System and Security** > **System**.
4. In the **Computer name, domain, and workgroup settings** section, click **Change settings**.
5. Click the **Computer Name** tab.
6. Click **Change**.
7. Type the new server name.
8. Click **OK**.
9. When you receive a prompt, click **Yes** to restart the server.
10. If you are using a Domain Name Service (DNS), contact your local network administrator to update the DNS with the new server name.

Updating the HOSTS file on the Avaya Contact Center Select server

Before you begin

- Determine if you need to update the HOSTS table on your server.

  Important:

  Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows Server 2012 R2.

About this task

If you do not have a DNS server, you must manually update the HOSTS file on the Avaya Contact Center Select server with the new server name and IP address. This ensures that all servers can interpret the new server name.

Procedure

1. Log on to the Avaya Contact Center Select server.

2. Browse to the HOSTS file in the installation directory, `C:\Windows\system32\drivers\etc`.
3. Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4. Update the file to reflect the new server name, IP address, or both.
5. On the **File** menu, click **Save**.
6. Close all windows.

Verifying the server name change

About this task

Verify that the Domain Name Service server or network has the correct server name.

Procedure

1. On the **Desktop** screen, right-click on the Windows icon and select **Run**.
2. In the **Open** box, enter `cmd`.
3. In a Command line window, type `ping` *`<server name>`*.

   Where *<server name>* is the new name of the Avaya Contact Center Select server.
4. Verify that the IP address matches the IP address of the server with the new name.

Synchronizing the operating system name with the Avaya Contact Center Select server name

About this task

Synchronize the operating system name with the Avaya Contact Center Select server name to ensure that the Contact Center suite uses the new server name.

Important:

Ensure that Avaya Contact Center Select services are stopped before you run the Computer Name Synchronisation Utility.

Procedure

1. Log on to the Avaya Contact Center Select server as an administrator.
2. Close the **System Control and Monitor Utility** if it is running.
3. On the **Apps** screen, in the **Avaya** section, select **Computer Update Utility**.
4. Verify that the new Avaya Contact Center Select server name appears in the **New Computer Name** box.

5. Under **System Account Configuration**, in the **Password** box, type the password for the Avaya Contact Center Select administration account. The password is not checked against the server security policy for minimum password requirements. Avaya recommends that you enter a password that conforms to your corporate password policy.
6. In the **Confirm Password** box, type the password.
7. Click **Apply** and click **Yes** to confirm.
8. After the synchronization process is complete, click **Restart** to restart the server.

   Note:

   The Computer Name Synchronisation Utility provides information about the success of the synchronization process for each of the components: Avaya Contact Center Select, Avaya Aura® Media Server, and Avaya IP Office. If you want to view the log file for the synchronization process, click **Open log file** before you click **Restart**.

Configuring the external Web Communications server

Before you begin

- Know the custom interface folder names and paths for the web.xml and .jsp files for the sample Web communications installation.

About this task

If your solution uses an external Web Communications server, configure the Web Communications server to update the files with the new server name.

You must update for .jsp files with Apache Tomcat. If you use a different servlet engine (for example, JRun or WebLogic) or a different technology (ASP.NET), you must use the standard procedures for your environment.

Procedure

1. Log on to your external Web Communications Web server.
2. Open the config file located at `C:\xampp\htdocs\Code\include` in Notepad or another text editor.
3. Locate the text string CCMM_MACHINE_NAME and update the new server name after the ’=’ sign.
4. Save and close the file.

Updating the HOSTS file for clients

Before you begin

- Determine if you need to update the HOSTS table on your client.

Important:

Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows.

About this task

If you do not have a DNS server, you must manually update the HOSTS file on each client in your contact center with the new computer IP address. This ensures that all clients can interpret the new server name.

Procedure

1. Log on to the client computer.
2. Browse to the HOSTS file in the Windows installation directory, `C:\Windows\system32\drivers\etc`.
3. Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4. Update the HOSTS file to reflect the new Avaya Contact Center Select server name or IP address.
5. On the **File** menu, click **Save**.
6. Close all windows.
7. Repeat this procedure on each client computer.

Updating client browsers and shared folders

Before you begin

- Ensure that you export scheduled reports in your Contact Center.
- Ensure that you updated the HOSTS file on the clients with the new Avaya Contact Center Select server name.

Important:

Administrators cannot update the browsers and shared folders for each user, therefore users needs to update their respective browsers and shared folders.

