AVAYA

Avaya Aura® Contact Center Client Administration

Contents

Comments on this document?

Chapter 1: Introduction

Purpose

This guide describes the tasks that administrators and supervisors of Avaya Aura® Contact Center can perform in Contact Center Manager Administration.

Intended audience

This guide is for personnel who administer and customize the Avaya Aura® Contact Center solution.

Related resources

Avaya Aura® Contact Center documentation

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

Title	Document purpose	Audience
Overview		

Table continues…

Title	Document purpose	Audience
Avaya Aura® Contact Center Overview and Specification	This document provides the high-level technical details you need to set up your Contact Center suite. The document contains background planning and engineering information, including server preparation information, routing options, licensing configurations, and hardware configuration information. It also contains the background information you require to install all software components that are part of and work with Contact Center. General information about considerations for upgrading your existing Contact Center is also included. This document contains strategies and requirements to plan your network configuration and prepare your servers for Contact Center software installations.	Customers and sales, services, and support personnel
Avaya Aura® Contact Center and Avaya Aura® Unified Communications Solution Description	This document describes the solution architecture, suggested topologies, and capacities for the Avaya Aura® Unified Communications (UC) platform. This document also describes the features and functional limitations of certain configurations.	Customers and sales, services, and support personnel
Avaya Aura® Contact Center and Avaya Communication Server 1000 Solution Description	This document describes the solution architecture, suggested topologies, and capacities for the Avaya Communication Server 1000 platform. This document also describes the features and functional limitations of certain configurations.	Customers and sales, services, and support personnel
Avaya Aura® Contact Center Documentation Catalog	This document contains high-level information about Avaya Aura® Contact Center documentation resources and the type of information in each document.	Customers and sales, services, and support personnel
Avaya Aura® Contact Center Terminology	This document contains definitions for the technical terms specific to Contact Center.	Customers and sales, services, and support personnel
Contact Center Performance Management Data Dictionary	This document contains reference tables that describe statistics and data in historical and real-time reports generated in Contact Center.	System administrators and contact center supervisors

Table continues…

Title	Document purpose	Audience
Implementing		
Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration	This document contains information and procedures to integrate the Avaya Aura® UC platform with Contact Center.	Implementation personnel
Avaya Aura® Contact Center and Avaya Communication Server 1000 Integration	This document contains information and procedures to integrate the Avaya Communication Server 1000 platform with Contact Center.	Implementation personnel
Deploying Avaya Aura® Contact Center DVD for Avaya Aura® Unified Communications	This document contains information about Contact Center DVD installation, initial configuration, and verification for the Avaya Aura® UC platform.	Implementation personnel
Deploying Avaya Aura® Contact Center DVD for Avaya Communication Server 1000	This document contains information about Contact Center DVD installation, initial configuration, and verification for the Avaya Communication Server 1000 platform.	Implementation personnel
Deploying Avaya Aura® Contact Center Software Appliance for Avaya Aura® Unified Communications	This document describes how to deploy the Avaya Aura® Contact Center Software Appliance for the Avaya Aura® UC platform.	Implementation personnel
Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications	This document describes Contact Center preparation, initial configuration, and verification of the installation on the Avaya Aura® UC platform.	Implementation personnel
Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000	This document describes Contact Center preparation, initial configuration, and verification of the installation on the Avaya Communication Server 1000 platform.	Implementation personnel
Avaya Aura® Contact Center and Proactive Outreach Manager Integration	This document provides conceptual and procedural information on the integration between Avaya Aura® Contact Center (AACC) and Avaya Proactive Outreach Manager (POM). It describes the tasks required for AACC and POM integration.	Implementation personnel
Upgrading and patching Avaya Aura® Contact Center	This document contains information and procedures to upgrade from previous releases to Contact Center, migrating the databases, and information and procedures to download and install service packs.	Implementation personnel and system administrators

Table continues…

Title	Document purpose	Audience
Administering		
Avaya Aura® Contact Center Server Administration	This document contains information and procedures for day-to-day maintenance of all servers in the Contact Center suite, including server maintenance tasks, administrative tasks, managing data, configuring data routing, performing archives, and backing up data. It also describes optional configuration procedures.	System administrators
Avaya Aura® Contact Center Client Administration	This document contains information and procedures to configure users and user access, skillsets, server management, and configuration data in the Contact Center database.	System administrators and contact center supervisors
Using Contact Center Orchestration Designer	This document contains information and procedures to configure script and flow applications in Orchestration Designer.	System administrators
Maintaining		
Maintaining Avaya Aura® Contact Center	This document contains routine maintenance procedures, such as installing service packs and maintaining the databases for the Contact Center system.	System administrators and support personnel
Troubleshooting Avaya Aura® Contact Center	This document contains system-wide troubleshooting information and procedures for Contact Center hardware, software, and network.	System administrators and support personnel
Contact Center Event Codes	This Microsoft Excel spreadsheet contains a list of errors in the Contact Center suite and recommendations to resolve them.	System administrators and support personnel
Using		
Using Avaya Aura® Contact Center Reports and Displays	This document contains procedures to generate performance reports, and to monitor and analyze performance data and performance measurements.	System administrators and contact center supervisors
Using Agent Desktop for Avaya Aura® Contact Center	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

Table continues…

Title	Document purpose	Audience
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
Using Avaya Workspaces for AACC and ACCS	This document describes the tasks that Contact Center agents can perform using Avaya Workspaces.	Contact center agents and supervisors
Release Notes		
Avaya Aura® Contact Center Release Notes	The Release Notes contain information about known issues, patches, and workarounds.	System administrators and support personnel

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.

2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.

3. Click **Product Support** > **Documents**.

4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.

5. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.

6. **(Optional)** In **Enter Keyword**, type keywords for your search.

7. From the **Select Content Type** list, select one or more content types.

   For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.

8. Click 🔍 to display the search results.

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.

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

  ✱ **Note:**

    Videos are not available for all products.

Support

Go to the Avaya Support website at https://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 detail what changed in *Avaya Aura® Contact Center Client Administration* in Release 7.1.x.

Features

See the following sections for information about new features in Release 7.1.x.

New features in the Release 7.1 base build

See the following sections for information about new features in the Release 7.1 base build:

Avaya Aura® Contact Center interoperates with Avaya Vantage™

From Release 7.1, Avaya Aura® Contact Center supports Avaya Vantage™. The Avaya Vantage™ device combines the advantages of a customizable unified communications solution and a fully functional Android device.

Avaya Workplace Client is a supported SIP phone application on Avaya Vantage™.

Support for Avaya Workspaces

From Release 7.1, Contact Center supports Avaya Workspaces — a client for voice, video, email and webchat contact types.

Video contacts

From Release 7.1, Contact Center supports routed video contacts. Contact Center supports both skillset and non-skillset video contacts. Video contacts are reported on in both real-time and historical reports. You can view video calls using Avaya Workplace Client or Avaya Vantage™, but you must use Avaya Agent Desktop or Avaya Workspaces for call control actions.

To support video contacts, your solution must include Avaya Aura® Web Gateway 3.3 or later.

Unsent email monitoring

From Release 7.1, you can use the Contact Center Multimedia Dashboard utility to view the number of unsent emails, analyze why emails were not sent, and manage unsent emails. The spike detection feature provides automatic monitoring of unsent messages and generates alarms

when the number of unsent emails exceeds the defined threshold. You can configure spike detection values, such as the number of days and the percentage of unsent emails.

New features in Release 7.1 Service Pack 1 and 2

There are no new features in Release 7.1 Service Pack 1 and 2.

New features in Release 7.1 Service Pack 3

There are no new features in this document for Release 7.1 Service Pack 3.

New features in Release 7.1 Feature Pack 1

See the following sections for information about new features in Release 7.1 Feature Pack 1:

Avaya Workspaces supports Open Queue

From Release 7.1 Feature Pack 1, agents using Avaya Workspaces can handle Open Queue contacts. Avaya Workspaces displays Open Queue contacts as Generic.

Avaya Workspaces supports outbound campaign contacts

From Release 7.1 Feature Pack 1, agents using Avaya Workspaces can handle outbound campaign calls. The feature provides the interface that presents outbound campaign contacts to agents, provides agents with preview dial capability, displays agent call scripts (if configured), and saves disposition codes and script results.

Lockout of inactive CCMA accounts

From Release 7.1 Feature Pack 1, you can configure CCMA to lock accounts that have not been used for a configured period of time. Only administrators can unlock the locked accounts.

Multimedia Data Management utility access

From Release 7.1 Feature Pack 1, you must access the Multimedia Data Management utility using CCMA. The Multimedia Data Management utility is no longer available from the Windows start menu.

New features in Release 7.1 Feature Pack 2

See the following sections for information about new features in Release 7.1 Feature Pack 2:

CCMA Password Policy configuration for human and programmatic accounts

From Release 7.1 Feature Pack 2, Contact Center provides the ability to configure CCMA Password Policy. Password Policy is a set of rules that CCMA uses to validate passwords for CCMA accounts. You can select one of the CCMA Password Policy modes: Basic Security mode and Advanced Security mode. You can either use default Basic Security mode with fixed password rules, or enable Advanced Security mode, which allows you to customize your Password Policy

for human and programmatic accounts. When creating or updating a CCMA user, you can view current CCMA password rules.

Contact Center Manager Administration supported in Microsoft Edge with IE mode

From Release 7.1 Feature Pack 2, you can access Contact Center Manager Administration using Microsoft Edge with Internet Explorer (IE) mode.

New features in Release 7.1 Feature Pack 2 Post GA Patches

See the following sections for information about new features in Release 7.1 Feature Pack 2 Post GA Patches:

Avaya Aura® Contact Center Release 7.1 Feature Pack 2 Post GA Patches supports Microsoft Windows 11

From Release 7.1 Feature Pack 2 Post GA Patches, Avaya Aura® Contact Center supports Microsoft Windows 11 for Avaya Agent Desktop, Contact Center Manager Administration, Contact Center Multimedia Administration, and Communication Control Toolkit.

Avaya Aura® Contact Center Release 7.1 Feature Pack 2 Post GA Patches supports Microsoft Windows Server 2019

Avaya Aura® Contact Center Release 7.1 Feature Pack 2 Post GA Patches supports the Microsoft Windows Server 2019 operating system. Customers that upgrade to Avaya Aura® Contact Center Release 7.1 Feature Pack 2 Post GA Patches and want to use Windows Server 2019 must perform a fresh installation on a new Microsoft Windows Server 2019. For more information about restoring the database to the new server, see *Upgrading and patching Avaya Aura® Contact Center*.

New features in Release 7.1.2 Service Pack 2

Release 7.1.2.2 introduces new Avaya Workspaces features. Other changes, which are described later in this chapter, include interoperability and related updates.

Avaya Workspaces features for Release 7.1.2.2

Release 7.1.2.2 introduces the following Avaya Workspaces features for Avaya Aura® Contact Center (AACC) and Avaya Contact Center Select (ACCS). For more information about Avaya Workspaces features, see *Using Avaya Workspaces for AACC and ACCS*.

Consult, transfer, and conference options for web chat

You can consult with another agent during a chat interaction. Messages between agents are whispered so the customer does not see them.

If the other agent agrees, you can do one of the following when ending the consultation:

- Transfer the web chat to the other agent.
- Start a conference.

Observe web chat

A supervisor can observe a chat interaction from the My Agents widget.

Whisper coaching during web chat

While observing a chat interaction, the supervisor can start coaching. During the coaching session, the supervisor can whisper guidance to the agent. The customer does not see whispered messages.

Barge in to web chat

A supervisor can barge in to the chat interaction and communicate with the customer directly.

Email approval

A supervisor can approve or reject an email and add review comments. The agent can edit the email and add comments if it is rejected.

Reschedule email

You can postpone work on an email and reschedule it for a later time. This is a useful option if you need more time to gather information before completing the email.

Email transfer enhancements and new forwarding option

Previously, you could only transfer an email interaction to a skillset. Now, you can also transfer the email to another agent. In addition, you can also forward an email to any email address.

Multiple keyword search

You can use multiple keywords when searching through email templates and suggested content.

Customer history view

Customer history information for all contact types (voice and multimedia) is now displayed together in the same table.

Other changes

See the following sections for information about other changes in Release 7.1.x. Outdated interoperability information has been removed.

Other changes in Release 7.1 Service Packs 1, 2, and 3

There are no other changes in these Service Packs. Outdated interoperability information for Release 7.1 base build has been removed.

Other changes in Release 7.1 Feature Pack 2

The following section contains interoperability information for this Feature Pack. Outdated information has been removed from this document.

Avaya Proactive Outreach Manager update

From Release 7.1 Feature Pack 2, Avaya Aura® Contact Center supports Avaya Proactive Outreach Manager Release 3.1.3.x and 4.0.

Other changes in Release 7.1.2 Service Pack 2

The following sections outline interoperability and other changes in Release 7.1.2.2:

Interoperability with the latest WebLM releases

In Release 7.1.2.2, the latest versions of WebLM 8.1.3.x and 10.1.x are supported.

VMware support

Contact Center Release 7.1.2.2 supports ESXi 7.0 and 8.0 Update 2. Earlier VMware versions, including 6.5 and 6.7, are no longer supported.

See the VMware website for general lifecycle policy information.

End of support for Internet Explorer

Microsoft ended support for the Internet Explorer (IE) web browser in June 2022.

Many Contact Center applications, such as Contact Center Manager Administration (CCMA), Contact Center Multimedia (CCMM), and Communication Control Toolkit (CCT) require the IE engine. To run these applications, you must use Microsoft Edge in IE mode. If you are using Windows 10, IE can be disabled but cannot be removed from your computer. With Windows 11, you do not need to install the IE browser because Edge already includes the IE engine.

Windows operating system support

The following Microsoft operating systems are no longer supported:

- Windows 7 and 8.1
- Windows Server 2012 R2 and earlier versions

See the Microsoft website for lifecycle policy information.

Avaya Aura® Media Server interoperability

Contact Center now supports Avaya Aura® Media Server Release 10.1.x. Release 8.0.x is also supported.

Interoperability with Avaya Aura®

Avaya Aura® Contact Center Release 7.1.2.2 supports interoperability with Avaya Aura® Release 8.1.3, 10.1.x, and 10.2.

Chapter 3: Contact Center Manager Administration client operation

This section describes the procedures to operate the Contact Center Manager Administration (CCMA) client.

Prerequisites

Ensure you have a username and password to access Contact Center Manager Administration.

Contact Center Multimedia Administration and Multimedia Data Management utility access

Access Contact Center Multimedia (CCMM) Administration and the Multimedia Data Management utility by using Contact Center Manager Administration (CCMA). Use CCMM Administration to configure and maintain multimedia resources. Use the Multimedia Data Management utility to manage database contacts and customer privacy requests. This guide explains how to access CCMM Administration and the Multimedia Data Management utility.

For more information about accessing these utilities, see Starting the Contact Center Multimedia Administration utility on page 27 and Starting the Multimedia Data Management Administration utility on page 27. For information about using these utilities, see *Avaya Aura® Contact Center Server Administration*.

Logging in to Contact Center Manager Administration for the first time

About this task

Log in to configure and administer Contact Center Manager Server (CCMS). To access CCMA, use Microsoft Edge in Internet Explorer (IE) mode.

Log in for the first time as the default administrator, webadmin. For security reasons, change the default password when you first log in to the application. CCMA user passwords can contain only English characters and special characters. Passwords must be at least eight characters long with no spaces, and include at least one number, one uppercase letter, and one lowercase letter.

If you have a High Availability campus solution, log in to the CCMA web client using the managed name of the High Availability server pair. If an active application or server fails, the CCMA client web browser continues to use the managed name and you can continue working without interruption.

> **Important:**
>
> CCMA supports one concurrent user session only. If the same credentials are used to log in to CCMA on a different client, the active session is terminated.

Procedure

1. In your browser, type the server URL and then press `Enter`.

   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. Do not use the server IP address.

   If your site does not use the default port for Internet Information Services (IIS), the URL of the server is `https://<server name>: <port number>`, where *<server name>* is the computer name of the Contact Center server, and *<port number>* is the port for the CCMA site in IIS. For example, `https://ccserver:81.`

2. In the main login window, in the **User ID** field, type the username.

3. In the **Password** field, type the password.

4. Click **Login**.

5. On the Change Password window, in the **Old password** field, type the old password.

6. In the **New password** field, type the new password.

7. In the **Confirm password** field, retype the new password.

8. Click **Change Password**.

   The main login window is displayed.

9. In the **User ID** field, type the username.

10. In the **Password** field, type the new password.

11. Click **Login**.

Logging out of Contact Center Manager Administration

About this task

Log out to exit Contact Center Manager Administration.

Procedure

On the Contact Center Manager Administration Launchpad, click **Logout**.

Changing a user password

About this task

As an administrator, you can configure a setting that forces users to change their password when they log in to Contact Center Manager Administration for the first time. By default, the force password change feature is enabled.

Change a default user password in CCMA for security reasons. Before you change a user password, you must authenticate using your password.

Avaya highly recommends that you change default passwords. 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: \ & : < > |

Before you begin

Log in to Contact Center Manager Administration using the credentials for the user whose password you are changing.

Procedure

1. On the Launchpad, click **Change Password**.
2. In the **Old password** field, type the old password.
3. In the **New password** field, type the new password.
4. In the **Confirm password** field, type the new password again.
5. Click **Change Password**.

   You must log in again with the new password.

Starting the Contact Center Multimedia Administration utility

About this task

Use this procedure to log in to the CCMM Administration utility, which you can use to configure and maintain multimedia resources. For information about using CCMM Administration, see *Avaya Aura® Contact Center Server Administration*.

Procedure

1. Log in to Contact Center Manager Administration.

   If configured in the security settings, CCMA displays the date and time of your last login and the number of failed login attempts since your last successful login.

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

3. In the left pane, select the CCMM server to administer.

4. Select **Install prerequisite software**.

5. Click **Launch Multimedia Client**.

6. In the File Download box, click **Run**.

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

Starting the Multimedia Data Management Administration utility

About this task

Use this procedure to log on to the Multimedia Data Management utility, so that you can manage database contacts and customer privacy requests. For information on using the Data Management Administration utility, see *Avaya Aura® Contact Center Server Administration*.

Procedure

1. Log on to Contact Center Manager Administration.

   If configured in Contact Center Manager Administration (CCMA) Security Settings, CCMA displays the date and time of your last login and also the number of failed login attempts since your last successful login.

2. On the Launchpad, click **Data Management**.

3. In the left pane, select the CCMM server to administer.

   The system displays the Multimedia Administration screen in the right pane.

4. Select **Install prerequisite software**.

5. Click **Launch Data Management Client**.

6. On the File Download box, click **Run**.

   The prerequisite software takes some time to install. After the install, the system displays the CCMM Data Management Administration utility.

Opening the Connection Status window

Before you begin

- Log on to Contact Center Manager Administration.

About this task

Open the Connection Status window to display a list of servers currently administered by CCMA, along with the local time and connection status of each server.

Procedure

1. On the CCMA launchpad, click a component.

2. From the **Status** menu, choose **Connection Status**.

   A green dot beside the server indicates that it is online and operational. A red dot indicates that the server is off-line or not responding. A brown dot indicates that the server is in grace period.

3. In the CCM Server Connection Status window, click **Refresh** to refresh the status and local time of all the servers listed.

4. Click **Close**.

Using the Audit Trail

Before you begin

- Log on to Contact Center Manager Administration.

About this task

Use the Audit Trail to view a list of actions performed in Contact Center Management, Access and Partition Management, Historical Reporting, Scripting, Configuration, and Prompt Management as well as the user ID of the person who made the changes.

You can also monitor when a user logs on or logs off of Contact Center Manager Administration.

Procedure

On the Contact Center Manager Administration **Launchpad** banner, click the **Audit Trail** link.

OR

To open the Audit Trail if you are within a component, click the **Launchpad** menu of that component.

Configuring the size of the Audit Trail

Before you begin

- Log on to Contact Center Manager Administration application. See Logging in to Contact Center Manager Administration for the first time on page 24.

About this task

Configure the size of the Audit Trail to configure the number of stored Audit Trail events.

By default, the number of events stored is 1000, but can be increased to a maximum of 10 000. However, the more events you store, the longer it takes to retrieve the event information and display it online. If you reduce the maximum number of events, then events over the new maximum are permanently deleted from the database.

Procedure

1. On the CCMA launchpad, click **Audit Trail**.

2. On the Audit Trail page, from the **Administration** menu, choose **Edit Database Size**.

3. In the Change Audit Trail Preferences window, in the **Maximum number of events stored** box, type the maximum number of events to store in the database.

4. Click **Submit**.

5. Click **OK**.

Accessing Contact Center Manager Administration from Microsoft Edge in Internet Explorer mode

You can access Contact Center Manager Administration using the Microsoft Edge browser in Internet Explorer (IE) mode. To enable IE mode in Microsoft Edge, perform the following procedures:

1. Adding the Microsoft Edge administrative templates on page 30.
2. Configuring integration with Internet Explorer on page 31.
3. Configuring the Enterprise Mode Site List on page 31.

Before enabling IE mode in Microsoft Edge, install all recent Windows updates. Ensure that Microsoft Edge is installed at the system level. You can check it by typing `edge://version` in the Microsoft Edge address field. The executable path must start with `C:\Program Files`, which indicates a system install.

For more information about IE mode in Microsoft Edge, refer to the Microsoft documentation.

> ❗ **Important:**
> - Always start CCMA in a new browser tab.
> - If you enabled SSO for your Contact Center, add the System Manager server FQDN to the Enterprise Mode Site List.
> - For solutions with geographic redundancy, add the RGN server short name and FQDN to the Enterprise Mode Site List.
> - For High Availability solutions, add the Managed Name and Managed FQDN of the HA pair to the Enterprise Mode Site List. Do not add short names and FQDNs of your active and standby servers.

Adding the Microsoft Edge administrative templates

About this task

Use this procedure to add the Microsoft Edge administrative templates to your computer.

Procedure

1. On the Microsoft website, go to the Edge for Business download page: https://www.microsoft.com/en-us/edge/business/download.

2. From the lists, select your current browser version, build, and platform.

3. Click the **Get Policy Files** button.

4. Click **Accept and download** to download the `MicrosoftEdgePolicyTemplates` file.

   The `MicrosoftEdgePolicyTemplates` archive is downloaded to the default folder on your computer.

5. Unzip the `MicrosoftEdgePolicyTemplates` archive.

6. Open the `MicrosoftEdgePolicyTemplates` folder and navigate to `windows\admx`.

7. From the `admx` folder, copy the `msedge.admx` file.

8. Navigate to `C:\Windows\PolicyDefinitions` and paste the `msedge.admx` file to the `PolicyDefinitions` folder.

9. In the `admx` folder, open the required language folder.

   For example, for the United States, open the `en-Us` folder.

10. From the language folder, copy the `msedge.adml` file.

11. Navigate to `C:\Windows\PolicyDefinitions` and paste the `msedge.adml` file to the matching language folder in the `PolicyDefinitions` folder.

12. **(Optional)** Verify that you have added the Microsoft Edge administrative template correctly by doing the following:

    a. Press `Win+R` and run `gpedit.msc` to open the Local Group Policy Editor.

      b. Click **Computer Configuration** > **Administrative Templates**.

      The `Administrative Templates` folder contains folders with the Microsoft Edge administrative templates.

Next steps

Configure web browser integration using Local Group Policy Editor.

Configuring integration with Internet Explorer

About this task

Use this procedure to enable your browser to work with Local Group Policy Editor.

Before you begin

Add the Microsoft Edge administrative templates to your computer.

Procedure

1. Press `Win+R` and run `gpedit.msc` to open the Local Group Policy Editor.

2. Click **Computer Configuration** > **Administrative Templates** > **Microsoft Edge**.

3. In the Microsoft Edge pane, double-click **Configure Internet Explorer integration**.

4. In the Configure Internet Explorer integration window, select **Enabled**.

5. From the **Configure Internet Explorer integration** list, select **Internet Explorer mode**.

   This is the default option for accessing CCMA in Microsoft Edge.

6. Click **OK**.

Result

IE mode in Microsoft Edge is now enabled.

Next steps

Configure the site list that you want to access using IE mode in Microsoft Edge.

Configuring the Enterprise Mode Site List

About this task

Use this procedure to configure the Enterprise Mode Site List.

On your computer, create an XML file with the list of sites that you want to access using Microsoft Edge in Internet Explorer mode.

The XML file must contain the following elements:

- **site-list version** number: The browser uses this number to verify whether the site list is new. Approximately 65 seconds after the browser starts, it compares your site list version to the stored version number. You must increase the site-list version number every time you update the Enterprise Mode Site List version.

- **<compat-mode>** tag: This tag specifies the compatibility settings for a specific site or domain. Use the `default` value.

- **<open-in>** tag: This tag specifies which browser version opens for a specific site or domain. Use the latest supported browser version.

Before you begin

- Add the Microsoft Edge Policy templates to your computer.

- Ensure that you have your Contact Center server short name and FQDN.

- If you enabled SSO for your Contact Center, ensure that you have your System Manager server FQDN.

- For a solution with geographic redundancy, ensure that you know your RGN server short name and FQDN.

- For a HA solution, ensure that your have your HA pair managed name and managed FQDN.

Procedure

1. On your computer, create the `sites.xml` file using the following template:

   ```
   <site-list version="1">
       <!-- File creation header -->
       <created-by>
           <tool>EnterpriseSitelistManager</tool>
           <version>10240</version>
           <date-created>20200717.142200</date-created>
       </created-by>
       <!-- Begin Site List -->
       <site url="server short name">
           <compat-mode>default</compat-mode>
           <open-in>IE11</open-in>
       </site>
       <site url="server FQDN">
           <compat-mode>default</compat-mode>
           <open-in>IE11</open-in>
       </site>
   </site-list>
   ```

2. In the first `<site>` element, for the `url` attribute, type the Contact Center server short name.

   For example, if your Contact Center server short name is `auracc12680`, use the following code: `<site url="auracc12680">`.

   For a HA solution, you must use your HA pair managed name instead of the server short name.

3. In the second `<site>` element, for the `url` attribute. type the Contact Center server FQDN.

   For example, if your Contact Center server FQDN is `auracc12680.aacc7dc2012.com`, use the following code: `<site url="auracc12680.aacc7dc2012.com">`.

   For a HA solution, you must use your HA pair managed FQDN instead of the server FQDN.

4. **(Optional)** Add your System Manager server to the site list using the following template:

```
<site url="SMGR server FQDN">
        <compat-mode>default</compat-mode>
        <open-in>IE11</open-in>
</site>
```

For example, if your System Manager server FQDN is `smgr80176.aacc7dc2012.com`, use the following code: `<site url="smgr80176.aacc7dc2012.com">`.

5. **(Optional)** Add your RGN server to the site list using the following template:

```
<site url="RGN server short name">
        <compat-mode>default</compat-mode>
        <open-in>IE11</open-in>
</site>
<site url="RGN server FQDN">
        <compat-mode>default</compat-mode>
        <open-in>IE11</open-in>
</site>
```

6. Press `Win+R` and run `gpedit.msc` to open the Local Group Policy Editor.

7. Click **Computer Configuration** > **Administrative Templates** > **Microsoft Edge**.

   Local Group Policy Editor displays the Microsoft Edge pane.

8. In the Microsoft Edge pane, double-click **Configure the Enterprise Mode Site List**.

9. In the Configure the Enterprise Mode Site List window, select **Enabled**.

10. In the Options field, type the `sites.xml` location.

    For example: `file:///c:/Users/user_name/Documents/sites.xml`.

11. Click **OK**.

12. **(Optional)** In the Microsoft Edge address bar, type `edge://compat/enterprise` and press `Enter`.

    Microsoft Edge displays the Enterprise Mode Site List page, where you can view the current list of sites that Microsoft Edge opens in IE mode. Microsoft Edge automatically checks if there is a newer site list version and updates it approximately 65 seconds after launch. However, you can also manually configure Microsoft Edge to use the latest site list version by clicking **Force Update**.

Next steps

Launch Microsoft Edge and wait for approximately 65 seconds. You can now access CCMA using Microsoft Edge in IE mode.

Internet Explorer mode and Compatibility View configuration on the domain server

If you cannot configure IE mode or Compatibility View from a local computer, you can configure these settings on the domain server. For example, if you cannot use Internet Explorer according to your enterprise security policies, you can configure Compatibility View settings on the domain server.

To enable IE mode for Microsoft Edge on the domain server, perform the following procedures:

1. Adding the Microsoft Edge administrative templates to the domain server on page 34.
2. Creating a configuration file for Internet Explorer mode on page 35.
3. Enabling IE mode on the domain server on page 38.
4. Completing IE mode configuration on a local computer on page 39.

To enable Compatibility View on the domain server, see Configuring Compatibility View settings on the domain server on page 40.

For more information about IE mode in Microsoft Edge and Compatibility View, refer to the Microsoft documentation.

> 🛑 **Important:**
>
> - If you use Windows 10, do not delete the Internet Explorer browser from your computer. Microsoft Edge for Windows 11 includes the Internet Explorer engine. Microsoft Edge uses the Internet Explorer engine to launch CCMA.
> - Always launch CCMA in a new tab of Microsoft Edge.
> - If you enabled SSO, add the System Manager server FQDN to the Enterprise Mode Site List.
> - For solutions with geographic redundancy, add the RGN server short name and FQDN to the Enterprise Mode Site List.
> - For High Availability solutions, add only the Managed Name and Managed FQDN of the HA pair to the Enterprise Mode Site List. Do not add short names and FQDNs of your active and standby servers.

Adding the Microsoft Edge administrative templates to the domain server

About this task

Use this procedure to add the Microsoft Edge administrative templates to the domain server.

Procedure

1. On the Microsoft website, go to the **Edge for Business** download page: https://www.microsoft.com/en-us/edge/business/download.
2. Click the **GET POLICY FILES** button.
3. Click **Accept and download** to download the `MicrosoftEdgePolicyTemplates` file.

The `MicrosoftEdgePolicyTemplates` archive is downloaded to the default folder on your computer.

4. Unzip the `MicrosoftEdgePolicyTemplates` archive.

5. Open the `MicrosoftEdgePolicyTemplates` folder and navigate to `windows\admx`.

6. From the `admx` folder, copy the `msedge.admx` file.

7. Upload the `msedge.admx` file to the domain server to the `C:\Windows\PolicyDefinitions` folder.

   Use a file transfer program of your choice, such as SFTP, SCP, or WinSCP.

8. On your local computer, re-open the `MicrosoftEdgePolicyTemplates` folder and navigate to the `windows\admx\` folder.

9. In the `admx` folder, open a folder corresponding to the language and locale you use on Contact Center.

   For example, for the United States, open the `en-US` folder.

10. From the language folder, copy the `msedge.adml` file.

11. Upload the `msedge.adml` file to the domain server to the `C:\Windows\PolicyDefinitions\<LANGUAGE_FOLDER>` folder.

    In this file path, `<LANGUAGE_FOLDER>` is the language folder with the same name that you selected in step 9. For example, for the United States, copy `msedge.adml` to the `C:\Windows\PolicyDefinitions\en-US` folder.

Next steps

Create a configuration file for IE mode.

Creating a configuration file for Internet Explorer mode

About this task

Create an XML file that contains a list of sites you need to access from Microsoft Edge in IE mode. You will use this file to configure the Enterprise Mode Site List on the domain server.

The XML file must contain the following elements:

- **site-list version** number: The browser uses this number to verify whether the site list is new. Approximately 65 seconds after the browser starts, it compares your site list version to the stored version number. You must increase the site-list version number every time you update the Enterprise Mode Site List version.

- **<compat-mode>** tag: This tag specifies the compatibility settings for a specific site or domain. Use the `default` value.

- **<open-in>** tag: This tag specifies the browser version that opens for a specific site or domain.

  Use the latest supported browser version.

Before you begin

- Add the Microsoft Edge Policy templates to the domain server.

- Ensure that you have your Contact Center server short name and FQDN.

- If you enabled SSO for your Contact Center, ensure that you have your System Manager server FQDN.

- For a solution with geographic redundancy, ensure that you know your RGN server short name and FQDN.

- For a HA solution, ensure that your have your HA pair managed name and managed FQDN.

Procedure

1. Create an XML file using the following template:

```
<site-list version="1">
    <!-- File creation header -->
    <created-by>
        <tool>EnterpriseSitelistManager</tool>
        <version>10240</version>
        <date-created>20200717.142200</date-created>
    </created-by>
    <!-- Begin Site List -->
    <site url="<SERVER SHORT NAME>">
        <compat-mode>default</compat-mode>
        <open-in>IE11</open-in>
    </site>
    <site url="<SERVER FQDN>">
        <compat-mode>default</compat-mode>
        <open-in>IE11</open-in>
    </site>
</site-list>
```

2. In the first `<site>` element, for the `url` attribute, type the short name of your Contact Center server.

   For example, if the short name of your Contact Center server is `auracc12680`, use the following code:
   ```
   <site url="auracc12680">
   ```

   For a HA solution, you must use your HA pair managed name instead of the server short name.

3. In the second `<site>` element, for the `url` attribute, type the Contact Center server FQDN.

   For example, if your Contact Center server FQDN is `auracc12680.aacc7dc2012.com`, use the following code:
   ```
   <site url="auracc12680.aacc7dc2012.com">
   ```

   For a HA solution, you must use your HA pair managed FQDN instead of the server FQDN.

4. **(Optional)** If you use SSO on your Contact Center, add a new `<site>` element for System Manager to the file using the following template:
   ```
   <site url="SMGR server FQDN">
           <compat-mode>default</compat-mode>
   ```

```
        <open-in>IE11</open-in>
</site>
```

For example, if your System Manager FQDN is `smgr80176.aacc7dc2012.com`, use the following code:

```
<site url="smgr80176.aacc7dc2012.com">
        <compat-mode>default</compat-mode>
        <open-in>IE11</open-in>
</site>
```

5. **(Optional)** For a solution with geographic redundancy, add a new `<site>` element for your RGN server to the site list using the following template:

```
<site url="RGN server short name">
        <compat-mode>default</compat-mode>
        <open-in>IE11</open-in>
</site>
<site url="RGN server FQDN">
        <compat-mode>default</compat-mode>
        <open-in>IE11</open-in>
</site>
```

6. Save the file using the `sites.xml` name.

Next steps

- Upload the configuration file to one of the following locations:
  - To the CCMA server. For more information about uploading the file to the CCMA server, see
  - To a shared folder on the domain server.
- Enable IE mode on the domain server.

Uploading the configuration file for IE mode to the CCMA server

About this task

You can store the configuration file `sites.xml` for IE mode on the CCMA server.

Before you begin

Create the configuration file `sites.xml` for IE mode.

Procedure

1. Copy the `sites.xml` file to the CCMA server to the `D:\Avaya\Contact Center\Manager Administration\Apps` folder.

   Use a file transfer program of your choice, such as SFTP, SCP, or WinSCP.

2. If you use SSO, do the following:

   a. Add the following entry to the `AgentPromValues.xml` file, which is located in the `D:\Avaya\Contact Center\Manager Administration\Server\Data` folder:

      `<NOT_ENFORCED value="sites.xml*" />`

   b. On the Contact Center, disable SSO.

     c. Re-enable SSO.

3. Open Microsoft Edge, enable the Internet Explorer mode, and then type the following URL in the address bar:

   `https://<CCMA_FQDN>/sites.xml`

   In this URL, `<CCMA_FQDN>` is the FQDN of the CCMA server.

4. Ensure that you can view the `sites.xml` file contents in the browser.

Next steps

Enable IE mode on the domain server.

Enabling IE mode on the domain server

About this task

Enable IE mode on the domain server to access CCMA from Microsoft Edge.

Before you begin

- Add the Microsoft Edge Policy templates to your computer.

- Create the configuration file `sites.xml` for IE mode.

- Upload the configuration file to one of the following locations:

  - To the CCMA server. For more information about uploading the file to the CCMA server, see Uploading the configuration file for IE mode to the CCMA server on page 37.

  - To a shared folder on the domain server.

Procedure

1. On the domain server, navigate to **Control Panel** > **Administrative tools** > **Group Policy Management**.

2. Go to your domain.

3. Right-click the domain group policy and click **Edit**.

4. In the Group Policy Management Editor, go to **Computer Configuration** > **Policies** > **Administrative Templates** > **Microsoft Edge**.

   The Group Policy Management Editor displays the Microsoft Edge pane.

5. In the Microsoft Edge pane, double-click **Configure Internet Explorer integration**.

6. In the Configure Internet Explorer Integration window, select **Enabled**.

7. In the Options area, from **Configure Internet Explorer integration**, select one of the following:

   - **Internet Explorer mode**: To open sites in Microsoft Edge in IE mode.

   - **None**: To prevent users from configuring IE mode using `edge://flags` or CLI.

8. Click **OK**.

9. In the Group Policy Management Editor, go to **Computer Configuration** > **Policies** > **Administrative Templates** > **Microsoft Edge**.

10. In the Microsoft Edge pane, double-click **Configure the Enterprise Mode Site List**.

11. In the Configure the Enterprise Mode Site List window, select **Enabled**.

12. In the Options area, from **Configure the Enterprise Mode Site List**, specify the location of the `sites.xml` configuration file as follows:

    • If the `sites.xml` file is on the CCMA server, use the following format:

      `https://<CCMA FQDN>/sites.xml`

      In this entry, `<CCMA_FQDN>` is the FQDN of the CCMA server. For example:

      `https://192.0.2.1/sites.xml`

    • If the `sites.xml` file is in a shared folder on the domain server, use the following format:

      `\\<NETWORK_PATH>\sites.xml`

      In this entry, `<NETWORK_PATH>` is the full path to the `sites.xml` on the domain server. For example:

      `\\198.51.100.1\Shared\sites.xml`

13. Click **OK** to save the policy settings.

Next steps

Complete IE mode configuration on a client computer.

Completing IE mode configuration on a local computer

About this task

After configuring IE mode on the domain server, update group policies on the local computer you use to access CCMA and ensure you can access CCMA using Microsoft Edge.

Before you begin

• Configure IE mode on the domain server.

• Ensure that the operating system and Microsoft Edge browser installed on your local computer comply with the system requirements for IE mode listed at https://docs.microsoft.com/en-us/deployedge/edge-ie-mode.

Procedure

1. On your local computer, run the following command:

   `gpupdate /force`

2. To check if Group Policy Objects are applied, run the following command:

   `gpresult /r`

In the command output, the Applied Group Policy Objects section must contain the domain group policy name that you configured on the domain server.

3. In the Microsoft Edge address bar, type `edge://compat/enterprise` and ensure that the Enterprise Mode Site List tab contains the `sites.xml` file you added to the domain server.

4. In Microsoft Edge, open the CCMA site.

Next steps

Configure the Compatibility View List on the domain server.

Configuring Compatibility View settings on the domain server

About this task

Compatibility View is a feature that enables you to open websites that are incompatible with the latest browser version. If Microsoft Edge cannot display the CCMA site even in IE mode, you can configure Compatibility View settings for the CCMA site. If you cannot configure the Compatibility View settings on your local computer, you can configure them on the domain server.

If you are using Windows 11, you do not need to enable Compatibility View.

❗ Important:

In this procedure, you will add a registry key to Group Policy Objects. If you change your Compatibility View settings, you must delete this registry key and then add it again.

Procedure

1. On the domain server, start Microsoft Edge with Internet Explorer mode.

2. Click the **Tools** icon and then click **Compatibility View Settings**.

   The browser displays the Compatibility View Settings window.

3. In **Add this website**, type your domain name and then click **Add**.

4. On the domain server, go to **Control Panel** > **Administrative tools** > **Group Policy Management**.

5. Select your domain.

6. Right-click the domain group policy and click **Edit**.

   You can also create a new domain group policy and link it to the domain.

7. In the Group Policy Management Editor, go to **User Configuration** > **Preferences** > **Windows Settings** > **Registry**.

8. Right-click **Registry** and click **New** > **Registry Wizard**.

9. In the Registry Wizard, select the local machine and then navigate to **HKEY_CURRENT_USER** > **Software** > **Microsoft** > **Internet Explorer** > **BrowserEmulation** > **ClearableListData**.

10. Select the check box for the UserFilter parameter.

11. Click **Finish**.

12. On your local computer, to update the group policy settings, run the following command:

    ```
    gpupdate /force
    ```

13. To check if Group Policy Objects are applied, run the following command:

    ```
    gpresult /r
    ```

    In the command output, the Applied Group Policy Objects section must contain the domain group policy name that you configured on the domain server.

14. **(Optional)** Verify that the registry key `HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\BrowserEmulation\ClearableListData\UserFilter` contains the same value that is configured on the domain server.

15. Restart Microsoft Edge in Internet Explorer mode to apply the changes in the Compatibility View settings.

Chapter 4: System configuration and management

This chapter provides procedures to manage and configure your system.

Adding a server

Before you begin

- Obtain a user ID and password with administrative privileges for the Contact Center Manager Administration client application. Only an administrator can add a server.

- Know the computer name of the server to add.

- Change the default server password in the Contact Center Manager Server Utility.

- To add Contact Center Manager Server, know the logon ID. This logon ID corresponds to a user account created using the Contact Center Manager Server Utility.

- To add Communication Control Toolkit, add Contact Center Manager Server with Open Queue enabled. Know the Communication Control Toolkit Tomcat website port number.

- To add a Proactive Outreach Manager (POM) server, you must have a user name and password for that server.

- To add an Avaya Aura® Communication Manager, you must obtain the name, IP address and server id for the Avaya Aura® Communication Manager server.

- Log on to Contact Center Manager Administration. For more information, see [Logging in to Contact Center Manager Administration for the first time](#) on page 24.

About this task

Add a server to Contact Center Manager Administration to administer the server from the Contact Center Manager Administration client application. You can add multiple Contact Center Manager Server, Communication Control Toolkit (CCT), Contact Center Multimedia (CCMM), and Avaya Aura® Communication Manager (CM) servers.

> ❗ **Important:**
>
> Do not add servers from an Avaya Contact Center Select (ACCS) solution. In Avaya Aura® Contact Center (AACC), CCMA can manage only servers that are in AACC solutions.

Procedure

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

2. From the **Server** menu, choose **Add Server**.

3. From the **Type** list, select one of the following server types:

   • To add a Contact Center Manager Server, select **CCMS**.

   • To add a Contact Center Multimedia server, select **CCMM**.

   • To add a POM server, select **CCPO**.

   • To add Communication Control Toolkit, select **CCT**.

   • To add a Communication Manager server, select **CM**.

   • For all other server types, select **Other Avaya**.

4. In the right pane, in the **Server Name** box, type the computer name of the server.

5. Press **Tab**. The server IP address automatically appears in the IP Address box and the system automatically assigns a display name that is the same as the server name.

6. To use a different display name, in the **Display Name** box type the name of the Contact Center server as you want it to appear in the system tree in Contact Center Manager Administration.

7. To add Contact Center Manager Server, in the **Login ID** box, type your logon ID for the server.

8. To add a Contact Center Multimedia server, in the **Login ID** box, type `mmReport.`

9. To add a Communication Manager server, in the **Communication Manager server ID** box, type the unique server ID for your Communication Manager.

10. In the **Password** box, type your password.

11. If you select **CCMS**, **CCMM**, or **CM**, proceed to .

12. If you select **Other Avaya**, in the **DSN Prefix** box, type the DSN prefix for the server.

13. If you select CCT, in the **CCT Website: Port Number** box, type the port number of the Communication Control Toolkit server website.

14. If you select CCT, from the **Associated CCMS Servers** list, select the Contact Center Manager Server with which to associate this Communication Control Toolkit server.

15. Click **Submit**.

16. In the left pane, expand the server name to access it.

    > ❗ **Important:**
    >
    > The Contact Center Manager Server logon ID and password that you specify when you configure a new server in Contact Center Manager Administration must match an existing login ID and password on the Contact Center Manager Server. Therefore, if you or another administrator uses the Server Utility to change a server logon ID

or password that you already entered in Contact Center Manager Administration, you must update the information in the Configuration component of Contact Center Manager Administration to match the new logon information.

Variable definitions

Name	Description
Login ID	For Contact Center Multimedia, the Login ID corresponds to the user account that runs historical reports in Contact Center Manager Administration. This user is configured in the Multimedia database and has access to data within that database. The Login ID is always mmReport.
Password	For Contact Center Multimedia, the default password is mmRep. To change this password, use the Contact Center Multimedia Administrator.
Communication Manager server ID	The unique server ID for the Communication Manager.
DSN prefix	For server types CCMS and CCMM, the default DSN prefix is CCMS and CCMM respectively. For these server types, the DSN prefix is read-only.
Associated CCMS Servers	For server types that you can associate with a Contact Center Manager Server, lists the available Contact Center Manager Servers. Select a Contact Center Manager Server with which to associate this server.
CCT Website: Port Number	For the CCT server type, the default port number is 8081. Change this value if you change the port number on the Communication Control Toolkit server Tomcat configuration files.
CCT Website: HTTPS URL	For the CCT server type, if security is enabled, this box displays the secure URL for the Communication Control Toolkit server administration Web page. This is for information only.
CCT Website: HTTP URL	For the CCT server type, if you turned off Web Services security, this box displays the URL for the Communication Control Toolkit server administration Web page. This is for information only.

Associating servers to a Contact Center Manager Server

Before you begin

- Add the server to Contact Center Manager Administration. See

About this task

Associate Contact Center Multimedia servers with a Contact Center Manager Server to enable reporting for that server. Associate Avaya Aura® Communication Manager with a Contact Center Manager Server to support Avaya Aura® agents.

Procedure

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

2. In the left pane, right-click the Contact Center Manager Server to associate with a reporting server.

3. Choose **Server** > **Edit Properties**.

   The properties for the Contact Center Manager Server appear in the right pane.

4. To associate reporting server, in the **Associated Reporting Server** list, select the reporting servers with which to associate this CCMS server.

   > 🛈 **Important:**
   >
   > Associate only one of each server type with a Contact Center Manager Server. If you attempt to associate more than one of the same server type with a Contact Center Manager Server, an error message indicates that you can select only one associated reporting server of that type.

5. To associate one or more Communication Managers, in the **Associated Communication Manager servers** list, select the servers with which to associate this CCMS server.

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

Deleting a server

Before you begin

- Log on to Contact Center Manager Administration with administrative privileges.

About this task

Use this procedure to delete a server from Contact Center Manager Administration. You must have administrative privileges to delete a server.

> ⚠️ **Warning:**
>
> Deleting a CCMS server impacts many items in the CCMA database. If you delete a CCMS server, the following data is lost:
>
> - User-defined partition content (Agents, Applications, Skillsets, Report groups, CDNs, DNISs, ScriptVars, Prompt, and other)
> - Server permission (No Data/Full Data/Configure)
> - Standard partitions
> - Reporting agent
> - RTD Report groups
> - HR Report groups
> - Filter content (Agent, Skillset, Application)
> - Supervisor associated with CCMA users
> - Private realtime tabular displays and private graphical displays
> - Private HR reports of the server
> - Content of access class
>
> If you re-add the deleted CCMS server, you must re-configure all the above-mentioned settings.

Procedure

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

2. In the left pane, select the server to delete.

3. From the **Server** menu, choose **Delete Server**.

   You can also right-click the server to delete, and select **Delete Server** from the shortcut menu.

4. Click **OK** to delete the server from the system tree.

Refreshing your servers

Before you begin

- Log on to Contact Center Manager Administration with administrative privileges.

About this task

Refresh your servers after you:

- upgrade the Contact Center Manager Server
- enable a Contact Center Manager Server feature (for example Networking or Open Queue)
- accept a new license file on the Contact Center Manager Server

- change the sysadmin password on the Contact Center Manager Server
- apply a service pack (SP) to the Contact Center Manager Administration server or to the Contact Center Manager Server

Procedure

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

2. In the left pane, select the server to refresh.

3. From the **Server** menu, choose **Refresh Server,** or right-click on the server, and choose **Refresh Server**.

   OR

   To refresh all servers, click **Refresh All Servers**.

4. In the confirmation window, click **Yes**.

   A message box appears stating that you must refresh all browsers attached to Contact Center Manager Administration. If a Contact Center Manager Server feature changes, that change is reflected in the browsers only when you refresh them.

5. Click **Yes** to refresh the server.

   After the Refresh or Refresh All is complete, Contact Center Manager Administration displays a message informing you that the operation was successful.

Editing a server

Before you begin

- Log on to Contact Center Manager Administration with administrative privileges.

About this task

Edit server properties, such as display name, server name, or IP address.

Procedure

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

2. In the left pane, select the server to edit.

3. From the **Server** menu, choose **Edit Properties**.

   You can also right-click the server and select **Edit Properties**.

4. Make the required changes. You can edit the following information:

   - Display Name for the server
   - Login ID for the server in Contact Center Manager Server
   - Password for the server in Contact Center Manager Server

- Server Name

- IP Address

- Associated Servers

- Avaya Aura® Communication Manager server ID for the Avaya Aura® Communication Manager

- CCT Port Number

5. Click **Submit**.

Part 1: Contact Center Configuration

Chapter 5: Contact Center Configuration fundamentals

Use the Contact Center Manager Administration Configuration component to configure and administer Contact Center Manager Server. Before you can configure the server, you must add a server to the system tree.

Perform the following tasks using the Configuration component:

- Add, configure, and delete Contact Center Manager Server instances.
- Add, configure, and delete resources using one of the following methods:
  - individually using the Web-based user interface
  - using the Configuration Tool spreadsheets to upload and download bulk data

You must log on to Contact Center Manager Administration as an administrator to add and configure servers, and to upload and download data using the Configuration Tool spreadsheets.

Use the Configuration component to configure the following resource types:

- activity codes
- agent greetings
- blending configuration (for solutions using POM)
- call presentation classes
- Call Recording and Quality Monitoring server details
- controlled directory numbers (CDN)
- contact types
- dialed number identification services (DNIS)
- formulas
- global settings
- historical statistics
- IVR ACD-DNs
- Media Servers
- Media Services and routes

- multiplicity presentation classes

- networking communication parameters

- phone displays

- phones and voice ports

- real-time statistics

- routes

- skillsets

- threshold classes

Chapter 6: Contact Center Configuration

The server Contact Center Manager Administration (CCMA) is installed on hosts the server application for configuring Avaya Aura® Contact Center. Use the Contact Center Manager Administration application to configure servers, agents, supervisors, skillsets, route points, and many other tools for routing contacts to agents.

Use the Configuration component to configure and administer Contact Center Manager Server.

For information about configuring a Network Control Center server, see *Avaya Aura® Contact Center Server Administration*.

Prerequisites to configuration

Ensure that you have administrative privileges in the Contact Center Manager Administration application.

Logging in to Contact Center Manager Administration for Contact Center configuration

About this task

The server where Contact Center Manager Administration is installed hosts the server application for configuring Avaya Aura® Contact Center. Use the CCMA client to access the server and to configure servers, agents, supervisors, skillsets, route points, and other tools for routing contacts to agents.

If you have a High Availability campus solution, log in to the CCMA web client using the managed name or managed IP address of the High Availability server pair. If an active application or server fails, the CCMA client web browser continues to use the managed name or IP address and you can continue working without interruption.

Use this procedure to log in to CCMA to view, add, change, and delete items from the CCMA database.

Before you begin

- Ensure that you have administrator privileges.

- Before logging in to the CCMA client application for the first time, configure your browser settings. You must use Microsoft Edge with Internet Explorer mode enabled.
- Ensure that you know the CCMA user ID and password.

Procedure

1. In your browser, type the URL of the 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.

   If your site does not use the default port for Internet Information Services (IIS), the URL of the server is `https://<server name>: <port number>`, where *<server name>* is the computer name of the Contact Center server, and *<port number>* is the port for the CCMA site in IIS. For example, `https://ccserver:81`.

   🛈 **Important:**

   You must log on using the Contact Center server name. Do not use the server IP address.

2. In the **User ID** box, type your user ID.

3. In the **Password** box, type your password.

4. Click **Login**.

   If configured in CCMA Security Settings, CCMA displays the date and time of your last login and also the number of failed login attempts since your last successful login.

Chapter 7: Activity codes

An activity code is a number that an agent can enter on a phone or on Agent Desktop to track time spent on activities and service areas, not ready reasons, and after call work.

A supervisor or system administrator configures activity codes. Administrators define activity codes in Contact Center Manager Administration. Activity codes can be alphanumeric. Administrators configure each newly entered code with a discrete type so that Agent Desktop displays the each code under one of three separate controls:

- Activity codes
- Not Ready Reason codes
- After Call Work Item (ACW) codes

Administrators configure activity codes that correspond to a contact type and a skillset. Therefore, activity codes are filtered on a contact type and skillset basis. Agent Desktop displays the activity codes list based on either the contact skillset or the contact type. For example, if you are handling email contacts, Agent Desktop populates the Activity Code list both with activity codes that correspond to the email contact type and with activity codes that map to the skillset.

> **❗ Important:**
>
> If you are migrating or upgrading your contact center, the existing activity codes are not migrated automatically. However, you can use Contact Center Manager Administration to upgrade the codes. If you do not upgrade the codes to have a specific type, it can impact reporting and how after call work or post-call processing time is calculated.

Activity codes

An agent can enter Activity codes (that are not defined as either ACW or Not Ready Reason codes) when they are on a Contact Center call.

If an agent does not enter an activity code, Contact Center assigns a default activity code to the contact.

- System default activity code—If an agent does not enter an activity code while working on a contact, and if the contact is not queued to a skillset, the system assigns the System default activity code to the contact.
- Skillset default activity code—If an agent presses the activity code key twice during a contact without entering an activity code, the system assigns the Skillset default activity code to the contact. Skillset default activity codes apply to AML-based contact centers only.

Not Ready Reason codes

An agent can enter Not Ready Reason codes when they are on a Contact Center call or when they are idle. If an agent enters a Not Ready Reason code while on a call, then the agent transitions to the Not Ready state immediately following the call. If an agent enters a Not Ready Reason code when idle, the agent transitions to the Not Ready state. When the agent is in a Not Ready state,

the agent can enter a different Not Ready Reason code, if the agent wants to change the reason for being in the Not Ready state. Some examples of Not Ready Reason codes are Lunch or Tea Break.

After Call Work Item codes

An agent can use Agent Desktop to enter an After Call Work Item (ACW) code either while working on a contact, or immediately after the releasing the contact.

Agents must enter ACW codes to perform post call processing work, such as adding contact information to a CRM system. Agents can enter ACW codes only for post call processing work related to the contact that they just released.

Agents can enter ACW codes:

- while working on a contact, which prevents Agent Desktop from presenting new contacts to the agent
- after releasing the contact, and before Agent Desktop presents a new contact to the agent or the agent goes into the Not Ready state.

