Cisco Unified Contact Center Enterprise Features Guide, Release 11.6(1)

First Published: 2017-08-24

Last Modified: 2018-06-29

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

Change History

This table lists changes made to this guide. Most recent changes appear at the top.

Table 1:

Change	See	Date
New chapter has been added	Digital Channels with imiconnect	August, 2021
Clean up of Contact Sharing chapter. Added some clarifying notes to the installation process. Removed use of the Unified CCE Target Instance Replication process.	Contact Sharing chapter	January 29, 2018
Accumulated minor fixes	Context Service chapter	October 10, 2017
Added information about SAML 2.0 support	Single Sign-On chapter	September 29, 2017

Change	See	Date
Initial Release of Document for Release 11.6(1)		August 2017
Added a note in "Deployment Options for Cisco Identity Service"	Single Sign-On chapter	
Added Multi Domain SSO feature		
Support in Single Sign-on for the SAM-Account Name or UPN choice based on User-ID Configuration.		
Restructured and revised the Context Service chapter.	Context Service chapter	
Added the supported Java version information for Context Servce.	Context Service chapter	

About This Guide

This guide explains features you can use in conjunction with Cisco Unified Contact Center Enterprise. For each feature, there is a description, procedures for initial setup, and details on the functionality the feature provides.

Audience

This guide is prepared for Contact Center administrators who configure and run the contact center, manage agents, and address operational issues.

Related Documents

Subject	Link
Design considerations and guidelines for deploying a Unified CCE solution, including its various components and subsystems.	*Solution Design Guide for Cisco Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at https://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

Field Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround, or other user action. For more information, see *Product Field Notice Summary* at https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html.

You can create custom subscriptions for Cisco products, series, or software to receive email alerts or consume RSS feeds when new announcements are released for the following notices:

- Cisco Security Advisories
- Field Notices
- End-of-Sale or Support Announcements
- Software Updates
- Updates to Known Bugs

For more information on creating custom subscriptions, see *My Notifications* at https://cway.cisco.com/mynotifications.

Documentation Feedback

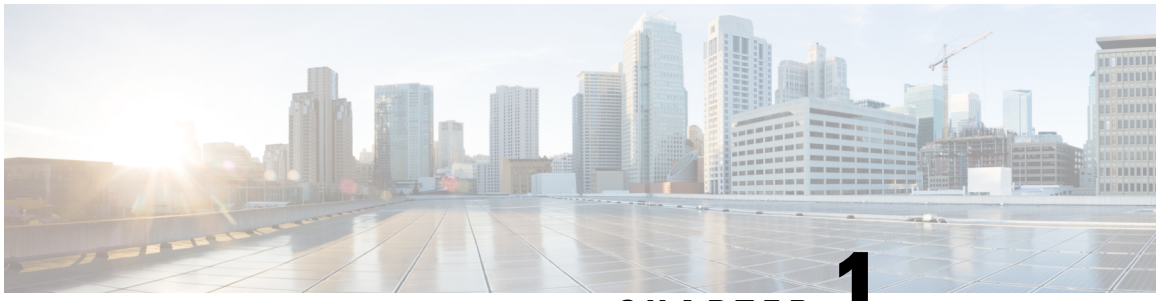
To provide comments about this document, send an email message to the following address: contactcenterproducts_docfeedback@cisco.com

We appreciate your comments.

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, folder names, and submenu names. For example: • Choose **Edit** > **Find**. • Click **Finish**.
italic font	Italic font is used to indicate the following: • To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills. • A syntax value that the user must replace. Example: IF (*condition, true-value, false-value*) • A book title. Example: See the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*.
`window font`	Window font, such as Courier, is used for the following: • Text as it appears in code or that the window displays. Example: `<html><title>Cisco Systems, Inc. </title></html>`
`< >`	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.



CHAPTER 1

Agent Greeting

Capabilities

The Agent Greeting feature lets an agent record a message that plays automatically to callers when they connect to the agent. The greeting message can welcome the caller, identify the agent, and include other useful contextual information. With Agent Greeting, each caller can receive a clear, well-paced, language-appropriate, and enthusiastic introduction. Another benefit is that it saves the agent from having to repeat the same introductory phrase for each call. It also gives the agent a moment to review the desktop software screen popups while the greeting plays.

The process of recording a greeting is much the same as recording a message for voicemail. Depending on how the call center is set up, agents may be able to record different greetings that play for different types of callers. For example, agents can record an English greeting for English speakers or an Italian greeting for Italian speakers.

Agent Greeting Phone Requirements (for Local Agents Only)

Agent Greeting is available to agents and supervisors who use IP Phones with Built-In Bridge (BIB). These agents are typically located within a contact center. Phones used with Agent Greeting must meet these requirements:

- The phones must have the BIB feature.

Note If you disable BIB, the system attempts to use a conference bridge for Agent Greeting call flow and raises a warning event.

- In an IPv6-enabled environment, Agent Greeting may require extra Media Termination Points (MTPs).

See the *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html for the list of supported Cisco Unified Call Center phone models.

Agent Greeting Functional Limitations

Agent Greeting is subject to these limitations.

- Agent Greeting does not support outbound calls made by an agent. The announcement plays for inbound calls only.
- Only one Agent Greeting file plays per call.
- Supervisors cannot listen to agent recorded greetings.
- Agent Greetings do not play when the router selects the agent through a label node.
- Agent Greeting supports Unified CM based Silent Monitoring with this exception: Supervisors cannot hear the greetings themselves. If a supervisor tries to start a silent monitoring session while a greeting is playing, a message displays stating that a greeting is playing and to try again shortly.

Whisper Announcement with Agent Greeting

You can use Agent Greeting with the Whisper Announcement feature. Here are some things to consider when using them together:

- On the call, the Whisper Announcement always plays first.
- To shorten your call-handling time, use shorter Whisper Announcements and Agent Greetings than if you were using either feature by itself. A long Whisper Announcement followed by a long Agent Greeting equals a long wait before an agent actively handles a call.
- If you use a Whisper Announcement, your agents probably handle different types of calls: for example, “English-Gold Member-Activate Card,” “English-Gold Member-Report Lost Card,” “English-Platinum Member-Account Inquiry.” Therefore, you may want to ensure that greetings your agents record are generic enough to cover the range of call types.

For more information about Whisper Announcement, see Whisper Announcement, on page 195

Initial Setup

This section is intended for system administrators responsible for installing and configuring Unified CCE. It describes the one-time tasks required to set up Agent Greeting.

Configuration Requirements

The following configuration components must be in place to deploy Agent Greeting.

Where	What
Unified Communications Manager	For phones that use Agent Greeting, you must set the Built-in-Bridge option to On or Default (if the value of Default is On). To verify, in Unified CM Administration, select **Device** > **Phone** > **Built in Bridge**.
Unified CCE	Agent Greeting is supported with Type 10 Network VRUs only. (Type 10 is required to allow CVP to control the call). If your current Unified CCE deployment is not configured for a Type 10 VRU, you must modify it accordingly. Agent Greeting requires at minimum three expanded call variables. • user.microapp.ToExtVXML: This is used twice in an Agent Greeting record script: the first time is to queue the Unified CVP RecordAgentGreeting application; the second time is to tell the recording application where to save greeting files. Configure it as an array with size 3. Use the Unified CCE Administration tool to ensure this variable includes these settings: Maximum Length - 100 and Enabled. • user.microapp.app_media_lib:This is required in Agent Greeting record and play scripts to specify the dedicated directory on the media server where your greeting audio files are stored. Maximum Length - 100 and Enabled. • user.microapp.input_type: This is required in Agent Greeting record scripts to limit the allowable input type to DTMF. Maximum Length - 100 and Enabled. No other ECC (Expanded Call Variable) are needed if you serve your files from the Unified CVP default media server, and your files are in the media server default locale directory ("<*web_server_root*>\en-us\app"). However, if you store your files in a location other than these defaults, you must use one or more of the ECC in the next row in your scripts.

Where	What
Unified CCE (optional variables, used to override defaults)	To make these variables available to your script authors, confirm that they are defined in the Unified CCE Administration tool. For instructions about defining ECC variables for CVP, see the *Administration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html. • user.microapp.media_server: Use to identify the Unified CVP media server if it is other than the default. • user.microapp.locale: Use to specify the name of the locale directory on the media server if it is other than the default ("en-us"). • user.microapp.UseVXMLParams: Required in your record script if you include the user.microapp.media_server variable. It tells the external VXML recording script to use the name/value pair of the application that you pass in the user.microapp.ToExtVXML variable.
Unified CVP	Unified CVP Server must be installed and configured, as described in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Deploy Agent Greeting

Agent Greeting Deployment Tasks

Procedure

Step 1 Ensure that your system meets the baseline requirements for software, hardware, and configuration described in the System Requirements and Limitations section.

Step 2 Configure one or more servers to act as media servers. Configuration requirements include IIS and FTP.

Step 3 In Unified CVP, add media servers, configure FTP connection information, and deploy the media servers.

Step 4 Configure a Unified CVP media server, if you have not already done so. See Configure Media Server for Agent Greeting, on page 5. .

Step 5 In Unified CVP, republish the VXML Gateway.tcl scripts with updated Agent Greeting support. See Republish the tcl scripts to VXML Gateway, on page 9 for Agent Greeting support.

Step 6 Set the cache size on the VXML Gateway. See Set Cache Size on VXML Gateway, on page 9.

Step 7 Record the voice prompts to play to agents when they record a greeting and to deploy the audio files to your media server. See Create Voice Prompts for Recording Greetings, on page 9.

Step 8 Configure call types to record and play agent greetings. See Configure Call Types, on page 10.

Step 9 Configure dialed numbers to record and play agent greetings. See Configure Dialed Numbers, on page 11.

Step 10 Schedule the Script, on page 11.

Step 11 Define Network VRU Scripts for Agent Greeting, on page 11.

Step 12 In Script Editor:

- To use the installed scripts to record and play agent greetings, see Import Example Agent Greeting Scripts, on page 13.
- To create your own scripts, see Agent Greeting Scripts, on page 17.

Step 13 Modify the Unified CCE call routing scripts to use Play Agent Greeting script, on page 15.

Configure Media Server for Agent Greeting

Agent Greeting uses the Unified CVP media server. If you previously configured and deployed one or more Unified CVP media servers for other features, you do not have to configure any additional servers for Agent Greeting. You can optionally add additional media servers.

Agent Greeting uses the Unified CVP media server to store and serve the following types of files:

- Prompt files, prepared by Administrators. These files supply the prompts that agents hear when they record their greetings. The Administrator must manually add the prompt files to all the media servers that their Agent Greeting scripts will query to retrieve those files.
- Greeting files, recorded by agents. These files are the actual greetings that play to callers. They are recorded by individual agents. The system handles the storage of these files as follows:
  - A greeting file is named using the convention *PersonID_AgentGreetingType*. For more about *AgentGreetingType*, see Specify AgentGreetingType Call Variable, on page 15.
  - When a greeting is first recorded, it is stored temporarily on the Unified CVP Server, where an agent can listen to it before confirming its use.
  - When the agent confirms the greeting, the file is transferred, using FTP, to all media servers that are deployed and are configured with FTP enabled. Make sure that an FTP server is installed and configured for the correct version of IIS on the media server. For instructions, consult your Microsoft documentation (http://microsoft.com).
  - To satisfy a request for the greeting to play to a caller, the greeting file is copied from the media server to the VXML Gateway, where it is cached. The cached copy is used to satisfy subsequent requests for the greeting. Content expires in the cache based on the cache timeout period defined on the media server.

The routing scripts look for the prompt and greeting files either on the configured default Unified CVP media server or on a specific server identified in the script. Some typical scripting scenarios for retrieving files for Agent Greeting include:

- All files are retrieved from the default server.
- All files are retrieved from the default server if available; otherwise, a redundant server is queried.
- For security, the prompt files are retrieved from one server and the greetings files are retrieved from a different server.

- For load balancing, the greetings files are dispersed among several servers and retrieved based on tests in the script.

Media Server Hardware and Network Requirements

Ensure the server is accessible to CVP, Unified CCE, and your agent desktops.

Prepare a Media Server

1. Ensure that IIS is properly configured and running on the server. It must be listening on port 80.
2. Ensure the server is accessible to CVP, Unified CCE, and your agent desktops.
3. Perform the following steps:
   a. On the taskbar, click **Start**, point to **Administrative Tools**, and then click **Server Manager**.
   b. In the **Server Manager** hierarchy pane, expand **Roles**, and then click **Web Server (IIS)**.
   c. In the **Web Server (IIS)** pane, scroll to the **Role Services** section, and then click **Add Role Services**.
   d. On the **Select Role Services** page of the **Add Role Services** wizard, expand **FTP Server**.
   e. Select **FTP Service**.

Note To support ASP.NET membership or IIS Manager authentication for the FTP service, you need to select **FTP Extensibility**.

   f. Click **Next.**
   g. On the **Confirm Installation Selections** page, click **Install.**
   h. On the **Results** page, click **Close.**
   i. In the sites section, click **Add FTP Site**. Provide a site name and path to the same location as the http directory c:\inetpub\wwwroot.
   j. Select your desired binding method, specify to start automatically, select **No SSL** and click **Next.**
   k. On the **Authentication and Authorization** section select the type of authentication required. If using basic, note the name and password of the account.
   l. Select the authorization; for anonymous select **Anonymous users**.
   m. Set the read and write permissions.

Note Make note of your FTP connection information -- connection type, user name, password, and port number.

4. Make sure that the FTP and the IIS share the same root directory, because the recording application writes the file to the media server directory structure, and the greeting playback call uses IIS to fetch the file. The `en-us/app` directory should be under the same root directory for FTP and IIS.

5. Create a dedicated directory on the server to store your greeting files. This lets you specify a lower cache timeout of 5 minutes for your agent greeting files that does not affect other more static files you may be serving from other directories. By default, the Record Greeting application posts the `.wav` file to the `en-us/app` directory under your web/ftp root directory. You may create a dedicated directory such as `ag_gr` under the `en-us/app` directory, and then indicate this in the Unified CCE script that invokes the recording application. Use the array for the ECC variable **call.user.microapp.ToExtVXML** to send the ftpPath parameter to the recording application. Make sure the ECC variable length is long enough, or it may get truncated and fail.
6. In IIS Manager, set the cache expiration for the dedicated directory to a value that allows re-recorded greetings to replace their predecessor in a reasonable amount of time, while minimizing requests for data to the media server from the VXML Gateway. The ideal value varies depending on the number of agents you support and how often they re-record their greetings. Two minutes may be a reasonable starting point.
7. Also find the site you are using, go to the agent greeting folder you created (ag_gr), and then select **HTTP Response Headers**.
8. Select **Add**, then **Set Common Headers**.
9. Select **Expire Web Content** and set your desired value.

Note After specifying the cache timeout, it is a good idea to clear the cache on the VXML Gateway. This ensures the gateway requests the latest files from the media server. You need only clear the gateway cache once. Open a command prompt on the CVP VXML Gateway, log into IOS, and enter the following commands:

```
my_server# conf t
my_server(config)# clear http client cache
my_server(config)# exit
my_server(config)# wr
```

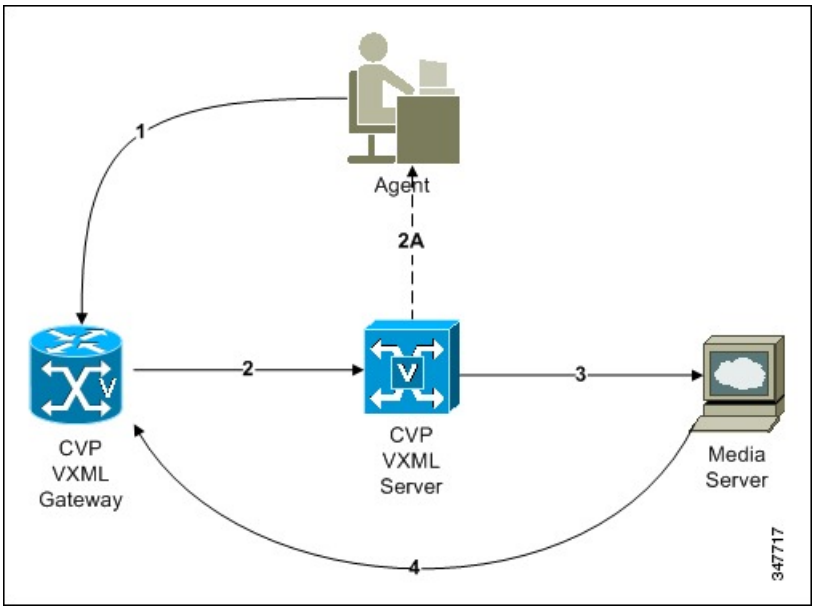
Note The HTTP client response timeout setting on the gateway must be greater than the time it takes to complete the largest anticipated FTP file transfer. If an FTP file transfer takes longer than the configured duration in seconds for HTTP client response timeout, the FTP transfer completes correctly, but the call drops as soon as the configured timeout duration is met. To change the HTTP client response timeout setting, open a command prompt on the CVP VXML Gateway, log into IOS, and enter the following commands:

```
my_server# conf t
my_server(config)# http client response timeout <new value in seconds>
my_server(config)# exit
my_server(config)# wr
```

By default, the HTTP client response timeout value for CVP is 30 seconds.

How Greeting Files Are Recorded and Served

Following is an illustration of how Greeting files are recorded and served, followed by a step by step description.



1. An agent initiates a greeting recording session and records a greeting.
2. The VXML Gateway passes the recorded (but unsaved) greeting file to the VXML Server.
3. The agent asks to listen to the greeting before saving it. The file is played from the VXML Server.
4. The agent saves the greeting. The file is named (based on the Person ID + AgentGreetingType) and stored on the media server.
5. Requests for the greeting file come in through the VXML Gateway. The VXML Gateway examines its web server cache for the file. If the file is present and not expired, the cached version is served. If the file is not present, or if its timestamp exceeds the cache expiration, the file is retrieved from the media server and cached again.

Add and Configure Media Servers in CVP

You can add one or more servers to CVP to act as media servers. If you add multiple media servers, note the following:

- CVP automatically propagates files that are added to one media server out to all media servers in the list that have FTP enabled. To enable FTP on a media server, use the following procedure.
- You can designate one media server as the default. If a default media server is defined, requests for files are automatically sent to that server without your having to specify that server in your routing scripts.

1. Access the CVP Operations Console by typing **https://<OAMP_server_IP>:9443/oamp**.
2. At the CVP Operations Console, select **Device Management** > **Media Server**.
3. Add a server to the list of CVP media servers.
4. Select **FTP Enabled**.
5. Configure the credentials and port settings that will permit CVP to write files to the server using FTP.
6. Optionally, you can designate one of your media servers as the Default Media Server.

7. Click the **Deploy** button to deploy the list of media servers to your CVP Servers.

   Note: If you deploy the list of media servers and then designate a default, you must redeploy the list.

Republish the tcl scripts to VXML Gateway

The .tcl script files that ship with Unified CVP include updates to support Agent Greeting. You must republish these updated files to your VXML Gateway.

Republishing scripts to the VXML Gateways is a standard task in CVP upgrades. You must republish the scripts before you can use Agent Greeting.

Procedure

Step 1 In the Unified CVP Operation Console, select **Bulk Administration** > **File Transfer** > **Scripts and Media**.

Step 2 Set Device to Gateway.

Step 3 Select the gateways you want to update. Typically you would select all of them unless you have a specific reason not to.

Step 4 Select **Default Gateway Files**.

Step 5 Click **Transfer**.

Set Cache Size on VXML Gateway

To ensure adequate performance, set the size of the cache on the VXML Gateway to the maximum allowed. The maximum size is 100 megabytes; the default is 15 kilobytes. Failure to set the VXML Gateway cache to its maximum can result in slowed performance to increased traffic to the media server.

Use the following Cisco IOS commands on the VXML Gateway to reset the cache size:

```
conf t
http client cache memory pool 100000
exit
wr
```

For more information about configuring the cache size, see the *Configuration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html.

Create Voice Prompts for Recording Greetings

You must create audio files for each of the voice prompts that agents hear as they record a greeting. The number of prompts you require can vary, but a typical set can consist of:

- A welcome followed by a prompt to select which greeting to work with (this assumes you support multiple greetings per agent)
- A prompt to select whether they want to hear the current version, record a new one, or return to the main menu
- A prompt to play if a current greeting is not found.

To create voice prompts for recording greetings:

Procedure

Step 1 Create the files using the recording tool of your choice. When you record your files:

- The media files must be in `.wav` format. Your `.wav` files must match Unified CVP encoding and format requirements (G.711, CCITT A-Law 8 kHz, 8 bit, mono).
- Test your audio files. Ensure that they are not clipped and that they are consistent in volume and tone.

Step 2 After recording, deploy the files to your Unified CVP media server. The default deployment location is to the *<web_server_root>*`\en-us\app` directory.

Step 3 Note the names of the files and the location where you deployed them on the media server. Your script authors need this information for the Agent Greeting scripts.

Built-In Recording Prompts

The Unified CVP Get Speech micro-application used to record Agent Greetings includes the following built-in prompts:

- A prompt that agents can use to play back what they recorded
- A prompt to save the greeting, record it again, or return to the main menu
- A prompt that confirms the save, with an option to hang up or return to the main menu

You can replace these `.wav` files with files of your own. For more information, see the Unified Customer Voice Portal Call Studio documentation at https://www.cisco.com/c/en/us/support/unified-communications/unified-call-studio/tsd-products-support-series-home.html.

Example Record Greeting Prompts

Unified CCE includes three example record greeting audio prompts. These are installed on each ICM server at <icm_root>\wav. These example files are referenced in the example recording script that are included with ICM. If you plan to deploy the example script, copy the audio prompts to the <web_server_root>en-us\app directory on your media server.

Configure Call Types

To record and play agent greetings, create the following call types: RecordAgentGreeting and PlayAgentGreeting.

Procedure

Step 1 From the Configuration Manager, select **Tools** > **List Tools**.

Step 2 Select **Call Type List**.

Step 3 Click **Retrieve**.

Step 4 Click **Add**.

Step 5 Create a call type to record agent greetings and use the name RecordAgentGreeting. Then click **Save**.

Step 6 Create a call type to play agent greetings and use the name PlayAgentGreeting. Then click **Save**.

Configure Dialed Numbers

To record and play agent greetings, create the following dialed numbers: RecordAgentGreeting and PlayAgentGreeting.

Procedure

Step 1 From the Configuration Manager, select **Tools** > **List Tools**.

Step 2 Select **Dialed Number/Script Selector List**.

Step 3 Click **Retrieve**.

Step 4 Click **Add**.

Step 5 On the **Attributes** tab, do the following:

a) Create a dialed number to record agent greetings; use the name RecordAgentGreeting. (The name must match exactly and is case-sensitive.) Set the **Media routing domain** to **Cisco_Voice**, and then click **Save**.

b) Create a dialed number to play agent greetings; use the name PlayAgentGreeting. (The name must match exactly and is case-sensitive.) Set the **Media routing domain** to **Cisco_Voice**, and then click **Save**.

Step 6 On the **Dialed Number Mapping** tab, do the following:

a) Click **Add** and map the RecordAgentGreeting dialed number to its call type; click **OK**.

b) Click **Add** and map the PlayAgentGreeting dialed number and its call type; click **OK**.

Schedule the Script

Procedure

Step 1 In the **Script Editor**, select **Script** > **Call Type Manager**.

Step 2 From the Call Type Manager screen, select the **Schedules** tab.

Step 3 From the Call type drop-down list, select the call type to associate with the script; for example, PlayAgentGreeting.

Step 4 Click **Add** and select the script you want from the Scripts box.

Step 5 Click **OK** twice to exit.

Define Network VRU Scripts for Agent Greeting

For Agent Greeting record and play scripts to interact with Unified CVP, Network VRU scripts are required. The number of VRU scripts that you require and how you configure them depends on how you choose to script Agent Greeting.

To create these scripts, use the Network VRU Script List Tool found in Configuration Manager.

The following table lists an example set of Agent Greeting Network VRU scripts based on the example Agent Greeting scripts that are included with the software.

Note If you require the following example VRU scripts, you must manually create them.

- The Network VRU must be a Type10
- The default timeout 180 is acceptable
- Leave Overridable unchecked

Table 3: Agent Greeting Network VRU Scripts

Name / VRU Script Name	Configuration Parameter	Interruptible (Y/N)	What it does
`AgentGreeting` `PM,-a`	null	N	Causes a saved greeting audio file to play. The `-a` parameter automatically generates the file name by concatenating the Person ID with the AgentGreetingType variable value set in your routing scripts that target an agent.
`GreetingMenu_1_to_9` `M,press_1_thru_9_greeting,A`	`1-9`	Y	During a recording session, play an audio file that presents a voice menu prompting the agent to press the number corresponding to the greeting he or she wants to record. The `1-9` configuration parameter defines the range of allowable keys. So this value also determines the number of concurrent greetings agents can have. The `A` parameter specifies that the file is in the (default) Application directory on the Unified CVP Server.
`GreetingSubMenu` `M,press1-press2-press3,A`	`1-3`	Y	During a recording session, play an audio file that prompts the agent to press 1 to listen to a greeting, 2 to record, or 3 to go to the main menu.
`Greeting_Not_Found` `PM,no_greeting_recorded,A`	`Y`	Y	During a recording session, if an agent tries to play back a greeting that does not exist, play the no_greeting_recorded audio file. The `Y` configuration parameter in this instance allows barge-in (digit entry to interrupt media playback).
`T10_GS_AUDIUM` `GS,Server,V, FTP`	`,,,,,,,,,,Y`	Y	This starts the external VXML application that records the greeting. The VRU script name must be specified exactly as shown and is case-sensitive. The `Y` parameter in the eleventh position of the Configuration Parameter is required. It allows the script to pass FTP connection information to the VXML server. The VXML server then uses this information to make an FTP connection to the media server when saving greeting files.

Name / VRU Script Name	Configuration Parameter	Interruptible (Y/N)	What it does
`GreetingReview` `PM,-a,A`	`Y`	Y	This script allows the agent to review the recorded greeting audio file.

Note For descriptions of VRU Script Name parameters and detailed instructions on creating Network VRU scripts for CVP micro-applications, see the Configuration and Administration Guide for Cisco Unified Customer Voice Portal.

Import Example Agent Greeting Scripts

To view or use the example Agent Greeting scripts, you must first import them into Script Editor. To import the scripts:

Procedure

Step 1 Launch Script Editor.

Step 2 Select **File** > **Import Script** and select a script to import.

The scripts are located in the `icm\bin` directory on the data server (DS) node.

Note When you import the example scripts, Script Editor maps objects that are referenced in the scripts. Some of the objects, such as the external Network VRU scripts, skill groups, route to skill group, or precision queue, do not map successfully. You must create these manually or change these references to point to existing scripts, skill groups, and precision queues in your system.

What to do next

In addition to importing the scripts, you may need to modify the following items. For more information, see Agent Greeting Scripts, on page 17.

- If you do not use a default media server, you must modify the media server specification.
- If you do not use the default values for application and locale (`en-us/app`), you must modify the path name of greeting files.
- Using the Unified CCE Administration tool, enable all expanded call variables referenced by the following sample scripts.

Agent Greeting Example Routing Scripts

The example routing script files in the `icm\bin` directory include:

- **AG.ICMS—**This script sets up an Agent Greeting by setting the greeting type to be used on the call and then queueing the call to a skill group or precision queue. Once an agent is selected from the skill group

or precision queue and the call routed to the agent, the PAG.ICMS script is invoked. It requires that you define an AgentGreeting VRU script (described in Define Network VRU Scripts for Agent Greeting, on page 11) and a skill group.

- **PAG.ICMS—**This script causes an Agent Greeting to play. It is invoked by the PlayAgentGreeting dialed number that you configured earlier in the configuration process. This number must be associated with a call type that then executes the script. It requires that you define an AgentGreeting VRU script, described in Define Network VRU Scripts for Agent Greeting, on page 11.
- **RECORD_AG.ICMS—**This script lets agents record a greeting. It is called from the agent desktop when an agent clicks the Record Agent Greeting button. It prompts the agent to select which greeting to play or record. This script is invoked by the RecordAgentGreeting dialed number that you configured earlier in this configuration process. It requires that you define all five VRU scripts described in Define Network VRU Scripts for Agent Greeting, on page 11.
- **WA_AG.ICMS—**This script plays a Whisper Announcement and an Agent Greeting together on the same call flow. It requires that you define an AgentGreeting VRU script (described in Define Network VRU Scripts for Agent Greeting, on page 11) and a skill group.

Note The PAG.ICMS and RECORD_AG.ICMS example scripts assume that a default media server is configured in Unified CVP, and the greeting files are stored in a dedicated directory named ag_gr directory. The WA_AG.ICMS script does not include a dedicated directory.

Note For greeting, the initial script sets up the call between caller and agent, and a different script plays the greeting to the agent after the caller is connected. If the initial Unified CCE script overrides the default media server with a SET node, the call context of expanded call variables is preserved on the greeting playback call as well, and the Default Media Server may be overridden. In this case, modify the greeting playback script to use a SET node with the correct media server.

Test Agent Greeting File Path

When an agent records a greeting, the greeting file is saved with a system-generated name as follows:

- The Person ID number is prepended to the starting string. For example, an agent with a Person ID of 5050 would have greeting files named 5050_1 or 5050_French.
- The filename ends with the value of the Call.AgentGreetingType variable associated with the choice the agent made when recording the greeting. For example, if the agent selected the first option, and the Agent Greeting record script sets the first option to "1," then the greeting filename is appended with _1. As another example, if descriptive strings were implemented, and the first option is associated with the string "French," then the greeting filename is appended with _French.

The greeting file is saved in a directory whose path is determined by the following variables in the Agent Greeting record script:

- A specific media server, or the default media server. (The file is later pushed to all FTP-enabled media servers.)
- A specific application directory, or the default application directory.

- A specific locale directory, or the default locale directory.

To test the path you defined to the greeting file in your script variables, plug the complete URL into a browser. The `.wav` file should play. For example:

- If your script uses a default media server whose IP is *192.1.1.28 + the default locale + an application directory named greet + 5050_im1.wav*, then the generated URL should be `http://192.1.1.28/en-us/app/greet/5050_1.wav`. Entering this URL into a browser should cause this agent's greeting to play.
- If your script includes: *http://my_server.my_domain.com + the default locale + an application directory app/greet + 5050_1.wav*, then the path should be `http://my_server.my_domain.com/en-us/app/greet/5050_1.wav`.

Modify the Unified CCE call routing scripts to use Play Agent Greeting script

For an Agent Greeting play script to run, you must add an AgentGreetingType Set Variable node to your existing Unified CCE call routing scripts: This variable's value is used to select the audio file to play for the greeting. Set the variable before the script node that queues the call to an agent (that is, the Queue [to Skill Group or Precision Queue], Queue Agent, Route Select, or Select node).

Specify AgentGreetingType Call Variable

To include Agent Greeting in a script, insert a Set Variable node that references the AgentGreetingType call variable. The AgentGreetingType variable causes a greeting to play and specifies the audio file it should use. The variable value corresponds to the name of the greeting type for the skill group or Precision Queue. For example, if there is a skill group or Precision Queue for Sales agents and if the greeting type for Sales is '5', then the variable value should be 5.

You can use a single greeting prompt throughout a single call type. As a result, use one AgentGreetingType set node per script. However, as needed, you can set the variable at multiple places in your scripts to allow different greetings to play for different endpoints. For example, if you do skills-based routing, you can specify the variable at each decision point used to select a particular skill group or Precision Queue.