About this task

Update the client browsers and shared folders to reference the new Avaya Contact Center Select server name in the browser.

Procedure

1. Log on to Contact Center Manager Administration as an administrator.
2. From the Launchpad, click **Historical Reporting**.
3. In the Historical Reporting main window, click the **CC** server.

4. For each report associated with the new server, click the report name.
5. In the Report Properties window, click the **Output Options** heading to expand the section.
6. Select the **Output to file** check box.
7. In the **Output** box, browse to the path of the report.
8. Click **Save Report**.
9. Click **Activate**.
10. Close the report.
11. Repeat step 4 to step 10 for each report.

Reinstalling Agent Desktop

Before you begin

- Change the name of the Avaya Contact Center Select server.
- Uninstall Agent Desktop. For more information on installing and uninstalling Agent Desktop, see *Using Agent Desktop for Avaya Contact Center Select* .

About this task

Reinstall Agent Desktop to allow agents to monitor calls and make calls.

Procedure

Install Agent Desktop.

Important:

Install Agent Desktop using the new server name.

Avaya Contact Center Select server IP address change

Change the IP address of the Avaya Contact Center Select server. You must also update the Avaya Aura® Media Server IP address.

Stopping Avaya Contact Center Select

About this task

You must stop the Avaya Contact Center Select system before changing the server name or IP address.

Procedure

1. Log on to the Avaya Contact Center Select server.
2. On the Windows System Tray, right-click on the System Management and Monitoring Component (SMMC) system tray icon, and select **Stop System**.

   Avaya Contact Center Select services begin shutting down. When all services are shut down, the SMMC icon in the Windows System Tray changes to the stopped state.

Changing the contact center subnet IP address of the Avaya Contact Center Select server

About this task

You must perform the following steps to update the Avaya Contact Center Select server IP address references.

Procedure

1. Log on to the Avaya Contact Center Select server.
2. On the **Apps** screen, in the **Avaya** section, select **System Control and Monitor Utility**.
3. On the System Control & Monitor Utility window, click **Shut down Contact Center**.
4. On the **Start** screen, click **Control Panel**.
5. Click **Network and Internet** > **Network and Sharing Center**.
6. Click **Change adapter settings**.
7. Right-click the LAN connection of the contact center subnet network interface card and select **Properties**.
8. Select **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties**.
9. In the **IP address** field, type the new IP address and click **OK**.
10. Click **Close**.
11. Restart the server.
12. If you are using a Domain Name Service (DNS), contact your local network administrator to update the DNS with the new IP address.

Verifying the server IP address change

About this task

Verify that the Domain Name Service server or network has the correct server IP address.

Procedure

1. On the **Desktop** screen, right-click on the Windows icon and select **Run**.
2. In the **Open** box, enter `cmd`.
3. In a Command line window, type `ping <server name>`.

   Where *<server name>* is the name of the Avaya Contact Center Select server.
4. Verify that the IP address matches the new IP address of the server.

Synchronizing the operating system IP address with the Avaya Contact Center Select server IP address

About this task

Synchronize the operating system IP address with the Avaya Contact Center Select server IP address to ensure that the Contact Center suite uses the new server IP address.

Important:

Ensure that Avaya Contact Center Select services are stopped before you run the Computer Name Synchronisation Utility.

Procedure

1. Log on to the Avaya Contact Center Select server as an administrator.
2. Close the **System Control and Monitor Utility** if it is running.
3. On the **Apps** screen, in the **Avaya** section, select **Computer Update Utility**.
4. Verify that the new Avaya Contact Center Select server IP address appears in the **New IP Address** box.
5. Click **Apply** and click **Yes** to confirm.
6. After the synchronization process is complete, click **Restart** to restart the server.

   Note:

   The Computer Name Synchronisation Utility provides information about the success of the synchronization process for each of the components: Avaya Contact Center Select, Avaya Aura® Media Server, and Avaya IP Office. If you want to view the log file for the synchronization process, click **Open log file** before you click **Restart**.

Updating the Avaya Aura® Media Server IP Interface Assignment

About this task

Perform the following procedure if you need to change the IP address of a Windows-based Avaya Aura® Media Server. After you change the IP Interface Assignment, you must start Avaya Aura® Media Server.

Procedure

1. Log on to Avaya Aura® Media Server Element Manager (EM).

   If you are using a remote browser to gain access to EM, use the new IP address in the URL for the EM login.