A new control that agents can use to track ACW time, **Set ACW Code**, is available on the Agent Desktop Top bar menu. Alternatively, administrators can select the **Enter ACW using Not Ready Without Reason Code** option under **Global Settings**, so that agents can continue to work as they did before the introduction of ACW codes. Agents can then mimic the Post Call Processing (PCP) time model of earlier releases by pressing Not Ready without specifying a code. In this case Contact Center puts the agent into ACW with the default code ACW code 00000.

> 🛈 **Important:**
>
> If you are upgrading from a release prior to Avaya Aura® Contact Center Release 6.3 SP10, where agents used Not Ready reason codes to track after call work, you must update the existing Not Ready codes to have a type of ACW. Retrain your agents to use the new control **Set ACW Code** on Agent Desktop to set ACW codes. If you continue to use Not Ready reason codes for after call work, Contact Center does not report after call work correctly.

The After Call Work Item codes are not available when:

- the agent first logs on to Agent Desktop
- when the agent has gone into the Not Ready state after a call and then returned to an Idle state

Activity codes in Real-time Reports

Not Ready Reason codes relate to the overall status of an agent. After Call Work Item codes relate to the activity of an agent on a specific contact. When an agent uses multiplicity, Real-time Reports show both the Not Ready Reason code and the After Call Work Item code on the first contact listed for the agent.

Configuring activity codes

Before you begin

- Log on to Contact Center Manager Administration.
- Open the Configuration component.

About this task

Configure activity codes that agents can enter on a phone or on Agent Desktop to track time agents spend on activities and service areas, Not Ready reasons and After Call Work Item (ACW) items.

You can configure activity codes that correspond to a type and to a skillset. Therefore, activity codes are filtered on contact type or skillset basis, or both. Agent Desktop displays the activity codes list based on either the skillset of the call or the contact type of the call.

You cannot overwrite the following default activity codes:

- activity code 00000 (Default_ACW)
- activity code 0000 (NotRdy_Pull_Mode_Default_Code)
- activity code 000 (Not_Ready_Default_Reason_Code)
- activity code 00 (Skillset_Default_Activity_Code)
- activity code 0 (System_Default_Activity_Code)

You can add Not Ready Reason codes and After Call Work Item codes in the same way that you add activity codes. Use unique numbers for Not Ready Reason codes, Activity codes, and After Call Work Item codes. Agent Desktop displays a maximum of 16 digits for Not Ready Reason codes, Activity codes, and After Call Work Item codes.

✱ Note:

If you associate an activity code with both contact types and skillsets, the activity codes appears on Agent Desktop for all of the skillsets of the selected contact type and for all of the skillsets individually selected.

Procedure

1. In the system tree, expand the server on which you need to add the activity code.

   The server displays the server resources.

2. Select the **Activity Codes** folder.

3. In the right pane of the Activity Codes section, click **New**.

4. In the **Name** field, type the name of the new activity code.

5. In the **Number** field, type the number of the new activity code.

6. In the **Display Name** field, type the name of the new activity code that the system displays in reports.

7. From the **Type** drop-down list, select the type of the new activity code. You can choose from the following:

   - **Not Ready Reason**
   - **Activity Code**
   - **After Call Work Item**

> *** Note:**
>
> You cannot change the code type once the code is created.

8. If you are creating an activity code of type **Activity Code** that applies to all of the skillsets of a particular contact type, select the contact type that corresponds to the activity code by clicking the right arrow (**>**) under the Available Contact Types list. If the activity code applies only to a limited number of skillsets, skip to step 10.

   The contact type moves to the Selected Contact Types list.

   > *** Note:**
   >
   > Assigning both contact types and skillsets to activity codes is not required. You must map skillsets to an activity code only if the activity code is applicable to specific set of skillsets.

9. **(Optional)** To associate all the contact types with an activity, click the double right arrow (**>>**) under the Available Contact Types list.

   All the contact types move to the Selected Contact Types list.

10. **(Optional)** If you are creating an activity code of type **Activity Code**, select the skillsets that correspond to the activity code by clicking the right arrow (**>**) under the Available Skillsets list.

    This skillset moves to the Selected Skillsets list.

11. **(Optional)** To associate all the skillsets with an activity, click the double right arrow (**>>**) under the Available Skillsets list.

    All the skillsets move to the Selected Skillsets list.

12. Click **Save**.

Variable definitions

Name	Description
Name	The name assigned to the activity code. Valid values: Maximum 30 characters (no special characters).

Table continues…

Name	Description
Number	The number assigned to the activity code. Agents enter this number on their phones to assign the activity code to a contact. Valid values: Maximum 32 digits. **Important:** You cannot change the activity code number once you save the activity code. To change the activity code number, delete the activity code, and create a new activity code.
Display Name	The description that corresponds to the activity code. This description appears in custom private real-time displays when agents enters an activity on their phone. Valid values: Maximum 30 characters.
Type	The type of activity code. You can choose from the following: • **Not Ready Reason** • **Activity Code** • **After Call Work Item** • **All** — This type appears after migrations. It is not possible to create a new code of type 'All'. For migrated data, the type of 'All' is displayed and must be changed.

Editing an activity code

Before you begin

- Log on to Contact Center Manager Administration.
- Open the Configuration component.
- Configure at least one activity code. See [Configuring activity codes](#) on page 55.

About this task

Edit an activity code to change the name or display name. If the activity code is of the type **Activity Code**, you can also change the contact type and skillset that corresponds to the activity code.

You cannot change the activity code number or type. To change an activity code number or type, you must delete the activity code and create a new activity code with the new number or type.

> ⊛ **Note:**
>
> You cannot edit the default activity codes.

Procedure

1. In the left pane, expand the server that contains the activity code to change.

   The server displays the server resources.

2. Select the **Activity Codes** folder.

3. In the right pane, highlight the activity code to change.

4. In the **Name** field, type the new name of the activity code.

5. In the **Display Name** field, type the new name that of the activity code the system displays in reports.

6. If you are editing an activity code of type **Activity Code**, you can change the contacts types that correspond to the activity code by clicking the right arrow (**>**) or left arrow (**<**) under the Available Contact Types list.

   If you click the right arrow (**>**) the contact type moves to the Selected Contact Types list.

   If you click the left arrow (**<**) the contact type moves to the Available Contact Types list.

7. If you are editing an activity code of type **Activity Code**, you can change the skillsets that correspond to the activity code by clicking the right arrow (**>**) or left arrow (**<**) under the Available Skillsets list.

   If you click the right arrow (**>**) the contact type moves to the Selected Skillsets list.

   If you click the left arrow (**<**) the contact type moves to the Available Skillsets list.

8. Click **Save**.

Deleting an activity code

Before you begin

- Log on to Contact Center Manager Administration.

- Open the Configuration component.

- Configure at least one activity code. See

About this task

Delete an activity code that you no longer require.

> ⊛ **Note:**
>
> You cannot delete any of the default activity codes.

Procedure

1. In the system tree, expand the server that contains the activity code to delete.

   The server displays the server resources.

2. Select the **Activity Codes** folder.

3. In the right pane, highlight the activity code to delete.

4. Click **Delete**.

5. Click **OK** to confirm the deletion.

Searching for an activity code

Before you begin

- Log on to Contact Center Manager Administration.
- Open the Configuration component.

About this task

You can search for activity codes based on the name or type of the activity code.

Procedure

1. In the system tree, expand the server that contains the activity codes.

   The server displays the server resources.

2. Select the **Activity Codes** folder.

3. In the right pane of the Activity Codes section, under the Search area, in the **Name** field, type the name of the activity code to search.

   Or

   From the **Type** drop-down list, select the type of activity code to search. You can choose from the following:

   - **Not Ready Reason**
   - **Activity Code**
   - **After Call Work Item**
   - **All**

   To list all your activity codes, click **List All**.

4. Click **Search**.

   The system displays the activity codes that match your criteria.

Chapter 8: Agent Greeting and Announcement Recorder

Agent Greeting

The Agent Greeting feature allows agents to pre-record greetings. Contact Center automatically plays an agent's greeting when the agent answers a call.

Agent Greeting provides the following benefits:

- Each agent's greeting is consistent for all callers.
- The agent has time to prepare for the call.
- The agent can customize their greeting according to the time of the day. For example, agents can customize the greetings to play at specific times during the morning, afternoon, or evening.

Agent Greeting is a licensed feature, and you must commission the Agent Greeting feature before you can enable it in Contact Center Manager Administration.

Announcement Recorder

Solutions that use Agent Greeting can enable supervisors and supervisor agents to record or modify prompts using the Announcement Recorder application. Announcement Recorder is a Telephony User Interface (TUI) that supervisors access from their telephone.

This gives supervisors flexibility to modify announcements to improve the callers' experience. For example, a supervisor can change the initial welcome greeting that a caller hears to inform callers that a featured special offer has sold out: the caller can hang up straight away instead of holding for an agent.

Configuring Agent Greeting

Before you begin

- Log on to Contact Center Manager Administration. For more information, see Logging in to Contact Center Manager Administration for Contact Center configuration on page 52.
- Open the Configuration component.

About this task

Configure Agent Greeting for the greeting to play automatically when an agent answers a call.

Procedure

1. In the system tree, expand the server on which to configure Agent Greeting.

2. In the left pane, click **Agent Greeting**.

3. Under **General Settings**, select the options which you require.

4. Under **Time of Day Settings**, select the options which you require.

5. Click **Submit**.

Variable definitions

Name	Description
Agent Greeting enabled	Select to enable Agent Greeting at a system level.
Mute agent on greeting playback	Select to automatically mute the agent while the greeting plays.
"No greeting" warning tone	Select to ensure a warning tone is played, audible to the agent and the caller, if an agent answers a call for which no greeting is available.
Allow an agent to interrupt the greeting	Select to allow an agent to terminate the greeting to speak directly to the caller.
Maximum allowed greeting length	The maximum length of the greeting. Valid values: 12-30 seconds
Agent greeting record number	This is the number of the route on the PABX that routes to Agent Greeting on the Contact Center server.
Prompt language	Lists the languages from which you can choose a language for the prompt. Agents hear the selected language when they dial into the recording application.
Enable time of day greetings	Select to enable or disable the playback of time of day greetings.
Morning start time	Select to specify the time for morning greeting to play.
Afternoon start time	Select to specify the time for afternoon greeting to play.
Evening start time	Select to specify the time for evening greeting to play.
Playback position	Select to specify if the time of the day greeting is played before or after the main greeting.

Deleting agent greetings

About this task

If you are using Agent Greeting agents and supervisor/agents have recorded individual greetings, you must manually delete these greetings if you delete the agent or supervisor/agent in Contact Center Manager Administration (CCMA).

Procedure

1. Log on to Avaya Aura® Media Server Element Manager.

2. Open **Tools** > **Media Management**.

3. Select the Agent Greeting Content Namespace, and click **Browse**.

   The Agent Greeting Content Namespace is CCAG_*<IP address>*, where *<IP address>* is the IP address of the Avaya Aura® Media Server.

4. On the Provision Media screen, select the ID of the agent you deleted in CCMA.

5. Click **Delete**.

6. On the Confirm Media Delete dialog, click **Confirm**.

Logging on to the Announcement Recorder application

About this task

Log on to the Announcement Recorder application to modify or record announcements.

Before you begin

- You must be enabled for Agent Greeting to use the Announcement Recorder application.

Procedure

1. On your telephone, dial the number of the Announcement Recorder application (If you do not know this number, ask the Contact Center system administrator).

   The Announcement Recorder application plays a welcome prompt and prompts you for your agent ID.

2. Using your telephone keys, enter your agent ID followed by pound (#).

   The Announcement Recorder application prompts you for your password.

3. Using your telephone keys, enter your agent password followed by (#).

   The application plays the main menu.

Next steps

Use the Announcement Recorder menus to change or record announcements.

Changing an announcement using Announcement Recorder

About this task

Change an announcement to modify what callers to the contact center hear as they progress through the application flow.

Before you begin

- Log on to the Announcement Recorder application.

Procedure

1. From the **Announcement Recorder** main menu, select 1 to go to the Update Announcement option.

2. If you know the number of the announcement that you want to change, when the application prompts you, enter the announcement number.

3. If you do not know the number of the announcement that you want to change:

   a. Wait for the application to begin playing announcement titles.

   b. Enter 6 if you want to skip to the next announcement.

   c. Enter 4 if you want to return to the previous announcement.

   d. Enter 1 to change the current announcement.

4. When the application prompts you to record the announcement, speak the new announcement.

   Contact Center plays the new announcement back to you.

5. In the **Updating Announcement** menu, to listen to the announcement again, select 1.

6. To replace the new announcement, select 2, and record the new announcement.

7. To update the new announcement title, select 3, and record the new announcement title.

8. Select (#) to return to the main menu.

Next steps

Avaya recommends that you place a call to the CDN and check that the prompt you changed sounds correct to a caller and is in the correct context for the flow application.

Recording a new announcement using Announcement Recorder

About this task

Record a new announcement that you can use in a flow application.

Before you begin

- Log on to the Announcement Recorder application.

Procedure

1. From the **Announcement Recorder** main menu, select 2 to go to the Record New Announcement option.

2. When the application prompts you to record the announcement title, speak the title for the new announcement.

   Contact Center plays the title of the new announcement back to you.

3. When the application prompts you to record the announcement, speak the new announcement.

   Contact Center plays the new announcement back to you.

4. If you want to listen to the announcement again, select 1.

5. If you want to replace the new announcement, select 2.

6. If you want to replace the new announcement title, select 3.

7. Select (#) to return to the main menu.

Next steps

To use the new prompt you must modify or create a flow application in Orchestration Designer.

Chapter 9: Call presentation classes

A call presentation class comprises a collection of preferences that determines how contacts are presented to an agent. A call presentation class specifies whether a break time between contacts is permitted, whether an agent can place DN calls on hold for incoming ACD calls, and whether an agent phone displays that the agent is reserved for a network call.

Call Force Answer Zip Tone and Whisper Skillset

In a SIP-enabled solution, Contact Center supports an optional configuration to give Call Force Answer (CFA) Zip Tone to agents. This is configurable for all agents assigned to a call presentation class where the Call Force Delay or Return to Queue option is selected. A zip tone is a tone or beep that a contact center agent hears before they are connected to a customer call. You can also configure a silence period to fall after the zip tone, and before the agent and customer are connected on a call.

Call Force Answer Zip Tone works in conjunction with Agent Greeting. Agent Greeting is delayed until the end of the Call Force Answer Delay period.

This feature presents the customer call to the agent while the agent is still hearing the zip tone and the silence that follows. The agent is connected for the duration of this time. This causes the CCMA reports for the Call Delay Time and Active fields to be inaccurate by the length of time of the zip tone and the Call Force Answer Delay Timer setting.

Contact Center supplies a default zip tone. You can replace this default zip tone with a different one. If you want to play zip tones for individual skillsets or call presentation classes, configure Whisper Skillset as the custom zip tone. Additional zip tones, if provisioned, are played on a customer call in the following order of priority:

- skillset
- call presentation class
- default tone

> **Note:**
>
> Only one of the zip tones above is played.

Contact Center also supports an optional configuration to provide Whisper Skillset to agents. The Whisper Skillset feature allows a brief skillset-specific announcement to be played to agents before they are connected to a customer call. This is configurable for all agents assigned to a call presentation class.

Whisper Skillset configuration and functionality is similar to Call Force Answer Zip Tone. The Whisper Skillset feature uses the same source location for skillset-specific announcements as CFA Zip Tone.

Creating a call presentation class

Before you begin

- Log on to Contact Center Manager Administration. For more information, see Logging in to Contact Center Manager Administration for Contact Center configuration on page 52.

- Open the Configuration component.

  ❗ **Important:**

  In a SIP-enabled Contact Center, Call Force Delay is not supported for Instant Message contacts, and Let Call Ring is not supported for voice or Instant Message contacts.

About this task

Create a call presentation class to determine how contacts are presented to an agent's phone. You can choose the following presentation methods:

- Automatically answer the contact at the agent's phone.

- Return the contact to the queue if the contact is not answered within a specified period.

- Allow the contact to ring at the agent's phone until it is answered or abandoned.

In addition, you can choose whether to present contacts to agents when they are busy on a DN call, and whether to allow the agent time to finish a contact after it ends.

Procedure

1. In the system tree, expand the server on which to add the call presentation class.

   The server shows its resources.

2. Select the **Call Presentation Classes** folder.

3. In the right pane, in the **Name** box, type the name of the call presentation class as it appears in reports.

4. From the **Presentation Option** list, select one of the following call presentation options:

   - Return to Queue

   - Call Force Delay

   - Let Call Ring

5. If you select the **Call Force Delay** presentation option, in the **Call Force Delay Timer** box, type the number of seconds after which the contact is automatically answered at the agent's phone and proceed to step 8 on page 68.

> **✳ Note:**
>
> In a SIP-enabled contact center, you can configure the Call Force Answer Zip Tone feature. If this is configured in a contact center where the agent's phone ringer is disabled, in order to reduce customer wait time, Avaya recommends setting the Call Force Delay Timer to zero seconds. Call Force Answer Zip Tone is supported only when the **Call Force Delay** or **Return to Queue** presentation option is selected on the call presentation class.

6. In the **Return to Queue After N Seconds** box, type the time after which the contact returns to the queue if not answered.

7. From the **After Return to Queue, Make Phoneset** list, select the mode in which the phone is placed after the contact returns to the queue.

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

9. From the **Prompt On Answer** list, select one of the following:

   • None

   • Zip Tone

   • Whisper Skillset

   > **✳ Note:**
   >
   > If you want to play zip tones for individual skillsets or call presentation classes, select Whisper Skillset and upload the custom zip tone as a Whisper Skillset announcement file.

10. In the **Prompt On Answer Silence Timer** box, type the amount of time to pass after the zip tone is played and before the agent and customer are connected on a call. This option is available only when you select **Zip Tone**.

11. Select the **Answer by Placing DN call on Hold** check box so that agents can place DN calls on hold to answer Contact Center Manager Server calls. This check box does not appear on a SIP-enabled server.

12. Select the **Agent Reserved for Network Call** check box to display the message "Reserved" on the agent's phone when the server reserves the agent for a network call.

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

Variable definitions

Name	Description
Name	The name assigned to the call presentation class. Valid values: 30-character maximum (no special characters, no spaces)
Presentation Option	Select one of the following call presentation options for the call presentation class: • Call Force Delay—Choose this option to force a call on an agent if the agent does not answer the call within the specified amount of time. If you select this option, you must specify the time delay in seconds in the Call Force Delay Timer box. Call Force Delay is not supported for Instant Message contacts in a SIP-enabled Contact Center. • Return to Queue—Choose this option to return a call to the queue if the agent does not answer the call within the specified amount of time. ✱ **Note:** In SIP-enabled Contact Centers, Voice and IM contacts return to the queue after 30 seconds. • Let Call Ring—Choose this option to let the call ring at the phone until the agent answers the call. Let Call Ring is not supported for voice or Instant Message contacts in a SIP-enabled Contact Center.
Call Force Delay Timer	If you select Call Force Delay from the Presentation Option list, in the Call Force Delay Timer box, type the time delay in seconds. ✱ **Note:** In a SIP-enabled contact center, you can configure the Call Force Answer Zip Tone feature. If this is configured in a contact center where the Agent's phone ringer is disabled, in order to reduce customer wait time, Avaya recommends setting the Call Force Delay Timer to zero seconds.

Table continues…

Name	Description
Return to Queue After N Seconds	If you select Return To Queue from the Presentation Option list, in the Return To Queue After N Seconds box, type the wait interval in seconds.
	If you do not select Return to Queue as the presentation option, the value is N/A.
	Valid values: 1 — 1200 (seconds)
Prompt On Answer	• None—Do not play a Zip Tone or Whisper Skillset announcement.
	• Zip Tone—Play the default Zip Tone.
	• Whisper Skillset—Play a Whisper Skillset announcement or custom zip tone. If there is an announcement file matching the skillset name for the call then play this otherwise play the default announcement.
	✳ **Note:**
	If you want to play zip tones for specific skillsets or call presentation classes, select Whisper Skillset and upload the custom zip tone as a Whisper Skillset announcement file.
Prompt On Answer Silence Timer	The amount of time to pass after the zip tone is played and before the agent and customer are connected on a call.
	Valid values: 0 — 5 (seconds)
After Return to Queue, Make Phoneset	If you select Return To Queue from the Presentation Option list, from the After Return To Queue, Make Phoneset list, select one of the following values:
	• Logout
	• Not Ready
	• N/A

Table continues…

Name	Description
After Call, Break for N Seconds	The amount of time, in seconds, that an agent is in break state at the end of a call and before the next call. The agent can use this time to complete processing related to the finished call. This applies to Contact Center calls only (not to DN calls). It is supported on both SIP-enabled and AML-based Contact Centers. **ⓘ Important:** After an agent completes a blind transfer of a Contact Center call, the agent is available to receive another voice contact. To avoid the transferred call being returned to the same agent, configure a break time. On the CS 1000, there can be variations in the implementation of the break timer. To avoid noticeable variations, do not use short break settings; for example, do not create breaks less than eight seconds. Valid values: 0–300 (seconds)
Answer By Placing DN Call On Hold	This field is not applicable on a SIP-enabled server. Select this check box so that agents can place DN calls on hold to answer an incoming call. If you select this option, calls are presented to agents when they place the DN call on hold and signal to the PABX that they are waiting for a call. However, calls are not automatically answered. Agents must press the ACD key on the telephone or be in Ready state on the Agent Desktop to receive the CDN call. If, through the Agent Desktop Display, an agent sees that a call is waiting while active on a DN call, the agent can place the DN call on hold and press the dark In-Calls key to return to the idle agent queue. The In-Calls key stays dark until a call is presented. If you do not select the Answer By Placing DN Call On Hold check box, calls are not presented to an agent while the agent has a DN call on hold.
Agent Reserved for Network Call	Select this check box to display the message *Reserved* on the agent's phone when the server reserves the agent for a network call.

Deleting a call presentation class

Before you begin

- Log on to Contact Center Manager Administration.
- Open the Configuration component.
- Ensure that the call presentation class is not assigned to an agent.

About this task

Delete a call presentation class that is no longer required to save room in your database.

Procedure

1. In the left pane, expand the server from which to delete the call presentation class.
2. Select the **Call Presentation Classes** folder.
3. In the right pane, in the table, highlight the row containing the call presentation class to delete.
4. Press **Delete**.
5. On the **Confirm Delete** message box, click **Yes** to delete the call presentation class.

Chapter 10: Contact Recording and Quality Monitoring server details

Contact Recording and Quality Monitoring (CRQM) management applies to the following types of servers:

- Contact Recording
- Quality Monitoring
- Viewer
- Archiver

Use the Configuration component to associate the CRQM servers with a specific Contact Center Manager Server. After you configure this association, users can navigate from Contact Center Manager Administration to the Web-based management tools for the CRQM servers.

Configuring Contact Recording and Quality Monitoring URLs

Before you begin

- Log on to Contact Center Manager Administration. For more information, see Logging in to Contact Center Manager Administration for Contact Center configuration on page 52.
- Open the Configuration component.

About this task

Configure Contact Recording and Quality Monitoring (CRQM) URLs to allow users to access the CRQM management tools from the Contact Center Manager Administration Launchpad.

Procedure

1. In the left pane, expand the server under which to configure a CRQM server.

2. Select the **Call Recording and Quality Monitoring** folder.

3. In the right pane, if you are adding an Avaya Contact Recording server, click the **Call Recording** heading.

4. Complete the details for the Call Recording server.

5. If you are adding an Avaya Quality Monitoring server, click the **Quality Monitoring** heading.

6. Complete the details for the Quality Monitoring server.

7. If you are adding an Avaya Viewer server, click the **Viewer** heading.

8. Complete the details for the Viewer server.

9. If you are adding an Avaya Archiver server, click the **Archiver** heading.

10. Complete the details for the Archiver server.

11. Click **Submit**.

Chapter 11: Controlled directory numbers

To queue contacts to the PABX and to send messages to the Contact Center Manager Server regarding these contacts, use a controlled directory number (CDN) (Route Point). To ensure that the Contact Center Manager Server can track when contacts terminate at a CDN (Route Point), you must first add a CDN (Route Point) at the PABX, then add the corresponding information at the server, and then acquire the CDN (Route Point).

Configuring and acquiring a CDN (route point)

Before you begin

- Log on to Contact Center Manager Administration. For more information, see Logging in to Contact Center Manager Administration for Contact Center configuration on page 52.

- Open the Configuration component.

- Configure the CDN (Route Point) on the PABX.

- To use the CDN (Route Point) for MCDN Network calls, the server must have Network Skills Based Routing enabled and must be connected to an Avaya Communication Server 1000.

- To use the CDN (Route Point) for DNIS Network calls, the server must have Universal Networking enabled.

About this task

Configure and acquire the CDN (route point) on the Contact Center Manager Server to enable the system to track contacts terminated on it.

Procedure

1. In the left pane, expand the Contact Center Manager Server to which to add the CDN (Route Point).

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

3. In the right pane, in the **Name** box, type the name of the CDN (Route Point) as you want it to appear in reports.

4. In the **Number** box, type the CDN (Route Point) number. This number must match the number configured on the PABX.

5. From the **Call Type** list, select whether you want to use the CDN (Route Point) for Local, MCDN Network, or DNIS Network calls.

6. Click any other row of the table to add the CDN (Route Point).

   Not Acquired appears in the Status column.

7. Select the **Acquired?** check box for the CDN (Route Point).

8. Click any other row of the table to acquire the CDN (Route Point).

9. Click **Refresh Status** to view the current status.

Variable definitions

Name	Description
Name	The name of the CDN (Route Point) as you want it to appear in reports. Valid value: 30-character maximum (no special characters)
Number	The number assigned to the CDN (Route Point). This is the number passed to the PABX in requests to acquire or deacquire the CDN (Route Point). This number must match the number configured at the PABX. ❗ **Important:** You cannot change a saved CDN (Route Point) number. You must delete the CDN and then recreate it. Valid values for SIP and ACCS: 15-digit maximum Valid values for AML: 7-digit maximum
Call Type	❗ **Important:** This box is applicable only if the networking option is enabled. From the Call Type list, select Local, MCDN Network or DNIS Network. To use the CDN (Route Point) for network calls, select a network option. To use the CDN (Route Point) for local calls, select a local option.

Table continues…

Name	Description
Acquired?	**ⓘ Important:** You must configure the CDN (Route Point) on the PABX and add it on Contact Center Manager Server before you can acquire it. Select the Acquired? check box to acquire or deacquire the CDN (Route Point) and then click Refresh Status to refresh the Status column. If the acquisition is successful, Acquired appears in the Status column. When you successfully deacquire the CDN (Route Point), Not Acquired appears in the Status column.
Status	The Status column displays the acquisition status of the CDN (Route Point) or Open Queue CDN (Route Point). When you deacquire the CDN (Route Point), the value Not Acquired appears in this column. Valid values: • Not Acquired • Acquire Pending • Acquired • Acquire Failed • Deacquire Failed • Deacquire Pending The data is read-only.
Refresh Status	Click Refresh Status to refresh the status of the resources that you acquire or deacquire. The current status appears in the Status column.

Configuring and acquiring an Open Queue CDN (route point)

Before you begin

- Log on to Contact Center Manager Administration. For more information, see <u>Logging in to Contact Center Manager Administration for Contact Center configuration</u> on page 52.

- Open the Configuration component.

- To use the CDN (Route Point) for network calls, ensure that Universal Networking is enabled.

About this task

Complete this procedure to configure and acquire an Open Queue CDN (route point).

If you add an Open Queue CDN (route point) you do not need to configure the CDN (route point) on the PABX.

Procedure

1. In the left pane, expand the Contact Center Manager Server to which to add the Open Queue CDN (Route Point).

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

3. In the right pane, select the **OpenQueue** tab.

4. In the **Name** box, type the name of the Open Queue CDN (Route Point) as you want it to appear in reports.

5. From the **Call Type** list select one of the following.

   - Select **Open Queue Local** to use the CDN (Route Point) for local calls.

   - Select **Open Queue Network** to use the CDN (Route Point) for network calls.

6. Click any other row of the table to add the Open Queue CDN (Route Point).

   Not Acquired appears in the Status column.

7. Select the **Acquired?** check box for the Open Queue CDN (Route Point).

8. Click any other row of the table to acquire the Open Queue CDN (Route Point).

9. Click **Refresh Status** to view the current status.

Variable definitions

Name	Description
Name	The name of the CDN (Route Point) as you want it to appear in reports.
	Valid value: 30-character maximum (no special characters)
Call Type	This box is applicable only if the networking option is enabled.
	Select Open Queue Network or Open Queue Local.
	To use the CDN (Route Point) for network calls, select a network option. To use the CDN (Route Point) for local calls, select a local option.

Table continues…

Name	Description
Acquired?	**ⓘ** **Important:** You must configure the CDN (Route Point) on the PABX and add it on Contact Center Manager Server before you can acquire it. Select the Acquired? check box to acquire or deacquire the CDN (Route Point) and then click Refresh Status to refresh the Status column. If the acquisition is successful, Acquired appears in the Status column. When you successfully deacquire the CDN (Route Point), Not Acquired appears in the Status column.
Status	The Status column displays the acquisition status of the CDN (Route Point) or Open Queue CDN (Route Point). When you deacquire the CDN (Route Point), the value Not Acquired appears in this column. Valid values: • Not Acquired • Acquire Pending • Acquired • Acquire Failed • Deacquire Failed • Deacquire Pending The data is read-only.
Refresh Status	Refresh the status of the resources that you acquire or deacquire. The current status appears in the Status column.

Configuring and acquiring a CDN (route point) Landing Pad

Before you begin

- Log on to Contact Center Manager Administration. For more information, see [Logging in to Contact Center Manager Administration for Contact Center configuration](#) on page 52.

- Open the Configuration component.

- Configure the CDN (route point) Landing Pad on the PABX.

About this task

Complete this procedure to configure and acquire a CDN (Route Point) landing pad on the server.

Procedure

1. In the left pane, expand the Contact Center Manager Server to which to add the Landing Pad CDN (Route Point).

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

3. In the **CDNs (Route Points)** window, select the **Landing Pads** tab.

4. In **Name** box, type a name for the CDN (Route Point) Landing Pad.

5. In the **Number** box, type the number for the CDN (Route Point) Landing Pad. This number must match the number configured on the PABX.

6. Click any other row in the grid to add the CDN (Route Point) Landing Pad.

   Not Acquired appears in the Status column.

7. For SIP Contact Centers, you must configure the Landing Pad URI. This field is only present for SIP Contact Centers. In the **URI** box, type the value for the Universal Resource Indicator (URI) of the CDN (Route Point) on the SIP server.

8. Select the **Acquired?** check box for the CDN (Route Point) Landing Pad.

9. Click any other row of the table to acquire the CDN (Route Point) Landing Pad.

10. Click **Refresh Status** to view the current status.

Variable definitions

Name	Description
Name	The name of the CDN (Route Point) as you want it to appear in reports.
	Valid value: 30-character maximum (no special characters)

Table continues…

Name	Description
Number	The number assigned to the CDN (Route Point). This is the number passed to the PABX in requests to acquire or deacquire the CDN (Route Point). This number must match the number configured at the PABX. ❗ **Important:** You cannot change a saved CDN (Route Point) number. You must delete the CDN and then recreate it. • Valid values: Avaya Communication Server 1000—7-digit maximum • SIP—15-digit maximum
URI	The URI box is only present for SIP connected Contact Centers. The Universal Resource Identifier (URI) of the CDN (Route Point). The URI must equate to the fully qualified SIP address for the CDN (Route Point). Valid values: maximum 255 characters, including numbers, English characters, /, \, ?, &, periods, '@' symbol, underscores, and dashes. This field is mandatory. You cannot modify the URI of a saved CDN (Route Point). The URI must be unique to URIs currently assigned to other CDNs, DNISs, or agents.
Acquired?	❗ **Important:** You must configure the CDN (Route Point) on the PABX and add it on Contact Center Manager Server before you can acquire it. Select the Acquired? check box to acquire or deacquire the CDN (Route Point) and then click Refresh Status to refresh the Status column. If the acquisition is successful, Acquired appears in the Status column. When you successfully deacquire the CDN (Route Point), Not Acquired appears in the Status column.

Table continues…

Name	Description
Status	The Status column displays the acquisition status of the CDN (Route Point) or Open Queue CDN (Route Point). When you deacquire the CDN (Route Point), the value Not Acquired appears in this column. Valid values: • Not Acquired • Acquire Pending • Acquired • Acquire Failed • Deacquire Failed • Deacquire Pending The data is read-only.
Refresh Status	Refresh the status of the resources that you acquire or deacquire. The current status appears in the Status column.

Configuring and acquiring a SIP CDN (route point)

Before you begin

- Log on to Contact Center Manager Administration. For more information, see Logging in to Contact Center Manager Administration for Contact Center configuration on page 52.

- Open the Configuration component.

- To use the CDN (Route Point) for network calls, you must enable networking.

About this task

Complete this procedure to configure Contact Center SIP termination addresses.

Procedure

1. In the left pane, expand the SIP-enabled Contact Center Manager Server to which to add the CDN (Route Point).

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

3. In the right pane, in the **Name** box, type the name of the CDN (Route Point) as you want it to appear in reports.

4. In the **Number** box, type the CDN (Route Point) number.

5. In the **URI** box, type the type in a value for the Universal Resource Indicator (URI) of the CDN (Route Point) on the SIP server.

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

7. Click any other row of the table to add the CDN (Route Point).

   Not Acquired appears in the Status column.

8. Select the **Acquired?** check box for the CDN (Route Point) Landing Pad.

9. Click any other row of the table to acquire the CDN (Route Point) Landing Pad.

10. Click **Refresh Status** to view the current status.

Variable definitions

Name	Description
Name	The name of the CDN (Route Point) as you want it to appear in reports. Valid values: Any freeform string that describes the route point, type, or function (for example, IM_sales for an IM route point that handles sales)
Number	The number assigned to the CDN (Route Point). This is the number passed to the PABX in requests to acquire or deacquire the CDN (Route Point). This number must match the number configured at the PABX. For example you can configure an E.164 dial plan, that routes calls to the contact center, to allow 15–digit route points. If you configure your route point as a 15–digit number on the PABX, you must enter the matching 15–digit value here. 🛈 **Important:** You cannot change a saved CDN (Route Point) number. You must delete the CDN and then recreate it. Valid values: 15-digit maximum
URI	The Universal Resource Identifier (URI) of the CDN (Route Point). The URI must equate to the fully qualified SIP address for the CDN (Route Point). Valid values: maximum 255 characters, including numbers, English characters, /, \, ?, &, periods, '@' symbol, underscores, and dashes. This field is mandatory. You cannot modify the URI of a saved CDN (Route Point). The URI must be unique to URIs currently assigned to other CDNs, DNISs, or agents.

Table continues…

Controlled directory numbers

Name	Description
Call Type	ⓘ **Important:** This box is applicable only if the networking option is enabled. Select Local, MCDN Network or DNIS Network. To use the CDN (Route Point) for network calls, select a network option. To use the CDN (Route Point) for local calls, select a local option.
Acquired?	ⓘ **Important:** You must configure the CDN (Route Point) on the PABX and add it on Contact Center Manager Server before you can acquire it. Select the Acquired? check box to acquire or deacquire the CDN (Route Point) and then click Refresh Status to refresh the Status column. If the acquisition is successful, Acquired appears in the Status column. When you successfully deacquire the CDN (Route Point), Not Acquired appears in the Status column.
Status	The Status column displays the acquisition status of the CDN (Route Point) or Open Queue CDN (Route Point). When you deacquire the CDN (Route Point), the value Not Acquired appears in this column. Valid values: • Not Acquired • Acquire Pending • Acquired • Acquire Failed • Deacquire Failed • Deacquire Pending The data is read-only.
Refresh Status	Click Refresh Status to refresh the status of the resources that you acquire or deacquire. The current status appears in the Status column.

Acquiring multiple configured CDNs (Route Points)

About this task

Follow this procedure to acquire a large number of CDNs (Route Points). You can do this, for example, to acquire a number of CDNs (Route Points) imported into CCMA using a bulk import. If you have a large number of CDNs (Route Points) to acquire, this operation can take some time.

Procedure

1. In the left pane, expand the Contact Center Manager Server on which you want to acquire multiple CDNs (Route Points).

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

3. Click **Acquire All CDNs**.

4. On the Acquire Confirmation dialog, click **Yes**.

   Contact Center acquires all the CDNs (Route Points) that are not in the Acquired state. Depending on the number of CDNs that are not in the Acquired state, this can take some time.

5. When Contact Center finishes acquiring the CDNs (Route Points), click **Refresh Status** and check the status of all the CDNs (Route Points).

Deacquiring a CDN (route point)

Before you begin

- Log on to Contact Center Manager Administration.
- Open the Configuration component.

About this task

Deacquire a CDN (route point) to stop the system from tracking calls terminated on it. Before you can delete a CDN (route point), you must deacquire it.

Procedure

1. In the system tree, expand the server on which you need to deacquire the route point.

   The server displays the server resources.

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

3. In the right pane, select the applicable tab.

   For example, to deacquire an Open Queue CDN (Route Point) select the OpenQueue tab.

4. Clear the **Acquired?** check box for the CDN (Route Point) to deacquire.

5. Click any other row in the table to deacquire the CDN (Route Point).

   The status appears in the Status column.

6. To view the current status, click **Refresh Status**.

Deleting a CDN (route point)

Before you begin

- Log on to Contact Center Manager Administration. For more information, see Logging in to Contact Center Manager Administration for Contact Center configuration on page 52.
- Open the Configuration component.
- Deacquire the CDN. See Deacquiring a CDN (route point) on page 85.

About this task

When you delete a CDN (Route Point) from the Contact Center Manager Server, the CDN (Route Point) does not delete from the PABX.

Procedure

1. In the left pane, expand the Contact Center Manager Server that contains the CDN (Route Point) to delete.

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

3. In the right pane, select the applicable tab.

   For example, to delete an Open Queue CDN (Route Point) select the OpenQueue tab. There is no tab to select if you delete a SIP CDN (Route Point).

4. Select the CDN (Route Point) to delete.

5. Press **Delete**.

6. In the **Confirm Delete** message box, click **Yes** to delete the CDN (Route Point) from the server.

Deacquiring all CDNs (Route Points)

Before you begin

- ⚠ **Caution:**

  Ensure your contact center is not actively processing customer contacts. Deacquiring all CDNs (Route Points) stops all call processing in Contact Center.

About this task

Follow this procedure to deacquire all the CDNs (Route Points) that are in the Acquired state. Deacquire all the CDNs (Route Points) only in exceptional circumstances, such as troubleshooting. Deacquiring all CDNs (Route Points) stops all call processing in Contact Center.

Procedure

1. In the left pane, expand the Contact Center Manager Server on which you want to deacquire multiple CDNs (Route Points).

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

3. Click **De-acquire All CDNs**.

4. On the De-acquire Confirmation dialog, click **Yes**.

   Contact Center deacquires all the CDNs (Route Points) that are in the Acquired state. Depending on the number of CDNs that are in the Acquired state, this can take some time.

5. When Contact Center finishes deacquiring the CDNs (Route Points), click **Refresh Status** and check the status of all the CDNs (Route Points).

Chapter 12: Contact types

Contact types are the media types by which (inbound) contacts arrive into a contact center and by which a contact center sends (outbound) contacts.

A contact type determines how a contact center handles contacts. An example is email: when a contact center customer sends an email message, the contact center receives the message, and routes the message according to various email-specific rules. If required, an agent with email ability processes the email message.

The following table lists the default contact types.

Table 1: Contact types

Default contact type	Skillset prefix	Description	Supported on
Voice	None	Default Voice Contact Type	Open Queue-enabled Contact Center Manager Server SIP-enabled Contact Center Manager Server
Email	EM_	Default CCMM email Contact Type	Open Queue-enabled Contact Center Manager Server
Fax message	FX_	Default CCMM Fax message Contact Type	Open Queue-enabled Contact Center Manager Server SIP-enabled Contact Center Manager Server
Scanned Document message	SD_	Default CCMM Scanned Document message Contact Type	Open Queue-enabled Contact Center Manager Server SIP-enabled Contact Center Manager Server
SMS Text message	SM_	Default CCMM SMS Text message Contact Type	Open Queue-enabled Contact Center Manager Server SIP-enabled Contact Center Manager Server
Voice Mail message	VM_	Default CCMM Voice Mail message Contact Type	Open Queue-enabled Contact Center Manager Server SIP-enabled Contact Center Manager Server

Table continues…

Default contact type	Skillset prefix	Description	Supported on
Web_Communications	WC_	Default CCMM Web communication Contact Type	Open Queue-enabled Contact Center Manager Server
Outbound	OB_	Default CCMM Outbound Contact Type	Open Queue-enabled Contact Center Manager Server
IM	IM_	Default IM Contact Type	SIP-enabled Contact Center Manager Server
Social_Networking	SN_	Default Social Networking Contact Type	Open Queue-enabled Contact Center Manager Server
POM_Outbound	PO_	Default POM Contact Type	Open Queue-enabled Contact Center Manager Server
Video	VI_	Default Video Contact Type	SIP-enabled Contact Center Manager Server
OpenQ	OQ_	Default Open Queue Contact Type	Open Queue-enabled Contact Center Manager Server

Editing a contact type

Before you begin

- Log on to Contact Center Manager Administration.

- Open the Configuration component.

- Note the following:

  - You cannot delete a default contact type.

  - You cannot edit the contact type name or the skillset prefix.

About this task

Edit a contact type to change the description of the contact type or to change the default skillset assigned to that contact type.

Procedure

1. In the system tree, expand the server on which you need to edit the contact type.

   The server displays the server resources.

2. Select the **Contact Types** folder.

3. In the right pane, select the Contact Type to edit.

4. To sort the contact types, click a column header.

   For example, if you click the Name column header, the contact types are sorted alphabetically according to Contact Type name.

5. From the **Default Skillset** list, select a new default skillset, and then press Tab.

6. In the **Description** box, type a new description for the contact type.

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

Variable definitions

Name	Description
Name	The name of the contact type. ❗ **Important:** You cannot modify contact type names.
Skillset Prefix	The prefix that identifies the default skillset that handles contacts of this contact type. There is no skillset prefix for the default contact type, voice. Skillsets without a skillset prefix default to the voice contact type. Valid value: 3-character maximum, the last of which must be an underscore (_) (no special characters, must be unique) ❗ **Important:** You cannot modify a skillset prefix for a default contact type.
Default Skillset	Select the skillset to which contacts route for processing when they are not handled in a script. Valid values: 30-character maximum, no special characters allowed. ❗ **Important:** You must first configure the default skillset in Contact Center Manager Administration. The default skillset must have the same skillset prefix as the contact type.
Description	The description for the contact type. Valid value: Maximum 60 characters (optional, can be updated, special characters are allowed).

Chapter 13: Dialed number identification services

A dialed number identification service (DNIS) is an optional service that allows Contact Center Manager Server to identify the phone number dialed by the incoming caller. An agent can receive calls from customers calling in to different DNISs and, if the DNIS appears on the phone display, can prepare a response according to the DNIS.

Configuring a DNIS

Before you begin

- Configure the CDN, ACD-DN, or supplementary DN on the PABX.
- Log on to Contact Center Manager Administration. For more information, see Logging in to Contact Center Manager Administration for Contact Center configuration on page 52.
- Open the Configuration component.

About this task

A Dialed Number Identification Service (DNIS) is a method by which the system recognizes the phone number that a caller dials. Agents can receive contacts from customers calling in on different DNISs and customize their response according to the DNIS that appears on the phone display. Based on the DNIS, the system can direct contacts to a controlled CDN and supply different treatments.

You cannot modify a saved DNIS. You can delete a saved DNIS and add a new DNIS.

Procedure

1. In the left pane, expand the server on which to add the DNIS.
2. Select the **DNISs** folder.
3. In the right pane, select the **Local** tab.
4. In **Name** box, type the name of the new DNIS as you want it to appear in reports.
5. In the **Number** box, type the DNIS number.
6. If you add a DNIS on a SIP-enabled server, in the **URI** box, type a URI for the DNIS, and then press **Tab**. Otherwise, proceed to the next step.

> 🛈 **Important:**
>
> The URI must be unique to URIs currently assigned to other DNISs, CDNs, or agents and must not begin with SIP.

7. In the **Service Level Threshold** box, type the time in seconds within which all contacts coming in on this DNIS must be answered or abandoned. The threshold value is used for historical reporting.

8. In the **Description** box, type the description of the DNIS. For example, type the DNIS prefix. You can use the description to sort, filter, and group individual DNIS numbers in user-created, custom historical reports.

9. Click any other row in the grid to save the DNIS.

Variable definitions

Name	Description
Name	The name of the DNIS as you want it to appear in reports. Valid values: 30-character maximum (no special characters)
Number	The number assigned to the DNIS. This is the directory number at which the contact arrives at the PABX. 🛈 **Important:** You cannot change a saved DNIS. You must delete the DNIS and then recreate it. Valid values: 31-digit maximum. Avaya recommends that you enter only 30 digits, as callers can use the pound sign (#) as a delimiter, and this counts towards the 31-digit limit.
URI	For SIP-enabled servers only. In the URI box, type the Universal Resource Identifier (URI) of the DNIS on the SIP-enabled server. Valid values: maximum 255 characters, including numbers, English characters, /, \, ?, &, periods, '@' symbol, underscores, and dashes. This field is mandatory. Once you save the URI, you cannot modify it. The URI must be unique to URIs assigned to other DNISs, CDNs, or agents and must not begin with SIP.

Table continues…

Name	Description
Service Level Threshold	Not applicable for DNIS Landing Pads.
	The service level threshold assigned to the DNIS. This is the time, in seconds, in which all contacts coming through on this DNIS are to be answered or abandoned.
	Valid values: 4-digit maximum
Description	The description of the DNIS number. For example, type a DNIS prefix, such as 1-800. You can use this description to sort, to filter and to group individual DNIS numbers in user-created custom reports.
	Valid values: maximum 16 characters

Configuring a DNIS landing pad

Before you begin

- Ensure that the CDN, ACD-DN, or supplementary DN is configured on the PABX.

- Log on to Contact Center Manager Administration. For more information, see Logging in to Contact Center Manager Administration for Contact Center configuration on page 52.

- Open the Configuration component.

About this task

Configure DNIS Landing Pads for routing calls between sites when you have Universal Networking enabled.

A Landing Pad identifies the call that is sent to a target site. The target site reserves a Landing Pad for the call ID at the source site. The source site then requests the PABX to send the call to the Landing Pad. When the call arrives on the Landing Pad at the target site, the Contact Center Manager Server maps the call to the original call ID at the source to determine to which agent to present the call. Landing Pads can be either CDNs or DNISs. For information about CDN Landing Pads, see Configuring and acquiring a CDN (route point) Landing Pad on page 79.

Procedure

1. In the left pane, expand the server on which to add the DNIS Landing Pad.

2. Select the **DNISs** folder.

3. In the DNISs window, select the **Landing Pads** tab.

4. In **Name** box, type the name of the new DNIS.

5. In the **Number** box, type the DNIS number. This number must match the number configured on the PABX.

6. Optionally, in the **Description** box, type a description for the DNIS Landing Pad.

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

Variable definitions

Name	Description
Name	The name of the DNIS as you want it to appear in reports. Valid values: 30-character maximum (no special characters)
Number	The number assigned to the DNIS. This is the directory number at which the contact arrives at the PABX. ⓘ **Important:** You cannot change a saved DNIS. You must delete the DNIS and then recreate it. Valid values: 31-digit maximum. Avaya recommends that you enter only 30 digits, as callers can use the pound sign (#) as a delimiter, and this counts towards the 31-digit limit.
Description	The description of the DNIS number. For example, type a DNIS prefix, such as 1-800. You can use this description to sort, to filter and to group individual DNIS numbers in user-created custom reports. Valid values: maximum 16 characters

Chapter 14: Formulas

Use the Formulas window to create custom real-time statistics fields by combining existing statistics fields with mathematical operators. You can save these custom statistics fields as formulas and use them in your private Real-Time Reporting displays. For example, you can create a custom formula to calculate the service level.

Creating a custom formula

Before you begin

- Log on to Contact Center Manager Administration.
- Open the Configuration component.
- Ensure that you are familiar with the available real-time statistics fields. For more information, see *Using Avaya Aura® Contact Center Reports and Displays*.

About this task

Create a custom formula to create custom real-time statistics fields by combining existing statistics fields with mathematical operators. You can then save these custom statistics fields as formulas and use the formulas in your private Real-Time Reporting displays.

Procedure

1. In the left pane, expand the server on which to create the formula.

2. Select the **Formulas** folder.

3. In the right pane, in the **Available Formulas** box, type the name of the new formula, and then press Tab.

4. From the **Statistics Group** list, select the statistics group that contains the statistics field to include in your formula.

5. Press **Tab** or **Enter** to display the **Formula Editor**.

6. In the Formula Editor, in the **Comment** box, type information about the formula (optional).

7. From the **Variables** list, select the variable to use in the formula.

> ❗ **Important:**
>
> When you select a variable, it appears in the Formula box with a percent symbol (%) preceding it. The percent symbol identifies it as a variable; it is not a mathematical operator.

8. From the numeric keypad, select any numeric input to apply to the formula.

9. After you select a mathematical operator, you can select another variable to add to the formula. For example a formula for service level is Calls Answered – Calls Answered Aft Threshold / Calls Answered. The formula can be up to 250 characters.

10. To use the higher or lower of two values in your formula, click **Max** or **Min**.

11. After you finish creating the formula, click **Save**.

12. Click **Close** to return to the Formulas window.

Variable definitions

Name	Description
Available Formulas	Type a name for the custom formula and then press Tab to select the Statistics Group for the formula. To edit an existing formula, double-click the formula name in the Available Formulas column. The Formula Editor appears, listing the Formula components.
Statistics Group	Select the statistic group for the formula. Statistics groups are sets of related statistics defined in the database, such as agent statistics or skillset statistics. After you select the statistics group, press Enter or Tab. The Formula Editor appears, in which you can create your custom formula.
Formula Name	The name of the formula, as you entered it in the Available Formulas box in the Formulas window. You can change formula name in the Formula Editor.
Comment	Type any additional information about your custom formula.
Formula	The variables and mathematical operators that you choose for your custom formula. You can add new variables and operators, or edit the existing ones.

Table continues…

Name	Description
Variables	The existing statistics fields that you can combine to create custom formulas. After you create a formula, you can apply it to your private Real-Time Reporting displays to control the type of data that you see.
	From the Variables list, select the variables to add to your custom formula. After you select a variable, you must choose a mathematical operator (/, *, -, or +) before you can select another variable, or before you can enter any numeric values.
	When you select a variable, it appears in the Formula box with a percent symbol (%) preceding it. The percent symbol identifies it as a variable; it is not a mathematical operator.
Numeric keypad	ⓘ **Important:**
	After each variable, you must select a mathematical operator before you can select another variable.
	• Back Space — Removes the last item that you enter in your formula. To remove more items, you must click C to clear the entire formula.
	• C — Clears the entire formula from the Formula box.
	• / — Divides the variables in the formula.
	• * — Multiplies the variables in the formula.
	• - — Subtracts the variables in the formula.
	• + — Adds the variables in the formula.
	• , — Separates the Max and Min variables in the formula.

Table continues…

Name	Description
Max and Min	Use the Max and Min buttons to use the higher of two values (Max), or the lower of two values (Min) in your formula.
	When you click Max or Min, a set of brackets appears in the Formula box. In these brackets, add the two values to compare, separated by a comma.
	The format must be as follows: Max[a,b], where a can be one variable, or two variables separated by an operator, and b can be one variable, or two variables separated by an operator.
	For example, if you specify Max[Agent_Available+Agent_Not_Ready, Agent_In_Service+Agent_On_This_Skillset_Call], the system calculates the values for Agent_Available+Agent_Not_Ready and for Agent_In_Service+Agent_On_This_Skillset_Call, and uses the higher of the two values in the formula. If you use Min in this example, the system calculates the lower of the two values.
Save	Save changes you make in the Formula Editor.
Close	Exit the Formula Editor.

Editing or viewing formulas

Before you begin

- Create at least one custom formula.

About this task

You cannot edit standard formulas; you can edit only custom formulas.

Procedure

1. In the left pane, expand the server containing the formula you want to edit.

2. Select the **Formulas** folder.

3. In the right pane, in the **Available Formulas** column, double-click the name of the formula to edit.

4. In the Formula Editor, you can modify the formula name, the formula comment, and the formula.

5. To add a new variable to an existing formula, you must click an operator (/, *, −, +) to add it to the end of the formula, and then select the new variable from the **Variables** list.

6. To delete elements from the formula, in the **Formula** box, select the elements, and then press **Delete**.

7. After you finish your changes, click **Save** to save the formula.

8. Click **Close** to close the Formula Editor.

Chapter 15: Global settings

In the Global Settings window, you can configure the global values on the Contact Center Manager Server, which include Agent Order preference, default RAN route, default IVR DN, Expected Wait Time algorithm, Broadcast Ports and default timer, and where the historical reporting statistics are gathered. You can also configure Toll Free Queuing.

Toll Free Queuing

Regulations introduced in Germany in 2012 require that callers to special service numbers for contact centers must not be charged for their call while their reason for calling is not being attended to. A transitional arrangement allowed for a two-minute free period during queuing, but as of June 2013 call queues must either be a fixed price or free of charge. The Avaya Aura® Contact Center Toll Free Queuing feature supports free queuing of calls within certain technical constraints.

While the German regulations relate to all queues, Toll Free Queuing affects only the caller's first queue; that is, the queue in which the caller waits for their initial contact with the contact center. Toll Free Queuing does not support secondary queues. For example, if an agent answers a caller, and then forwards the caller to another agent, places the call on hold, or forwards the caller to a Route Point where they queue for another agent, the second queue is not toll free.

Operation:

When you enable Toll Free Queuing, Contact Center does not send a SIP 200 OK final response to the caller SIP INVITE when it queues the call. Instead, Contact Center sends a 183 Session Progress message. The 183 Session Progress message is a reliable provisional response, that Contact Center resends periodically. This delays the PABX from sending the carrier an ISDN CONNECT thus delaying the carrier from establishing the call. The Contact Center Orchestration Designer application flows can give ringback, recorded announcements (RAN), silence, IVR Play Prompt, and music without affecting call completion. During this time, the carrier cannot start charging the caller. During this period the carrier bears the cost of the call. Some carriers place a time limit on this period, after which they drop the call if Contact Center has not answered it.

Implementation:

In Contact Center, you enable this feature using a checkbox on the Contact Center Manager Administration Global Settings page. You also set the time after which the Contact Center enables billing to start.

The best solution results where the external carrier, connected to the CM by ISDN trunks, supports Annex K (Procedure for establishment of bearer connection prior to call acceptance) of the ISDN specification. In this case you set PROGRESS with Progress Indicator 8 indicating in band information. The caller can hear ringback, RAN, IVR Play Prompt, and music that Contact Center provides, without incurring a charge from the carrier.