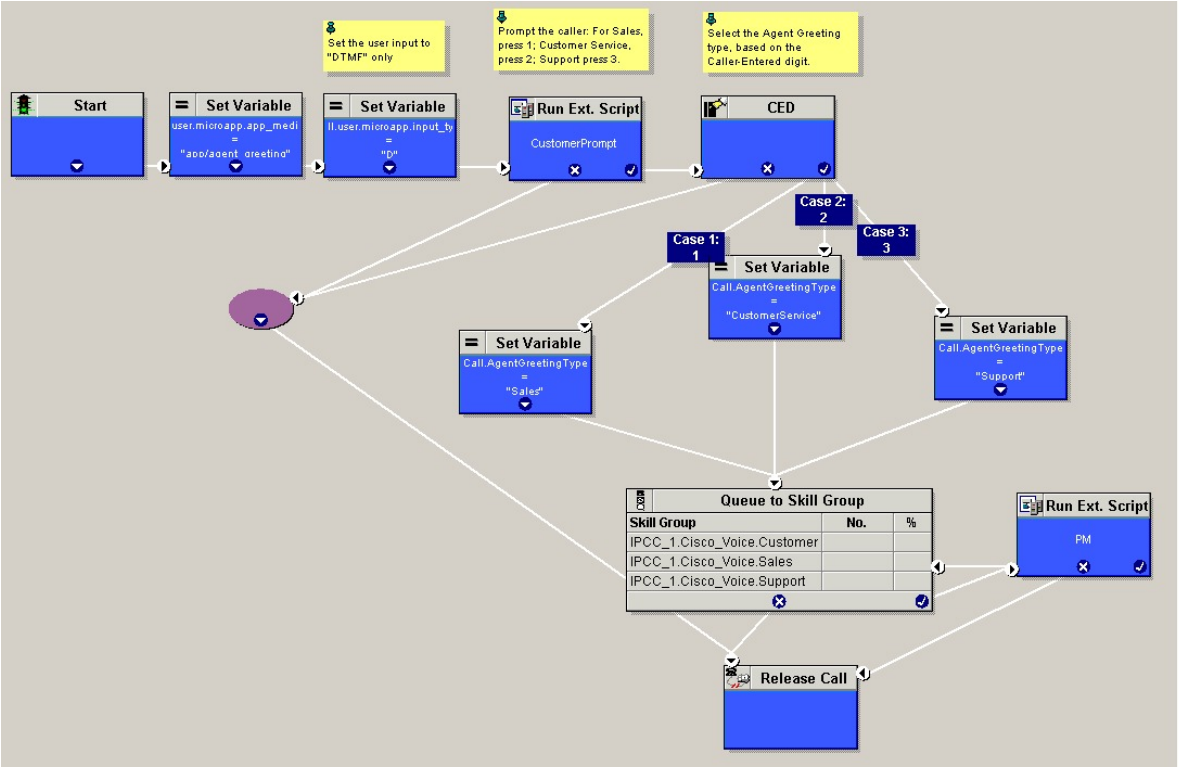
Note Only one greeting can play per call. If a script references and sets the AgentGreetingType variable more than once in any single path through a script, the last value to be set is the one that plays.

Use these settings in the Set Variable node for Agent Greeting:

- Object Type: Call.
- Variable: Must use the AgentGreetingType variable.
- Type: Must use the PersonID_AgentGreetingType type.
- Value: Specify the value that corresponds to the greeting type you want to play. For example: “2” or “French”
  - You must enclose the value in quotes.
  - The value is not case-sensitive.
  - The value cannot include spaces or characters that require URL encoding.

The following script example illustrates how to include Agent Greeting in a script using the Set Variable node:

Figure 1: Modified Call Routing Script to Enable Greeting Play



Scripting Agent Greeting for Multiple Customers

In the out-of-box method for deploying Agent Greeting, Unified CCE uses the customer information from the built-in “PlayAgentGreeting” dialed number to choose the correct network VRU to play the greeting. If your deployment has multiple customers configured within your Unified CCE instance and you want to use Agent Greeting with all of them, you must configure things differently to work around customer associations.

Configure Custom Dialed Number for Agent Greeting Play

To play Agent Greetings for multiple customer instances, configure the built-in PlayAgentGreeting dialed number for each Unified CM routing client, but do not associate it with a specific customer. The Unified CM peripheral uses this number to initiate Agent Greeting play. If you want your greetings to be played from a different network VRU, use the TranslationRouteToVRU node in your routing scripts to explicitly choose the network VRU.

Configure Custom Dialed Number for Agent Greeting Record

To record Agent Greetings when you have multiple customers, you must create your own custom dialed number for recording. You may want to create different dialed numbers for different customers. As with Agent Greeting play, if you want to use different network VRUs to record Agent Greetings for different customers, use the TranslationRouteToVRU node in your routing script to explicitly select the network VRU.

Create your own custom button or have your agents enter the record dialed number using the dial pad on their desktops.

Agent Greeting Scripts

Agent Greeting requires two call routing scripts: one that agents can use to record greetings and one to play a greeting to callers. Examples of these scripts are included in your installation. This section describes the elements in the installed example scripts, including optional features and other modifications that you can make. To create scripts from scratch, use this section to understand the required elements in Agent Greeting scripts.

Note If you plan to use the installed example scripts out of the box, you can ignore this section.

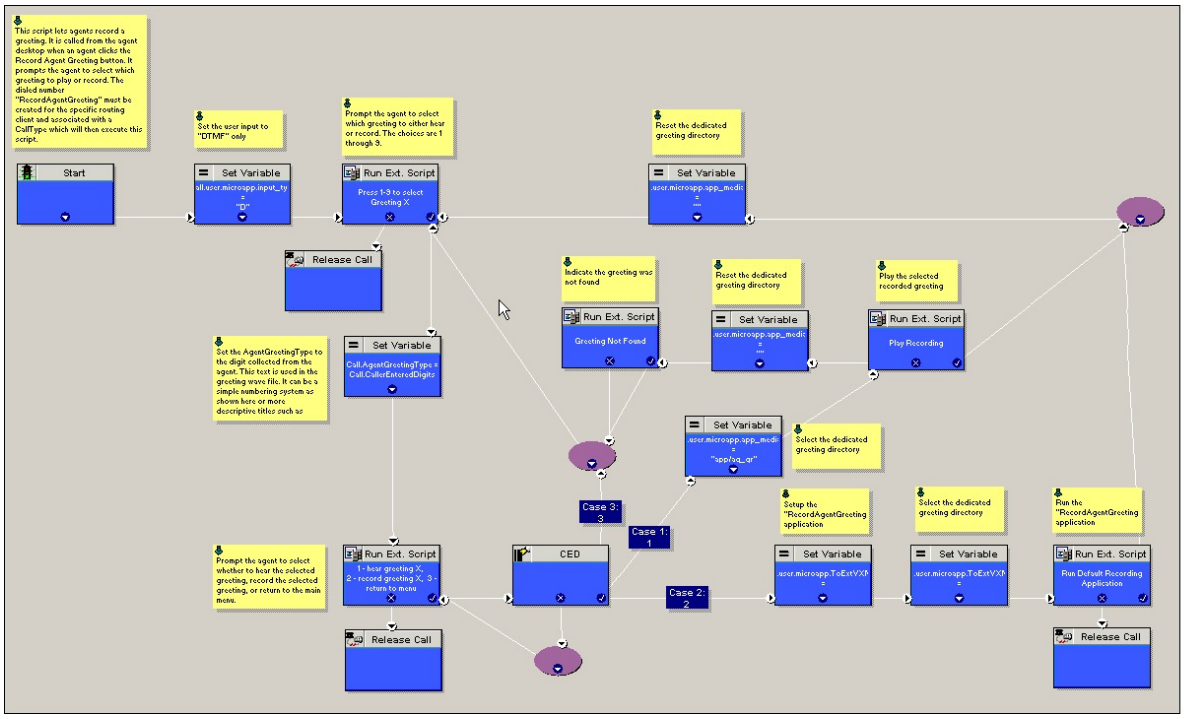
Agent Greeting Recording Script

The Agent Greeting recording script is a dedicated routing script that allows agents to record greetings. You can use the installed example scripts or create your own.

In the example script shown here, the agent is first prompted to select one of nine possible greeting types. After selecting a greeting type, the agent chooses whether to 1) listen to the existing greeting for that type; 2) record a new greeting for that type, or 3) return to the main menu. If the agent selects the option to listen, the name of the application directory on the media server is set and the external VRU script that plays the greeting is triggered. Then the agent is returned to the main menu. If the agent selects the option to record, the Unified CVP recording application is called. The recording application contains its own built-in audio prompts that step the agent through the process of recording and saving a greeting. At the end, the agent is returned to the main menu.

There are several other behaviors in the script to note. An agent may select to listen to a greeting type for which no greeting exists. In that event, a VRU script that plays an error message is called. Also, in two places in the script, the path to the application directory is reset to the default. This is because (in this example) that is where the files for the audio files reside. The only files that reside outside of the default directory are the greetings themselves.

Figure 2: Agent Greeting Record Script



RecordAgentGreeting Micro-application

Unified CVP includes a dedicated micro-application -- RecordAgentGreeting -- for recording agent greetings. The application lets agents record, review, re-record, and confirm the save of a greeting. It includes audio files to support each of these functions. If an agent is not satisfied with a greeting, it can be re-recorded up to three times. Upon confirmation of a save, the application FTPs the saved file to the media server.

Built-in error checking includes checks for the data required to name the file (*Person ID* + *AgentGreetingType* variable value), media server specification, valid menu selections made by the agent, and successful FTP of the greeting file.

Agent Greeting Record Script Nodes

Using the example script as a reference, here are descriptions of the functions its nodes perform.

Table 4: Script Node Functions for Agent Greeting

Node	Value	What it does
Variable:Call:user. microapp.input_type	`D`	Sets the allowable input type to DTMF (touch tone).
RunExtScript:Press 1-9 to Select Greeting X	`M,press_1_thru_9_greeting,A`	Runs the VRU script that defines which digits are valid to select an AgentGreetingType and plays a voice prompt describing the options.

Node	Value	What it does
Variable:Call:AgentGreetingType	`Call.CallerEnteredDigits`	Sets the AgentGreetingType to the digit the agent pressed. This text is used in the greeting wave file. It can be a simple numbering system or more descriptive titles such as “English.”
RunExtScript: 1 - hear greeting X, 2 - record greeting X, 3 - return to menu	`M,press1-press2-press3,A`	Runs the VRU script that defines which digits are valid to select a desired action and plays a voice prompt describing the options.
CED	`1,2,3`	Tells the script how to handle the caller entered digits in response to the 1,2,3 external script.
Variable:Call: user.microapp.app_media_lib	Set three times: • Once to `"app/ag_gr"` • Twice to `""` (an empty string; that is, the default)	Defines the path to the application directory on the Unified CVP media server. Prior to playing the greeting file, it is set to the dedicated greeting file directory (in this example, `app/ag_gr`). After the greeting file plays, it is reset to the default application directory where (in this example) the files for voice prompts are stored. If the voice prompts were stored in the same directory as the greeting files, there would be no need to reset the path.
RunExtScript: Play Recording	`PM,-a,A`	Runs the VRU script that plays the selected Agent Greeting.
RunExtScript:Greeting Not Found	`PM,no_greeting_recorded,A`	Runs the VRU script that plays an error message if the Agent Greeting selected to play does not exist.

Node	Value	What it does
Variable: Call:user.microapp. ToExtVXML[]	Array Index: 2 Value: "ftpPath=<*path_to_dedicated/directory*>" For example: "ftpPath=en-us/app/ag_gr"	Specifies the FTP information that the VXML server uses to write greeting files to the media server. The information must match the FTP information configured for the media server in the Unified CVP Operations Console. The value for array index must be 2. The value consists of: • ftpPath= to set the path to the dedicated directory for agent greeting files. • The path must begin with the locale directory. To view additional setting options, see CVP documentation.
Variable: Call:user.microapp. ToExtVXML[]	Array Index: 0 Value: "application=RecordAgentGreeting"	Identifies the external Unified CVP micro-application (RecordAgentGreeting) that is used to record the greeting. The value for array index must be 0.
RunExtScript: Run Default Recording Application	GS,Server,V	Runs the VRU script that launches the Get Speech micro-application on the VXML server.

Specify Media Server in Routing Scripts

When you configure media servers in CVP, you can specify a default media server. The benefit to specifying a default media server is that your scripts do not need a Set Variable node to access the default media server. For this to work, you must make sure that the files a script requests are stored on the default server.

If you do not define a default media server, or if you define a default but the files that your script requires are not stored on the default, then the script must include a Set Variable node to identify a media server.

To specify a media server that stores the files required by your script, use the following settings in the Set Variable node:

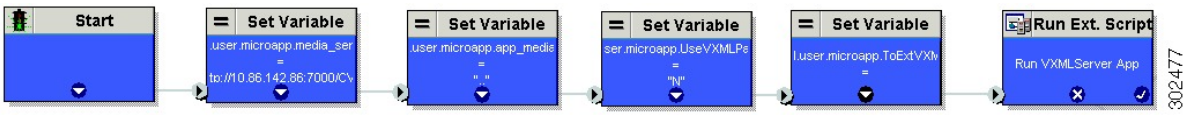
- Object Type: Call.
- Variable: Must use the user.microapp.media_server expanded call variable.
- Value: Specify the HTTP path to the server. For example: “http://myserver.mydomain.net.” You must enclose the path in quotes.
- Alternately you can specify an IP address in place of a hostname.

In scripts that invoke an external VXML application (as the Agent Greeting record script does), if you explicitly set a variable for the media server (user.microapp.media_server), then you must also set the following variables:

- The path to the media server application directory (user.microapp.app_media_lib)
- The CVP UseVXMLParams value to N.(user.microapp.UseVXMLParams)

See the following example.

Figure 3: Additional Required Variables When Specifying a Media Server



Specify Greeting File Locale and Application Directories in Routing Scripts

CVP uses a default storage directory for media files: `<web_server_root>/en-us/app`. To take advantage of this, Unified CCE call routing scripts automatically add `en-us/app` to the server name when constructing HTTP requests for media files. For example:

- If the script node that defines the media server has a value of “http://myserver.mydomain.com,” and
- The script node that defines which audio file to play has a value of “5050_1.wav” (for an agent with a Person ID of 5050), then
- The HTTP request for the file is automatically constructed as `http://myserver.mydomain.com/en-us/app/5050_1.wav`

If your greeting audio files are stored in a different locale directory, you must add a Set Variable node to your script that identifies the locale directory. As you must store your greeting files in a dedicated subdirectory under the locale, you must always add a Set Variable node that identifies that directory.

Use these settings in the Set Variable node to specify your locale directory:

- Object Type: Call.
- Variable: Must use the user.microapp.locale expanded call variable.
- Value: Specify the directory name. For example: “pt-br” (Portuguese-Brazil). You must enclose the path in quotes.

Use these settings in the Set Variable node to specify your application directory:

- Object Type: Call.
- Variable: Must use the user.microapp.app_media_lib expanded call variable.
- Value: Specify the directory name. For example: to use a directory “greet” in place of the default directory “app”, enter “greet”. To use a sub-directory “greet” under “app” enter “app/greet”. You must enclose the path in quotes.

Verify Length for Media Server Locale and Application Directory Variables

If you include Set Variable nodes for the media server, locale, and/or application directories, make sure that the values you set for them do not exceed the Maximum Length settings for their corresponding expanded call variables.

For example, if you include a Set Variable node for the media server with a value of "http://mysubdomain.mydomain.co.uk", the string is 33 characters long. Therefore, the Maximum Length setting for the user.microapp.media_server expanded call variable must be 33 or greater. Otherwise, the server name is truncated in the HTTP request for the file and the file is not found.

To configure ECC variables, use the Unified CCE Configuration Manager. Select **List Tools** > **Expanded Call Variables List**.

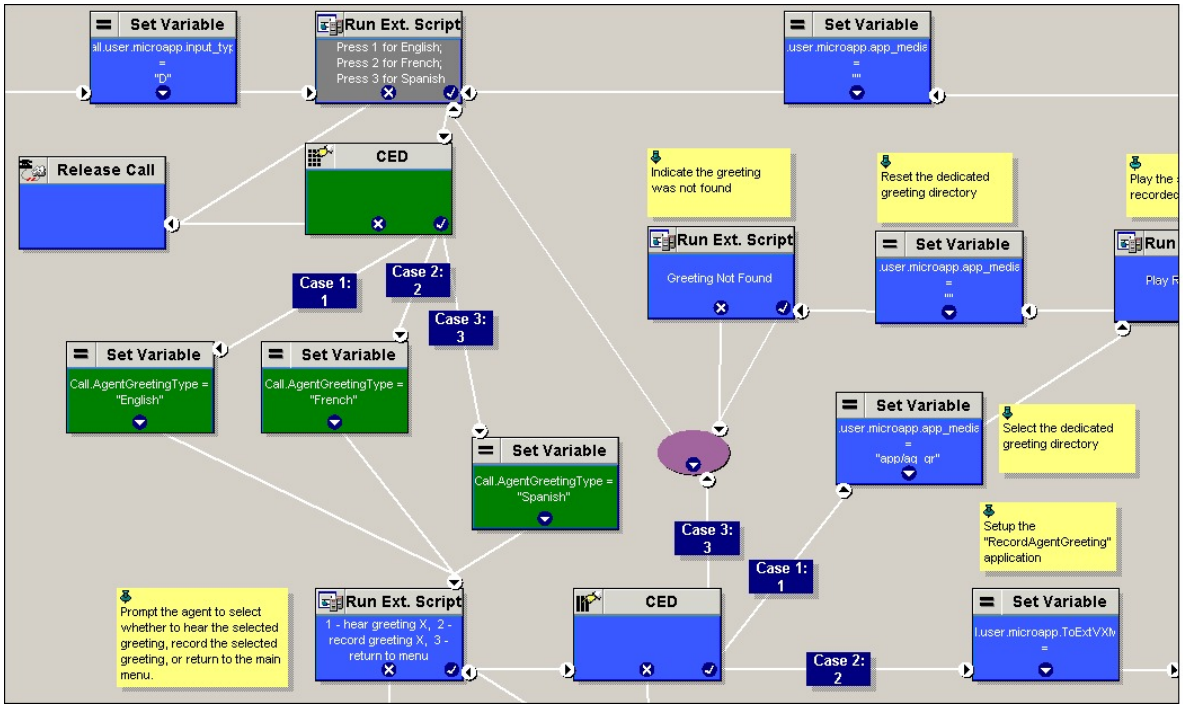
Descriptive Agent Greeting Type Strings

The previous Agent Greeting record script example stores Agent Greeting Type values as numbers (although in string format). But suppose you prefer more descriptive string names. For example, "English," "French," and "Spanish." Or "Sales," "Billing," and "Tech Support."

Descriptive names can make it easier to understand at a glance what different numeric key selections in your scripts correspond to. Note that they also affect how greeting files are named (for example, for an agent whose Person ID is 5050, `5050_English.wav` as opposed to `5050_1.wav`).

The following script example is almost identical to the previous record script, except that it includes four additional nodes (highlighted in green). They consist of an additional CED node that maps the keys 1, 2, and 3 to language names. The Run Ext Script node (in gray) was modified for the new options. The rest of the script is the same with no other changes required. Note that your routing scripts require a corresponding mapping of numeric keys to language names.

Figure 4: Script with Descriptive Greeting Type Strings



Agent Greeting Play Script

The Agent Greeting feature requires a dedicated routing script that causes the agent greeting to play. This script is invoked by the PlayAgentGreeting dialed number.

The Play script must contain at least two and possibly four specific nodes, depending on other factors.

You always need the following nodes:

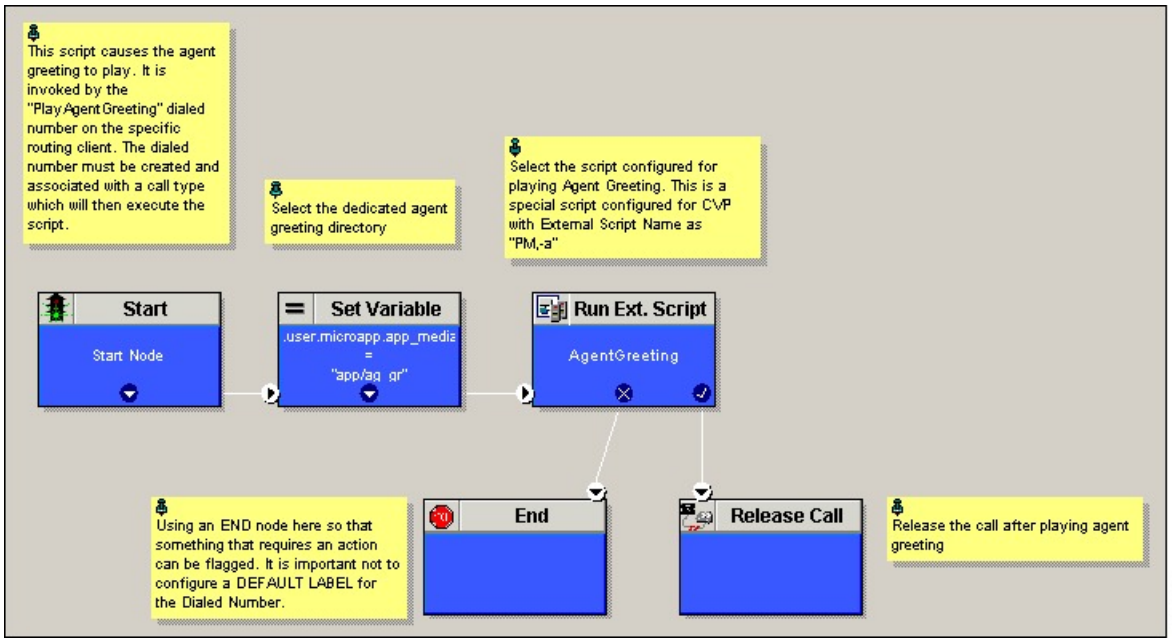
- A Run External Script node that calls the VRU script that plays the greeting.
- A Set Variable node that sets the directory path to your greeting files.

You may also need to include in your scripts Set Variable nodes that:

- Specify the Media Server: Unified CVP lets you specify a default media server. If you are not serving your audio files from the default media server, your scripts must include a variable that identifies the server where your audio files are stored.
- Specify the Locale Directory: Additionally, if you are not storing your files in the default locale directory `en-us` on the media server, you must include a variable that specifies the name of the locale directory where the files are stored.

Note The Locale Directory set variable node is optional. It is needed only if you decide to use a directory other than the default one.

Figure 5: Agent Greeting Play Script Example



On a Mobile Agent callflow, CUCM may return a 404 error due to the absence of Agent Greeting, leading to call failure. To fix this issue, do the following:

1. Add a new Run External Script node with its backup media mapped to the agent greeting.
2. Add the Run External Script node between the failure path of the AgentGreeting Run External Script node and the End node.
3. Connect the Run External Script node's success path to the existing Release call node and failure path to the existing end node.

Adding the Run External Script node may add a short delay of one to two seconds to the call flow.

Reporting

In agent, skill group, and precision queue reports, greeting time is not specifically broken out. The period during which the greeting plays is reported as talk time. Record time is counted as an internal call by the default skill group.

Calls that involve Agent Greeting consist of two call legs: the inbound call from the customer and the call to Unified CVP for the greeting. Both of these legs have the same RouterCallKeyDay and RouterCallKey values in the TCD and RCD tables in the database. You can use these values to link the two legs together for reporting purposes.

Greeting Call Statistics

To view greeting call statistics, create a separate call type and associate it with the routing script that plays agent greeting. New Cisco Unified Intelligence Center templates for the agent greeting call type are created based on the data in the existing Call_Type_Real_Time and Call_Type_Interval table in the database.

Peripheral Call Types for Agent Greeting

There are two peripheral call types specific to Agent Greeting that you can use to track and report on the feature.

- Call Type 39: Play Agent Greeting. Route request to play an Agent Greeting.
- Call Type 40: Record Agent Greeting. Agent call for recording an Agent Greeting.

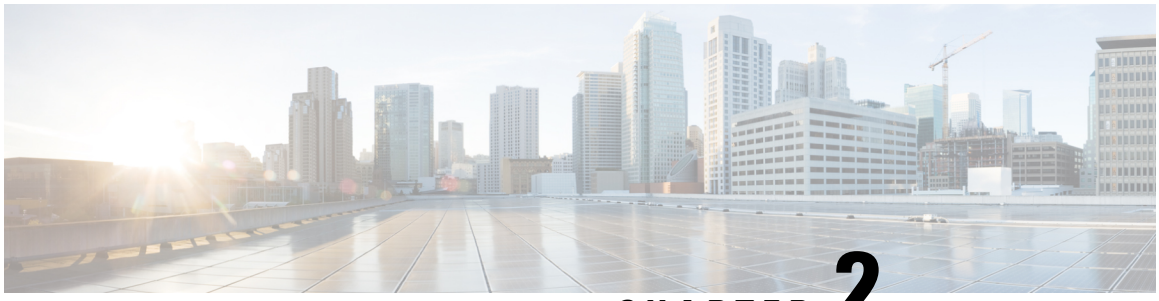
Extra TCDs and RCDs are generated for the agent greeting call leg, and they can be linked to the first call leg by the same RouterCallKeyDay and RouterCallKey.

Serviceability

Serviceability for Agent Greeting includes SNMP events captured by your Network management software that indicate reasons for greeting failures and counters to track the number of failed greeting events.

Note There is no counter for the number of failed agent greeting calls.

When system components fail, Agent Greeting may be impacted. For example, if a requested greeting audio file cannot be found for any reason, the call proceeds normally without the Agent Greeting.



CHAPTER 2

Agent Request

Agent Request Feature Description

The Agent Request feature allows a customer to initiate a request on the web that results in a call from an agent.

To use Agent Request, your solution requires the Cisco SocialMiner optional component. Cisco SocialMiner works in a Contact Center Enterprise (Unified CCE) solution to process the request from its inception through the delivery of the callback.

Important The Agent Request feature can be used only if the customer or a partner develops a custom application. There is sample code on DevNet (formerly Cisco Developer Network) that you can use to understand how to start building your custom application to submit callback requests to SocialMiner.

SocialMiner and Agent Request

SocialMiner provides the Callback API used by a custom application to request a phone call from a contact center agent.

The API works in conjunction with SocialMiner callback feeds, campaigns, and notifications to pass callback requests to the contact center for routing.

The Callback API:

- Allows custom applications to initiate a callback.
- Forwards the callback request and callback details to Unified CCE using a notification mechanism (the Connection to Unified CCE notification type) through a Media Routing (MR) connection.

- Allows custom applications to retrieve the state of the callback as well as the estimated wait time (EWT) until an agent becomes available.
- Allows custom applications to cancel a requested callback.

The Callback API supports the use of Call variables and ECC variables for callback requests. Call variables and ECC variables send customer-specific information with the request. When you create a callback contact, the social contact associated with the callback contact includes all of the specified variables as extension fields.

Unified CCE and Agent Request

When it receives an Agent Request, Unified CCE performs these tasks:

- Process the callback request.
- Route the callback request to an agent and place a call from the agent's phone to the customer.
- Notify SocialMiner that the agent has been selected.

Agent Desktops and Agent Request

Cisco Finesse supports Agent Request.

Enterprise Chat and Email and Agent Request

To configure prefixes and filters for dialed numbers in Enterprise Chat and Email, you must use the Unified CCE Script Editor.

Unsupported Environments

Agent Request is not supported:

- In a Parent/Child deployment
- With Mobile Agents
- In a hybrid deployment

Related Topics

Create Script for Agent Request, on page 32

Agent Request Prerequisites

Install and configure SocialMiner before implementing Agent Request. SocialMiner must be geographically colocated with one side of the Media Routing Peripheral Gateway (MR PG).

The customer or partner must build a custom application for the Agent Request feature. See Use the Sample Code to Create a Customer Callback Request, on page 34.

SocialMiner is always deployed in a DMZ. Remember to open the port you have configured for the MR PG. See Set up the Media Routing PG and PIM, on page 29.

Agent Request Call Flow

The flow proceeds as follows:

1. The customer application initiates an agent request by requesting a callback.
2. SocialMiner sends the request to the Media Routing PG.
   a. The Media Routing PG sends the request to the Router.
   b. The Router sends the request to the Agent PG.
   c. The Agent PG sends the request to the agent.
3. A call is initiated from the agent's phone, on behalf of the agent, dialing the customer's phone number.

Note The agent does not control when the call is placed.

Figure 6: Agent Request Call Flow

Agent Request Scenarios

1. From the web, the customer requests to speak to an agent.
2. The customer receives feedback that the request is accepted.
3. The customer receives feedback that the call is queued and the estimated wait time.
4. The customer receives feedback that a call is on its way.
5. The agent's phone places an outbound call.
6. The agent is presented with call context.

If	Then
The customer is available	The customer receives and answers the call, and speaks to the agent
The customer is busy when the callback occurs	The agent receives a busy tone
The customer does not answer when the callback occurs	The agent hears ringing
The customer cancels the callback before an agent is selected	There is no impact on the agent

Configure Unified CCE for Agent Request

The following information describes how to configure Agent Request for a Unified CCE deployment.

Important Configure Unified CCE before you configure SocialMiner.

Configuration Manager

Use these Configuration Manager tools and procedures to configure Agent Request.

Configure Network VRU and Network VRU Script

Procedure

Step 1 In the Configuration Manager, use the Network VRU Explorer tool to configure and save a type 2 VRU. The Network VRU is used to queue voice callback tasks if an agent is not available to handle them.

Step 2 In the Configuration Manager, use the Network VRU Script List tool to add a Network VRU Script that references the Network VRU that you configured in Step 1.

The Network VRU Script is used for Estimated Wait Time.

Configure the Media Routing PG and PIM

Procedure

Step 1 In Configuration Manager, open the PG Explorer tool to configure a media routing PG.

Step 2 Create a media routing PIM and routing client for SocialMiner.

Write down the Logical Controller ID and the Peripheral ID. You will use them when you set up the PG.

Step 3 On the Peripheral tab in the PG Explorer tool, check the **Enable post routing** check box.

Step 4 On the Routing Client tab in the PG Explorer tool, select the **Multichannel** option from the **Routing Type** drop-down list box.

Step 5 On the Advanced tab in the PG Explorer tool, select the type 2 Network VRU that you created.

Configure Call Type

Procedure

Open the Call Type List tool, and create a call type to handle calls from an agent request voice callback.

Configure Dialed Number/Script Selector

Procedure

Step 1 Open the Dialed Number/Script Selector List tool, and create a script selector on the routing client that you configured. SocialMiner uses this script selector to request agents for voice callback. (The script selector configured here must be the same as the one entered in the SocialMiner notification.)

Step 2 On the Attributes tab, select **Cisco_Voice** from the **Media routing domain** drop-down list box.

Step 3 On the **Dialed Number Mapping** tab, map the script selector to the call type you created.

Configure ECC Variables

Procedure

Step 1 Open the **Expanded Call Variable List** tool.

Step 2 Add one or more ECC Variables for the callback request.

Note Arrays are not supported with the Agent Request feature.

CCE solutions support the Latin 1 character set only for Expanded Call Context variables and Call variables when used with CVP, Finesse, and SocialMiner. CCE also supports the use of multi-byte character sets in limited usage for ECC and call variables when setting them in Script Editor using double quotes.

Set up the Media Routing PG and PIM

Procedure

Step 1 From Cisco Unified CCE Tools, select **Peripheral Gateway Setup**.

Step 2 On the Components Setup screen, in the Instance Components panel, select the PG Instance component. If the PG does not exist, click **Add**. If it exists, click **Edit**.

Step 3 In the Peripheral Gateways Properties screen, click **Media Routing**. Click **Next**.

Step 4 Click **Yes** at the prompt to stop the service.

Step 5 From the Peripheral Gateway Component Properties screen, click **Add**, select the next PIM, and configure with the Client Type of Media Routing as follows.

a) Check **Enabled**.

b) In the **Peripheral Name** field, enter `MR`.

c) For **Application Hostname (1)**, enter the hostname or IP address of SocialMiner.