2. Navigate to **EM** > **System Configuration** > **Network Settings** > **IP Interface Assignment**.
3. The **IP Interface Assignment** fields show errors as a result of the IP address change. Select valid IP addresses from the drop-down menus for the each field showing **Invalid**.
4. Click **Save**.
5. Click **Confirm**.
6. Navigate to **EM** > **System Status** > **Element Status**.
7. Click **Start**.
8. Click **Confirm** to proceed with the action.

   The Avaya Aura® Media Server system starts.

Updating the HOSTS file for clients

Before you begin

- Determine if you need to update the HOSTS table on your client.

  Important:

  Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows.

About this task

If you do not have a DNS server, you must manually update the HOSTS file on each client in your contact center with the new computer IP address. This ensures that all clients can interpret the new server name.

Procedure

1. Log on to the client computer.

2. Browse to the HOSTS file in the Windows installation directory, `C:\Windows\system32\drivers\etc`.
3. Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4. Update the HOSTS file to reflect the new Avaya Contact Center Select server name or IP address.
5. On the **File** menu, click **Save**.
6. Close all windows.
7. Repeat this procedure on each client computer.

Appendix B: Server name or IP address change - software appliance

This Appendix describes the procedures you must perform to change the server names or IP addresses of the Avaya Contact Center Select software appliance. You must perform a server name or IP address change during a Contact Center maintenance window.

Important:

Avaya Contact Center Select does not support changing the server name or IP address of servers configured for Business Continuity. Avaya recommends that you configure the final production name of the Avaya Contact Center Select servers before configuring Business Continuity.

Avaya Contact Center Select server name change

Change the name of the Avaya Contact Center Select server. The new name of the server must meet the specifications of the server names in the Contact Center suite.

Security considerations

If you change the name of a secured Contact Center server, Avaya recommends that you create a new security store with a server certificate that matches the new server name.

Each server certificate has a name, which normally derives from the server Fully Qualified Domain Name (FQDN). If a server certificate name does not match the name of the website or web service to which a client connects, the client generates a warning. Normally on a GUI, a user can bypass the warning and continue. If the client is a service on another system, it does not handle and bypass the warning unless coded to do so.

If you change the server name and do not change the server certificate, users always see warnings when they connect to Contact Center web services.

Solutions that require server certificates

- Solutions that use TLS security for the CTI link to IP Office.
- Solutions using the Agent Browser application. These always use TLS security for the Agent Browser application client.
- Solutions on which you enabled Web Services security.

- Solutions using Secure Real Time Protocol for voice traffic.

Preparing a server certificate before changing the server name

If you use an external Certificate Authority (CA), it can sometimes take an extended period to receive a signed server certificate after submitting your Certificate Signing Request (CSR) to the CA. To minimize the time elapsed for a server name change, you can create a CSR and request and receive a new server certificate before changing the server name. The following high-level procedures outline how to create a new CSR to send to the CA.

Important:

> If the CA you use to sign the new server certificate is different to the CA you used to sign the old server certificate, you must also distribute a new root certificate to all the relevant clients and servers after changing the server name and applying the new server certificate.

To create a new CSR in the Contact Center security store using Security Manager:

- Schedule a maintenance window for this task, because you must stop the Contact Center services.
- In Security Manager, back up the Contact Center security store.
- Delete the existing security store.
- Create a new security store, specifying the planned new server name as the common name for the certificate.
- Copy the CSR content from the new security store, to send to the CA to request a server certificate.
- Restore the Contact Center security store that you backed up.

You can now use the CSR you generated to request a server certificate from a CA. When the CA provides the new server certificate, you can schedule the Contact Center server name change.

In Avaya Aura® Media Server, you can create a new CSR at any time without stopping the server or impacting the existing certificates. Create a new CSR to request a new server certificate from a CA. When the CA provides the new server certificate, you can schedule the server name change.

Avaya Contact Center Select server name change prerequisites

Procedure

- Ensure that the new server name is unique.
- Ensure that the new server name is from 6 to 15 characters and that the first character is alphabetical.
- Ensure that the new server name contains no underscores (_), spaces ( ), or punctuation.

Turning off Web Services security

About this task

Turn off Web Services security before you rename the server. If Web Services security is not enabled on your contact center, you can skip this procedure.

Procedure

1. Log on to the Contact Center server as a local administrator.

   ❗ **Important:**

   If you log on to the server as a domain administrator, this procedure does not complete successfully.