If a carrier does not support Annex K of the ISDN specification, you must set the ALERTING interworking message on Communication Manager. The caller can hear only ringback provided by the network and cannot hear Contact Center treatments.

For more information about configuring Communication Manager for Toll Free Queuing, see *Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration*.

A practical limitation on how you implement Toll Free Queuing on special service numbers is the length of time that the carrier retains the call while not receiving an answer response from the Contact Center. Many carriers have a two or three minute limit, after which they drop the call and give a disconnect tone to the caller. This is because they have not received an ISDN CONNECT message for the call.

In situations where the carrier allows only a limited time without an ISDN CONNECT response, you need to decide how to treat these calls. To be fully compliant with the German regulations, and ensure no billing at all of customers, you set the time limit in CCMA Global Settings to a value greater than that supported by the carrier. In this case the carrier does not receive the ISDN CONNECT, and drops the call. The caller receives a disconnect tone.

Alternatively you can add code to your Orchestration Designer application flows to anticipate whether an agent answers the call within the toll-free time. If this is unlikely, you can give a RAN or IVR Play Prompt treatment to explain the reason for disconnecting the call, and then disconnect the call gracefully.

For example, a carrier implements a two minute limit on the amount of time it waits for an acknowledgement. You write your flow application to compare the age of the call with the Expected Wait Time (EWT) for the contact center. When the age of the call is 90 seconds and the EWT is still greater than 30 seconds (the call cannot be answered within two minutes), the flow application plays a recorded announcement to the caller, followed by a GIVE BUSY treatment.

An alternative approach is to give IVR Play and Collect treatment to the caller when the call age is 115 seconds.

In a contact center that can take calls to special service, fixed charge, and local numbers, your Orchestration Designer application flows must include logic to handle all call types. If you enable Toll Free Queuing in Contact Center, you must add logic to immediately connect calls to fixed charge and local numbers. These are not subject to the legislation, and so charging must start immediately. For calls to these numbers, add a Free Form IVR block with the **Toll_Free_Queuing_Connect** parameter.

Limitations:

Contact Center supports this feature only in integrations with Avaya Aura® Communication Manager (CM) where the customer call arrives on the CM through an ISDN trunk. Where the PABX is an Avaya Communication Server 1000, the PABX itself can accommodate toll free queuing on native ACD calls, with the application and configuration of patch MPLR31699. However, calls to CDNs acquired by Contact Center do not support Toll Free Queuing.

SIP-enabled contact centers on an Avaya Communication Server 1000 PABX do not support Toll Free Queuing. In a mixed environment, calls to the contact center CM from other PABXs or other types of trunk do not support Toll Free Queuing.

Contact Center can implement Toll Free Queuing only for calls over which it has call control. For example, if a flow application implements a ROUTE CALL command, Contact Center no longer has control of the call, and cannot apply Toll Free Queuing settings such as `Maximum time to delay`

`call establish`. Where Toll Free Queueing is enabled, the ROUTE CALL command is always uncontrolled, even where the flow application uses the CONTROLLED keyword.

When you implement Toll Free Queuing, any call that does not come directly from Communication Manager (CM) or Session Border Controller (SBC) to AACC is not supported, and AACC rejects the call. For example, consider the following call flow:

1. A call for a non-agent extension number comes in to the customer premises through an ISDN trunk.

2. The CM re-routes the call with Cover No answer to Avaya Aura® Messaging voicemail.

3. The caller presses 0 to use the zero out feature of Avaya Aura® Messaging, routing the call to an AACC CDN.

AACC rejects the call, because the call to the CDN comes from Avaya Aura® Messaging, not from the CM or SBC.

Non-skillset call monitoring beep tone

In a SIP-enabled contact center based on a Communication Manager PABX, Contact Center supports supervisor/agents observing and barging-in to non-skillset calls. You can configure beep tones for both observe and barge-in events. In the Global Settings window, you can enable beep tone, and specify the Communication Manager, the CTI station, and beep tone announcement extensions. Before enabling beep tone in CCMA, configure the CTI station and announcement extensions on Communication Manager. For more information about configuring beep tone on Communication Manager, see *Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration*.

Configuring Global Settings Common Settings

Before you begin

- Log on to Contact Center Manager Administration.
- Open the Configuration component.

About this task

In the Global Settings window, you can set the global values on the Contact Center server.

The Redirection Settings tab allows you to configure global settings for call redirection. How your contact center handles redirected calls depends on your solution and your solution's available routing options. For more information about call redirection, see "Call Redirection with AACC Application Note" available at http://support.avaya.com.

Procedure

1. In the left pane, expand the server on which to configure global settings.

2. Select the **Global Settings** folder.

3. Select **Common Settings**.

4. Configure the global settings for your system based on the fields listed in the Global Settings window.

5. Click **Submit**.

Variable definitions

Name	Description

Agent Order Preference	Choose how to present contacts to agents based on their idle time.
	
	Valid values:
	
	• Longest total time in idle state since login—Choose this option to present contacts to the agent who accumulated the most idle time since logging on.
	
	   Contact Center calculates this time differently for an agent with a Multiplicity Presentation Class (MPC) who has one or more open contacts. In this case Contact Center uses the time since the agent last opened a contact, minus the Delay value in the MPC.
	
	• Longest time in idle state since last status change—Choose this option to present contacts to the agent who accumulated the most idle time since the last status change for that agent (this is the system default setting).
	
	• Longest total time since last CDN/ACD call or contact—Choose this option to present contacts to the agent with the longest elapsed time since handling a CDN/ACD call.
	
	❗ **Important:**
	
	   The system does not reset the timer when the agent switches to the Not Ready state.

Default Ran Route (CS1000 only) Default DN (SIP only)	The default treatment DN to use when a script contains voice processing commands. The Default Ran Route box does not explicitly state a treatment DN.
Maximum Ports with Queuing for Broadcast (CS1000 only)	The total number of IVR ports that can be user-controlled for broadcast at any time. Valid values: 191 maximum
Broadcast Voice Port Wait Timer (CS1000 only)	The number of seconds the system waits for a voice port to become available.

Table continues…

Name	Description
Default Access IVR DN (CS1000 only)	Select the default DN to use in the event that a script contains voice processing commands that can take an IVR ACD-DN as a parameter, but does not explicitly state an IVR ACD-DN. Valid values: 7-digit maximum IVR DN, followed by the name of the default IVR DN (for example, 999, Default_IVRQ)
Expected Wait time (EWT) Algorithm (CS1000, SIP)	Select either NES EWT or Enhanced EWT as required. Valid values: • NES EWT—This is a legacy algorithm for calculating the expected wait time using real data available in the system. (Actual wait time of previously serviced contacts.) • Enhanced EWT—This is a new algorithm, which is more accurate than the NES EWT. This also uses actual wait time data available in the system. Selecting the Enhanced EWT algorithm affects only the Task Flow Executor (TFE). CCMA Real Time Displays (RTDs) continue to use the NES EWT algorithm to display expected wait times.
Report against standby CCMS	Select to enable historical report statistics to be gathered from the standby server specified in the Address box. The check box is available if High Availability is configured and shadowing is operational in your Contact Center. The IP address in the Standby Server Address box is the physical IP address of the standby server. If the standby server goes down, then historical reporting statistics are automatically taken from the primary server. If an Avaya Aura® Contact Center switchover occurs, then historical reporting statistics are automatically taken from the server that is currently active.
Media Server Zoning	Select to enable Avaya Aura® Media Server Zoning, if licensed.

Table continues…

Name	Description
Enter ACW using Not Ready without Reason Code	Select the **Enter ACW using Not Ready Without Reason Code** option under **Global Settings**, so that agents can continue to work as they did before the introduction of ACW codes. Agents can then mimic the Post Call Processing (PCP) time model of earlier releases by pressing Not Ready without specifying a code. In this case Contact Center puts the agent into ACW with the default code ACW code 00000. Post Call Processing (PCP) time starts to peg against the default ACW code 00000 immediately after the agent completes the contact.

Enabling Toll Free Queuing

Before you begin

- Configure the Communication Manager to support Toll Free Queuing. For more information about configuring Communication Manager, see *Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration*.
- Understand the carrier's time limitations on retaining a call when it has not received an ISDN CONNECT message, and plan the method by which you treat calls that exceed the time limit.

About this task

Enable Toll Free Queuing to comply with German regulations that specify that a caller to a special service number must not be charged for their call while their reason for calling is not being attended to.

Procedure

1. Log on to Contact Center Manager Administration with Administrative privileges.
2. On the Launchpad, select **Configuration**.
3. In the left pane, expand the Contact Center Manager Server on which to configure Toll Free Queuing.
4. Select the **Global Settings** folder.
5. Select the **Common Settings** tab.
6. To enable Toll Free Queuing, select **Toll Free Queuing**.
7. In the **Maximum time to delay call establish** field, enter the number of seconds that Contact Center waits before sending a call connect message to the PABX.

> ! **Important:**
>
> When Contact Center sends the 200 OK response to the PABX, the PABX connects the call and the carrier starts charging the caller. Ensure that the value you put in the **Maximum time to delay call establish** field enables your contact center to meet toll free queue regulatory requirements.

8. Click **Submit**.

Next steps

If the carrier implements a limit on the time it waits for an ISDN CONNECT message, modify your Avaya Orchestration Designer flow applications to ensure callers receive either a controlled disconnect before charging starts, or a relevant IVR treatment when the carrier starts charging.

Toll Free Queuing is a global setting, and applies to all inbound customer calls in Contact Center. Where you want to immediately connect some calls (e.g. fixed charge calls, or calls from another jurisdiction), use an Avaya Orchestration Designer flow application with a Free Form IVR block that includes the Toll_Free_Queuing_Connect parameter. This block ensures that AACC sends a SIP 200 OK (ISDN CONNECT) message, and the carrier can start charging the caller.

Configuring Non-Skillset Call Monitoring

Before you begin

- Complete beep tone configuration on Communication Manager. For more information about beep tone configuration on Communication Manager, see *Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration*.

About this task

Enable beep tone for Non-Skillset Call Monitoring, and specify the Communication Manager parameters to support it.

Procedure

1. Log on to Contact Center Manager Administration with Administrative privileges.

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

3. In the left pane, expand the Contact Center Manager Server on which to enable beep tone for Non-Skillset Call Monitoring.

4. Select the **Global Settings** folder.

5. Select the **Non-Skillset Call Monitoring** tab.

6. To enable beep tone for Non-Skillset Call Monitoring, select **Enable Beep Tone**.

7. In the **Proxy URI** field, enter the SIP URI of the CTI station that you configured on the Communication Manager.

8. In the **Announcement IP address** field, enter the IP address of the Communication Manager on which you configured the announcements for the beep tones.

9. In the **Observe Extension** field, enter the extension number of the announcement that you configured on the Communication Manager for the Observe beep tone.

10. In the **Barge-In Extension** field, enter the extension number of the announcement that you configured on the Communication Manager for the Barge-in beep tone.

11. Click **Submit**.

Configuring Media Settings

Before you begin

- Log on to Contact Center Manager Administration.
- Open the Configuration component.

About this task

Contact Center provides observe, barge-in, and whisper coach features for voice contacts. These actions are performed by agent-supervisors on Agent Desktop.

If you want to enable agent-supervisors to silently observe and barge-in on voice contacts, mute the observation and barge-in tones. Note that many jurisdictions have legal requirements concerning observing calls: ensure your configuration is compliant with relevant national and local legislation.

This procedure relates only to observing incoming Contact Center voice contacts. It does not affect the beep tone for non-skillset call monitoring.

By default, the agent and the customer on the voice contact hear the observation tone when an agent-supervisor joins or leaves the voice contact. They also hear the observation tone repeatedly at regular intervals during the voice contact.

Procedure

1. In the left pane, expand the server on which to configure global settings.

2. Click **Configuration**.

3. Select the **Global Settings** folder.

4. Select **Media Settings**.

5. Select **Barge In Tone** to enable the barge-in tone for voice contacts. Clear the **Barge In Tone** check box, to disable the barge-in tone for voice contacts.

6. Select **Observation Tone** to enable the observation for voice contacts. Clear the **Observation Tone** check box, to disable the observation tone for voice contacts.

7. In the **Observation Tone Timer (sec)** box, type the number of seconds between observation tones. This configures the observation tone interval for voice contacts.

8. Select **Record Tone** to enable the record tone for voice contacts. Clear the **Record Tone** check box, to disable the record tone for voice contacts.

9. In the **Record Tone Timer (sec)** box, type the number of seconds between record tones. This configures the record tone interval on voice contacts.

10. Click **Save**.

Chapter 16: Historical statistics

To use the Historical Reporting feature, you must first gather historical statistics. You can configure the following historical statistics collection options:

- The general system parameter values, such as the number of skillsets

- The type of call flow, agent, and IVR historical statistics to collect

- The applications for which call-by-call data is collected

- The length of time that historical statistics are stored on Contact Center Manager Server

You can calculate the amount of disk space required to run your selected configuration and specify the first business day of the week. The database size calculation depends on parameters, duration, call center busy count (CBC), and statistic values. These statistics are used to generate tabular and graphical historical reports. For more information about historical reporting, see *Using Avaya Aura*®️ *Contact Center Reports and Displays*.

You can also designate the standby server in an HA environment to run historical reports to reduce the load on the primary server. For more information about using the standby server for historical statistics, see .

Configuring Historical statistics

About this task

Configure historical statistics to configure the following collection options:

- The general system parameter values, such as the number of skillsets

- The type of call flow, agent, and IVR historical statistics to be collected

- The applications for which call-by-call data is collected

- The length of time that historical statistics are stored on Contact Center Manager Server

Before you begin

- Log in to Contact Center Manager Administration.

- Open the Configuration component.

Procedure

1. In the left pane, select the **Historical Statistics** folder.

2. In the right pane, enter your configuration data in the following tables:

- **Parameters table**: For each parameter, enter a value that is less than or equal to the purchased value, and greater than or equal to the measured value. When choosing a value, remember to allow for future growth.

- **Collect the following statistics table**: For each statistic type, in the Collect column, select the check box beside the statistics to collect, or clear the check box beside the statistics not to collect.

- **Call-by-Call table**: For each application, from the Statistics Collection Method list, select the type of contacts for which to collect call-by-call statistics.

- **Duration table**: Enter the amount of time the statistic is stored on the server. The time units vary depending on the statistic. The limit for each statistic, with the exception of the **Length of Business day** and **Business week contains** statistics, is 1825 time units (days, weeks, or months).

  To reduce the duration of a statistic, Contact Center purges all data for a statistic that is older than the new specified duration.

3. From the **Business week starts** list, select the day to start accumulating weekly statistics.

4. Click **Calculate** to determine if sufficient disk space is available for the selected historical statistics collection configuration.

   The **Call-by-Call Database** and **System Database Required** fields display the disk space requirements for the selected configuration. The **Call-by-Call Database** and **System Database Actual** fields display the available disk space.

   > ❗ **Important:**
   >
   > If the disk space required is greater than the disk space available, reduce the number of days the data is stored or change the number of estimated contacts per hour until sufficient disk space is available for your configuration.

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

Chapter 17: IVR ACD-DNs

An IVR ACD-DN is a queue to which voice-processing contacts are directed. Each IVR ACD-DN must have dedicated voice ports to provide voice-processing treatment for various contact types. An IVR ACD-DN must be acquired for both integrated and non-integrated systems.

IVR ACD-DNs do not apply when you configure a SIP-enabled Contact Center Manager Server.

Configuring and acquiring an IVR ACD-DN

Before you begin

- Configure the IVR ACD-DN on the PABX.
- Each IVR ACD-DN must have dedicated voice ports to provide voice-processing treatment for different contact types.
- You cannot modify a saved IVR ACD-DN. You can delete a saved IVR ACD-DN and add a new IVR ACD-DN.
- Log on to Contact Center Manager Administration. For more information, see Logging in to Contact Center Manager Administration for Contact Center configuration on page 52.
- Open the Configuration component.

About this task

Configure and acquire an IVR ACD-DN to configure a queue to which voice-processing contacts are directed.

To include GIVE IVR elements in your scripts, you must configure IVR ACD-DNs.

IVR ACD-DNs do not apply if you configure a SIP-enabled server.

Procedure

1. In the left pane, expand the Contact Center Manager Server on which to configure the IVR ACD-DN.

2. Select the **IVR ACD-DNs** folder.

3. In the **IVR ACD-DNs** window, in the **Name** box, type the name of the IVR ACD-DN as you want it to appear in reports.

4. In the **Number** box, type the IVR ACD-DN number. This number must match the number configured on the PABX.

5. From the **Threshold Class** list, select the threshold class for the IVR ACD-DN.

6. Click any other row of the table to add the IVR ACD-DN.

   Not Acquired appears in the Status column.

7. Select the **Acquired?** check box for the IVR ACD-DN.

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

9. Click **Refresh Status** to view the current status.

Variable definitions

Name	Description
Name	The name assigned to the IVR ACD-DN. If you add an AAEP IVR ACD-DN, it must contain the AAEP_ prefix in its name. For example, AAEP_180000. Valid values: 30-character maximum (no special characters)
Number	The number of the IVR ACD-DN that is passed to the Avaya Communication Server 1000 PABX to acquire or deacquire the IVR ACD-DN. You cannot change an IVR ACD-DN number once you save it. You must delete the IVR ACD-DN number and then recreate it. **❗ Important:** Be careful to include only IVR ACD-DNs in this list. Including agent ACD-DNs in this list causes issues with the provision of IVR treatments. Valid values: 7-digit maximum
Threshold Class	The name of the threshold class assigned to this IVR ACD-DN. Valid values: 30-character maximum (no spaces or special characters)
Acquired?	Select the Acquired? check box to acquire the IVR ACD-DN. Clear the Acquired? check box to deacquire the IVR ACD-DN. After you select or clear the Acquired? check box, click Refresh Status to refresh the Status box.
Status	The status of the acquisition of the IVR ACD-DN. Valid values: Not Acquired, Acquire Pending, Acquired, Acquire Failed, Deacquire Failed, and Deacquire Pending

Table continues…

Name	Description
Refresh Status	Refresh the status of the resources that you acquire or deacquire. The current status appears in the Status column.

Chapter 18: Media servers

Avaya Aura® Contact Center supports the following media servers:

- Avaya Aura® Media Server
- Avaya Experience Portal

A SIP-enabled Contact Center requires one or more Avaya Aura® Media Servers. Avaya Experience Portal is an optional media server used to process external Interactive Voice Response (IVR) dialogs.

Adding a media server

Before you begin

- Log on to Contact Center Manager Administration (CCMA). For more information, see [Logging in to Contact Center Manager Administration for Contact Center configuration](#) on page 52.
- Open the Configuration component.

About this task

Add an Avaya Aura® Media Server or Avaya Experience Portal media server to Contact Center. Contact Center uses Avaya Aura® Media Server to provide default media and conference services. Contact Center uses Avaya Experience Portal to support external Interactive Voice Response (IVR) dialogs.

To configure prompts in the Prompt Management component, you must associate an existing CCMS server with the Avaya Aura® MS server.

> ✳️ **Note:**
>
> Ensure that the CCMA server has been added as a trusted node in Element Manager in order to manage media server prompts.

Procedure

1. In the left pane, expand the server to which to add a Media Server.

   The server expands to show its resources.

2. Select the **Media Servers** folder.

3. In the right pane, in the **Server Name** box, type the Avaya Aura® MS name.

Avaya recommends that you use the Avaya Aura® MS network name for Contact Center Manager Administration as the trusted host name (AMS server name or AMS FQDN name). The trusted host name is the Avaya Aura® Media Server name or Avaya Aura® Media Server FQDN name that is used to sign the certificate.

> ✳ **Note:**
>
> If you are using the Avaya Aura® Media Server HA feature enter the AMS managed name (short name or FQDN name) already signed in the certificate.

4. In the **IP address** box, type the IP address of the Avaya Aura® MS or Avaya Experience Portal server.

5. In the **Port Number** box, type the port number for the Avaya Aura® MS server. The default port number is 5060.

6. Select the **Master Content Store** check box for the Avaya Aura® MS server that manages prompts.

   Master Content Store is the Avaya Aura® MS server that manages the prompts.

   > ✳ **Note:**
   >
   > You can select the **Master Content Store** check box for only one media server. If you try to select the **Master Content Store** check box for another media server, the system displays a warning message.

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

8. From the **Transport** drop-down list, select the transport type for Avaya Aura® MS.

   Select **TCP**, **TLS**, or **UDP**.

9. Click **Update Transport**.

   This updates the transport type for all media servers.

Chapter 19: Media services and routes

In the Media Services and Routes window, you can configure the media services to which calls are routed from within a script to receive media treatments. The Media Services and Routes window applies only to SIP-enabled contact centers. Media services are treated as SIP addresses.

The contact center invokes the following media services throughout the lifetime of a call:

- Conversation Space service
- Treatments service
- Announcements service for recorded announcements (RAN)
- Announcements service for music (supports audio-only files)
- Interactive Voice Response (IVR) service
- Multimedia treatments service
- External dialog media server

Each media service has a unique SIP address.

Adding a media service

Before you begin

- Log on to Contact Center Manager Administration. For more information, see Logging in to Contact Center Manager Administration for Contact Center configuration on page 52.
- Open the Configuration component.
- Add a media server. See Adding a media server on page 114.

About this task

Configure each Avaya Aura® Media Server in the Contact Center solution as a media server and assign it to provide ACC_APP_ID media services.

Configure each Avaya Experience Portal in the Contact Center solution as a media server and assign it to provide XDIALOG media services.

Note that you cannot modify or delete the following default Media Services:

- ACC_APP_ID (service for conference)

Procedure

1. In the left pane, select the SIP-enabled server on which to add the Media Server.

   The server expands to show its resources.

2. Select the **Media Services and Routes** folder.

3. In the right pane, in the **Service Name** box, type a name for the media service.

4. In the **Treatment Address** box, type a treatment address.

5. Click any other row in the table to save the changes.

6. Once you add a ACC_APP_ID Media Services and Routes specification for a particular Media Server, and if you are using WebLM, you must restart Contact Center License Manager to ensure that Contact Center License Manager pushes the required license to the current Avaya Aura® Media Server.

Variable definitions

Name	Description
Service Name	The name for the media service. There are three standard Media Services: dialog, announcement and conference. You cannot delete these Media Services.
Treatment Address	The address for routing contacts to a particular treatment. The address can be up to 255 characters.
Available Media Servers	The list of Media Servers configured in the Media Servers window.
Selected Media Servers	A subset of the Media Servers configured previously. This is the list of servers that are considered in a routing decision.
Rank arrow	Use the Rank arrow buttons to change the order of the Media Servers.
Submit	Save your changes.

Associating routes to a media service

Before you begin

- Log on to Contact Center Manager Administration. For more information, see Logging in to Contact Center Manager Administration for Contact Center configuration on page 52.

- Open the Configuration component.

- Add an Avaya Aura® Media Server (route). See Adding a media server on page 114.

About this task

Complete this procedure to associate a route to a media service.

Procedure

1. In the left pane, select a SIP-enabled server.

   The server expands to show its resources.

2. Select the **Media Services and Routes** folder.

3. On the **Media Services & Routes** table, select a media service.

4. From the **Available Media Servers** list, select a route to associate with the selected media service.

5. To associate a media service with the proxy address, select the **Use Proxy Server** check box and proceed to .

6. Click the right arrow (**>**).

   The route moves to the Selected Media Servers list.

7. To select all Avaya Aura® Media Servers from the **Available Media Servers** list, click the double right arrow (**>>**).

8. Repeat to until you select all of the routes to associate with the selected media service.

9. Use the up and down **Rank** arrows to order the selected routes.

Removing routes from a media service

Before you begin

- Log on to Contact Center Manager Administration. For more information, see .

- Open the Configuration component.

About this task

Complete this procedure to remove routes from a media service.

Procedure

1. In the left pane, expand the SIP-enabled server from which to remove a route from a media service.

   The server expands to show its resources.

2. Select the **Media Services and Routes** folder.

3. On the **Media Services & Routes** table, select a media service.

The Avaya Aura® Media Servers associated with that media service appear in the Selected Media Servers list.

4. Click the left arrow (**<**).

   The route moves to the Available Media Servers list.

5. To select all Media Servers from the **Selected Media Servers** list, click the double left arrow (**<<**).

Deleting a media service

Before you begin

- Log on to Contact Center Manager Administration. For more information, see Logging in to Contact Center Manager Administration for Contact Center configuration on page 52.

- Open the Configuration component.

- Remove any routes associated to the media service. See Removing routes from a media service on page 118.

About this task

Complete this procedure to delete a media service.

Procedure

1. In the left pane, select the SIP-enabled Contact Center Manager Server on which to delete the media service.

2. Select the **Media Services and Routes** folder.

3. In the right pane, select the media service to delete.

4. Press **Delete**.

5. In the message box that appears asking you to confirm your choice, click **OK**.

Chapter 20: Multiplicity presentation classes

A multiplicity presentation class is a collection of preferences that determines the number and types of contacts that Contact Center presents to a multiplicity-enabled agent. A multiplicity presentation class specifies the minimum time between contacts being presented on Agent Desktop, the skillsets or types of Multimedia contacts, and the number of concurrent contacts the agent can receive.

> **Note:**
>
> You cannot select Voice or Voice Mail contact types when creating a Multiplicity Presentation Class (MPC). By default, each MPC has one Voice and one Voice Mail contact type.

Creating a multiplicity presentation class

Before you begin

- Log on to Contact Center Manager Administration.
- Open the Configuration component.

About this task

Create a multiplicity presentation class (MPC) to determine how an agent using Agent Desktop can work with multiple contacts at one time. Use a multiplicity presentation class to specify the following:

- which contact types to present to the agents
- the maximum number of active contacts an agent has at one time by contact type or skillsets
- whether voice contacts can interrupt Multimedia contacts
- whether Multimedia contacts are presented while agent is on a voice call

Procedure

1. In the system tree, expand the server on which to add the multiplicity presentation class.

   The server shows its resources.

2. Select the **Multiplicity Presentation Classes** folder.

3. In the right pane, click **Create New**.

4. In the **Name** box, type the name of the new multiplicity presentation class.

5. From the **Value** list, select the maximum number of multimedia contacts that an agent using this MPC is allowed to have active at one time.

6. In the **Delay** box, type a delay in seconds that occurs between each contact presented to the agent.

7. To allow agents using this MPC to receive multimedia contacts while they are active on voice contacts, select **Agent will remain in a Ready state when a voice call is answered**.

8. To allow agents using this MPC to receive voice contacts while they have active multimedia contacts, select **Agent will remain in a Ready state when a multimedia contact is answered or presenting for more than 10 seconds**.

9. Select **Place active contact on hold when voice call becomes active** to set the active multimedia contact on hold when the agent accepts a presenting voice contact.

10. In the **Assigned Contact Types** list, use the **Value** list for each contact type to specify the maximum number of contacts from each contact type that the agent can have active at one time.

11. Click **Unassigned Skillsets**.

12. Use the **Skillset name** search fields to search for a specific list of skillsets, or click **List All** to list all the skillsets configured in the Contact Center.

13. Check the **Assign** check box for any skillset that you want to assign to this MPC. You can only assign skillsets if the corresponding contact type has a zero value in its **Value** list in **Assigned Contact Types**.

14. Click **Submit**.

    The skillset becomes available in the Assigned Skillsets list, with the default value of 1.

15. In the **Assigned Skillsets** list, use the **Value** list for each skillset to specify the maximum number of contacts from that skillset that the agent can have active at one time.

16. Click **Submit** to submit your changes and to save the multiplicity call presentation class.

Variable definitions

Name	Description
Name	The name assigned to the multiplicity presentation class. Valid value: 30-character maximum

Table continues…

Name	Description
Value	Select the maximum number of multimedia contacts that an agent can keep active at one time on Agent Desktop. When the agent reaches this limit, the Contact Center does not present any more multimedia contacts to the agent until the agent closes a multimedia contact.
Delay	The time that the Contact Center waits between sending contacts to the agent. This prevents the agent from receiving multiple simultaneous contacts. If an agent configured with this MPC also has a call presentation class with a value for After Call Break for N Seconds, Contact Center Manager Server uses the greater of the two values between contacts. Valid values: 10-300 (seconds)
Agent will remain in a Ready state when a voice call is answered	Select to allow the agent to receive multimedia contacts while they are on a voice call.
Agent will remain in a Ready state when a multimedia contact is answered or presenting for more than 10 seconds	Select to allow the agent to receive a voice call while they are working on a Multimedia contact.
Place active contact on hold when voice call becomes active	Select to set the active multimedia contact on hold when the agent accepts a presenting voice call, allowing the agent to focus on the voice contact.
Assigned Contact Types	List the contact types that you can include in the multiplicity presentation class.
Assigned Contact Types–Value	Select the maximum number of contacts of this contact type that the agent can have active on Agent Desktop. These lists automatically have a maximum value equal to the number set in the Value field. The cumulative total of the values you select for all contact types does not impact the overall maximum number of contacts as set in the Value field.
Assigned Skillsets	Display skillsets selected for this multiplicity presentation class.

Table continues…

Name	Description
Assigned Skillsets –Value	Select the maximum number of contacts from this skillset that the agent can have active on Agent Desktop. These lists automatically have a maximum value equal to the number set in the Value field. The cumulative total of the values you select for all contact types does not impact the overall maximum number of contacts as set in the Value field.
Unassigned Skillsets	Allows you to search for and select skillsets to assign to this multiplicity presentation class. You can select skillsets only if there is a zero value for their corresponding contact type in the Assigned Contact Types list. The skillsets you select appear in the Assigned Skillset list when you click Submit.
Skillset name	The drop down list allows you to specify a search option. The text box allows you to specify the text for which to search the CCMS skillsets.
Search	Initiate a search of the CCMS skillset list using the criteria in the Skillset Name fields. Matching skillsets display in a list below. You can only select skillsets if there is a zero value for their corresponding contact type in the Assigned Contact Types list.
List All	Display the complete CCMS skillset list. You can only select skillsets if there is a zero value for their corresponding contact type in the Assigned Contact Types list.
Delete	Delete the selected multiplicity presentation class. You can delete only an updated or completed multiplicity presentation class.
Create New	Create a new multiplicity presentation class.
Submit	Save changes to the selected multiplicity presentation class.

Deleting a multiplicity presentation class

Before you begin

- Log on to Contact Center Manager Administration.

- Open the Configuration component.
- Ensure that the multiplicity presentation class is not assigned to an agent.

About this task

Delete a multiplicity presentation class that is no longer required to save room in your database.

Procedure

1. In the left pane, expand the server from which to delete the multiplicity presentation class.

2. Select the **Multiplicity Presentation Classes** folder.

3. In the right pane, in the **MPC List** list, select the multiplicity presentation class to delete.

4. Press **Delete**.

5. On the **Confirm Delete** message box, click **Yes** to delete the multiplicity presentation class.

Chapter 21: Networking communication parameters

In the Networking Communication Parameters window, you can view or modify the networking communication parameters for any site in the network. You must configure the following network communication parameters on each server in the network:

- the number that your PABX dials to route a contact to that server
- the number of times your server tries to queue contacts to the site after a route attempt fails, and the number of seconds between retries
- the duration for which an agent at the site is reserved to answer a contact routed from your server
- the amount of time your server waits for a reply from the remote sites, if routing is based on longest idle agent or average speed of answer
- the Landing Pad type, if the server has Universal Networking enabled

For more information about configuring networking communication parameters, see *Avaya Aura® Contact Center Server Administration*.

Chapter 22: Phoneset displays

You can customize the phone LCD displays so that all phones of a specific type display information the same way. For example, if you configure the display for a 1 × 16 alphanumeric phone, then all phones of that type use the same custom display.

You can create custom labels that help define the information appearing on the phone display. For example, if you customize the phone display by making the skillset name appear you can create a custom label called SKILLSET, and place the label on the display directly before the skillset name field.

The Phoneset displays feature is not supported on a SIP-enabled Contact Center. You cannot configure display information such as the agent skillset on a phone in a SIP Contact Center configuration. You can display the skillset name on the Agent Desktop.

Configuring a phone display

Before you begin

- Configure the phone type on the Avaya Communication Server 1000 PABX.

- Log on to Contact Center Manager Administration. For more information, see Logging in to Contact Center Manager Administration for Contact Center configuration on page 52.

- Open the Configuration component.

About this task

Configure a phone display to customize the LCD displays on phones.

Procedure

1. In the left pane, expand the Contact Center Manager Server on which to configure a phone display.

2. Select the **Phoneset Displays** folder.

3. In the right pane, select the phone type to configure.

4. Use a drag-and-drop action to move the configuration labels to the desired place in the row at the bottom of the window.

5. If you want to create a custom label to appear on the phone display before the configuration label, in the **Label** box, type a name for the label (for example, SKILLSET).

> ❗ **Important:**
>
> Label names cannot contain special characters.

6. Click the pencil and paper icon beside the label box to generate the label.

   The custom label appears above the Label box.

7. Use a drag-and-drop action to move the custom label to the desired place in the display row at the bottom of the window.

   > ❗ **Important:**
   >
   > If your custom label is too long for the display, you cannot place it in the display row. In this case, click in the Label box and retype the label. Click the pencil and paper icon again to update your custom label. Use a drag-and-drop action to move the new label to the desired place in the display row at the bottom of the window.

8. Drag the corresponding configuration label (for example, the skillset label) and drop it in the display row directly after the custom label.

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

Chapter 23: Phonesets and voice ports

In the Phonesets and Voice Ports window, you can add and acquire each phone that an agent or supervisor uses to log on to the system. After Contact Center Manager Server acquires a phone, the Avaya Communication Server 1000 PABX sends messages about the phone to the system.

The following phoneset information applies to the CS1000 PABX only. Phonesets and voice ports do not apply when you configure a SIP server.

Only supervisors are associated with a specific phone. Agents are dynamically assigned a position ID, while supervisors are associated with a specific phone and position ID.

Configuring and acquiring a phone or voice port

Before you begin

- Configure the phone on the PABX.

- Log on to Contact Center Manager Administration. For more information, see Logging in to Contact Center Manager Administration for Contact Center configuration on page 52.

- Open the Configuration component.

About this task

Configure and acquire each phone that an agent or supervisor uses to log on to the system.

You cannot modify a saved phone or voice port. You can delete a saved phone or voice port and you can add a new phone or voice port. For example, you cannot change a voice port to a phone, or a phone to a voice port. You must delete the voice port or phone and add a new phone or voice port.

Procedure

1. In the left pane, expand the Contact Center Manager Server to which to add the phone or voice port.

2. Select the **Phonesets and Voice Ports** folder.

3. In the right pane, in the **Name** box, type the name of the phone or voice port as you want it to appear in reports.

4. From the **Type** list, select the one of the following terminal types:

   - Voice Port

- Not Voice Port

5. In the **Address** box, type the address of the phone or the voice port on the telephony server.

   🛈 **Important:**

   You must delete the leading zeros or the TN acquire fails.

6. For access voice ports only, in the **Channel** box, type the channel number.

7. Click any other row of the table to add the phone or the voice port.

   Not Acquired appears in the Status column.

8. Select the **Acquired?** check box.

9. Click any other row in the table to acquire or deacquire the phone or voice port.

10. Click **Refresh Status** to view the current status.

Variable definitions

Name	Description
Name	The name assigned to the phone or voice port. Valid values: 30-character maximum (no special characters)
Type	The terminal type. Valid values: • Voice Port—for voice services only (for example, Avaya CallPilot™ Voice Ports). Users are logged in automatically. • Not Voice Port—are actual phones that the agent or supervisor logs into. After the system acquires a non-voice port, the value in this box automatically changes to either Agent, Supervisor, or Error, based on the port address you enter for the phone. If an agent logs on to the port address, then the Type is Agent. Likewise, if a supervisor logs on to the port address, the Type is Supervisor. If the Type is Error, then the submitted port address does not exist on the server. 🛈 **Important:** You cannot change the voice port type after you configure it. To change the voice port type, you must delete the corresponding phone and create a new voice port, or delete the voice port and create a new phone.

Table continues…

Name	Description
Address	The address of the voice port or phone on the telephony server. Valid values: Loop, Shelf, Card, Unit (for example, 4-0-0-1)
Channel	The channel number of the access voice port. This number must match the Class number shown in the Channel Allocation Table window of the Avaya CallPilot™ system, where the access port is defined. For non-access voice ports, this box is blank. Valid range: 0–8999 Valid value: 4-digit maximum **Important:** You cannot change the voice port channel after the voice port has been configured. To change the voice port channel, you must delete the corresponding phone, create a new phone (as a voice port), and configure the voice port with the correct channel number.
IVR Name	The IVR queue associated with the voice port. Valid values: read-only box
Acquired?	Select the Acquired? check box to acquire phone or voice port. Clear the Acquired? check box to deacquire the phone or voice port. After you select or clear the Acquired? check box, click Refresh Status to refresh the Status box.
Status	The status of the acquisition of the phone/voice port. Valid values: Not Acquired, Acquire Pending, Acquired, Acquire Failed, Deacquire Failed, and Deacquire Pending
Refresh Status	Refresh the status of the resources that you acquire or deacquire. The current status appears in the Status column.

Chapter 24: Real-time statistics

The Contact Center Manager Administration Real-Time Reporting displays provide up-to-date statistics for your Contact Center and its resources. With access to statistics that update in real time, such as the number of contacts waiting to be answered, the number of agents assigned to each skillset, and the number of abandoned calls, you can view changes in contact activity as they occur.

To use the Real-Time Reporting feature, you must first configure Contact Center Manager Server to collect the types of statistics to see in the Real-Time Reporting displays. You can configure the following seven types of real-time statistics:

- skillset statistics (mandatory)
- nodal statistics (mandatory)
- application statistics
- IVR statistics
- route statistics
- agent statistics
- network statistics

For each type of real-time statistics you must indicate the viewing mode (moving window or interval-to-date). The interval-to-date settings that you choose start immediately and apply to all real-time displays at all sites on your network that use the interval-to-date mode.

For more information about the Real-Time Reporting feature, see *Using Avaya Aura® Contact Center Reports and Displays*.

Configuring real-time statistics collection

Before you begin

- Log on to Contact Center Manager Administration.
- Open the Configuration component.

About this task

Configure real-time statistics collection to provide information for real-time displays with access to statistics that update in real time. You can configure the following types of real-time statistics:

- skillset statistics (mandatory)
- nodal statistics (mandatory)
- application statistics
- IVR statistics
- route statistics
- agent statistics
- network statistics

For each of these real-time statistics, you must indicate the viewing mode (moving window or interval-to-date). The interval-to-date settings that you choose start immediately and apply to all real-time displays at all sites on your network that use the interval-to-date mode.

When you configure the interval-to-date real time statistics display, there are two required fields: Data Collection Interval and One of the intervals starts at.

The interval statistics reset after the Data Collection Interval. The One of the intervals starts at option is used to synchronize the initial interval. For example, if you configure the real-time data at 1 p.m. on April 2, and the Data Collection Interval is 15 hours, and the One of the intervals starts at 8 a.m., the real time statistics are reset and the system starts collecting interval data at 11 p. m. (08:00 + 15:00). The statistics are next reset at 2 p.m. (15 hours later) on April 3. The statistics do not reset at 8 a.m. on April 3 unless you designate an appropriate interval.

Procedure

1. In the left pane, expand the server on which to configure the real-time statistics.

2. Click the **Real-time Statistics** folder.

3. In the right pane, select the viewing mode for the following statistics:

   - Skillset Statistics—You must select a viewing mode value for this statistic. The system automatically collects this statistic because it is required for intrinsics in writing scripts.

   - Nodal—You must select a viewing mode for this statistic. The system automatically collects this statistic because it is required for intrinsics in writing scripts.

   - Application Statistics—Optional

   - IVR Statistics—Optional

   - Route Statistics—Optional

   - Agent Statistics—Optional

   - Network Statistics—Optional

4. In the **Data Collection Interval** boxes, type the interval duration to use in the interval-to-date data collection mode.

5. In the **One of the intervals starts at** box, type the start time for statistics collection in the interval-to-date collection mode.

The system calculates and synchronizes the days remaining intervals based on the time that you specify. Your changes take effect immediately.

6. Under **Minimum Refresh rates**, in the **Agent Real-time Displays** box, type the minimum refresh rate in seconds for Agent Real-time Displays.

7. In the **Other Real-time Displays** box, type the minimum refresh rate in seconds for all other Real-time Displays.

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

Chapter 25: Routes

Routes defined in Contact Center Manager Administration differ depending on the type of PABX with which Contact Center integrates.

On a SIP-enabled Contact Center, a route links announcements and music provided by Avaya Aura® Media Server to the RAN block configured in an Orchestration Designer (OD) flow application or script.

The Route Name is a string that must be identical to the announcement (WAV) file name or music content group (for example, classical, jazz, easy listening) stored on Avaya Aura® Media Server. For announcements the Route Name must be identical to the announcement (WAV) file name under the locale content group on Avaya Aura® Media Server. For streaming music, the Route Name must match the Stream Key configured on Avaya Aura® Media Server.

The OD flow application uses the Route Number mapping to invoke this file for playback. This configuration allows the announcement file name and music content group to appear on the generated RAN and MUSIC reports.

On a legacy AML-based PABX, a route defines a group of trunks. Each trunk carries either incoming or outgoing calls to the PABX. To create All Trunks Busy (ATB) reports, you must acquire at least one route. Before you can create a route, you must configure it on the Avaya Communication Server 1000, and add the threshold class that is assigned to it in Contact Center Manager Server.

Configuring routes

Before you begin

- Ensure that you are connected to a PABX.
- If using AML, configure the route on the PABX.
- Log on to Contact Center Manager Administration. For more information, see Logging in to Contact Center Manager Administration for Contact Center configuration on page 52.
- Open the Configuration component.

About this task

Use this procedure to:

- Create Recorded Announcement (RAN) routes for SIP-enabled Contact Centers.
- Configure and acquire routes to define groups of trunks that carry either incoming or outgoing contacts to an AML-based Avaya Communication Server 1000 PABX.

On a SIP-enabled Contact Center, the Route Name must be identical to the announcement file name or music content group configured on the Avaya Aura® Media Server. For streaming music, the Route Name must match the Stream Key configured on Avaya Aura® Media Server. The Route Number can be arbitrary (though it must be unique) and the RAN or MUSIC block in Orchestration Designer uses this number to identify the file to play. See *Using Contact Center Orchestration Designer*.

You cannot modify a saved route. You can delete a saved route and add a new route.

Procedure

1. In the left pane, expand the server to which to add the route.

2. Select the **Routes** folder.

3. In the right pane, in the **Name** box, type the name of the route.

4. In the **Number** box, type the route number. For an AML-based PABX, this number must match the number configured on the PABX.

5. From the **Threshold Class** list, select the threshold class assigned to this route.

6. Click any other row of the table to add the route.

Variable definitions

Name	Description
Name	The name assigned to the route.
	On a SIP-enabled Contact Center, the Route Name is a string which must be identical to the announcement filename or music content group configured on Avaya Aura® Media Server.
	For announcements the Route Name must be identical to the announcement (WAV) file name under the locale content group on Avaya Aura® Media Server.
	For streaming music, the Route Name must match the Stream Key configured on Avaya Aura® Media Server.
	Valid value: 30-character maximum (no special characters)

Table continues…

Routes

Name	Description
Number	The number of the route. You cannot change a route number once you save it; you can only delete it and create a new one.
	On a SIP-enabled Contact Center the value is arbitrary but must be unique.
	On a legacy AML-enabled Contact Center the route must match the route number configured on the PABX.
	Valid value: 3-digit maximum; External route: 1–511
Threshold Class	The name of the threshold class assigned to this route.
	Valid values: 30-character maximum (no spaces or special characters)
Refresh Status	Refresh the status of the resources that you acquire or deacquire. The current status appears in the Status column.

Chapter 26: Skillsets

A skillset is a group of abilities necessary to answer a specific type of contact. Skillsets are the basic building blocks of skill-based routing.

Skill-based routing

Skill-based routing uses skillsets to match callers with the agents who can best meet their needs.

Out of service skillsets

Skillsets automatically go out of service when all agents log off, or when a supervisor or an administrator changes the Out Of Service Mode in the Skillsets window of the Configuration component.

Two out of service modes are available:

- Transition mode: Transition mode means that agents can answer queued contacts but the skillset accepts no new incoming contacts. New contacts receive night service treatments defined in the script or the default skillset. You must initiate Transition mode manually by selecting Transition from the Out of Service Mode list in the Skillset window of the Configuration component. After all existing queued contacts for a skillset in Transition mode are answered or abandoned, the skillset automatically enters into Night mode. A skillset manually placed in Transition mode that goes into Night mode remains in this state until it is cancelled by selecting N/A from the Out of Service Mode list.

- Night mode: Night mode means that the agents in a particular skillset no longer answer queued contacts and the skillset accepts no new contacts. New contacts or queued contacts receive treatments defined in the script or the default skillset. You can initiate Night mode manually in the Skillset window of the Configuration component, or automatically if all agents belonging to that skillset log off. When you manually place a skillset in Night mode, the skillset remains in this state until you cancel the state by selecting N/A from the Out of Service Mode list in the Skillset window of the Configuration component. Canceling Night mode returns the skillset to In-service mode.

Contacts in queue

Contact Center Manager Server must determine the following to present contacts:

- If multiple agents are available, to which agent does it present the contact?
- If multiple contacts are waiting, which contact does it present first?

Agent selection

If two agents are available to answer an incoming contact, Contact Center Manager Server presents the contact to the agent with the highest priority level for the skillset to which the contact is queued. A supervisor bases the priority level of a skillset on the agent's skill level for that particular skillset. You typically assign a higher priority level to a skillset assigned to an agent with a higher skill level, and assign a lower priority level to a skillset assigned to an agent with a lower skill level. Priority levels range from 1 to 48, with 1 being the highest priority.

To use the enhanced Service Level Routing and Service Level Management, you can set a target service level and assign a standby priority to an agent. When the target service level is achieved, an agent with the highest standby priority is able to handle the contact. Standby priority levels range from 1 to 48, with 1 being the highest priority.

If more than one agent has the same priority, the server presents the contact to an agent based on the Agent Order Preference idle time setting. Your administrator can configure the Agent Order Preference setting in the Global Settings area of the Configuration component of Contact Center Manager Server to base idle time on one of the following:

- longest total time in Idle state since logon
- longest time in Idle state since last status change
- longest total time since last CDN/ACD call or contact

Contact selection

If two contacts are waiting in a skillset queue when an agent for that skillset becomes available, Contact Center Manager Server uses the following criteria (in the order shown) to determine which contact to present first:

- Call priority—This is a numeric value assigned in a script that defines the relative importance of a contact. All priority 1 contacts are always answered before contacts of priority 2 or greater.
- Call source preference (networking environment only)—The server determines the presentation order of contacts within the same priority by first checking the call source preference, and then checking the call age preference. The administrator determines which contacts—local or network—receive preference, or the administrator can choose not to

prioritize contacts based on source. If the administrator sets the call source preference to none, the server does not consider the call source when presenting contacts and, instead, passes directly to the call age preference.

- Call age preference—The administrator specifies incoming contact position in the pending request queue based on the age of the contact. For each skillset, the administrator can specify Oldest or First in Queue as the call age preference. The two age preferences differ as follows:

  - Oldest—Each contact enters the queue according to the time elapsed since entering the Master script for Contact Center Manager Administration. When the contact enters the pending request queue, the time associated with the age of the contact starts when the contact enters the Master script. The older the contact is, the further toward the front of the queue the contact is inserted. The system orders queue requests in a front-to-back sequence.

  - First in Queue—Represents the age of the contact since it was queued to the skillset. For First in Queue order, the contact enters at the back of the queue, regardless of its age relation to other contacts. For example, if a contact was queued 10 seconds ago, its First in Queue age is 10 seconds. Any contact entering the queue after this contact enters at the back of the queue and is considered the youngest contact in the queue. The time associated with the age of the contact starts when it enters the pending request queue.

Example

The following example outlines how Contact Center Manager Server uses a combination of call priority, call source preference, and call age preference to present calls in the queue to agents.

In this example, the call source preference is network. Three contacts are waiting in the queue:

- A priority 2 local contact waiting in the queue for 1 minute
- A priority 3 local contact waiting in the queue for 3 minutes
- A priority 3 network contact waiting in the queue for 2 minutes

Because call priority is the first consideration when routing contacts, Contact Center Manager Server presents the priority 2 contact first, even though it was in the queue for the least amount of time.

Then, because call source preference is the second consideration when routing contacts, the server presents the network priority 3 contact next, even though it was in the queue for less time than the local priority 3 contact. Finally, the server presents the local priority 3 contact.

If the administrator does not set the call source preference, the only two criteria for routing contacts are call priority and call age preference. Therefore, in this example, the priority 2 contact is presented first, followed by the priority 3 local contact that was in the queue for 3 minutes, and lastly the priority 3 network contact that waits for 2 minutes.

To queue to a default skillset

Your administrator can define a default skillset. Any contacts not queued by the end of script execution automatically queue to this skillset.

In the Avaya Communication Server 1000 PABX environment, your administrator can create a separate default skillset for each media type. For example, Best Air defined Bookings as the default voice skillset. Voice contacts not queued by the end of the script execution are presented to agents assigned to the Bookings skillset.

Activity codes

Agents can assign activity codes to the contacts they answer. The system uses activity codes to track the amount of time spent on the various types of incoming contacts. To generate reports with meaningful activity code names, the administrator must define these activity codes in Contact Center Manager Administration.

Global settings properties

Your administrator defines global properties for your system in the Global Settings window of the Configuration component. The global skillset properties that the administrator defines apply to all skillsets defined on your Contact Center Manager Server. These properties include:

- recorded announcement (RAN) route
- agent order preference

On a networked Contact Center, if the default skillset is a network skillset, contacts not queued by the end of script execution are queued to this skillset on the local server.

Adding a local skillset

Before you begin

- Log on to Contact Center Manager Administration. For more information, see Logging in to Contact Center Manager Administration for Contact Center configuration on page 52.
- Open the Configuration component.
- Define the activity code to be assigned as the default activity code for the skillset if you do not want to use system-defined default.
- Define the ACD-DN on the PABX to which contacts for this skillset are directed if the system is not available.
- Define the threshold class to assign to this skillset if you do not want to use the default threshold class.
- Define the contact type to assign to a skillset if you do not want to use the default contact types. This is applicable only if Open Queue is enabled on the Contact Center Manager Server.

About this task

A skillset is the ability or group of abilities necessary to answer a specific type of contact. Skillsets are the basic building blocks of skill-based routing. Skillsets are used to match callers with the agents who can best meet the callers' needs.

If you want to add one or more skillsets quickly, you can use the Contact Center Management component. If you have sufficient access levels, in the left pane you can right-click a server to which to add the skillset and click **Add Skillset**. Specify the **Contact Type** and **Skillset Name**. However, to add all the other attributes of the skillset, you must edit the skillset as outlined in this procedure.

Procedure

1. In the left pane, expand the server to which to add the skillset.

2. Select the **Skillsets** folder.

3. If you are on an Open Queue-enabled server, you can assign a contact type to the skillset. Select a value from the **Contact Type** drop-down list. CCMA automatically populates the **Prefix** field with the appropriate skillset name prefix. If you do not select a type, the skillset defaults to the Voice type.

4. In the **Skillset Name** box, type a name for the skillset.

   ✳ **Note:**

   The maximum length of a skillset name allowed, including the prefix, is 30 characters. The name must not have a numeral as the first character, and not use spaces, special characters, or languages other than English. While skillsets and applications can share the same name without affecting pegging, to help distinguish skillset names from application names, you can add _SK to the end of the name. For example, Sales_SK or Service_SK.

5. From the **Default Activity Code** list, select the activity code that is registered whenever this skillset is used.

6. From the **Threshold Class** list, select the threshold class associated with this skillset.

7. From the **Call Age Preference** list, select the method to configure the order of contacts in the queue. If you want priority given to the oldest contact in the system, select **Oldest**. If you want to give priority to the first contact in the queue, select **First In Queue**.

8. Optionally, in the **Map To ACD-DN** box, type the ACD-DN number to which the skillset can map.

   If you map the skillset to an ACD-DN, calls to that ACD-DN are pegged against the skillset in reports.

9. From the **Out Of Service Mode** list, select a value to take the skillset offline and specify the service mode for the manual night service PABX.

10. Optionally, if you want to enable Service Level Routing, Service Level Management enhancement or both, perform steps 10 and 11 otherwise skip to step 12.

11. In the **Target Service level** field, enter target service level threshold value.

12. Select the **Service Level Routing** check box.

    You can enable Service Level Routing enhancement by selecting the Service Level Routing check box and setting a valid Target Service Level value.

    🛈 **Important:**

    At least one agent within the range of normal priorities and one agent within the range of standby priorities must be assigned to the skillset in order to enable Service Level Management enhancement.

13. Optionally, in the **Comment** box, type any comments you have about the skillset.

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

Chapter 27: Threshold classes

A threshold class is a set of options that determines how statistics are treated in reports and real-time displays. You must assign an agent threshold class to each agent; you must assign a skillset threshold class to each skillset.

Because you can define multiple threshold classes of each type, you can treat statistics differently for different agents and skillsets.

- Display thresholds
- Pegging thresholds

Display thresholds

A display threshold is used in real-time displays to determine the lower and upper end of the normal range for a statistic. In your real-time display, you can assign different colors for statistics below the normal range, in the normal range, or above the normal range.

Pegging thresholds

Pegging thresholds are used to define a cut-off value for a statistic such as Short Call, Delay Before Answer, or Abandon.

For example, you can set the Short Call length to 10 seconds in a skillset threshold class. If a contact to a skillset with that threshold class lasts less than 10 seconds while connected to an agent, the contact is pegged as a Short Call.

Creating a threshold class

Before you begin

⊘ **Important:**

Display thresholds apply to both nodal and network-consolidated real-time displays. Therefore, when you define threshold classes on multiple servers in a networked environment, consider making the values the same on each server. This way, when users launch network-consolidated real-time displays, the threshold conditions shown reflect uniform settings across all servers.

- You must define two values for display thresholds—the low end and the high end of the normal range.

- For pegging thresholds, define only the cut-off limit for statistics.

- Log on to Contact Center Manager Administration. For more information, see Logging in to Contact Center Manager Administration for Contact Center configuration on page 52.

- Open the Configuration component.

About this task

Create a threshold class to specify how statistics are treated in reports and real-time displays. You can create threshold classes to distinguish between types of information that the system collects.

For example, you can create different agent threshold classes for customer service trainees and for senior customer service representatives. You can also create different skillset threshold classes for weekday performance and weekend performance.

Procedure

1. In the left pane, expand the server on which to create the threshold class.

2. Select the **Threshold Classes** folder.

3. In the right pane, in the **Name** box, type the name of the new threshold class.

4. From the **Type** list, select the threshold class type.

5. Click any other row in the grid to update the table and submit the threshold class name.

   The Thresholds table appears in the right pane.