Note The system does not support IP address change. Use the hostname if you foresee a change in IP address. This is applicable for all the **Hostname/ IP Address** fields.

d) By default, SocialMiner accepts the MR connection on **Application Connection Port** 38001. The Application Connection Port setting on SocialMiner must match the setting on the MR PG; if you change the port on one side of the connection, you must change it on the other side.
e) Leave the **Application Hostname (2)**, field blank.
f) Keep all other values.
g) Click **OK**.

Step 6 On the Peripheral Gateway Component Properties screen, enter the Logical Controller ID that you recorded when you configured the Media Routing PG and PIM.

Step 7 Accept defaults and click **Next** until the Setup Complete screen opens.

Step 8 At the Setup Complete screen, check **Yes** to start the service. Click **Finish**.

Step 9 Click **Exit Setup**.

Step 10 Repeat from Step 1 for Side B.

Step 11 Navigate to **Unified CCE Administration** > **Infrastructure Settings** > **Inventory**.

Step 12 Add SocialMiner as an external machine.

a) Click Add.
b) Select SocialMiner from the drop-down list.
c) Enter the required information.
d) Click **Save**.

The system automatically enables and completes the **CCE Configuration for Multichannel Routing** settings in SocialMiner Administration, including the **Application Connection Port** you specified.

Configure SocialMiner for a Voice Callback Agent Request

To support a callback request, SocialMiner must be configured with:

- A callback feed
- A campaign
- A Connection to CCE notification configured for the campaign mentioned above that will be triggered by incoming callback requests with a matching tag.

Create Feed

Procedure

Step 1 Sign in to SocialMiner.

Step 2 Click **Configuration**.

Step 3 On the **Manage Feeds** panel, click **New**.

Step 4 For **Type**, select **Callback**.

Step 5 Name the feed.

Step 6 For **Reply Template**, retain the default, *No reply template*.

Step 7 Configure the feed to automatically tag all callback requests that come in on that feed. For example, autotag with 'sendtocontactcenter'.

Make a note of the tag. It is used to trigger the notification to CCE.

Step 8 Click **Save**.

Create Campaign

Procedure

Step 1 Sign in to SocialMiner.

Step 2 Click **Configuration**.

Step 3 On the **Manage Campaigns** panel, click **New**.

Step 4 Name the campaign.

Step 5 Enter an optional description.

Step 6 Make no selection in the **Chat Invitation Feed** drop-down list.

Step 7 Locate the Callback feed in the **Available** panel and move it to **Selected**.

Step 8 Click **Save**.

Create Notification

Procedure

Step 1 Sign in to SocialMiner.

Step 2 Click **Administration**.

Step 3 On the **Manage Notifications** panel, click **New**.

Step 4 For **Type**, select **Connection to CCE**.

Step 5 Name the notification.

Step 6 From the **Campaigns** drop-down list, select the campaign that you created for the callback.

Step 7 In the **Tags** field, enter the tag that is automatically applied to callback requests by the feed. In our example 'sendtocontactcenter'.

Step 8 For **Request Type**, select **Callback**.

Step 9 In the **Dialed Number/Script Selector** field, enter the dialed number string that you have configured.

See Configure Dialed Number/Script Selector, on page 29.

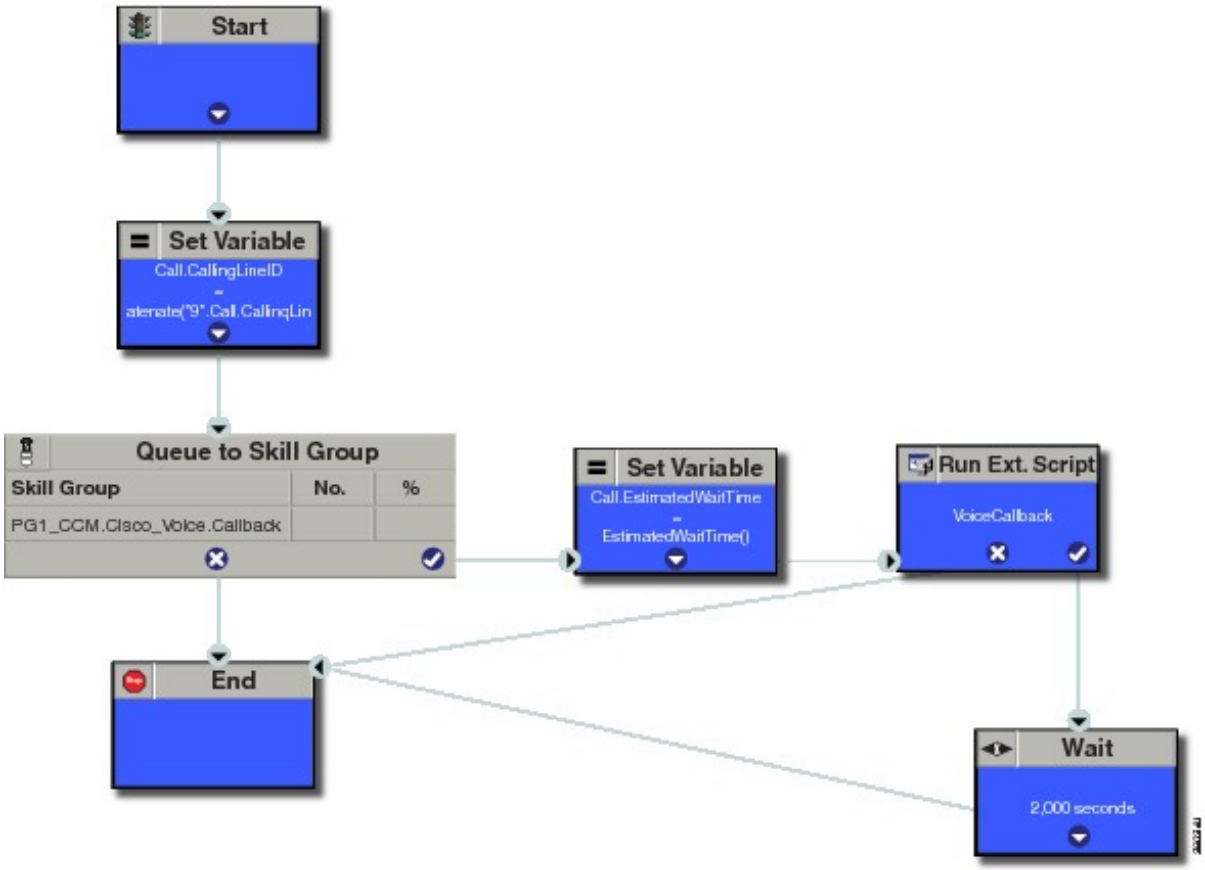
Step 10 Click **Save**.

What to do next

For more SocialMiner configuration information, see the *Cisco SocialMiner User Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/socialminer/products-user-guide-list.html.

Create Script for Agent Request

This illustration shows a sample script. The key below explains the nodes.



Start node: Create the **Start** node by selecting a new Routing Script from the Script Editor.

Set Variable (Call.Calling Line ID) node: (optional). If required, you can set the CallingLineID (CLID/ANI) variable to implement a "dial-plan," pre-pending a set of digits to the phone number provided by the customer so that it can be correctly routed. For example, it is often necessary to add 9 to the phone number to reach an outside line. In other cases, more pre-pended digits may be required to reach the end customer.

You can also set up Unified Communications Manager Route Patterns to respond to a certain set of digits by routing the call to an outside line with a specified area code. To implement a dial-plan, add a Set Variable node before the queue, as shown in this example. In this case, a 9 is pre-pended to the customer phone number using the built-in concatenate function.

Queue to Skill Group node: The Agent Request call can be queued against one or more Skill Groups, Precision Queues, or a queue-to-agent node. In the example script, the call is queued against a single skill group.

Set Variable (Call.Estimated Wait Time) node: A customer who requests a voice callback might want to know approximately how long it will be before the call is returned. You can configure voice callback to provide an estimate of the wait time back to the customer. The estimated wait time is calculated once, when the call enters the queue. The time is not updated as the position in the queue changes.

The default estimated wait time algorithm is based on a running five minute window of the rate of calls leaving the queue. Any calls that are routed or abandoned during the previous 5 minutes are taken into account as part of the rate leaving queue. For Precision Queues, the rate leaving queue represents the rate at which calls are delivered or abandoned from the entire precision queue, not any individual recision Queue steps. The algorithm computes the wait time for each of the queues against which the call is queued (Skill Groups or Precision Queues) and then returns the minimum estimated wait time. Queue to Agent is not supported.

While the queue builds, the small number of calls in the queue makes the estimated wait time less accurate and the value fluctuates rapidly. As the queue operates with more calls over time, the estimated wait time is more accurate and consistent.

Note that the built-in function also applies to inbound calls that queue.

Set the Call Wait time as follows:

1. From the Set Variable node, select **Call** from the Object type drop-down menu.
2. From the Variable drop-down menu, choose **Estimated Wait Time()**.

   You can then work with the Formula Editor to use the default estimated wait value or create a formula and use your own value.
3. Click **Formula Editor**, and do either of the following:
   - To use the default estimated wait value, click the Built-In Functions tab and choose EstimatedWaitTime()
   - To create a formula and use your own value, click the Variables tab and choose an entry in the Object type list and an entry in the Object list. Then double-click a variable in the Variable list.

Run Ext Script node: Apply the Network VRU script as follows:

1. Click the Queue tab.
2. Click **Run External Script**.
3. Click inside the script. A Run External Script node appears.
4. Double-click the node and choose the Network VRU script from the list; then click **OK**.

   The call variable Estimated Wait Time now contains a value in the EstimatedWaitTime field and can be passed to peripherals.

   Note that a Run External Script node is required to send the EstimatedWaitTime to SocialMiner.

Wait node: The wait period before an agent becomes available.

End node: The script ends if no agent becomes available.

Use the Sample Code to Create a Customer Callback Request

Cisco Systems has made sample callback application code available to use as a baseline in building your own application. This sample includes retrieving and displaying the estimated wait time, assuming it has been configured in Unified CCE. You can find the sample code on DevNet.

Note You cannot copy and paste this code to achieve a working application. It is a only a guideline.

For more information about how to use the Callback API, see the *Cisco SocialMiner Developer Guide* at https://developer.cisco.com/site/socialminer/documentation/.

Procedure

Step 1 Retrieve the feed id by entering this URL in a browser: **https://<SocialMiner_Hostname_or_Ip>/ccp-webapp/ccp/feed**.

In the example output below, note that the value in the <name> field is "Callback." Look for the number of the feed id identified at the end of the refURL path (in this case, it is 100000) just before the </refURL> tag. Copy this number.

```
<feeds>
<Feed>
<changeStamp>0</changeStamp>
<name>Callback</name>
<pushFeedURL>https://128.107.81.27/ccp/callback/feed/100000</pushFeedURL>
<refURL>https://128.107.81.27/ccp-webapp/ccp/feed/100000</refURL>
<status>1</status>
<tags>
<tag>trial</tag>
</tags>
<type>10</type>
</Feed>
</feeds>
```

Step 2 Access the sample application from DevNet: https://developer.cisco.com.

Step 3 Enter values in the fields:

- Title: A title or subject for the callback request.
- Author: The name of the person submitting the callback request.
- Phone: The phone number to call back.
- Feed Id: The value from the refURL above.

Step 4 Click **Call me back**.

Agent Request Reporting

Cisco Unified Intelligence Center CCE reports include data for Agent Requests

Note Agent requests that fail before being routed to CCE will not be included in the CCE solution-level reports. The SocialMiner search function can be used to identify these requests.

Call Type and Call Type Skill Group Metrics

- **Calls Offered** — Incremented when Call Type is entered (through Script Selector or Call Type node).
- **Calls Abandoned in Queue** — Incremented when a Queued Callback request is canceled by the customer prior to when an Agent is selected to handle the Voice Callback call.
- **Calls Answered** — Incremented if the call is placed from the agent and represents work accepted by the agent.
- **Calls Handled** — Incremented if the customer answers the call. Calls Answered minus Calls Handled indicates how many calls failed to reach the intended customer.
- **Service Level Offered** — Incremented for all routed calls, including voice callback calls initiated through the agent request API.
- **ServiceLevelCalls** — Incremented if the call is presented to the agent within a service level.
- **Answer Intervals (1 - 10)** — The appropriate bucket is incremented based on how long the call was in the queue.

Skill Group Metrics

Call Type Skill Group and Skill Group metrics are not counted in the same way. The skill group metric treats each call as agent-initiated; therefore, Calls Answered and Calls Handled are not incremented. AgentOutCallsTime, AgentOutCalls, AgentOutCallsTalkTime, AgentOutCallsOnHold, and AgentOutCallsOnHoldTime are incremented.

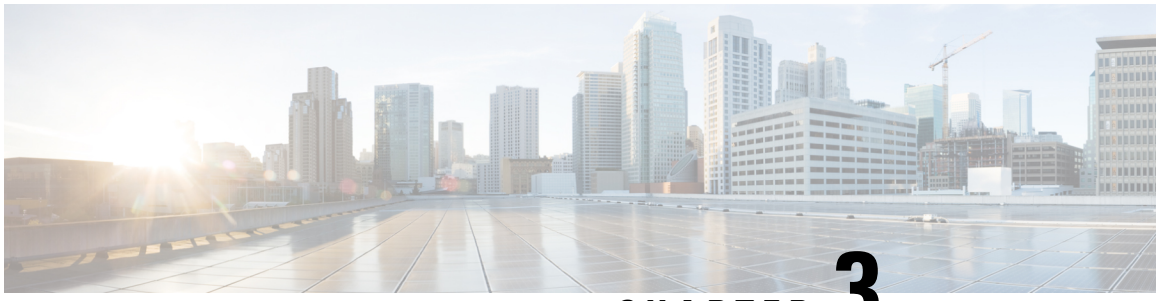
Agent Real Time

The direction in the Agent Real Time table is listed as Outbound.

Termination Call Detail

For custom reporting, the Termination Call Detail records contain a PeripheralCallType of 41 -Voice Callback.

Calls which do not successfully connect to a customer have a call disposition of **10 - Disconnect/Drop no answer**. This includes agent request calls to busy numbers.



CHAPTER 3

Contact Sharing

Contact Sharing Overview

Contact Sharing uses extrapolation to distribute calls and increase the overall agent and call handling capacity. Contact Sharing enables customers with multiple Unified Contact Center Enterprise (Unified CCE) systems to distribute calls across those systems. The Contact Director (sometimes called an IVR ICM) acts as an initial entry point for the call. If the call needs agent attention, Contact Sharing decides where to route the call based on Live Data real-time state information from the Unified CCE target systems. You can configure Contact Sharing to base routing decisions on factors such as the number of calls in queue, agent availability, average handle time, and custom calculations.

Use Unified CCE Administration to create and maintain the Contact Sharing groups and rules. A group is a collection of skill groups and precision queues across target systems. Each group has a rule that defines the logic for selecting the best skill group or precision queue in that group for a routing request. Each group has an `Accept Queue If` condition to include or exclude the individual skill groups and precision queues from the group for the routing decision. You can then route the call to the Unified CCE target system whose precision queue or skill group is the best match for the group's rule. The target system's routing scripts determine the final method for handling the request.

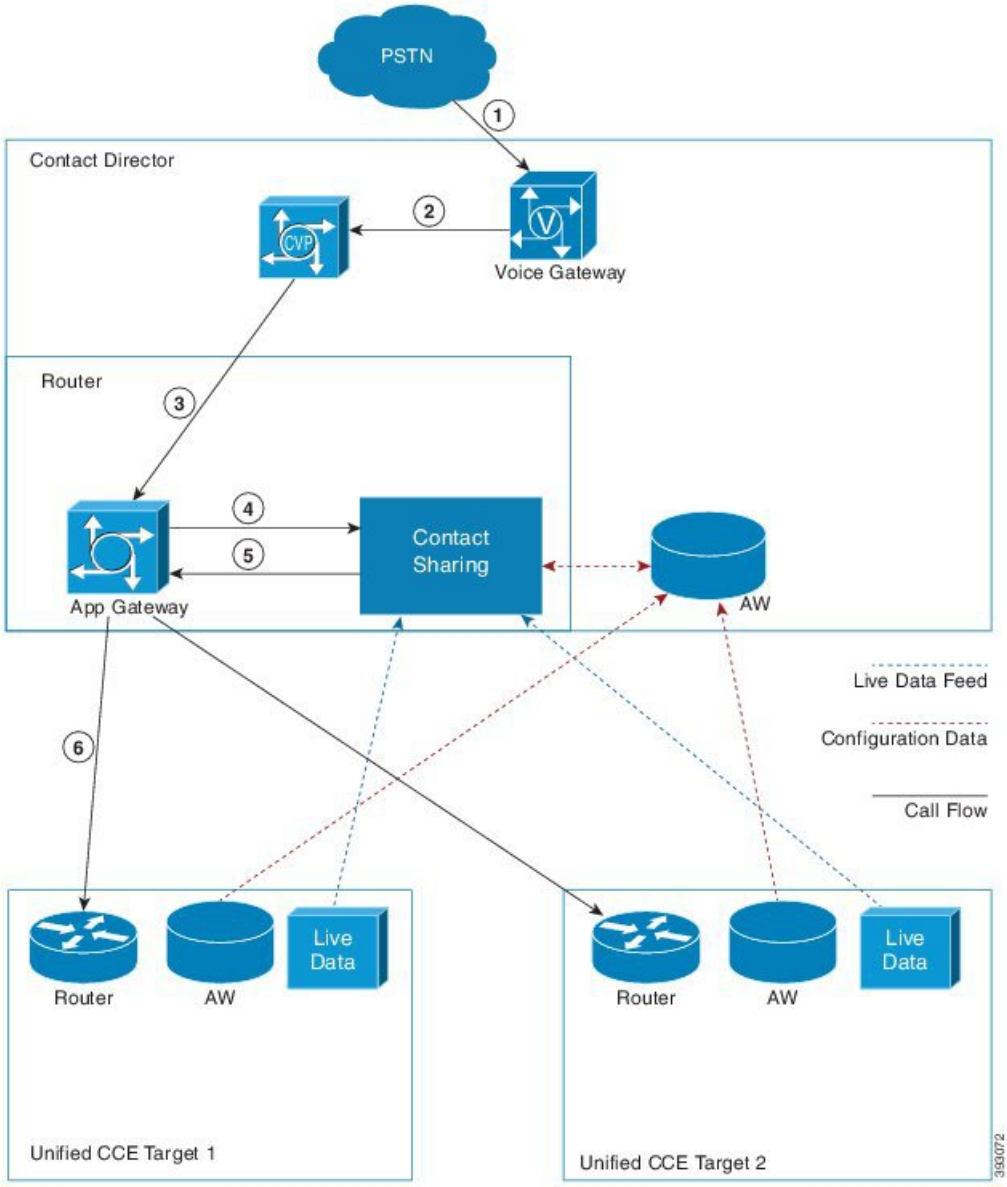
Note Contact Sharing gadgets are enabled only for the Contact Director deployment type.

For Contact Director configuration limits, see the chapter on configuration limits in the *Solution Design Guide for Cisco Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html.

Contact Sharing Call Flow

The basic Contact Sharing call flow runs as shown in this diagram:

Figure 7: Contact Sharing Call Flow



1. A call comes into the Voice Gateway on the Contact Director.
2. The Voice Gateway passes the call to CVP for VRU processing.
3. When the caller opts to speak to an agent, CVP passes the call data to the Router through the VRU PG.
4. The Router runs a script that assigns the call to a particular Contact Sharing Group. The Router sends the call data to the Application Gateway to pass to that Contact Sharing node.
5. The Contact Sharing node uses the Group Rule to determine which skill group or precision queue in its Queue should get the call. The node passes the selected target instance and its extrapolated guess of the best skill group or precision queue back to the Application Gateway.

6. The Application Gateway passes the information to the Router which routes the call to the selected target instance.

Failover for Contact Sharing

Like all the main components in Unified CCE, Contact Sharing nodes run in redundant pairs. The redundant pair operates in hot-standby mode. Side B's data is kept in sync with Side A to ensure minimum failover time.

When the Side A process fails over, Side B takes over routing. Because the nodes operate in hot-standby mode, Side B does not reread Queues from the database. Side B requests a snapshot from Live Data. Until the snapshot arrives, Side B continues routing based on the last available Live Data modified by the current extrapolated data.

During failover, some route requests may receive an error. Error handling sends those requests to the default route. When Side A comes back online, it does not take over immediately. Side A remains in a ready state until Side B fails over.

The Contact Sharing process monitors the AW to see whether it has the latest configuration changes. If the AW configuration database does not have those changes or is not accessible, the Contact Sharing process switches to the alternate AW configuration data source.

When core components fail over on a target instance, reporting data can occasionally zero out. In that case, the Contact Sharing routing sends calls to the instance with reported resources. If Live Data does not zero out reporting data, then Contact Sharing continues to route on stale data until the snapshot information begins to arrive. If the active Contact Sharing side loses both Live Data connections, that side goes inactive and fails over to other side.

Contact Director Installation and Setup

Contact Sharing runs on a Contact Director that you connect with two target Unified CCE deployments. You configure the Contact Director to monitor the Live Data feed from the targets. The task flow for installing a Contact Director is as follows:

Task	See
Ensure that virtual machines are ready for installation.	*Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*
Install Unified Communications Manager.	*Installation Guide for Cisco Unified Communications Manager and IM and Presence Service*
Install Unified CCE components (Router, Logger, Administration & Data Servers, peripherals).	*Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*
Optionally, install Cisco Unified Intelligence Center.	*Installation and Upgrade Guide for Cisco Unified Intelligence Center*
Install Unified CVP.	*Installation and Upgrade Guide for Cisco Unified Customer Voice Portal*

Install Unified CCE

This section expands the installation process outlined in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

After setting up the VMs for the Contact Director, you install the Unified CCE components. The install and configuration of a Contact Director varies slightly from a Unified CCE deployment. The following table lists the applicable parts of the Unified CCE install procedures with any necessary changes for the Contact Director:

Task	Steps	Contact Director Notes
Install Unified CCE Component Software (running the ICM-CCE-CCHInstaller)	—	—
Set up Organizational Units	Add a Domain	—
	Add Organizational Units	—
	Add Users to Security Groups	—
Set Up Unified CCE Central Controller Components	Add Unified CCE Instance	—
	Create Logger Database	Select **NAM**.
	Create HDS Database	—
	Add Logger Component to Instance	Choose **Hosted** > **Network Application Manager (NAM)** for the **Logger Type**.
	Add Router Component to Instance	Set the following values for a Contact Director: • Check **Enable Remote Network Routing**. • Set the **NAM ID**. • Check **Contact Sharing** when you create the Router.
	Add Administration & Data Server Component to Instance	For a Contact Director, choose **Hosted** > **Network Administration & Data Server for Network Application Manager (NAM)** for the **Deployment Type**.

Task	Steps	Contact Director Notes
Set up Peripheral Gateways	Configure Peripheral Gateways	—
	Add Peripherals to Peripheral Gateways	—
	Set Up Peripheral Gateways	—
After completing the standard installation, perform these Contact Director-specific setup procedures.		
Application Gateway Access Between Systems	Create Unified ICM Application Gateway	—
	Create an INCRP on Each Target Instance	—
	Set Application Gateway Default Values	—

Related Topics

Application Gateway Access Between Systems, on page 41
Create Unified ICM Application Gateway, on page 41
Create an INCRP on Each Target Instance, on page 43
Set Application Gateway Default Values, on page 44

Application Gateway Access Between Systems

The Contact Director uses a type of Unified ICM Application Gateway to access a target instance. After adding the components to the target instance, set up a Unified ICM Application Gateway in the Configuration Manager on the Administration & Data Server.

After setting up the Unified ICM Application Gateway, you can reference it with a Unified ICM Remote ICM node in a routing script on the Contact Director.

Create Unified ICM Application Gateway

This procedure creates a Unified ICM Application Gateway on the Contact Director. You also need an application gateway on each target Unified CCE system.

Procedure

Step 1 Open the **Configuration Manager** on an Administration & Data Server that your Contact Director uses.

Step 2 Select **Tools** > **List Tools** > **Application Gateway List**.
The **Application Gateway List** window appears.

Step 3 Click **Retrieve**.

Step 4 Click **Add**.
The **Attributes** tab appears.

Step 5 Specify the following values on the **Attributes** tab:

Field	Description
Name	A name for the Unified ICM Application Gateway
Type	Select **Remote ICM**.
Preferred Side	Indicates the preferred side of the Application Gateway to use when both are available. If only one side is available, that side is always used. This option applies only for Custom Gateways. For Remote ICM systems, a suffix on the connection address indicates the preference.
Encryption	Indicates whether requests to the Application Gateway are encrypted. Select **None**.
Fault Tolerance	Specify the fault-tolerance strategy that the Application Gateway uses.
Connection	Select **Duplex**.
Description	Any additional information about the Unified ICM Application Gateway.

Step 6 Save your changes to create the Unified ICM Application Gateway.

Note Copy down the Unified ICM Application Gateway ID value. You use the ID when you set up the INCRP NIC on the target instance.

Step 7 Select either of the **Connection** tabs to set the connection information.

Step 8 Click **Enter Address**.
The **Enter Contact Director Address** dialog appears.

Step 9 Specify the following information:

Field	Description
IP Address/Name	Enter the Public (high priority) IP address of the target instance. Alternatively, You can use the SAN with assistance from your Cisco certified partner or TAC. Use the *same address* that you specified for the INCRP NIC on the target instance. You can use the hostname in place of the address.
Instance Number	Enter the number of the customer ICM on the target instance (0 — 24).
Side	Indicate which side of the Contact Director prefers this connection: • **Side A**—Contact Director Side A prefers to use this connection. • **Side B**—Contact Director Side B prefers to use this connection. • **None**—Neither side of the Contact Director prefers to use this connection. • **Both Side A and B**—Both sides of the Contact Director prefer to use this connection. **Note** Use this setting to avoid unnecessary WAN traffic. For example, if you collocate Contact Director Side A with target instance Side A, this correct choice avoids WAN traffic to the other side.

Note The **Enter Contact Director Address** dialog displays different fields depending on the type of Application Gateway chosen.

Step 10 Repeat this process for the other side of the redundant pair.

Step 11 Save your work and exit the dialog.

Create an INCRP on Each Target Instance

The Contact Director communicates with the target instance by an INCRP NIC. Perform this procedure on each target instance.

Procedure

Step 1 From the Configuration Manager menu on the target instance, select **Tools > Explorer Tools > NIC Explorer**. The **NIC Explorer** window appears.

Step 2 In the **Select Filter Data** box, click **Retrieve**.

Step 3 Select a NIC or click the **Add NIC** button to create a new NIC.

Step 4 Specify the following values on the **Logical Interface Controller** tab:

Field	Description
Name	An enterprise name that serves as the NIC name.
Client Type	Select **INCRP**.

Step 5 Click the **Add Physical Interface Controller** button.
The Physical Interface Controller dialog displays.

Step 6 Specify an **Enterprise Name** and click **OK**.

Step 7 In the NIC tree window, click the routing client for your newly created NIC.

Step 8 Specify the following values on the **Routing Client** tab:

Option	Description
Name	An enterprise name that serves as the Routing Client name.
Configuration Parameters	`/customerID <RCID>` where <RCID> is the Routing Client ID of the matching routing client on the Contact Director.
Network Routing Client	The same value as the **Name** field.

Step 9 Click **Save**.
The newly defined NIC is saved in the database. A **Physical Controller ID** is assigned, and the **To Be Inserted** icon is removed from the tree window.

Set Application Gateway Default Values

If you see performance issues, the Cisco Technical Assistance Center might advise you to change some of the application gateway's default values. Use the following procedure to change these values.

Procedure

Step 1 In the **Configuration Manager**, select **Enterprise** > **System Information** > **System Information**. The **System Information** dialog appears.

Step 2 In the **Application Gateway** section, select **Remote ICM**.

Step 3 Use the other tabs to set the default values for the Unified ICM Application Gateway connections. Take account of the Contact Director NIC settings for timeout, late, and so on as you set the Unified ICM Application Gateway timeout settings for a target Unified CCE system.

Step 4 Click **OK** and close the dialog.

Install Cisco Unified Intelligence Center (Optional)

To run the Contact Sharing reports at the Contact Director site, you can install Cisco Unified Intelligence Center there. For installation procedures, see the *Installation and Upgrade Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html.

Install Unified CVP

The Contact Director uses Unified CVP for VRU processing of the incoming calls. For installation procedures, see the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html.

Note The Unified CCE Reference Designs specify that you use Unified CVP. In a non-Reference Design deployment, you can alternately use Unified IP IVR or a third-party VRU.

Set Up Contact Sharing

After installing the Contact Director and connecting the Contact Director to the target Unified CCE instances, you set up the contact sharing feature as follows:

Task	See this Topic
Set up the contact sharing node on the Contact Director.	Set Up a Contact Sharing Node
Set up the machine inventory for the contact sharing node.	Set up Contact Sharing Machine Inventory

Task	See this Topic
Add contact sharing rules.	Add and Maintain Rules
Add contact sharing groups.	Add and Maintain Groups

Note Your solution can only have one contact sharing node.

Set Up a Contact Sharing Node

You set up a contact sharing node, as opposed to the target instances, with the same procedure for setting up an application gateway.

Procedure

Step 1 In the Configuration Manager, select **Tools** > **List Tools** > **Application Gateway List**. The **Application Gateway List** window appears.

Step 2 To enable **Add**, click **Retrieve**.

Step 3 Click **Add**. The **Attributes** tab appears.

Step 4 Fill out the **Attributes** tab as follows:

Option	Description
Name	Name of your contact sharing node
Type	Contact Share

Note The remaining fields are preset and cannot be modified.

Step 5 On the **Connection Side A** tab, set the **Address** field to the router's IP address. The default port is 5070.

Step 6 On the **Connection Side B** tab, set the **Address** field to the router's IP address. The default port is 5070.

Step 7 Click **Save** to create the contact sharing node.

Set up Contact Sharing Machine Inventory

You set up the machine inventory for contact sharing through the `icm/bin/csMachineInventory.csv` file. Changes to the machine inventory do not take effect until the router restarts.

Procedure

Step 1 Open your machine inventory file for contact sharing, by default `csMachineInventory.csv`.

Step 2 Follow the instructions for editing the `csMachineInventory.csv` file. The instructions are contained within the file.

Step 3 Run the following command:

csMachineInventory.bat *[options] username password inputfile*
options: /list, /help, /config

/list - This option lists the contact sharing machine inventory.

/help - This option displays the usage of the tool.

/config - This option configures the contact sharing machine inventory based on the input file.

username

Username for the REST API request

password

Password for the REST API request.

inputfile

Machine inventory file, including the path, for contact sharing, by default `csMachineInventory.csv`

What to do next

If the router has already started, restart the router after setting up the machine inventory.

Add and Maintain Rules

Note Contact Sharing comes with a default rule that cannot be deleted or modified. The name of this rule is **DefaultRule**.

Procedure

Step 1 Navigate to **CCE Web Administration** > **Feature** > **Contact Share Rules**.

Step 2 Click **New** to open the **New Rule** window, or click an existing rule to open the **Edit Rule** window.

Step 3 Complete the following fields:

Field	Required	Description
Name	Yes	Enter a name using up to 32 alphanumeric characters, periods (.), and underscores (_). The name must start with an alphanumeric character.
Expression	Yes	Enter a formula that the Contact Share server uses to select the skill group or precision queue from a Contact Sharing group for a routing request.
Description	No	Enter up to 255 characters to describe the rule.

Step 4 Click **Save** to return to the List window.

Step 5 To delete a rule, do one of the following:

- To delete a single rule, hover over the row for that rule and click the **trash can** icon at the end of the row.
- To delete up to 50 rules, check the check box for each rule that you want to delete. To select all rules in a list, check the **Select All** check box in the list header. Click **Delete**.

Deleting a rule is permanent.

Add a New Rule by Copying an Existing Rule

You can also create a new rule by copying an existing rule. The **Description** and **Expression** fields are copied to the new rule.