2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. On the Store Access dialog, type the password for the security store, and click **OK**.
4. On the Security Manager screen, select the **Security Configuration** tab.
5. Click **Security Off**.
6. Click **Apply**.
7. On the Security Change Confirmation dialog, click **Confirm**.
8. Click **Log Out**.
9. Restart the Contact Center server.

Stopping Avaya Contact Center Select

About this task

You must stop the Avaya Contact Center Select system before changing the server name or IP address.

Procedure

1. Log on to the Avaya Contact Center Select server.
2. On the Windows System Tray, right-click on the System Management and Monitoring Component (SMMC) system tray icon, and select **Stop System**.

   Avaya Contact Center Select services begin shutting down. When all services are shut down, the SMMC icon in the Windows System Tray changes to the stopped state.

Changing the server name in the operating system

About this task

Change the server name of the Avaya Contact Center Select server operating system to reflect the new name of the server.

Procedure

1. Log on to the Avaya Contact Center Select server as an administrator.
2. On the **Start** screen, click **Control Panel**.
3. Click **System and Security** > **System**.
4. In the **Computer name, domain, and workgroup settings** section, click **Change settings**.
5. Click the **Computer Name** tab.
6. Click **Change**.
7. Type the new server name.
8. Click **OK**.
9. When you receive a prompt, click **Yes** to restart the server.
10. If you are using a Domain Name Service (DNS), contact your local network administrator to update the DNS with the new server name.

Updating the HOSTS file on the Avaya Contact Center Select server

Before you begin

- Determine if you need to update the HOSTS table on your server.

  ! **Important:**

  Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows Server 2012 R2.

About this task

If you do not have a DNS server, you must manually update the HOSTS file on the Avaya Contact Center Select server with the new server name and IP address. This ensures that all servers can interpret the new server name.

Procedure

1. Log on to the Avaya Contact Center Select server.

2. Browse to the HOSTS file in the installation directory, `C:\Windows\system32\drivers\etc`.
3. Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4. Update the file to reflect the new server name, IP address, or both.
5. On the **File** menu, click **Save**.
6. Close all windows.

Verifying the server name change

About this task

Verify that the Domain Name Service server or network has the correct server name.

Procedure

1. On the **Desktop** screen, right-click on the Windows icon and select **Run**.
2. In the **Open** box, enter `cmd`.
3. In a Command line window, type `ping <server name>`.

   Where *<server name>* is the new name of the Avaya Contact Center Select server.
4. Verify that the IP address matches the IP address of the server with the new name.

Synchronizing the operating system name with the Avaya Contact Center Select server name

About this task

Synchronize the operating system name with the Avaya Contact Center Select server name to ensure that the Contact Center suite uses the new server name.

Important:

Ensure that Avaya Contact Center Select services are stopped before you run the Computer Name Synchronisation Utility.

Procedure

1. Log on to the Avaya Contact Center Select server as an administrator.
2. Close the **System Control and Monitor Utility** if it is running.
3. On the **Apps** screen, in the **Avaya** section, select **Computer Update Utility**.
4. Verify that the new Avaya Contact Center Select server name appears in the **New Computer Name** box.

5. Under **System Account Configuration**, in the **Password** box, type the password for the Avaya Contact Center Select administration account. The password is not checked against the server security policy for minimum password requirements. Avaya recommends that you enter a password that conforms to your corporate password policy.
6. In the **Confirm Password** box, type the password.
7. Click **Apply** and click **Yes** to confirm.
8. After the synchronization process is complete, click **Restart** to restart the server.

   Note:

   The Computer Name Synchronisation Utility provides information about the success of the synchronization process for each of the components: Avaya Contact Center Select, Avaya Aura® Media Server, and Avaya IP Office. If you want to view the log file for the synchronization process, click **Open log file** before you click **Restart**.

Configuring Avaya Aura® Media Server name resolution

About this task

Configure Avaya Aura® Media Server to resolve the hostname and Fully Qualified Domain Name (FQDN) of the Contact Center Manager Administration server. The Contact Center Manager Administration (CCMA) software is installed on the Contact Center server.

Procedure

1. Log on to Element Manager with administrative privileges.
2. Navigate to **EM** > **System Configuration** > **Network Settings** > **Name Resolution**.
3. Click **Add**.
4. In the **IP Address** box, enter the Contact Center Manager Administration IP address.
5. In the **Hostname** box, enter the Contact Center Manager Administration hostname.
6. Click **Save**.