6. In the **Enabled** box of the **Thresholds** table, select the check box for each statistic for which to define thresholds.

7. In the **Level 1** box, type the value for the low end of the normal range for display thresholds.

8. For display thresholds only, in the **Level 2** box, type the value for the high end of the normal range.

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

Avaya Aura® Contact Center Client Administration

Variable definitions

Name	Description
Level 1	The low end of the normal range for display thresholds. For pegging thresholds, enter the cut-off value for this statistic.
	You must define the service level threshold for both Application and Skillset statistics. However, the values for each type of statistic can be different.
	The Calls Answered After Threshold value for Skillset statistics is the number of local and incoming network skillset calls answered after a delay greater than or equal to the service-level threshold for this skillset. Delays are calculated from the time the call is queued at the skillset to the time the call is answered.
Type	The type of threshold class that you can create depends on the type of PABX or server on which you create the threshold class.
	You can choose from Agent, Application, Skillset, IVR ACD-DN, and Route threshold classes.
	For a CS1000 switch, you can choose from Agent, Application, IVR ACD-DN, and Skillset threshold classes.
	For SIP servers you can choose from Agent, Application, Skillset, and Route threshold classes.

Chapter 28: Configuration Tool spreadsheet

Use the Configuration Tool spreadsheet to save time when configuring a new Contact Center. You can upload data that you want to transfer from the spreadsheet to Contact Center, and download data from Contact Center to the spreadsheet. Instead of entering data for each resource individually, you can simultaneously upload all configuration data that you entered in the spreadsheet. When you upload the data from the spreadsheet, you can choose to upload all configuration items at once or only a portion.

You normally only use the Configuration Tool to add or download data, but you can also use it to edit certain configuration details. For example, you can use the Configuration Tool to bulk change your agent account mappings. The Configuration Tool spreadsheet does not enable you to edit all fields on every tab. You must use the Configuration component in Contact Center Manager Administration to modify or delete data that cannot be edited in the Configuration Tool spreadsheet.

Prerequisites for Configuration Tool procedures

- Ensure that you are logged in to Contact Center Manager Administration as an administrator.

- You must have Microsoft Excel.

  Note that the procedures in this chapter are intended as a guideline, but the exact steps might vary depending on the version of Microsoft Excel you are using

Downloading the Configuration Tool spreadsheet

About this task

You can use the Configuration Tool spreadsheet to add configuration data for all resources at once. You must download the formatted Contact Center Manager Configuration Tool spreadsheet from the Configuration window.

> ⚠ **Important:**
>
> You cannot delete data in the Configuration Tool. If you need to delete data, use the Configuration component in Contact Center Manager Administration.

Procedure

1. From the Configuration component of Contact Center Manager Administration, click **Download** > **Configuration Tool**.

2. Click **Run**.

3. In the WinZip Self-Extractor window, do one of the following:

   • Click **Unzip** to extract the spreadsheet and its associated files to the default directory.

   • To navigate to another directory of your choice, click **Browse**.

   > ❗ **Important:**
   >
   > The validation template file and the Online Help file must be in the same folder as the spreadsheet. The naming convention for these files is `Consolidated_ConfigurationTool.chm` for Help files and `Consolidated_Validation.xml` for validation files.

4. Click **OK**.

Entering data in the Configuration Tool spreadsheet

About this task

You can enter Contact Center configuration data in the Configuration Tool spreadsheet and then transfer the data to Contact Center Manager Server. The spreadsheet includes a separate worksheet for each configuration item.

> ❗ **Important:**
>
> You must use the Configuration component in Contact Center Manager Administration to modify or delete data that cannot be edited in the Configuration Tool spreadsheet.

Before you begin

Download the Configuration Tool spreadsheet from Contact Center Manager Administration.

Procedure

1. Open the Configuration Tool spreadsheet.

2. If prompted, click **Enable Macros**.

3. Click the tab for the content you want to configure.

   For example, click the **Users** tab in the spreadsheet to configure user data.

4. Enter the configuration data.

5. **(Optional)** If you need help with entering data in the Configuration Tool spreadsheet:

   a. Place your cursor in the column heading to display a comment.

The comment indicates the types of values you can enter and whether the data is mandatory or optional.

   b. If you need more detailed information, click the **Add-ins** tab in the spreadsheet and then click **Configuration Tool Help**.

6. Save your entries.

Validating data in the Configuration Tool spreadsheet

About this task

To reduce upload time, the Configuration Tool spreadsheet includes a Validation feature. Use this feature to identify and correct any invalid entries you made in the spreadsheet before uploading data.

Before you begin

Enter data in the Configuration Tool spreadsheet.

Procedure

1. Open the Configuration Tool spreadsheet with the data you want to validate and enable macros if prompted.

2. Verify that the validation template file is in the same folder as the spreadsheet.

   If this file is not in the same folder, navigate to it and place a copy of it in the spreadsheet folder.

3. In the Configuration Tool spreadsheet, click the **Add-ins** tab.

4. Click **Data Validation**.

5. In the Data Validation - Configuration Tool window, select the data to validate.

   You can validate all the data you entered or a portion of it.

6. Click **OK**.

   The validation tool highlights incorrectly-formatted values and mandatory cells with missing information. An error message is displayed in any row containing an error.

Correcting invalid entries in the Configuration Tool spreadsheet

About this task

Invalid data entries in the Configuration Tool spreadsheet are identified during the data validation or upload process. You see an error message in the Status Message column in the row containing the invalid data. After you locate and correct the errors, validate the data again.

Before you begin

Validate the data entries in the Configuration Tool spreadsheet.

Procedure

1. In the Configuration Tool spreadsheet, click the tab containing the invalid configuration data.

2. In the **Status Message** column, locate the error message and the cells that contain errors.

   Cells containing errors are highlighted in yellow.

3. Enter the correct data.

4. Save the spreadsheet.

Uploading data from the Configuration Tool spreadsheet

About this task

After you enter and validate the Contact Center configuration data in the Configuration Tool spreadsheet, you can use the Upload feature in the spreadsheet to transfer data to Contact Center Manager Server.

The upload of existing and acquired resources reloads these resources in a Not Acquired state and they need to be acquired manually. You cannot add phones, voice ports, or IVR ACD-DNs to a SIP system.

Procedure

1. Open the Configuration Tool spreadsheet you want to upload and enable macros if prompted.

2. Verify that the validation template file is located in the same folder as the spreadsheet.

   If this file is not in the same folder, navigate to it and place a copy of it in the spreadsheet folder.

3. Click the **Add-ins** tab in the spreadsheet.

4. Click **Data Upload**.

5. Under **CCMA Server Login**, in the **Server Name** field, type the name or IP address of the Contact Center server.

6. Enter the Administrator user ID and password for Contact Center Manager Administration.

7. If security is enabled on the Contact Center server, click **Use SSL**.

8. Click **Login**.

   The Data Upload - Configuration Tool window is displayed,

9. From the **Available Servers** list, select the Contact Center server to which data will be uploaded.

10. Select the type of configuration data to upload.

11. Click **OK**.

    The system displays the **Upload Status - Configuration Tool** dialog box.

    As your data uploads, the upload status is displayed. The current status information lists the records that are read. After the upload process is complete, the summary status lists the data that was successfully uploaded, as well as any errors that occurred. If there are any errors, they are also displayed in the Status Message column of the spreadsheet.

Recording the upload results

About this task

Upload results are displayed as configuration data is uploaded from the Configuration Tool. To record the upload results for future reference, you can copy them to a text file and save the file on your computer.

Before you begin

Upload configuration data from the Configuration Tool spreadsheet to Contact Center Manager Server.

Procedure

1. In the Upload Status - Configuration Tool window, place your cursor in the **Summary Status** box.

2. Press `Ctrl+A` to select all the text

3. Press `Ctrl+C` to copy the selected text.

4. Open a text editor, such as Notepad, and paste the text you copied.

5. Save the file.

Downloading data to your Configuration Tool spreadsheet

About this task

You can transfer existing configuration data from the Contact Center server to the Configuration Tool spreadsheet.

About this task

Ensure that you know which Contact Center server has the data you want to download to the Configuration Tool spreadsheet.

Procedure

1. Open the Configuration Tool spreadsheet and enable macros if prompted.

2. Click the **Add-ins** tab in the spreadsheet.

3. Click **Data Download**.

4. If prompted, log in to Contact Center Manager Administration from the Configuration Tool spreadsheet:

   a. In the **Server Name** field, type the name or IP address of the Contact Center server.

   b. Enter the Administrator user ID and password for Contact Center Manager Administration.

   c. If security is enabled on the Contact Center server, click **Use SSL**.

   d. Click **Login**.

5. In the Data Download - Configuration Tool window, from the **Available Servers** list, select the Contact Center server from which to download data.

6. Select the type of data to download.

   If a user ID and password were not provided when the server was added to the system, you are prompted to enter this information in a login window

7. Click **OK**.

8. In the Save As window, type a name for the spreadsheet.

   > 🛈 **Important:**
   >
   > If you do not enter a different name for the spreadsheet, you overwrite the existing spreadsheet. If you do not want to change the spreadsheet name but want to maintain an archive of spreadsheets, save the spreadsheet in a different directory.

9. Navigate to the directory where the validation template file and the Online Help file are located.

   If you saved the new spreadsheet in a different folder, you must place a copy of the validation template file and the Online Help file in the same folder.

10. Click **Save**.

The system saves the current spreadsheet and opens the new one. The Download Status - Configuration Tool window is displayed. As your data is downloaded, the current status information lists the records that are being read. After the download process is complete, the summary status lists the data that was successfully downloaded, as well as any errors that occurred.

Part 2: Contact Center Management

Chapter 29: Contact Center Management fundamentals

Contact Center Management contains the following five main data views:

- Supervisors view
- Agents view
- Skillsets view
- Assignments view
- Network Agent Admin view

Based on your access class, you can use Contact Center Management to perform the following tasks:

- Add, edit, view, and delete users defined in Contact Center Manager Server (CCMS).
- Add agents to user-defined partitions.
- Add, edit, view, delete, and schedule agent to supervisor assignments.
- Add, edit, view, delete, and schedule agent to skillset assignments.

To add a CCMS user (agent, supervisor, or supervisor/agent), you must use the Contact Center Management component or the Configuration Tool spreadsheet in the Configuration component. Some CCMS users (supervisors and supervisor/agents) can also be Contact Center Manager Administration (CCMA) users and can have a CCMA user ID and password to access the CCMA client application; however, many CCMS users do not use CCMA.

Network Agent Admin view

You can use the Network Agent Admin view to search for agents by agent properties or by skillset assignment across multiple servers in the network. You can also view skillset assignments for each agent and modify skillset assignment priority levels for each agent.

To access the Network Agent Admin view and search for agents, you must assign the user access to the Network Agent Admin view and must assign the CCM access privilege. To view, search or modify skillset assignments or to view skillset assignment priorities, you must also grant the user Skillset Assignment access privileges.

XML automated assignments

The XML automated assignments feature includes a component service that can help you create or update multiple assignments simultaneously by parsing through agent-to-skillset and agent-to-supervisor assignment data in XML files that you create. After the service parses the data, it either creates a new assignment on the indicated server, or it updates an existing assignment (if the assignment name in the XML file matches an existing assignment name on the selected server in Contact Center Manager Server).

When you create the XML file, you can specify whether you want the service to create an immediate assignment or a scheduled assignment. If the service creates a new scheduled assignment, you must use the Contact Center Management component to manually schedule and activate the assignment; if the service updates an existing scheduled assignment, the schedule still applies and the assignment remains active. However, if you want the assignment to run only at the scheduled time, you must select the Schedule option in the XML file. If you choose the Execute Now option, the scheduled assignment runs twice: it runs immediately and at the scheduled time. If you do not include the <EXECUTENOW> field in your XML file, or if you type an invalid value in this field, the system defaults to scheduling the assignment, and you must use Contact Center Management to manually schedule the new assignment.

This feature does not include an interface for writing the XML files. You must create the files using a proprietary tool of your choice, and you must design the files based on the specifications in [Specifications for XML files](#) on page 158. For guidance on creating the XML files, you can view the sample files that are shipped with the Contact Center Manager Administration software. These files are on the Contact Center Manager Administration server in the folder <install drive>:\Avaya\Contact Center\Manager Administration\Server\XMLAssignments\Sample XML Files, where <install drive> is the drive on which you installed Contact Center Manager Administration.

Who uses this feature

The XML automated assignments feature provides an interface for third-party applications to issue scheduled or immediate assignments.

For example, you can use this feature in the following scenarios:

- An agent is assigned to three skillsets during normal traffic periods, but during busy hours, you can use the XML automated assignments feature to assign this agent to additional skillsets.

- An agent is in Standby mode for certain skillsets during non-peak times. However, during busy periods, you can use this feature to schedule an assignment that gives the agent a priority for these skillsets. You can run a second assignment later to put the agents into Standby mode again.

- An agent receives contacts in the morning; in the afternoon, the agent is in training, in meetings, or doing other work. You can use this feature to place these agents in Standby mode in the afternoon. You can also use this feature where agents handle voice calls in the morning, and then, in the afternoon, handle email or Web requests.

Before you can use the XML automated assignments feature, you must

- install it manually on the Contact Center Manager Administration server. To install the XML automated assignments feature, run the .msi file, located in <install drive>:\Avaya\Contact Center\Manager Administration\Apps\SupportUtil. For information about obtaining the XML Automated Assignment toolkit, contact a member of the Developer Program through the Contact Us link at www.avaya.com/developer. General information about the Developer Program, including an online membership application, is also available on this site.

- be familiar with creating XML files

  This feature does not include an interface for creating the XML files. However, it does include an XML Schema. The XML Schema file describes the format in which you must generate the files using the tool of your choice—either a Work Force Management (WFM) system or another third-party application—so that they can be interpreted by this feature. The file is called SWCXMLAssignments.xsd and is in the following folder on the Contact Center Manager Administration server: <install drive>:\Avaya\Contact Center\Manager Administration\Server\XMLAssignments, where <install drive> is the drive on which you installed Contact Center Manager Administration.

Example

Your contact center has 250 agents, each of whom rotates daily in free-seating mode within their team with the skillset changing according to the seat the agent occupies.

In this example, agent John Smith works with skillsets S1, S2, and S3. On Monday morning, John works in area 1 (dedicated to S1); in the afternoon, he works in area 2 (dedicated to S2); on Tuesday he works in area 3 (dedicated to S3).

You must create separate XML files—for agent-to-skillset and agent-to-supervisor assignments—that contain the assignment data for all 500 agents and their supervisors for each seat-rotation period. In this scenario, therefore, you create separate agent-to-skillset and agent-to-supervisor assignment files for the Monday morning period, new files for Monday afternoon, more files for Tuesday morning, and so on.

After you create the files and are satisfied that they conform to the standards listed in the section Specifications for XML files on page 158, you must copy them to the designated drop folder. When you place the files in this folder, the program automatically parses the assignment data and creates or updates the assignments for all 250 agents. If you create new scheduled assignments, you must use Contact Center Management to schedule and activate the assignments. If you update existing scheduled and activated assignments, the assignments still use the same schedule and you do not need to use Contact Center Management.

Limitations

This section lists the maximum number of agent-to-skillset and agent-to-supervisor assignments that you can set up and schedule to run concurrently using the XML automated assignments feature.

Supervisor assignment limits

You can create an agent-to-supervisor assignment that contains a maximum of 1000 entries, where assigning an agent to a supervisor is considered an entry. Avaya recommends that you do not run multiple supervisor assignments concurrently.

Skillset assignment limits

You can create an agent-to-skillset assignment that contains a maximum of 1500 entries, where assigning an agent to a skillset is considered an entry and where the number of skillsets multiplied by the number of agents involved is less than 5000. Avaya recommends that you do not run multiple skillset assignments concurrently.

Generally, Avaya recommends that you do not assign more than 2500 entries per hour, a figure based on operational experience. However, due to the broad spectrum of processor speeds and the diversity of contact centers, this value is a guideline rather than a strict limit.

Overview of steps

About this task

The XML automated assignments feature involves the following general steps:

1. Create XML files for agent-to-supervisor and agent-to-skillset assignments using the tool of your choice (for example, a WFM system).

   Because agent-to-supervisor and agent-to-skillset assignment data cannot exist in the same XML file, you must create separate XML files for each type of assignment.

2. Place the XML files in the designated drop folder. This is the folder that you specified during the installation of the XML automated assignments feature. If you did not choose a specific folder, then place the files in the default folder: <install drive>:\Avaya\Contact Center\Manager Administration\Assignments\XMLAssignments, where <install drive> is the drive on which you installed Contact Center Manager Administration.

3. When you place a file in this folder, the service automatically detects it and parses the file. If you specified a new assignment name in the file, the program creates a new assignment on the Contact Center Manager Server that you indicated in the file. If you specified an assignment name that exists on the selected server, the program updates the existing assignment with the new details.

4. After it parses the file, the service deletes it from the drop folder, thus ensuring that only new files are parsed. The system notifies you of the successful assignments in the Audit Trail component.

5. If you created a new ad hoc assignment and specified it to Execute Now, the assignment runs immediately. If you created a new scheduled assignment, you must schedule and activate it using the Contact Center Management interface.

   New scheduled assignments created with the XML automated assignments feature do not run until you activate and schedule them in the Contact Center Management component. However, if you update an existing activated and scheduled assignment with the XML automated assignments feature, the schedule remains intact and the assignment remains activated. If you want the assignment to run only at the scheduled time, you must select the Schedule option in the XML file. If you choose the Execute Now option, the scheduled assignment runs twice: it runs immediately and at the scheduled time. If you do not include the <EXECUTENOW> field in your XML file, or if you type an invalid value in this field, the system defaults to scheduling the assignment, and you must use Contact Center Management to manually schedule the new assignment.

6. If the service encounters errors in the XML file that you created, it stops parsing the file, it does not create or update the assignment, and it moves the file to the designated drop folder for problem files. If you did not choose a specific location for problem

files during the installation, the program places the files in the default location: <install drive>:\Avaya\Contact Center\Manager Administration\Assignments\XMLAssignmentError, where <install drive> is the drive on which you installed Contact Center Manager Administration. The system notifies you of problem assignments in the Audit Trail component.

The program rejects files that contain more than 1 000 entries and notifies you of rejected assignments in the Audit Trail component. An example of an entry is assigning an agent to a supervisor or to a skillset. To prevent the program from rejecting your files, limit each file to 1 000 entries or less. For more information, see Limitations on page 156.

7. If the service rejects the XML file you create, fix the problem and place the file in the drop folder to be parsed again. Continue this process until the service successfully parses the file and creates or updates the assignment, and then schedule and activate the assignment in Contact Center Management, if required.

Specifications for XML files

Valid XML files must contain the following data items for the service to parse them successfully:

- Version—The service uses the version field to identify the XML Schema version used by the XML file.

- Assignment name—This is an alphanumeric data field that identifies the name of the assignment to be created or updated. This data is enclosed in the XML tags <ASSIGNMENTNAME> </ASSIGNMENTNAME>.

- Execute option—Use this is optional field to specify whether you want to run the assignment immediately or schedule it. If you want to run the assignment immediately, type the value Execute Now. If you want to save and schedule a new assignment in Contact Center Management, or if you want to update an existing scheduled assignment, type the value Schedule. (If you do not include this field in your XML file, or if you type an invalid value in this field, the system defaults to scheduling the assignment, and you must use Contact Center Management to manually schedule the new assignment.) The value you choose is enclosed in the XML tags <EXECUTEOPTION> </EXECUTEOPTION>.

- Contact Center Manager Server IP address—This is an alphanumeric field used to identify the IP address of the Contact Center Manager Server on which you want to create or update the assignment. This data is enclosed in the XML tags <IPADDRESS> </IPADDRESS>.

- Agent details—The agent details section contains data that uniquely identifies an agent (for example, the agent's first name, last name, and phone login ID). In this section, the first name and last name are optional; the login ID is mandatory. This data is enclosed in the following XML tags:

```
<AGENT>
<FIRSTNAME> </FIRSTNAME>
<LASTNAME> </LASTNAME>
<LOGINID> </LOGINID>
</AGENT>
```

- Skillset details—The skillset details contain the skillset name and priority for the agent-to-skillset assignment. This data is enclosed in the following XML tags:

```
<SKILLSET>
<NAME> </NAME>
<PRIORITY></PRIORITY>
</SKILLSET>
```

The XML skillset tag <SKILLSET> is embedded in the agent XML tag <AGENT> for each skillset that is assigned/unassigned to an agent, as shown below:

```
<AGENT>
<FIRSTNAME> </FIRSTNAME>
<LASTNAME> </LASTNAME>
<LOGINID> </LOGINID>
<SKILLSET>
<NAME> </NAME>
<PRIORITY> </PRIORITY>
</SKILLSET>
<SKILLSET>
<NAME> </NAME>
<PRIORITY> </PRIORITY>
</SKILLSET>
..............
..............
</AGENT>
```

- Supervisor details—The supervisor details section contains data that uniquely identifies the supervisor to whom the agent is to be assigned. This data is enclosed in the following XML tags:

```
<PRIMARYSUPERVISOR>
<ID> </ID>
<NAME> </NAME>
</PRIMARYSUPERVISOR>
```

The supervisor XML tag <PRIMARYSUPERVISOR> is embedded in the agent XML tag <AGENT>. The supervisor tag appears once in the agent tag for each agent-to-supervisor assignment, as shown in the following script example. In this section, the agent first name, last name, and primary supervisor name are optional; the login ID and ID values are mandatory:

```
<AGENT>
<FIRSTNAME> </FIRSTNAME>
<LASTNAME> </LASTNAME>
<LOGINID> </LOGINID>
<PRIMARYSUPERVISOR>
<ID> </ID>
<NAME> </NAME>
</PRIMARYSUPERVISOR>
</AGENT>
```

Sample XML data files

This section contains examples of XML files with agent-to-skillset assignment data and agent-to-supervisor assignment data. Both examples are based on the XML Schema definition file, SWCXMLAssignments.xsd, in the following folder on the Contact Center Manager Administration server: C:\Program Files\Avaya\Contact Center\Manager Administration\Server\XMLAssignments, where C is the drive on which you installed Contact Center Manager Administration.

Agent-to-skillset assignment data and agent-to-supervisor assignment data cannot exist in the same XML file.

Sample agent-to-skillset assignment XML file

```
<?xml version="1.0" encoding="UTF-8"?>
<ASSIGNMENTS xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="E:\Documents\Web Client\SWCXMLAssignments.xsd">
    <VERSION>1.0.0</VERSION>
```

```
     <IPADDRESS>10.10.10.10</IPADDRESS>
     <ASSIGNMENTNAME>AgentSalesAssign</ASSIGNMENTNAME>
     <EXECUTEOPTION>Schedule</EXECUTEOPTION>
     <AGENT>
          <FIRSTNAME>John</FIRSTNAME>
          <LASTNAME>Smith</LASTNAME>
          <LOGINID>2312</LOGINID>
          <SKILLSET>
               <NAME>SalesOrange</NAME>
               <PRIORITY>1</PRIORITY>
          </SKILLSET>
          <SKILLSET>
               <NAME>SalesGreen</NAME>
               <PRIORITY>3</PRIORITY>
          </SKILLSET>
          <SKILLSET>
               <NAME>SalesBlue</NAME>
               <PRIORITY>Standby</PRIORITY>
          </SKILLSET>
     </AGENT>
</ASSIGNMENTS>
```

Sample agent-to-supervisor assignment XML file

```
<?xml version="1.0" encoding="UTF-8"?>
<ASSIGNMENTS xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="E:\Documents\Web Client\SWCXMLAssignments.xsd">
     <VERSION>1.0.0</VERSION>
     <IPADDRESS>10.10.10.10</IPADDRESS>
     <ASSIGNMENTNAME>AgentSalesAssign</ASSIGNMENTNAME>
     <EXECUTEOPTION>Execute Now</EXECUTEOPTION>
     <AGENT>
          <FIRSTNAME>John</FIRSTNAME>
          <LASTNAME>Smith</LASTNAME>
          <LOGINID>2312</LOGINID>
          <PRIMARYSUPERVISOR>
               <ID>007</ID>
               <NAME>James Monroe</NAME>
          </PRIMARYSUPERVISOR>
     </AGENT>
     <AGENT>
          <FIRSTNAME>Pat</FIRSTNAME>
          <LASTNAME>Jones</LASTNAME>
          <LOGINID>4523</LOGINID>
          <PRIMARYSUPERVISOR>
               <ID>3221</ID>
               <NAME>James Monroe</NAME>
          </PRIMARYSUPERVISOR>
     </AGENT>
</ASSIGNMENTS>
```

Force Agent Log out and Change Agent Status

The Force Agent Log out feature allows a supervisor to remotely log an agent out of Contact Center from the Contact Center Manager Administration (CCMA) user interface. This allows supervisors to log out agents who forget to log out or to go not-ready at the end of their shift.

> ❗ **Important:**
>
> Use the option to log out an agent only in exceptional circumstances, where there is no other option. If an agent has active contacts and a supervisor forces them to log out, Agent Desktop shuts down: in certain scenarios this leaves their active contacts in an incorrect state. The following use cases indicate situations in which a supervisor can use the force log out feature:
>
> - An agent falls sick at work, and transfers their current contacts, but leaves their desk without logging off. A locked screensaver prevents anyone accessing their desktop to close Agent Desktop. The supervisor forces this agent to log off, and there is no impact to customer contacts.
>
> - Agents in a global networked contact center leave their desks, forgetting to log off. After their site has closed, their active Agent Desktop log-ons are consuming licenses needed in Contact Center sites in other timezones. The supervisor forces these agents to log off, because that site is closed and no contacts are routing to that site.

The supervisor can also force an agent state change to toggle it between Ready or Not Ready. When they force an agent into the Not Ready state, supervisors have the option to enter a Not Ready Reason code for the agent. The following use cases indicate situations in which a supervisor chooses to force an agent state change:

- A trainee agent goes Not Ready, entering a reason code of At_Lunch. They return from lunch but forget to reset their status to Ready. Their supervisor can see that they are at their desk, and also that they show Not Ready on the Real time Display (RTD). The supervisor uses the Change State button to make the agent Ready.

- A trainee agent leaves their desk for lunch, but forgets to set their status to Not Ready. Contacts continue to alert on their Agent Desktop. The supervisor notices that the agent is not at their desk, and that they show Ready on the RTD. The supervisor uses the Change State button to make the agent Not Ready.

When a supervisor logs out an agent, or changes the agent's status, the agent receives a notification in Agent Desktop. With normal usage of the Force Agent Log out option, this is not required, because the agent is not present at their desktop. However, if a supervisor accidentally selects the wrong agent to log out, this notification gives the agent a time period in which to gracefully complete their active contacts. This time period is configurable in Multimedia Administration. If the agent has an active voice contact, they are able to continue the call on their physical phoneset after Agent Desktop closes; where the agent is using the Agent Desktop softphone, this is not possible and the voice contact drops.

In AML-based contact centers, you cannot force log out or change the state of an agent who is logged-on only to a deskphone. For this feature, CCT must have control of the agent endpoint.

Administrators can use a new Access and Partition management setting to restrict access to the Force Agent Log out feature. A new Force Agent State Change access privilege controls access to Force Agent Log out and Change Agent State. Only supervisors who have the Force Agent State Change privilege can use the feature, and supervisors can log out or change the state of only those agents that they can see in their partition.

Supervisors access the Force Agent Log out feature either from an agent Real-Time Display (RTD) or from the Contact Center Management user interface. From the CCM interface, Force

Agent Log out enables a supervisor to log out a single agent or a group of agents. Changing an agent's ready state is possible only from a Real Time Display (RTD).

The columns that display the Force Agent Log out and Change State buttons on an RTD are optional, and are not available on the standard RTDs. To use the buttons, supervisors must create a private RTD with the Change State and Logout columns included. While a supervisor can make public an RTD with these columns, supervisors viewing the public RTD cannot use the buttons if they do not have the "Force Agent State Change" access privilege.

The CCMA audit trail records both the force logout and the force state change events. The audit details the time at which the event happened, the agent that the supervisor modified, and the CCMA user id of the supervisor who carried out the action.

Chapter 30: Contact Center Management configuration

After you add and configure each server in Contact Center Manager Server, you can use the Contact Center Management component to perform the following tasks:

- Add, edit, view, or delete users on a server in Contact Center Manager Server.

- Add, edit, view, or delete agent-to-supervisor assignments.

- Add, edit, view, or delete agent-to-skillset assignments.

- View the schedule of all agent-to-skillset and agent-to-supervisor assignments.

- Run user-defined assignments on an ad hoc basis.

- Apply assignment changes to multiple agents simultaneously.

- Display agent logon status in Agents, Supervisors, Skillsets and Assignments and Agent Details views.

- Search by agent logged in or logged out status.

- Display agent TN name in Agent Details view.

- Assign an agent to default queue management.

- Use Contact Center Management to quickly assign agents to existing partitions instead of opening the Access and Partition Management component.

Prerequisites to Contact Center Management configuration procedures

Add and configure each server in CCMA Configuration.

Logging in to Contact Center Manager Administration for Management

About this task

Log in to Contact Center Manager Administration to configure and administer your Contact Center Manager Server.

Contact Center Management contains the following five main data views:

- Supervisors view
- Agents view
- Skillsets view
- Assignments view
- Network Agent Admin view

Based on your access class, you can use Contact Center Management to perform the following tasks:

- Add, edit, view, and delete users defined in Contact Center Manager Server.
- Add agents to user-defined partitions.
- Log out one agent or multiple agents.
- Add, edit, view, delete, and schedule agent-to-supervisor assignments.
- Add, edit, view, delete, and schedule agent-to-skillset assignments.

Procedure

1. Start Microsoft Edge with IE mode.

2. In the **Address** box, type the URL of the 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. Do not use the server IP address to log in.

   If your site does not use the default port for Internet Information Services (IIS), the URL of the server is `https://<server name>:<port number>`, where *<server name>* is the computer name of the Contact Center server, and *<port number>* is the port for the CCMA site in IIS. For example, `https://ccserver:81`.

3. In the **User ID** box, type your user ID.

4. In the **Password** box, type your password.

5. Click **Login**.

   If configured in the security settings, CCMA displays the date and time of your last login and the number of failed login attempts since your last successful login.

6. Click **Contact Center Management**.

Chapter 31: Supervisors

When you open Contact Center Management from the CCMA launchpad, the Contact Center Management window opens in Supervisors view. You can use this view to:

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

Adding a supervisor

Before you begin

🛈 **Important:**

This procedure applies to SIP-enabled Contact Centers. To add a supervisor to an AML-based Contact Center, see Adding a supervisor to an AML-based Contact Center on page 167.

- Ensure that you have a domain user account for your Contact Center domain with privileges to list the domain users.
- Ensure that you have the appropriate access class to add supervisors in Contact Center Management.
- Log on to CCMA. For more information, see Logging in to Contact Center Manager Administration for Management on page 164.
- Open the Contact Center Management component.

About this task

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

Procedure

1. In the left pane, select the Contact Center Manager Server to which you want to add the supervisor.

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

3. In the right pane, enter the following mandatory information about the supervisor:

- First name

- Last name

- Login ID

4. Enter any optional information about the supervisor (for example, Title or Department).

5. To allow the new supervisor to log on to the Contact Center Manager Administration client application, enter a Contact Center Manager Administration Login Account and password for the supervisor.

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: \ & : < > |

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

Variable definitions

Name	Description
First Name	First name of the supervisor. The first name is mandatory for all users and can be a maximum of 30 characters long. The first name input is automatically filled in if the user is associated with a Windows user account using the Associate User Account option.
Last Name	Last name of the supervisor. The last name is mandatory and can be a maximum of 30 characters long. The last name input is automatically filled in if the user is associated with a Windows user account using the Associate User Account option.
Title	The title for the user. The title is optional and can be up to 40 characters long.
Department	The user's department. The department is optional and can be up to 40 characters long.
Language	Select the language preference for the user. Language selection is mandatory for all users.

Table continues…

Name	Description
Comment	Comments you have about the user. Comments are optional and can be up to 127 ASCII characters in length. The 127 character limit can be lower if using non-ASCII characters.
User Type	Select the Supervisor user type. This value is mandatory. Supervisors are responsible for a group of agents, and can monitor agents' performance in the real-time displays in CCMA. Supervisors are not assigned skillsets and do not handle contacts. Supervisors cannot log on to Agent Desktop.
Login ID	The number that the user enters to log on to the Contact Center. This value is mandatory for all users. For the Avaya Communication Server 1000, the login ID can be a maximum of 16 digits long.
CCMA Login Account Details– User Name	The supervisor's Contact Center Manager Administration user ID. This is the user ID that the supervisor uses to access the CCMA client application. When you give the supervisor a CCMA user ID in Contact Center Management, the supervisor's profile automatically copies to the Users tree in Access and Partition Management. An administrator must then grant the supervisor basic access rights to the appropriate CCMA components before the supervisor can log on to the server and use the client application. If an administrator does not finish configuring the CCMA user in this way, then the supervisor cannot use CCMA. After you save the CCMA user ID, you cannot change it.
CCMA Login Account Details– Password	Enter a password the supervisor uses to log in to the Contact Center Manager Administration server and access the Contact Center Manager Administration client application.

Adding a supervisor to an AML-based Contact Center

Before you begin

- Ensure that you have a domain user account for your Contact Center domain with privileges to list the domain users.

- Ensure that you have the appropriate access class to add supervisors in Contact Center Management.
- Log on to CCMA. For more information, see [Logging in to Contact Center Manager Administration for Management](#) on page 164.
- Open the Contact Center Management component.

About this task

Complete this procedure in Contact Center Management to add a supervisor to an AML-based Contact Center.

Procedure

1. In the left pane, select the Contact Center Manager Server to which you want to add the supervisor.

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

3. In right pane, enter the following mandatory information about the supervisor:

   - First name

   - Last name

4. Enter any optional information about the supervisor (for example, Title or Department).

5. To allow the supervisor to log on to the Contact Center Manager Administration server, enter a Contact Center Manager Administration Login Account and password for the supervisor.

   Passwords must be at least eight characters long, and include at least one number, at least one uppercase letter, at least one lowercase letter, and no spaces.

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

Variable definitions

Name	Description
First Name	The first name of the user. The first name is mandatory for all users and can be a maximum of 30 characters long.
Last Name	The last name of the user. The last name is mandatory and can be a maximum of 30 characters long.
Title	The title for the user. The title is optional and can be up to 40 characters long.
Department	The user's department. The department is optional and can be up to 40 characters long.
Language	Select the language preference for the user. Language selection is mandatory for all users.

Table continues…

Name	Description
Comment	Comments you have about the user. Comments are optional and can be up to 127 ASCII characters in length. The 127 character limit can be lower if using non-ASCII characters.
User Type	Select the user type. This value is mandatory. Select Supervisor—Supervisors are responsible for a group of agents, and can monitor agents' performance in the real-time displays in Contact Center Manager Administration. Supervisors are not assigned skillsets.
CCMA Login Account Details– User Name	The supervisor's Contact Center Manager Administration user ID. This is the user ID that the supervisor uses to access the CCMA client application.

When you give the supervisor a CCMA user ID in Contact Center Management, the user's profile automatically copies to the Users tree in Access and Partition Management. An administrator must then grant the supervisor basic access rights to the appropriate CCMA components before the user can log on to the server and use the client application. If an administrator does not finish configuring the CCMA user in this way, then the user cannot use CCMA.

After you save the CCMA user ID, you cannot change it. |
| CCMA Login Account Details– Password | Enter a password the supervisor uses to log in to the Contact Center Manager Administration server and access the Contact Center Manager Administration client application. |
| Supervisor Information–Telephony Port | The position ID of the supervisor's telephone (SPID). This is mandatory only when adding a supervisor as only supervisors have an SPID. The PABX maps agent keys of the supervisor's reporting agents to the telephone identified by this field.

To communicate with reporting agents through the telephone (for example, using the Emergency and Answer Emergency keys), the supervisor must log on to the telephone using this specified address. Supervisors cannot roam; their location is fixed.

The telephony/port address is mandatory for all supervisors and supervisor/agents, and can be a maximum of 7 digits long. |

Deleting a supervisor

Before you begin

- Log on to CCMA. For more information, see Logging in to Contact Center Manager Administration for Management on page 164.
- Open the Contact Center Management component.
- Ensure that the supervisor has no assigned agents. Before you delete a supervisor, you must first reassign all agents who report to that supervisor to another supervisor.

About this task

Delete a supervisor to remove the supervisor from your system.

Procedure

1. From the **View/Edit** menu, select **Supervisors**.

2. In the left pane, click the server containing the supervisor to delete.

   The server expands to show the list of supervisors configured on it.

3. Right-click the supervisor to delete, and then click **Delete Supervisor**.

4. In the message box that appears asking you to confirm your choice, click **Yes**.

Modifying supervisor details

Before you begin

- Log on to CCMA. For more information, see Logging in to Contact Center Manager Administration for Management on page 164.
- Open the Contact Center Management component.

About this task

Complete the following procedure to modify the details of a supervisor or a supervisor/agent.

Procedure

1. From the **View/Edit** menu, select **Supervisors**.

2. In the left pane, expand the server on which to work with the supervisor/agent profile.

   The list of supervisors configured on the server appears.

3. Right-click the supervisor whose profile you want to edit, and then select **View Supervisor Details**.

4. On the Supervisor Details window, in the **User Details** section, you can change details, such as first name, last name, phone login ID, title, language, department, or comments.

5. If your contact center is licensed for Agent Greeting, complete the details under **Agent Greeting**.

6. In the **Supervisor Information** area, you can change the telephony port address, and assign or change the Contact Center Manager Administration user ID.

   🛈 **Important:**

   If you assign the user a Contact Center Manager Administration user ID and password, an administrator must complete configuration of the user profile in the Access and Partition Management component.

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

Chapter 32: Agents

In the Agents view, you can search for particular agents or list all agents on a server. You can also use the agents view to

- view and edit the agents' properties, including the skillsets and partitions to which the agents are assigned

- delete the agents from the server one at a time or in bulk

- quickly create a new agent by copying an agent's properties

- quickly create many new agents by importing a CSV file

- associate an agent with a Communication Control Toolkit user

- log out an agent or multiple agents

Partly configured agents appear in the Contact Center Management Agents list with a grey agent icon. You can only delete these agents.

Two types of agents are available in Contact Center Management:

- Agents

- Supervisor/agents

Adding an agent

Before you begin

> ⓘ **Important:**
>
> This procedure applies to SIP-enabled Contact Centers. To add an agent to an AML-based Contact Center, see <u>Adding an agent to an AML-based Contact Center</u> on page 178.

- Ensure that you have a domain user account for your Contact Center domain with privileges to list the domain users.

- You must have the appropriate access class to access and work in this window. If you cannot open part of the window that you need to work with, ask your administrator to update the access class assigned to you. To work with all sections of this window and add and edit all types of users, you need the Add/Edit/Delete Agents and Supervisors access level.

- Log on to CCMA. For more information, see <u>Logging in to Contact Center Manager Administration for Management</u> on page 164.

- Open the Contact Center Management component.

About this task

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

If you select Copy Agent Properties from a Functions menu, or click Create Many while viewing an existing agent, the window appears and the User Details and User Information sections expand and contain some information from the copied agent profile.

Procedure

1. In the left pane, click the Contact Center Manager Server under which to add the agent.

2. From the **Add** menu, select **Agent**.

3. In the New Agent Details window, enter the following mandatory information about the agent:

   - First name
   - Last name
   - Login ID
   - Voice URI
   - Create CCT Agent
   - Primary supervisor

   ✱ **Note:**

   Login ID = 1 is reserved for the system use.

4. Enter information about the agent (for example, Call Presentation Class, Threshold, Title, Department, or Comments).

5. If available, click **Create CCT Agent**, and complete the **Associate User Account** fields to create a CCT user for this agent.

6. If this agent uses the multiplicity feature on Avaya Agent Desktop, select a multiplicity presentation class from the **Multiplicity Presentation Class** list.

   If multiplicity is not enabled, the Multiplicity Presentation Class list does not appear.

7. If Agent Greeting is enabled, click the **Agent Greeting** heading and complete the fields for Agent Greeting.

8. If Offsite Agent is enabled on your system, click the **Offsite Agent** heading and complete the fields.

9. If Open Queue is enabled on the Contact Center Manager Server, click the **Contact Types** heading.

10. Select the check box beside each **Contact Type** to assign to the agent.

11. Click the **Skillsets** heading.

12. In the **Skillsets** area, click **List All** to list all skillsets configured on the server.

If a skillset is not included in your partition, it does not appear. Contact your administrator and request that the administrator add the skillset to the partition assigned to you.

13. From the **Priority** list for each skillset to assign to the agent, select the priority level or select **Standby** to put the agent in standby mode for this skillset.

   Priority levels range from 1 to 48, with 1 being the highest priority for the skillset.

14. If you have administrator privileges, you can add this new agent to the partitions assigned to the agent's supervisor (instead of having to do so in Access and Partition Management). Click the **Partitions** heading.

   The list of partitions configured on the server appears.

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

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

Variable definitions

Name	Description
First Name	The first name of the user. The first name is mandatory for all users and can be a maximum of 30 characters long.
Last Name	The last name of the user. The last name is mandatory for all users and can be a maximum of 30 characters long.
Title	The title for the user. The title is optional and can be up to 40 characters long.
Department	The user's department. The department is optional and can be up to 40 characters long.
Language	Select the language preference for the user. Language selection is mandatory for all users.
Comment	Comments you have about the user. Comments are optional and can be up to 127 ASCII characters in length. The 127 character limit can be lower if using non-ASCII characters.
User Type	Select the user type. This value is mandatory. Select the agent user type. Agents are users who are assigned skillsets and who answer contacts in the Contact Center. All agents must be assigned to a supervisor.
Login ID	The number that the user enters to log on to the phone. This value is mandatory for all users. For the Avaya Communication Server 1000, the log on ID can be a maximum of 16 digits long.

Table continues…

Name	Description
Voice URI	The SIP address of the TR87-controlled terminal dedicated to this agent, in the format sip:agent. If using an Avaya Aura® PBX, use Extension@Session Manager IP address. For example, sip:4400@47.166.115.99.
IM URI	The SIP address of the TR87-controlled terminal dedicated to this agent, in the format sip:agent for IM.
Create CCT Agent	Select this box to display the Associate User Account fields. This field is mandatory on a SIP-enabled Contact Center.
Primary Supervisor	The agent's supervisor. You can choose from all supervisors configured on the server to which you are currently logged on.
Call Presentation	The call presentation class to assign to this agent. The call presentation class determines whether the agent can take a break between calls, whether the agent can put DN calls on hold for incoming ACD calls, and whether the agent phone shows that the agent is reserved for a network call. Call Presentation is mandatory for all users with agent and supervisor/agent capability.
Multiplicity Presentation Class	The multiplicity presentation class to assign to this agent. The multiplicity presentation class determines the type and number of Multimedia contacts an agent can have open simultaneously on Avaya Agent Desktop. If multiplicity is not enabled, the Multiplicity Presentation Class list does not appear.
Agent Greeting Enabled	Select to enable Agent Greeting for the agent.
Agent Greeting Password	The password the agent uses to dial into the Agent Greeting recording application.
Agent Greeting Recorded	The system indicates that an agent greeting is recorded.
Communication Manager Agent ID	The Avaya Aura® Communication Manager ID for this Agent.
Communication Manager Server	The display name of the Avaya Aura® Communication Manager server for this Agent.
Threshold	The threshold class to assign to this user. The threshold class is mandatory for all users with agent and supervisor/agent capability.

Table continues…

Name	Description
Offsite Agent Enabled	Select to allow this agent to use Offsite Agent. Available only if the Contact Center is licensed for Offsite Agent.
Phone 1	The primary telephone number at which this agent receives calls from the Contact Center when working as an offsite agent. The phone number has a maximum of 15 digits. ⊛ **Note:** Ensure that this number is not an Avaya Aura® Communication Manager station number.
Phone 2	The secondary telephone number at which this agent receives calls from the Contact Center when working as an offsite agent. The phone number has a maximum of 15 digits. ⊛ **Note:** Ensure that this number is not an Avaya Aura® Communication Manager station number.
Allow agent to enter an alternate phone	Select to allow the agent to enter an alternate number to the numbers configured in Phone 1 or Phone 2. The agent can enter a different number when they log into Agent Desktop as an offsite agent.
Search local operating system	Select if you want the user to be able to log on using accounts from the operating system on the local server (i.e., the CCMA server). Select this for a single-server install. Applies to supervisor/agents and agents.
Search domain users	Select to search for users from the Contact Center domain. Applies to all user types.
Domain Details - Server IP (or DNS)	If you selected Search domain users, enter the IP address of the domain controller from which you want to select the user account (mandatory).
Domain Details - Specify Domain Account	Select to allow you to specify a user account with which to search the domain as an authenticated domain user.

Table continues…

Name	Description
Domain Account	If you select Specify Domain Account, complete the following: • (Domain\User ID) – enter the domain user name to use to authenticate on the domain. This user must have the correct privileges to list domain users. ⊛ **Note:** The domain name is case sensitive and can not contain the following characters: ",", "+", """, "\", "<", ">" or ";". • Password–enter the password for the user name you want to use to authenticate on the domain. • Base DN–enter the FQDN of the domain from which you want to select the user account. • Use Secure Connection–select to search over a secure connection. Mandatory if the domain requires secure access. • Port Number–if the domain controller is not using the default port, enter the port number. If you selected Use Secure Connection, you must specify the secure port here (the default for domain controllers is 626).
Search all user accounts where:	Select the domain user field to search on. You can search on the user Last Name, First Name, Group Name, or User ID.
starts with	Enter a string with which you want to search user accounts. The search matches this string only against the start of the selected user account field.
and includes	Select from this list to refine your search to return: • all users–lists all users in the domain. • available users only–lists only the users in the domain that are not already associated with a supervisor or an agent.
Search	Click to search for users in the domain that match your search criteria. The Results grid appears and displays the domain users matching the search.
List All	List everything in the domain without applying search criteria.

Table continues…

Name	Description
Results	Display the users returned by your search. Click on a user to associate the account with this agent. You can associate only those users where the Status is Available.

Adding an agent to an AML-based Contact Center

Before you begin

- Ensure that you have a domain user account for your Contact Center domain with privileges to list the domain users.

- You must have the appropriate access class to access and work in this window. If you cannot open part of the window that you need to work with, ask your administrator to update the access class assigned to you. To work with all sections of this window and add and edit all types of users, you need the Add/Edit/Delete Agents and Supervisors access level.

- Log on to CCMA. For more information, see Logging in to Contact Center Manager Administration for Management on page 164.

- Open the Contact Center Management component.

About this task

In this window, you can add new agents. What you see in this window depends on how you launch the window and the access class assigned to you.

If you select Copy Agent Properties from a Functions menu, or click Create Many while viewing an existing agent, the window appears and the User Details and User Information sections expand and contain information.

Procedure

1. In the left pane, click the Contact Center Manager Server under which to add the agent.

2. From the **Add** menu, select **Agent**.

3. In the New Agent Details window, enter the following mandatory information about the agent:

   - First name

   - Last name

   - Login ID

   - Primary supervisor

   - Call presentation

   - Threshold

4. Enter any optional information about the agent (for example, Title, Department, or Comments).

5. If you want to create a CCT user for this agent, select **Create CCT Agent**.

6. If you selected **Create CCT Agent**, click **Associate User Account**, and complete the Associate User Account fields to create a CCT user for this agent.

7. If this agent uses the multiplicity feature on Agent Desktop, select a multiplicity presentation class from the **Multiplicity Presentation Class** list.

    If multiplicity is not enabled, the Multiplicity Presentation Class list does not appear.

8. If Agent Greeting is enabled, click the **Agent Greeting** heading and complete the fields for Agent Greeting.

9. If Open Queue is enabled on the Contact Center Manager Server, click the **Contact Types** heading.

    If Open Queue is not enabled, the Contact Types section does not appear.

10. Select the check box beside each **Contact Type** to assign to the agent.

11. Click the **Skillsets** heading.

12. In the **Skillsets** area, click **List All** to list all skillsets configured on the server.

    If a skillset is not included in your partition, it does not appear. Contact your administrator and request that the administrator add the skillset to the partition assigned to you.

13. From the **Priority** list for each skillset to assign to the agent, select the priority level or select **Standby** to put the agent in standby mode for this skillset.

    Priority levels range from 1 to 48, with 1 being the highest priority for the skillset.

    ⓘ Important:

    With a Open Queue-enabled Contact Center Manager Server, you can only assign skillsets to an agent that belongs to the same contact type.

14. If you have administrator privileges, you can add this new agent to the partitions assigned to the agent's supervisor (instead of having to do so in Access and Partition Management). Click the **Partitions** heading.

    The list of partitions configured on the server appears.

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

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

Variable definitions

Name	Description
First Name	The first name of the user. The first name is mandatory for all users and can be a maximum of 30 characters long.

Table continues…

Agents

Name	Description
Last Name	The last name of the user. The last name is mandatory and can be a maximum of 30 characters long.
Title	The title for the user. The title is optional and can be up to 40 characters long.
Department	The user's department. The department is optional and can be up to 40 characters long.
Language	Select the language preference for the user. Language selection is mandatory for all users.
Comment	Comments you have about the user. Comments are optional and can be up to 127 ASCII characters in length. The 127 character limit can be lower if using non-ASCII characters.
User Type	Select the user type. This value is mandatory. Select the agent user type: Agents are users who are assigned skillsets and who answer contacts in the Contact Center. All agents must be assigned to a supervisor.
Login ID	The number that the user enters to log on to the phone. This value is mandatory for all users. For the Avaya Communication Server 1000, the log on ID can be a maximum of 16 digits long.
Personal DN	The directory number where the agent can receive personal calls. The personal DN is optional and can be up to 7 digits long.
ACD Queue	Use this field to assign an ACD Queue to the agent for calls defaulted and when you use Queue to NACD. An Agent can log into any phone and the default ACD Queue automatically updates to the appropriate queue for the agent.
ACD Queue Error	This is a read-only field. When you assign ACD Queue to an agent that is logged in, the following error message is returned from Avaya Communication Server 1000 or Contact Center Manager Administration: "Agent is required to login again for the ACD Queue to be assigned."
Create CCT Agent	If CCMS is associated with CCT, select this box to display the Associate User Account fields. This field is not mandatory on an AML-enabled Contact Center.

Table continues…

Name	Description
Primary Supervisor	The agent's supervisor. You can choose from all supervisors configured on the server to which you are currently logged on.
Agent Key	The number on the supervisor's phone corresponding to the agent's phone. This key enables the supervisor to communicate with the agent. This field is not applicable nor available when connected to a SIP server.
Login Status	The current status of the agent (Logged In or Logged Out), which is useful when you want to quickly reassign agents to skillsets. This data is read-only.
Call Presentation	The call presentation class to assign to this agent. The call presentation class determines whether the agent can take a break between calls, whether the agent can put DN calls on hold for incoming ACD calls, and whether the agent phone shows that the agent is reserved for a network call. Call Presentation is mandatory for all users with agent and supervisor/agent capability.
Multiplicity Presentation Class	The multiplicity presentation class to assign to this agent. The multiplicity presentation class determines the type and number of Multimedia contacts an agent can have open simultaneously on Agent Desktop. If multiplicity is not enabled, the Multiplicity Presentation Class list does not appear.
Agent Greeting Enabled	Select to enable Agent Greeting for the agent.
Agent Greeting Password	The password the agent uses to dial into the Agent Greeting recording application.
Agent Greeting Recorded	The system indicates that an agent greeting is recorded.
Threshold	The threshold class to assign to this user. The threshold class is mandatory for all users with agent and supervisor/agent capability.
Tn Name	The Terminal Number at which the agent's phone is wired into the PABX. This box displays a value only if the agent is logged on; it is blank if the agent is logged off.

Table continues…

Name	Description
Search local operating system	Select if you want the user to be able to log on using accounts from the operating system on the local server (i.e., the CCMA server). Select this for a single-server install. Only applies to supervisor/agents and agents.
Search local security server	If you implemented single sign-on (SSO) on this Contact Center deployment, select to search for users on the System Manager server. Only applies to supervisors and supervisor/agents.
Search domain users	Select to search for users from the Contact Center domain. Applies to all user types.
Domain Details - Server IP (or DNS)	If you select Search domain users, enter the IP address of the domain controller from which you want to select the user account (mandatory).
Domain Details - Specify Domain Account	Select to allow you to specify a user account with which to search the domain as an authenticated domain user.
Domain Account	If you select Specify Domain Account, complete the following: • (Domain\User ID)–enter the domain user name to use to authenticate on the domain. This user must have the correct privileges to list domain users. • Password–enter the password for the user name you want to use to authenticate on the domain. • Base DN–enter the FQDN of the domain from which you want to select the user account. • Use Secure Connection–select to search over a secure connection. Mandatory if the domain requires secure access. • Port Number–if the domain controller is not using the default port, enter the port number. If you selected Use Secure Connection, you must specify the secure port here (the default for domain controllers is 626).
Search all user accounts where	Select the domain user field to search on. You can search on the user Last Name, First Name, Group Name, or User ID.
starts with	Enter a string with which you want to search user accounts. The search matches this string only against the start of the selected user account field.

Table continues…

Name	Description
and includes	Select from this list to refine your search to return: • all users–lists all users in the domain. • available users only–lists only the users in the domain that are not already associated with a supervisor or an agent.
Search	Click to search for users in the domain that match your search criteria. The Results grid appears and displays the domain users matching the search.
List All	List everything in the domain without applying search criteria.
Results	Display the users returned by your search. Click on a user to associate the account with this supervisor or supervisor/agent. You can associate only those users where the Status is Available.

Adding a supervisor/agent

Before you begin

- Log on to CCMA. For more information, see <u>Logging in to Contact Center Manager Administration for Management</u> on page 164.
- Open the Contact Center Management component.

About this task

A user with Supervisor/Agent capability is assigned skillsets, answers contacts in the Contact Center, and can perform some of the duties of a regular supervisor, such as monitor real-time displays in the Contact Center Manager Administration client application, and answer agent queries. All Supervisor/Agents must be assigned to a supervisor. If the supervisor/agent is going to use the CCMA client application, you must assign a Contact Center Manager Administration user ID and password to this user.

Procedure

1. In the left pane, click the Contact Center Manager Server under which to add the supervisor/agent.

2. From the **Add** menu, select **Supervisor/Agent**.

3. In the New Supervisor/Agent Details window, enter the following mandatory information about the supervisor/agent:

   - First name

   - Last name

   - Login ID

- Call presentation class

- Threshold

- Supervisor

- Telephony/port address

  ⓘ **Important:**

     Voice URI, IM URI, and Create CCT Agent are mandatory when adding a supervisor/agent on a SIP-enabled Contact Center.