Procedure

Step 1 Navigate to **Unified CCE Administration** > **Feature** > **Contact Share Rules**.

Step 2 Either:

- Click the rule you want to copy, and then click the **Copy** button in the **Edit Rule** window.
- Hover over the row for that rule, and click the **copy** icon that appears at the end of the row.

The **New Rule** window opens.

Step 3 Enter a **Name** for the rule, using up to 32 alphanumeric characters, periods (.), and underscores (_). The name must start with an alphanumeric character.

Step 4 Review **Description** and **Expression** fields that were copied from the original rule, and make any necessary changes.

Step 5 Click **Save**.

Add and Maintain Groups

Before you begin

Ensure that the Live Data connection is active before you configure Groups.

Procedure

Step 1 Navigate to **CCE Web Administration** > **Feature** > **Contact Share Groups**.

Step 2 Click **New** to open the **New Group** window, or click an existing group to open the **Edit Group** window.

Step 3 Complete the following fields:

Field	Required	Description

Name	Yes	Enter a name using up to 32 alphanumeric characters, periods (.), and underscores (_). The name must start with an alphanumeric character.
Description	No	Enter up to 255 characters to describe the group.
Rule	Yes	Select a rule that defines the logic for selecting a skill group or precision queue in this group for a routing request: **a.** Click the **magnifying glass** icon to display the **Select Rule** window. **b.** Click the row to select a rule.
Accept Queue If	No	Enter a logical expression to determine if the individual skill groups and precision queues in the group can be included in the routing decision.

Step 4 Complete the Queues tab:

This tab shows the list of queues for this group.

a) Click **Add** to open **Add Queues**.
b) Click the queues you want to add to this group. The queues you chose appear on the **List of Queues**.
c) Close **Add Queues**.
d) Click **Save** on this tab to return to the List window.

Note The maximum number of queues is 100.

Step 5 To delete a group, do one of the following:

- To delete a single group, hover over the row for that group and click the **trash can** icon at the end of the row.
- To select all groups in a list, check the **Select All** check box in the list header. Click **Delete**.

Deleting a group is permanent.

Related Topics

About Contact Sharing Expression Formula, on page 48

Scripting for Contact Sharing

Expression Formula for Contact Sharing

About Contact Sharing Expression Formula

You can enter expressions for the following fields:

Field	Description
Accept Queue If for a group	A logical expression to determine whether to include the individual skill groups or precision queues in the Contact Sharing group in the routing decision. The field is a freeform editor with a maximum length of 512 characters. Any result except zero evaluates as TRUE. There is an implicit **Accept Queue If** of `Queue.*.LoggedOn > 0`. You cannot override this implicit check.
Expression for a rule	A formula that the Contact Share server uses to calculate the value to be considered against other queues in a Contact Sharing group. The expression always selects the queue with the minimum value. The field is a freeform editor with a maximum length of 512 characters.

Contact Sharing Expression Format

To evaluate all the skill groups and precision queues in a Contact Sharing group, use this syntax:

```
Queue.*.<FieldName>
```

Where *FieldName* is the name of the field that the expression evaluates, for example, `Ready`.

To evaluate a specific skill group or precision queue, use this syntax:

```
<ObjectType>.<InstanceName>/<TargetQueueName>.<FieldName>
```

- *ObjectType* must be SkillGroup or PrecisionQueue.
- *InstanceName* is the application gateway name.
- *TargetQueueName* is the enterprise name of the skill group or precision queue in the target system.
- *FieldName* is the name of the field that the expression evaluates.

Contact Sharing Expression Examples

The following examples demonstrate some basic Contact Sharing expressions.

Expression for a Group

A Contact Sharing group can take an Accept Queue If expression. The expression determines whether to include specific skill groups and precision queues in the group in the routing decision.

```
Queue.*.Avail > 5
```

This expression accepts all queues with more than five agents that are available.

Expression for a Skill Group

```
SkillGroup.<InstanceName>/<TargetQueueName>.Avail > 5
```

This expression accepts the named skill group if it has more than five agents available.

Expression for a Precision Queue

```
PrecisionQueue.<InstanceName>/<TargetQueueName>.Avail > 5
```

This expression accepts the named precision queue if it has more than five agents available.

Expression for a Rule

A rule must take an expression. The expression selects a skill group or precision queue from a Contact Sharing group.

```
-1 * (Queue.*.Avail)
```

This expression selects the queue with the most available agents.

Expression for MED Only

This expression calculates the Minimum Expected Delay (MED) to determine which target system receives the call for routing.

```
(Queue.*.QueuedNow+1)*(Queue.*.AvgHandledCallsTimeToInterval>0?
Queue.*.AvgHandledCallsTimeToInterval: 120) / (Queue.*.Ready>0?Queue.*.Ready:1)
```

The Default Rule

Contact Sharing comes with a default rule. You cannot modify or delete the default rule. The default rule combines a MED calculation with an Agent Occupancy calculation to determine which target system receives the call for routing.

If there are calls in queue,

```
Queue.*.QueuedNow > 0?
```

Then use the MED calculation:

```
((Queue.*.QueuedNow+1)*(Queue.*.AvgHandledCallsTimeToInterval>0?
 Queue.*.AvgHandledCallsTimeToInterval: 120)/(Queue.*.Ready>0?Queue.*.Ready:1)):
```

Otherwise, use the Agent Occupancy calculation:

```
(((Queue.*.LoggedOnTimeToInterval - Queue.*.NotReadyTimeToInterval)==0
||(Queue.*.AvailTimeToInterval <= 10 * Queue.*.XAvail) )?
0: -1*(Queue.*.AvailTimeToInterval-10 * Queue.*.XAvail)/
(Queue.*.LoggedOnTimeToInterval - Queue.*.NotReadyTimeToInterval))
```

This expression chooses a queue on the target instance with the least occupied agents or the least queued calls.

Note The default rule is only an example. Customize the rule to match your needs or write your own rules.

Contact Sharing Expression Reference

Supported Operations

The following table lists the supported operations:

Type of Operation	Operator	Description
Conditional	&&	Conditional-AND
	||	Conditional-OR
	? :	Ternary (shorthand for if-then-else statement) ex. A **?** B **:** C If A, then B, otherwise C.
Relational	==	Equal to
	!=	Not equal to
	>	Greater than
	>=	Greater than or equal to
	<	Less than
	<=	Less than or equal to
Bitwise and Bit Shift	~	Unary bitwise complement
	<<	Signed left shift
	>>	Signed right shift
	&	Bitwise AND, for strings, also used for string concatenation
	^	Bitwise exclusive OR
	|	Bitwise inclusive OR
Arithmetic	+	Addition
	-	Subtraction
	*	Multiplication
	/	Division
	%	Percentage
Prefix	+	Unary plus operator; indicates positive value
	-	Unary minus operator; negates an expression
	!	Logical complement operator; inverts the value of a boolean

Type of Operation	Operator	Description
Wildcard	*	Wildcard support similar to the expression used in router. For example, in `SkillGroup.*.Ready`, the actual target replaces the asterisk when applying the expression.

Supported Objects and Fields

The following table lists the fields available from the Live Data feed or calculated by Contact Sharing for use in Contact Sharing expressions:

Field Name	Description
ApplicationAvailable	The number of agents belonging to this Queue who are currently ApplicationAvailable for the MRD to which the Queue belongs. An agent is Application available if the agent is Not Routable and Available for the MRD.
Avail	The extrapolated number of agents in the READY state for this Queue. The extrapolation is as follows: (The number of agents that Live Data reports in READY state) - XAvail If the extrapolation results in a negative number, Contact Sharing sets this field to zero.
AvailTimeToInterval	Total seconds agents in the Queue have been in the READY state during the current interval.
AvgHandledCallsTimeToInterval	Average handle time in seconds for calls counted as handled by the Queue during the interval.
BusyOther	Number of agents currently in the BusyOther state for this Queue.
CallsHandledToInterval	Calls that by been answered and have completed wrap-up by the Queue during the interval.
Hold	The number of agents that have all active calls on hold.
ICMAvailable	The number of agents belonging to this Queue who are currently ICMAvailable for the MRD to which the Queue belongs. An agent is ICM available if the agent is Routable and Available for the MRD.
LoggedOn	Number of agents that are currently logged on to the Queue.
LoggedOnTimeToInterval	Total time, in seconds, agents were logged on to the Queue during the current interval.
NotReady	Number of agents in the Not Ready state for the Queue.
NotReadyTimeToInterval	Total seconds agents in the Queue have been in the Not Ready state during the interval.

Field Name	Description
QueuedNow	The extrapolated number of calls currently queued to this Queue. The extrapolation is as follows: (The number of calls that Live Data reports queued to the Queue) + XQueuedNow
Ready	The number of agents who are Routable for the MRD associated with this Queue, and whose state for this Queue is not currently NOT_READY or WORK_NOT_READY.
ReseveredAgents	The number of agents for the Queue currently in the Reserved state.
TalkingAutoOut	The number of agents in the Queue currently talking on AutoOut (predictive) calls.
TalkingIn	The number of agents in the Queue currently talking on inbound calls.
TalkingOther	The number of agents in the Queue currently talking on internal calls, rather than inbound or outbound calls. Examples of other calls include agent-to-agent transfers and supervisor calls.
TalkingOut	The number of agents in the Queue currently talking on outbound calls.
TalkingPreview	The number of agents in the Queue currently talking on outbound Preview calls.
TalkingReserve	The number of agents in the Queue currently talking on agent reservation calls.
WorkNotReady	The number of agents in the Queue in the Work Not Ready state.
WorkReady	The number of agents in the Queue in the Work Ready state.
XAvail	The number of Contact Sharing requests assigned to the available agent count for this Queue during the extrapolation period. The extrapolation period defaults to 10 seconds. Contact Sharing request increments this field when QueuedNow = 0 and Avail > 0.
XQueuedNow	The number of Contact Sharing requests assigned to the queued call count for this Queue during the extrapolation period. The extrapolation period defaults to 10 seconds. Contact Sharing request increments this field when one of the following conditions apply: • QueuedNow = 0 and Avail = 0 • QueuedNow > 0 and Avail = 0 • QueuedNow > 0 and Avail > 0

The following table lists the Call Variables that are available for use in Contact Sharing expressions:

Call Variable Name	Description
CallerEnteredDigits	Digits caller entered in response to prompts.
CallingLineID	Billing phone number of the caller. (Commonly referred to as CLID).
CustomerProvidedDigits	Digits to be passed to the call recipient.
DialedNumberString	Phone number dialed by the caller.
PeripheralVariable1 through 10	Value passed to and from the peripheral.
RouterCallDay	An encoded value that indicates the date on which the software processes the call.
RouterCallKey	A value that is unique among all calls the software has processed since midnight. RouterCallDay and RouterCallKey combine to form a unique call identifier.
RoutingClient	Name of the routing client making the route request.

Routing and Scripting for Contact Sharing

Contact Sharing uses two non-persistent call variables, `Call.ContactShareStatus` and `Call.ContactShareTarget`.

A successful route request returns `Call.ContactShareStatus` populated with the application gateway selected to receive the call. Use the call variable to route the call to the target Unified CCE instance.

`Call.ContactShareTarget` is populated only when the Gateway node takes a success path. The variable contains the target queue type and the target queue id. The target queue id is the Skill Group ID or Precision Queue ID on the target instance. The format is "Target Type, Target Queue ID". For example, "SG,5000 or PQ,5005". You can pass this data to the target instance in a call or ECC variable. Then, you have the Contact Sharing result available to use in scripting on the target instance.

Error Handling for Contact Sharing

If a Contact Share route request fails, the router populates `Call.ContactShareStatus` with the following error codes. The call flow takes the failure branch out of the Gateway node. The error codes appear in the RCD table.

Status Variable	Description
CS_NOT_CONNECTED (2)	No connection to the contact share process.
CS_TIMED_OUT (3)	Request to the contact share process failed.
CS_CONFIG_ERROR (4)	Contact share process encountered a configuration related error.
CS_EXECUTION_ERROR (5)	Contact share process encountered an expression execution related error.

Status Variable	Description
CS_APPGTW_ERROR (8)	Unable to lookup the application gateway with the code that the contact share process returned.
CS_UNKNOWN_ERROR (9)	Contact sharing encountered an unknown error.

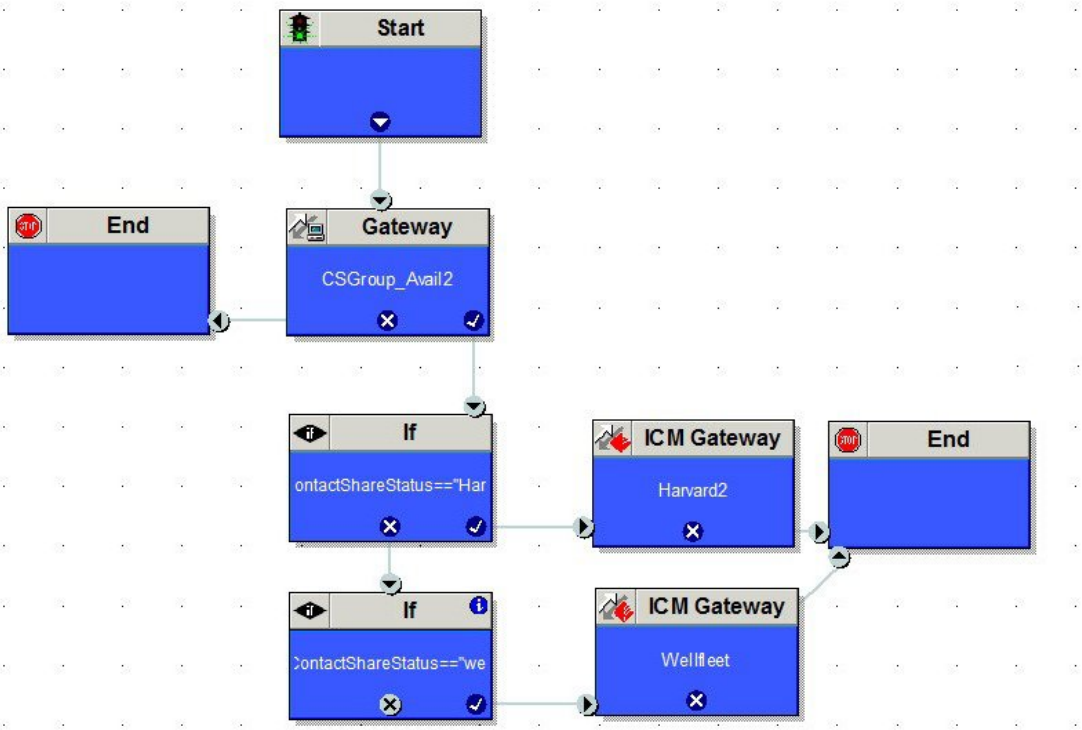
The following error messages can also appear:

Status Variable	Description
ERROR_CONTACT_SHARE_GROUP_NOT_FOUND (1)	The Contact Share Group with the listed ID was not found.
ERROR_CONTACT_SHARE_RULE_NOT_FOUND (2)	The Contact Share Rule with the listed ID was not found.
ERROR_CONTACT_SHARE_RULE_EXPRESSION_INVALID (3)	The Contact Share Rule has an invalid rule expression.
ERROR_CONTACT_SHARE_GROUP_CONSIDERIF_EXPRESSION_INVALID (4)	The Contact Share Rule has an invalid AcceptQueueIf expression.
ERROR_CONTACT_SHARE_GROUP_NO_QUEUE_CONFIGURED (5)	There are no queues configured for the Contact Share Group.
ERROR_CONTACT_SHARE_ROUTING_EXCEPTION (6)	The route request failed for an unspecified reason.
ERROR_CONTACT_SHARE_ROUTING_NO_ELIGIBLE_TARGET (7)	No eligible queue was found for the route request.
ERROR_CONTACT_SHARE_ROUTING_TARGET_CONGESTED (8)	No eligible queue was found for the route request because of congestion control.

Other Scripting Considerations

A simple Contact Sharing script looks like the following:

Figure 8: Sample Contact Sharing Script



Consider the following points when you create Contact Sharing scripts:

- Always double check the logic in the routing to the Contact Sharing node.

Tip If you see all calls routing to one target system, check the IP Addresses in the machine inventory table and your script. The relationship between the Application Gateway ID and the IP Addresses might be wrong.

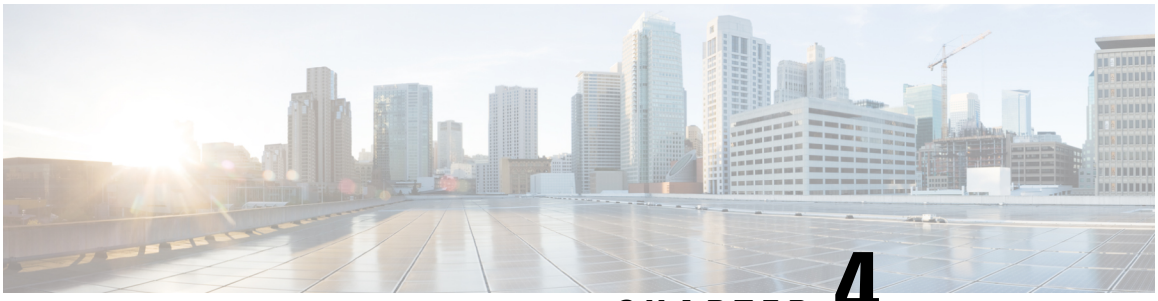
- Use Call Tracer to test your call flows.
- Never put two Contact Sharing nodes in the same path of your script.
- To search for a particular Contact Sharing node, use the string selection type to search for the Contact Sharing Group name.
- Contact Sharing returns the current Application Gateway name, not the ID. If you change the Application Gateway name for one of your target systems, change your scripts to match the new name.

Script with Extrapolation in Mind

Contact Sharing's extrapolation assumes that the target systems route calls within the same Contact Sharing Group that the Contact Director used. If the target system's router does not follow this assumption, Contact Sharing's extrapolated data gets out of sync.

For Contact Sharing, have the target system route by one of the following methods:

- Route to the skill group or precision queue specified in `Call.ContactShareTarget`. You can pass the value from the Contact Director to the target system in a call or ECC variable.
- Route only among the same skill groups and precision queues that are part of the Contact Sharing Group that the Contact Director used.



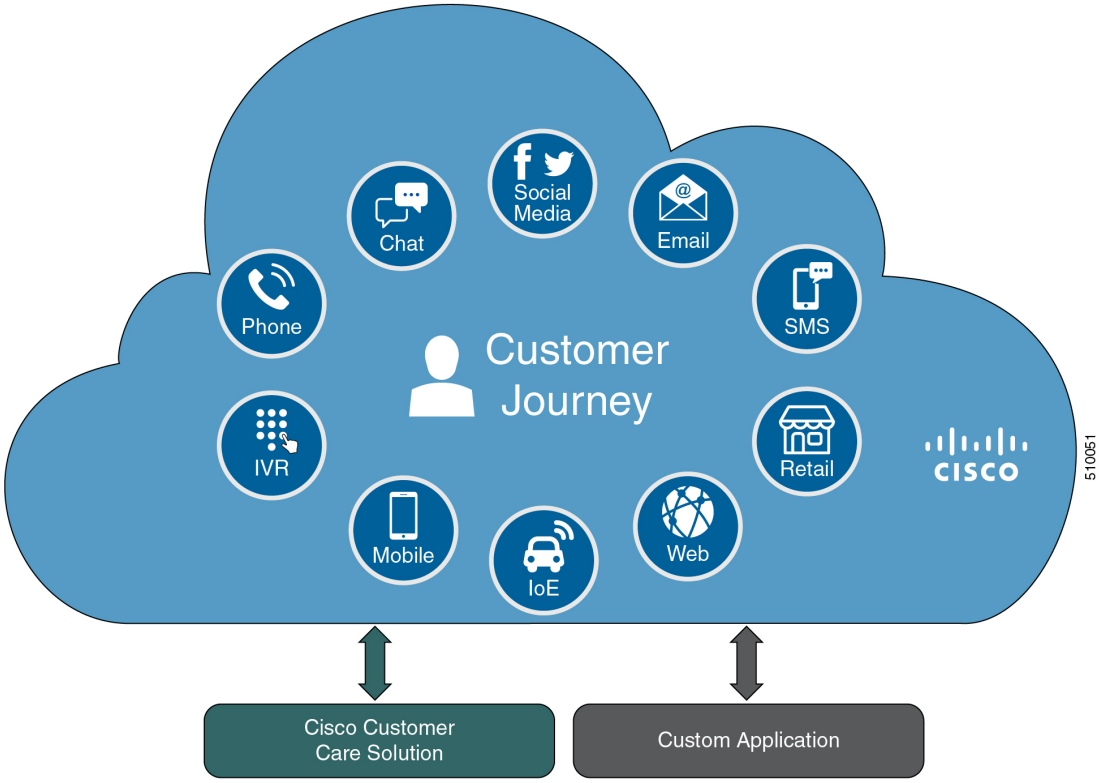
CHAPTER 4

Context Service

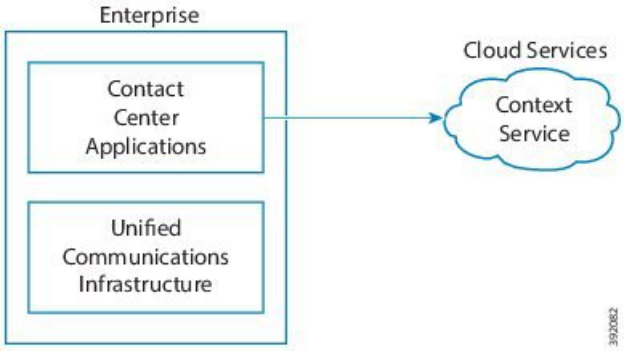
Context Service

Cisco Context Service is a cloud-based, omnichannel solution. Context Service captures customer interaction history and provides flexible storage of the customer interaction data across all channels (including voice, chat, email, and Internet of Things).

Context Service



Context Service provides an out-of-the-box integration with Unified Contact Center Enterprise. You do not need to install any additional components. With Context Service integrated with your contact center, agents can access a customer's previous interactions with your organization. Context Service provides this information to your agents through the Customer Context gadget in the Cisco Finesse desktop.



Context Service provides a flexible data store for storing customer interaction data. You can define what data you want to store and how to store it. Cisco hosts and manages the service, eliminating the need for your organization to deploy and manage servers. Your organization owns the data, even though it's stored in the cloud. Your organization controls access to sensitive data. Cisco partners cannot access protected data unless you grant them access.

The Context Service object stores context data:

- Customer data—Describes who the customer is and includes information such as name, address, and phone number. A Customer provides a way to link personally identifiable information (PII) with a

customer ID. It can link to an existing data store that contains your customer data with key fields, such as name or account number, stored in Context Service. The agent's desktop displays these details in the Customer Context gadget.

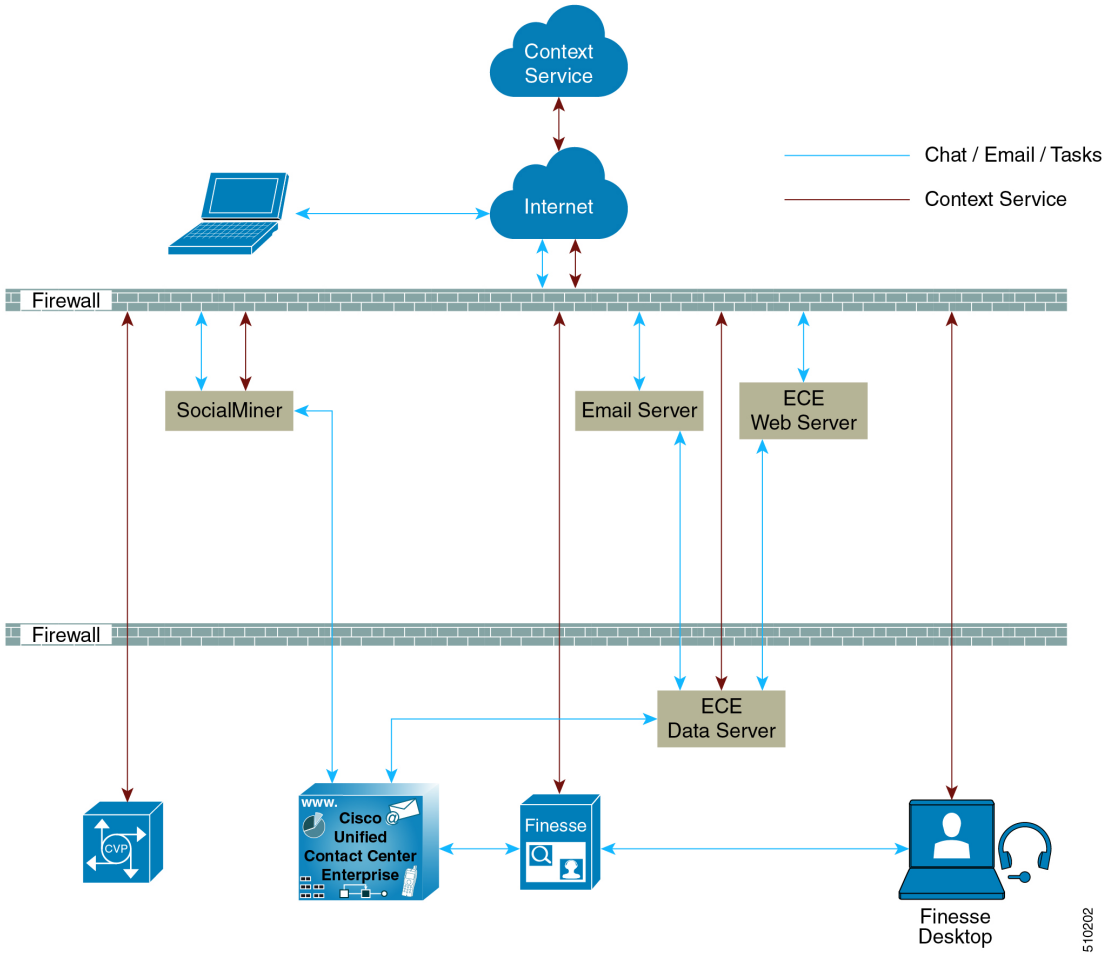
- Activity—Describes a specific interaction associated with a customer or request. An activity reflects one or more steps in the customer journey. Activities tie together all objects within a particular customer journey. For example:
  - VRU menu that a customer selects.
  - Notes made by the agent.
  - A website URL that the customer visited.
  - Chat metadata.
- Request data—Describes what the customer wants. Requests are about one or more customer interactions for a specific issue. The request reflects the customer's view of an issue, indexes the customer journey and interaction, and groups related requests together. For example, a customer goes online to make a credit card payment and runs into an issue. The customer decides to call to make the payment instead. The separate requests represent the two interactions but belong to the same request (making a credit card payment).

The following contact center components integrate with Context Service:

- Cisco Unified CVP—Looks up customer and creates or updates activities for every voice call.
- Cisco Enterprise Chat and Email—Creates activities for every nonvoice chat and email task.
- Cisco SocialMiner—Creates customer records for every Task Routing task.
- Cisco Finesse—Contains the Customer Context gadget where agents can view and update customers and activities for the tasks that they handle.

For more information about Context Service, see Cisco Context Service Help Central at https://help.webex.com/community/context-service.

Design Considerations



Omnichannel Customer Journey

The omnichannel customer journey captures and displays a customer's complete interaction history.

A customer purchases a motorcycle from a company (Cumulus Motorcycle). The customer now has a problem with the motorcycle, so he needs to schedule an appointment with Cumulus Motorcycle for repair. The customer browses the Cumulus web site to locate the nearest service center and chats with a Cumulus agent to determine if the service center that he selected is open on Sundays. In the chat, he tells the agent that he will call when he is ready to schedule an appointment.

The customer calls to schedule a service appointment. The VRU detects his chat and sends his call to a Cumulus Motorcycle agent who is context aware. The customer agrees on a date for service. The agent confirms the appointment, and sends the appointment details to the customer. When the customer realizes that he has a conflict with the appointment, he sends the SMS a new proposed date. The agent receives a screen pop with the customer's proposed date. The agent sends the customer the details for the new appointment. The customer

brings his motorcycle into Cumulus Motorcycle for the scheduled service appointment, then picks up his repaired motorcycle.

Table 5: Components that enable the omnichannel customer journey

Activity	Components
The motorcycle dashboard indicates an error, and instructs the customer to contact Cumulus Motorcycle Customer Service immediately.	The motorcycle sends diagnostic metadata to the Cumulus data center which is connected to Context Service.
The customer browses the Cumulus website to locate the nearest service center. He clicks the **Schedule Service Appointment** link to view the Cumulus Service Centers located near him. The customer views the nearest Cumulus Service Center and clicks the link to chat with a Cumulus agent.	Enterprise Chat and Email Finesse The Cumulus backend server sends the IoT event data and creates an activity to show the current breadcrumbs in Context Service.
The customer calls to schedule a service appointment. The VRU detects his chat and sends his call to an agent.	SMS Unified CVP Finesse Other components
The customer receives the appointment details.	SMS
The customer has a conflict with the scheduled date. The customer proposes a new date. The agent receives a screen pop with the customer's new date.	SMS Finesse
The customer receives a SMS confirmation with the new date.	SMS (for example, Tropo).
The customer picks up his repaired motorcycle.	

Task Flow to Enable Context Service

To enable Context Service in your contact center solution, follow this task flow:

Sequence	Task
Enable Context Service	
1	Work with your Cisco account partner to onboard your organization: Enable Context Service for Your Organization, on page 65
Configure and Register Components	
2	Register your Unified CVP Call Servers: Register Unified CVP with Context Service, on page 67.

Sequence	Task
3	Configure connection data in CVP Call Studio: Configure Context Service Connection Data in Call Studio, on page 69.
4	Register your Cisco Finesse Servers: Register Cisco Finesse with Context Service, on page 69.
5	Set the principal Administration & Data Server: Set the Principal AW for Context Service, on page 70.
6	Register Unified CCE Administration to support SocialMiner and ECE servers: Register Unified CCE Administration to Support Components, on page 71.
7	Enable the POD.ID expanded call variable: Enable the POD.ID Expanded Call Variable, on page 72.
Create scripts	
8	Add Context Service to your CVP scripts: https://developer.cisco.com/site/context-service/index.gsp.

Context Service Setup

Context Service Prerequisites

Complete the following tasks before you enable Context Service.

- Install and configure your contact center solution and any components that you plan to integrate with Context Service (Unified CVP, SocialMiner, ECE, and Cisco Finesse).
- Ensure that port 443 (HTTPS) is available for Context Service to use.
- Add the following URLs to your allowed list in your firewall so that your contact center components can connect to, and receive data from, the internet:
  - `*.webex.com`
  - `*.wbx2.com`
  - `*.ciscoccservice.com`

Note You must use wildcard URLs in your allowed list because Context Service is accessed through multiple subdomains. Context Service subdomain names can dynamically change.

- If Context Service uses a proxy server, configure the browser proxy with the URL specified in the Context Service Management gadget.

Enable Context Service for Your Organization

Context Service enables you to store and access customer interaction data in the cloud, creating a flexible and seamless omnichannel customer journey experience. To use Context Service:

- Work with your Cisco account partner to enable Context Service for your organization.
- Register Context Service for your organization to use with your contact center application.
- Connect your contact center application to Context Service.

Note You need Java Runtime Environment (JRE) version to 1.8.0_151 or later to use Context Service. Refer to the Compatibility Information for your specific release and update accordingly.

Create a Customer Organization and Enable Context Service

Your Cisco account partner can provide Context Service entitlement to your Cisco Webex Control Hub account.