Configuring the external Web Communications server

Before you begin

- Know the custom interface folder names and paths for the web.xml and .jsp files for the sample Web communications installation.

About this task

If your solution uses an external Web Communications server, configure the Web Communications server to update the files with the new server name.

You must update for .jsp files with Apache Tomcat. If you use a different servlet engine (for example, JRun or WebLogic) or a different technology (ASP.NET), you must use the standard procedures for your environment.

Procedure

1. Log on to your external Web Communications Web server.
2. Open the config file located at `C:\xampp\htdocs\Code\include` in Notepad or another text editor.
3. Locate the text string CCMM_MACHINE_NAME and update the new server name after the '=' sign.
4. Save and close the file.

Updating the HOSTS file for clients

Before you begin

- Determine if you need to update the HOSTS table on your client.

  Important:

  Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows.

About this task

If you do not have a DNS server, you must manually update the HOSTS file on each client in your contact center with the new computer IP address. This ensures that all clients can interpret the new server name.

Procedure

1. Log on to the client computer.
2. Browse to the HOSTS file in the Windows installation directory, `C:\Windows\system32\drivers\etc`.
3. Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4. Update the HOSTS file to reflect the new Avaya Contact Center Select server name or IP address.
5. On the **File** menu, click **Save**.
6. Close all windows.
7. Repeat this procedure on each client computer.

Updating client browsers and shared folders

Before you begin

- Ensure that you export scheduled reports in your Contact Center.
- Ensure that you updated the HOSTS file on the clients with the new Avaya Contact Center Select server name.

  ❗ **Important:**

  Administrators cannot update the browsers and shared folders for each user, therefore users needs to update their respective browsers and shared folders.

About this task

Update the client browsers and shared folders to reference the new Avaya Contact Center Select server name in the browser.

Procedure

1. Log on to Contact Center Manager Administration as an administrator.
2. From the Launchpad, click **Historical Reporting**.
3. In the Historical Reporting main window, click the **CC** server.
4. For each report associated with the new server, click the report name.
5. In the Report Properties window, click the **Output Options** heading to expand the section.
6. Select the **Output to file** check box.
7. In the **Output** box, browse to the path of the report.
8. Click **Save Report**.
9. Click **Activate**.
10. Close the report.
11. Repeat step 4 to step 10 for each report.

Reinstalling Agent Desktop

Before you begin

- Change the name of the Avaya Contact Center Select server.
- Uninstall Agent Desktop. For more information on installing and uninstalling Agent Desktop, see *Using Agent Desktop for Avaya Contact Center Select* .

About this task

Reinstall Agent Desktop to allow agents to monitor calls and make calls.

Procedure

Install Agent Desktop.

Important:

Install Agent Desktop using the new server name.

Avaya Contact Center Select server IP address change

Change the IP address of the Avaya Contact Center Select server.

Important:

After you change the IP address of the virtualized Avaya Contact Center Select server, you must request a new license. Your existing license is no longer valid after you change the IP address.

Stopping Avaya Contact Center Select

About this task

You must stop the Avaya Contact Center Select system before changing the server name or IP address.

Procedure

1. Log on to the Avaya Contact Center Select server.
2. On the Windows System Tray, right-click on the System Management and Monitoring Component (SMMC) system tray icon, and select **Stop System**.

   Avaya Contact Center Select services begin shutting down. When all services are shut down, the SMMC icon in the Windows System Tray changes to the stopped state.

Changing the contact center subnet IP address of the Avaya Contact Center Select server

About this task

You must perform the following steps to update the Avaya Contact Center Select server IP address references.

Procedure

1. Log on to the Avaya Contact Center Select server.
2. On the **Apps** screen, in the **Avaya** section, select **System Control and Monitor Utility**.

3. On the System Control & Monitor Utility window, click **Shut down Contact Center**.
4. On the **Start** screen, click **Control Panel**.
5. Click **Network and Internet** > **Network and Sharing Center**.
6. Click **Change adapter settings**.
7. Right-click the LAN connection of the contact center subnet network interface card and select **Properties**.
8. Select **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties**.
9. In the **IP address** field, type the new IP address and click **OK**.
10. Click **Close**.
11. Restart the server.
12. If you are using a Domain Name Service (DNS), contact your local network administrator to update the DNS with the new IP address.