4. Enter any optional information about the supervisor/agent (for example, Title or Department).

5. If your contact center is licensed for Agent Greeting, configure the details for the Agent Greeting.

6. Under **Non-Skillset Call Monitoring**, select whether to allow the supervisor/agent to observe, or to observe and barge-in to, agents' non-skillset calls.

   This feature is available only for SIP-enabled contact centers using a Communication Manager PABX.

7. If the supervisor/agent has to log on to the Contact Center Manager Administration server and use Contact Center Manager Administration, enter a Contact Center Manager Administration user ID and password for the supervisor/agent.

   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: \ & : < > |

8. Click the **Skillsets** heading.

9. In the **Skillsets** area, click **List All** to list all skillsets configured on the server.

   ⓘ **Important:**

      If a skillset is not included in your partition, it does not appear. Contact your administrator and request that the skillset be added to the partition assigned to you.

10. In the table listing all skillsets, select the priority numbers beside the skillsets to which you want to assign the supervisor/agent, or select Standby to put the supervisor/agent in standby mode for this skillset.

    Skillset priority can range from 1 to 48, with 1 being the highest priority for this skillset.

11. If you have administrator privileges on CCMA, you can now add this new supervisor/agent to the user-defined partitions assigned to the agent's supervisor (instead of having to do so in Access and Partition Management). Click the **Partitions** heading.

The list of user-defined partitions configured on the server appears.

12. Select the check box for each partition to which you want to add the new supervisor/agent.

13. Click **Submit** to save the new user profile.

Creating a bulk import file

Before you begin

- Log on to CCMA. For more information, see Logging in to Contact Center Manager Administration for Management on page 164.

- Open the Contact Center Management component.

About this task

Follow this procedure to download a .CSV (Comma Separated Value) template file and populate it with agent and supervisor information for a bulk import. The template file you download varies depending on the release of the contact center server that you select.

Procedure

1. In the left pane, select the server to which you want to add multiple agents, supervisors, and/or supervisor/agents.

2. From the **Add** menu, choose **Many Users**.

3. Beside the **Import list of agents from** box, click **Download template file** and select **Save Target As**.

4. In the Save As dialog box, select a location on your local PC in which to store the .CSV file, and enter a descriptive name for the file.

5. Click **Save**.

6. Open the .CSV file using an editor of your choice.

7. Complete a line in the .CSV file for each agent, supervisor, and/or agent supervisor that you want to import to the contact center.

Procedure job aid: Preparing a .CSV file for Avaya Aura® Contact Center

A .CSV file downloaded for an Avaya Aura® Contact Center server has the fields described in the following table:

Field	Description
Last name	The last name of the user. The last name is mandatory and can be a maximum of 30 characters long.

Table continues…

Field	Description
First name	The first name of the user. The first name is mandatory for all users and can be a maximum of 30 characters long.
Login ID	The number that the user enters to log on to the phone. This value is mandatory for all users.
Personal DN	The directory number where the agent can receive personal calls. The personal DN is optional and can be up to 7 digits long.
Agent type	Select the user type. This value is mandatory. The valid values are: • Agent • Agent\Supervisor • Agent/Supervisor • Supervisor\Agent • Supervisor/Agent • Supervisor Agent • Agent Supervisor • Supervisor These string values are localized so this field accepts locale-specific values
Supervisor telephony port	The required telephone port for supervisors.
Agent key	The number on the supervisor's phone corresponding to the agent's phone. This key enables the supervisor to communicate with the agent. This field is not applicable if adding agents to a SIP-enabled Contact Center server.
ACD queue	The ACD Queue to assign to the agent for calls defaulted and when you use Queue to NACD.
Domain	Mandatory if you want to create a CCT user for this agent, mandatory if adding to a SIP-enabled Contact Center server. The FQDN of the domain from which you want to select the user account to associate with this agent.
Username	Mandatory if you want to create a CCT user for this agent, mandatory if adding agents a SIP-enabled solution with an Avaya Aura® Unified Communications platform. The domain user name to use to authenticate on the domain.
Voice URI	Mandatory if you are adding agents in a SIP-enabled solution with an Avaya Aura® Unified Communications platform.
IM URI	Mandatory if you are adding agents in a SIP-enabled solution with an Avaya Aura® Unified Communications platform.
isCTIEnabled	Mandatory if you are adding agents in a SIP-enabled solution with an Avaya Aura® Unified Communications platform. Valid values: Y or N

Adding multiple agents, supervisors, or supervisor/agents

Before you begin

- Log on to CCMA. For more information, see [Logging in to Contact Center Manager Administration for Management](#) on page 164.

- Open the Contact Center Management component.

- Create and save a comma-separated value (CSV) file containing the unique user details for each new user you are creating. The file must contain the information for each user (as applicable). See [Creating a bulk import file](#) on page 185.

About this task

Use the Create Many feature of Contact Center Manager to save time by adding large numbers of agents, supervisors, or supervisor/agents sequentially.

Procedure

1. In Contact Center Management, choose **View/Edit** > **Supervisors**.

   The system tree refreshes and the list of servers appears.

2. In the left pane, select the server to which you want to add users.

3. From the **Add** menu, choose **Many Users**.

4. Beside the **Import list of agents from** box, click **Browse**, and then locate and select the CSV file containing the new user information.

5. From the **Primary Supervisor** list, select the supervisor for the new users.

6. Complete other optional fields that are common for all the imported agents.

7. Click **Submit** to create the new users.

   The system creates the new users and lists any agents that cannot be added in a new window with the reason for the failure. If there are errors in the csv file, the system prompts the user to either cancel the upload and review the errors, or continue and ignore the users containing the errors.

8. Fix any failed entries in the CSV file (if applicable), and repeat steps 3 to 7.

   The system saves the users under the supervisor that you specified, and the agent or supervisor icons appear in the system tree.

9. Update the individual supervisor or agent/supervisor details.

Creating an agent/supervisor assignment

Before you begin

- Log on to CCMA. For more information, see [Logging in to Contact Center Manager Administration for Management](#) on page 164.

- Open the Contact Center Management component.
- Ensure that you have access to the New Agent to Supervisor Assignment window.
- Ensure that you understand reset assignments. For information, see [Creating a reset assignment](#) on page 204.

About this task

Create agent-to-supervisor assignments to temporarily assign multiple agents to a different supervisor when supervisors are on breaks, are sick, are on vacation, or are taking a course.

Procedure

1. In Contact Center Management, on the menu, choose **View/Edit** > **Assignments**.
2. In the left pane of the Assignments view, expand the server on which to assign agents to skillsets.

   The server shows the assignment folders.
3. Right-click the Agent Supervisor Assignments folder, and then click **Add Assignment**.
4. In the New Agent to Supervisor Assignment window, in the **Assignment Details** area, click the **List Available Agents** heading to search for agents to add to the assignment.

   The heading expands to show the agent search boxes.

   You can search for agents by first name, last name, department, comment, or login ID. You can also search by the current agent login status (Logged In or Logged Out).
5. Enter your search details up to a maximum of five different criteria.
6. Click **Search**.

   The agents that match your criteria appear in a table.

   If you search by login status, you can search by this one criterion only.
7. To list all agents configured on the server (your partitioned agents and any agents in the reporting agent combinations assigned to you), click **List All**.
8. In the **Available Agents** table, note the agents logged on, and then select the check box for each agent to include in the assignment.
9. Click **Update Table**.

   The agents with their currently assigned skillsets appear in the Assignment Details table.
10. Click the **Save/Schedule Assignments** heading.
11. In the **Save Assignment As** box, type a unique name for the assignment.
12. Select the **Create Reset Assignment** check box to create a reset assignment.
13. Click **Save** to save the reset assignment before altering the original assignment.
14. Click **Save Assignment** to save the assignment in the Assignments folder.

Deleting an agent

Before you begin

- Ensure that the agent is logged out.

- Ensure the agent is not referred to in scripts.

- Log on to CCMA.

- Open the Contact Center Management component.

About this task

Several options are available to delete an agent or a supervisor/agent. This procedure lists one possible way.

If you delete an agent who has agent greetings stored, you must delete the agent greetings for the agent ID. See Deleting agent greetings on page 63.

> ⊛ **Note:**
>
> After you delete an agent, Agent Desktop displays the agent's logon ID against historical actions for a contact instead of displaying the agent name.

Procedure

1. From the **View/Edit** menu, select **Supervisors**.

2. In the left pane, click the server containing the agent to delete.

3. Click the agent's primary supervisor.

   All agents assigned to the supervisor appear.

4. Right-click the agent to delete, and then click **Delete Agent**.

5. In the message box that appears asking you to confirm your choice, click **Yes**.

Logging out multiple agents from the Agents list

Before you begin

- Log on to CCMA.

- Open the Contact Center Management component.

- Ensure you have an Access Class that allows you to force agent state changes.

About this task

Use this procedure to force log out multiple agents.

> ❗ **Important:**
>
> Forcing multiple agents to log out can have detrimental effect to contact center operation. Consider this option only in exceptional circumstances where there is no alternative method of

logging out these agents. If an agent has active contacts and you force them to log out, Agent Desktop closes, and in certain scenarios this leaves their active contacts in an incorrect state.

Procedure

1. From the **View/Edit** menu, select **Agents**.

2. In the left pane, click the server on which the agents you want to log off are logged on.

3. In the list of agents, select each agent that you want to log off.

4. Click **Logout**.

5. On the **Message from Webpage** dialog box, click **OK**.

    Contact Center logs out the agents, and displays a message on the agents' Agent Desktop interfaces informing them that a supervisor has logged them out.

Logging out an agent from the Agent Details screen

Before you begin

- Log on to CCMA.

- Open the Contact Center Management component.

- Ensure you have an Access Class that allows you to force agent state changes.

About this task

Use this procedure to force log out a single agent and drop active voice contacts.

> 🛈 **Important:**
>
> Use Force Agent Log out only in exceptional circumstances when there is no other option to log out an agent.

Procedure

1. From the **View/Edit** menu, select **Agents**.

2. In the left pane, click the server on which the agent you want to log off is logged on.

3. In the list of agents, double click the agent that you want to log off.

    CCMA displays the Agent Details screen.

4. On the **Agent Details** window, in the **Agent Information** section, check the status of the agent in the **Login Status** field.

5. Click the **Logout Agent**.

    CCMA displays the confirmation dialog box, prompting you to drop active agent contacts.

6. On the confirmation dialog box, click one of the following:

    - **Yes**: If you want to drop all active voice contacts.

If the agent is participating in a conference, the whole conference will be dropped.

> ✱ **Note:**
>
> You can drop only voice contacts. If you apply force log out to an agent that has active contacts other than voice (instant messages, emails and other), such contacts remain active. In this case the logged out agent might have difficulties when logging in again.

- **No**: If you want to log out the agent without dropping active contacts.

> ✱ **Note:**
>
> Use this option with caution. In certain scenarios active contacts might remain in an incorrect state.

- **Cancel**: If you want to stop the logout process and leave the agent logged in.

Contact Center logs out the agent and displays a message on the agent's Agent Desktop interface informing them that a supervisor has logged them out.

Modifying agent details

Before you begin

- Log on to CCMA. For more information, see [Logging in to Contact Center Manager Administration for Management](#) on page 164.
- Open the Contact Center Management component.
- Ensure that you have access to required skillsets.

About this task

Complete this procedure to edit the details of an agent or supervisor/agent.

Procedure

1. From the **View/Edit** menu, select **Supervisors**.

2. In the left pane, click the server on which to work with the supervisor/agent profile.

   The list of supervisors configured on the server appears.

3. Click the supervisor to whom the agent is assigned.

   The tree expands to show the list of agents assigned to this supervisor.

4. Right-click the agent whose profile you want to edit, and then select **View Agent Details**.

5. On the Supervisor/Agent Details window, in the **User Details** and **Agent Information** sections, you can change agent details, such as first name, last name, User Type, phone login ID, SIP Voice URI, primary supervisor, call presentation, threshold, title, department, or comments.

> ⚠️ **Warning:**
>
> If you are modifying an agent's voice URI, ensure the agent's Agent Desktop is shut down before the voice URI is changed.

6. To change the **User Type** from **Agent** to **Supervisor/Agent** (or vice versa), you must first disassociate the agent from their Domain Account:

   a. Clear the **Create CCT Agent** check box.

   b. Click **Submit** to save the agent details.

   c. Change the **User Type** to **Agent** or **Supervisor/Agent** and re-associate the agent with their Domain Account.

7. To change the current settings for the Agent Greeting, click the **Agent Greeting** heading and modify the settings.

8. To change the current skillset assignment or assign the agent to new skillsets, click the **Skillsets** heading.

   The list of currently assigned skillsets appears.

9. To change the priority level for a skillset, in the table of assigned skillsets, from the **Priority** list, select a new priority level.

10. To assign the agent to new skillsets, click **List All** to list all skillsets configured on the server.

11. In the table listing all skillsets, from the **Priority** list, select the priority level for each skillsets to which you want to assign the agent.

    OR

    Select Standby to put the agent in standby mode for this skillset.

    Skillset priority levels range from 1 to 48, with 1 being the highest priority for this skillset.

12. To remove the skillset from the agent, select **Unassigned**.

13. If you have administrator privileges and you reassigned this agent to a new supervisor, you can now add this agent to the user-defined partitions assigned to the agent's supervisor (instead of having to do so in Access and Partition Management). Click the **Partitions** heading.

    The list of user-defined partitions configured on the server appears.

14. Select the check box for each partition to which you want to add the agent.

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

Copying agent properties

Before you begin

- Log on to CCMA. For more information, see <u>Logging in to Contact Center Manager Administration for Management</u> on page 164.
- Open the Contact Center Management component.

About this task

There are several ways to copy an agent's properties. This procedure lists one possible way. You can also click Copy Agent Properties on the Functions menu in the Agents List window, or you can right-click an agent name in the system tree, and then click Copy Agent Properties from the resulting pop-up menu.

You can create new agents quickly by copying the properties of existing agents. New agents assume the following properties from the existing agent:

- Skillset assignment
- Department
- User type
- Language
- Comment
- Supervisor
- Call presentation
- Threshold
- ACD queue
- Contact type
- Agent greeting

When you copy an agent's properties, you must type in the new agent's name and phone login ID.

You cannot copy the information from half agents.

Procedure

1. From the **View/Edit** menu, select **Supervisors**.

2. In the left pane, click the server containing the agent to copy.

3. In the left pane, click the agent's supervisor.

   The Supervisor window appears in the right pane, listing the assigned agents in a table.

4. In the table, click **Functions** beside the agent to copy, and then select **Copy Agent Properties**.

   The agent's properties appear in the New Agent Details window.

5. In the **User Details** section, type the new agent's name and phone login ID.

6. Optionally, type the agent's personal DN and any comments you have about the agent. You can also change any of the copied properties. For example, you can assign the agent to new skillsets or partitions in the appropriate areas of this window.

7. After you configure the new agent, click **Submit** to save the agent under the specified supervisor.

   The agent's icon appears in the system tree.

Searching for agents

Before you begin

- Log on to CCMA. For more information, see [Logging in to Contact Center Manager Administration for Management](#) on page 164.

- Open the Contact Center Management component.

About this task

You can use the agent search feature in each of the five data views in Contact Center Management: Supervisor, Agent, Skillset, Assignment, and Network Agent Admin.

In supervisor view, you can search for agents to assign to the currently selected supervisor.

In agent view, you can search for specific agents on a particular server. Then, when you find the agents, you can view or change their properties, delete their profiles from the server, or copy their properties and create new agents.

In skillset view, you can search for agents to immediately assign to the currently selected skillset (ad hoc assignment).

In assignment view, you can search for new agents to add to saved agent to supervisor and agent to skillset assignments (and then you can schedule these assignments).

In Network Agent Admin view, you can search for specific agents across multiple servers. Then, when you find the agents, you can view their skillset assignments, change skillset priority levels, view/edit agent details.

You can search by first name, last name, department, comment, login ID, logged in/logged out status or a combination of all of these criteria (up to a maximum of five levels). You cannot use the wildcard symbol (*) in your search.

You can search only among the agents included in the partition assigned to you, and in any supervisor/reporting agent combinations assigned to you, unless you have been assigned the Full Data Across All Servers partition, or the All Agents & Supervisors partition for CCM, in which case you can search among all agents on the applicable servers.

Procedure

1. From the first list, select the criterion by which you want to search.

2. From the second list, select **Starts With**, **Contains**, or **Equals**.

3. In the third box, type the value you want to search for, or type a partial value.

For example, to search for agents with the first name of either Frank, Francis, or Francisco, you can type Fran. You cannot use the wildcard symbol (*) in your search.

4. Optionally, from the fourth list, select **and** to search by two criteria. Select **or** to search by either one criterion or another.

   A second row of lists appears from which you can select the second criterion.

   You can continue to refine your search this way, entering a maximum of up to five criteria.

5. When you finish, click **Search**. Your search results appear in the agents table.

6. If you are not satisfied with the search results, or if you want to start a new search, from the fourth list in the first search row, select the blank value to clear all entered search criteria.

Searching for agents by skillset

Before you begin

🛈 **Important:**

You can search for a maximum of five skillsets. You can search only among those skillsets in the partitions assigned to you.

- Log on to CCMA. For more information, see [Logging in to Contact Center Manager Administration for Management](#) on page 164.
- Open the Contact Center Management component.

About this task

When you need to quickly locate all agents on a server either assigned to a skillset, in Standby for a skillset, or not assigned to a particular skillset, you can use the skillset search feature of Contact Center Management. You can use this feature in the Agent to Skillset Assignment window in Assignment view of Contact Center Management. This feature is particularly useful when you notice high contact volume for a skillset. You can locate all agents who are in Standby mode for the skillset so that you can assign them to handle the excess contacts.

✳ **Note:**

If you have access to the Network Agent Admin view and depending on your access level in Contact Center Management, you can search for agents based on skillset assignment across multiple servers.

Procedure

1. In the Agent to Skillset Assignment window, click **List Available Skillsets**.

   The heading expands to show a table listing all the skillsets not currently included in the assignment.

2. Beneath this table, click **Skillset Search**.

3. From the search boxes, choose the skillsets that you want to search for, up to a maximum of five.

4. After you choose your criteria, click **Search**.

   The agents that match your search criteria appear in a new table.

5. Note the Logged In agents, and then select the check box for each agent to add to the assignment.

6. Click **Update Table**.

   The agents appear in the Assignment Details table.

7. To search for agents by more than one skillset, from the last list, select **and**, select the new skillset and skillset status, and then click **Search**.

   Agents assigned to all of the specified skillsets appear in a new table.

8. To search for agents by one skillset out of a number of skillsets that you specify, from the last list, select **or**, select the new skillset and skillset status, and then click **Search**.

   Agents assigned to at least one of the specified skillsets appear in a new table.

9. To search for agents who are either in Standby mode for a skillset or not assigned to the skillset, from the first list, select the skillset, from the second list, select Standby, and from the last list, select **or**. From the first list in the second row, select the same skillset, from the second list, select **Not Assigned**, and then click **Search**.

   Agents who are either in Standby mode or not assigned to the skillset appear in a new table.

Searching for agents by supervisors

Before you begin

- Log on to CCMA. For more information, see [Logging in to Contact Center Manager Administration for Management](#) on page 164.
- Open the Contact Center Management component.

About this task

You can use this window to search for agents assigned to or not assigned to a particular supervisor.

Procedure

1. On the menu, choose **View/Edit** > **Supervisors**.

2. In the left pane, select a server on which to search for agents.

3. In the expanded list, select a supervisor.

   A list of agents assigned to the selected supervisor appears in the right pane.

4. Click the **Assign Agents** heading.

   The heading expands, and a series of search boxes appear.

5. Select the **Search by Supervisors** option.

6. From the first list, select **Assigned** to search for agents assigned to a particular supervisor

   OR

   Select **Not Assigned** to search for agents not assigned to a particular supervisor.

7. From the second list, select the supervisor.

8. To search for agents assigned to (or not assigned to) additional supervisors, from the third list select **and**. You can search for agents assigned to (or not assigned to) up to three supervisors.

9. Click **Search**.

   Agents that match your search criteria appear in a new list.

Searching for agents across multiple servers

Before you begin

- Log on to CCMA. For more information, see [Logging in to Contact Center Manager Administration for Management](#) on page 164.
- Open the Contact Center Management component.

About this task

In Network Agent Admin view, you can search for specific agents across multiple servers. When you find the agents, you can view their skillset assignments, change skillset priority levels, and view or edit agent details.

Procedure

1. In the Contact Center Management window, on the menu, choose **View/Edit** > **Network Agent Admin**.

2. In the **Server** table, select the check box for each server on which to search.

   To search on all servers, select the **Select All** check box.

3. Select the **Network Agent Search** option.

   Agent search boxes appear.

4. From the first list, select the criterion by which to search.

5. From the second list, select **Starts With**, **Contains**, or **Is Equal To**.

   If you search by agent login status, then the second and third boxes are not enabled.

6. In the third box, type the value to search for, or type a partial value. For example, to search for agents with the first name of either Frank, Francis, or Francisco, you can type Fran. You cannot use the wildcard symbol (*) in your search.

7. In the fourth box, select valid values, if required to complete the search.

8. Click **Search**.

   The results of your search appear in the agents table.

9. To start a new search, from the fourth list, select the blank value to clear all entered search criteria.

Searching for agents by skillset across multiple servers

Before you begin

- Log on to CCMA. For more information, see Logging in to Contact Center Manager Administration for Management on page 164.

- Open the Contact Center Management component.

About this task

In Network Agent Admin view, you can search for specific agents across multiple servers. When you find the agents, you can view their skillset assignments, change skillset priority levels, and view or edit agent details.

Procedure

1. In the Contact Center Management window, on the menu, choose **View/Edit** > **Network Agent Admin**.

2. In the **Server** table, select the check box for each server on which to search.

3. To search on all servers, select the **Select All** check box.

4. Click the **Network Skillset Search** heading.

   Agent to Skillset Assignment search boxes appear.

5. From the first list, select the criterion by which to search.

6. From the boxes, choose the skillsets to search for, up to a maximum of five.

7. Click **Search**.

   The agents that match your search criteria appear in a new table.

Chapter 33: Skillsets

A skillset is a group of abilities necessary to answer a specific type of contact. Skillsets are the basic building blocks of skill-based routing. Use skillsets to match a caller with the agent who can best meet the caller's needs.

In the Skillsets view, you can create new ad-hoc agent-to-skillset assignments and change the priority of skillsets already assigned to agents. Click View/Edit, Skillsets to change the system tree to the skillset view. Then select a server in the system tree to log on to the server and work with the configured skillsets and agents.

When you click a skillset in the system tree, the Skillsets window appears, listing the agents who are currently assigned to the skillset and the priority for that skillset.

Based on the access class that you are assigned, the data that you can see and the procedures that you can perform in the Skillsets view vary.

If you have View access to Agent Properties, then you can use this window to view the agents assigned to the currently selected skillset (only those agents in your partition, and your reporting agents). You can also view each agent's priority for the skillset.

If you have at least Edit access to Agent Properties, then you can use this window to quickly assign new agents to the currently selected skillset (only those agents in your partition, and your reporting agents), or to change the priority of agents assigned to this skillset. You can use the search feature in this window to find new agents to assign to the skillset.

Creating a skillset assignment

Before you begin

- Log on to CCMA. For more information, see Logging in to Contact Center Manager Administration for Management on page 164.
- Open the Contact Center Management component.
- Ensure that you understand Reset Assignments. For information, see Creating a reset assignment on page 204.
- Ensure that you have the Schedule Assignments access level for Skillset Assignments. If you are unsure, contact the administrator.

About this task

Create agent-to-skillset assignments to temporarily assign agents to different skillsets when agents are on breaks, are sick, are on vacation, or are on a course and to schedule future contact

center configurations (for example, in response to planning through a work force management tool).

Procedure

1. In the Contact Center Management window, on the menu, choose **View/Edit** > **Assignments**.

2. In the left pane, expand the server on which to assign agents to skillsets.

3. Right-click the **Agent Skillset Assignments** folder, and then click **Add Assignment**.

4. In the New Agent to Skillset Assignment window, in the **Assignment Details** area, click the **List Available Agents** heading to search for agents to add to the assignment.

   You can search for agents by first name, last name, department, comment, or login ID. You can also search by the current agent login status (Logged In or Logged Out).

5. Enter your search details up to a maximum of five different criteria.

6. Click **Search**. The agents that match your criteria appear in a table. If you search by login status, you can search by this one criterion only.

7. To list all agents configured on the server (your partitioned agents and any agents in the reporting agent combinations assigned to you), click **List All**.

8. In the **Available Agents** table, note the agents logged on, and then select the check box for each agent to include in the assignment.

9. Click **Update Table**.

   The agents with their currently assigned skillsets appear in the Assignment Details table.

10. To remove an agent from the Assignment Details table, select the agent to remove and click **Remove Agent**.

11. To reset the Assignment Details table to the last saved configuration, click **Reset Assignment Details**.

12. To add new skillsets to the table, click the **List Available Skillsets** heading.

    > ❗ **Important:**
    >
    > You can use this function to change only those skillsets that currently have priority values assigned, or all skillsets if that option is selected.

13. In the **Available Skillsets** table, select the check box for each skillset to add to the assignment.

14. Click **Update Table**.

    The skillsets appear in the Assignment Details table.

15. To add agents assigned to a particular skillset to the assignment, click **Skillset Search**. The heading expands to show a series of search boxes.

16. From the boxes, choose the skillsets to search for, up to a maximum of five levels.

17. Click **Search**. The agents that match your search criteria appear in a table.

18. Select the check box for each agent to add to the assignment, and then click **Update Table**.

    The agents appear in the Assignment Details table.

19. In the **Assignment Details** table, from the skillset lists, select the skillset priority level. You can choose from 1 to 48, or Standby, and then press **Tab**.

20. Click the **Save/Schedule Assignments** heading.

    The heading expands to show a series of boxes.

21. In the **Skillset Search** box, type a unique name for the assignment.

22. To create a reset assignment, select the **Create Reset Assignment** check box.

23. Click **Save** to save the reset assignment before altering the original assignment.

24. Click **Save Assignment** to save the assignment in the **Assignments** folder.

Chapter 34: Assignments

In the Assignments view of Contact Center Management, you can create, view, and edit agent-to-skillset and agent-to-supervisor assignments. To run saved and scheduled assignments immediately, use the Run Now feature.

Assignment types

You can create two types of assignments in Contact Center Management:

- agent-to-supervisor assignments
- agent-to-skillset assignments

Agent-to-supervisor assignments

You can create agent-to-supervisor assignments to temporarily assign multiple agents to a different supervisor when supervisors are on breaks, are sick, are on vacation, or are taking a course.

Agent-to-skillset assignments

You can create agent-to-skillset assignments to temporarily assign agents to different skillsets when agents are on breaks, are sick, are on vacation, or are on a course.

Reset assignments

When you create a scheduled agent-to-supervisor assignment or an agent-to-skillset assignment in the Assignments view, you can create a reset assignment. A reset assignment is a record of the original data that existed at the time you created the assignment. For example, it contains a record of the original list of agents assigned to a supervisor before you modify an agent-to-supervisor assignment.

You can use a reset assignment to change and run the assignment as many times as you require, and then run the reset assignment to return conditions to their original state. This feature is particularly useful when you create an assignment to cover agent or supervisor breaks, and then want to return conditions to their normal state when the agent or supervisor returns to work.

You can modify a reset assignment just as you modify any other assignment.

Saving assignments

You cannot save multiple assignments simultaneously. If another user is saving an Agent-to-Supervisor or Agent-to-Skillset assignment, you cannot run your assignment save. If an

assignment save is attempted while another assignment save is in progress, an error message is displayed on CCMA informing the user that another save is in progress and to try again soon.

Agent-to-supervisor assignment scenarios

The following scenarios provide some examples of when to create agent-to-supervisor assignments.

Example 1: Supervisor is sick

Pat Wilson, one of Best Air's supervisors, calls in sick for the day. The contact center manager creates and saves an agent-to-supervisor assignment and a reset assignment that lists all of the agents assigned to Pat. The manager schedules the reset assignment to run the following day. The manager then modifies the agent-to-supervisor assignment to assign half of Pat's agents to Chris Konings, and the other half to Cindy Wong. The manager applies the assignment immediately, which assigns all agents to their temporary supervisors for the day. When the reset assignment runs, the system reassigns all agents back to Pat.

Example 2: Supervisor is on vacation

Pat booked vacation from August 17-28. The contact center manager creates and saves an agent-to-supervisor assignment and reset assignment that lists all of the agents assigned to Pat. The manager schedules the reset assignment to run August 28 at 5:00 p.m. The manager then modifies the agent-to-supervisor assignment to reassign Pat's agents and schedules it to run August 17. When the reset assignment runs, the system reassigns the agents back to Pat.

Example 3: Supervisor is on regularly scheduled training

At Best Air, all supervisors must participate in regular upgrading. Every four weeks, the supervisor must spend half a day in training. Training sessions are staggered to ensure adequate supervision of the contact center. Pat's training occurs every third Thursday of the month. The contact center manager sets up an agent-to-supervisor assignment that automatically reassigns Pat's agents for that time.

Agent-to-skillset assignment scenarios

The following scenarios provide some examples of when you create agent-to-skillset assignments.

Example 1: Agents are sick

Mark Schultz, an agent in Best Air's Cargo Tracing skillset, is sick and absent from work today. This leaves the Cargo Tracing skillset understaffed, particularly for the period from 10:00 a.m. to 4:00 p.m., the skillset's busiest time. The contact center manager creates and saves an agent-to-skillset assignment and reset assignment that lists Rose Stefanopolis as one of the agents. The manager then modifies the agent-to-skillset assignment to assign Rose Stefanopolis (an agent who worked in this skillset before) to the Cargo Tracing skillset. The manager runs the agent-to-skillset assignment immediately, and Rose is automatically reassigned. When Mark

returns to work the following day, the manager runs the reset assignment to reassign Rose to her normal skillset.

Example 2: Shifts

During the early morning and evening periods, few agents are available. As a result, many skillsets are understaffed. Others, such as the Cargo Tracing skillset, do not go into service until 9:00 A.M., and go out of service at 5:00 p.m. Best Air's contact center manager creates and saves an agent-to-skillset assignment and reset assignment that lists all agents that are assigned to the Cargo Tracing skillset. The manager modifies the agent-to-skillset assignment to assign the agents to Bookings and schedules it to run during early morning and evening periods.

Canceling a scheduled assignment

Before you begin

- Log on to CCMA.

- Open the Contact Center Management component.

About this task

You can cancel a scheduled agent to skillset assignment or a scheduled agent to supervisor assignment. When you cancel the schedule, the assignment is still saved for future reference.

Procedure

1. From the **View/Edit** menu, choose **Assignments**.

2. In the left pane, click the server containing the scheduled assignment to cancel.

3. Select the **Agent Skillset Assignments** folder or the **Agent Supervisor Assignments** folder.

   The list of assignments appears.

4. Click the scheduled assignment to cancel.

5. In the **Save/Schedule Assignments** section, from the **Schedule Type** list, select **Not Scheduled**.

6. Click **Schedule** to cancel the schedule.

   The assignment is cancelled and remains in the Assignments folder.

Creating a reset assignment

Before you begin

- Log on to CCMA.

- Open the Contact Center Management component.

About this task

When you create a scheduled agent-to-supervisor assignment or an agent-to-skillset assignment in the Assignments view, you can create a reset assignment. A reset assignment is a record of the original data that existed at the time you created the assignment. For example, it contains a record of the original list of agents assigned to a supervisor before you modify an agent-to-supervisor assignment.

You can use a reset assignment to change and run the assignment as many times as you require, and then run the reset assignment to return conditions to their original state. This feature is particularly useful when you create an assignment to cover agent or supervisor breaks, and then want to return conditions to their normal state when the agent or supervisor returns to work.

Example:

Supervisor Pat Jones takes a lunch break every day from 12:00 p.m. to 1:00 p.m. You want to reassign Pat's agents to Mike Smith every day from 12:00 p.m. to 1:00 p.m. To do so, follow these steps:

> ⓘ **Important:**
>
> If you delete the assignment, the system deletes the corresponding reset assignment.

Procedure

1. Create an agent-to-supervisor assignment that lists all of the agents assigned to Pat.

2. Enter a name for the assignment, such as Lunchbox.

3. Select the **Create Reset Assignment** check box, and then click **Save Assignment**. When you create a reset assignment, the system saves it with the same name as the original assignment, but adds two underscores (__) at the end of the name. If you save the assignment as Lunchbox, the reset assignment name is Lunchbox__.

4. Modify the Lunchbox assignment to reassign Pat's agents to Mike and schedule it to run at 12 noon every day.

5. Schedule the Lunchbox__ reset assignment to run every day at 1:00 p.m., thereby reassigning all Pat's agents back to Pat when she returns from her lunch break.

Creating a supervisor assignment

Before you begin

- Log on to CCMA.

- Open the Contact Center Management component.

- Ensure that you understand Reset Assignments. See <u>Creating a reset assignment</u> on page 204.

About this task

You can schedule a supervisor assignment to reassign agents when supervisors are unavailable for some reason, for example break time or vacation.

Procedure

1. In the Contact Center Management window, on the menu, choose **View/Edit** > **Assignments**.

2. In the left pane, expand the server on which to assign agents to skillsets.

3. Right-click the **Agent Supervisor Assignments** folder, and then click **Add Assignment**.

4. In the New Agent to Supervisor Assignment window, in the **Assignment Details** area, click the **List Available Agents** heading to search for agents to add to the assignment.

   The heading expands to show the agent search boxes.

   You can search for agents by first name, last name, department, comment, or login ID. You can also search by the current agent login status (Logged In or Logged Out).

5. Enter your search details up to a maximum of five different criteria.

6. Click **Search**.

   The agents that match your criteria appear in a table.

   If you search by login status, you can search by this one criterion only.

7. To list all agents configured on the server (your partitioned agents and any agents in the reporting agent combinations assigned to you), click **List All**.

8. In the **Available Agents** table, note the agents logged on, and then select the check box for each agent to include in the assignment.

9. Click **Update Table**.

   The agents with their currently assigned supervisors appear in the Assignment Details table.

10. Click the **Save/Schedule Assignments** heading.

11. In the **Save Assignment as** box, type a unique name for the assignment.

12. Select the **Create Reset Assignment** check box to create a reset assignment.

13. Click **Save** to save the reset assignment before altering the original assignment.

14. Click **Save Assignment** to save the assignment in the Assignments folder.

Running an assignment immediately

Before you begin

- Log on to CCMA.
- Open the Contact Center Management component.
- Create at least one skillset or supervisor assignment.

About this task

When you create and save an agent to skillset or agent to supervisor assignment in Contact Center Management, you can run it immediately by using the Run Now option. You can use this option to run saved assignments or scheduled assignments immediately.

You cannot run the same agent skillset assignment concurrently. You must wait until the assignment completes before you run it again. This prevents a potential CCMA performance impact.

When you click Run Now to run a scheduled assignment immediately, the schedule still applies and the assignment is still run at the scheduled time.

If you make any changes to the assignment, you must first click Save Assignment before clicking Run Now. If you do not click Save Assignment, then the assignment runs without the changes you have made.

When you run an assignment immediately, the Run Now button is temporarily disabled while the assignment runs. CCMA displays a message while the assignment is running, and when it completes.

Procedure

1. In Contact Center Management, on the menu, choose **View/Edit** > **Assignments**.

2. In the left pane, click the server containing the assignment that you want to run.

3. Select the folder containing the saved or scheduled assignment that you want to run.

4. If you do not want to review the assignment details before running it, and you are sure of the assignment name, in the left pane, right-click the assignment name, and then click **Run Now**.

   The assignment runs immediately.

   OR

   Click the assignment.

   The assignment details appears in the right pane.

5. Review the assignment details in the assignment table and make any changes, if necessary.

6. If you make any changes to the saved or scheduled assignment, or if you schedule the assignment, click **Save Assignment**.

7. Click **Run Now**.

   The assignment runs immediately.

Assigning agents to skillsets

Before you begin

- Log on to CCMA. For more information, see [Logging in to Contact Center Manager Administration for Management](#) on page 164.

- Open the Contact Center Management component.

- Ensure that you have access to the required skillsets. If you are unsure, contact the administrator.

  > 🛈 **Important:**
  >
  > The maximum number of skillsets you can assign to an agent is 150.

About this task

When you immediately assign one or more agents to a skillset without scheduling the assignment, you create an ad hoc assignment. Before you can assign an agent to a skillset, the agent's profile must exist on the server. For more information about adding new agents, see [Adding an agent](#) on page 172.

> ✳ **Note:**
>
> If you unassign all agents from a skillset, the skillset is taken out of service.

Procedure

1. In Contact Center Management, on the menu, choose **View/Edit** > **Skillsets**.

2. In the left pane, click the server on which to work with agents and skillsets.

3. Select a skillset.

   A list of agents assigned to the skillset appear in the right pane.

4. From the **Priority** list, select the new priority level.

5. To remove the skillset from the agent, select **Unassigned**.

6. To put the agent in Standby mode for this skillset, select **Standby**.

7. Click the **Assign Agents** heading to assign a new agent to this skillset.

   The search feature appears.

8. To list all agents configured on the selected server (only those agents in your partition and your reporting agents), click **List All**.

9. From the search lists, choose the criteria for your search.

   You can search for agents by first name, last name, department, comment, login ID, or a combination of any of these criteria. You can also search by current login status (either Logged In or Logged Out).

10. Click **Search** to return agents matching your criteria in a table.

    Only agents having the correct contact type for the skillset selected are returned.

11. From the **Priority** list, select the priority level for each agent to assign to this skillset.

12. To assign multiple agents to the same skillset priority at once, from the **Set all Skillsets by priority** list, select the priority level, and then click **Apply**.

13. Click **Submit** to assign the agents to the skillset.

    The agents appear in the Assigned Agents table.

Assigning agents to supervisors

Before you begin

- Log on to CCMA.
- Open the Contact Center Management component.

About this task

To reassign agents when supervisors go on break or on vacation, you can immediately assign agents to new supervisors.

Procedure

1. On the menu, choose **View/Edit** > **Supervisors**.

2. In the left pane, click the server on which you want to work with supervisors and agents.

3. Click the supervisor to whom the agent is currently assigned.

    The supervisor icon expands to show all the assigned agents.

4. From the list of agents, left-click the agent who you want to reassign to another supervisor and, without releasing the mouse button, drag the agent icon over the new supervisor icon until the supervisor icon changes color.

5. Release the left mouse button to reassign the agent to the new supervisor.

Copying an assignment

Before you begin

- Log on to CCMA.
- Open the Contact Center Management component.
- Ensure that you understand Reset Assignments. See Creating a reset assignment on page 204.

About this task

To copy an existing assignment that you have created and saved in the Assignments folder, you must type a new assignment name and save the assignment.

If the assignment is scheduled, you must also click Schedule to activate the new schedule for the assignment.

Procedure

1. From the **View/Edit** menu, select **Assignments**.

2. In the left pane, click the server containing the assignment to copy.

3. Select the **Agent Skillset Assignments** folder.

   OR

   Select the **Agent Supervisor Assignments** folder.

   The list of assignments appears.

4. Click the assignment to copy.

5. In the **Save/Schedule Assignments** section, in the **Save Assignment As** box, type the new name of the assignment.

   ❶ Important:

   This name must be unique.

6. To create a reset assignment, select the **Create Reset Assignment** check box.

7. Click **Save Assignment** to save the assignment.

   A copy of the assignment appears in the Assignments folder. A message appears, notifying you that the assignment successfully saved.

8. If you scheduled the assignment, click **Schedule** to activate the scheduled assignment.

Deleting an assignment

Before you begin

- Log on to CCMA.

- Open the Contact Center Management component.

   ❶ Important:

   When you delete an assignment, the system deletes the corresponding reset assignment. You can, however, delete a reset assignment and keep the original assignment. You cannot retrieve an assignment once it is deleted. Instead, you must create the assignment again.

About this task

You can delete agent to skillset assignments and agent to supervisor assignments.

Procedure

1. In the Contact Center Management window, on the menu, choose **View/Edit** > **Assignments**.

2. In the left pane, click the server containing the assignment to delete.

3. Select the **Agent Skillset Assignment** folder.

   OR

   Select the **Agent Supervisor Assignment** folder.

   The list of assignments appears.

4. In the left pane, right-click the assignment to delete, and then click **Delete Assignment**.

5. In the message box that appears asking you to confirm your choice, click **Yes**.

   The system deletes the assignment and the corresponding reset assignment.

Viewing a scheduled assignment

Before you begin

- Log on to CCMA.

- Open the Contact Center Management component.

About this task

Based on the access class that you have for assignments, and the servers upon which your access class is configured, in this window, you can view the schedules of agent-to-skillset and agent-to-supervisor assignments created and saved by all users across all servers in the network. You can also view details about the scheduled assignment, such as the name, type, the server on which it is run, and details about the schedule time.

You must have View Assignments access for both agent-to-skillset assignments and agent-to-supervisor assignments to see both of these types of assignments in this window. If you have access to only one of these types of assignments, then you can only see the schedules for this type of assignment. Likewise, you can see only those assignments scheduled on the servers on which your access class is configured.

With Schedule Assignments access, however, you can also use this window to delete the schedules of the assignments listed, leaving the assignments intact on the server. If you have the View Assignments access or less, however, you cannot delete schedules, you can only view the assignments.

Procedure

1. On the menu, choose **View/Edit** > **Assignments**.

2. In the left pane, click the **Scheduled Events** folder.

The Scheduled Events window opens, listing all scheduled assignments to which you have access on the servers included in your access class.

Part 3: Access and Partition Management

Chapter 35: Access and Partition Management fundamentals

You can use the Access and Partition Management component to create Contact Center Manager Administration users and to assign to users appropriate access privileges to the system. CCMA users can log on and use the CCMA components to which they have access. You can control user access privileges by assigning Launchpad options, access classes, and partitions, including reporting agent combinations.

You can use Access and Partition Management to add, edit, view, or delete:

- access classes
- report groups (you cannot edit report groups)
- standard partitions
- user-defined partitions
- Contact Center Manager Administration users

If you are removing and then adding a previously configured Contact Center Manager Server to your Contact Center Manager Administration, you must perform extra steps to ensure that all of the configured data is available when you add the server.

- Ensure the host name of the Contact Center Manager Server can be resolved to an IP address.
- Under **User Details** > **Partitions** > **Standard and Reporting Agents**, select Configure for the added Contact Center Manager Server. Click **Submit** to add the user details.

Chapter 36: Access and Partition Management configuration

You can use the Access and Partition Management component to create Contact Center Manager Administration users and to assign to users appropriate access privileges to the system.

Prerequisites to Access and Partition Management procedures

- Log on to Contact Center Manager Administration as an administrator or as a user with sufficient access levels (access class) to use the Access and Partition Management component.
- Ensure that you have a thorough understanding of Access and Partition Management.

Logging on to Contact Center Manager Administration Access and Partition Management

Before you begin

- Install and commission Contact Center Manager Administration.
- Ensure that you have access to Access and Partition Management.

About this task

Log on Contact Center Manager Administration to configure and administer your Contact Center Manager Server.

Complete this procedure to access the Access and Partition Management component.

Procedure

1. Start Microsoft Edge with IE mode.

2. In the **Address** box, type the URL of the 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.

If your site does not use the default port for Internet Information Services (IIS), the URL of the server is `https://<server name>:<port number>`, where **<server name>** is the computer name of the Contact Center server, and **<port number>** is the port for the CCMA site in IIS. For example, `https://ccserver:81`.

> ❗ **Important:**
>
> You must log on using the Contact Center server name. Do not use the server IP address.

3. In the **User ID** box, type your user ID.

4. In the **Password** box, type your password.

5. Click **Login**.

   If configured in the security settings, CCMA displays the date and time of your last login and the number of failed login attempts since your last successful login.

6. Click **Access and Partition Management**.

Chapter 37: Access classes

You can use access classes to control the actions that users can perform in the Contact Center Management, Real-Time Reporting, Historical Reporting, Prompt Management, Configuration, Scripting, and Access and Partition Management components.

Access classes and servers

If you work in a multiple Contact Center Manager Server environment, each access class that you create spans multiple servers. However, to configure and manage the access classes you need to log on to only one server—the Contact Center Manager Administration server, where access classes are stored.

The following diagram shows a simple network configuration for Contact Center Manager Administration. When you log on to the Contact Center Manager Administration server from a client workstation, you can use the Access and Partition Management component to configure access classes for the Contact Center Manager Servers, and for the Network Control Center (NCC) server.
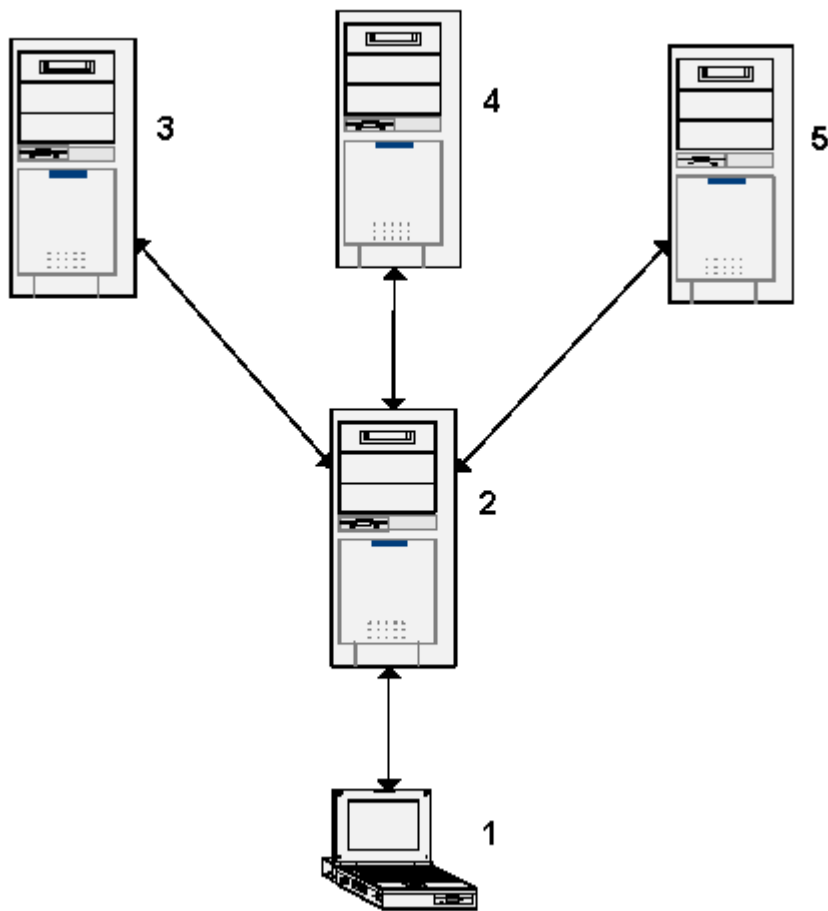
Figure 1: Network configuration

1	Client workstation
2	Contact Center Manager Administration server
3	Network Control Center server
4	Contact Center Manager Server
5	Contact Center Manager Server

Each access class that you create spans all servers in the network, even if you select no access class elements on a particular server. For example, in the preceding network scenario, you create an access class that contains Configuration access elements only on the NCC server, and you assign it to a user. By specifying no access elements on any other server in the network, you limit the user's actions on all servers, not only on the NCC server. This user does not have access to any of the Configuration elements on either Contact Center Manager Server; the user can perform only the actions included in the access class to configure the NCC server.

If the user needs to configure either server in Contact Center Manager Server, you must edit the user's access class to include access rights on the other servers.

When you grant a user access privileges that span multiple servers, the user needs only to log on to one server—the application server—to access all servers included in the access class. Users no longer need to log on to each server to which they have access.

Creating an access class

Before you begin

- Log on to CCMA. For more information, see Logging on to Contact Center Manager Administration Access and Partition Management on page 215.
- Open the Access and Partition Management component.
- Ensure that you know what access levels you want to assign to users.

About this task

Create an access class to control the actions that the user can perform in the following Contact Center Manager Administration components:

- Contact Center Management
- Configuration
- Historical Reporting
- Real-Time Reporting
- Scripting
- Access and Partition Management (under the default Administration server)
- Call Recording and Quality Monitoring
- Prompt Management

Access classes do not apply to the Audit Trail, Outbound, or Multimedia components. To perform functions in these components, users require only Launchpad option rights to the components.

Procedure

1. On the menu, choose **Add** > **New Access Class**.

2. In the New Access Class window, in the **New Access Class Name** box, type the name of the new access class.

   Use a descriptive name for the user type having this access level, or the type of privileges available at this access level.

3. Click **Submit**.

4. In the left pane, click the new access class.

   The name expands to reveal the list of servers in your network.

5. Click the server on which to create the access class.

   The server access class elements appear in the Access Class Properties window.

You can create an access class that spans all servers in your network (if you work on a network), but you must choose the access class properties on one server before selecting the next server.

6. From the list of access class elements, select the access levels for the elements that you want to make available to this access class.

7. Click **Submit** to save your choices on the current server.

8. Repeat step 5 on page 219 to step 7 on page 220 for each server that you want this access class to have.

9. Click **Submit** to save the new access class.

Editing an access class

Before you begin

• Log on to CCMA. For more information, see Logging on to Contact Center Manager Administration Access and Partition Management on page 215.

• Open the Access and Partition Management component.

• Create an access class. See Creating an access class on page 219.

About this task

Edit an access class to change any configured access class property except the access class name. To change the access class name, you must delete the access class and create a new access class with a new name.

Procedure

1. On the menu, choose **View/Edit** > **Access Classes**.

2. In the left pane, click the access class to edit.

   The access class name expands to reveal the servers in your network.

3. In the left pane, expand the server on which to edit the access class.

   You can add a server to an existing access class by clicking the server in the system tree and then choosing the access levels for each element. You can create an access class on multiple servers, but you must choose the access class properties on one server before selecting the elements on the next server.

4. In the right pane, from the list of access class elements, select the access levels for the elements to make available to this access class.

5. Repeat step 3 on page 220 to step 4 on page 220 for each of the servers and levels that you want this access class to have.

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

Assigning an access class to a user

Before you begin

- Log on to CCMA.

- Open the Access and Partition Management component.

- Create an access class.

- Create a Contact Center Manager Administration user.

About this task

For each component controlled by access classes, you must assign at least one access privilege to the user, or the user cannot work in the component.

If the user has basic access to Contact Center Management, you must assign the user an access class that includes CCM access, Skillset Assignment access, or Supervisor Assignment access. If you assign the user an access class without at least one of these privileges, then the user cannot work in Contact Center Management.

If the user has basic access to Historical Reporting, you must assign the user an access class that includes either Run and Import access or Report Creation access. If you assign the user an access class without either of these access levels, then the user cannot work in Historical Reporting.

If the user has basic access to Real-Time Reporting, you must assign the user an access class that includes either Launch access, Create Private access or Create Public access for either the tabular or graphical displays (or both). If you assign the user an access class without at least one of these access levels, then the user cannot work in Real-Time Reporting.

If the user has basic access to Configuration, you must assign the user an access class to the user that includes at least one of the Configuration access class elements, such as skillsets. If you assign the user an access class without at least one of these privileges, the user cannot work in Configuration.

If the user has basic access to Scripting, you must assign the user an access class that includes privileges in at least one of the following Scripting components: Scripts, Script Variables, or Application Thresholds.

If you assign the user an access class without privileges in at least one of these components on at least one server, the user cannot work in Scripting.

If the user has basic access to Prompt Management, you must assign the user an access class that includes at least one of the Prompt Management access class elements, such as Read Update Create/Delete or Read and Update. If you assign the user an access class without at least one of these privileges, the user cannot work in Prompt Management.

If you assign a user to multiple access classes, Contact Center grants the highest level of access from the combined access classes to the user.

Procedure

1. On the menu, choose **View/Edit** > **User Administration**.

2. Select the user for whom you want to assign an access class.

3. Click the **Access Classes** heading.

   The list of configured access classes appears.

4. Select the check box for each access classes to assign to the user.

5. To assign all access classes, select the **Select All** check box.

6. To remove all access classes from the user, clear the **Select All** check box.

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

Viewing the users assigned to an access class

Before you begin

- Log on to CCMA.

- Open the Access and Partition Management component.

About this task

View the users assigned to an access class to see a list of Contact Center Manager Administration users assigned to the access class and access and partition details for each user.

This information is read-only; you cannot assign or unassign access classes in this window. For information about assigning and unassigning access classes, see Assigning an access class to a user on page 221.

Procedure

1. On the menu, choose **View/Edit** > **Access Classes**.

2. In the left pane, select the access class to view the list of assigned users.

3. In the Access Class Members window, click the **Members** heading.

   The list of users currently assigned to the access class appears in a table.

4. To sort the list of access class members alphabetically, click the **Members Name** heading.

5. To view the access and partition details for a user, click the user.

Deleting an access class

Before you begin

- Ensure that the access class has no members or that the existing members of the access class no longer require its access privileges.

- Log on to CCMA.

- Open the Access and Partition Management component.

About this task

Delete an access class to remove it from Contact Center Manager Administration.

Procedure

1. On the menu, choose **View/Edit** > **Access Classes**.

2. In the left pane, right-click the access class to delete, and then click **Delete**.

3. In the message box that appears asking you to confirm your choice, click **Yes**.

Chapter 38: Report groups

Two categories of report groups are available in Historical Reporting:

- Public report groups—These report groups contain the standard public report templates. The public report groups are:

  - Agent Performance

  - Call-by-Call

  - Configuration

  - Contact Summary

  - Multimedia

  - Networking

  - Outbound

  - Others

  - NCC (on the NCC only)

    > **Important:**
    >
    > The available reports depend on your feature set.

- User-defined report groups—These report groups contain the report templates that users belonging to the group customized and want to share with other members of the report group. The user-defined report groups that you create in this window are for use in Historical Reporting. You can assign any unique name to these groups.

Public report groups versus user-defined report groups

Unlike the public report groups that contain all of the standard templates, user-defined report groups contain no standard templates. The user-defined report groups that you create in Access and Partition Management are folders for Historical Reporting users who belong to the same group to share their customized reports. Users can customize a standard template and save it in their group folder so that other group members can use the same custom report.

You can create user-defined report groups to reflect each department in your Contact Center, such as the Sales Group or the Marketing Group. If you configure a shared Contact Center, you can also create separate groups for each company sharing the Contact Center, such as the Best

Air Group and the Econo Air Group. In this way, you can keep customized reports that contain company information separate from other companies in the same Contact Center.

The data shown in each report is based on the partitions assigned to the user and the selection criteria the user applies to the report.

You can use report groups to grant a user access to a very limited number of reports. For example, if you do not want to give a user access to any of the standard report templates, you can create a user-defined report group and add it to the partition assigned to the user. When the user opens Historical Reporting, they see only the user-defined report group folder, and can only see reports that other members of the group saved in the group folder.