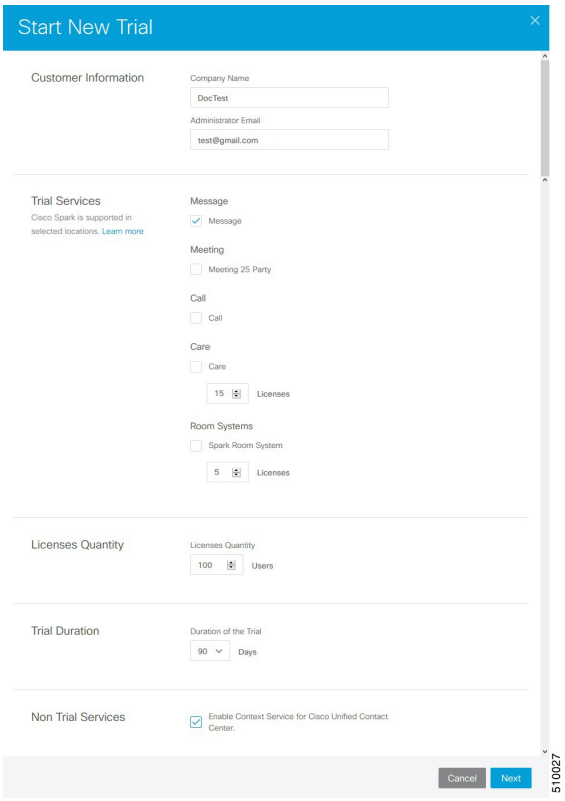
This example shows how a partner adds a Context Service subscription to a customer organization. The example assumes that:

- The partner is a full administrator or sales administrator and can add trials.
- The Cisco Webex Control Hub account or the organization and accounts associated with the organization have been created.

Example: Add a Trial Service

Context Service is not tied to the trial services, and does not expire when the trial period is complete.

1. Log in with your partner credentials to the Cisco Webex Control Hub.
2. Click **Start Trial** on the Overview page. The **Start New Trial** window opens.



3. Enter details about the trial:
   - **Customer Information:** Enter the name of the customer company and an email for the administrator.
   - **Trial Services:** Select the trials to add to this customer. To enable Context, select **Message**.
   - **Licenses Quantity:** Specify the number of licenses required for this customer trial. This number is usually the number of users who use this service. This option applies only to the Trial Services. Context Service is not bound by the number of licenses specified here.
   - **Trial duration** Specify the duration the trial lasts before you must purchase the service. This option applies only to the Trial Services and not Context Service.

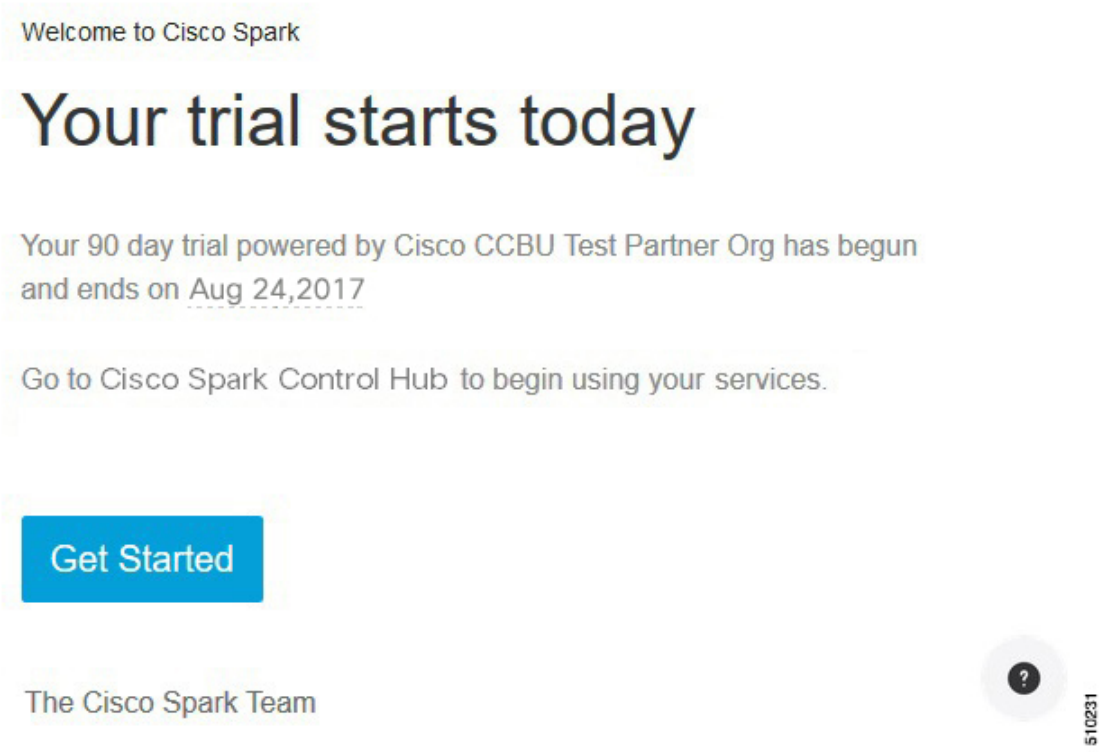
Note Context Service entitlement does not expire when the specified trial period ends. The organization can continue to use Context Service beyond the date of the specified Trial Duration.

Note You cannot change the customer name and administrator email after you create the trial. You can modify the other terms of the trial as needed.

Make sure that the email you provide is not already associated with a Cisco Webex Control Hub account.

4. Scroll down to the **Non Trial Services** section and select **Enable Context Service for Cisco Unified Contact Center**.
5. Click **Next**.
6. A message is displayed that asks if you want to set up the services for the customer. Click **No**.

You now have provided Context Service entitlement to the organization. The customer now receives a welcome email at the specified email address with the subject line **Welcome to Cisco Spark Service**.



The customer must click **Get Started** in the email and sign in to Cisco Webex Control Hub to begin their trial. The customer uses the credentials in the email to sign in and is prompted to create a password.

Your Cisco Context Service is ready. To use the service, connect to Cisco Contact Center with Context Service Enabled. See Register Context Service for more information.

Component Configuration and Registration

Register Unified CVP with Context Service

The registration process has an inactivity session timeout of 10 minutes. If the session times out, sign in again.

Note For Unified CVP, Context Service is not supported for a VXML Server that is deployed in a standalone mode.

Before you begin

- Ensure that Unified CVP 11.6 is installed.
- Ensure that your web browser allows popups.
- If you are using Microsoft Internet Explorer, add a registry key, `TabProcGrowth`, at `HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main`. Set the type to **`String`** or **`DWORD`** (32-bit) and set the value to **`0`**.
- When your organization was entitled for Cisco Context Service, you received an email requesting a sign-in and a password change. Sign in using the registration email, and change the password. Now your organization is entitled to use Context Service.

Procedure

Step 1 In the **CVP Operations Console**, choose **System** > **Cloud Services** > **Context Service** to launch the **Context Service Management** page.

Step 2 Provide the following information for the CVP VXML server:

- **Proxy server URL**—Specify the URL if your solution uses an optional proxy server to reach Context Service.
- **Timeout**—The amount of time, in milliseconds, that the system waits for a response from Context Service for each operation.

  See the application's online help for the minimum, maximum, and default values for this setting for the component you are registering. Test this setting and tune it to match the latency for your solution.
- **Lab Mode**—Indicates whether Context Service is in lab mode. In lab mode, you can test, develop, and debug Context Service. Lab mode allows you to delete objects from Context Service.

Step 3 Click **Register**.

A popup window appears in your browser prompting you to sign in to Cisco Spark.

Step 4 Enter your Cisco Webex Control Hub admin credentials and complete the registration. (See https://help.webex.com/docs/DOC-4165 for more information.)

Note Use the same organization admin account to register all components in one contact center solution.

Step 5 Check the **Allow Access to Your Hybrid Services Node** check box and then click **Continue**.

Cisco Webex Control Hub redirects the browser back to the application from which you began the registration.

If the registration is successful, the connection details are deployed on all running VXML Servers in the pool. If you add a VXML Server after registration, click **Save & Deploy** on the **VXML server device configuration** page to deploy the connection data to the new server.

Configure Context Service Connection Data in Call Studio

You can configure Context Service connection data property to debug applications that interact with Context Service.

To debug a solution that uses Context Service, Call Studio requires your Context Service credentials and connection details.

Before you begin

Register Unified CVP with Context Service by using the Operations Console.

Procedure

Step 1 From the Operations Console, select **System** > **Cloud Services** > **Context Service**.

Step 2 Click **Connection Data**.

The system displays the credential information in the Connection Data area below the **Connection Data** button. The connection data is selected by default.

Note Carefully store the connection data. This data is the key to open your organization's data in the cloud.

Step 3 Copy the credentials onto the clipboard.

Step 4 Click **OK**.

Step 5 Launch Cisco Unified Call Studio.

Step 6 Choose **Window** > **Preferences**.

Step 7 On the **Preferences** window, choose **Call Studio** > **Debug Preferences**.

Step 8 In the Context Service area, paste the connection data from the clipboard into the **Connection Data** field.

Step 9 Click **OK**.

Step 10 Restart VXML service and Ops Console service.

Register Cisco Finesse with Context Service

Before you begin

- Ensure that your web browser allows popups.
- When your organization was entitled for Cisco Context Service, you received an email requesting a sign-in and a password change. Sign in using the registration email, and change the password. Now your organization is entitled to use Context Service.
- If you wish to configure a proxy server for Context Service, configure the browser proxy with the proxy server URL you specified. Refer to your browser’s documentation for information about configuring proxy settings.

Procedure

Step 1 Register Cisco Finesse with Context Service from the Finesse administration console **Context Service Management** gadget.

Note Ensure to register all Finesse primary nodes.

Step 2 Provide the following information:

- **Proxy server URL**—Specify the URL if your solution uses an optional proxy server to reach Context Service.
- **Timeout**—The amount of time, in milliseconds, that the system waits for a response from Context Service for each operation.

  See the application's online help for the minimum, maximum, and default values for this setting for the component you are registering. Test this setting and tune it to match the latency for your solution.
- **Lab Mode**—Indicate whether Context Service is in lab mode. In lab mode, you can test, develop, and debug Context Service. Lab mode allows you to delete objects from Context Service.

Step 3 Click **Register**.

A popup window appears in your browser prompting you to sign in to Cisco Spark.

Step 4 Enter your Cisco Webex Control Hub admin credentials. Complete the registration in Cisco Webex Control Hub. (See Register Your Applicartion with Context Service for more information.)

Note Use the same organization admin account to register all components in one contact center solution.

Cisco Webex Control Hub redirects the browser back to the application from which you initiated the registration.

What to do next

To change any of the settings after you register, edit the setting and save your change. You do not need to reregister.

After you register Cisco Finesse, agents can use the Context Service desktop gadget. It is available on the **Manage Customer** tab in the default agent desktop layout. If the gadget is not in your layout, you can add the gadget with the following XML:

```
<tab>
            <id>manageCustomer</id>
            <label>finesse.container.tabs.agent.manageCustomerLabel</label>
            <gadgets>
                     <gadget>/desktop/gadgets/CustomerContext.xml</gadget>
            </gadgets>
      </tab>
```

Set the Principal AW for Context Service

Set which Administration & Data Server (AW) manages the credentials for Context Service before registering with Context Service in Unified CCE Administration.

Procedure

Step 1 In **Unified CCE Administration**, navigate to **Infrastructure** > **Inventory**.

Step 2 In the **System Inventory**, click the AW that you want to manage the Cisco Spark Control Hub admin credentials for Context Service.

Step 3 In the **Edit AW** popup window, check the **Principal** check box.

Step 4 Enter your solution's **Diagnostic Framework** credentials.

Step 5 Click **Save**.

Register Unified CCE Administration to Support Components

You register Unified CCE through the Unified CCE Administration tool. This enables SocialMiner and Enterprise Chat and Email to access Context Service in a single operation.

Note Before you register with Context Service through Unified CCE Administration, upgrade the JRE on your primary AW to version 1.8.0_151 or higher. For information on upgrading JRE, see the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide.

Before you begin

- Use the **System Inventory** in **Unified CCE Administration** to set the Principal AW before registering Unified CCE. The Principal AW manages the Context Service credentials.
- When your organization was entitled for Cisco Context Service, you received an email requesting a sign-in and a password change. Sign in using the registration email, and change the password. Now your organization is entitled to use Context Service.

Procedure

Step 1 Register from the Unified CCE Administration **System** > **Feature** > **Context Service** menu.

Step 2 Provide the following information:

- **Proxy server URL**—Specify the URL if your solution uses an optional proxy server to reach Context Service.
- **Timeout**—The amount of time, in milliseconds, that the system waits for a response from Context Service for each operation.

  See the application's online help for the minimum, maximum, and default values for this setting for the component you are registering. Test this setting and tune it to match the latency for your solution.
- **Lab Mode**—Indicate whether Context Service is in lab mode. In lab mode, you can test, develop, and debug Context Service. Lab mode allows you to delete objects from Context Service.

Step 3 Click **Register**.

Your browser displays the Cisco Spark sign-in page.

Step 4 Enter your Cisco Webex Control Hub admin credentials. Complete the registration in Cisco Webex Control Hub. (See Register Your Application with Context Service for more information.)

Note Use the same organization admin account to register all components in one contact center solution.

Cisco Webex Control Hub redirects the browser back to the application from which you initiated the registration.

What to do next

Set up the ECE services in the System Console. For more information, see the *Enterprise Chat and Email Deployment and Maintenance Guide (for Unified Contact Center Enterprise)* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-maintenance-guides-list.html .

Configure Context Service in ECE. For more information, see the *Enterprise Chat and Email Administrator's Guide to System Console* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-maintenance-guides-list.html.

If you register CCE Context Service after it is deregistered, restart the ECE Context Service Process and Instance from the ECE System Console Page. To set up ECE services in the System Console, see the *Enterprise Chat and Email Deployment and Maintenance Guide (for Unified Contact Center Enterprise)* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-maintenance-guides-list.html.

Enable the POD.ID Expanded Call Variable

Enable the built-in POD.ID expanded call variable to send task context data through the system.

Note For a new incoming call, CVP creates a new POD and passes that POD information to CCE in *POD.ID ECC Variable* . In order for CVP to send POD.ID ECC variable to CCE, the Call Studio script must contain CVP Subdialog_Start at the beginning of the script with the business logic for creating or updating POD and .must end with *CVP Subdialog_Return. CVP Subdialog_Return* captures the caller input and passes the POD ID to CCE Application.

Procedure

Step 1 In the Configuration Manager, navigate to **Tools** > **List Tools**, and open the **Expanded Call Variable List**.

Step 2 Click **Retrieve**.

Step 3 Click the **POD.ID** expanded call variable to open that record in the **Attributes** panel.

Step 4 Check the **Enabled** check box.

Step 5 Click **Save**.

Solution Serviceability

This section provides the information and resources to troubleshoot Context Service.

You can view service status for Context Service and subscribe to updates at https://status.ciscospark.com.

For Enterprise Chat and Email troubleshooting information, see the *Enterprise Chat and Email Administrator's Guide to System Console* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-maintenance-guides-list.html.

Access Context Service Logs

The log file from Context Service is `CCBU-runtime.<YYYY-MM-DDTHH-MM-SS.sss>.log`.

The path to the log file is `/opt/cisco/mmca/logs/runtime`.

Context Service logs are stored at C:\icm\tomcat\logs\ContextService.*.log on the Principal AW.

CVP OAMP logs are stored at CVP_HOME\logs\OAMP

CVP VXML logs are stored at CVP_HOME\logs\VXML

Fusion Management Connector logs are stored at /opt/cisco/ccbu/logs/fusion-mgmt-connector directory

Cisco Finesse logs are stored at /opt/cisco/desktop/logs/finesse-auth

Cisco SocialMiner logs are stored at /opt/cisco/mmca/logs/runtime

For the location of Enterprise Chat and Email logs, see the *Enterprise Chat and Email Administrator's Guide to System Console* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-maintenance-guides-list.html.

View Context Service Customer Record Statistics on OAMP

You can check Context Service customer record statistics in OAMP from the VXML logs.

Verify the VXML logs for any exceptions. Search the log *$CVP_HOME/logs/VXML* for the instances “Context service client stats summary” - Verify the reachability /connectivity. The report displays the count, latency, etc for each record. In the Dashboard Login to **OAMP** > **System** > **ControlCenter** > **VXML Device's CS status**. Alerts are captured in *syslogServer*.

Troubleshooting Context Service Registration Process

This section lists the issues and the possible solutions during registration of the components with the Context Service Cloud.

Cannot Configure Cisco SocialMiner

You cannot configure Cisco SocialMiner, if Context Service fails to connect with it.

Check the Context service logs at `C:\icm\tomcat\logs\ContextService`. If there are connectivity errors, the Context Service logs provide information similar to this:

```
0000001306: *.*.*.*: Aug 12 2016 16:58:15.629 -0400:
%CCBU_pool-1-thread-35-Infrastructure-1548-3-REST_API_EXCEPTION:

%[exception=com.sun.jersey.api.client.ClientHandlerException:

java.net.SocketTimeoutException: connect timed out][message_string=Failed
to make request. Exception is caught for rest call:GET
https://*.*.*.*:443/ccp-webapp/ccp/contextServiceConfig]: The REST API
has caught an exception
```

To fix the issue, check to see if Cisco SocialMiner is up and running. If Cisco SocialMiner is up and running, check its connection with the principal AW Machine.

If your issue is still unresolved, contact Cisco customer support.

Cannot Register Context Service

When you try to register with Context Service, if registration fails with the following error, check to see if you have an internet connection.

```
Failed to register with the Context Service because of a connection error.
Verify that the server has internet access and/or the proxy server URL
is correct.
```

If your registration fails due to incorrect proxy server URL, check the proxy server configuration in your browser.

If you are still unable to register, the Context Service SDK could have been corrupted, when an automatic update was run.

To recover the corrupted Context Service SDK:

1. Stop the Cisco Tomcat service.
2. Delete the `C:\icm\ContextService` directory.
3. Restart the Cisco Tomcat service. The Context Service directory is recreated.

If your issue is still unresolved, contact customer support.

Cannot Deregister Context Service

If the AW-HDS-DDS side A can access only the key management system but not the rest of Context Service, registration succeeds. However, deregistration fails because the cluster was not created.

Check the Context Service logs on the Principal AW at: `C:\icm\tomcat\logs\ContextService.*.log`. If the cluster was not created, the SDK logs provide information similar to this:

```
0000000111: *.*.*.*: Aug 12 2016 10:46:59.835 -0400:
%_Thread-25-6-com.cisco.thunderhead.RESTClient: Error on CREATE:
https://hercules-a.wbx2.com/v1/connectors

0000000112: *.*.*.*: Aug 12 2016 10:46:59.835 -0400:
%_Thread-25-3-com.cisco.thunderhead.RESTClient: Error: try #1: Exception
trying to connect=com.sun.jersey.api.client.ClientHandlerException:
org.apache.http.conn.HttpHostConnectException: Connect to
```

```
hercules-a.wbx2.com:443 [hercules-a.wbx2.com/*.*.*.*,
hercules-a.wbx2.com/*.*.*.*] failed: Connection timed out: connect
```

To fix this issue, check to see if your server is up and running.

If you are still unable to deregister, the Context Service SDK could be corrupt.

To recover the corrupted Context Service SDK:

1. Stop the Cisco Tomcat service.
2. Delete the `C:\icm\ContextService` directory.
3. Restart the Cisco Tomcat service.

The Context Service directory is recreated. If the issue is still unresolved, contact Cisco support.

Cannot Register Context Service (Cisco Unified CVP)

Registration Failure

When you try to register with Context Service and if the registration fails, the following error message is displayed:

```
Registration with context Service failed. Try re-registering.
```

The reasons for this error can be the following:

- Dynamic Context Service extension jar failure
- Incorrect login credentials

To successfully register Context Service, follow these steps:

1. Check the network connectivity.
2. Check that the Context Service extension jar dynamically downloads in the following path:

   ```
   CVP_HOME\OPSConsoleServer\Tomcat\webapps\oamp\
   WEB-INF\contextService\context-service-sdk-downloads
   ```
3. If you use a proxy, ensure that the proxy is up and running.
4. Ensure that you use the valid organization account credentials that was used to enable Context Service.
5. Verify the OAMP log *$CVP_HOME/logs/OAMP* and search for instances of

   ```
   CS_SDK_STATUS
   ```
6. Verify the connectivity. In the **OAMP** dashboard, log in to **System** > **ControlCenter** > **OAMP CS status**. Alerts are captured in *syslogServer*.

Unable to Register and Deregister Unified CVP With Context Service

Registration or deregistration of CVP with Context Service fails with this error `Activity Failed/Register/Deregister failed`

This error occurs if there is a network issue. Make sure that your network is available and connected. You also need to check Context service connection status in OAMP and VXML logs. These logs are updated every 30 seconds. You can also find status information in the system logs also.

Verify the OAMP logs for any exceptions. Search the log *$CVP_HOME/logs/OAMP* for instances of "CS_SDK_STATUS" - Verify the reachability /connectivity. In the Dashboard Login to **OAMP** > **System** > **ControlCenter** > **OAMP CS status**. Alerts are captured in *syslogServer*.

Verify the VXML logs for any exceptions. Search the log *$CVP_HOME/logs/VXML* for the instances "CS_SDK_STATUS" - Verify the reachability /connectivity. In the Dashboard Login to **OAMP** > **System** > **ControlCenter** > **VXML Device's CS status**. Alerts are captured in *syslogServer*.

Context Service Registration Incomplete

When registering or de-registering Context Service with Finesse, the process stops responding and continues to display one of the following messages:

```
Registration is in progress
```

OR

```
Deregistration is in progress
```

These messages could occur for the following reasons:

- The proxy is invalid or not reachable. Make sure that the proxy URL is correct and reachable from Finesse.
- The browser pop-up is disabled. Ensure the browser pop-up is enabled.
- The Context Service Cloud services may not be reachable. For more information, see the Fusion Management Connector (FMC) logs located at: `/opt/cisco/ccbu/logs/fusion-mgmt-connector directory.`
- Fusion Management Connector (FMC) is still in the loading state.

Context Service Registration Status Invalid

Registering Context Service with Finesse clients can fail with this error:

```
The Context service registration status is invalid. Check the Settings
and try again.
```

This error could occur for the following reasons:

- An invalid client setting update results in an invalid registration state. To ensure that the update keeps the connector in registered state, perform the following:
  1. Correct the client settings.
  2. Save and refresh the page.

  If the update is unsuccessful, try restarting the Cisco Tomcat service. If the issue still persists, re-register Context Service.
- Connection data is invalid. Restart Cisco Tomcat service. If that doesn't help, contact Cisco Support.

Unable to Determine Context Service Registration Status or Client Settings

Context Service Management displays the following error messages in Cisco Finesse Administration:

- `Unable to determine registration status from system`

- `Error while retrieving Context Service client settings from Database`

These errors occur when the Fusion Management web application, deployed on the Platform Tomcat is down, or the Cisco Tomcat service is down in Cisco Finesse.

When this occurs:

- Verify that the Cisco Tomcat service is up and running. The service may not respond with an XML in some error scenarios.
- Restart Platform Tomcat and try again.
- Check the logs under: `/opt/cisco/ccbu/logs/fusion-mgmt-connector` for more information.

Context Service Registration Incomplete Due to Pop-Up Window

As part of Context Service registration process, a pop-up window is displayed for Cisco Spark login. After the registration is complete, the popup window does not close automatically and the following error message is displayed:

```
Please wait while Finesse completes the Context Service registration.
CAUTION: Do not close this window, otherwise the registration may fail.
This window will close automatically when the registration is complete.
```

When this error message occurs:

Check the registration status in the Finesse Administration page. If the registration is complete, the pop-up window closes automatically.

Note If you are using Firefox, enable the `dom.allow_scripts_to_close_windows config` to ensure that any additional tabs opened for context service registration close as expected.

Context Service Registration Incomplete Due to Page Refresh

As part of Context Service registration process, do not refresh the pop up page while the registration or deregistration process is in progress. This may result in an **Undefined** state for that respective component.

Troubleshooting Context Service Connectivity Process

This section describes the various connectivity related issues that are encountered and the troubleshooting that can be performed for a possible solution.

Activity Operation

`Exception related to Activity operation failure`

Deployment failure, dynamic jar download failure, context service client initialization failure, or incorrect connection data.

Check if the deployment of Context Service related data from OAMP to VXML server is successful from the **Deployment Status** button in OAMP.

- If the deployment failed, in OAMP, select **Device Management** > **Unified CVP XML Server**. Select the failed VXML server and click **Save & Deploy**.
- Ensure that VXML Server status is up.

Check that the Context Service extension jar dynamically downloads in the following path:

CVP_HOME\VXMLServer\Tomcat\webapps\CVP\ WEB-INF\contextservice\context-service-sdk-downloads

- Check the network connectivity.
- If you use a proxy server, make sure that it is working.

Ensure that the Context Service client initialization is successful.

- Restart the VXML Server service.

Verify that the customer ID is valid and exists.

- Create valid customers.

Verify the VXML logs for any exceptions. Search the log *$CVP_HOME/logs/VXML* for the instances "CS_SDK_STATUS" - Verify the reachability /connectivity. In the Dashboard Login to **OAMP** > **System** > **ControlCenter** > **VXML Device's CS status**. Alerts are captured in *syslogServer*.

Context Service Connection Data Not Published

The connection data is published to the configured subscribers in the following scenarios:

- De-registering or cancelling Context Service.
- Registering with Context Service.
- Updating connection data when Context Services sends a notification.

This issue can occur when there is a change in the connection data in the cloud. Also, check for the following log statements in the fusion-management-connector logs at `/opt/cisco/ccbu/logs/fusion-mgmt-connector/`:

- `Error occurred while fetching runtime connector information from DB`
- `There are no runtime connectors registered in system currently`
- `Exception ocurred while fetching connection data`
- `Exception occurred while publishing connection data`

If the issue persists, contact Cisco Support.

Activity Count Mismatch Between CVP and Other Components

This issue can occur if there is a count mismatch between CVP and other components due to a break in network or cloud connectivity. You will get this error message `Activity Failed`.

Check the statistics. Context Service Statistics: Unified CVP fetches the customer record related statistics every 30 minutes and writes in the VXML logs and syslogs. These statistics are flushed out immediately post fetching.

Verify the VXML logs for any exceptions. Search the log *$CVP_HOME/logs/VXML* for the instances "CS_SDK_STATUS" - Verify the reachability /connectivity. In the Dashboard Login to **OAMP** > **System** > **ControlCenter** > **VXML Device's CS status**. Alerts are captured in *syslogServer*.

Activity Failure in Debug Mode

`Error/Exception in VXMLlogs`

Network issue, incorrect connection data

- Verify that the proxy is correct.
- Check if the proxy is working on the web browser.
- Check if the connection data is valid.

Verify the VXML logs for any exceptions. Search the log *$CVP_HOME/logs/VXML* for the instances "CS_SDK_STATUS" - Verify the reachability /connectivity. In the Dashboard Login to **OAMP** > **System** > **ControlCenter** > **VXML Device's CS status**. Alerts are captured in *syslogServer*.

Periodic Logging of Context Service SDK Connector Status

- Context Service status information is logged periodically into the respective log files.
- The periodic interval is 30 minutes, and this is synchronized to the wall clock time. The log should appear at 1100hrs, 1130hrs, 1200hrs and so on.
- The status message lists the overall status, services used by the connector, information on whether it is reachable, latency and so on.
- Fusion Management Connector logs are located at `/opt/cisco/ccbu/logs/fusion-mgmt-connector`
- Finesse Auth logs are located at: `/opt/cisco/desktop/logs/finesse-auth`.

Periodic Logging of Context Service JMX Counters

The JMX statistics information is logged into the logs located at /opt/cisco/desktop/logs/finesse-auth directory" with the text "CS_SDK_STATS_SUMMARY".

Note This statistics information is not logged into the Fusion Management Connector logs.

Troubleshooting Context Service Runtime Process

This section describes the runtime related issues that are encountered during the runtime connection with the Context Service Cloud. The troubleshooting tips and the possible solution for each are presented.

Unable to Access Customer Context Information

In the Cisco Finesse desktop gadget, there may be instances where the customer's context information is not accessible and the following error message is displayed:

`Experiencing issues with accessing customer's context information`

This error message could occur due to the following reasons:

- Invalid client settings. Check and correct the client settings.
- Due to connectivity issues. Check if the Context Service connectivity is accessible from Cisco Finesse.
- Cisco Finesse is not registered with Context Service. Check your Context Service registration. If Context Services is not registered, try again

Deregister a Component with Context Service

After registering a server, you can deregister it if you decide to stop using Context Service with that server.

Before you begin

Ensure that your web browser allows popups.

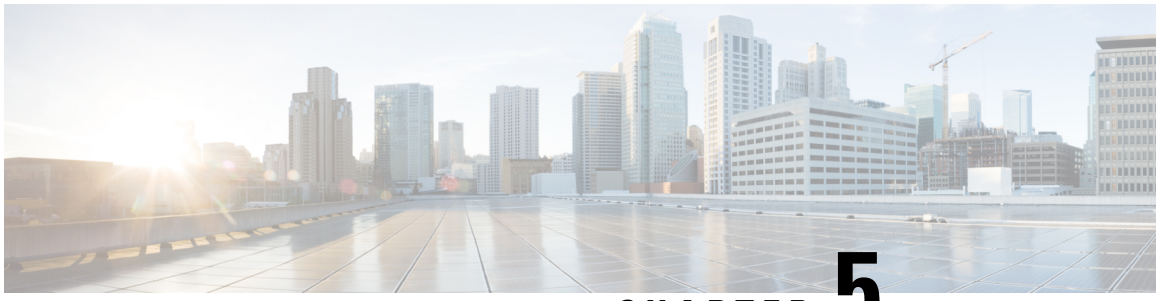
Procedure

Step 1 Launch the **Context Service Management** page for the server.

Step 2 Click **Deregister**.

Your browser displays the Cisco Spark sign-in page.

Step 3 Sign in with your Cisco Webex Control Hub admin credentials and confirm the removal of your Hybrid Services cluster.
You are redirected to the application page for the completion of the deregistration process. The browser window closes automatically after a successful deregistration. Avoid making any changes to the client settings until the deregistration is completed successfully.



CHAPTER 5

Mobile Agent

Capabilities

Cisco Unified Mobile Agent Description

Mobile Agent enables an agent to use any PSTN phone and a broadband VPN connection (for agent desktop communications). The agent has the same capabilities as an agent in your call center using a Cisco IP Phone.

Unified Mobile Agent supports call center agents using phones that your contact center enterprise solution does not directly control. You can deploy a Mobile Agent as follows:

- Outside the contact center, by using an analog phone or a mobile phone in the home.
- On an IP phone connection that is not CTI-controlled by Unified CCE or by an associated Unified Communications Manager.
- On any voice endpoint of any ACD (including endpoints on other Unified Communication Managers) that the contact center Unified Communication Manager can reach by a SIP trunk.

A Mobile Agent can use different phone numbers at different times; the agent enters the phone number at login time. An agent can access the Mobile Agent functionality using any phone number that is included in the Unified Communications Manager dial plan.

With Cisco Unified Mobile Agent, contact centers can:

- Add or enable temporary staff during seasonal high call volume who can be brought on line with reduced startup costs
- Provide agents with the flexibility to work from home with similar quality, function, performance, convenience, and security as are available in the corporate headquarters contact center
- Allow agents to use the device they are most comfortable with, which improves agent productivity, helps to retain agents, and reduces training costs

- Hire skilled employees where they live and integrate remote workers into geographically dispersed teams with access to equivalent corporate applications

The sections that follow highlight some of the benefits of Unified Mobile Agent, and describe its features.

Unified Mobile Agent Extends Unified CCE Capabilities

Before Mobile Agent, Unified CCE used a JTAPI interface to Unified CM to connect customer calls arriving on a voice gateway to an agent's IP phone. Mobile Agent enables the Unified CCE architecture to connect customer calls to an agent phone that Unified CCE does not directly control.