Verifying the server IP address change

About this task

Verify that the Domain Name Service server or network has the correct server IP address.

Procedure

1. On the **Desktop** screen, right-click on the Windows icon and select **Run**.
2. In the **Open** box, enter `cmd`.
3. In a Command line window, type `ping <server name>`.

   Where *<server name>* is the name of the Avaya Contact Center Select server.
4. Verify that the IP address matches the new IP address of the server.

Synchronizing the operating system IP address with the Avaya Contact Center Select server IP address

About this task

Synchronize the operating system IP address with the Avaya Contact Center Select server IP address to ensure that the Contact Center suite uses the new server IP address.

Important:

Ensure that Avaya Contact Center Select services are stopped before you run the Computer Name Synchronisation Utility.

Procedure

1. Log on to the Avaya Contact Center Select server as an administrator.
2. Close the **System Control and Monitor Utility** if it is running.
3. On the **Apps** screen, in the **Avaya** section, select **Computer Update Utility**.
4. Verify that the new Avaya Contact Center Select server IP address appears in the **New IP Address** box.
5. Click **Apply** and click **Yes** to confirm.
6. After the synchronization process is complete, click **Restart** to restart the server.

   Note:

   The Computer Name Synchronisation Utility provides information about the success of the synchronization process for each of the components: Avaya Contact Center Select, Avaya Aura® Media Server, and Avaya IP Office. If you want to view the log file for the synchronization process, click **Open log file** before you click **Restart**.

Configuring Avaya Aura® Media Server name resolution

About this task

Configure Avaya Aura® Media Server to resolve the hostname and Fully Qualified Domain Name (FQDN) of the Contact Center Manager Administration server. The Contact Center Manager Administration (CCMA) software is installed on the Contact Center server.

Procedure

1. Log on to Element Manager with administrative privileges.
2. Navigate to **EM** > **System Configuration** > **Network Settings** > **Name Resolution**.
3. Click **Add**.
4. In the **IP Address** box, enter the Contact Center Manager Administration IP address.
5. In the **Hostname** box, enter the Contact Center Manager Administration hostname.
6. Click **Save**.

Updating Avaya Aura® Media Server trusted node IP addresses

About this task

After you change the Avaya Contact Center Select IP address, you must update the Avaya Aura® Media Server trusted node IP addresses in Element Manager (EM).

Procedure

1. Log on to Avaya Aura® Media Server Element Manager.

2. Navigate to **EM** > **System Configuration** > **Signaling Protocols** > **SIP** > **Nodes and Routes**.
3. Click **Add**.
4. On the **Add SIP Trusted Node** page, in the **Host or Server Address** field, type the new IP address of the Avaya Contact Center Select server.
5. Click **Save**.
6. In the navigation pane, click **System Configuration** > **Network Settings** > **General Settings**.
7. Click **SOAP**.
8. In the **Trusted Nodes** box, type the new IP address of the Avaya Contact Center Select server.
9. Select **Enable Trusted SOAP Nodes**.
10. Click **Save**.

Updating the HOSTS file for clients

Before you begin

- Determine if you need to update the HOSTS table on your client.

Important:

Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows.

About this task

If you do not have a DNS server, you must manually update the HOSTS file on each client in your contact center with the new computer IP address. This ensures that all clients can interpret the new server name.

Procedure

1. Log on to the client computer.
2. Browse to the HOSTS file in the Windows installation directory, `C:\Windows\system32\drivers\etc`.
3. Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4. Update the HOSTS file to reflect the new Avaya Contact Center Select server name or IP address.
5. On the **File** menu, click **Save**.
6. Close all windows.

7. Repeat this procedure on each client computer.

Avaya Aura® Media Server name change

Change the server name of Avaya Aura® Media Server and update the Avaya Contact Center Select server to reflect the changes.

Changing the name of the Avaya Aura® Media Server on Linux

Before you begin

- Stop Avaya Contact Center Select using System Control and Monitor Utility (SCMU) or System Management and Monitoring Component (SMMC).

About this task

Perform the following procedure if you need to change the host name of a Linux-based Avaya Aura® Media Server.

Procedure

1. Log on to Avaya Aura® Media Server Element Manager (EM).
2. Navigate to **EM** > **System Status** > **Element Status**.
3. Click **Stop**.
4. Click **Confirm** to proceed with the action.