After you create a report group, you can add it to a partition created under the same server as the report group. Then you can assign the partition to the users belonging to the report group. When these users log on to Contact Center Manager Administration, they see the report group name in Historical Reporting under the server where you created it.

Assign standard report groups to a user in the same way as standard partitions. There is no requirement to create and maintain a user-defined partition. The standard partition "All User Defined Report Groups" can also be assigned to a user on a per-sever basis. This allows the user access to any user-defined report groups created on that server.

Creating a report group

Before you begin

- Log on to CCMA. For more information, see Logging on to Contact Center Manager Administration Access and Partition Management on page 215.
- Open the Access and Partition Management component.

About this task

Create a report group to create a custom group to reflect a specific department in the Contact Center, such as the Sales Group or the Marketing Group. You can also create separate groups for each company sharing the Contact Center. In this way, custom reports that contain company information can be kept separate from other companies in the same Contact Center.

You can use report groups to grant a user access to a limited number of reports. For example, if you do not want to grant a user access to any standard report templates, you can create a custom report group and add it to the partition assigned to the user. When the user opens Historical Reporting, the user sees only the custom report group folder. The user can see reports only that other members of the group save in the report group folder.

After you create a report group, you must add it to a partition created under the same server as the report group. Then you must assign the partition to the users belonging to the report group. When these users log on to Contact Center Manager Administration, they see the report group name in Historical Reporting under the server where you created it. If you create a report group under one server, but include it in a partition created under a different server, the user does not see the report group in Historical Reporting.

Procedure

1. On the menu, choose **Add** > **New Report Group**.

2. In the Report Group Properties window, in the **Report group name** box, type the name of the new report group.

   Use a descriptive, unique name for the user types assigned to this group or the company, or the department the group represents.

3. From the **Create the group under server** list, select the server on which you want to create the report group.

   ❗ Important:

   When you add the report group to a partition, you must configure the partition on the same server on which you create the report group. If you do not configure the partition on the same server, the report group is not visible in Contact Center Manager Administration.

4. Click **Submit** to save the report group.

5. Add the report group to a partition.

Deleting a report group

Before you begin

- Log on to CCMA.
- Open the Access and Partition Management component.

About this task

Delete a report group to remove a custom report group from Contact Center Manager Administration. You cannot delete any of the standard report groups included with Contact Center Manager Administration. However, you can delete the custom report groups that you create in Access and Partition Management.

Procedure

1. On the menu, choose **View/Edit** > **Report Groups**.

   ❗ Important:

   When you delete a report group, you delete all reports that users saved in it. Therefore, before you delete a custom report group, ensure that users who belong to the group do not require any of the custom reports that they saved in the group folder.

2. In the left pane, click the server containing the custom report group to delete.

   The list of report groups appears.

3. Click the report group to delete.

4. In the Report Group Properties window, click **Delete**.

5. In the message box that appears asking you to confirm your choice, click **Yes**.

   The report group and all saved reports are deleted.

Chapter 39: Standard partitions and reporting agents

Partitions restrict the data that users can view in the following components of Contact Center Manager Administration:

- Historical Reporting
- Real-Time Reporting
- Contact Center Management
- Scripting
- Prompt Management

An administrator can use the following ways to partition the data that users see:

- Full data across all servers—When an administrator first creates a user, the user is assigned the Full Data Across All Servers option by default so the user can view all data on all servers. If a new server is added to the system, the user with this level of data access can see all data on that server too.
- Server rights—An administrator can assign a user access to all data or no data on particular servers. To configure standard partitions and reporting agents on a particular server, an administrator must assign the Configure option on that server.

Standard partitions (this includes report groups)—A Standard partition contains all data of a particular type on a particular server. The administrator can assign all data on a per-component basis (only among those components to which the user is granted basic access). For example, the administrator can choose to grant the user access to All agents and All skillsets in both Contact Center Management and Real-Time Reporting on one server only. The administrator can choose from:

- All Agents & Supervisors
- All Skillsets
- All Applications
- All CDNs (Route Points)
- All DNISs
- All Prompts
- All Script Variables

- All User Defined Report Groups

- All standard reports that are shipped with the software on selected servers and selected components

Standard partitions are dynamic, which means that anytime a new data element is added to the system, it is automatically available to the Contact Center Manager Administration user. In this regard, Standard partitions are similar to Reporting Agents. You can assign standard partitions on a per-component basis. For example, the administrator can assign the All Skillsets partition to the Real-Time Reporting component only.

To assign a user a Standard partition on a Contact Center Manager Server, under Partitions, click the Standard & Reporting Agents heading, select the Standards tab, select the Configure option for the server and then select the server from the Configure Server list.

It is possible to assign Standard partitions by component:

- CCM—Contact Center Management

- RTR—Real-Time Reporting

- HR—Historical Reporting

- Scripting—Scripting Component

- PTM—Prompt Management

In the preceding example, all agents and supervisors and all skillsets are assigned to the Contact Center Management and Real-Time Reporting components while only all CDNs (Route Points) are assigned to the Historical Reporting component.

Reporting agents

Use the Reporting Agent feature to dynamically link supervisors and all their reporting agents with one or more Contact Center Manager Administration users, thereby enabling the users to view the agents in Contact Center Manager Administration components, such as Real-Time and Historical Reporting, and Contact Center Management. You assign Supervisor/Reporting agent combinations to Contact Center Manager Administration users by using the Reporting Agents tab in the Standard & Reporting Agents section in the User Properties window of Access and Partition Management.

User types

It is important to know the difference between a Contact Center Manager Server user and a Contact Center Manager Administration user.

User type	User definition	Created in
Contact Center Manager Server user	agents, supervisors, supervisor/agents	Configuration Tool
Contact Center Manager Administration user	anyone who logs on to the Contact Center Manager Administration server and monitors the performance and activities of Contact Center Manager Server using Contact Center Manager Administration; this user can be a supervisor or an administrator	Contact Center Management and Access and Partition Management

After you create a supervisor's Contact Center Manager Server user profile in Contact Center Management (or Configuration Tool), to enable the supervisor to log on to the Contact Center Manager Administration server and use Contact Center Manager Administration, you must also configure a Contact Center Manager Administration user profile for this supervisor.

Users

Supervisors who do not need to use Contact Center Manager Administration do not need a Contact Center Manager Administration user profile; these supervisors require only a Contact Center Manager Server user profile.

When you configure the supervisor's Contact Center Manager Administration user profile, you can create a link between two user profiles (the Contact Center Manager Administration user profile and the supervisor's Contact Center Manager Server user profile) by using the Supervisors tab in the Standard & Reporting Agents area of the Partitions section in Access and Partition Management. Each name on the Supervisors tab represents a supervisor and all of their reporting agents by server. Therefore, when you link a supervisor's name with a Contact Center Manager Administration user, the user can automatically see all the supervisor's reporting agents.

This association is dynamic, meaning that each time a new agent is assigned to the supervisor, the agent is automatically associated with the supervisor's Contact Center Manager Administration user profile.

Use this feature to set up supervisors so they can view all of their own reporting agents, or you can enable one supervisor to see all the reporting agents of another supervisor. The following shows how to configure Reporting agents in Access and Partition Management.

Reporting agents and standard partition example

The company Best Air has two sales departments, Europe and Canada. The two corresponding supervisors for each department are Andrew Engel and Liz Matthews. The administrator creates

two new Contact Center Manager Administration users for the two supervisors and assigns them both the following standard partitions on the server:

- Contact Center Management—All Skillsets

- Real-Time Reporting—All Skillsets

- Historical Reporting—All standard report groups, all CDNs (Route Points), and all DNISs

The administrator assigned this reporting agent configuration for all available components: Contact Center Management, Real-Time Reporting and Historical Reporting. Additionally, each User profile is assigned as a Supervisor/Reporting Agent.

Result in real-time reporting

In Real-Time Reporting (including Filters), Andrew can use all skillsets as he is assigned the All Skillsets standard partition for this component. He can also see any agents reporting to him as he is configured with the supervisor "Andrew Engel" for all components.

Result in historical reporting

In Historical Reporting, Andrew can use all CDNs (Route Points) and DNISs as these standard partitions are assigned to his user properties. He can also use all agents reporting to him. This is true for both selection criteria and filters.

Andrew can also see all of the standard report groups as these are included in his Standard partition configuration.

Result in Contact Center Management

Andrew has access to all skillsets and only the agents that are assigned to him. In the Supervisors view, only one supervisor (himself) is displayed.

For Andrew Engel to view all of Liz's reporting agents, include Liz Matthews in Andrew's user profile (in the Reporting Agents Tab). The administrator can also specify the components to make available to these agents. If only a subset of these agents is required, you can create a user-defined partition and assign it to Andrew's properties. Assigning user-defined partitions is covered in the next section.

Assigning a standard partition to a user

Before you begin

- Log on to CCMA. For more information, see [Logging on to Contact Center Manager Administration Access and Partition Management](#) on page 215.

- Open the Access and Partition Management component.

- Create a Contact Center Manager Administration user.

About this task

You can use partitions to restrict the data that users can view in the real-time displays, historical reports, Prompt Management, Contact Center Management, and Scripting. You can assign standard and user-defined partitions to users in Contact Center Manager Administration. Choose the type that best suits your organization, or choose a combination of both types.

Use standard partitions to assign all data of a particular type on a particular server to the user on a per-component basis. For example, you grant the user access to all agents and all skillsets in both Contact Center Management and Real-Time Reporting on one server only.

Procedure

1. On the menu, choose **View/Edit** > **User Administration**.

2. In the left pane, select the user to whom you want to assign a Standard Partition.

3. In the right plane, click the **Partitions** heading to assign partitions to the user.

   The heading expands to reveal a series of choices.

4. Clear the **Full Data Across All Servers** check box.

5. Click the **Standard & Reporting Agents** heading.

6. In the **Standard & Reporting Agents** area, select one of the following options for each server:

   - No Data—Select this option if you do not want the user to see any data on this server.

   - All Data—Select this option if you want the user to see all configured data on this server.

   - Configure—Select this option if you want to specify the data that the user can see, and then proceed to the next step.

7. From the **Configure Server** list, select the first server to configure.

8. Select the **Standard** tab.

9. On the **Standard** page, select one or more of the following standard partitions:

   - All Agents & Supervisors

   - All Applications

   - All CDNs (Route Points)

   - All User Defined Report Groups

   - All DNIS

- All Prompts

- All Script Variables

- All Skillsets

- Standard Agent Performance Reports

- Standard Call by Call Reports

- Standard Configuration Reports

- Standard Contact Summary Reports (if applicable for the server)

- Standard Network Reports (if applicable for the server)

- Standard Other Reports

- Standard Outbound Reports

- Standard Multimedia Reports

  Only Contact Center Management, Real-Time Reporting, Historical Reporting, Scripting, and Prompt Management are applicable to partitions.

  If the check box for a standard partition is disabled under one of the component headings, then this partition is not applicable for this component. For example, applications are not applicable to Contact Center Management so the All Applications standard partition is disabled for this component.

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

Viewing the users assigned to a partition

Before you begin

- Log on to CCMA.

- Open the Access and Partition Management component.

About this task

View the users assigned to a partition to see a list of Contact Center Manager Administration users assigned to the currently selected partition.

This information is read-only; you cannot assign or remove partitions in this window.

Procedure

1. On the menu, choose **View/Edit** > **User Defined Partitions**.

2. In the left pane, select the partition for which you want to view the list of assigned users.

3. In the Partition Members window, click the **Members** heading.

   The list of users currently assigned to the partition appears in a table.

4. To sort the list of partition members alphabetically, click the **Members Name** heading.

5. To view the access and partition details for a user, click the user.

Editing user properties

Before you begin

- Log on to CCMA. For more information, see [Logging on to Contact Center Manager Administration Access and Partition Management](#) on page 215.
- Open the Access and Partition Management component.

About this task

Edit user properties to change properties such as the password, last name, and first name after you added the user to the database.

You cannot change a user name. Instead, you must delete the user and create a new user with the new user name.

Procedure

1. On the menu, choose **View/Edit** > **User Administration**.

   A list of configured users appears.

2. In the left pane, click the user whose properties you want to edit.

3. On the User Properties window, in the appropriate boxes, edit the following information about the user:

   - Password

   - Last name

   - First name

   - User type

   ⓘ **Important:**

   You cannot change the user name. To change the user type, you must be logged on as an administrator.

4. Click the **Access Classes heading** to review the access classes assigned to the user.

5. To change the user's Launchpad Options, select or remove any of the following:

   - Access and Partition Management access

   - Real-Time Reporting access

   - Historical Reporting access

   - Configuration access

- Contact Center Management access

- Scripting access

- Emergency Help access

- Audit Trail access

- Outbound access

- Multimedia

- Call Recording and Quality Monitoring

- Prompt Management

6. Click the **Partitions** heading to review the current partitions assigned to the user. The heading expands to reveal a series of choices.

7. To grant the user full access to all data across all servers, select the **Full Data Across All Servers** check box.

   OR

   To refine the data that the user can see, clear the **Full Data Across All Servers** check box, and then proceed to the next step.

8. To review the standard partitions and supervisor/reporting agent combinations assigned to the user, click the **Standard & Reporting Agents** heading.

   OR

   If you do not want to make any changes to this area, proceed to step 16.

9. In the first table, there are three choices. You can choose a combination of all three. Select the option at the top of the table to make the same choice for all servers listed.

10. Select the **No Data** option for each server on which you do not want the user to see any data.

11. Select the **All Data option** for each server on which you want the user to see all configured data.

12. Select the **Configure** option for each server on which you want to specify the data that the user can see, and then proceed to the next step.

13. If you select the **Configure** option, from the **Configure Server** list, select the server to configure.

14. To select standard partitions on the current server, select the check box for each item that you want the user to see in the applicable Contact Center Manager Administration component. You can choose from the following standard partitions:

- All Agents & Supervisors

- All Skillsets

- All Applications

- All CDNs (Route Points)

- All DNIS
- All Prompts
- All Script Variables
- All Custom Reports
- Standard Agent Performance Reports
- Standard Call by Call Reports
- Standard Configuration Reports
- Standard Contact Summary Reports (if applicable for the server)
- Standard Networking Reports (if applicable for the server)
- Standard Other Reports
- Standard Outbound Reports
- Standard Multimedia Reports

🛈 **Important:**

Only Contact Center Management (**CCM**), Real-Time Reporting (**RTR**), Historical Reporting (**HR**), Scripting (**SCR**), and Prompt Management (**PTM**) are applicable to partitions. When you select the **PTM** check box, the current user gains access to all the prompts for that server in the Prompt Management component.

15. To review the supervisor/reporting agents currently assigned to the user, click the **Reporting Agents** tab.

   The table lists all the supervisors configured on the currently selected server.

   Each supervisor name represents the supervisor and all their reporting agents.

16. To grant the current user access to the supervisor's reporting agents in the components that you select, select the check box for each supervisor.

   OR

   To select all supervisors in a particular component, select the check box for that component.

17. To assign standard partitions and reporting agents on another server, select the next server from the list, and then repeat steps 10 to 12.

18. To review the user-defined partitions assigned to the user, click the **User Defined** heading.

   The heading expands to reveal the list of User Defined partitions configured across all servers.

19. Under the applicable components, select the check box for each partition to assign to the user.

   OR

   To select all partitions across a component, select the check box for that component.

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

Removing a partition from a user

Before you begin

- Log on to CCMA.

- Open the Access and Partition Management component.

- Before you remove a partition, ensure that the user does not need access to any of the partition properties.

About this task

When you remove a partition from a user, the user can no longer view the partitioned data in the real-time displays, historical reports, in Contact Center Management, or in Prompt Management.

Procedure

1. On the menu, choose **View/Edit** > **User Administration**.

2. In the left pane, select the user whose properties you want to edit.

3. In the User Properties window, click the **Partitions** heading.

4. To remove a standard partition from a user, click the **Standard & Reporting Agents** heading.

5. On the **Standard** tab, locate the partition to unassign, and clear the check box.

   You can assign or remove a standard partition based on a component (Contact Center Management, Historical Reporting, Real Time Reporting, Scripting, and Prompt Management).

6. To remove a User Defined partition, click the **User Defined** heading.

7. Locate the User Defined partition to unassign, and then clear the check box.

   You can assign or remove a User Defined partition based on a component (Contact Center Management, Historical Reporting, Real Time Reporting, Scripting, and Prompt Management).

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

Chapter 40: User-defined partitions

User-defined partitions are useful to restrict a user access to a specific list of data. You can use user-defined partitions in conjunction with standard partitions and reporting agents.

> 🛈 **Important:**
>
> To improve performance, use standard partitions and reporting agents instead of user-defined partitions.

If you create user-defined partitions to contain all of a particular element, for example, All agents or All CDNs (Route Points) on a particular server, use standard partitions instead. You can configure standard partitions in the user properties window. Standard partitions require no maintenance when you add new elements to the Contact Center Manager Server. Use user-defined partitions only if a specific set of data is required for the user.

To give users access to data on more than one server in your network, you can create a partition that spans multiple servers. However, note that when doing so, you must choose the partition properties on each server so the user can see the data on these servers. For example, for a user to see agents configured on two servers, you must select this agent on each server individually when configuring the partition. If you choose elements on one server for the partition, then the users assigned the partition can see only the data on this one server.

When you edit user-defined partitions, note that the greater the number of users assigned to the partition that you edit, the greater your performance hit, particularly if these users have Real-Time Reporting filters configured.

Avaya recommends that you:

- keep the amount of data included in each partition as minimal as possible because small partitions lead to more efficient application response time.

- configure and assign your partitions according to your company internal departmental organization, granting users access only to the data that they regularly need to see.

- use standard partitions where possible, including server rights options that can be configured for any configured server; for example, All Data on one of the servers in your contact center solution. Standard partitions require no maintenance and are more efficient to use than user-defined partitions that can contain large amounts of data.

Partition properties

When you create a partition, you can specify the following types of data:

- agents
- skillsets
- report groups
- applications
- CDNs (Route Points)
- DNISs
- script variables
- prompts

When you assign a partition that contains all eight types of data to a user, the user sees either all data types in the partition, or a fraction of them, depending on the component to which the partition is assigned. The Contact Center Manager Administration components are each designed so users can work with particular types of data. For example, Contact Center Management is used strictly to configure and manage Contact Center supervisors and agents, and to assign agents to skillsets; therefore, the only partition elements that appear in Contact Center Management are agents and skillsets. If you configure for a user a combination of user-defined partitions, standard partitions and reporting agents, then the user sees the union of this data when using Contact Center Manager Administration components.

If you do not include certain types of data in a user's partition, then the user does not see this data. For example, if you do not include CDNs (Route Points) in the user's partition, then the user sees no CDNs (Route Points) in Historical Reporting.

A partition can contain any combination of the eight elements, but it does not have to contain all elements. For example, it can contain only skillsets and agents, but not CDNs (Route Points), applications, or report groups.

After you create the partition, you can select it in the user properties window, in the User Defined area of the Partitions section.

Partitions and your Contact Center

User-defined partitions are especially useful when competing companies share the same Contact Center. In the following example, the two companies that share the Contact Center are Best Air and Econo Air.

To grant users access to data pertaining only to their company, administrators can create partitions within the Contact Center and assign the partitions to different users, thereby restricting each user's view of the Contact Center data.

For example, there are 18 skillsets configured in Contact Center Manager Administration. Ten skillsets apply to agents answering calls for Best Air, while the remaining eight skillsets apply to agents answering calls for Econo Air. To divide the Contact Center so that supervisors see

only the contact activity applicable to their company, the Contact Center administrator creates the following two partitions:

- The first partition contains the 10 Best Air skillsets and the agents that answer these calls.
- The second partition contains the 8 Econo Air skillsets and the agents that answer these calls.

After creating these partitions, the Contact Center administrator assigns them to the appropriate supervisors. When the supervisors view the Real-Time Reporting displays or the historical reports, they see only those elements in the partitions to which they belong.

Partitions can restrict only one element at a time. For example, when a user runs a Skillset by Agent Performance report, they can choose to view agents from among those in their partition configurations. However, sometimes an agent in the user's partition configuration is assigned to a skillset that is outside the user's partition configuration. If a contact is routed to an agent for a skillset that is not in the user's partition configuration, then the call statistic (and possibly the skillset details) appear in the Skillset by Agent Performance report.

Partitions are also useful if you want to separate your Contact Center into different departments within the same company. For example, the administrator can create separate partitions for the Sales and Marketing departments, and assign each partition to supervisors working in each department.

When creating and assigning user-defined partitions, note that the following factors increase the performance hit for the users to whom you assign the partitions when they connect to Contact Center Manager Administration:

- The greater the amount of data that you include in each partition, the greater the performance hit.
- The more partitions you assign to users, the greater the performance hit.

Avaya recommends that you configure and assign your partitions according to your company internal departmental organization, granting users access only to the data that regularly need to see. Additionally, Avaya recommends that you use standard partitions whenever possible.

Creating a user-defined partition

Before you begin

- Log on to CCMA. For more information, see Logging on to Contact Center Manager Administration Access and Partition Management on page 215.
- Open the Access and Partition Management component.
- Create report groups.
- Ensure that you have associated a media server with the CCMS server. For more information, see Adding a media server on page 114.

About this task

User-defined partitions are different from the Standard partitions that come with Contact Center Manager Administration in that you specify certain types of data on particular servers. For example, you can specify seven agents and two skillsets on the Toronto server. Standard partitions, however, include all of a certain type of data on particular servers in particular components. For example, All Agents & Supervisors and All Skillsets on the Toronto and Montreal (example) servers in both real-time reporting and historical reporting.

Procedure

1. On the menu, choose **Add** > **New User Defined Partition**.

2. In the New Partition window, in the **New Partition Name** box, type the name of the new partition.

3. Click **Submit**.

   The user-defined partition appears in the left pane.

4. In the left pane, select the new user-defined partition.

   The partition name expands to reveal the list of servers in your network.

5. Click the server that contains the data to add to the partition.

   The server partition elements appear in the partition properties window as a series of tabs.

   ⓘ **Important:**

   If any of the pages for partition elements are disabled in the Partition Properties window, then the currently selected server does not contain this type of data.

6. You can include multiple servers in a single partition. Select the items on the first server, and then repeat the process with the remaining servers that you want to include in the partition.

   ⓘ **Important:**

   When you add a custom report group to a partition, you must configure the partition on the same server on which you create the report group. If you do not configure the partition on the same server, the report group is not visible in Contact Center Manager Administration.

7. To add agents to the partition, click the **Agents** tab.

   ⓘ **Important:**

   If a large number of agents are configured on the server, when you click the Agents tab, you must wait a few moments while the system retrieves the agent data.

8. On the Agents page, click the **Assign Agents** heading. You can search for agents by name, supervisor, or by skillset.

9. To list all agents, click **List All**.

10. Select the check box for each agent to add to the partition.

11. To add skillsets, click the **Skillset** tab.

12. On the Skillset page, click the **Assign Skillsets** heading.

13. Select the check box for each skillset to add to the partition.

14. To add report groups, click the **Report Groups** tab.

15. On the Report Groups page, select the check box for each report group to add to the partition.

16. To add applications, click the **Applications** tab.

17. On the Applications page, select the check box for each application to add to the partition.

18. To add CDNs (Route Points), click the **CDNs (Route Points)** tab.

19. On CDNs (Route Points) page, select the check box for each CDN (Route Point) to add to the partition.

20. To add DNISs, click the **DNISs** tab.

21. On the DNISs page, select the check box for each DNIS to add to the partition.

22. To add script variables to a partition, click the **Script Variables** tab.

23. On the Script Variables page, click the **Assign Script Variables** heading. You can search for script variables by name or type.

24. To list all script variables, click **List All**.

25. Select the check box for each script variable to add to the partition.

26. To add prompts to a partition, click the **Prompts** tab.

    When you click the **Prompts** tab, the system checks if the CCMS server is associated with a media server. If the CCMS server does not have an associated media server, the system displays an error message. If the CCMS server has an associated media server, the system retrieves all the prompts for the namespace that matches the CCMS SIP domain. The system retrieves all namespace prompts, including the name of the content group that the prompt belongs to. The prompts that are assigned to the partition have a selected check box. If the namespace is not present the system displays an error message.

27. Select the check box for each prompt to add to the partition.

28. Click **Submit** to save your changes on the selected server.

29. To add elements from other servers to the partition, click the server name, and then repeat

Variable definitions

Name	Description
Agents tab	When you click this tab, two sections appear. The first section displays the agents included in the partition and in the second section you can search for agents to add to the partition. Select the check boxes beside the agents you want to include; clear the check boxes beside the agents you do not want to include.
Skillsets tab	When you click this tab, two sections appear. The first section displays the skillsets included in the partition, and the second section displays the available skillsets to add to the partition. In the table of available skillsets, select the check boxes beside the skillsets to add to the partition, or select the Select All check box to add all skillsets to the partition. To remove a skillset currently in the partition, clear the check box beside the skillset, and then click Submit.
Report Groups, CDN (Route Points), DNISs, Applications tabs	When you click these tabs, a table appears from which you can select the items to add to the partition by selecting the check boxes beside the item. In each table, you can select the Select All check box to select all items in the table. To remove any items currently in the partition, clear the check box beside the item, and then click Submit.
Script Variables tab	When you click this tab, two sections appear. The Assigned section displays all script variables assigned to this partition. In the Assign section, you can search for script variables by name or type. You can also list all script variables. Use the check boxes to determine which variables are included.
Prompts Tab	When you click the **Prompts** tab, the system displays a table from which you can select the prompts to add to the partition by selecting the check box beside the prompt. You can select the **Select All** check box to select all prompts in the table. To remove any prompt currently in the partition, clear the check box beside the prompt. You can sort the prompts by **Prompt Name**. Once you have completed making your changes, click **Submit** to save your changes.

Editing a user-defined partition

Before you begin

- Log on to CCMA. For more information, see [Logging on to Contact Center Manager Administration Access and Partition Management](#) on page 215.
- Open the Access and Partition Management component.
- Create a user-defined partition. See [Creating a user-defined partition](#) on page 240.

About this task

Edit a user-defined partition to add new elements, remove elements, or add new servers to the partition.

Procedure

1. On the menu, choose **View/Edit** > **User Defined Partitions**.

2. In the left pane, click the partition to edit.

   The partition name expands to reveal the list of servers in your network.

3. Click the server containing the elements to add to or remove from the partition.

4. In the Partition Properties window, click the tabs containing the elements to add to or remove from the partition.

5. To add an element, on the relevant page, select the check box for that element.

6. To remove an element, on the relevant page, clear the check box for that element.

7. To add elements from other servers to the partition, click the server name, and then repeat [step 3](#) on page 244 to [step 7](#) on page 244.

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

Assigning a user-defined partition to a user

Before you begin

- Log on to CCMA. For more information, see [Logging on to Contact Center Manager Administration Access and Partition Management](#) on page 215.
- Open the Access and Partition Management component.
- Create at least one user-defined partition.
- Create at least one Contact Center Manager Administration user.

About this task

You can use partitions to restrict the data that users can view in the real-time displays, historical reports, and Contact Center Management. You can assign standard and user-defined partitions to users in Contact Center Manager Administration. Choose the type that best suits your organization, or choose a combination of both types.

User-defined partitions are different from the Standard partitions that come with Contact Center Manager Administration in that you specify certain types of data on particular servers. For example, you can specify seven agents and two skillsets on the Toronto server. Standard partitions, however, include all of a certain type of data on particular servers in particular components. For example, All Agents & Supervisors and All Skillsets on the Toronto and Montreal servers in both Real-Time Reporting and Historical Reporting.

Procedure

1. On the menu, choose **View/Edit** > **User Administration**.

2. In the left pane, select the user to whom you want to assign a user-defined partition.

3. In the User Properties window, click the **Partitions** heading.

4. Clear the **Full Data Across All Servers** check box.

5. Click the **User Defined** heading.

   The heading expands to reveal the list of user-defined partitions configured across all servers.

6. For each component, select each partition to assign to the user.

   OR

   To select all user-defined partitions for Contact Center Management, Real-Time Reporting, Historical Reporting, Scripting, or Prompt Management, select the **CCM**, **RTR**, **HR**, **SCR**, or **PTM** check boxes, respectively.

7. To list all current members assigned to this partition, click the partition name.

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

Deleting a user-defined partition

Before you begin

- Log on to CCMA.

- Open the Access and Partition Management component.

- Before you delete a user-defined partition, verify that it is not assigned to users who need to view the partitioned data.

About this task

Complete this procedure to delete a user-defined partition.

Procedure

1. On the menu, choose **View/Edit** > **User Defined Partitions**.

2. In the left pane, right-click the user-defined partition, and then click **Delete**.

3. In the message box that appears asking you to confirm your choice, click **Yes**.

Chapter 41: Contact Center Manager Administration users

These are the users who log on to the Contact Center Manager Administration server to use Contact Center Manager Administration.

When you define Contact Center Manager Administration users, you assign to them:

- a role within the application, Administrator or Standard.
- basic access to the appropriate components within the Launchpad Options section of Contact Center Manager Administration.
- access classes that control the actions they can perform in these components. You can view the Access Classes that you create in the Access Classes section.
- partitions and supervisor/reporting agent combinations that control the data they can see in these components. You can view the standard partitions and the list of all supervisors who are configured on each server in your network in the Standard & Reporting Agents area of the Partitions section. Each supervisor name represents the supervisor and all of their reporting agents. You can view the partitions that you create in the User Defined area of the Partitions section.

Users configured with Launchpad Options to Access and Partition Management access also require an access class with privileges set for each of the Access and Partition Management views. Users with full access rights in Access and Partition Management can perform almost all administrative functions. Two user types are available (Standard and Administrator). However, only administrators can access and use the Configuration Tool spreadsheets for uploading and downloading configuration data, and can add, edit, delete and refresh servers in Configuration.

If the User Administration access class configuration allows, users can update their own user details in Access and Partition Management. Users must authenticate using their current password before updating their user details.

> **✱ Note:**
>
> If the deployment uses single sign-on (SSO), users do not need to authenticate before updating their user details.

Comments on this document?

Creating a Contact Center Manager Administration user

Before you begin

- Log on to CCMA. For more information, see Logging on to Contact Center Manager Administration Access and Partition Management on page 215.

- Open the Access and Partition Management component.

- Create access classes. See Creating an access class on page 219.

- Create user-defined partitions (optional). See Creating a user-defined partition on page 240.

- If the user has basic access to Contact Center Management, you must assign the user an access class that includes CCM access, Skillset Assignment access, or Supervisor Assignment access on at least one server.

  Important:

  If you assign the user an access class without at least one of these privileges on at least one server, the user sees nothing in Contact Center Management.

- If the user has basic access to Historical Reporting, you must assign the user an access class that includes either Run and Import access or Report Creation access.

  Important:

  If you assign the user an access class without either of these access levels, the user cannot work in Historical Reporting.

- If the user has basic access to Real-Time Reporting, you must assign the user an access class that includes either Launch access, Create Private access or Create Public access for either the tabular or graphical displays (or both).

  Important:

  If you assign the user an access class without at least one of these access levels, the user cannot work in Real-Time Reporting.

- If the user has basic access to Configuration, you must assign the user an access class to the user that includes at least one of the Configuration access class elements, such as skillsets or DNISs.

  Important:

  If you assign the user an access class without at least one of these privileges on at least one server, the user sees nothing in Configuration.

- If the user has basic access to Scripting, you must assign the user an access class that includes privileges in at least one of the following Scripting components: Scripts, Script Variables, or Application Thresholds.

  Important:

  If you assign the user an access class without privileges in at least one of these components on at least one server, the user sees nothing in Scripting.

- If the user has basic access to Prompt Management, you must assign the user an access class that includes at least one of the Prompt Management access class elements, such as Read Update Create/Delete or Read and Update.

  > 🛈 **Important:**
  >
  > If you assign the user an access class without at least one of these privileges on at least one server, the user sees nothing in Prompt Management.

About this task

Create a Contact Center Manager Administration user to grant the users access to the appropriate components within Contact Center Manager Administration. Assign access classes to users to control the actions that they can perform, and assigns supervisor/reporting agent combinations and partitions to users to control the data that they can see.

You can create two types of users within Access and Partition Management:

- Administrator—This type of user has complete access to all aspects of the system and is equivalent to the default webadmin account. If a user is configured as an administrator, all other options (such as Access Classes, Partitions, or Launchpad Options) are disabled.

  Administrators can also access and use the configuration spreadsheets for uploading configuration data and can add, edit and delete servers in the Configuration component.

- Standard—This type of user requires access rights and a partition profile to be defined to log on and use Contact Center Manager Administration.

If you enable the Advanced Security mode, you can also configure a user as programmatic. Programmatic accounts are the accounts that you create for the non-interactive establishment of secure communication between internal processes, for example, when using Web Services for integration with third-party applications.

If this deployment uses single sign-on (SSO), instead of creating a Contact Center Manager Administration user, you must map a System Manager local or external account to a Contact Center Manager Administration account. See <u>Associating a System Manager local account to an existing CCMA account</u> on page 252 and <u>Associating an external account to an existing CCMA account</u> on page 256.

Procedure

1. On the menu, choose **Add** > **New User**.

2. In the User Properties window, in the **User Details** section, type the relevant information about the user in the following boxes:

   - First Name

   - Last Name

   - User Name

     You cannot modify the user name after you add the user. For a different user name, you must delete the user and create a new one with the new name.

   - Password

     To view the password rules, hover the cursor over the **Info** icon next to the Password box.

3. To configure a user as programmatic, select the **Programmatic account** check box.

4. From the **User Type** list, select one of the following user types:

   • Administrator

   • Standard

5. For standard users, in the **Launchpad Options** section, select the check box for each of the following components that the user can access:

   • Access and Partition Management

   • Real-Time Reporting

   • Historical Reporting

   • Configuration

   • Contact Center Management

   • Scripting

   • Emergency Help

   • Audit Trail

   • Outbound

   • Multimedia

   • Call Recording and Quality Monitoring

   • Prompt Management

6. In the **Access Classes** section, select the check box for each access class to assign to the user.

7. Click the **Partitions** heading to assign partitions to the user.

8. To grant the user full access to all data across all servers, select the **Full Data Across All Servers** check box, and then proceed to [step 18](#) on page 251.

9. To refine the data that the user can see, clear the **Full Data Across All Servers** check box.

10. To assign the user access to data, standard partitions, or supervisor/reporting agent combinations on particular servers, click the **Standard & Reporting Agents** heading.

11. In the **Standard & Reporting Agents** area, select one of the following options for each server:

    • No Data—Select this option if you do not want the user to see any data on this server.

    • All Data—Select this option if you want the user to see all configured data on this server.

    • Configure—Select this option if you want to specify the data that the user can see, and then proceed to the next step.

12. If you selected the **Configure** option for at least one server, from the **Configure Server** list, select a server.

13. On the Standard page, for each component, select one or more of the following Standard partitions:

- All Agents & Supervisors

- All Applications

- All CDNs (Route Points)

- All User Defined Report Groups

- All DNIS

- All Prompts

- All Script Variables

- All Skillsets

- Standard Agent Performance Reports

- Standard Call by Call Reports

- Standard Configuration Reports

- Standard Contact Summary Reports (if applicable for the server)

- Standard Network Reports (if applicable for the server)

- Standard Other Reports

- Standard Outbound Reports

- Standard Multimedia Reports

    ❗ Important:

    Only Contact Center Management (**CCM**), Real-Time Reporting (**RTR**), Historical Reporting (**HR**), Scripting (**SCR**), and Prompt Management (**PTM**) are applicable to partitions. When you select the **PTM** check box, the current user gains access to all the prompts for that server in the Prompt Management component.

14. To grant access to reporting agents, or to grant access to the reporting agents of other supervisors, click the **Reporting Agents** tab.

    The Reporting Agents page lists all supervisors configured on the selected server. Each supervisor name represents the supervisor and all their reporting agents.

15. On the Reporting Agents page, under each component, select the supervisors for whom you want the user to have access.

    OR

    To select all supervisors for Contact Center Management, Real-Time Reporting, or Historical Reporting, select the **CCM**, **RTR**, **HR**, or **Scripting** check boxes, respectively.

16. To assign standard partitions and reporting agents on another server, select the next server from the **Configure Server** list, and then repeat

17. To assign a user-defined partition to the user, click the **User Defined** heading.

    The heading expands to reveal the list of user-defined partitions configured across all servers.

18. For each component, select each partition to assign to the user.

    OR

    To select all user-defined partitions for Contact Center Management, Real-Time Reporting, Historical Reporting, Scripting, or Prompt Management, select the **CCM**, **RTR**, **HR**, **SCR**, or **PTM** check boxes, respectively.

19. Click **Submit**, to save your changes.

Variable definitions

Name	Description
First Name	The first name of the Contact Center Manager Administration (CCMA) user.
Last Name	The last name of the CCMA user.
User Name	The name that users type when they log on to CCMA. **❗ Important:** Do not use an ampersand (&) in the user name.
User Type	Select Administrator or Standard. Only administrators can modify this field for other users.
Account Type	This field is automatically populated if single sign-on (SSO) is enabled in this deployment.
Password	The user's password to access CCMA. A CCMA 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: \ & : < > |

Table continues…

Name	Description
Associate User Account	If SSO is enabled in this deployment, instead of creating a Contact Center Manager Administration user, you must map a local or external System Manager account to a Contact Center Manager Administration account. Use the fields in this section to configure the associate user account.
Submit	Save the information.
Create Copy	To create a new CCMA user based on the properties of an existing user, click Create Copy. When you click this button, the system copies all the user's properties, except the following: • First Name • Last Name • User name • Password Type the user details for the new user, change any of the user's access and partition information (if desired), and then click Submit to save the new CCMA user.
Delete	Delete the current user.
Unassign User	If SSO is enabled, click to un-assign the associate user account.

Associating a System Manager local account to an existing CCMA account

Before you begin

- Create the local account on System Manager.

- Log on to CCMA. For more information, see Logging on to Contact Center Manager Administration Access and Partition Management on page 215.

- Open the Access and Partition Management component.

- Create access classes. See Creating an access class on page 219.

- Create user-defined partitions (optional). See Creating a user-defined partition on page 240.

- If the user has basic access to Contact Center Management, you must assign the user an access class that includes CCM access, Skillset Assignment access, or Supervisor Assignment access on at least one server.

> ❗ **Important:**
>
> If you assign the user an access class without at least one of these privileges on at least one server, the user sees nothing in Contact Center Management.

- If the user has basic access to Historical Reporting, you must assign the user an access class that includes either Run and Import access or Report Creation access.

  > ❗ **Important:**
  >
  > If you assign the user an access class without either of these access levels, the user cannot work in Historical Reporting.

- If the user has basic access to Real-Time Reporting, you must assign the user an access class that includes either Launch access, Create Private access or Create Public access for either the tabular or graphical displays (or both).

  > ❗ **Important:**
  >
  > If you assign the user an access class without at least one of these access levels, the user cannot work in Real-Time Reporting.

- If the user has basic access to Configuration, you must assign the user an access class to the user that includes at least one of the Configuration access class elements, such as skillsets or DNISs.

  > ❗ **Important:**
  >
  > If you assign the user an access class without at least one of these privileges on at least one server, the user sees nothing in Configuration.

- If the user has basic access to Scripting, you must assign the user an access class that includes privileges in at least one of the following Scripting components: Scripts, Script Variables, or Application Thresholds.

  > ❗ **Important:**
  >
  > If you assign the user an access class without privileges in at least one of these components on at least one server, the user sees nothing in Scripting.

- If the user has basic access to Prompt Management, you must assign the user an access class that includes at least one of the Prompt Management access class elements, such as Read Update Create/Delete or Read and Update.

  > ❗ **Important:**
  >
  > If you assign the user an access class without at least one of these privileges on at least one server, the user sees nothing in Prompt Management.

About this task

Associate a System Manager local account to an existing Contact Center Manager Administration (CCMA) account to configure access rights and allow the user to log on to the CCMA client.

This procedure applies only if SSO is enabled in this deployment.

Procedure

1. On the menu, choose **Add** > **New User**.

2. In the User Properties window, in the **User Details** section, click **Associate User Account**.

3. Select **Search local security server**.

4. Select the search criteria to find the user account you want to map, or click **List All** to list all accounts.

5. Select the System Manager user account you want to associate with a Contact Center Manager Administration account.

   The details for the user populate into the User Details section.

6. In the **Launchpad Options** section, select the check box for each of the following components that the user can access:

   - Access and Partition Management

   - Real-Time Reporting

   - Historical Reporting

   - Configuration

   - Contact Center Management

   - Scripting

   - Emergency Help

   - Audit Trail

   - Outbound

   - Multimedia

   - Call Recording and Quality Monitoring

   - Prompt Management

7. In the **Access Classes** section, select the check box for each access class to assign to the user.

8. Click the **Partitions** heading.

9. To grant the user full access to all data across all servers, select the **Full Data Across All Servers** check box, and then proceed to .

10. To refine the data that the user can see, clear the **Full Data Across All Servers** check box.

11. To assign the user access to data, standard partitions, or supervisor/reporting agent combinations on particular servers, click the **Standard & Reporting Agents** heading.

12. In the **Standard & Reporting Agents** area, select one of the following options for each server:

    • No Data—Select this option if you do not want the user to see any data on this server.

    • All Data—Select this option if you want the user to see all configured data on this server.

    • Configure—Select this option if you want to specify the data that the user can see, and then proceed to the next step.

13. If you selected the **Configure** option for at least one server, from the **Configure Server** list, select a server.

14. On the Standard page, for each component, select one or more of the following Standard partitions:

    • All Agents & Supervisors

    • All Applications

    • All CDNs (Route Points)

    • All User Defined Report Groups

    • All DNIS

    • All Prompts

    • All Script Variables

    • All Skillsets

    • Standard Agent Performance Reports

    • Standard Call by Call Reports

    • Standard Configuration Reports

    • Standard Contact Summary Reports (if applicable for the server)

    • Standard Network Reports (if applicable for the server)

    • Standard Other Reports

    • Standard Outbound Reports

    • Standard Multimedia Reports

    ⓘ **Important:**

    Only Contact Center Management (**CCM**), Real-Time Reporting (**RTR**), Historical Reporting (**HR**), Scripting (**SCR**), and Prompt Management (**PTM**) are applicable to partitions. When you select the **PTM** check box, the current user gains access to all the prompts for that server in the Prompt Management component.

15. To grant access to reporting agents, or to grant access to the reporting agents of other supervisors, click the **Reporting Agents** tab.

    The Reporting Agents page lists all supervisors configured on the selected server. Each supervisor name represents the supervisor and all their reporting agents.

16. On the Reporting Agents page, under each component, select the supervisors for whom you want the user to have access.

    OR

    To select all supervisors for Contact Center Management, Real-Time Reporting, or Historical Reporting, select the **CCM**, **RTR**, **HR**, or **Scripting** check boxes, respectively.

17. To assign standard partitions and reporting agents on another server, select the next server from the **Configure Server** list, and then repeat [step 14](#) on page 255 to [step 16](#) on page 256.

18. To assign a user-defined partition to the user, click the **User Defined** heading.

    The heading expands to reveal the list of user-defined partitions configured across all servers.

19. For each component, select each partition to assign to the user.

    OR

    To select all user-defined partitions for Contact Center Management, Real-Time Reporting, Historical Reporting, Scripting, or Prompt Management, select the **CCM**, **RTR**, **HR**, **SCR**, or **PTM** check boxes, respectively.

20. Click **Submit**, to save your changes.

Associating an external account to an existing CCMA account

Before you begin

- Log on to CCMA. For more information, see [Logging on to Contact Center Manager Administration Access and Partition Management](#) on page 215.

- Open the Access and Partition Management component.

- Create access classes. See [Creating an access class](#) on page 219.

- Create user-defined partitions (optional). See [Creating a user-defined partition](#) on page 240.

- If the user has basic access to Contact Center Management, you must assign the user an access class that includes CCM access, Skillset Assignment access, or Supervisor Assignment access on at least one server.

  🛈 Important:

    If you assign the user an access class without at least one of these privileges on at least one server, the user sees nothing in Contact Center Management.

- If the user has basic access to Historical Reporting, you must assign the user an access class that includes either Run and Import access or Report Creation access.

> ❗ **Important:**
>
> If you assign the user an access class without either of these access levels, the user cannot work in Historical Reporting.

- If the user has basic access to Real-Time Reporting, you must assign the user an access class that includes either Launch access, Create Private access or Create Public access for either the tabular or graphical displays (or both).

> ❗ **Important:**
>
> If you assign the user an access class without at least one of these access levels, the user cannot work in Real-Time Reporting.

- If the user has basic access to Configuration, you must assign the user an access class to the user that includes at least one of the Configuration access class elements, such as skillsets or DNISs.

> ❗ **Important:**
>
> If you assign the user an access class without at least one of these privileges on at least one server, the user sees nothing in Configuration.

- If the user has basic access to Scripting, you must assign the user an access class that includes privileges in at least one of the following Scripting components: Scripts, Script Variables, or Application Thresholds.

> ❗ **Important:**
>
> If you assign the user an access class without privileges in at least one of these components on at least one server, the user sees nothing in Scripting.

- If the user has basic access to Prompt Management, you must assign the user an access class that includes at least one of the Prompt Management access class elements, such as Read Update Create/Delete or Read and Update.

> ❗ **Important:**
>
> If you assign the user an access class without at least one of these privileges on at least one server, the user sees nothing in Prompt Management.

About this task

Associate an external account to an existing Contact Center Manager Administration account to configure access rights and allow the user to log on to the Contact Center Manager Administration client.

This procedure applies only if SSO is enabled.

Procedure

1. On the menu, choose **Add** > **New User**.

2. In the User Properties window, in the **User Details** section, click **Associate User Account**.

3. Select **Search domain users**.

4. In the **Domain Details** section, in the **Domain Server FQDN** box, type the fully qualified domain name of the domain server.

5. Select **Specify Domain Account**.

6. In the **Domain Account** section, in the **User ID (Domain\User ID)** box, type the user ID to log on to the domain server.

7. In the **Password** box, type the password to log on to the domain server.

8. Select the search criteria to find the user account you want to map, or click **List All** to list all accounts.

9. Select the user account you want to associate with a Contact Center Manager Administration account.

   The details for the user populate into the User Details section.

10. In the **Launchpad Options** section, select the check box for each of the following components that the user can access:

    • Access and Partition Management

    • Real-Time Reporting

    • Historical Reporting

    • Configuration

    • Contact Center Management

    • Scripting

    • Emergency Help

    • Audit Trail

    • Outbound

    • Multimedia

    • Call Recording and Quality Monitoring

    • Prompt Management

11. In the **Access Classes** section, select the check box for each access class to assign to the user.

12. Click the **Partitions** heading.

13. To grant the user full access to all data across all servers, select the **Full Data Across All Servers** check box, and then proceed to .

14. To refine the data that the user can see, clear the **Full Data Across All Servers** check box.

15. To assign the user access to data, standard partitions, or supervisor/reporting agent combinations on particular servers, click the **Standard & Reporting Agents** heading.

16. In the **Standard & Reporting Agents** area, select one of the following options for each server:

    • No Data—Select this option if you do not want the user to see any data on this server.

- All Data—Select this option if you want the user to see all configured data on this server.

- Configure—Select this option if you want to specify the data that the user can see, and then proceed to the next step.

17. If you selected the **Configure** option for at least one server, from the **Configure Server** list, select a server.

18. On the Standard page, for each component, select one or more of the following Standard partitions:

- All Agents & Supervisors

- All Applications

- All CDNs (Route Points)

- All User Defined Report Groups

- All DNIS

- All Prompts

- All Script Variables

- All Skillsets

- Standard Agent Performance Reports

- Standard Call by Call Reports

- Standard Configuration Reports

- Standard Contact Summary Reports (if applicable for the server)

- Standard Network Reports (if applicable for the server)

- Standard Other Reports

- Standard Outbound Reports

- Standard Multimedia Reports

> ❶ **Important:**
>
> Only Contact Center Management (**CCM**), Real-Time Reporting (**RTR**), Historical Reporting (**HR**), Scripting (**SCR**), and Prompt Management (**PTM**) are applicable to partitions. When you select the **PTM** check box, the current user gains access to all the prompts for that server in the Prompt Management component.

19. To grant access to reporting agents, or to grant access to the reporting agents of other supervisors, click the **Reporting Agents** tab.

    The Reporting Agents page lists all supervisors configured on the selected server. Each supervisor name represents the supervisor and all their reporting agents.

20. On the Reporting Agents page, under each component, select the supervisors for whom you want the user to have access.

    OR

To select all supervisors for Contact Center Management, Real-Time Reporting, or Historical Reporting, select the **CCM**, **RTR**, **HR**, or **Scripting** check boxes, respectively.

21. To assign standard partitions and reporting agents on another server, select the next server from the **Configure Server** list, and then repeat

22. To assign a user-defined partition to the user, click the **User Defined** heading.

    The heading expands to reveal the list of user-defined partitions configured across all servers.

23. For each component, select each partition to assign to the user.

    OR

    To select all user-defined partitions for Contact Center Management, Real-Time Reporting, Historical Reporting, Scripting, or Prompt Management, select the **CCM**, **RTR**, **HR**, **SCR**, or **PTM** check boxes, respectively.

24. Click **Submit**, to save your changes.

Copying the properties of an existing Contact Center Manager Administration user

Before you begin

- Log on to CCMA.

- Open the Access and Partition Management component.

About this task

Copy the properties of an existing Contact Center Manager Administration user to create a new user based on the properties of an existing user.

Procedure

1. Select a user to copy.

   You copy all basic access rights, access classes, and partition information for the selected user.

2. Click **Create Copy**.

3. Type the new user details, change any partition or access information.

4. Click **Submit** to save the new user.

Deleting a Contact Center Manager Administration user

Before you begin

- Log on to CCMA.

- Open the Access and Partition Management component.

About this task

Delete a Contact Center Manager Administration user to remove a user that is no longer required.

Procedure

1. On the menu, choose **View/Edit** > **User Administration**.

2. In the left pane, right-click the user to delete, and then click **Delete**.

3. Click **Yes**.

Unassigning users

Before you begin

- Log on to Contact Center Manager Administration. For more information, see Logging on to Contact Center Manager Administration Access and Partition Management on page 215.

- Open the Access and Partition Management component.

About this task

If SSO is enabled, you can remove the association between a System Manager local account or an external account and a Contact Center Manager Administration account.

Procedure

1. On the menu, choose **View/Edit** > **User Administration**.

2. In the left pane, right-click the agent whose association you want to remove and select **Unassign user**.

3. In the message box, click **OK**.

Assigning supervisor/reporting agent combinations to a user

Before you begin

- Log on to CCMA. For more information, see Logging on to Contact Center Manager Administration Access and Partition Management on page 215.

- Open the Access and Partition Management component.
- Create at least one Contact Center Manager Administration user.

About this task

When you configure a Contact Center Manager Administration user, you can assign the user one or more supervisor/reporting agent combinations to enable the user to see all the corresponding agents in the historical reports, real-time displays, and Contact Center Management. Each name on the Reporting Agents tab in the User Properties window represents a supervisor and all of their reporting agents on a per-server basis. Therefore, when you link a supervisor's name with a Contact Center Manager Administration user, you automatically enable this user to see all the supervisor's reporting agents.

Procedure

1. On the menu, choose **View/Edit** > **User Administrator**.

2. In the left pane, click the user to whom you want to assign a supervisor/reporting agent combination.

3. In the User Properties window, click the **Partitions** heading.

4. Clear the **Full Data Across All Servers** check box.

5. Click the **Standard & Reporting Agents** heading.

6. In the **Standard & Reporting Agents** area, select one of the following options for each server:

    - No Data—Select this option if you do not want the user to see any data on this server.

    - All Data—Select this option if you want the user to see all configured data on this server.

    - Configure—Select this option if you want to specify the data that the user can see, and then proceed to the next step.

7. If you selected the **Configure** option for at least one server, from the **Configure Server** list, select a server.

8. On the Standard page, for each component, select one or more of the following Standard partitions:

    - All Agents & Supervisors

    - All Applications

    - All CDNs (Route Points)

    - All User Defined Report Groups

    - All DNIS

    - All Prompts

    - All Script Variables

    - All Skillsets

    - Standard Agent Performance Reports

Avaya Aura® Contact Center Client Administration

- Standard Call by Call Reports

- Standard Configuration Reports

- Standard Contact Summary Reports (if applicable for the server)

- Standard Network Reports (if applicable for the server)

- Standard Other Reports

- Standard Outbound Reports

- Standard Multimedia Reports

> **ⓘ Important:**
>
> Only Contact Center Management (**CCM**), Real-Time Reporting (**RTR**), Historical Reporting (**HR**), Scripting (**SCR**), and Prompt Management (**PTM**) are applicable to partitions. When you select the **PTM** check box, the current user gains access to all the prompts for that server in the Prompt Management component.

9. To grant access to reporting agents, or to grant access to the reporting agents of other supervisors, click the **Reporting Agents** tab.

   The Reporting Agents page lists all supervisors configured on the selected server. Each supervisor name represents the supervisor and all their reporting agents.

10. On the Reporting Agents page, under each component, select the supervisors for whom you want the user to have access.

    OR

    To select all supervisors for Contact Center Management, Real-Time Reporting, Historical Reporting, or Scripting, select the **CCM**, **RTR**, **HR**, or **Scripting** check boxes, respectively.

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

Configuring a supervisor or supervisor/agent

Before you begin

- Log on to CCMA. For more information, see Logging on to Contact Center Manager Administration Access and Partition Management on page 215.

- Open the Access and Partition Management component.

- Create any required access classes. See Creating an access class on page 219.

- Create any required user-defined partitions. See Creating a user-defined partition on page 240.

- If you grant the supervisor or supervisor/agent basic access to Contact Center Management, you must also assign an access class to the user containing at least one of the CCM, Skillset Assignments, or Agent to Supervisor Assignments access rights. If you do not assign this kind of access class to the user, then the user sees nothing in Contact Center Management.

If the user's partitions do not contain any agents or skillsets, then the user sees no data in Contact Center Management.

About this task

When you create supervisors and supervisor/agents in Contact Center Management and give them a Contact Center Manager Administration user ID and password to use Contact Center Manager Administration, their user profile automatically appears in Access and Partition Management under the Users folder. (In addition to being Contact Center users, they are also Contact Center Manager Administration users.) To properly configure these users, you must open their profile and give them basic access rights to the Contact Center Manager Administration components that they need to use.

When you configure these Contact Center Manager Administration users, you can assign the following to them:

- supervisor/reporting agent combinations—To enable the user to automatically see all of their reporting agents, or all the reporting agents of another supervisor. On the Reporting Agents tab of the User Properties window, click the check box beside the appropriate supervisor names.

- access classes—You must configure the access class that the user needs to work in Contact Center Management, and assign it to the user.