Mobile Agent uses a pair of CTI ports that function as proxies for the Mobile Agent phone and the caller phone. Every logged-in Mobile Agent requires two CTI ports (local and remote). The two CTI ports take the place of the Cisco IP Phone monitored and controlled by Unified CM JTAPI. The agent at login uses the local CTI port DN. When this agent is selected, the router transfers the caller to that CTI port. The remote CTI port calls the agent either at login for a nailed (permanent) connection or upon being selected for a call-by-call connection.

Cisco Unified Contact Center functionality remains intact whether an agent is mobile or local:

- Mobile Agents have the same capabilities and functionality that local agents have.
- Mobile Agents do not need any specialized equipment; they can receive calls on an analog or mobile phone.
- Unified Mobile Agent supports Cisco Finesse.
- Mobile Agent activity is recorded in the same contact center reports as local agent activity.
- Mobile Agent CTI and application data uses the same security mechanisms as local agent data.

Unified Mobile Agent Provides Agent Sign-In Flexibility

Agents can be either local agents or Mobile Agents, depending on how they sign in at various times.

Regardless of whether agents sign in as local or Mobile Agents, their skill groups do not change. Because agents are chosen by existing selection rules and not by how they are connected, the same routing applies regardless of how the agents log in. If you want to control routing depending on whether agents are local or mobile, assign the agents to different skill groups and design your scripts accordingly.

Connection Modes

Cisco Unified Mobile Agent allows system administrators to configure agents to use either call by call dialing or a nailed connection, or the administrator can configure agents to choose a connection mode at login time.

Mobile Agents are defined as agents using phones not directly controlled by Unified CC, irrespective of their physical location. (The term local agent refers to an agent who uses a phone that is under control of Unified CC, irrespective of physical location.)

You can configure Mobile Agents using either of two delivery modes:

- Call by Call—In this mode, the Mobile Agent's phone is dialed for each incoming call. When the call ends, the Mobile Agent's phone is disconnected before being made ready for the next call.
- Nailed Connection—In this mode, the agent is called at login time and the line stays connected through multiple customer calls.

Note The administrator can select the *Agent chooses* option, which allows an agent to select a call delivery mode at login.

Call by Call

In a *call by call* delivery mode, the Mobile Agent's phone is dialed for each incoming call. When the call ends, the Mobile Agent's phone disconnects before is it made ready for the next call.

The *call by call* call flow works as follows:

1. At login, the agent specifies an assigned extension for a CTI port.
2. A customer call arrives in the system and, through normal Unified ICM configuration and scripting, is queued for a skill group or an agent. (This is no different than existing processing for local agents.)
3. The system assigns an agent to the call. If the agent's Desk Setting is Unified Mobile Agent-enabled and configured for either call by call or Agent chooses mode, the router uses the extension of the agent's CTI port as a label.
4. The incoming call rings at the agent's CTI port. The JTAPI Gateway and PIM notice this but do not answer the call.
5. A call to the agent is initiated on another CTI port chosen from a preconfigured pool. If this call fails, Redirect on No Answer processing is initiated.

Note In call by call mode, the Answer Wait Time is 3 to 15 seconds longer than in a local agent inbound call scenario. Specify a Redirect on No Answer setting large enough to accommodate the extra processing time.

6. When the agent takes the remote phone off-hook to answer the call, the system directs the customer call to the agent's call media address and the agent's call to the customer's call media address.
7. When the call ends, both connections are terminated and the agent is ready to accept another call.

Note To configure Mobile Agent in call by call delivery mode, you must set the wrap-up timer to at least one second using the Agent Desktop Settings List tool in the Configuration Manager.

In call by call delivery mode, callers often perceive a longer ring time compared to nailed connection delivery mode. This is because callers hear the ringtone during the call flow; ringing stops only after the agent answers. From the Unified CCE reporting perspective, a Mobile Agent in call by call delivery mode has a longer Answer Wait Time for the same reason.

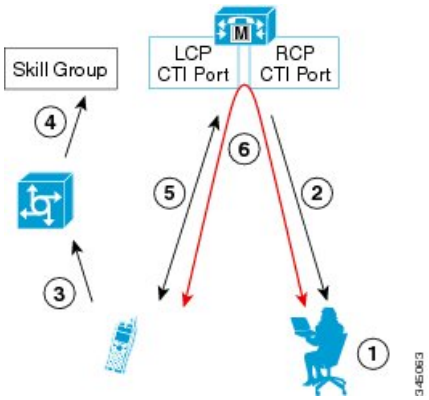
Related Topics

Configure Agent Desk Settings with Configuration Manager, on page 101

Nailed Connections

In *nailed connection* delivery mode, the agent is called once, at login, and the phone line remains connected through multiple customer calls. See the following figure.

Figure 9: Nailed Connection Call Flow



The nailed connection call flow works as follows:

1. At login, the agent specifies an assigned extension for a CTI port from a pool.
2. A call to the agent is initiated on another CTI port chosen from a preconfigured pool. The agent answers the call. (The agent must answer this setup call to complete the connection and finalize the login procedure.)
3. A customer's call arrives in the system and, through normal Packaged CCE configuration and scripting, is queued for a skill group or an agent. (This is no different than existing processing for local agents.)
4. The system assigns an agent to the call. If the agent's Desk Setting is Unified Mobile Agent-enabled and configured for either nailed connection or Agent chooses mode, the router uses the extension of the agent's CTI port as a label.
5. The incoming call rings at the agent's CTI port. The JTAPI Gateway and PIM notice this but does not answer the call.
6. The agent desktop indicates a call is ringing and the agent clicks **Answer**.
7. When the agent indicates that they will answer the phone, the system directs the customer call to the agent's call media address and the agent call to the customer's call media address.
8. When the call ends, the customer connection is terminated and the agent state is set to Ready.

Connect Tone

The *Connect Tone* feature in the nailed connection mode enables the system to play a tone to the Mobile Agent through the agent's headset to let the agent know when a new call is connected. In the nailed connection mode, you can configure an audible connect tone in addition to a call arrival notice (on the desktop only).

Connect Tone is particularly useful when Auto Answer is enabled or the agent is an Outbound agent. Here are its features:

- An audible tone (two beeps) is sent to the Mobile Agent headset when the call to the nailed connection Mobile Agent is connected. It is a DTMF tone played by Unified CM and cannot be modified.
- The Connect Tone plays only when the nailed connection Mobile Agent receives a call, as in the following examples:
  - The agent receives a consultation call.
  - The agent receives an outbound call.

- The Connect Tone does not play when the nailed connection Mobile Agent initiates a call, as in the following examples:
  - The agent makes a call.
  - The agent makes the consultation call.
  - Outbound direct preview call is made.
  - Supervisor barge-in call is made.

Related Topics

Enable Mobile Agent Connect Tone, on page 106

Agent Greeting and Whisper Announcement

The Agent Greeting and Whisper Announcement features are available to Unified Mobile Agents. The following sections explain more about how these features apply to Unified Mobile Agents.

Agent Greeting

You can use the Agent Greeting feature to record a message that plays automatically to callers when they connect to you. Your greeting message can welcome the caller, identify you, and include other useful information.

Limitations

The following limitations apply to the Agent Greeting feature for Mobile Agents.

- If a Mobile Agent hangs up when an Agent Greeting plays, the customer still hears the complete Agent Greeting before the call ends. This applies for both call by call and nailed-up calls.

Note In the Agent Greeting Call Type Report, this call does not appear as a failed agent greeting call.

- A supervisor cannot barge in when an Agent Greeting is playing.
- If a Peripheral Gateway (PG), JTAPI Gateway (JGW), or PIM failover occurs when an Agent Greeting plays for a Mobile Agent, the call fails.
- If a Mobile Agent hangs up when an Agent Greeting plays, the customer still hears the complete Agent Greeting before the call ends.

Note In the Agent Greeting Call Type Report, this call does not appear as a failed agent greeting call.

- If a Peripheral Gateway (PG), JTAPI Gateway (JGW), or PIM failover occurs when an Agent Greeting plays for a Mobile Agent, the call fails. This applies for both call-by-call and nailed-up calls.

Note You can use Agent Greeting for Mobile Agents only with parent/child deployments that are approved by Cisco Assessment-to-Quality (A2Q) with Design Mentoring Services (DMS).

For more information about Agent Greeting, see Capabilities, on page 1.

Whisper Announcement

With Whisper Announcement, agents can hear a brief prerecorded message just before they connect with each caller. The announcement plays only to the agent; the caller hears ringing (based on existing ringtone patterns) while the announcement plays. The announcement can contain information about the caller, such as language preference or customer status. This information helps the agent prepare for the call.

Configuration Requirement

For the Whisper Announcement feature for Unified Mobile Agents, you require a Media Termination Point (MTP) resource on an incoming SIP device.

Feature Requirements

Hardware and Software Requirements

Hardware and software requirements for the Unified Mobile Agent are identical to those of Unified CCE. For more information on feature requirements, consult these documents:

- *Solution Design Guide for Cisco Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html
- *Virtualization for Unified Contact Center Enterprise* at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html
- *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html

Phone Requirements

A Unified Mobile Agent can use an analog, digital, or IP phone to handle calls.

Conference Requirements

To use Agent Greeting for Mobile Agents, you must configure external conference-bridge (hardware) resources. To estimate the number of required resources, you can use the following formula:

Number of conference bridge resources = Mobile Agent call rate × Average greeting time (in seconds)

For information about configuring external conference-bridge resources, see the `dspfarm profile 1 for conference` configuration section in the sample configuration gateway, listed in Media Termination Points Configuration, on page 102.

CTI Port Requirements

You need two CTI ports (local and remote) for every logged-in Mobile Agent.

Unified Mobile Agent uses Unified CM CTI Port as a proxy for the agent's phone. When this proxy is set up, whenever a Mobile Agent is selected to handle a customer call, the following happens:

- The call is directed to the CTI port extension.
- Unified CCE, using the JTAPI Gateway, intercepts the call arriving on the CTI Port and directs Unified CM to connect the call to the Mobile Agent.

Unified Mobile Agent requires that maximum number of calls is set to 2 and busy trigger is set to 1.

For Unified Mobile Agent to work properly, you must configure two CTI ports:

- One port to serve as the agent's virtual extension.
- The other port to initiate calls to the agent.

You must assign these CTI ports to the Unified ICM application. The ports are recognized by Unified ICM when receiving the Unified CM configuration.

For these CTI ports in IPv6 enabled deployments, you have to set **IP Addressing Mode** to **IPv4 Only**. You do this by creating a **Common Device Configuration** and referencing it to these CTI ports.

Supported Unified CCE/Unified CCH Features

The following features are supported:

- Unified CCE supports temporary uninstallation while preserving Mobile Agent data.

  For more information about temporary uninstallation, see the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*.
- Mobile Agents can participate in outbound campaigns, but they must use a nailed-up connection for all outbound dialing modes.
- Unified Mobile Agent supports Redirect on No Answer (RONA). If the Mobile Agent fails to answer, the agent is made Not Ready, and the call is redirected to a RANA DN route point.
- Unified Mobile Agent supports G.711A-law, G.711u-law, and G.729 codecs.
- There is no direct interaction between Unified Mobile Agent and multichannel applications. Email and Chat are IP applications that continue to operate normally, assuming the Mobile Agent has a desktop with enough bandwidth on the broadband connection to support them.
- Unified Mobile Agent supports Cisco Unified Customer Voice Portal (Unified CVP) and Cisco Unified IP-IVR (Unified IP IVR).

Related Topics

Silent Monitoring, on page 89

Fault Tolerance Support

Fault tolerance for the Unified Mobile Agent follows the behavior of Unified CCE:

- The JTAPI Gateway, Unified CCE PIM, and CTI components record key events related to Unified Mobile Agent as part of their normal logging.
- As with standard Unified CCE calls, if a Peripheral Gateway (PG) component such as the JTAPI Gateway fails, the phone call is not lost, but subsequent call control (transfer, conference, or hold) might not be possible after a failover. The Mobile Agent is notified of a failure (on the desktop), but they must log in again after a Unified CM or Unified ICM failure occurs.
- Where CTI data is delivered for screen pops, CTI data is preserved.

Unified Mobile Agent can experience many of the same failure cases as Unified CCE:

- Side A/B failure
- VRU failure
- Unified CM failure
- CTI server failure

There are also some failure cases that are unique to Unified Mobile Agent:

- A situation where a Mobile Agent is using a cellular phone and the connection is dropped due to non-availability of a signal, is deemed as external failure. The agent must call back and log-in again.
- If a Mobile Agent's phone line disconnects while using nailed connection mode, the agent must log in again to receive new calls.

Related Topics

Failover, on page 88

Important Considerations

Before you proceed, consider the following Unified Mobile Agent limitations and considerations:

Failover

- During a failover, if an agent in call by call mode answers an alerting call, the call can drop. This occurs because the media cannot be bridged when there is no active PG.
- During a prolonged Peripheral Gateway (PG) failover, if an agent takes call control action for a Unified Mobile Agent-to-Unified Mobile Agent call, the call can drop. This occurs because the activating PG may not have information for all agents and calls at that point.
- Unified Communications Manager failover causes a Mobile Agent call to be lost.
- If a call by call Mobile Agent initiates a call (including a supervisor call) and does not answer the remote leg of the call before PG failover, the call fails. The agent must disconnect the remote agent call leg and reinitiate the call.

Performance

- Mobile Agent call processing uses more server resources and therefore reduces the maximum number of supported agents on both Unified CM and the Unified ICM Agent PG.

For more information about sizing Mobile Agents, see the *Solution Design Guide for Cisco Unified Contact Center Enterprise*.

- Because Unified Mobile Agent adds processing steps to Unified CCE/Unified CCH default functionality, Mobile Agents may experience some delay in screen popup windows.
- From a caller's perspective, the call by call delivery mode has a longer ring time compared with the nailed connection delivery mode. This is because Unified CCE/Unified CCH does not start to dial the Mobile Agent's phone number until *after* the call information is routed to the agent desktop. In addition, the customer call media stream is not connected to the agent until after the agent answers the phone.

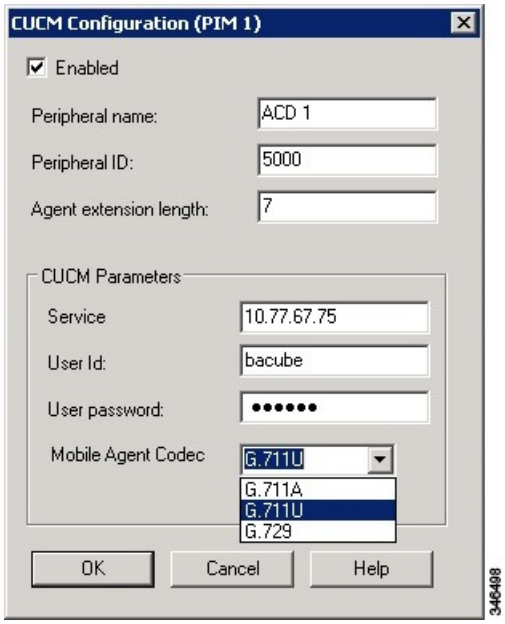
  The caller hears a repeated ringtone while Unified CCE/Unified CCH makes these connections.

Codec

The codec settings on the Peripheral Gateway and Voice Gateway must match. Perform the following procedure:

1. Launch the Peripheral Gateway Setup.
2. In the Peripheral Gateway Component Properties, select the UCM PIM and click **Edit.**
3. In the CallManager Parameters section, select the appropriate codec from the Mobile Agent Codec drop down list.

Figure 10: Mobile Agent Codec Selection



Silent Monitoring

Unified Mobile Agent provides the following silent monitoring support:

- Unified Mobile Agent requires that caller and agent voice gateways be on separate devices if silent monitoring is to be used.
- Unified Mobile Agent does not support desktop monitoring.

- Whenever silent monitoring is used on Unified Mobile Agent, caller and agent voice gateways must be on separate devices. Similarly, if MTP is enabled when silent monitoring is used, MTP resources for caller and agent must also be on separate devices.

Mobile Agent Scalability

Mobile Agent scalability may be contingent on specific Unified CM versions. For more information, see the *Solution Design Guide for Cisco Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html.

Unsupported Features

The following is a list of unsupported features for Mobile Agent:

- Web Callback
- Blended Collaboration
- Unified CM-based Silent Monitoring
- Agent Request

Unified Mobile Agent Call Flows

This section provides sample Unified Mobile Agent call flows for:

- Inbound calls
- Local consultation calls
- Remote consultation calls
- Remote conference calls

In all Unified Mobile Agent call flows, the JTAPI Gateway maintains the signaling association between the inbound and outbound calls and, if necessary, performs further operations on the call. JTAPI Gateway, however, does not terminate media; it uses CTI to deliver the customer call from the inbound gateway port to the outbound gateway port.

This means that a Mobile Agent *must* use an agent desktop application to log in, change agent state, log out, send dual-tone multifrequency (DTMF) digits, and perform call control.

About Figures in This Section

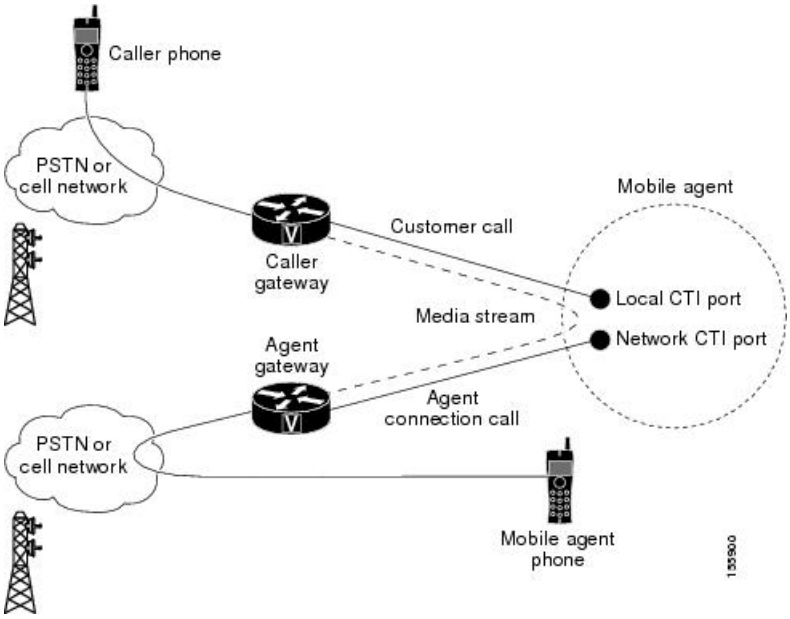
The figures in this section:

- Show a caller and a Mobile Agent in a cellular network. However, the same concepts apply whether the Mobile Agent is using an enterprise desk phone, an IP Phone spanning another Unified CM cluster, standard analog phone, or a third-party ACD phone.
- Focus solely on call media flow; a Mobile Agent must use a CTI Desktop with broadband access to perform agent state and call control.
- Show only a sampling of the call flows possible with Unified Mobile Agent.

Inbound Call Flow

The following figure shows an inbound call flow.

Figure 11: Mobile Agent Inbound Call Flow



Note Caller and Agent voice gateways can coreside on one device, except in deployments where Silent Monitoring is required.

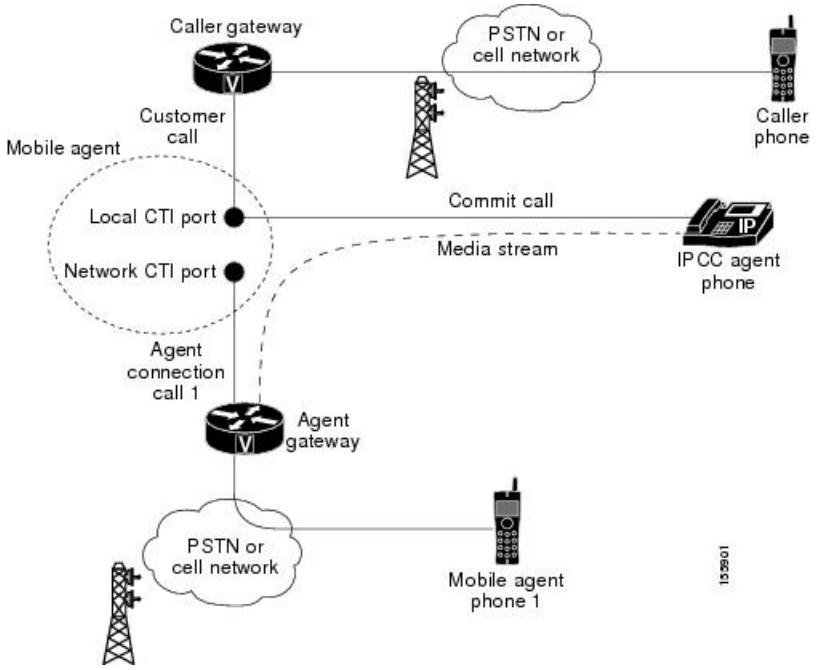
The following describes an inbound call flow:

1. The Mobile Agent becomes available to answer calls by:
   - Logging in to the corporate domain using VPN over the ADSL/Cable connection
   - Launching the agent desktop interface and logging in with their remote phone information
   - Entering the Ready mode
2. A customer call arrives at the Unified CC.
3. The JTAPI Gateway creates a Mobile Agent class to manage local and network CTI ports for a Mobile Agent.
4. The Router passes the call to the *local* CTI Port of a Mobile Agent.
5. The JTAPI Gateway places a call on a *network* CTI port to the agent's cell phone.
6. The JTAPI Gateway uses local and network CTI ports of the Mobile Agent to stream the media for the call from the inbound (caller) gateway port to the outbound (agent) gateway port.

Local Consult Calls

The following figure shows a consult call flow between a Mobile Agent and a local agent.

Figure 12: Mobile Agent Consult Call Flow



Note Caller and Agent voice gateways can coreside on one device, except in deployments where Silent Monitoring is required.

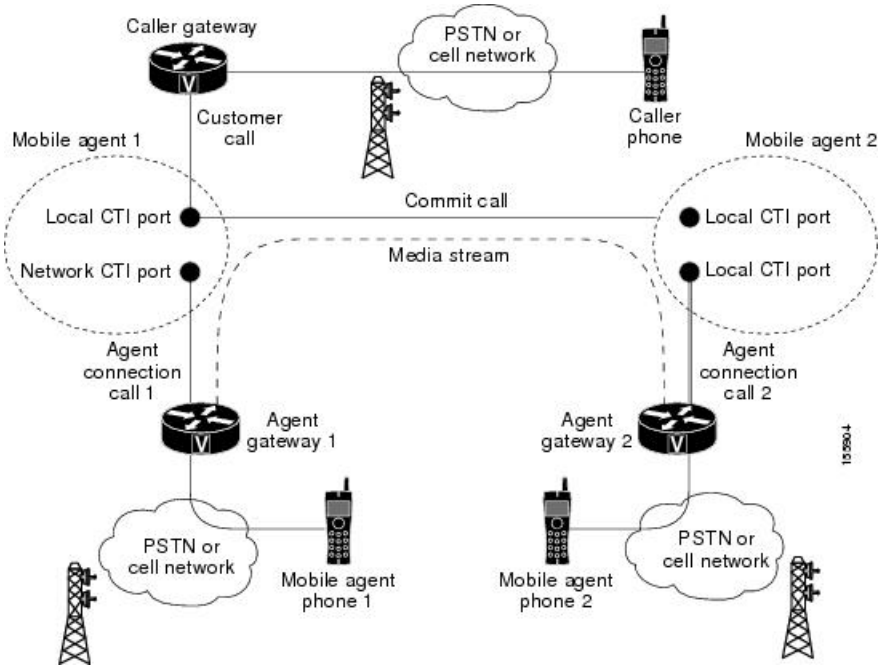
The following describes a local consult call flow:

1. The Mobile Agent becomes available to answer calls by:
   - Logging in to the corporate domain using VPN over the ADSL/Cable connection
   - Launching the agent desktop interface and logging in with their remote phone information
   - Entering the Ready mode
2. A customer call arrives at the Unified CC.
3. The JTAPI Gateway creates a Mobile Agent class to manage local and network CTI ports for a Mobile Agent.
4. The Router passes the call to the *local* CTI Port of a Mobile Agent.
5. The JTAPI Gateway places Agent Connection Call 1 on a *network* CTI port to the agent's cell phone.
6. The Mobile Agent places the customer call on hold and consults a local Unified CCE/Unified CCH agent.
7. The JTAPI Gateway uses local and network CTI ports of the Mobile Agent to stream the media for the call from the IP hard phone to the outbound gateway port.

Remote Consult Calls

The following figure shows a remote consult call flow between two Mobile Agents.

Figure 13: Mobile Agent Remote Consult Call Flow



Note Caller and Agent voice gateways can coreside on one device, except in deployments where Silent Monitoring is required.

The following describes a remote consult call flow:

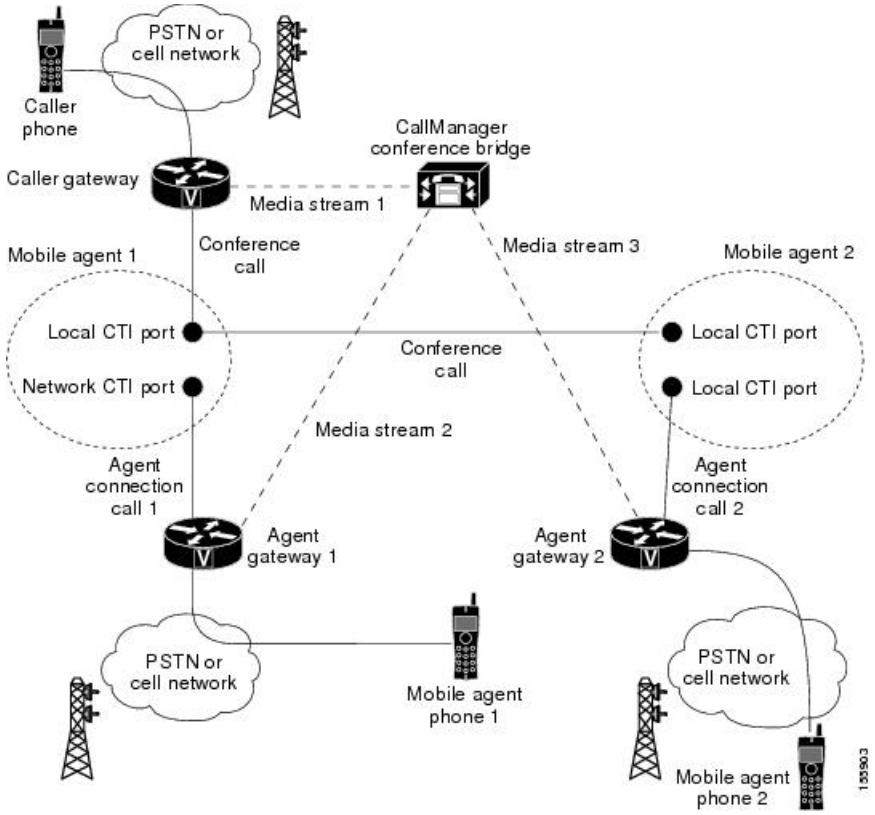
1. The Mobile Agent becomes available to answer calls by:
   - Logging in to the corporate domain using VPN over the ADSL/Cable connection
   - Launching the agent desktop interface and logging in with their remote phone information
   - Entering the Ready mode
2. A customer call arrives at the Unified CC.
3. The JTAPI Gateway creates a Mobile Agent class to manage local and network CTI ports for a Mobile Agent.
4. The Router passes the call to the *local* CTI Port of a Mobile Agent.
5. The JTAPI Gateway places Agent Connection Call 1 on a *network* CTI port to the agent's cell phone.
6. Mobile Agent 1 puts the customer call on hold and consults Mobile Agent 2.

7. The JTAPI Gateway uses the network CTI port of Mobile Agent 1 and the network CTI port of Mobile Agent 2 to stream the media for the call from the outbound gateway port on Agent Gateway 1 to the outbound gateway port on Agent Gateway 2.

Remote Conference Calls

The following figure shows a remote conference call flow between two Mobile Agents.

Figure 14: Mobile Agent Remote Conference Call Flow



Note Caller and Agent voice gateways can coreside on one device, except in deployments where Silent Monitoring is required.

The following describes a remote conference call flow:

1. The Mobile Agent becomes available to answer calls by:
   - Logging in to the corporate domain using VPN over the ADSL/Cable connection
   - Launching the agent desktop interface and logging in with their remote phone information
   - Entering the Ready mode
2. A customer call arrives at the Unified CC.

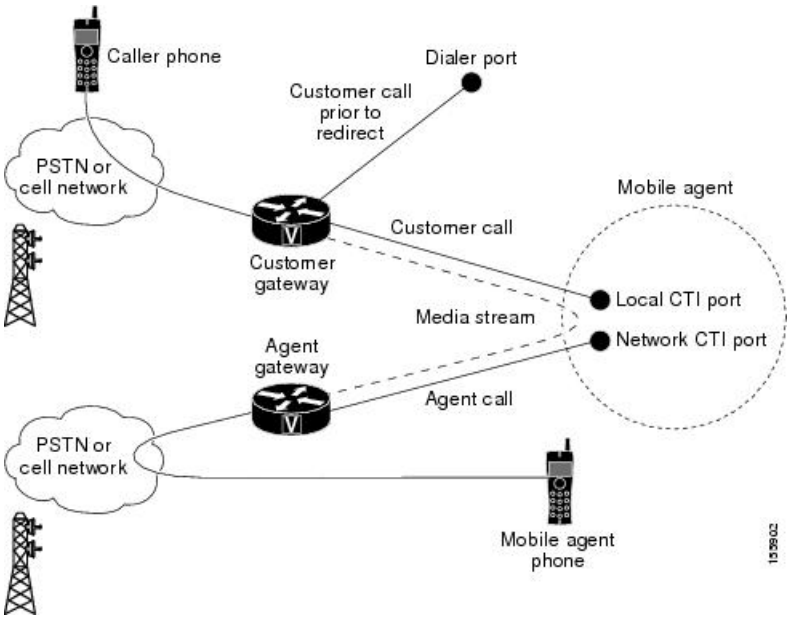
3. The JTAPI Gateway creates a Mobile Agent class to manage local and network CTI ports for a Mobile Agent.
4. The Router passes the call to the *local* CTI Port of a Mobile Agent.
5. Unified CM redirects the media stream 1 from inbound gateway on the Caller Gateway to the conference bridge during call merging process.
6. The JTAPI Gateway uses local and network CTI ports of Mobile Agent 1 to loop the Media Stream 2 for the call from the outbound gateway port on the Agent Gateway 1 to the conference bridge.
7. The JTAPI Gateway uses local and network CTI ports of Mobile Agent 2 to loop the Media Stream 3 for the call from the outbound gateway port on the Agent Gateway 2 to the conference bridge.

Outbound Option Call Flow

The following figure shows a Outbound Option call flow between a customer and a Mobile Agent.

Note Unified Mobile Agent supports Outbound Option calls in nailed connection delivery mode *only*.

Figure 15: Mobile Agent Outbound Call Flow



Note Caller and Agent voice gateways can coreside on one device, except in deployments where Silent Monitoring is required.

The following describes an Outbound Option call flow:

1. The Mobile Agent becomes available to answer calls by:
   - Logging in to the corporate domain using VPN over the ADSL/Cable connection

- Launching the agent desktop interface and logging in with their remote phone information
- Entering the Ready mode

2. The JTAPI Gateway creates a Mobile Agent class to manage local and network CTI ports for a Mobile Agent.
3. Outbound Option dials the customer number and, after reaching a live customer, the Dialer redirects the customer call to the *local* CTI Port of an Outbound Option Mobile Agent.
4. The JTAPI Gateway places a call on a *network* CTI port to the agent's cell phone.
5. The JTAPI Gateway uses local and network CTI ports of the Mobile Agent to stream the media for the call from the inbound gateway port to the outbound gateway port.