   After a few seconds, the system updates the status fields and activates or deactivates the buttons based on the new state of the media server.
5. On the Linux server, edit the file `/etc/hosts`.
6. Update the host name wherever the host name appears in the file.
7. Save the file.
8. Edit the file `/etc/sysconfig/network`.
9. Update the host name wherever the host name appears in the file.
10. Save the file.
11. Using a Linux shell, enter the following command to apply the host name change to the system:

    ```
    hostname <new_hostname>
    ```

    Where <new_hostname> is the new name for the server.
12. In Element Manager, navigate to **EM** > **System Status** > **Element Status**.
13. Click **Start**.

14. Click **Confirm** to proceed with the acti

Updating the Avaya Aura® Media Server details in CCMA

About this task

Update the media server details configured in Contact Center Manager Administration to match the new Avaya Aura® Media Server changes. Avaya Contact Center Select uses Avaya Aura® Media Server media processing capabilities to support conferencing, announcements and dialogs.

Procedure

1. Log on to Contact Center Manager Administration with administrator privileges.
2. On the **Launchpad**, click **Configuration**.
3. In the left pane, expand **CC**.
4. Select **Media Servers**.
5. On the **Media Servers** window, in the **Server Name** box, type the server name of the Avaya Aura® Media Server server.
6. In the **IP Address** box, type the IP address of the Avaya Aura® Media Server server.
7. In the **Port Number** box, type the port number.

   Important:

   The port number must match the Avaya Aura® Media Server port number. The default is 5060.
8. Click the next row of the grid to save your changes.

Avaya Aura® Media Server IP address change

Change the IP address of Avaya Aura® Media Server and update the Avaya Contact Center Select server to reflect the changes.

Changing the Avaya Aura® Media Server IP address on Linux

Before you begin

- Stop Avaya Contact Center Select using System Control and Monitor Utility (SCMU) or System Management and Monitoring Component (SMMC).

About this task

Perform the following procedure if you need to change the IP address of a Linux-based Avaya Aura® Media Server. The network adapter names and network configuration file names can differ to the names on your server.

After you change the Avaya Aura® Media Server IP address, you must update the Avaya Aura® Media Server IP Interface Assignment in Element Manager (EM).

Procedure

1. Log on to Avaya Aura® Media Server Element Manager.
2. Navigate to **EM** > **System Status** > **Element Status**.
3. Click **Stop**.
4. Click **Confirm** to proceed with the action.

   After a few seconds, the system updates the status fields and activates or deactivates the buttons based on the new state of the media server.
5. On the Linux server, edit the file `/etc/hosts`.
6. If the hosts file contains an existing entry for the Avaya Aura® Media Server, remove the entry. Do not update the entry or add an Avaya Aura® Media Server entry to the hosts file.
7. Save the file.
8. Edit the file `/etc/sysconfig/network-scripts/ifcfg-eth0`.
9. Update the IP address wherever the IP address appears in the file.
10. Save the file.
11. Using the local Linux console shell, enter the following commands to apply the IP address change to the system:

    ```
    /etc/init.d/network stop
    ```

    ```
    /etc/init.d/network start
    ```
12. Log on to Element Manager using the new IP address in the URL for the EM login.
13. In the navigation pane, click **System Configuration** > **Network Settings** > **IP Interface Assignment**.
14. **IP Interface Assignment** fields show errors, as a result of the IP address change. Select valid IP addresses from the drop-down menus for each field showing **Invalid**.
15. Click **Save**.
16. Click **Confirm**.
17. Using the local Linux console shell, enter the following commands to restart Avaya Aura® Media Server:

    ```
    reboot
    ```

Updating the Avaya Aura® Media Server details in CCMA

About this task

Update the media server details configured in Contact Center Manager Administration to match the new Avaya Aura® Media Server changes. Avaya Contact Center Select uses Avaya Aura® Media Server media processing capabilities to support conferencing, announcements and dialogs.

Procedure

1. Log on to Contact Center Manager Administration with administrator privileges.
2. On the **Launchpad**, click **Configuration**.
3. In the left pane, expand **CC**.
4. Select **Media Servers**.
5. On the **Media Servers** window, in the **Server Name** box, type the server name of the Avaya Aura® Media Server server.
6. In the **IP Address** box, type the IP address of the Avaya Aura® Media Server server.
7. In the **Port Number** box, type the port number.

   Important:

   The port number must match the Avaya Aura® Media Server port number. The default is 5060.
8. Click the next row of the grid to save your changes.

Index