- partitions—In the User Properties window, assign the user the appropriate partitions containing the data that the user needs to see. You can assign a combination of standard partitions, user-defined partitions, or full data access.

Procedure

1. On the menu, choose **View/Edit** > **User Administration**.

2. In the left pane, select the user created in Contact Center Management.

3. In the User Properties window, click the **Launchpad Options** heading The heading expands to reveal a list of applications.

4. In the **Launchpad Options** section, select the check box for each of the following component that the user can access:

    - Access and Partition Management

    - Real-Time Reporting

    - Historical Reporting

    - Configuration

    - Contact Center Management

    - Scripting

    - Emergency Help

    - Audit Trail

    - Outbound

    - Multimedia

- Call Recording and Quality Monitoring

- Prompt Management

5. In the **Access Classes** section, select the check box for each access class to assign to the user.

6. Click the **Partitions** heading to assign partitions to the user.

7. To grant the user full access to all data across all servers, select the **Full Data Across All Servers** check box, and then proceed directly to step 18 on page 266.

8. To refine the data that the user can see, clear the **Full Data Across All Servers** check box.

9. To assign the user access to data, Standard partitions, or supervisor/reporting agent combinations on particular servers, click the **Standard & Reporting Agents** heading, and proceed to step 11 on page 265.

10. To assign user-defined partitions, click the **User Defined** heading, and proceed to step 17.

11. In the **Standard & Reporting Agents** area, select one of the following options for each server:

- No Data—Select this option if you do not want the user to see any data on this server.

- All Data—Select this option if you want the user to see all configured data on this server.

- Configure—Select this option if you want to specify the data that the user can see, and then proceed to the next step.

12. If you selected the **Configure** option for at least one server, from the **Configure Server** list, select a server.

13. On the Standard page, for each component, select one or more of the following Standard partitions:

- All Agents & Supervisors

- All Applications

- All CDNs (Route Points)

- All User Defined Report Groups

- All DNIS

- All Prompts

- All Script Variables

- All Skillsets

- Standard Agent Performance Reports

- Standard Call by Call Reports

- Standard Configuration Reports

- Standard Contact Summary Reports (if applicable for the server)

- Standard Network Reports (if applicable for the server)
- Standard Other Reports
- Standard Outbound Reports
- Standard Multimedia Reports

> 🛈 **Important:**
>
> Only Contact Center Management (**CCM**), Real-Time Reporting (**RTR**), Historical Reporting (**HR**), Scripting (**SCR**), and Prompt Management (**PTM**) are applicable to partitions. When you select the **PTM** check box, the current user gains access to all the prompts for that server in the Prompt Management component.

14. To grant access to reporting agents, or to grant access to the reporting agents of other supervisors, click the **Reporting Agents** tab.

    The Reporting Agents page lists all supervisors configured on the selected server. Each supervisor name represents the supervisor and all their reporting agents.

15. On the Reporting Agents page, under each component, select the supervisors for whom you want the user to have access.

    OR

    To select all supervisors for Contact Center Management, Real-Time Reporting, Historical Reporting, or Scripting, select the **CCM**, **RTR**, **HR**, or **Scripting** check boxes, respectively.

16. To assign standard partitions and reporting agents on another server, repeat step 12 on page 265 to step 15 on page 266.

17. To assign a user-defined partition to the user, click the **User Defined** heading.

    The heading expands to reveal the list of user-defined partitions configured across all servers.

18. For each component, select each partition to assign to the user.

    OR

    To select all user-defined partitions for Contact Center Management, Real-Time Reporting, Historical Reporting, Scripting, or Prompt Management, select the **CCM**, **RTR**, **HR**, **SCR**, or **PTM** check boxes, respectively.

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

Unlocking locked Contact Center Manager Administration users

Before you begin

- Log on to CCMA as an administrator.

- Open the Access and Partition Management component.

About this task

For security reasons, Contact Center Manager Administration locks user accounts that have not been logged in to the system for a long time period. When a locked user attempts to log in to Contact Center Manager Administration, the lockout notification appears and the login attempt fails. Locked users must contact their administrator, as only CCMA administrators have rights to unlock locked users.

Procedure

1. On the menu, choose **View/Edit** > **User Administration**.

2. In the left pane, select the user you want to unlock.

3. Deselect the **Inactive Account Lockout** check box.

4. Click **Submit**.

   Contact Center Manager Administration unlocks the user account. The unlocked user now can log in to the system.

Part 4: Prompt Management

Chapter 42: Prompt Management

Using Prompt Management, Contact Center Manager Administration (CCMA) users can manage prompts on one or more Avaya Aura® Media Server (Avaya Aura® MS) servers. Prompt Management provides access control and partitioning.

Avaya Aura® MS servers work in clusters. A cluster consists of one or more masters and possibly a number of slave servers. In Avaya Aura® Contact Center, the master servers are associated with Contact Center Manager Server (CCMS). All servers in a cluster have the same set of prompts. To replicate the prompts to the slave servers, you must add the prompts to the master servers.

CCMA uses a set of SOAP Web services that Avaya Aura® MS provides to provision the prompts. You must configure CCMA as a SOAP trusted host in Avaya Aura® MS to configure the prompts. For more information on how to configure CCMA as a trusted node in Avaya Aura® MS, see *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications*.

When you enter the Prompt Management module, the system displays a list of all the configured CCMS servers that have an associated Avaya Aura® MS server. An associated Avaya Aura® MS server is one whose **Master Content Store** checkbox is selected on the Media Servers page. The tree server node text displays both the CCMS server and Avaya Aura® MS server names for clarity. If there are no servers to display, the system displays an error message. If the servers are present but the access class of the user for this CCMS server is set to None, then the user is not able to access the CCMS server and the system displays an error message.

When you click the CCMS server node, CCMA retrieves content groups contained within the contact center namespace on the associated Avaya Aura® MS server. The contact center namespace must match the SIP domain name that is configured in server configuration. If the namespace is not found or if the namespace does not match the CCMS SIP domain namespace, the system displays an error message. You cannot use CCMA to add a new namespace to the media server. The content groups contain the media prompts.

CCMA supports single-level content groups at the namespace level. You cannot create nested content groups in CCMA. CCMA does not display any nested content groups that you create using Avaya Aura® Media Server Element Manager.

Prompts and Music media files

Prompt Management supports media files for prompts and music. The media files for prompts are stored in a Prompts Content Group in the CCMS SIP domain namespace. The media files for music are stored in a Music Content Group in the *streamsource* namespace.

Comments on this document?

> ⊛ **Note:**
>
> When you upload files to the streamsource namespace, it can take up to 15 minutes before they become available for use on Avaya Aura® Media Server. If you restart Avaya Aura® Media Server, the files become available immediately.

Media file formats

Avaya Aura® Media Server provides optimum playback performance with .WAV files encoded as Linear 16-bit PCM, 8KHz Mono with a sampling rate of 128kbits/sec. Create your media files with this encoding.

Prompt Management in a geographic redundancy environment

If a failover occurs to the Remote Geographic Node (RGN) site, you must update the Master Content Store setting to point to your local Master Content Store node at the RGN site. When you update this setting, you can use Contact Center Manager Administration for prompt management at the RGN site.

After a failover, the user-defined partitions applied to prompts do not apply on the RGN server. Users with access to Prompt Management can access all prompts on an RGN server. If necessary, an administrator must reconfigure user-defined prompt partitions on the RGN server. If an administrator makes prompt changes to new or existing user-defined partitions on the RGN server, these prompt changes are not replicated on the servers at the campus site and do not apply when campus High Availability is reinstated.

Prerequisites to Prompt Management procedures

- Log on to Contact Center Manager Administration as an administrator or as a user with sufficient access levels (access class) to use the Prompt Management component.

- Ensure you configure Contact Center Manager Administration as a SOAP trusted node in Avaya Aura® Media Server Element Manager. For more information, see *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications*.

Logging in to Contact Center Manager Administration Prompt Management

About this task

Log in to Contact Center Manager Administration to configure and administer your prompts. Complete the following procedure to gain access to the Prompt Management component.

Before you begin

- Install and commission Contact Center Manager Administration.

- Ensure that you have a Contact Center Manager Administration username and password.

• Ensure that you are using Microsoft Edge in Internet Explorer mode.

Procedure

1. In your browser, type the URL of the server and then press `Enter`.

   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. Do not use the server IP address to log in.

   If your site does not use the default port for Internet Information Services (IIS), the URL of the server is `https://<server name>:<port number>`, where **<server name>** is the computer name of the Contact Center server, and **<port number>** is the port for the CCMA site in IIS. For example, `https://ccserver:81`.

2. In the **User ID** field, type your user ID.

3. In the **Password** field, type your password.

4. Click **Login**.

   If configured in the security settings, CCMA displays the date and time of your last login and the number of failed login attempts since your last successful login.

5. Click **Prompt Management**.

Adding a new Prompts Content Group

Before you begin

• Ensure that you are assigned an access class of Read Update Create/Delete. For more information, see [Access classes](#) on page 217.

• Ensure that you have associated the media server with the CCMS server. For more information, see [Adding a media server](#) on page 114.

• Ensure that you have selected the **Prompt Management** component in your Launchpad options. For more information, see [Creating a Contact Center Manager Administration user](#) on page 247.

• Create any required user-defined partitions. For more information, see [Creating a user-defined partition](#) on page 240.

• Log on to CCMA. For more information, see [Logging in to Contact Center Manager Administration Prompt Management](#) on page 270.

• Open the Prompt Management component.

About this task

Add a new create prompts content groups to store media prompts.

Procedure

1. From the left-hand pane, right-click the CCMS server in which you want to add a content group.

2. Select the **Add new prompts content group**.

3. In the **Content Group** box, type the name of the new prompts content group. You must use US ASCII characters only.

4. Click **Add Content Group**.

   The system creates a new prompts content group folder under the selected CCMS server. This new content group is in the CCMS SIP domain Namespace.

Adding a Media Prompt

Before you begin

- Ensure that you are assigned an access class of Read Update Create/Delete. For more information, see Access classes on page 217.

- Ensure that you have associated the media server with the CCMS server. For more information, see Adding a media server on page 114.

- Log on to CCMA. For more information, see Logging in to Contact Center Manager Administration Prompt Management on page 270.

- Open the Prompt Management component.

- Ensure that you have created a Content Group. For more information, see Adding a new Prompts Content Group on page 271.

About this task

You can add media files to the media server to provide prompts.

Procedure

1. From the left-hand pane, click the CCMS server in which you want to add the media prompt.

   The system displays the content groups associated with that namespace.

2. Click the content group in which you want to add media prompts.

   The system displays a new page that lists all the prompts stored under that content group.

   The Content Group page displays the following:

   - Page title that contains the namespace name, the content group name, and the server name

   - Grid that contains information about all the prompts

   - Buttons that depend on your Prompt Management access class:

     - **Add Media**

     - **Save**

     - **Download Media**

- **Delete Media**

- **Rename Content Group**

- **Delete Content Group**

- **Cancel**

3. To create and upload a new media prompt, click the **Add Media** button.

4. Click **Select** under the Add Media section to navigate to the media prompt file that you want to upload.

5. To provide a new name for the media prompt file, type the new name in the **Media Name** field.

   Valid values for **Media Name** are numbers, uppercase and lowercase letters, and underscores.

6. To assign the prompt to any or all user-defined partitions, select the user-defined partitions from the User Defined Partitions section.

7. Click **Save**.

   The system uploads prompt to the media server and adds the new prompt to the grid.

Variable definitions

Name	Description
Add Media	If the Prompt Management access class is set to Read Update Create/Delete the system displays the **Add Media** button. Click **Add Media** to create and upload a new media prompt to the media server.
Save	If the Prompt Management access class is set to Read and Update or greater access class the system displays the **Save** button. Click **Save** to save your current actions.
Download Media	If the Prompt Management access class is set to Read Only or greater access class the system displays the **Download Media** button. Click **Download Media** to download the selected media prompt.
Delete Media	If the Prompt Management access class is set to Read Update Create/Delete the system displays the **Delete Media** button. Click **Delete Media** to delete the selected media prompt.
Delete Content Group	If the Prompt Management access class is set to Read Update Create/Delete the system displays the **Delete Content Group** button. Click **Delete Content Group** to delete the selected content group.

Table continues…

Name	Description
Rename Content Group	If the Prompt Management access class is set to Read and Update or greater the system displays the **Rename Content Group** button. Click **Rename Content Group** to rename the selected content group.
Cancel	If the Prompt Management access class is set to Read Only or greater access class the system displays the **Cancel** button. Click **Cancel** to cancel your current actions.
Media Name	Type a new name for the media prompt file in the **Media Name** field.

Adding a new Music Content Group

Before you begin

- Ensure that you are assigned an access class of Read Update Create/Delete. For more information, see Access classes on page 217.
- Ensure that you have associated the media server with the CCMS server. For more information, see Adding a media server on page 114.
- Ensure that you have selected the **Prompt Management** component in your Launchpad options. For more information, see Creating a Contact Center Manager Administration user on page 247.
- Create any required user-defined partitions. For more information, see Creating a user-defined partition on page 240.
- Log on to CCMA. For more information, see Logging in to Contact Center Manager Administration Prompt Management on page 270.
- Open the Prompt Management component.

About this task

Add a new create music content groups to store music.

Procedure

1. From the left-hand pane, right-click the CCMS server in which you want to add a content group.

2. Select the **Add new music content group**.

3. In the **Content Group** box, type the name of the new music content group. You must use US ASCII characters only.

4. Click **Add Content Group**.

   The system creates a new music content group folder under the selected CCMS server. This new content group is in the **streamsource** Namespace.

Adding a music media file

Before you begin

- Ensure that you are assigned an access class of Read Update Create/Delete. For more information, see Access classes on page 217.

- Ensure that you have associated the media server with the CCMS server. For more information, see Adding a media server on page 114.

- Log on to CCMA. For more information, see Logging in to Contact Center Manager Administration Prompt Management on page 270.

- Open the Prompt Management component.

- Ensure that you have created a music content group. For more information, see Adding a new Prompts Content Group on page 271.

About this task

You can add media files to the media server to provide music.

Procedure

1. From the left-hand pane, click the CCMS server in which you want to add the media prompt.

   The system displays the content groups.

2. Click the music content group in which you want to add the music media file.

   The system displays a new page that lists all the media files stored under that content group.

3. Click **Add Media**.

4. Click **Select** and navigate to the music file that you want to upload.

5. In the **Media Name** box, type the name of the music media.

   Valid values for **Media Name** are numbers, uppercase and lowercase letters, and underscores.

6. Click **Save**.

   The system uploads the music media to the media server and adds the new music to the grid.

Changing a Media Prompt

Before you begin

- Ensure that you are assigned an access class of Read Only for downloading a media prompt, Read and Update for renaming a media prompt, and Read Update Create/Delete for deleting a media prompt. For more information, see Access classes on page 217.

- Ensure that you have associated the media server with the CCMS server. For more information, see [Adding a media server](#) on page 114.

- Log on to CCMA. For more information, see [Logging in to Contact Center Manager Administration Prompt Management](#) on page 270.

- Open the Prompt Management component.

- Ensure that you have added a media prompt. For more information, see [Adding a Media Prompt](#) on page 272.

About this task

You can edit media prompts to change any of the configured properties for the media prompt.

Procedure

1. Select a prompt that you want to modify from the grid on the Content Group page.

2. To change the prompt name, type the new name in the **Media Name** field and click **Save**.

   The system changes the prompt name and updates the new prompt name to the grid.

3. To add or remove the prompt to any or all user-defined partitions, select the user-defined partitions from the User Defined Partitions section.

4. Click **Save**.

5. To download the prompt, click the **Download Media** button.

6. To delete the prompt, click the **Delete Media** button.

   The system displays a confirmation dialog box.

7. Click **OK** to delete the selected media prompt.

Overwriting an existing Media Prompt

Before you begin

- Ensure that you are assigned an access class of Read Update Create/Delete. For more information, see [Access classes](#) on page 217.

- Ensure that you have associated the media server with the CCMS server. For more information, see [Adding a media server](#) on page 114.

- Log on to CCMA. For more information, see [Logging in to Contact Center Manager Administration Prompt Management](#) on page 270.

- Open the Prompt Management component.

- Ensure that you have added a media prompt. For more information, see [Adding a Media Prompt](#) on page 272.

About this task

You can overwrite an existing media prompt. For example, you have a prompt named Morning_Greeting that states the date and therefore requires to be updated daily. You can add a new prompt with the same name, Morning_Greeting, which overwrites the existing prompt.

Procedure

1. To overwrite an existing prompt, click the **Add Media** button.

2. Click **Select** under the Add Media section to navigate to the media prompt file that you want to upload.

3. In the **Media Name** field, enter the same name as the media prompt that you want to overwrite.

4. To add or remove the prompt to any or all user-defined partitions, select the user- defined partitions from the User Defined Partitions section.

5. Click **Save**.

   The system displays an overwrite confirmation message.

6. Click **OK** to overwrite the prompt.

   Or

   Click **Cancel** to cancel the process.

Changing a Content Group

Before you begin

- Ensure that you are assigned an access class of Read and Update for renaming a content group, and Read Update Create/Delete for deleting a content group. For more information, see Access classes on page 217.

- Ensure that you have associated the media server with the CCMS server. For more information, see Adding a media server on page 114.

- Log on to CCMA. For more information, see Logging in to Contact Center Manager Administration Prompt Management on page 270.

- Open the Prompt Management component.

- Ensure that you have created a Content Group. For more information, see Adding a new Prompts Content Group on page 271.

About this task

You can edit a content group to change the configured properties of the content group

Procedure

1. From the left-hand pane, select the CCMS server in which you want to change the content group.

The system displays the content groups associated with that namespace.

2. To rename a content group, right-click the content group.

   The system displays a popup containing some options.

3. Select the **Rename Content Group** option.

4. Type the name of the content group.

5. Click the **Rename Content Group** button.

   The system renames the content group.

6. To delete a content group, right-click the content group.

   When you delete a content group, you also delete the media present in the content group.

   The system displays a popup containing some options.

7. Select the **Delete Content Group** option.

8. To delete the selected content group, click the **Delete Content Group** button.

Configuring Whisper Skillset announcement files

Before you begin

- Generate or obtain a Whisper Skillset announcement .WAV file, encoded as Linear 16-bit PCM, 8KHz Mono with a sampling rate of 128kbits/sec. The .WAV file must be a minimum of one second long.

  > 🛈 **Important:**

   - The Whisper Skillset .WAV file must be named WSP_<SkillsetName> where <SkillsetName> is the name of the skillset for which you are provisioning the Whisper Skillset announcement file.

   - If you want to provision a zip tone for a specific skillset, the zip tone .WAV file must be named WSP_<SkillsetName> where <SkillsetName> is the name of the skillset for which you are provisioning the custom zip tone.

   - If you want to provision a zip tone for a specific call presentation class, the zip tone .WAV file must be named WSP_<CallPresentationClassName> where <CallPresentationClassName> is the name of the call presentation class for which you are provisioning the custom zip tone.

   The file names are case sensitive.

- Ensure that you are assigned an access class of Read Update Create/Delete. For more information, see <u>Access classes</u> on page 217.

- Ensure that you have associated the media server with the CCMS server.

- Log on to CCMA.

- From the Launchpad, select the Prompt Management component.

About this task

Contact Center supports an optional configuration to provide Whisper Skillset or Call Force Answer (CFA) Zip Tone to agents.

The Whisper Skillset feature allows a brief skillset-specific announcement to be played to agents before they are connected to a customer call. Provision a Whisper Skillset announcement file to support the playing of this skillset-specific announcement.

CFA Zip Tone provides a zip tone to agents who answer a voice call. The zip tone that the agents hear is a default tone. You can provision additional zip tones for individual skillsets or call presentation classes. This file name is case sensitive.

Procedure

1. From the left-hand pane, click the CCMS server in which you want to add the media prompt.

   The system displays the content groups associated with that namespace.

2. Click the content group in which you want to add media prompts.

   The system displays a new page that lists all the prompts stored under that content group.

3. In the left pane, right-click **tones** and select **Add Media**.

   CCMA displays an **Add Media** section.

4. In the **Add Media** section, click **Select** and navigate to the Whisper Skillset announcement or zip tone WAV file.

5. In the **Media Name** box, type the wav file name.

6. To assign the announcement to any or all user-defined partitions, select the user-defined partitions from the User Defined Partitions section.

7. Click **Save**.

   The system uploads the announcement to the media server and adds the new announcement to the grid.

Part 5: Emergency Help

-

Chapter 43: Emergency Help

Use Emergency Help to monitor whether the agents configured on the server require your assistance. You can simultaneously open an Emergency Help display for each server to which you have access. You can keep the displays open on your desktop, or you can minimize the displays to continue working in Contact Center Manager Administration. When an agent presses the Emergency key, the minimized Emergency Help display for the corresponding server automatically opens on your desktop.

For each agent who presses the Emergency key, one line of data appears in the Emergency Help display. The display shows information about the agent, including the agent's name, location, and time when the agent pressed the Emergency key.

Agents can press the Emergency key when they require assistance from the supervisor, for example, if the caller is abusive.

> ✳ **Note:**
>
> In a SIP-enabled Contact Center, after a supervisor releases an Emergency call, the Emergency report displays the status of the Emergency call as "Closed".
>
> In an AML-based Contact Center, after a supervisor releases an Emergency call, the Emergency report continues to display the status of the Emergency call as "Active" until the agent releases the call.

Starting the Emergency Help display

Before you begin

- Ensure that you have a Contact Center Manager Administration user name and password with access to Emergency Help.

About this task

Start the Emergency Help display for the server of your choice to monitor whether the agents configured on the server require your assistance. You can simultaneously open an Emergency Help display for each server to which you have access. You can keep the displays open on your desktop, or you can minimize the displays to continue working in Contact Center Manager Administration. When an agent presses the Emergency key, the minimized Emergency Help display for the corresponding server automatically opens on your desktop.

Procedure

1. Log on to Contact Center Manager Administration.

2. On the Launchpad, click **Emergency Help**.

3. In the left pane, select the server on which to monitor agents.

   The Emergency Help display appears.

Printing an Emergency Help display

Before you begin

- Log on to Contact Center Manager Administration Emergency Help.

About this task

Complete this procedure to print an Emergency Help display.

Procedure

In the **Emergency Help** display, click **Print**.

Exporting an Emergency Help display

Before you begin

- Log on to Contact Center Manager Administration Emergency Help.

About this task

You can export a snapshot of an Emergency Help display to the application server for future reference. The system saves the snapshot data as HTML files with a name containing your user name, a prefix relating to the type of display that you are exporting, and the date and time when you exported the data.

Procedure

1. In the **Emergency Help** display, click **Export**.

   A message box appears, informing you of the HTML file name that you exported.

2. To view the exported display, click **View**.

Viewing an exported Emergency Help display

Before you begin

- Log on to Contact Center Manager Administration Emergency Help.

About this task

View an exported Emergency Help display to view a snapshot of an Emergency Help display that you exported as an HTML file to the Contact Center Manager Administration server.

Procedure

1. In the **Emergency Help** display, on the menu, choose **Displays** > **Manage Exported Displays**.

2. On the Exported Displays dialog box, from the list of HTML files, click the file to view.

   The snapshot of the Emergency Help display appears in a browser window.

Deleting an exported Emergency Help display

Before you begin

- Log on to Contact Center Manager Administration Emergency Help.

About this task

You can delete from the Contact Center Manager Administration server Emergency Help displays that you exported as HTML files.

Procedure

1. On the menu, choose **Displays** > **Manage Exported Displays**.

2. In the **Exported Displays** section, from the list of HTML files, select the check box for each file to delete.

3. Click **Delete** to remove the selected files from the Contact Center Manager Administration server.

Part 6: Outbound configuration

Avaya Aura® Contact Center Client Administration

Chapter 44: Outbound configuration

Use the Outbound Campaign Management Tool to create, modify, and monitor outbound campaigns. OCMT monitors a maximum of 100 simultaneous outbound campaigns with a maximum of 20 000 contacts (email or outbound) per campaign. For more information about Outbound capacity, see *Avaya Aura® Contact Center Overview and Specification*.

About Outbound Campaign Manager Tool

Use Outbound Campaign Manager Tool (OCMT) to create, monitor, and modify outbound telephone campaigns.

You can gain access to the components of OCMT from the toolbar on the left side of the OCMT window.

- **Create & Append**: Create a new campaign, or add call data to an existing campaign. You can add call data manually, import data from an external source, edit the data, and export the data.

- **Modify Campaign**: Pause, restart, or cancel a campaign. You can also change the properties of the campaign, including start date and time, end date and time, and daily start and end times.

- **Progress & Results**: Monitor an ongoing campaign, view results of a completed campaign, and print a campaign summary. The system displays information on the screen graphically in a pie or bar chart.

- **Agent Script**: Create and preview the agent script that includes an introduction and a conclusion, and design the interface for the questions with check boxes and drop-down lists for possible answers.

- **Disposition Codes**: Add, update, and delete disposition codes that you can use in the agent script.

- **General Settings**: View the Time Zone list and the configurations for the log files that are used to track problems in OCMT.

Comments on this document?

- **Help**: Get information on using OCMT.

Historical Reports

You can use historical reports to review campaign performance. Historical reports are available in the Historical Reporting component of Contact Center Manager Administration. Use the following standard historical reports to review outbound campaigns:

- Campaign Call by Call Details: Use this report to list all calls made for each campaign. If an agent does not process a contact, no call record exists in this report. If you select a data range for the report, the data range is based on Contact Closed Time.

- Campaign Script Result Details: Use this report to view the script answers for each campaign.

- Campaign Summary: Use this report to view a summary of each campaign and the disposition codes associated with each campaign.

- Script Summary: Use this report to view a summary of the answers for each agent script.

Scheduling callbacks

Agents can schedule callbacks using Agent Desktop. Agents specify a time and date for the scheduled callback. The Campaign Scheduler Service, which handles callback scheduling, runs at 10 minute polling intervals. If the agent schedules a callback to occur less than 10 minutes after the time of the original call, in certain scenarios the callback does not occur precisely at the scheduled time.

Daily Start and Stop Times

When you define a campaign, you can specify a start time for the campaign. If you do not define the campaign start time, the campaign starts immediately. When you define the campaign start time, the campaign starts at the specified time. When the campaign starts, the system queues all contacts from that campaign to the chosen skillset. The system presents the contacts from the campaign to the agents who are assigned to that skillset.

To avoid calling customers at unsociable hours, you can define Campaign Dialing Hours, that is, the daily start and end time for a campaign. Use OCMT to specify a time the system starts to offer contacts to logged-on agents and a time the system stops presenting contacts to agents. For example, you can specify that the system offers contacts from the outbound campaign to agents who log on to the skillset at 08:00 and finish at 17:00.

Use Campaign Dialing Hours to ensure that you respect the regulatory requirements that surround dialing hours. You specify the time according to the local time of the location of the Contact Center server. You can use the Time Zone list to ensure that the calls made to other time zones also meet the regulatory requirements for dialing hours.

Outbound capacity management

OCMT monitors a maximum of 100 simultaneous outbound campaigns. You cannot define more than 500 active and inactive campaigns. Active campaigns are campaigns that are currently running, waiting to run (pending a start time), or are paused. Inactive campaigns are campaigns that are completed, or cancelled, or expired. You must regularly archive your campaigns to ensure operational efficiency.

Each campaign can have up to 20 000 contacts (email or outbound). However, in order to optimize the system, you must not have more than 1 million contacts in the Multimedia database. You can use the following strategies to ensure that you do not exceed this limit, if your contact center operates at high capacity:

- Define campaigns only as needed, for example by, creating campaigns immediately prior to their usage. This prevents campaigns that are not required for some time from building up in the database. To avoid affecting system performance, load contacts into a campaign during non-peak or out-of-office hours.

- Cancel campaigns that you do not require manually. Use the Pause capability to defer campaigns indefinitely. If you resume a campaign, the system does not present the contacts that are already completed to agents the second time. For more information, see Canceling a campaign on page 314.

- Archive completed, cancelled, and expired campaigns when you no longer need the campaigns for reporting purposes.

Prerequisites to Outbound procedures

- Configure a Contact Center Multimedia server in the Configuration component of Contact Center Manager Administration.

- Assign users basic access rights to the Outbound component in Access and Partition Management using Contact Center Manager Administration.

Logging in to Contact Center Manager Administration for Outbound campaigns

About this task

Open the Outbound Campaign Management Tool in the Contact Center Manager Administration to configure, monitor, and maintain an outbound contact campaign.

Before you begin

- Install and commission Contact Center Manager Administration.

- Ensure that your contact center is licensed for Outbound campaigns.
- Ensure that you have a Contact Center Manager Administration username and password.
- Ensure that you are using Microsoft Edge in Internet Explorer mode.

Procedure

1. In your browser, type the URL of the 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. Do not use the server IP address to log in.

2. In the **User ID** field, type your user ID.

3. In the **Password** field, type your password.

4. Click **Login**.

   If configured in the security settings, CCMA displays the date and time of your last login and the number of failed login attempts since your last successful login.

5. Click **Outbound**.

6. In the left pane, select the appropriate Contact Center Multimedia server.

7. In the right pane, click **Launch Outbound Client**.

   ℹ Important:

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

Defining campaign settings

Before you begin

- Log on to Contact Center Manager Administration.
- Open the Outbound component.

About this task

Define campaign settings as the first step to creating an outbound campaign. You must define the following settings:

- campaign name
- campaign start date and time
- call priority
- daily start and end times (if required to comply with local laws)
- disposition codes

The following settings are optional:

- campaign description
- agent script
- dialer settings
- custom fields
- campaign end date and time

Procedure

1. In the Outbound Campaign Management Tool, click **Create & Append**.
2. On the **Campaign Settings** tab, click **Start Configuring New Campaign**.
3. Select **Create New Campaign**.
4. Under **Campaign Details**, type a name for the campaign and a description (optional).
5. Under **Campaign Start Date & Time**, select either **Start Immediately** or **Start at**.

    ❗ Important:

    The campaign scheduler interval impacts the actual campaign start date and time. For example, if a campaign starts at 9:00 AM and the campaign scheduler interval is one minute, the first contact is queued to the Contact Center Manager Server at 9:01 AM.

6. If you chose **Start At** to start the campaign at a later date, select the start date and time.
7. From the **Call Priority** list, select a priority from 1 to 6, where 1 is the highest.

    Consider the priority of your incoming calls when you select the priority for the outbound campaign. In most Contact Centers, incoming voice calls usually have a higher priority than outbound calls.

8. Under **Agent Desktop Script**, select a script. If you choose **None**, a script is not available for the agents who are handling the outbound calls in this campaign.

    If you want to save the agent script results for a campaign, you must create disposition codes with the Save Agent Script option "yes", and you must instruct your agents to use the disposition codes that save the agent script answers when the contact is closed.

    The system disposition code Completed saves the agent script answers.

9. To display the optional fields, click **Additional Options**. To hide the optional fields again, click **Additional Options** again.
10. Select the Dialer option:
    - If you want the agent to dial the number, select **Manual Agent Dial (Preview)**.
    - If you want the call dialed automatically for the agent, select **Auto Dial Immediately (Progressive)**.
    - If you want the call dialed after the agent reviews the contact details, select **Auto Dial after (seconds)**, and then specify a number of seconds to allow the agent to review the information.

11. Click **Enable Minimum Dial Time**. If you enable the Minimum Dial Timeout, the telephone rings for the specified time. You can set a time between 1 and 180 seconds.

    The Minimum Dial Time setting prevents an agent from making a call and then immediately hanging up.

12. If the agent needs to dial a number to access an external line for an outbound call, in the **Trunk Access Code** box, type the digit or ASCII character.

13. Optionally, add a custom field. Use custom fields to map information in the imported call data that cannot be mapped to the standard fields, or to provide editable fields on Agent Desktop where the agent can gather additional information from the customer (for example, the customer's birth date).

    To add a custom field, in the **Custom fields** section click **Add**.

    In the Insert Custom Field dialog box, type the custom field name, and then click **Insert**.

14. To specify an end date for the campaign, click **Enable**, and then select the date and time.

15. To specify the campaign dialing hours, you can choose **Anytime**, **Local - Current Time Zone Only**, or **Use Customers Time Zone**. If you want to consider the Time Zones for all the customers, choose **Use Customers Time Zone**.

    For more information about the Use Customers Time Zone option, see

16. From the list of available **Disposition Codes**, select the codes available to the Agent at the end of the calls for this campaign.

Procedure job aid: Using time zones

After you select the Use Customer Time Zone option in a campaign, the Time Zone tab appears in the Call Settings section. On the Time Zone tab, you can check which calls are linked to what time zone by checking the Use Time Zone check box. Three possible results can occur:

- Match
- Partial Match
- No Match Found

A Match occurs when the international code and area code are found in your time zone list.

A Partial match occurs when the international code is found but an area code is not. For example, Ireland has an international code of 353 and Dublin has an area code of 1. If you are creating an outbound campaign to Ireland, if you do not want to put in every possible area code, a partial match on 353 puts the contacts into the first found time zone for an area code.

A No Match occurs when neither the international code nor the area code are found. In this case, the contact is called on the Contact Center server time zone.

Any contacts that result in a Partial Match or a No Match are highlighted on the grid. You can still create the campaign with these warnings.

Example of using time zones

About this task

This example creates a campaign configured for time zones by importing contacts from a text file.

Procedure

1. Log on to Contact Center Manager Administration and launch the Outbound Campaign Management Tool.

2. Click **Create & Append**.

3. In the **Name** box, type a unique name for the campaign (for example, My_Time_Zone_Camp).

4. Click **Additional Options**.

5. In the **Campaign Dialing Hours** section, select **Use Customers Time Zone** from the list.

6. Configure the remaining campaign settings as required, and then click the **Call Settings** tab.

7. On the **Call Data Import** tab, click **Import Call Data**.

8. On the **Select Import Type** dialog box, select **Import from Text File**.

9. Click **Next**.

10. Click **Browse** and navigate to your contact list text file.

    For this example, we are using the following contacts:

Steve	Smyth	17895555555
John	Doe	12105555555
Gary	Io	19075555555
Eddy	Walsh	19175555555
Mary	More	16045555555
Brian	Bush	15205555555

11. Click **Next**.

12. In the **Field delimiter** section, select **Tab**.

13. Click **Next**.

14. Map **Field 1** to **First Name** by dragging the Field 1 to the blank space to the left of First Name.

15. Map **Field 2** to **Last Name**.

16. Map **Field 3** to **Phone Number**.

17. Click **Finish**.

18. To split the phone number into an international code and an area code, click the **Call Data Cleanup** tab.

19. Click the **Split Phone Number** tab.

20. Beside **Split Field into**, select **Intl. Code**.

21. From the **Number of digits to split** list, select **1**.

22. Click **Split Phone Number**.

23. On the **OCMT Call Cleanup** message box, click **Continue**.

    The international code is removed from the Phone Number field and appears in the Intl Code field.

24. Beside **Split Field into**, select **Area Code**.

25. From the **Number of digits to split** list, select **3**.

26. Click **Split Phone Number**.

27. On the **OCMT Call Cleanup** message box, click **Continue**.

    The area code is removed from the Phone Number field and appears in the Area Code field.

28. Click the **Skillset Assignment** tab.

29. From the **Attach This Skillset To Rows** list, select **OB_Default_Skillset**.

30. From the **..This Field Is..** list, select **Intl Code**.

31. In the **..To..** field, enter **1**.

32. Click **Update**.

33. Click the **Time Zone** tab.

34. Select the **Use Time Zone** check box.

    A message box appears, indicating that one call is in a warning state. This warning is highlighted on the Call Data Table as a Partial Match. You can either add a new time zone for this area code or accept the partial match. For this example, accept the partial match.

    If your contact list does not have an international code, you can use the International Code feature on the Time Zone tab to quickly fill the entire data grid.

35. Click the **Campaign Activation** tab.

36. In the Campaign Summary, ensure that **Time Zone** is set to **Enabled**.

37. Click **Create Campaign**.

    A message box appears indicating that no agent script has been configured for the campaign.

38. Click **Yes**.

    A message box appears stating that the campaign was created successfully.

39. Click **OK**.

40. To review your campaign, click **Progress & Results**.

41. In the **Campaign List** section, select **My_Time_Zone_Camp**.

42. Click the **Call Details** tab.

   You notice that not all contacts are running. The contacts that are currently in a waiting state are those that are not within the daily start and end times (9:00 to 18:00) in their time zone. You can also confirm the time zone for each contact under the Time Zone column.

Adding a time zone

Before you begin

• Log on to Contact Center Manager Administration.

• Open the Outbound component.

About this task

A list of time zones is configured by default in the Outbound Campaign Management Tool, however the default time zones cover the common countries. You can create your own entries in the time zone list to ensure that outbound calls are placed at appropriate times for various time zones.

> **Important:**
>
> If you have more than one Area Code in a location, you must create a new entry in the Time Zone list for each area code.

Outbound campaigns do not support Daylight Saving Time. The scheduled outbound campaign is set according to the configured system time and adjusts according to the configured time zone, regardless of whether the server or the customer time zone observes Daylight Saving Time.

Procedure

1. On the OCMT toolbar, click **General Settings**.

2. Click the **Time Zone** tab.

3. Review the list of predefined settings to see if the required time zone setting is present. The default time zone settings include those settings for Europe and North America.

4. If the time zone is not configured, click **Insert**.

5. In the **Location Name** box, type the name of the town or city for your time zone.

6. In the **International Code** box, type the number that is used to dial out of the country.

7. In the **Area Code** box, type an area code for the numbers in your location.

8. In the **Time Zone** box, select the time zone for the location. The abbreviations are expanded when you hover your mouse over the list of possible time zones.

9. Click **Insert**.

Updating a time zone

Before you begin

- Log on to Contact Center Manager Administration.
- Open the Outbound component.

About this task

Update a time zone to change the location name, international code, area code, or time zone.

Procedure

1. On the OCMT toolbar, click **General Settings**.

2. Click the **Time Zone** tab.

3. In the table, select the Time Zone you want to update.

4. Click **Update**.

5. In the **Update Time Zone** dialog box, make the required changes.

6. Click **Update**.

Deleting a time zone

Before you begin

- Log on to Contact Center Manager Administration.
- Open the Outbound component.

About this task

Delete a time zone that is no longer required to remove it from the system.

Procedure

1. On the OCMT toolbar, click **General Settings**.

2. Click the **Time Zone** tab.

3. In the table, select the Time Zone you want to delete.

4. Click **Delete**.

5. In the message box, confirm the deletion and click **Yes**.

Importing call data from a text file

Before you begin

- Prepare the call data in a text file.

  🛈 **Important:**

    Ensure that the data you prepare for import does not contain information that violates legal requirements, such as numbers on a national or international Do Not Call register.

- Log on to Contact Center Manager Administration.

- Open the Outbound component.

- Define the campaign settings. See [Defining campaign settings](#) on page 288.

About this task

Import call data from a text file database into your new outbound campaign to save time and prevent data entry errors. You can also add call data manually.

You can also import call data from one of the following sources:

- ODBC database (Open Database Connectivity) — The database can be a user or system DSN, or a file DSN from the directory where the file DSNs are stored. Note: A user name and password can be required. See [Importing call data from an ODBC database](#) on page 296.

- Existing campaign — You can import call data from any existing campaign. See [Importing call data from an existing campaign](#) on page 298.

If a text file contains contacts with a restricted flag, the system deletes these contacts after clicking **Create Campaign** and displays the corresponding message.

Procedure

1. In the Outbound Campaign Management Tool, click **Create & Append**.

2. Click the **Call Settings** tab.

3. On the bottom of the **Call Settings** page, click the **Call Data Import** tab.

4. Click **Import Call Data**.

   If the call data table already contains data, a confirmation message appears.

5. To replace the information in the Multimedia database, select the **Overwrite existing customer data with new customer data** option.

6. In the Select Import Type window, select the **Import From Text File** option.

7. Click **Next**.

8. Click **Browse** to navigate to the appropriate directory.

9. Select the file, and then click **Open**.

10. Click **Next**.

11. To select how the fields are separated in your source file, click Tab, Space, or Character. The default character is a comma.

12. To import a selection of records only from the source file, select the **Enable Record Selection** check box, and then select the beginning and end of the range of records to be imported.

13. If the first row of the source file contains column headers, select the check box.

14. Click **Next**.

15. In the **File Source Fields** box, click the first field name.

16. Drag the name to the **Mapping** column on the appropriate line of the OCMT Fields table.

17. To see which data Field #1 contains, refer to the **Mapping Results** table.

18. Check the mapping for all File Source Fields.

   ❗ Important:

   If the area code and/or international code is in the same field as your telephone number in the source file, map that field to Phone Number in the OCMT Fields. You can split the number up into international code, area code and phone number in the Call Settings window.

19. Review the **Mapping Results** table.

20. To remove the mapping, select the mapping column in the **OCMT Fields** table and click **Clear Mapping**.

21. When you are satisfied with the mapping, click **Finish**.

Importing call data from an ODBC database

Before you begin

- Prepare the call data in an ODBC database.

   ❗ Important:

   Ensure that the data you prepare for import does not contain information that violates legal requirements, such as numbers on a national or international Do Not Call register.

- Log on to Contact Center Manager Administration.

- Open the Outbound component.

- Define campaign settings. See Defining campaign settings on page 288.

About this task

Import call data from an ODBC database into your new outbound campaign to save time and prevent data entry errors. You can also add call data manually instead of, or after you import call data.

You can also import call data from one of the following sources:

- Text file — The data fields within a text file can be in any order; however, the order and the delimiter must be consistent throughout the file. See <u>Importing call data from a text file</u> on page 295.

- Existing campaign — You can import call data from any existing campaign. See <u>Importing call data from an existing campaign</u> on page 298.

If an ODBC database contains contacts with a restricted flag, the system deletes these contacts after clicking **Create Campaign** and displays the corresponding message.

Procedure

1. On the Outbound Campaign Management Tool, click **Create & Append**.

2. Click the **Call Settings** tab.

3. On the bottom of the Call Settings page, click the **Call Data Import** tab.

4. Click **Import Call Data**.

   If the call data table already contains data, a confirmation message appears.

5. To replace the information in the Multimedia database, select the **Overwrite existing customer data with new customer data** option.

6. In the Select Import Type window, select the **Import From ODBC** option.

7. Click **Next**.

8. To select an **ODBC System DSN**, select the ODBC System DSN from the list.

9. To select an **ODBC User DSN**, select the ODBC User DSN from the list.

10. To select an **ODBC File DSN**, click **Browse** and then navigate to the location of the DSN file.

11. Select the DSN file and click **Save**.

12. If the ODBC source requires a logon ID, in the **Login Information** section, type the user name and password.

13. Click **Next**.

14. Click the table name or view name from which to import.

15. Click **Next**.

16. In the **Data Source Table Columns** box, click the first column name.

17. Drag the column name to the **Mapping** column on the appropriate line of the **OCMT Fields** table.

18. Check the Data Source Table Columns mapping for all **Data Source Table Columns.**

19. If the area code and/or international code is in the same field as the telephone number in the source database table, map that field to **Phone Number** in the fields.

   You can use the Call Settings window to split the number up into international code, area code and phone number.

20. To remove the mapping, select the mapping column in the **OCMT Fields** table and click **Clear Mapping.**

21. To import only a selection of records from the source file, click the **Select Range** check box, and then select the beginning and end of the range of records to import.

   If the start record is the same as the end record, the data in that record (at least one) is imported.

22. When you are satisfied with the mapping, click **Finish**.

Importing call data from an existing campaign

Before you begin

- Log on to Contact Center Manager Administration.

- Open the Outbound component.

- Define campaign settings. See <u>Defining campaign settings</u> on page 288.

About this task

Import call data from an existing campaign into your new outbound campaign to save time and prevent data entry errors. You can also add call data manually. See <u>Adding call data manually</u> on page 299.

Avaya recommends that you ensure the new campaign uses the same custom fields as the campaign from which you are importing call data. You can ensure this by clicking Start Configuring New Campaign and selecting Create using previous campaign settings. and choosing a previous campaign. A list of available campaigns appears. Select the campaign you want to import contacts from and click OK.

Procedure

1. Click **Create & Append**.

2. Click the **Call Settings** tab.

3. On the bottom of the Call Settings page, click the **Call Data Import** tab.

4. Click **Import Call Data**.

   If the call data table already contains data, a confirmation message appears.

5. To replace the information in the Multimedia database, select the Overwrite existing customer data with new customer data option.

6. In the Select Import Type window, select the **Create From Existing Campaign** option.

7. Click **Next**.

8. From the list, select the appropriate campaign.

9. Click **Next**.

10. To import all calls, select the **Import All Calls** option.

11. To filter the calls to import, select the **Filter Calls** option.

12. In the **Call Filter** list, select the check box for each Disposition Codes that determine which calls to import.

13. Click **Finish**.

Adding call data manually

Before you begin

- Log on to Contact Center Manager Administration.

- Open the Outbound component.

- Define campaign settings. See [Defining campaign settings](#) on page 288.

About this task

Add call data manually if you have no data to import to add the information to the call record for an outbound campaign.

Procedure

1. On the Outbound Campaign Management Tool, click **Create & Append**.

2. Click the **Call Settings** tab.

3. Click in the first empty row of the **Call Data Table**.

4. Type the customer information in the appropriate fields.

Validating a telephone number or code

Before you begin

- Log on to Contact Center Manager Administration.

- Open the Outbound component.

- Define campaign settings. See [Defining campaign settings](#) on page 288.

- Add call data using an importing method, or by adding call data manually.

About this task

Validate a telephone number or code to ensure that the Phone Number, Area, and Intl Code columns contain only numbers and spaces. You must ensure that there are no non-numeric characters, such as hyphens or brackets.

Procedure

1. On the Outbound Campaign Management Tool, click **Create & Append**.

2. Click the **Call Settings** tab.

3. Click **Call Data Cleanup**.

4. On the **Call Data Cleanup** page, click **Validate Call data**.

   The Call Validation window reports how many calls failed validation and gives you the option to delete or review these calls.

5. To review and correct the data, click **Review**.

   The invalid calls are highlighted in the table.

6. To delete all the invalid calls, click **Delete**.

Inserting text

Before you begin

- Log on to Contact Center Manager Administration.
- Open the Outbound component.
- Define campaign settings. See <u>Defining campaign settings</u> on page 288.
- Ensure that you have data in the Call Data table.

About this task

Insert text into the call data to replace or change customer data for the outbound campaign. You can append, prepend, or replace the existing text.

Procedure

1. On the Outbound Campaign Management Tool, click **Create & Append**.

2. Click the **Call Settings** tab.

3. Click **Call Data Cleanup.**

4. Click the **Insert Text** tab.

5. Select one of the text change options, overwrite, prepend, or append.

6. In the **Text to Add** box, type the text you want to append, prepend, or replace in a field.

7. From the **Select Field** list, select a column to change or replace the text.

8. To search for and replace text in all rows of the table, click **All Calls**.

9. To search for and replace text in only selected rows of the table, select the specific rows, and then click **Selected Calls**.

10. Click **Insert Text**.

11. Click **Continue** to confirm you want to add the selected text.

12. Click **OK**.

Procedure job aid

Value	Variable
Overwrite	Replace the current contents of the field.
Prepend	Add the text to the beginning of the current text in the field.
Append	Add the text to the end of the current text in the field.
Text to add	Type the text you want to appear.

Removing text

Before you begin

- Log on to Contact Center Manager Administration.
- Open the Outbound component.
- Define campaign settings. See [Defining campaign settings](#) on page 288.
- Ensure that you have data in the Call Data table.

About this task

Remove text from the Call Data table that is no longer valid.

Procedure

1. On the Outbound Campaign Management Tool, click **Create & Append**.

2. Click the **Call Settings** tab.

3. On the Call Settings page, click **Call Data Cleanup**.

4. Click the **Remove Text** tab.

5. In the **Text to remove** box, type the text for which to search and remove

6. To remove all text from the selected column, click **Remove All Text**.

7. From the **Select Field** list, select the column from which to search and remove the text.

8. From the **Occurrence** list, select the option that describes what you want to remove.

9. To search for and remove text in all rows of the table, click **All Calls**.

10. To search for and remove text in only selected rows of the table, select the specific rows, and then click **Selected Calls**.

11. Click **Remove Text**.

12. Click **Continue** to confirm that you want to delete the selected text.

13. Click **OK**.

Replacing text

Before you begin

- Log on to Contact Center Manager Administration.

- Open the Outbound component.

- Define campaign settings. See

- Ensure that you have data in the Call Data table.

About this task

Replace text in your Call Data table with corrected information in one location or more.

Procedure

1. On the Outbound Campaign Management Tool, click **Create & Append**.

2. Click the **Call Settings** tab.

3. Click **Call Data Cleanup**.

4. Click the **Replace Text** tab.

5. In the **Text to replace** box, type the existing text for which to search and replace.

6. In the **Text to replace with** box, type the new text to replace.

7. From the **Select Field** list, select the column from which to search and replace the text.

8. To search for and replace text in all rows of the table, click **All Calls**.

9. To search for and replace text in only selected rows of the table, select the specific rows, and then click **Selected Calls**.

10. Click **Replace Text**.

11. Click **Continue** to confirm that you want to replace the selected text.

12. Click **OK**.

Splitting a phone number

Before you begin

- Log on to Contact Center Manager Administration.

- Open the Outbound component.

- Define campaign settings. See

- Ensure that you have data in the Call Data table.

About this task

Split a phone number in your Call Data table if the international code or area code is combined with the telephone number in the imported data. You must ensure that the phone number in the Call Data table is valid by removing a specified number of digits from the beginning of the Phone Number and adding those digits to the selected Intl or Area Code column.

Procedure

1. On the Outbound Campaign Management Tool, click **Create & Append**.

2. Click the **Call Settings** tab.

3. Click **Call Data Cleanup**.

4. Click the **Split Phone Number** tab.

5. From the **Split Field into** list, select **Intl Code** or **Area Code**.

6. In **Number of digits to split**, type or select the number of digits to remove from the **Phone Number** and add to the selected **Code** column.

7. To split the phone number in all rows of the table, click **All Calls**.

8. To split the phone number in only selected rows of the table, select the specific rows, and then click **Selected Calls**.

9. Click **Split Phone Number**.

10. Click **Continue** to split the phone number.

11. Click **OK**.

Adding area and international codes

Before you begin

- Log on to Contact Center Manager Administration.

- Open the Outbound component.

- Define campaign settings. See .

- Ensure that you have data in the Call Data table.

About this task

Add area and international codes if your imported data does not include area and/or international codes to ensure that your Call Data is complete. You can add the same code to multiple rows at the same time.

This operation overwrites existing data in the selected column and rows.

Procedure

1. On the Outbound Campaign Management Tool, click **Create & Append**.

2. Click the **Call Settings** tab.

3. At the bottom of the **Call Settings** tab, click **Call Data Cleanup**.

4. Click the **Insert Text** tab.

5. Select **Overwrite**.

6. In the **Text To Add** box, type the international code or area code to add.

7. In **Select Field**, select either **Intl Code** or **Area Code** in which to add the code.

8. To add the code in all rows of the table, click **All Calls**.

9. To add the code in only selected rows of the table, select the specific rows, and then click **Selected Calls**.

10. Click **Insert Text**.

Checking the length of fields

Before you begin

- Log on to Contact Center Manager Administration.

- Open the Outbound component.

- Define campaign settings. See .

- Ensure that you have data in the Call Data table.

About this task

Check the length of fields in the Call Data table to determine the validity of a field in a customer record. For example, you can see which records contain the incorrect number of digits for the telephone number. When the search results appear, you can either correct the content of the field or delete the record.

Procedure

1. On the Outbound Campaign Management Tool, click **Create & Append**.

2. Click the **Call Settings** tab.

3. On the Call Settings tab, click **Call Data Search**.

4. Click the **Length Search** tab.

5. From the **Select Field** list, select the column on which to search the length.

6. In the **Operation** box, select that mathematical operation that applies to your search:

   - Greater than

- Equal to

- Less than

7. In the **Number of digits** box, type or select the number of digits that each entry in the column must contain.

8. If you want the length check to ignore spaces, select the **Ignore Spaces** check box.

9. To check the length on specific rows of the table, select the rows, and then click **Selected Calls**.

10. Click **Search**.

    Call data that matches your criteria are highlighted and moved to the top of the Call Data Table.

11. Change the data.

12. To delete the rows, click **Delete Checked Calls**.

Checking for alphabetic characters

Before you begin

- Define campaign settings. See

- Ensure that you have data in the Call Data table.

About this task

Check the fields for particular alphabetic characters or symbols to correct the data or delete the entire record from the Call Data table in the outbound campaign.

Procedure

1. On the Outbound Campaign Management Tool, click **Create & Append**.

2. Click the **Call Settings** tab.

3. On the Call Settings page, click **Call Data Search**.

4. Click the **Numeric Search** tab.

5. From the **Select Field** list, select the column on which to do the digit check.

6. To do the digit check on specific rows of the table, select the rows, and then click **Selected Calls**.

7. Click **Search**.

    Rows that include non-numeric characters in the selected column are highlighted and moved to the top of the table.

8. Change the data.

9. To delete the rows, click **Delete Checked Calls**.

Checking for a value

Before you begin

- Define campaign settings. See [Defining campaign settings](#) on page 288.

- Ensure that you have data in the Call Data table.

About this task

Check for fields that contain a specific value (for example, to find records with a particular area code) in your Call Data table to ensure that the records are all valid. For example, you can search for records where the telephone numbers are not in your local area.

Procedure

1. On the Outbound Campaign Management Tool, click **Create & Append**.

2. Click the **Call Settings** tab.

3. On the Call Settings page, click **Call Data Search**.

4. Click the **Value Search** tab.

5. From the **Select Field** list, select the column on which to do the value search.

6. In the **Operation** box, select the operation for the required condition:

    - Equal to

    - Not equal to

    - Contains

    - Does not contain

7. In the **Select Value** box, type the information that corresponds to the operation and selected field to locate.

8. To do the length check on specific rows of the table, select the rows, and then click **Selected Calls**.

9. Click **Search**.

    Call data that matches your criteria are highlighted and moved to the top of the Call Data table.

10. Change the data.

11. To delete the rows, click **Delete Checked Calls**.

Checking for duplicate call data

Before you begin

- Define campaign settings. See [Defining campaign settings](#) on page 288.

- Ensure that you have data in the Call Data table.

About this task

Check the records in your Call Data table for duplicates in a field or in fields that you select. You can choose to delete all duplicate records, to review them before changing or deleting them, or to allow duplicate calls in the campaign.

Procedure

1. On the Outbound Campaign Management Tool, click **Create & Append**.

2. Click the **Call Settings** tab.

3. At the bottom of the Call Settings page, click **Call Data Cleanup**.

4. Click **Duplicate Calls**.

5. In the **Select fields:** list, select the field or fields on which to search for duplicate information.

6. Click **Select Duplicate Calls**.

   If duplicate records are found, the Outbound Campaign Management Tool Duplicate Calls dialog box asks if you want to delete or review the duplicates.