Unified Mobile Agent Reporting

Unified Mobile Agent-specific call data is contained in the following Cisco Unified Intelligence Center reports: Agent Team Historical, Agent Real Time, and Agent Skill Group Historical. These "All Field" reports contain information in multiple fields that show what kind of call the agent is on (nonmobile, call by call, nailed connection) and the Unified Mobile Agent phone number.

Notes about Mobile Agents and reporting:

- The Mobile Agent must be logged in through the agent desktop for call data to be recorded in Unified CC reports.
- Service level for Mobile Agent calls might be different than local agent calls, because it takes longer to connect the call to the agent.

  For example, a call by call Mobile Agent might have a longer Answer Wait Time Average than a local agent. This is because Unified CCE/Unified CCH does not start to dial the Mobile Agent phone number until *after* the call information is routed to the agent desktop. In addition, the customer call media stream is not connected to the agent until after the agent answers the phone.

  For more information about Unified Mobile Agent fields in the database schema, see *Database Schema Handbook for Cisco Unified Contact Center Enterprise*.

Initial Setup

Summary of Unified Mobile Agent System Configuration Tasks

The following table describes system configuration tasks for Unified Mobile Agent.

Table 6: Unified Mobile Agent System Configuration Tasks

Task	See
Configure Unified CM CTI Port pools	Unified CM CTI Port Configuration and Mapping for Unified Mobile Agent, on page 97

Task	See
Configure Unified CM Call Duration Timer	Maximum Call Duration Timer Configuration, on page 100
Configure Agent Desk Settings	Agent Desk Setting Configuration for Unified Mobile Agent, on page 101
Configure Devices	Device Configuration for Unified Mobile Agent, on page 102
Configure Media Termination Points	Media Termination Points Configuration, on page 102

Unified CM CTI Port Configuration and Mapping for Unified Mobile Agent

This section describes the CTI Port Pool configuration tasks *specific* to Mobile Agent Option configuration. It does not discuss installation or configuration of Unified CCE.

Note For more information about installing and configuring Unified CM with Unified CCE, see the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*.

Unified Mobile Agent must have two CTI ports configured on Unified CM:

- A *local* CTI port, which Unified Mobile Agent uses as the agent's virtual extension.
- A *remote* CTI port, which Unified Mobile Agent uses to initiate a call to the Mobile Agent's phone.

Naming Conventions for Local and Network Ports

- The local port *must* begin with the string LCP.
- The remote port *must* begin with the string RCP.
- The remaining characters in the device names for the LCP and RCP pair *must match*. For example an LCP port named LCP0000 has a corresponding RCP port named RCP0000.
- For example, you can use the following naming convention:
  - For a local CTI Port pool name, configure a name in the format LCP*xxxxFyyyy*, where LCP identifies a local CTI Port Pool, *xxxx* is the peripheral ID for the Unified CM PIM, and *yyyy* is the number of local CTI Port.

    Example: LCP5000F0000 represents CTI Port: 0 in a local CTI Port pool for the Unified CM PIM with the peripheral ID 5000.
  - For a network CTI Port pool name, use the same format, except substitute RCP as the first three characters.

Note While you do not require a naming convention, the substrings identifying the Unified CM PIM peripheral ID and the CTI Port *must* match for each local/network pair.

CTI Port configuration consists of the following steps:

1. Add the CTI port as you would for an IP Phone.
2. Use the naming convention described above to map the local and network CTI ports.

Note Each local CTI port must have a corresponding network CTI port.

3. Add a directory number for the local CTI port (that is, the agent's virtual extension).
4. Map the local and network CTI ports with the PG user.

Music on Hold Design

If you want callers to hear music when a Mobile Agent places the caller on hold, you must assign Music on Hold (MoH) resources to the ingress voice gateway or trunk that is connected to the *caller* (as you do with traditional agents). In this case, the user or network audio source is specified on the local CTI port configuration. Similarly, if a Mobile Agent must hear music when the system puts the agent on hold, you must assign MoH resources to the ingress voice gateway or trunk that is connected to the *Mobile Agent.* In this case, the user or network audio source is specified on the remote CTI port configuration.

Do not assign MoH resources to local ports and remote CTI ports, because it might affect the system performance.

If a remote Mobile Agent calls over a nailed connection and if there is no active call to the agent, the agent is put on hold. Enable MoH to the Mobile Agent phone for nailed connection calls. If MoH resources are an issue, consider multicast MoH services.

If a remote Mobile Agent calls over a nailed connection, and if MoH is disabled, the hold tone plays to the agent phone during the hold time. This depends on the call processing agent that controls the Mobile Agent remote phone. For Unified CM, the hold tone is enabled by default (it is similar to the Mobile Agent connect tone). Because the hold tone is similar to the connect tone, it is difficult for the agent to identify if a call arrived from listening to the Mobile Agent connect tone. The hold tone prevents the agent from hearing the connect tone.

Therefore, disable the hold tone by changing the setting of the Tone on Hold Timer service parameter to 0. For more information about setting this parameter, see the Unified CM product documentation available at: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html.

Configure Unified CM CTI Port Pools for Unified Mobile Agent

Perform the following steps to configure CTI Ports.

Procedure

Step 1 In Unified CM Administration, select **Device** > **Phone**.

Step 2 Click **Add a New Phone**.

Step 3 From Phone Type, select **CTI Port**.

Step 4 Click **Next**.

Step 5 In Device Name, enter a unique name for the local CTI Port pool name; click **OK** when finished.

Using the naming convention format LCP*xxxxyyyy*:

- LCP identifies the CTI Port as a local device.
- *xxxx* is the peripheral ID for the Unified CM PIM.
- *yyyy* is the local CTI Port.

The name LCP5000F0000 would represent CTI Port: 0 in a local CTI Port pool for the Unified CM PIM with the peripheral ID 5000.

The name LCP0000 represents the local port.

Step 6 In Description, enter text that identifies the local CTI port.

Step 7 Use the **Device Pool** drop-down list to choose the device pool to which you want to assign the network CTI port pool. Do not select Default. (The device pool defines sets of common characteristics for devices.)

Step 8 Click **Save**.

Step 9 Highlight a record and select **Add a New DN**.

Step 10 Add a unique directory number for the CTI port you just created.

Step 11 In Maximum Number of Calls, enter **2**.

Step 12 In Busy Trigger, enter **1**.

Step 13 When finished, click **Save**, and click **Close**.

Step 14 Repeat the preceding steps to configure the network CTI port pool.

In Device Name, using the naming convention format RCP*xxxxyyyy*, where:

- RCP identifies the CTI port as the Remote CTI port where the call between the agent's remote device and the Unified CM Port is nailed up at agent login time.
- *xxxx* is the peripheral ID for the Unified CM PIM.
- *yyyy* is the network CTI port.

The name RCP5000F0000 represents CTI Port: 0 in a network CTI Port pool for the Unified CM PIM with the peripheral ID 5000.

Step 15 In Description, enter text that identifies the network CTI port pool.

Step 16 Use the **Device Pool** drop-down list to choose the device pool to which you want to assign the network CTI port. Do not select Default. pool. (The device pool defines sets of common characteristics for devices.)

Step 17 Click **Save**.

Step 18 Highlight a record and select **Add a New DN**.

Step 19 Add a unique directory number for the CTI port you just created.

The extension length can be different from the extension length of the LCP Port if your dial plan requires it.

Step 20 When finished, click **Save**, and click **Close**.

Map Local and Remote CTI Ports with Peripheral Gateway User

After you define the CTI Port pool, you must associate the CTI Ports with PG users.

Procedure

Step 1 In Unified CM Administration, select **Application User**.

Step 2 Select a username and associate ports with it.

Step 3 When finished, click **Save**, and then click **Close**.

Note If CTI ports for Unified Mobile Agent are disassociated at the Unified CM while a Mobile Agent is on an active call, the call can drop.

Maximum Call Duration Timer Configuration

By default, Mobile Agents in nailed connection mode log out after 12 hours. This happens because a Unified CM Service Parameter—the Maximum Call Duration Timer—determines the amount of time an agent phone can remain in the Connected state after login.

If you anticipate that nailed connection agents in your Unified Mobile Agent deployment will be logged on *longer than* 12 hours, use the following instructions to either:

- Increase the Maximum Call Duration Timer setting.
- Disable the timer entirely.

Configure Maximum Call Duration Timer

Note This procedure applies only to Unified Mobile Agent deployments where agents logged in to nailed connection mode are to remain connected *longer than* 12 hours. Also, if your Mobile Agent deployment uses intercluster trunks, you must perform the following steps on both local and network Unified CM clusters.

Procedure

Step 1 In Unified CM Administration, choose **System** > **Service Parameters**.

Step 2 In the Server drop-down list, choose a server.

Step 3 In the Service drop-down list, choose a server .

The **Service Parameters Configuration** windowappears.

Step 4 In the Cluster-wide Parameters section, specify a **Maximum Call Duration Timer** setting.

The default is 720 minutes (12 hours); the maximum setting allowed is 35791 minutes.

Note To disable the timer, enter **0**.

Step 5 Click **Save**.

Agent Desk Setting Configuration for Unified Mobile Agent

This section describes Agent Desk Settings that you must modify to accommodate Unified Mobile Agent features.

Configure Agent Desk Settings with Configuration Manager

This section describes Agent Desk Settings configuration settings you should specify in Unified ICM Configuration Manager to accommodate Unified Mobile Agent features.

The following instructions describe how to configure *one* Agent Desk Setting. Repeat this process for each different Agent Desk Setting in your deployment.

Procedure

Step 1 From the Unified ICM Configuration Manager, choose **Configure ICM** > **Enterprise** > **Agent Desk Settings List**.

The Unified ICM Agent Desk Settings List dialog box opens.

Step 2 Click **Retrieve**.

Step 3 Click **Add**.

Step 4 Fill in the following Attributes tab information, making sure to include settings for the following fields and check boxes:

- **Ring no answer time**. The system allows a call to ring at the agent's station before redirecting the call. This can be from 1 to 120 seconds.

  Note If you use call by call mode, the answer wait time will be longer than in a local agent inbound call scenario, so specify a value in this field to accommodate the extra processing time.

- **Logout non-activity time**. The number of seconds of agent inactivity while in the not ready state before the system logs out the agent. A blank entry disables the timer.
- **Cisco Unified Mobile Agent** (check box). Enables the Mobile Agent feature so that the agent can log in remotely and take calls from any phone.
- **Mobile Agent mode**. Select how call connections are made to the Mobile Agent's phone:
  - **Agent chooses**. Agent selects call by call or nailed connection at login.
  - **Call by call**. Agent's phone is dialed for each incoming call. When a call ends, the connection is terminated before the agent is made ready for next call.
  - **Nailed connection**. Agent is called once, at login. The line stays connected through multiple customer calls.

Step 5 Click **Save**.

Note For more information about configuring Agent Desk Settings in Unified CCE, see *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*.

Device Configuration for Unified Mobile Agent

Use the Agent Targeting Rules (ATR) mechanism described in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* to configure a device as you would for a phone, but using the LCP Port in place of the agent's phone extension.

Media Termination Points Configuration

If you use SIP trunks, you must configure Media Termination Points (MTPs). You must also configure MTPs if you use TDM trunks to create an interface with service providers.

Additionally, MTPs are required for Mobile Agent call flows that involve a Cisco Unified Customer Voice Portal (CVP) solution. Because in DTMF signaling mode the Mobile Agent uses out-of-band signaling, whereas Unified CVP supports in-band signaling, the conversion from out-of-band to in-band signaling requires an MTP resource.

MTPs may be allocated as required in deployments that use a mix of IPv4 and IPv6 connections. MTP resources are allocated provided that the Media Resource Group List is configured on the IPV4 endpoint.

MTPs are available in the following forms, but not all are supported in Mobile Agent environments:

- Software-based MTPs in Cisco IOS gateways—use these MTPs for Mobile Agent as they provide codec flexibility and improved scalability compared with other MTP options. The following is a sample configuration on a gateway.

```
sccp local GigabitEthernet0/0
sccp ccm 10.10.10.31 identifier 1 priority 1 version 7.0
sccp ccm 10.10.10.131 identifier 2 priority 2 version 7.0
sccp
!
sccp ccm group 1
 associate ccm 1 priority 1
 associate ccm 2 priority 2
 associate profile 3 register gw84xcode
 associate profile 1 register gw84conf
 associate profile 2 register gw84mtp
!
dspfarm profile 3 transcode
 codec g729abr8
 codec g729ar8
 codec g711alaw
 codec g711ulaw
 codec g729r8
 codec g729br8
 maximum sessions 52
 associate application SCCP
!
dspfarm profile 1 conference
 codec g729br8
 codec g729r8
 codec g729abr8
 codec g729ar8
```

```
 codec g711alaw
 codec g711ulaw
 maximum sessions 24
 associate application SCCP
!
dspfarm profile 2 mtp
 codec g711ulaw
 maximum sessions software 500
 associate application SCCP
```

- Hardware-based MTPs in Cisco IOS gateways—These MTPs are supported. If you choose these, consider the extra cost, codec restrictions, and scalability constraints.
- Software-based MTPs using the Cisco IP Voice Media Streaming Application—These MTPs are not supported with Mobile Agents.

Note Because Unified CM-based software MTPs are used implicitly, you must add a special configuration to avoid using them. Create a new Media Resource Group (MRG) as a place holder, and place the software MTPs in that MRG. For instructions, refer to the Unified CM help documentation.

Configure Media Termination Points in Unified CM

Add MTP Resources to Unified CM

Perform these steps to add media termination points (MTPs) to Unified CM.

Procedure

Step 1 In Unified CM Administration click **Media Resources** > **Media Termination Point**.

Step 2 Click Add New.

Step 3 Choose **Cisco IOS Enhanced Software Media Termination Point** from the **Media Termination Point Type** drop-down list.

Step 4 Enter an MTP name. This name must match the device name you chose in IOS. In the example in the previous section, the MTP was called gw84mtp, as from the config line: **`associate profile 2 gw84mtp`**.

Step 5 Choose the appropriate device pool.

Step 6 Click **Save** and then click **Apply config**.

Step 7 Navigate back to **Media Termination Point** and ensure the newly added MTP is listed as being registered with <*Unified CM subscriber IP address*> in the Status column.

Step 8 Repeat steps 1 through 7 for each sccp ccm group you configured on each of your gateways.

Configure Media Termination Point Resources in Unified CM

This section explains how to create media resource groups and media resource group lists.

Procedure

Step 1 Navigate to **Media Resources** > **Media Resource Group** in Unified CM Administration.

Step 2 Click **Add New**.

Step 3 Specify a name and description.

Step 4 From the Available Media Resources that you just created, move the those devices from the Available to the Selected list by clicking the down arrow. Ensure that you do *not* include Unified CM Software resources. For example, type anything that starts with ANN_, MTP_, or MOH_ .

Step 5 Navigate to **Media Resources** > **Media Resource Group List**.

Step 6 Click **Add New**.

Step 7 Move the Media Resource Group you just created from the Available Media Resource Groups to the Selected Media Resource Groups.

Step 8 Click **Save**.

Associate Media Resource Group List with Device Pools

Procedure

Step 1 Navigate to **System** > **Device Pool** and click on the device pool that contains the CTI ports for Mobile Agent. If there are multiple pools, perform the next step for each device pool that applies.

Step 2 In the Media Resource Group List drop-down list, select the Media Resource Group List that you just created, click **Save** and then click **Apply config**.

Quarantine Unified CM Software-Based Resources

Unified CM-based software MTPs are used by default. However, Cisco contact center deployments do not support these resources because they may cause performance problems in call processing. You must quarantine them with a special configuration. Perform the following steps:

Procedure

Step 1 Create a new Media Resource Group (MRG) as a place holder.

Step 2 Place the software MTPs in that MRG.

For further instructions, refer to the Unified CM help documentation.

Insert MTPs

If you use SIP trunks, you must configure MTPs. This also applies if you use TDM trunks to interact with service providers. Mobile Agent cannot use an MTP with codec pass through. When you configure the MTP, you must select No pass through. KPML is not supported with Mobile Agent.

Procedure

Step 1 Log in to Unified CM Administration and select **Device** > **Trunk**.

Step 2 Select the trunk on which you want to configure MTPs.

Step 3 Depending on the scenario listed below, perform the corresponding step listed in the Description column. Note that if you configure Trunk Groups to dynamically insert MTPs, only the calls that require MTPs use them.

- If you want to always insert MTPs for inbound and outbound calls through a given trunk: In the Trunk Configuration settings, select the **Media Termination Point Required** check box.
- If you want to dynamically insert MTPs when Unified ICM detects media or signaling incompatibility between the caller and called endpoints: In the Trunk Group Configuration settings, in DTMF Signaling Method, select **RFC2833**.

Enable Call Progress Tones for Agent-Initiated Calls

Procedure

When **MTP Required** is not enabled, extra configuration is required to enable an agent to hear call progress tones for agent initiated calls. If instead you have dynamic MTP allocation by forcing mismatched DTMF settings, then configure the Unified Communications Manager to enable Early Offer.

For information on configuring the Unified Communications Manager, see the Unified Communications Manager product documentation at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html. The Cisco Annunciator does not generate ringback and other call progress tones, as it does for regular phones and softphones. Instead, Mobile Agent relies on the called party generating these tones (and the early offer setting triggers sending these tones to the agent).

Note This selection does not affect MTP sizing for IP Phones and other endpoints that support RFC2833 signaling, as is the case for many Cisco phones. For more information about supported phones, see the Contact Center Enterprise Compatibility Matrix at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

Verify MTP Resource Utilization

Since Unified CM comes preconfigured with Software MTP resources, these resources may sometimes be used to provide MTP for Mobile Agent calls without proper configuration. Because we don't support the use of Unified CM based software MTPs, we explicitly quarantined them in the above section, Disabling Unified CM Based Software MTPs. To ensure that the new IOS-based MTPs are the ones being used for Mobile Agents, perform the following steps to verify that correct MTPs are used.

Procedure

Step 1 Install the Unified CM Realtime monitoring tool. This tool can be downloaded under **Application** > **Plugins** within Unified CM Administration.

Step 2 Place a call to a logged-in Mobile Agent.

Step 3 Open the Unified CM Realtime monitoring tool and navigate to **System** > **Performance** > **Open Performance Monitoring**.

Step 4 Expand the node(s) that are associated with your IOS-based MTP resources and choose **Cisco MTP Device**.

Step 5 Double-click **Resources Active** and choose all of the available resources to monitor. This includes both IOS and Unified CM-based resources. Ensure that the only resources that are active during the Mobile Agent phone call are the IOS-based resources. Also, ensure that all UCM-based MTP resources are *not* active.

Step 6 Repeat the previous step for each node that has MTP resources associated with it.

Enabled Connect Tone Feature

In a nailed connection, the system can play a tone to the Unified Mobile Agent through the agent headset to let the agent know when a new call is connected. In the default Installation, the Mobile Agent Connect Tone feature is disabled.

Enable Mobile Agent Connect Tone

If you require Unified Mobile Agent Connect Tone, you must make the following change in the Windows Registry for the key PlayMAConnectTone under the JTAPI GW PG registry entries.

Perform the following procedure to allow a Mobile Agent in the nailed connection mode to hear a tone when a new call is connected.

Before you begin

MTP resources must be associated with the CUCM trunk that connects to the Agent Gateway.

Procedure

Step 1 On the PG machine, open the Registry Editor (regedit.exe).

Step 2 Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<InstanceName>\PG1A\PG\CurrentVersion\JGWS\jgw1\JGWData\Config\PlayMAConnectTone`.

The Edit DWORD Value dialog box appears.

Step 3 In the Value data: field, enter **1** to enable Mobile Agent Connect Tone and click **OK**.

Step 4 Exit the Registry Editor to save the change, and cycle the PG service.

Administration and Usage

Cisco Finesse

Finesse provides a browser-based desktop for agents and supervisors. Mobile agents can perform the same call control functions as Unified CCE agents. Mobile supervisors can perform all call control functions except for silent monitoring.

Sign in to Cisco Finesse Desktop

Procedure

Step 1 Enter the hostname of the Finesse server in the fully qualified domain name (FQDN) format: https://<FQDN of Finesse server>, where FQDN is the fully qualified domain name of the Finesse server.

In an IPv6-enabled environment, you must include the port number in the URL (https://*FQDN of Finesse server*:8082/desktop).

Step 2 In the ID field, enter your agent ID.

Step 3 In the Password field, enter your password.

Step 4 In the Extension field, enter your extension.

For a mobile agent, the extension represents the virtual extension for the agent, also known as the local CTI port (LCP).

Step 5 Check the **Sign in as a Mobile Agent** check box.

The Mode and Dial Number fields appear.

Step 6 From the Mode drop-down list, choose the mode you want to use.

In **Call by Call** mode, your phone is dialed for each incoming call and disconnected when the call ends.

In **Nailed Connection** mode, your phone is called when you sign in and the line stays connected through multiple customer calls.

Step 7 In the Dial Number field, enter the number for the phone you are using.

Option	Description
ID	The agent ID.
Password	Your supervisor assigns this password.
Extension	The agent's extension.
Sign in as Unified Mobile Agent	Select to sign in as a Unified Mobile Agent.
Mode	Call by Call or Nailed Connection
Dial Number	The number of the phone being used.

Step 8 Click **Sign In**.

Note In Nailed Connection mode, the desktop must receive and answer a setup call before sign-in is complete.

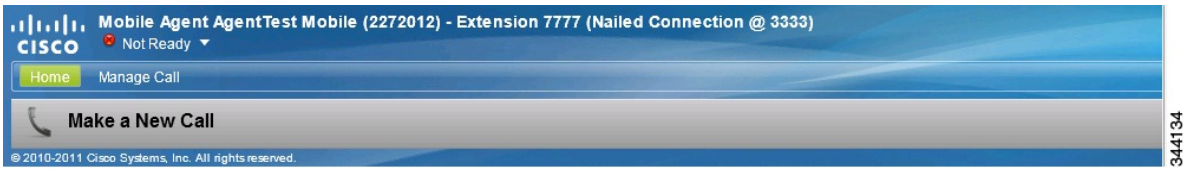
In Call by Call mode, the dial number provided is not verified. To ensure that the number is correct, verify the number in the header on the Agent Desktop after sign-in is complete.

Verify Sign-In to Cisco Finesse

Procedure

Check to be sure the Finesse Agent Desktop displays the following in the header:

- *Mobile Agent* before your agent name
- The mode used (Call by Call or Nailed Connection)
- The dial number you provided



Enable Ready State

You must be in Ready state to process incoming calls.

Procedure

Choose **Ready** from the drop-down list below the agent name.

Note If you are in call-by-call mode, you must answer and end each incoming call on your physical phone. After you answer a call, you must perform all other call control functions (such as Conference, Transfer, Hold, Retrieve) using the desktop.

With call-by-call connection, an agent cannot end one leg of a transfer without terminating it at the other end. The transfer must either be fully completed or both legs completely dropped.

If you are in Nailed Connection mode, after you answer the initial setup call, you must perform all other call control functions using the desktop.

Make a Call

Procedure

Step 1 From the drop-down list below the agent name, choose **Not Ready**.

Note You must be in Not Ready state to make a call.

Step 2 Click **Make a New Call**.

Step 3 Enter the number you want to call on the keypad, and then click **Call**.

If you are in Call by Call mode, the CTI server sends a setup call to your phone. A message appears on the keypad that states the following:

```
A call will be initiated to your phone which must be answered before an
outbound call to your destination can be made.
```

After the setup call is answered, the system establishes the outbound call to the destination specified.

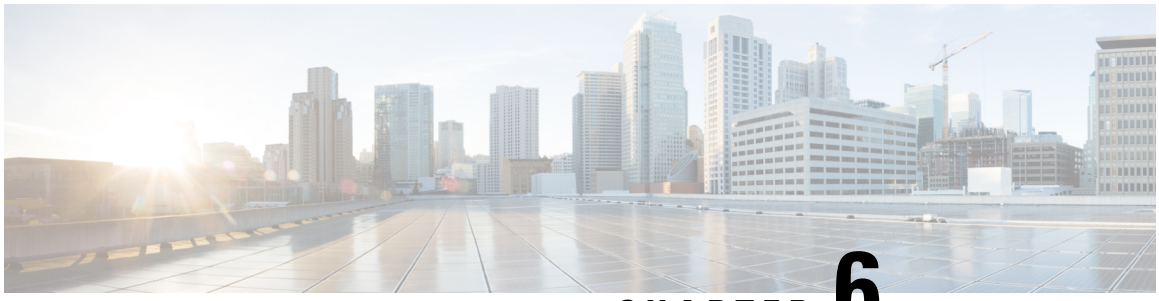
Serviceability

On a Mobile Agent call flow, CUCM may return a 404 error due to the absence of a agent greeting, leading to call failure. To fix this issue, do the following:

1. Create a new Run External Script node. Map the backup media of the script to the agent greeting recording (media file).
2. Add the Run External Script node between the failure path of the AgentGreeting Run External Script node and the End node.
3. Connect the Run External Script node's success path to the existing Release Call node and failure path to the existing End node.

Note This fix may add a short delay of one to two seconds to the call flow.

For information about Agent Greeting Play Script, on page 22.



CHAPTER 6

Precision Queue

Capabilities

Precision Queues

Precision routing offers a multidimensional alternative to skill group routing: using Unified CCE scripting, you can dynamically map the precision queues to direct a call to the agent who best matches the caller's precise needs. Precision queues are the key components of precision routing.

To configure Precision Routing, you must do the following:

1. Create attributes. Attributes are characteristics that can be assigned a True | False value or a Proficiency rating from 1 to 10.
2. Assign attributes to agents.
3. Create precision queues.
4. Create routing scripts.

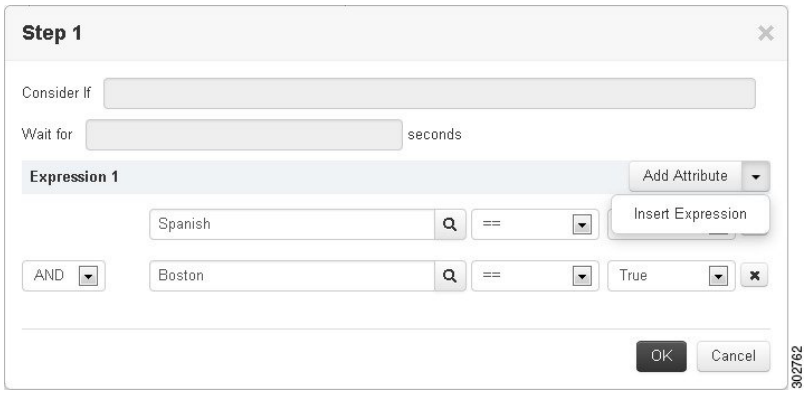
There is no need to add an agent to a precision queue; agents become members of precision queues automatically based on their attributes. If a precision queue requires an agent who lives in Boston, who speaks fluent Spanish, and who is proficient in troubleshooting a specific piece of equipment, an agent with the attributes *Boston = True*, *Spanish = True*, and *Repair = 10* is automatically part of the precision queue. A Spanish caller in Boston who needs help with equipment is routed to that agent.

A precision queue includes:

- **Terms:** A term compares an attribute against a value. For example, you can create the following term: Spanish == 10. The term of the attribute is the highest proficiency in Spanish.

  Each precision queue can have multiple attributes, and these attributes can be used in multiple terms. For example, to select an agent with a Spanish proficiency value between 5 and 10, you would create one term for Spanish > 5 and another for Spanish < 10.

- **Expressions:** An expression is a collection of one or more terms. The terms in an expression must share the same operator—they must all be AND or must all be OR relationships.



- **Steps:** A precision queue step is a time-based routing point within the precision queue. A step is a collection of one or more expressions.

  A step may also include wait time and a Consider If formula. Use wait time to assign a maximum amount of time to wait for an available agent. Use a Consider If formula to evaluate the step against predefined criteria, for example, another queue.

Administrators can see and manage attributes. Supervisors can configure attributes for their supervised agents on the Attributes tab of the Agents tool.

Skill Groups or Precision Queues?

Should you use skill groups or precision queues for the routing needs of your organization? This section distinguishes the two methods.

Use a Skill Group

A skill group represents a competency or responsibility. For example, it could be a predefined collection of traits, such as salespeople who are in charge of selling to England. The skill group could be called “English sales”. If you wanted to divide the agents in this group into two types of proficiencies (perhaps based on experience), you would need to set up two separate skill groups; for example, English Sales 1 and English Sales 2. You would then associate an agent with one of them, based on the agent's proficiency. Do this by accessing the skill group and locating the agent that you want to add to it (or add that skill group to the agent). To summarize, creating a skill group involves first building a concept of what combinations of traits you want for each agent, like English Sales 2.

Use a Precision Queue

In contrast to skill groups, a precision queue breaks down attribute definitions to form a collection of agents at an *attribute* level. The agents that match the attribute level of the precision queue become associated with that precision queue.

With precision queues, the preceding English sales example involves defining the attributes English and Sales, and associating agents that have those traits to them. The precision queue English Sales would dynamically

map all those agents that had those traits to the precision queue. In addition, you can define more complex proficiency attributes to associate with those agents. This would allow you to build, in a single precision queue, multiple proficiency searches like English language proficiency 10 and sales proficiency 5.

To break down the precision queue example into skill groups, you would need to set up two separate skill groups: English language proficiency 10 and sales proficiency 5. With precision queues, you can refine agents by attributes. With skill groups, you define a skill group and then assign agents to it.

Decide on Skill Groups or a Precision Queue

Precision routing enhances and can replace traditional routing. Traditional routing looks at all of the skill groups to which an agent belongs and defines the hierarchy of skills to map business needs. However, traditional routing is restricted by its single-dimensional nature.

Precision routing provides multidimensional routing with simple configuration, scripting, and reporting. Agents are represented through multiple attributes with proficiencies so that the capabilities of each agent are accurately exposed, bringing more value to the business.

If your routing needs are not too complex, consider using one or two skill groups. However, if you want to conduct a search involving as many as ten different proficiency levels in one easily managed queue, use precision queues.

Attributes

Attributes identify a call routing requirement, such as language, location, or agent expertise. You can create two types of attributes: Boolean or Proficiency.

When you create a precision queue, you identify which attributes are part of that queue and then implement the queue in a script. When you assign a new attribute to an agent and the attribute value matches the precision queue criteria, the agent is automatically associated with the precision queue.

You must take system limits into account when you assign attributes to agents, and satisfy both of the following conditions:

- A) an agent can have a maximum of 50 attributes

and

- B) an agent can belong to a maximum total of 50 combined precision queues and skill groups

Failure to meet both of these conditions will result in an unsuccessful configuration operation.

For example, if a particular attribute is used in many precision queues, and that attribute is assigned to an agent, that agent belongs to all of those precision queues. It is therefore possible to exceed condition B by assigning just a few attributes to an agent, if those attributes are used in many precision queues.

It is therefore prudent to plan carefully and to keep system limits in mind when creating attributes and adding them to precision queues.

Navigate to **Unified CCE Administration** > **Organization** > **Skills** > **Attributes** to configure attributes.

Administrators can see and manage attributes. Supervisors can configure attributes for their supervised agents on the Attributes tab of the Agents tool.

Precision Queue Call Flow Example

At a high level, consider a 5-step precision queue with a Consider If formula for *Caller is Premium Member* attached to the Step 1:

- Step 1 - Attribute: Skill > 8 - Consider If: Caller is Premium Member
- Step 2 - Attribute: Skill > 6
- Step 3 - Attribute: Skill > 4
- Step 4 - Attribute: Skill > 3
- Step 5 - Attribute: Skill >= 1

Caller John, who is not a premium customer, calls 1-800-repairs. John's call is routed to this precision queue.

- Since John is not a premium customer, he is immediately routed out of Step 1 (because of the Consider If on Step 1) and into Step 2 where he waits for his call to be answered.
- After the Step 2 wait time has expired, John's call moves to Step 3 to wait for an agent.
- After the Step 3 wait time has expired, John's call moves to Step 4 to wait for an agent.
- When it arrives at Step 5, John's call will wait indefinitely for an available agent. This step cannot be avoided by any call because there is no routing logic past this.