   ❗ Important:

   Duplicates are only found on records that you selected in the Duplicate Field Search. If you didn't choose all fields, you do not see unique records.

7. Click **Review** to review the duplicate calls.

   The duplicate calls appear at the top of the table and the second (and third or more) of each group of duplicate calls is highlighted.

8. To allow duplicate calls to remain in the campaign, select the duplicate calls and click **Allow Selected Duplicates**.

   Duplicate Allowed appears in the **Duplicate Status** column for the selected duplicate calls.

9. To delete the duplicate calls, click **Delete** to retain a single copy of each record and delete the duplicate records.

Checking customer matches

Before you begin

- Log on to Contact Center Manager Administration.

- Open the Outbound component.

- Define campaign settings. See [Defining campaign settings](#) on page 288.

- Ensure that you have data in the Call Data table.

About this task

Check customer matches to determine if customers present in the call data table match or closely match a customer record in the Contact Center Multimedia database. The customer match feature indicates a close match to existing customers in the Multimedia database so the Administrator creating the outbound campaign can determine whether the information in the call data table is a new customer, for which you must create a new record, or an existing customer.

For example, if Mike Smith 091 12345 is present in the Multimedia database, and Michael Smith 091 12345 is in the call data table, when you run a customer match, the similarities are displayed to the Administrator.

If Enable Partial Match is selected, similarities between the call data table and the Multimedia database are shown based on partial matches of the telephone number. For example, if the call table contains Michael Smith 12345, and the Multimedia Database contains Mike Smith 091 12345, the partial match highlights the similarities. If Partial Match is not enabled, the entry in the call data table is considered new.

Procedure

1. On the Outbound Campaign Management Tool, click **Create & Append**.

2. Click the **Call Settings** tab.

3. At the bottom of the **Call Settings** tab, click the **Customer Match** tab.

4. To compare information based on a partial phone match, select the **Enable Partial Match** check box.

5. Click **Check Customer Association**.

   All calls with matching phone numbers, but differences in the other fields, are highlighted in the call data table. A check box appears in the Customer Status column of each row.

6. To resolve the conflicting information for a call, select the check box in the **Customer Status** column.

7. In the Customer Matching window, compare the Campaign Customer Details with the Existing Customer Details.

8. Select whether to add this record as a new customer, or use the existing customer information.

9. Click **OK**.

10. Review all conflicting call data.

11. Click **OK**.

Procedure job aid

Variable	Value
Partial Match	Select to compare information based on a partial phone match. Entries can be matched with entries in the Contact Center Multimedia database where the area code and international code do not match. This allows information in the Contact Center Multimedia database or the call data table to be updated.

Comparing call data with the Do Not Call list

Before you begin

- Log on to Contact Center Manager Administration.
- Open the Outbound component.
- Define campaign settings. See
- Ensure that you have data in the Call Data table.

About this task

Compare call data with the Contact Center Multimedia Do Not Call list to ensure that you are not violating laws or making incorrect calls to numbers such as an emergency number.

Contact Center Multimedia maintains an internal Do Not Call list of numbers. This list contains numbers that Contact Center agents have dispositioned as Do Not Call after previous contacts with customers. When you import a new campaign you must check the campaign numbers against the internal Do Not Call list to remove Do Not Call numbers from the campaign.

> ❗ **Important:**
>
> The internal Do Not Call list is not the same as statutory registers of do not call numbers–you must check your call data against external registers before importing it to Contact Center.

If you do not run this check manually, or do not delete the highlighted calls, the calls are created in Contact Center Multimedia. However, the calls are closed immediately and the disposition code is set to Do Not Call, ensuring that the call is not presented to an agent.

Any customer number dispositioned as 'Do Not Call' is tagged as a 'Do Not Call' (DNC) number in the Contact Center Multimedia Do Not Call list. To set or clear the barred status of any required number, Agent Desktop is used to edit the phone number associated with the relevant customer record. You can use Agent Desktop to clear a number from the Do Not Call list or barred status.

Procedure

1. On the Outbound Campaign Management Tool, click **Create & Append**.

2. Click the **Call Settings** tab.

3. On the Call Settings page, click the **Do Not Call** tab.

4. Click **Select 'Do Not Call' Numbers**. The status of each call appears in the call data table, and any calls with the status Call Not Permitted is highlighted.

5. Review the highlighted calls and, if desired, delete them from the call data table.

Assigning skillsets to outbound campaign calls

Before you begin

- Define campaign settings. See [Defining campaign settings](#) on page 288.
- Ensure that you have data in the Call Data table.

About this task

Assign skillsets to outbound campaign calls to determine which groups of agents work on the campaign. You create the assignment based on the value of a field you specify from the outbound call data.

Procedure

1. On the Outbound Campaign Management Tool, click **Create & Append**.
2. Click the **Call Settings** tab.
3. On the Call Settings page, click the **Skillset Assignment** tab.
4. From the **Attach This Skillset To Rows** list, select a skillset to which you want to assign calls in this campaign.
5. From the **..This Field Is..** list, select the field that you want to use as a criterion for assigning a campaign call to the skillset.
6. In the **..To..** field, enter the value that you want to a campaign call to match in the specified field to assign it to the skillset.
7. Click **Update**.
8. Click **Continue**.
9. Click **OK**.

Printing a summary of a new campaign

Before you begin

- Log on to Contact Center Manager Administration.
- Open the Outbound component.
- Complete the outbound campaign.

About this task

Print a summary of a new campaign when you are finished defining the campaign settings to record all of the settings for the current campaign.

Procedure

1. On the Outbound Campaign Management Tool, click **Create & Append**.

2. Click the **Campaign Activation** tab.

3. Click **Print Campaign Summary**.

Activating a campaign

Before you begin

- Log on to Contact Center Manager Administration.

- Open the Outbound component.

- Complete configuring the outbound campaign.

About this task

Activate a campaign to load the call data and campaign settings into the Contact Center Multimedia database so that the campaign is ready to begin on the date selected.

You cannot activate a campaign until it is validated by the Outbound Campaign Manager Tool.

Procedure

1. On the Outbound Campaign Manager Tool, click **Create & Append**.

2. Click the **Campaign Activation** tab.

3. Click **Create Campaign**.

   A message confirms that the campaign was created successfully.

   ✱ **Note:**

   If call data contains contacts with a restricted flag, the system deletes these contacts from the campaign and displays the corresponding message.

4. Click **OK**.

Procedure job aid

The Outbound Campaign Manager Tool performs a validation on the Call Data table. The Call Data must meet the following requirements:

- The campaign size cannot exceed 20 000 contacts.

- Any customer can receive only one call per campaign.

- Duplicate customers based on an exact email match or exact first name and last name and phone number (international code, area code, and phone number) are not permitted.

- The mandatory phone number field must contain only numeric values and spaces, and cannot exceed 32 characters.

- The area code must contain only numeric values and spaces, and can not exceed 10 characters.

- The international code field must contain only numeric values and spaces, and cannot exceed 10 characters.

- The first name field cannot exceed 50 characters.

- The last name field cannot exceed 100 characters.

- If an email address field is included, an @ symbol is required, and the address cannot exceed 128 characters.

- All other Call Data table fields cannot exceed 128 characters.

Adding call data to an existing campaign

Before you begin

- Log on to Contact Center Manager Administration.

- Open the Outbound component.

- Understand how to add call data manually, or import call data from an external source.

- Understand how to edit the call data in your outbound campaign.

- Understand how to activate the campaign. See

About this task

Add call data to an existing campaign to add new customers to a campaign already in progress.

Procedure

1. On the Outbound Campaign Management Tool, click **Create & Append**.

2. On the **Campaign Settings** tab, click **Append Calls to Existing Campaign**.

3. In the **Existing Campaigns** box, select the campaign from the list.

4. Click **OK**.

5. On the **Call Settings** tab, add or import the call data.

6. Edit the new call data in your campaign.

7. Activate the changed campaign.

Changing campaign settings

Before you begin

- Log on to Contact Center Manager Administration.

- Open the Outbound component.

- Understand how to add call data manually, or import call data from an external source.

- Understand how to edit the call data in your outbound campaign.

- Understand how to activate the campaign. See

About this task

Change campaign settings such as the start and end date and time, the daily start and end times, the dialer settings, the agent script, and disposition codes to modify an existing campaign.

You cannot change other settings in the campaign, such as agent skillset.

If the campaign has already started, you cannot change the start date and time or the agent script.

Procedure

1. On the Outbound Campaign Manager Tool, click **Modify Campaign**.

2. In the **Campaign List** box, select the campaign to modify.

3. To change date and time information for the campaign, click the **Date/Time Settings** tab, and then select the new campaign start date and time, the new campaign end date and time, or the new daily start and end time.

4. Click **Modify Date/Time Settings** to save changes

5. To change the dialer settings for the campaign, click the **Dialer Settings** tab, and then specify the new dialer mode setting and the new dialer miscellaneous settings.

6. Click **Modify Dialer Settings** to save changes

7. To change the Agent Script for a campaign, click the **Agent Script** tab, and then specify the new agent script.

8. Click **Apply Selected Agent Script** to save any changes.

9. To change the disposition codes for a campaign, click the **Disposition Codes** tab, and then select the additional disposition codes, and clear check boxes beside the disposition codes you do not want.

10. Click **Apply Selected Disposition Codes** to save any changes.

Pausing a campaign

Before you begin

- Log on to Contact Center Manager Administration.

- Open the Outbound component.

- Ensure that your outbound campaign is running.

About this task

Pause a campaign to stop the current outbound campaign. This action changes the state of the contacts in the selected campaign in the Contact Center Manager Server and in the Contact Center Multimedia database to waiting.

Procedure

1. On the Outbound Campaign Management Tool, click **Modify Campaign**.

2. In the **Campaign List** box, select the campaign you want to pause.

3. Click the **Campaign Status** tab.

4. Click **Pause Campaign**.

5. Click **OK** to confirm the pausing of the campaign.

Canceling a campaign

Before you begin

- Log on to Contact Center Manager Administration.

- Open the Outbound component.

- Ensure that you have an outbound campaign configured.

About this task

Cancel a campaign to permanently stop routing the outbound calls from the campaign. By canceling a campaign, you delete the contacts in the selected campaign from the Contact Center Manager Server. Their status is set to Closed in the Contact Center Multimedia database, and the contacts are assigned the disposition code of Campaign cancelled.

Procedure

1. On the Outbound Campaign Management Tool, click **Modify Status**.

2. In the **Campaign List** box, select the campaign you want to cancel.

3. Click the **Campaign Status** tab.

4. Click **Cancel Campaign**.

5. Click **OK** to confirm the cancellation of the campaign.

Next steps

Campaigns remain in the OCMT Campaign List as long as any associated contacts remain in the Multimedia database. You cannot remove or delete a campaign directly from the OCMT.

If you want to remove the campaign from the Campaign List, create an Outbound Campaign cleanup rule, using the Delete Campaign option, and run a cleanup task with this rule.

Restarting a campaign

Before you begin

- Log on to Contact Center Manager Administration.

- Open the Outbound component.

About this task

Restart a campaign that you paused or cancelled to continue routing outbound calls to customers.

Procedure

1. On the Outbound Campaign Management Tool, click **Modify Campaign**.

2. In the **Campaign List** box, select the campaign you want to restart.

3. Click the **Campaign Status** tab.

4. Click **Restart Campaign**.

5. Click **OK** to confirm the restarting of the campaign.

Monitoring campaign progress and results

Before you begin

- Log on to Contact Center Manager Administration.

- Open the Outbound component.

- Ensure that an outbound campaign is running, or complete.

About this task

Monitor and outbound campaign progress and results to see how the outbound campaign is progressing, and the types of responses your agents are receiving. You can monitor the progress and results of any campaign. Both summary and detailed information are available for each campaign.

Procedure

1. On the Outbound Campaign Management Tool toolbar, click **Progress & Results**.

2. In the **Select Campaign** box, select the campaign you want to monitor.

   A summary of the campaign settings and progress appears in the Campaign Summary box.

3. To view a summary of the contact status for all contacts in the selected campaign, click the **Call Status Chart** tab.

4. To view a summary of the disposition codes for all closed contacts in the selected campaign, click the **Disposition Codes Chart** tab.

5. To view detailed information for each call in the campaign showing status of each call, as well as the customer information defined during the campaign setup, click the **Call Details** tab.

6. To view the history of status changes for the campaign, click the **Campaign History** tab.

7. To change the display in the Call Status Chart and Disposition Codes Chart tabs from a pie chart to a bar chart, or vice versa, click **Display Pie Chart** or click **Display Bar Chart**.

8. To refresh the data displayed in this window, click **Refresh**.

Printing a summary of an existing campaign

Before you begin

- Log on to Contact Center Manager Administration.

- Open the Outbound component.

- Ensure that the outbound campaign is complete.

About this task

Print a summary of an existing campaign to review the settings and results of the completed campaign in printed format.

Procedure

1. In the Outbound Campaign Management Tool, click **Progress & Results**.

2. In the **Campaign List** box, select the campaign you want to print.

   A summary of the campaign settings and progress appears in the Campaign Summary box.

3. Click the **Print Campaign Details** button.

Creating a new agent script

Before you begin

- Prepare between one and 40 questions for the agent script, an introduction and a conclusion.

- Prepare the possible answers for the agent if you want specific wording in a response from the customer.

- Log on to Contact Center Manager Administration.

- Open the Outbound component.

About this task

Create a new agent script that contains the introductory and concluding text the agent reads, as well as a maximum of 40 questions the agent can ask the customer. The campaign administrator can customize the script by specifying default and possible allowed answers to questions.

You cannot change an agent script after you save it. Avaya recommends that you click Preview Script, and carefully review the script before saving it.

To save the agent script results for a campaign, you must create a disposition code with the save agent script option set to Yes.

Procedure

1. In the Outbound Campaign Management Tool, click **Agent Script**.

2. Click **Configure New Agent Script**.

3. In the **Introduction** box, type the text the agent reads to begin the call.

4. In the **Conclusion** box, type the text the agent reads at the end of the call.

5. Under **Agent Script Questions**, in the **Question** box, type the first question.

6. If you want to specify the possible answers to the question, in the **Allowed Answers** box, type the answers, separated by a comma; otherwise, leave this box blank.

7. In the **GUI Component** box, select a format for the agent to record the response.

8. If you want the agent to see a default answer to a question, in the **Default Answer** box, type the appropriate response.

9. If the response requires a text box, for example, for name or address, then in the **Allow Free Text** box, click the check box.

10. Create additional questions.

11. Click **Preview Script**.

    The format of the script questions is validated. If errors are found, the incorrect questions are highlighted.

12. If errors are found, correct the errors, then click **Preview Script** again.

13. In the **Save Agent Script** box, type a name, and then click **Save Script**.

Variable definitions

Name	Description
Agent Script name	The name of the agent script. The agent script name must be unique.

Table continues…

Name	Description
Allow free text	A text box that allows an agent to type responses that cannot be recorded using a GUI component. You must have a text box if there is no other user interface component. You can also include a text box with a combo box or radio buttons. The text box allows the agent to enter addition information.
Allowed Answers	The possible answers an agent can enter based on the customer's answers to each question. Each answer must be separated by a comma. You can leave this box blank and allow any answers. The maximum number of allowed answers is 32.
Conclusion	The text that an agent reads to conclude the outbound call. A conclusion is a mandatory part of the agent script and cannot exceed 1024 characters.
Default answer	The answer automatically selected in the agent script. The default answer must exist in the allowed answers for a question in the agent script.
GUI component	If you specify allowed answers, you must also specify how the agent selects the answers. You can use one of the following: • None • Combo Box • Radio Button • Check Box • Check List Box If you select a GUI component, you must ensure there is at least one allowed answer.
Introduction	The text that an agent reads to begin the outbound call. An introduction is a mandatory part of the agent script and cannot exceed 1024 characters.
Questions	The text that an agent asks the caller in an outbound call. Between one and 40 questions can be included in a script. Each question cannot exceed 1024 characters.

Creating an agent script from an existing script

Before you begin

- Log on to Contact Center Manager Administration.

- Open the Outbound component.

- Prepare between one and 40 questions for the agent script, an introduction and a conclusion.

- Prepare the possible answers for the agent if you want specific wording in a response from the customer.

About this task

Create agent script from an existing script to copy details from another script to a new campaign and modify them.

You cannot make changes to an agent script after it has been saved.

Procedure

1. On the Outbound Campaign Management Tool, click **Agent Script**.

2. Click **Create from Existing Agent Script**.

3. In the **Existing Agent Scripts** box, from the list, select the script.

4. Change the introduction, questions, or conclusion as required.

5. Change or add questions as required.

6. To delete a question (or questions) from the script, select the row (or rows) containing the question you want to delete, and then click **Delete Selected Question**.

   To delete more than one question at a time, press the **CTRL** key while selecting the rows that contain the questions you want to delete.

7. To preview the script as the agent sees it, click **Preview Script**.

   The format of the script questions is validated. If errors are found, the incorrect questions are highlighted.

8. If errors are found, correct the errors, and then click **Preview Script** again.

9. To save the script, type a new name in the **Save Agent Script** box, and then click **Save Script**.

Adding a disposition code

Before you begin

- Log on to Contact Center Manager Administration.

- Open the Outbound component.

About this task

Add a disposition code to an outbound campaign to provide a mechanism for agents to record the status of an outbound call. You can view the disposition code status for each campaign.

Nine standard disposition codes are provided, but you can add more disposition codes. You can configure a maximum of 40 disposition codes.

Procedure

1. On the Outbound Campaign Management Tool, click **Disposition Codes**.

2. Click **Insert**.

3. In the **Insert Disposition Code** dialog box, in the **Disposition Code Name** box, type a descriptive name.

4. In the **Retry Timeout** box, type the length of time in minutes after which the contact is presented again to an agent.

5. If you do not want a retry call made, leave this field blank.

6. In the **Max Number of Retries** box, type the number of times a contact is presented after the initial offering to an agent.

7. To configure whether the agent script is saved on contact closure, Select **Yes** or **No**.

8. To configure whether a voice call is required to complete the contact, select **Yes** or **No**.

9. Click **Insert**.

Variable definitions

Name	Description
Disposition Code Name	The name of the disposition code. The name reflects the purpose of the closing of the outbound contact. Nine standard disposition codes are provided: • Number Busy • No Answer • Answer Machine • No such number • Hung up! • Wrong Number • Do Not Call • Re-schedule Call • Completed

Table continues…

Name	Description
Retry Timeout	The length of time in minutes after which the contact is presented again to an agent.
	If you create a disposition code that indicates the call was not completed, such as Re-schedule call, you can configure the amount of time before the contact is presented again to an agent.
	Only appropriate disposition codes, such as Number Busy, include a retry timeout.
Maximum number of retries	The number of times a contact is presented to an agent.
	If you create a disposition code that indicates the call was not completed, such as Re-schedule call, you can configure the maximum number of times to retry the call.
Save Agent Script	Click yes to save the agent script results for a campaign along with the disposition code. Instruct your agents to use the disposition codes that save the agent script answers when the contact is closed.
	If you sell a product, create a disposition code, Sale Made, with the Save Agent Script option Yes, to save the customer answers for future marketing.
Voice Call Required	Click yes if a voice call is required to complete the contact.
	If an agent cannot speak the same language as a customer, the agent can select a disposition code that does not require a voice call to be made.

Updating a disposition code

Before you begin

- Log on to Contact Center Manager Administration.
- Open the Outbound component.
- Create a disposition code. See [Adding a disposition code](#) on page 319.

About this task

Update a disposition code to change the properties of the code the agent uses to record the outcome of an outbound call.

Procedure

1. On the Outbound Campaign Management Tool, click **Disposition Codes**.

2. In the table, click the disposition code you want to update.

3. Click **Update**.

4. In the **Update Disposition Code** dialog box, change the **Name**, **Retry Timeout** and/or **Max Number of Retries** as required.

5. Click **Update**.

Deleting a disposition code

Before you begin

- Log on to Contact Center Manager Administration.

- Open the Outbound component.

- Ensure that the disposition code is not used in a campaign. If it is, you must first archive or purge the campaign from the Multimedia database using the Contact Center Multimedia Administration Archive utility.

- Ensure that the disposition code that you want to delete is not one of the nine standard disposition codes—Number Busy, No Answer, Answer Machine, No Such Number, Hung Up!, Wrong Number, Do Not Call, Re-schedule Call, or Completed.

About this task

Delete a disposition code only if no campaign uses that disposition code.

Procedure

1. On the Outbound Campaign Management Tool, click **Disposition Codes**.

2. In the table, click the disposition code to delete.

3. Click **Delete**.

4. Click **OK** to confirm the deletion.

Closing a contact with a disposition code

About this task

You can close one or more campaign contacts when a campaign is running, and can apply a disposition code to the closed contacts.

Before you begin

- Log on to Contact Center Manager Administration.

- Open the Outbound component.

- Ensure that your outbound campaign is running.

Procedure

1. On the Outbound Campaign Manager Tool, click **Progress & Results**.

2. Under Campaign List, select the campaign containing the contacts you want to close.

3. Click the **Call Details** tab.

4. From the list, select the call that you want to close.

   To select multiple calls, press the **Ctrl** key while you select each call.

5. Right-click on the selected calls and select **Close With Code**.

   The **Select Disposition Code** drop-down list appears.

6. From the drop-down list, select the disposition code and click **OK**.

   OCMT closes the selected calls and applies the selected disposition code.

   ❶ **Important:**

   System disposition codes configured with Max Number of Retries do not close a call until OCMT attempts all retries, and OCMT excludes these disposition codes from the drop-down list. OCMT also excludes user-defined disposition codes configured with Max Number of Retries from the drop-down list.

Including UTF-8 characters in exported data

About this task

If you want to export outbound campaign data or campaign summary information that contains UTF-8 characters such as Chinese or Japanese characters, you must perform the following steps to include the characters from the Chinese or Japanese operating systems to successfully display the characters in the exported data.

Procedure

1. On the Contact Center server, locate the **OCMTappsetting.xml** file.

2. Add the following line to the text file within `<appsetting>` and `</appsetting>`:

   `<EnableFileEncodingConfig>true</EnableFileEncodingConfig>`

Exporting manually entered call data

Before you begin

- Log on to Contact Center Manager Administration.
- Open the Outbound component.

- If you work on a Chinese or Japanese operating system, include the UTF-8 characters in the configuration file. See Including UTF-8 characters in exported data on page 323.

About this task

If you enter data manually, you can export it to an external file to re-import to future campaigns, create databases, or share the Call Data table entries with a different department or application.

Procedure

1. On the Outbound Campaign Management Tool, click **Create & Append**.

2. Click the **Campaign Settings** tab.

3. Click **Append Calls to Existing Campaign** or **Start Configuring New Campaign**.

4. Verify or enter the campaign settings.

5. Click **Call Settings**.

6. Manually enter additional call data in the **Call Data Table** rows.

7. Select the rows of the Call Data Table that you want to export. To select all the data, click **Check All**.

8. Click **Export Checked Calls**.

9. On the **Call Details** dialog box, in the **Call Details Fields** box, click the check box beside each field of data you want to export.

   If you are selecting many fields, click **Check All** to check each box, then click to clear the boxes for fields you do not want to export.

10. Click **Uncheck All** to clear all check boxes.

11. To change the order of fields, click the field name to highlight the row, and then click the up or down arrow.

12. To select how the fields are separated in the exported file, click **Tab**, **Space**, or **Character**. The default character is a comma. To change this character, type the desired character in the text box.

13. If you want the first row of the exported file to include the column headers, click the **First row shall contain column headers** check box.

14. Click **Next**.

15. In the **Preview** window, click **Next**.

16. In the **Select File** window, click **Browse** to navigate to directory where you want to save the exported data.

17. Type the name for your exported data file, and then click **Save**.

18. In the Export Wizard, click **Finish**.

Exporting campaign summary data

Before you begin

- Log on to Contact Center Manager Administration.

- Open the Outbound component.

- If you work on a Chinese or Japanese operating system, include the UTF-8 characters in the configuration file. See Including UTF-8 characters in exported data on page 323.

About this task

Export campaign summary data such as all calls, a specific call range, or all calls in a campaign with a certain disposition code, so that you can use the information in another outbound campaign.

Procedure

1. On the Outbound Campaign Management Tool, select **Progress & Results**.

2. In the **Select Campaign** box, select the campaign to export.

3. Click **Export Call Data**.

4. In the Outbound Campaign Management Tool Export Wizard, select **Campaign Summary**.

5. Click **Next**.

6. In the Select Campaign Summary Data window, in the **Campaign Summary Data** box, select the check box for each field of data to export.

   To select multiple fields, click **Check All**, and then click to clear the boxes of fields you do not want to export.

7. To clear all boxes, click **Uncheck All**.

8. To change the order of fields click on the field name to highlight the row, and then click the up or down arrow.

9. Click **Next**.

10. In the Preview Data window, click **Next**.

11. In the Select File window, click **Browse** to navigate to directory where you want to save the exported data.

12. Type the name for your exported data file, and then click **Save**.

13. In the Export Wizard, click **Finish**.

Exporting campaign call data

Before you begin

- Log on to Contact Center Manager Administration.

- Open the Outbound component.
- If you work on a Chinese or Japanese operating system, include the UTF-8 characters in the configuration file. See Including UTF-8 characters in exported data on page 323.

About this task

You can export either the campaign summary or all the call data, including the call status, to an external file.

Procedure

1. On the Outbound Campaign Management Tool, select **Progress & Results**.

2. In the **Campaign List** box, select the campaign to export.

3. Click **Export Call Data**.

4. In the Outbound Campaign Management Tool Export Wizard, select the **Campaign Call Data** option.

5. Click **Next**.

6. In the Select Calls to Export window, to export all calls in a campaign, select the **All Calls** option (This is the default option).

7. To select a specific call range, select the **Select Call Range** option, and then enter the start and end call records into the boxes provided.

8. To filter all calls in a campaign by disposition code, select the **Filter Calls by Disposition Code** option, and then click the check boxes beside the desired disposition codes.

   Only the calls that match the selected disposition codes are selected.

9. Click **Next**.

10. In the Select Call Details window, in the C**all Details Fields** box, select the check box for each field of data to export.

11. To select multiple fields, click **Check All**, and then click to clear the boxes for fields you do not want to export.

12. To clear all check boxes, click **Uncheck All**.

13. To change the order of fields, click on the field name to highlight the row, and then click the up or down arrow.

14. To select how the fields are separated in the exported file, click **Tab**, **Space**, or **Character**.

   The default character is a comma. To change this character, type the desired character in the text box.

15. If you want the first row of the exported file to include the column headers, click the check box.

16. Click **Next**.

17. In the Preview Data window, click **Next**.

18. In the Select File window, click **Browse** to navigate to directory where you want to save the exported data.

19. Type the name for your exported data file, and then click **Save**.

20. In the Export Wizard, click **Finish**.

Viewing log files

Before you begin

- Log on to Contact Center Manager Administration.
- Open the Outbound component.

About this task

You can open the OCMT log file to view action, warning and error log messages.

You can view the location of the current log file in the **Log file name** field. You cannot select the location of the log files in the **Log file name** field. You can select the location of the log files in the Contact Center Trace Control application. You can also view the logging level of the log files in the **Maximum log file size** field, the maximum log file size of the log files in the **Maximum log file size** field, and the number of backup log files that the system must create in the **Number of backup log files** field.

> 😊 **Note:**
>
> The **Log file name**, **Maximum log file size**, **Maximum log file size** and **Number of backup log files** fields are read-only.

Procedure

1. On the OCMT toolbar, click **General Settings**.

2. Click the **OCMT Client Logging** tab.

3. Click **View**.

   The system opens the OCMT log file, and you can view the log messages.

Part 7: Communication Control Toolkit

Chapter 45: Communication Control Toolkit resource fundamentals

Communication Control Toolkit resources are used to map the voice and multimedia contacts to terminals and to route them to agents in the Contact Center.

Use the CCT Web Administration client tree view to add, edit, delete, and assign the CCT resources. You can assign these resources to other resources, thereby granting them access or permission to use the other resources. You assign resources to ensure that the contacts are sent to the correct communications endpoint so that a user on a particular workstation can handle the contact.

The core CCT communication resources are Terminal, Address and Network IVR. These communication resources are supplied by a provider.

The core CCT user resources are User and Workstation. You can use the CCT Web Administration client to assign Terminals and Addresses to CCT Users, this gives the User control of those communications resources. The User can then handle customer contacts.

You can also use the CCT Web Administration client to assign Contact Center agents to CCT Users. Contact Center agents are added and configured in Contact Center Manager Administration. Contact Center agents are automatically assigned to CCT users if the Create CCT Agent check box is selected in CCMA. Further additions and updates to agent mappings can be made using CCT Web Administration. A Contact Center agent represents an agent, agent supervisor, or a supervisor.

Terminals and Addresses are maintained only in AML-based Contact Centers.

Resource assignments

Assignments use the following principles:

- When a terminal is assigned to an agent, CCT automatically assigns the terminal's associated addresses to the respective agent. When the agent logs in CCT checks changes to the agent's configuration. Any new addresses assigned to the terminal are automatically assigned to the agent. Also, any addresses un-assigned, are automatically un-assigned from agents.

- Assignments are distributed using groups. If you assign one resource to a second resource that is a group, and the second resource to a third, then the first resource also assigns to the third. For example, if you assign two users to a user group, and then assign the user group to

an address, the users are considered assigned to the address. Or, if you assign a user to a user group, the user inherits the user group terminals and addresses.

- Only terminals are assigned to workstations.

- When you assign a terminal to a user, you must assign an address.

- You do not assign route point addresses to terminals, route point addresses do not have associated terminals.

- Resource groups are collections of resources. For example, User groups are collections of users.

Table 2: Supported resource-to-resource assignments

Resource	Assignments
User	Terminals, Addresses, Terminal Groups, Address Groups, and Agents can be assigned to a User
Terminal	Addresses and Workstations can be assigned to Terminals
Address	No resources can be assigned to an Address
Workstation	No resources can be assigned to an Workstation

The CCT Web Administration supports the following resource assignments;

- [Assigning a user to a user group](#) on page 335

- [Assigning a terminal to a user or user group](#) on page 338

- [Assigning a terminal to a terminal group](#) on page 339

- [Assigning a terminal group to a user or user group](#) on page 340

- [Assigning an address to an address group](#) on page 343

- [Assigning an address to a terminal](#) on page 344

- [Assigning an address to a user or user group](#) on page 344

- [Assigning a workstation to a terminal](#) on page 347

- [Configuring hot desking](#) on page 353

Chapter 46: Communication Control Toolkit resource configuration

Use Communication Control Toolkit Web Administration to manage CCT resources. Use the CCT resources to map the voice and multimedia contacts to terminals and to route them to agents in the Contact Center.

It is possible to assign some of these resources to other resources, thereby granting them access or permission to use the other resources. Assign resources to ensure that the contacts are sent to the correct communications endpoint so that a user on a particular workstation can handle the contact.

Prerequisites to resource management

Understand the licensed features for your contact center.

Logging on to the Communication Control Toolkit Web Administration using CCMA

Before you begin

- Add the Communication Control Toolkit server to Contact Center Manager Administration and associate it with a Contact Center Manager Server.

About this task

Log on to the Communication Control Toolkit Web Administration to manage CCT resources.

In a Contact Center environment with Contact Center Manager Administration (CCMA) installed, you access the CCT Web Administration using the CCMA launchpad.

Procedure

1. Log on to Contact Center Manager Administration.

   If configured in the security settings, CCMA displays the date and time of your last login and the number of failed login attempts since your last successful login.

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

3. In the left pane, expand the Communication Control Toolkit server for which you want to access the management console.

   The server expands to show the CCT Administration folder.

4. Click **CCT Administration**.

5. In the right pane, click on the correct link open the CCT Web Administration client.

   A new browser window opens with the CCT Web Administration client.

Chapter 47: Communication Control Toolkit users

In a Contact Center environment, a Communication Control Toolkit (CCT) user is a Contact Center agent that is logged on to one or more communication terminals for the purpose of receiving queued contacts. In a Contact Center, use Contact Center Manager Administration (CCMA) to add Contact Center agents, supervisors, and agent supervisors (collectively called agents) to CCT. Then use CCMA to assign these agents to MS Windows users in CCT.

All Communication Control Toolkit users must be configured as Windows users. The user's computer must be in the same domain or a trusted domain with the Communication Control Toolkit server.

Use the Microsoft Security Support Provider Interface (SSPI) to authenticate the user associated with each new connection made to the Communication Control Toolkit server. While this requires that Communication Control Toolkit users also be Windows users, it provides the benefits of centralized user administration and single sign-on (SSO) capability.

A user can belong to a user group. A user group represents a logical group of users such as a sales group or a support group.

Adding a user

Before you begin

- Know the name, properties, and mappings for the user you want to add to the CCT database.

About this task

Add a user to CCT so the user can be assigned resources and can then log on and handle customer contacts.

> **Note:**
>
> To avoid errors, use the CCT Console to import users.

Procedure

1. Expand CCT Web Administration client.

2. In the tree-view pane, right-click **Users**.

3. Click **Add new User**.

4. Click the **User Details** tab.

5. In the **Login User Name** box, type the user name in the format domain\username.

6. In the **First Name** box, type the user's first name.

7. In the **Last Name** box, type the user's last name.

8. Click **Save**.

Deleting a user

Before you begin

• Ensure the user you are deleting is logged out.

About this task

Delete a CCT user so that user can no longer log on.

Procedure

1. Expand CCT Web Administration client.

2. Click **Users**.

3. In the details pane, locate and select the user to delete, and click **Delete**.

4. In the Confirm Deletion dialog box, click **Yes**.

Adding a user group

About this task

Add a user group so you can manage a logical group of users.

Procedure

1. Expand CCT Web Administration client.

2. In the tree-view pane, under **Groups**, right-click **User Groups**.

3. Click **Add new User Group**.

4. In the **Name** box, type the user group name.

5. Click **Save**.

Deleting a user group

About this task

Delete a CCT user group when you no longer need that logical group.

Procedure

1. Expand CCT Web Administration client.

2. Click **Users**.

3. In the details pane, locate and select the user group to delete, and click **Delete**.

4. On the Confirm Deletion dialog box, click **Yes**.

Assigning a user to a user group

About this task

Assign a user to a user group so the user becomes a member of that logical group.

Procedure

1. Expand CCT Web Administration client.

2. In the tree-view pane, select **Groups** > **User Groups**.

3. In the details pane, locate the user group and click on it.

4. Expand the **User assignments** section.

5. Select the users to assign to this user group.

6. Click the right-arrow button to move **Available Users** to **Assigned Users**.

7. Click **Save**.

Chapter 48: Communication Control Toolkit terminals

A Communication Control Toolkit terminal represents a physical communications endpoint (including software applications) such as a SIP soft-phone, an email client, or an IVR line.

Communication Control Toolkit provides an agent terminal type. An agent terminal can log on to a queue and, if scripted, can answer contacts routed to that queue. An agent terminal can also make contacts.

Communication Control Toolkit also defines a terminal by the CCT provider. For more information about providers, see . The Communication Control Toolkit terminal group represents a logical group of terminals such as a local office, a support office, or a sales office.

An agent is mapped to one or more terminals. In a SIP environment, a voice terminal is permanently associated with the agent and is automatically mapped. In CCT Web Administration, no manual mapping of SIP voice terminals is required. In other environments such as Avaya Communication Server 1000, one or more terminals are associated to agents. If an Administrator unmaps a terminal that is currently in use by an agent, the terminal is associated with the agent until the agent logs out of the Communication Control Toolkit terminal. Since the system must wait until the agent logs off the Contact Center, there can be a delay before the terminal is released.

Adding a terminal

Before you begin

- Know the name, properties, and mappings for the resource you are about to add to the CCT database.

About this task

Add a terminal so a CCT user can use it to handle customer contacts.

Procedure

1. Expand CCT Web Administration client.

2. In the tree-view pane, under **Providers** > **Passive**, right-click **Terminals**.

3. Click **Add new Terminal**.

The Terminal details appear in the details pane.

4. In the **Name** box, type a name for the terminal. The format for the terminal name is "Line <loop>.<Shelf>.<card>.<unit>".

5. From the **Terminal Type** list, select **Agent**.

6. Select the **Enabled** check box to enable this terminal.

7. In the **Provider-Specific Properties** section, select one or more line features, select the check box for each of the following:

   3-party conference (A03)

   6-party conference (A06)

   Call Transfer (TRN)

   Call Forward (CFW)

   Analog set

8. Click **Save**.

Deleting a terminal

Before you begin

- Ensure the terminal you are deleting is not in use. Note that when you delete a terminal any addresses mapped to that terminal are not deleted. Addresses must be manually deleted using the CCT Web Administration client.

About this task

Delete a CCT terminal when it is no longer required.

Procedure

1. Expand CCT Web Administration client.

2. In the tree-view pane, under **Providers** > **Passive**, click **Terminals**.

3. In the details pane, locate and select the terminal to delete, and click **Delete**.

4. In the Confirm Deletion dialog box, click **Yes**.

Updating a terminal

About this task

Update a CCT terminal. You must disable a CCT terminal before you can edit terminal details.

Procedure

1. Expand CCT Web Administration client.

2. In the tree-view pane, under **Providers** > **Passive**, click **Terminals**.

3. In the details pane, click on the terminal to update.

4. Clear the **Enabled** check box.

5. Click **Save**.

6. In the tree-view pane, under **Providers** > **Passive**, click **Terminals**.

7. In the details pane, click on the terminal to update.

8. On the **Update Terminal** page, update the terminal details.

9. Select the **Enabled** check box to enable the terminal.

10. In the **Provider-Specific Properties** section, select one or more line features as required.

11. Click **Save**.

Assigning a terminal to a user or user group

About this task

Assign a terminal to a user or user group, so those users can use the terminal.

Procedure

1. Expand CCT Web Administration client.

2. In the tree-view pane, click **Users**.

3. In the details pane, locate the user, and click it.

4. Expand the **Terminal Assignments** section.

5. Select the terminal to assign to this user.

6. Click the right-arrow button to move **Available Resources** to **Assigned Resources**.

7. Click **Save**.

Adding a terminal group

About this task

Add a terminal group so you can manage logical groups of terminals.

Procedure

1. Expand CCT Web Administration client.

2. In the details pane, under **Groups**, right-click **Terminal Groups**.

3. Click **Add new Terminal Group**.

4. In the **Terminal Group Name** box, type a name for the terminal group.

5. Click **Save**.

Deleting a terminal group

About this task

Delete a CCT terminal group when it is no longer required.

Procedure

1. Expand CCT Web Administration client.

2. In the details pane, locate the terminal group to delete, and click **Delete**.

3. In the Confirm Deletion dialog box, click **Yes**.

Assigning a terminal to a terminal group

About this task

Assign a terminal to a terminal group so the terminal becomes a member of that logical group.

Procedure

1. Expand CCT Web Administration client.

2. In the tree-view pane, click **Groups** > **Terminal Groups**.

3. In the details pane, locate the terminal group, and click it.

4. Expand the **Terminal assignments** section.

5. Select the terminal to assign to this terminal group.

6. Click the right-arrow button to move **Available Resources** to **Assigned Resources**.

7. Click **Save**.

Assigning a terminal group to a user or user group

About this task

Assign a terminal group to a user or user group, so the users can use the terminals in the terminal group.

Procedure

1. Expand CCT Web Administration client.

2. In the tree-view pane, click **Users**.

3. In the details pane, locate the user, and click it.

4. Expand the **Terminal Group assignments** section.

5. Select the terminal groups to assign to this user.

6. Click the right-arrow button to move **Available Group** to **Assigned Group**.

7. Click **Save**.

Chapter 49: Communication Control Toolkit addresses

A Communication Control Toolkit address represents a logical communications endpoint such as a telephone number, an email address, or a SIP Uniform Resource Identifier (URI).

Communication Control Toolkit defines the following three base types of addresses:

- Agent—An agent address represents a position ID (ACD key) for the Avaya Communication Server 1000 switch.

- Basic—A basic address is an address, which has an associated terminal (physical endpoint). Communication Control Toolkit users use the basic address to answer calls and to makes calls.

- Route Point—A route point address (or CDN) is a virtual address that can receive multiple, simultaneous calls for application-controlled redirection. A Telephony Service Provider uses the route point address to accept incoming calls, or as a point to which calls are routed.

The Communication Control Toolkit address group represents logical groups of addresses such as a sales group, a support group, or a group of route point (or CDN) addresses.

> **✱ Note:**
>
> You can update addresses of type Route Point only. If you want to update addresses of type Agent or Basic, you must delete the address and add the address again with the required updates.

Adding an address

Before you begin

- Know the name, properties, and mappings for the resource you are about to add to the CCT database.

About this task

Add an address so a CCT user can use it to handle customer contacts.

Procedure

1. Expand CCT Web Administration client.

2. In the tree-view pane, under **Providers** > **Passive**, right-click **Addresses**.

3. Click **Add new Address**.

   The Address details appear in the details pane.

4. In the **Name** box, type a name for the address.

5. In the **URI** box, type a URI for the address.

6. Select the **Enabled** check box to enable this address

7. From the **Type** list, select one of the following: **Basic**, **Agent**, or **Route Point**.

8. Click **Save**.

Deleting an address

About this task

Delete a CCT address when it is no longer required.

Procedure

1. Expand CCT Web Administration client.

2. In the tree-view pane, under **Providers** > **Passive**, click **Addresses**.

3. In the details pane, locate and select the address to delete, and click **Delete**.

4. On the Confirm Deletion dialog box, click **Yes**.

Updating a Route Point address

About this task

Update a CCT address. You must disable a CCT address before you can edit address details. You can update CCT addresses of type Route Point only.

Procedure

1. Expand CCT Web Administration client.

2. In the tree-view pane, under **Providers** > **Passive**, click **Addresses**.

3. In the details pane, click on the Route Point address to update.

4. Clear the **Enabled** check box.

5. Click **Save**.

6. In the tree-view pane, under **Providers** > **Passive**, click **Addresses**.

7. In the details pane, click on the address to update.

8. On the **Update Address** page, update the address details.

9. Select the **Enabled** check box to enable the address.

10. Click **Save**.

Adding an address group

About this task

Add an address group so you can manage logical groups of addresses.

Procedure

1. Expand CCT Web Administration client.

2. In the tree-view pane, under **Groups**, right-click **Address Groups**.

3. Click **Add new Address Group**.

4. In the **Address Group Name** box, type a name for the address group.

5. Click **Save**.

Deleting an address group

About this task

Delete a CCT address group when it is no longer required.

Procedure

1. Expand CCT Web Administration client.

2. In the tree-view, click **Groups** > **Address Groups**.

3. In the details pane, locate and select the address group to delete, and click **Delete**.

4. In the Confirm Deletion dialog box, click **Yes**.

Assigning an address to an address group

About this task

Assign an address to an address group so the address becomes a member of that logical group.

⊛ **Note:**

Communication Control Toolkit supports only adding route point addresses to an address group. Adding addresses of other types is not supported.

Procedure

1. Expand CCT Web Administration client.

2. In the tree-view pane, click **Groups** > **Address Groups**.

3. In the details pane, locate the address group, and click it.

4. Expand the **Address assignments** section.

5. Select the addresses to assign to this address group.

6. Click the right-arrow button to move **Available Resources** to **Assigned Resources**.

7. Click **Save**.

Assigning an address to a terminal

About this task

Assign an address to a terminal so the logical address is associated with a physical terminal or endpoint.

Procedure

1. Expand CCT Web Administration client.

2. In the tree-view pane, click **Providers** > **Passive** > **Terminals**.

3. In the details pane, locate the terminal, and click it.

4. Expand the **Address assignments** section.

5. Select the addresses to assign to this terminal.

6. Click the right-arrow button to move **Available Resources** to **Assigned Resources**.

7. Click **Save**.

Assigning an address to a user or user group

About this task

Assign an address to a user or user group, so those users can use the addresses.

Procedure

1. Expand CCT Web Administration client.

2. In the tree-view pane select **Users**.

3. In the details pane, locate the user and click it.

4. Expand the **Address assignments** section.

5. Select the addresses to assign to this user.

6. Click the right-arrow button to move **Available Resources** to **Assigned Resources**.

7. Click **Save**.

Chapter 50: Communication Control Toolkit workstations

A Communication Control Toolkit workstation represents a computer used by Communication Control Toolkit client applications. A Communication Control Toolkit workstation must share a domain security context with the Communication Control Toolkit server. The workstation must be in the same domain or a trusted domain with the server.

You can assign a workstation to a terminal to enable hot desking.

Adding a workstation

About this task

Add a workstation so a CCT user can use it to handle customer contacts at that location.

Procedure

1. Expand CCT Web Administration client.

2. In the tree-view pane, right-click **Workstations**.

3. Click **Add new Workstation**.

   The workstation details appear in the details pane.

4. In the **Workstation Name** box, type a name for the workstation.

5. Click **Save**.

Deleting a workstation

Before you begin

• Ensure the workstation you are deleting is not in use.

About this task

Delete a CCT workstation when it is no longer required.

Procedure

1. Expand CCT Web Administration client.

2. In the tree-view pane, click **Workstations**.

3. In the details pane, locate and select the workstation to delete, and click **Delete**.

4. On the Confirm Deletion dialog box, click **Yes**.

Assigning a workstation to a terminal

About this task

Assign a CCT workstation to a terminal to support hot desking (agent roaming).

CCT supports user hot desking (agent roaming). Hot desking enables CCT users to log on to CCT at any configured workstation and have access to the terminal associated with that workstation. For example, if the user logs on to a computer, agent roaming ensures that their calls are presented to the phone on the desk beside that computer.

To use hot desking, assign every terminal where they are permitted to sit to the users. You must then assign each workstation to the terminal on the desk beside it. This enables a user to sit at any permitted desk and have rights to use the terminal and the workstation on that desk.

Procedure

1. Expand CCT Web Administration client.

2. In the tree-view pane, select **Provider** > **Passive** > **Terminals**.

3. In the details pane, locate the terminal, and click it.

4. Expand the **Workstation assignment** section.

5. From the **Workstation** list, select the workstation.

6. Click the right-arrow button to move the **Available** workstation to an **Assigned** workstation.

7. Click **Save**.

Chapter 51: Communication Control Toolkit network IVR

The Network Interactive Voice Response (IVR) interface is used by CCT to transfer and collect IVR Call Attached Data (CAD). CCT Network IVR is used to configure the IVR Call Attached Data (CAD) interface and the CCT nodes for networked CAD.

The CCT Service Communication Control Toolkit provider for Avaya Communication Server 1000 provides this Network IVR interface.

The CCT Network IVR:

- Opens an IVR listening port so that IVR applications can register with CCT.
- Keeps this link open between CCT (CS 1000 Service Provider) and the IVR applications, so that the IVR applications can send call attached data to CCT.

※ Note:

When using Network Call Attached Data, CCT uses the Home Location Code (HLOC) of the originating node where the CAD was originally attached as a reference in conjunction with the original call ID. CCT does not reference any subsequent CAD attached at the local node for the remainder of the network call.

Adding a network IVR

Before you begin

- Know the name, properties, and mappings for the resource you are about to add to the database.

Procedure

1. Expand CCT Web Administration client.

2. In the tree-view pane, under **Providers**, right-click **IVRs**.

3. Click **Add new IVR**.

4. In the **IP Address** box, type the IP address of the server you are currently using.

5. In the **HLOC** box, type the home location code of the CS 1000 switch for the IVR system. This HLOC code is the same as the HLOC printed on the switch in overlay 21.

6. In the **TCP Port** box, type the TCP IP port to which other nodes connect. Avaya recommends that you use port 2000.

7. In the **Description** box, type a description.

8. Click **Save**.

Variable definitions

Name	Description
IP Address	The IP address of the server you are currently using.
HLOC	The home location code of the Avaya Communication Server 1000 for the IVR system. This HLOC code is the same as the HLOC printed on the switch in overlay 21.
Port Address	The TCP IP port to which other nodes connect. Avaya recommends that you use port 2000.
Network IVR Description	A description of the Network IVR.

Deleting a network IVR

About this task

Delete a network IVR when it is no longer required.

Procedure

1. Expand CCT Web Administration client.

2. In the details pane, locate the Network IVR to delete, and click **Delete**.

3. On the Confirm Deletion dialog box, click **Yes**.

Chapter 52: Communication Control Toolkit provider

Communication Control Toolkit (CCT) is a media-independent communications middle-ware toolkit. The CCT Software Development Kits (SDK) provide multiple levels of abstraction from the underlying telecommunications infrastructure. The media agnostic CCT SDK supports voice and multimedia contacts. CCT providers are the service providers used to connect to the underlying telecommunications or switching infrastructure.

CCT supports the following providers:

- MLS —MLS connectivity to the Contact Center Manager Server (CCMS). This Contact Center service provider provides the following communication resources:

  - [Communication Control Toolkit terminals](#) on page 336
  - [Communication Control Toolkit addresses](#) on page 341
  - [Communication Control Toolkit network IVR](#) on page 348

- SIP —Session Initiation Protocol (SIP). For TR87 voice call control in a SIP-enabled Contact Center.

Only one provider is supported per installation.

Configuring the Avaya Communication Server 1000 service provider

Before you begin

- Understand the server provider details for the switch.

About this task

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

Procedure

1. Log on to Contact Center Manager Administration server.

2. Start Communication Control Toolkit Web Administration client.

3. In the resource menu, select **Providers**.

   The details of the providers appear.

4. From the list of providers, select **Passive**.

5. In the **Basic Provider Information** section, in the **Passive Name** box, type the Provider name.

   > ❗ **Important:**
   >
   > The provider name must be Passive.

6. In the **IP Address** box, type the IP address of the provider.

7. In the **Port** box, type the port number `3000`.

8. In the **Provider Configuration** section, select the **Transport** type, `TCP`.

9. In the **Customer Number,** type the customer number.

10. In the **CS1000 Software Release**, select the correct version.

11. In the **Call Data Life Span (minutes)**, type the required value in minutes.

12. Select or clear the **Disable Copy of Data to Consult Call** check box.

13. In the **CS1000 Home location Code (HLOC)**, type the HLOC value.

14. In the **Network IVR Port**, type the port value.

15. In the **Initialization Timeout (seconds)** box, type the **Initialization timeout** setting in seconds.

16. In the **Command Timeout (seconds)** box, type the **Command** timeout setting in seconds.

17. Select **Save**.

Next steps

You must restart CCT using System Control and Monitor Utility (SCMU) after you change the service provider details. On the CCT tab of SCMU, click **Shut down CCT**. When the CCT services are shut down, click **Start CCT**.

Variable definitions

Name	Description
Provider Name	Name of the provider, Passive.
IP Address	In a Contact Center environment, the IP address of the CCMS.
Port	In a Contact Center AML environment, the default port value is 3000.
Transport	The transport protocol. The default is TCP.

Table continues…

Name	Description
Customer Number	The customer number for the switch. If multiple customers are configured, you must specify a specific one in this box.
CS1000 Software Release	The release number of Avaya Communication Server 1000 software.
Call data	Call data is the information attached to calls routed from the switch. The Life Span default is 10 minutes. This value must be less than the time it takes to recycle the Avaya Communication Server 1000 Call IDs. Use the **Disable copy of call data to consultative call** check box to avoid copying call data during consultative calls. When you select this option, you can copy call data when calls are transferred or conferenced for local transfers and conferences. However, selecting this option does not allow you to copy call data for calls that are transferred or conferenced to an Avaya Aura® Contact Center network node.
CS1000 Home Location Code (HLOC)	Avaya Communication Server 1000 Home Location Code (HLOC) of the switch is the address digits that specify a location node.
Network IVR Port	Port for the CCT network call attached data and for IVR call attached data.
Timeout in Seconds	Initialization—The length of time that the service provider waits to establish communication with the switch before generating an error. The default and minimum value is 32 seconds. If you use a large number of lines, you must increase this value accordingly. Command—The length of time that the service provider waits for a command response before generating an error. The default and minimum value is 10 seconds.

Chapter 53:   Communication Control Toolkit hot desking

Communication Control Toolkit supports user hot desking (agent roaming). Hot desking enables Communication Control Toolkit users to log on to Communication Control Toolkit (CCT) at any configured workstation and have access to the terminal associated with that workstation. For example, if the user logs on to a computer, agent roaming ensures that voice contacts are routed to the phone on the desk beside that computer.

To use hot desking, assign every terminal where they are permitted to sit (and their associated addresses) to the users. You must then assign each workstation to the terminal on the desk beside it. This enables a user to sit at any permitted desk and have rights to use the terminal and the workstation on that desk.

When a terminal is assigned to an agent, CCT automatically assigns the terminal's associated addresses (ACD/Agent and DN/Basic) to that agent. When the agent sits at a workstation configured for agent roaming and logs on to CCT (using Avaya Agent Desktop), the agent is automatically assigned the terminal and addresses (ACD & DN) of the phone on the desk beside the workstation.

> ✳ **Note:**
>
> The terminal number and addresses (ACD and DN number) do not move with the agent, the terminal number and addresses remain associated with the desk phone.

Configuring hot desking

Before you begin

- Create agents in CCMA and associate them with domain users.
- Assign each terminal to a workstation.
- Add terminals to a terminal group.
- Ensure that all terminals have the correct addresses assigned to them.

About this task

In some contact centers agents do not have a fixed desk and phone. An agent can pick a desk that is not being used and log on to the phone and workstation. An agent must be able to log on to any phone and workstation in this environment. This is called hotdesking or agent roaming, where an agent can work at multiple desks.

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

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

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

  For example, assume that User _1 is assigned to Terminal_1 and Terminal_2 and the respective addresses. If User_1 logs on to workstation_2, then the user also logs on to Terminal_2.

Procedure

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

   ❗ Important:

   A terminal can only be assigned to one workstation.

Part 8: Call Recording and Quality Monitoring

Chapter 54: Call Recording and Quality Monitoring

Use the Call Recording and Quality Monitoring Launchpad option to navigate between the Contact Center Manager Administration client application and the Web-based Avaya Experience Platform™ Workforce Engagement management tools for Avaya Contact Recording and Quality Monitoring (CRQM).

Launching the CRQM application

Before you begin

- Log on to Contact Center Manager Administration. Ensure you have sufficient permissions to access the CRQM application.
- Configure the URLs for the CRQM servers. See

About this task

Launch the CRQM application for the server of your choice to open a new browser window where you can access the CRQM management console.

Procedure

1. On the **Launchpad**, click **Call Recording and Quality Monitoring**.

2. In the left pane, click the server for which you want to access CRQM.

   The server expands to reveal nodes that represent the CRQM server types configured for the server.

3. Click the node for which you want to launch the relevant CRQM application.

   The details page for the CRQM application appears.

4. Click **Launch**.

Index

Comments on this document?