The overarching idea is that customer will use each successive step to expand the pool of available agents. Eventually, when you reach the "last" step (the step with the highest number), the call is waiting in a potentially very large pool of agents. With each extra step, the chances of the call being handled increase. This also puts the most valuable and skilled agents in the earlier precision queue steps. Calls come to them first before moving on the less appropriate agents in later steps.

Note When two or more agents have the same proficiently level for the attributes the PQ step leverages the Longest Available Agent (LLA).

Scripts for Precision Queues

To implement Precision Routing in your contact center, you must create scripts.

You can create and use configured (static) and dynamic precision queue nodes in your scripts.

- Static precision queue nodes target a single, configured precision queue. When the script utilizes a single precision queue, use static precision queues.
- Dynamic precision queue nodes are used to target one or more previously configured precision queues. Use dynamic precision queues when you want a single routing script for multiple precision queues (for example, when the overall call treatment does not vary from one precision queue to another). Dynamic precision queues can simplify and reduce the overall number of routing scripts in the system.

Precision Queue Script Node

Use the Precision Queue script node to queue a call based on caller requirements until an agent with desired proficiency become available. This node contains multiple agent selection criteria which are separated into steps.

A single call can be queued on multiple precision queues. If an agent becomes available in one of the precision queues, the call is routed to that resource. You cannot reference multiple precision queues with a single Precision Queue node. However, you can execute multiple Precision Queue nodes sequentially to achieve this.

The Precision Queue node includes a Priority field, which sets the initial queuing priority for the calls processed through this node versus other calls queued to the other targets using different nodes. The priority is expressed as an integer from 1 (top priority) to 10 (least priority). The default value is 5.

If more than one call is queued to a precision queue when an agent becomes available, the queued call with the lowest priority number is routed to the target first. For example, assume an agent in a precision queue becomes available and two calls are queued to that precision queue. If one call has priority 3 and the other has priority 5, the call with priority 3, the lower value, is routed to the precision queue while the other call continues to wait. If the priorities of the two calls are same, then the call queued first is routed first.

VRU (voice response unit) script instructions are not sent to the VRU. If a call enters the precision queue node and no resource is available, the call is queued to the precision queue and the node transfers the call to the default VRU, if the call is not already on a VRU. The script flow then exits immediately through the success branch. The script should then continue with a run external script node to instruct the VRU what to do while holding the call until an agent becomes available. Typically, this invokes a network VRU script that plays music-on-hold, possibly interrupted on a regular basis with an announcement. The script flow can also use other queuing nodes to queue the same call to other targets, for example, Queue to Skill Group and Queue to Agent.

Note Non-voice tasks can also be picked or pulled out of turn from queues, not necessarily based on the priority of the call. Such non-voice tasks that are picked or pulled by a specific agent, require a Pick/Pull node to be used in the ICM script. However, the agents belonging to other skill groups or precision queues can also pick tasks that may be queued in Skill Groups or Precision Queues other than their own. These are denoted by **Picked by another Skillgroup/PQ** or **Pulled by another Skillgroup/PQ** monitor labels, when viewing the scripts in monitor mode.

Queuing Behavior of the Precision Queue Node

Precision queues internally are configured with one or more time-based steps, each with a configured wait time. After a call is queued, the first step begins and the timer starts. This occurs although the execution path of the script exited the success node and a new node may be targeted (for example, Run Ext. Script).

If the timer for the first step expires, control moves to the second step (assuming one exists), and so on. As long as the call remains in queue and there are steps left to execute, the call internally continues to move between steps regardless of the path the call takes after it leaves the precision queue node. If a call is queued to two or more precision queues, the call internally walks through the steps for each precision queue in parallel. After the call reaches the last step on a precision queue, it remains queued on that step until the call is routed, abandoned, or ended.

If there is an update to the precision queue definition, then all queued calls in the precision queue are re-evaluated and the execution begins again from the first step.

For example, consider the wait time for an ongoing call at step 1 to be 1080 seconds, of which 1000 seconds has already elapsed. Now, suppose the wait time is changed to 900 seconds, then the wait time for this call is also reset to 900 seconds, even though only 80 more seconds are left to move to the next step.

Initial Setup

When you configure precision queues associated with a large number of agents, the system avoids potential overload conditions by updating the agent associations as system resources allow. Updates may take a few minutes. If you submit multiple configuration updates, the system has a threshold of five concurrent configuration updates, and will reject any updates that exceed the threshold.

Add Attributes

Procedure

Step 1 Navigate to **Unified CCE Administration** > **Organization** > **Skills** > **Attributes**.

Step 2 In the **List of Attributes** window, click **New**.

Step 3 Complete the following fields on the **General** tab:

Field	Required	Description
Name	yes	Type a unique attribute name. For example, to create an attribute for mortgage insurance, type *mortgage*.
Description	no	Enter a maximum of 255 characters to describe the attribute.
Type	no	Select the type: Boolean or Proficiency.
Default	no	Select the default (True or False for Boolean, or a number from 1 to 10 for Proficiency).

Step 4 Click **Save**.

Search for Agents

The Search field in the Agents tool offers an advanced and flexible search.

Click the + icon at the far right of the **Search** field to open a popup window, where you can:

- Select to search for agents only, supervisors only, or both.
- Select to search for all agents or only ECE enabled agents.
- Enter a username, agent ID, first or last name, or description to search for that string.

- Enter one or more site names separated by spaces. (Site is an OR search.)
- Enter one or more peripheral set names separated by spaces (Peripheral Set is an OR search). The search is case-insensitive and does not support partial matches.

Note Search by department is available only when departments are configured.

Assign Attributes to Agents

Procedure

Step 1 With the selected agent displayed, click the **Attributes** tab.

Step 2 Complete the **Attributes** tab:

This tab shows the attributes associated with this agent and their current values.

Click **Add** to open a popup list of all attributes, showing the name and current default value for each.

a) Click the attributes you want to add for this agent.
b) Set the attribute value as appropriate for this agent.

Add Precision Queue

Procedure

Step 1 Navigate to **Unified CCE Administration** > **Organization** > **Skills** > **Precision Queues**.

This opens a **List of Precision Queues** window showing all precision queues that are currently configured.

Step 2 Click **New** to open the **New Precision Queue** window. Complete the fields.

Name	Required	Description
Description	no	Enter up to 255 characters to describe the precision queue.
Media Routing Domain	no	MRDs organize how requests for media are routed. The system routes calls to skill groups or precision queues that are associated with a particular communication medium; for example, voice or email. This field defaults to *Cisco_Voice*.

Name	Required	Description
Service Level Type	yes	Select the service level type used for reporting on your service level agreement. Service level type indicates how calls that are abandoned before the service level threshold affect the service level calculation. • **Ignore Abandoned Calls** (the default): Select this option if you want to exclude abandoned calls from the service level calculation. • **Abandoned Calls have Negative Impact:** Select this option if you want only those calls that are answered within the service level threshold time to be counted as treated calls. The service level is negatively affected by calls that abandon within the service level threshold time. • **Abandoned Calls have Positive Impact:** Select this option if you consider a call that is abandoned within the service level threshold time as a treated call. With this configuration, abandoned calls have a positive impact on the service level.
Service Level Threshold	yes	Enter the time in seconds that calls are to be answered based on your service level agreement, from 0 to 2,147,483,647. The time that you enter in this field is used to report on service level agreements and does not affect how long a call remains in a precision queue. The length of time a call remains in a step is determined by the wait time for each individual step.

Name	Required	Description
Agent Order	yes	Select an option to determine which agents receive calls from this queue. The ordering of agents does not dictate the agents who are selected into a Precision Queue step. Agents are included or excluded based on the conditions specified for the step. • **Longest Available Agent** (the default): The default method of agent ordering for a precision queue. The call is delivered to the agent who has been in the available (or ready) state the longest. • **Most Skilled Agent:** The call is delivered to the agent who has the highest competency sum from all the attributes pertinent to the Precision Queue step. In an agent-rich environment, this can mean that more competent agents would be utilized more than less competent agents. • **Least Skilled Agent:** The call is delivered to the agent who has the lowest competency sum from all the attributes pertinent to the Precision Queue step.
Bucket Intervals	no	Select the bucket interval whose bounds are to be used to measure the time slot in which calls are answered. The field defaults to the system default. To select a different bucket interval:

Step 3 Click the numbered Step Builder link (Step 1, Step 2, and so on) to build a precision queue step in the **Step Builder** popup window.

Step 4 When you have finished adding, click **Save**.

Consider If Formula for Precision Queue

If you are not on the last step of the precision queue, then you can enter a *Consider If* formula for that step. A Consider If formula evaluates a call (within a step) against additional criteria. Each time a call reaches a step with a Consider If expression, the expression is evaluated. If the value for the expression returns as true, the call is considered for the step. If the value returns as false, the call moves to the next step. If no expression is provided for a step, the step is always considered for calls.

To add a Consider If formula, type the formula into the **Consider If** box. Alternatively, you can use the Script Editor to build the formula and then copy and paste it into the **Consider If** box. Objects used in Consider If formulas are case-sensitive. All Consider If formulas that you add to a precision queue must be valid. If you add an invalid formula, you cannot save the precision queue. To ensure that the formula is valid, use Script Editor to build and validate the formula.

Only the following scripting objects are valid in a Consider If formula:

- Call
- PQ
- Skillgroup
- ECC
- PQ Step
- Call Type
- Custom Functions (You can create custom functions in Script Editor.)

It is possible that a valid Consider If formula can become invalid. For example, if you delete an object used in the formula after you create or update the precision queue, the formula is no longer valid.

Consider If Formula Examples

- **PQ.PQ1.LoggedOn > 1**--Evaluates whether there is more than one agent logged in to this queue.
- **CallType.CallType1.CallsRoutedToday > 100**--Evaluates whether more than 100 calls of this call type were routed today.
- **PQStep.PQ1.1.RouterAgentsLoggedIn > 1**--Evaluates whether there is more than one router agent logged in to this queue for Step 1.
- **CustomFunction(Call.PeripheralVariable1) > 10**--Evaluates whether this formula using a custom function returns a value greater than 10.

Build Precision Queue Steps

Every precision queue must have a step, and every step must have an Expression. An Expression is a collection of attribute terms.

Procedure

Step 1 Click the numbered step link in the **Steps** panel (Step 1, Step 2, and so on).

The step number popup window opens.

Step 2 Build the first step as follows.

a) Click the **magnifying glass** icon to the right of the Select Attribute field in the Expression 1 panel.
b) Select an attribute from the list.
c) Use the two **Select** fields to establish the terms of the attribute. Click the first **Select** field to choose an operator.

- For Boolean attributes, choices are the operators for Equal and Not Equal.
- For Proficiency attributes, choices are the operators for True, False, Less Than, Less Than or Equal To, Greater Than, and Greater Than or Equal To.

d) Click the second **Select** field to choose a value.

- For Boolean attributes, values are True and False.
- For Proficiency attributes, values are numbers from 1 to 10.

Your selection creates an attribute term for the Expression.

Step 3 To add a second attribute to the first Expression, click **Add Attribute** in the **Expression 1** row.

a) Select **AND** or **OR** to establish the relationship between the first and second attributes.
b) Repeat steps 2b, 2c, and 2d.

Step 4 Continue to add attributes to Expression 1.

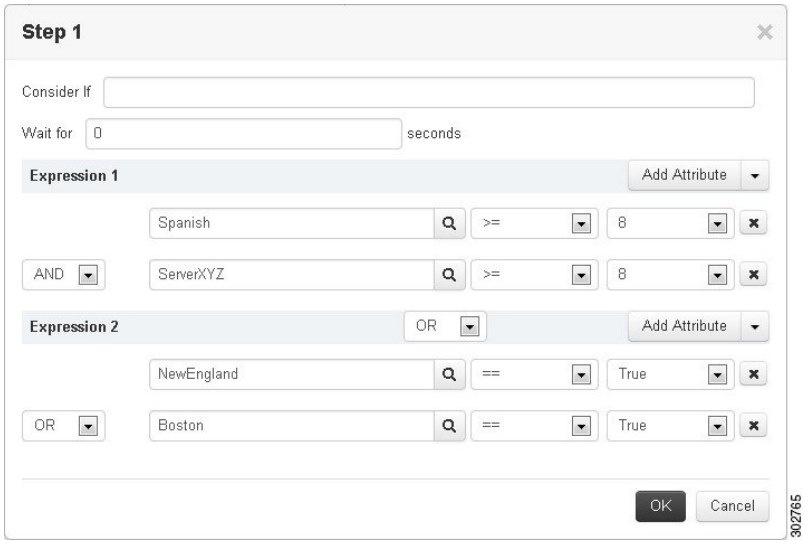
All attributes within an expression must be joined by the same logical operator. They must all be ANDs, or they must all be ORs.

Step 5 To add a second Expression, click the **Add Attribute** drop-down in the **Expression 1** row and select **Add Expression**.

Step 6 Select **AND** or **OR** to establish the relationship between the first and second Expressions.

Step 7 Add attributes to Expression 2.

Step 8 Continue to add Expressions as needed.



In this example, a Spanish caller located in the Boston area needs an onsite visit from a technician to repair his ServerXYZ. An ideal agent should be fluent in Spanish and have the highest proficiency in ServerXYZ. This can be seen in Expression 1. Expression 2 allows us to specify that the selected agent must also be from either Boston or the New England area.

Step 9 When you have completed the step, click **OK** to add it to the precision queue.

Step 10 To build the next step, click **Add Step**.

Each successive step is prepopulated with the Expressions and attributes of its predecessor. Decrease the attribute qualifications and competencies in successive steps to lower the bar such that the pool of acceptable agents increases.

Step 11 When you have created all steps, you can open any step *except the last* and enter values in the **Consider if** and **Wait for** fields.

- **Consider if** is a formula that evaluates a call within a step against additional criteria. (See Consider If Formula for Precision Queue, on page 120 for more information about Consider If.)
- **Wait for** is a value in seconds to wait for an available agent. A call will queue at a particular step and wait for an available agent matching that step criteria until the number of seconds specified. A blank wait time indicates that the call will proceed immediately to the next step if no available agents match the step criteria. Wait time defaults to 0 and can take a value up to 2147483647.

Configure a Static Precision Queue

Procedure

Step 1 In the **Precision Queue Properties** dialog box, select the **Statically** option.

Step 2 From the list, select a precision queue to which to route all calls that enter this node.

Step 3 In the **Priority selection** box, select the initial queuing priority for calls processed through this node. You can select from 1 - 10. The default is 5.

Step 4 Check the **Enable target requery** check box to enable the requery feature for calls processed through this node.

Step 5 Check the **Wait if Agents Not Logged In** check box.

If this check box is selected and the agents associated with this step are not logged in, then the router waits for the time that is configured for that step. Whereas, if this check box is not selected, the router does not wait on any step.

Note The router waits indefinitely on the last step, irrespective of the selection of this check box.

Step 6 To edit a precision queue, select a precision queue from the list, and then click **Edit Precision Queue**.

Configure a Dynamic Precision Queue

Procedure

Step 1 In the **Precision Queue Properties** dialog box, select the **Dynamically** option.

Step 2 In the **Priority selection** section, select the initial queuing priority for calls processed through this node. You can select from 1 - 10. The default is 5.

Step 3 Check the **Enable target requery** check box to enable the requery feature for calls processed through this node.

Step 4 Check the **Wait if Agents Not Logged In** check box.

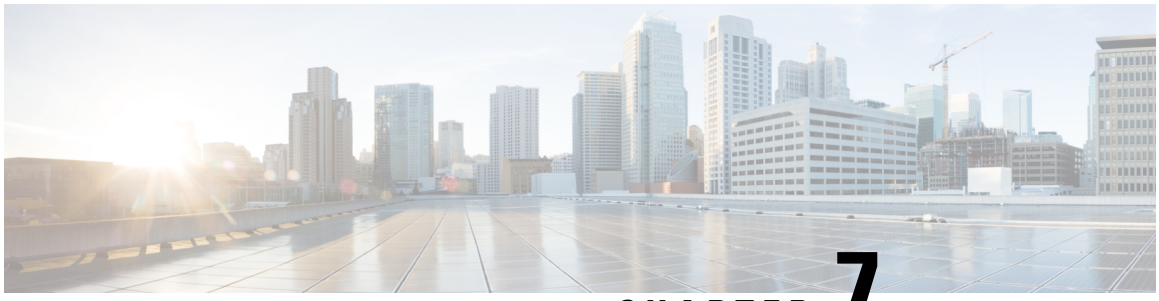
If this check box is selected and the agents associated with this step are not logged in, then the router waits for the time that is configured for that step. Whereas, if this check box is not selected, the router does not wait on any step.

Note The router waits indefinitely on the last step, irrespective of the selection of this check box.

Step 5 Select a queue option:

- To dynamically route calls that enter this node to a precision queue name, select the **Precision Queue Name** option.
- To dynamically route calls that enter this node to a precision queue ID, select the **Precision Queue ID** option.

Step 6 Click **Formula Editor** to create a formula that determines the precision queue name or ID to which to route calls.



CHAPTER 7

Single Sign-On

Single Sign-On

Single sign-on (SSO) is an authentication and authorization process. (Authentication proves that you are the user you say that you are, and authorization verifies that you are allowed to do what you want to do.) SSO allows you to sign in to one application and then securely access other authorized applications without a prompt to resupply user credentials. SSO permits Cisco supervisors or agents to sign on only once with a username and password. Supervisors and agents gain access to all of their Cisco browser-based applications and services within a single browser instance. By using SSO, Cisco administrators can manage all users from a common user directory and enforce password policies for all users consistently.

Note Before enabling SSO in Unified CCE, ensure to sign in to the Cisco Unified Intelligence Center OAMP interface and perform the Unified CCE User Integration operation (Cluster Configuration > UCCE User Integration) once manually to import the Supervisors with the required roles.

SSO is an optional feature whose implementation requires you to enable the HTTPS protocol across the enterprise solution.

You can implement single sign-on in one of these modes:

- **SSO** - Enable *all* agents and supervisors in the deployment for SSO.

- **Hybrid** - Enable agents and supervisors *selectively* in the deployment for SSO. Hybrid mode allows you to phase in the migration of agents from a non-SSO deployment to an SSO deployment and enable SSO for local PGs. Hybrid mode is useful if you have third-party applications that don't support SSO, and some agents and supervisors must be SSO-disabled to sign in to those applications.
- **Non-SSO** - Continue to use existing Active Directory-based and local authentication, without SSO.

SSO uses Security Assertion Markup Language (SAML) to exchange authentication and authorization details between an identity provider (IdP) and an identity service (IdS). The IdP authenticates based on user credentials, and the IdS provides authorization between the IdP and applications. The IdP issues SAML assertions, which are packages of security information transferred from the IdP to the service provider for user authentication. Each assertion is an XML document that contains trusted statements about a subject including, for example, username and privileges. SAML assertions are digitally signed to ensure their authenticity.

The IdS generates an authentication request (also known as a SAML request) and directs it to the IdP. SAML does not specify the method of authentication at the IdP. It may use a username and password or other form of authentication, including multi-factor authentication. A directory service such as LDAP or AD that allows you to sign in with a username and a password is a typical source of authentication tokens at an IdP.

Prerequisites

The Identity Provider must support Security Assertion Markup Language (SAML) 2.0. See the *Compatibility Matrix* for your solution at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.htmlhttps://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html for details.

Contact Center Enterprise Reference Design Support for Single Sign-On

Unified CCE supports single sign-on for these reference designs:

- 2000 Agents
- 4000 Agents
- 12000 Agents
- 24000 Agents
- Contact Director (Maximum of 24000 agents, Each target system must include a dedicated Cisco IdS deployment.)

Coresidency of Cisco Identity Service by Reference Design

Reference Design	Unified CCE
2000 Agent	Cisco IdS is coresident with Unified Intelligence Center and Live Data on a single VM.
4000 Agent	Standalone Cisco IdS VM
12000 Agent	Standalone Cisco IdS VM

Reference Design	Unified CCE
24000 Agent	Standalone Cisco IdS VM

Single Sign-On Support and Limitations

Note the following points that are related to SSO support:

- To support SSO, enable the HTTPS protocol across the enterprise solution.
- SSO supports agents and supervisors only. SSO support is not available for administrators in this release.
- In the 12,000 Agent Reference Design, a maximum of 12,000 agents use SSO at one time.
- SSO supports multiple domains with federated trusts.
- SSO supports only contact center enterprise peripherals.
- SSO support is available for Agents and Supervisors that are registered to remote or main site PG in global deployments.

Note the following limitations that are related to SSO support:

- SSO support is not available for third-party Automatic Call Distributors (ACDs).
- The SSO feature does not support Cisco Finesse IP Phone Agent (FIPPA).
- The SSO feature does not support Cisco Finesse Desktop Chat.

Allowed Operations by Node Type

The Cisco IdS cluster contains a publisher and a subscriber node. A publisher node can perform any configuration and access token operations. The operations that a subscriber node can perform depends on whether the publisher is connected to the cluster.

This table lists which operations each type of node can perform.

Table 7: Single Sign-On Allowed Operations

Operation	Allowed on Publisher	Allowed on Subscriber
Upload IdP metadata	Always	Never
Download SAML SP metadata	Always	Never
Regenerate SAML Certificate	Always	Never
Regenerate Token Encryption/Signing Key	Always	Never
Update AuthCode/Token Expiry	Always	Only when publisher is connected
Enable/Disable Token Encryption	Always	Only when publisher is connected

Operation	Allowed on Publisher	Allowed on Subscriber
Add/Update/Delete Cisco IdS client configuration	Always	Only when publisher is connected
View Cisco IdS client configuration	Always	Always
View Cisco IdS status	Always	Always
Set Troubleshooting Log Level	Always	Always
Set Remote Syslog server	Always	Always

Single Sign-On Log Out

For a complete logout from all applications, sign out of the applications and close the browser window. In a Windows desktop, log out of the Windows account. In a Mac desktop, quit the browser application.

Note Users enabled for single sign-on are at risk of having their accounts misused by others if the browser is not closed completely. If the browser is left open, a different user can access the application from the browser page without entering credentials.

Single Sign-On Configuration Flow

Note Synchronize the time in Cisco IdS and IdP for SSO to work effectively. It is recommended that the Cisco IdS and IdP are time-synchronized using NTP Server.

Note It is recommended that the Administrator configures SSO from the IdS publisher node.

1. Install the appropriate release of the CCE solution. For more information, see Cisco Unified Contact Center Enterprise Installation and Upgrade Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html
2. Install the Cisco Identity Service (Cisco IdS). For more information, see Cisco Unified Contact Center Enterprise Installation and Upgrade Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html
3. Configure an Identity Provider (IdP).
4. Configure System Inventory.
5. Configure the Cisco IdS.
6. Register and test SSO-compatible components with the Cisco IdS.

7. Choose the SSO mode.
8. Enable multiple users at once for SSO by using the SSO migration tool, or enable users one at time by using the configuration tools.

Related Topics

Configure the Cisco Identity Service, on page 141
Configure an Identity Provider (IdP), on page 146
Install Cisco Identity Service Standalone Deployment, on page 129
Migrate Agents and Supervisors to Single Sign-On Accounts, on page 157
Register Components and Set Single Sign-On Mode, on page 155
Set up the System Inventory for Single Sign-On, on page 152
Single Sign-On Migration and the Configuration Manager, on page 159

Single Sign-On Installation

Complete the installation or upgrade procedure. For more information, see Cisco Unified Contact Center Enterprise Installation and Upgrade Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Installation Task Flow for Cisco Identity Service

You can install Cisco Identity Service as a standalone or coresident deployment.

Task	See
Install Cisco Identity Service Standalone Deployment (4000, 8000, 12000 Agent Deployment) or Install Coresident Deployment (2000 Agent Deployment)	Install Cisco Identity Service Standalone Deployment, on page 129 or Install Coresident Deployment (Cisco Unified Intelligence Center with Live Data and IdS), on page 136

Install Cisco Identity Service Standalone Deployment

Follow this sequence of tasks to install the Cisco Identity Service (Cisco IdS) standalone deployment.

Sequence	Task
1	Verify that you created a separate virtual machine for the IdS publisher node and the IdS subscriber node. See Set Up Virtual Machines, on page 130.
2	Install IdS publisher node. See Install Publishers/Primary Nodes of VOS-Based Contact Center Applications, on page 137
3	Set IdS subscriber node. See Set IdS Subscriber Node, on page 133

Sequence	Task
4	Install IdS subscriber node. See Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 138
5	Upgrade VMware Tools. See Install VMware Tools for VOS, on page 136

Set Deployment Type in Unified CCE Administration Configuration

Before you install or upgrade, you must set the deployment type.

Procedure

Step 1 Navigate to **Unified CCE Administration** > **System** > **Deployment**.

Step 2 Select your deployment from the drop-down menu and click **Next**.

Set Up Virtual Machines

Verify Datastores

Before you install the VMs, verify that the datastore is in place. The type of datastore depends on the type of server on which you deploy the VMs. For example, UCS-B servers use a SAN datastore and UCS-C servers use DAS datastores.

For more information, see the VMware documentation at https://www.vmware.com/support/pubs/.

For more information, see *Virtualization for Unified Contact Center Enterprise* at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html.

Download Unified CCE OVA Files

The Unified CCE Open Virtualization Format (OVA) files define the basic structure of the corresponding VMs that are created. The structure definition includes the CPU, RAM, disk space, reservation for CPU, and reservation for memory.

Before you begin

You must have a valid service contract associated with your Cisco.com profile.

Procedure

Step 1 Go to the Unified CCE Download Software page on Cisco.com.

Step 2 Click **Download** to download and save the appropriate OVA file to your local hard drive. When you create VMs, you select the OVA required for the application.

Create Virtual Machines from OVA Files

To create virtual machines (VMs) from the OVA files, complete the following procedure.

Note ECE requires a second virtual hard drive on its VM. The OVA creates one virtual hard drive. Create a second hard drive of an appropriate size for your solution requirements.

Procedure

Step 1 Select the Host in the vSphere client.

Step 2 Choose **File** > **Deploy OVF Template**.

Step 3 Browse to the location on your local drive where you stored the OVA. Click **Open** to select the file. Click **Next.**

Step 4 Click **Next** at the **OVF Template Details** page.

Step 5 Enter the virtual machine name. It cannot contain spaces or special characters. Enter a maximum of 32 characters. Click **Next**.

Step 6 On the **Name and Location** page, enter a name of your choice in the **Name** field. Click **Next.**

Important After the VM is created, you cannot rename it.

Step 7 On the **Deployment Configuration** page, select the applicable configuration from the drop-down list. Click **Next**.

Step 8 Choose a data store on which to deploy the new virtual machine. Click **Next.**

Note Some deployments require two data stores.

Step 9 On the **Disk Format** page, choose **Thick provisioned Eager Zeroed format** for the virtual disk format. Click **Next**.

Note **Thick provisioned Lazy Zero** is also supported, but **Thin provisioned** is not supported.

Step 10 Confirm that the **Network Mapping** page is correct:

a) Public network adapter to Public network
b) Private network adapter to Private network

Note For some deployments, only one network interface is available.

Step 11 Click **Finish.**

Step 12 At the Successfully Completed message, click **Close**.

Note For more information, see *Virtualization for Unified Contact Center Enterprise* at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html.

Install Publishers/Primary Nodes of VOS-Based Contact Center Applications

Before you begin

DNS Configuration is mandatory for installation of Cisco Unified Communications Manager, Cisco Unified Intelligence Center, Cisco Finesse and Cisco Identity Service (IdS). To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

Procedure

Step 1 Create a virtual machine for your VOS-based contact center application using the OVA.

Step 2 Mount the ISO image for the software to the virtual machine.

Step 3 Select the virtual machine, power it on, and open the console.

Step 4 Follow the Install wizard, making selections as follows:

a) In the **Disk Found** screen, click **OK** to begin the verification of the media integrity.

b) In the **Success** screen, select **OK**.

c) In the **Product Deployment Selection** screen:

- For the Progger (Lab only) or 2000 agent reference design, choose the coresident deployment option **Cisco Unified Intelligence Center with Live Data and IdS**, and then select **OK**. The **Cisco Unified Intelligence Center with Live Data and IdS** option installs Cisco Unified Intelligence Center with Live Data and Cisco Identity Service (IdS) on the same server.
- For all other deployments, select one of the standalone install options. For example, select **Cisco Unified Intelligence Center**, **Live Data**, or **Cisco Identity Service (IdS)**. Then select **OK**.

d) In the **Proceed with Install** screen, select **Yes**.

e) In the **Platform Installation Wizard** screen, select **Proceed**.

f) In the **Apply Patch** screen, select **No**.

g) In the **Basic Install** screen, select **Continue**.

h) In the **Timezone Configuration** screen, use the down arrow to choose the local time zone that most closely matches where your server is located. Select **OK**.

Note For Live Data servers, use the same timezone for all the nodes.

i) In the **Auto Negotiation Configuration** screen, select **Continue**.

j) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units.

k) In the **DHCP Configuration** screen, select **No**.

l) In the **Static Network Configuration** screen, enter static configuration values. Select **OK**.

m) In the **DNS Client Configuration** screen, click **Yes** to enable DNS client.

n) Enter your DNS client configuration. Select **OK**.

o) In the **Administrator Login Configuration** screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.

p) In the **Certificate Information** screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.

q) In the **First Node Configuration** screen, select **Yes**.

r) In the **Network Time Protocol Client Configuration** screen, enter a valid NTP server IP address and select **OK**.
s) In the **Security Configuration** screen, enter the security password and select **OK**.
t) In the **SMTP Host Configuration** screen, select **No**.
u) In the **Application User Configuration** screen, enter the application username. Enter, and confirm the application user password. Select **OK**.
v) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and runs unattended.

- There is a reboot in the middle of the installation.
- The installation ends at a sign-in prompt.

Step 5 Unmount the ISO image.

Set IdS Subscriber Node

You must provide the publisher node the address of the subscriber node. You do this with the **set ids subscriber** command.

Procedure

Step 1 Log in to your publisher IdS node.

Step 2 Run the following command to set the subscriber node:

set ids subscriber *name*
name
Specifies the hostname or ip address of the IdS subscriber node address.

What to do next

You can use these Cisco IdS CLI commands only in an IdS standalone deployment. You run these commands on the IdS publisher node.

Required Minimum Privilege Level: Ordinary

Use this command to show IdS subscriber node information.

show ids subscriber

There are no required parameters.

Required Minimum Privilege Level: Advanced

Use this command to unset IdS subscriber node configuration.

unset ids subscriber

There are no required parameters.

Identity Service CLI Commands

You can use these Cisco IdS CLI commands only in an IdS standalone deployment. You run these commands on the IdS publisher node.

set ids subscriber

Required Minimum Privilege Level: Advanced

Use this command to set the single sign-on Identity Service (IdS) subscriber node address .

Command Syntax
set ids subscriber *name*
name
Specifies the hostname or ip address of the IdS subscriber node address.

unset ids subscriber

Required Minimum Privilege Level: Advanced

Use this command to unset IdS subscriber node configuration.

unset ids subscriber

There are no required parameters.

show ids subscriber

Required Minimum Privilege Level: Ordinary

Use this command to show IdS subscriber node information.

show ids subscriber

There are no required parameters.

Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications

Note This task is required for installation of the subscriber/secondary nodes of the three VOS-based contact center applications: Cisco Finesse, Cisco Unified Communications Manager, and Cisco Unified Intelligence Center.

Before you begin

DNS Configuration is mandatory for installation of Cisco Unified Communications Manager, Cisco Unified Intelligence Center, and Cisco Finesse. To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

Before you install the subscriber/secondary nodes, you must install the publisher/primary nodes and configure the clusters.

Procedure

Step 1 Create a virtual machine for your VOS-based contact center application using the OVA.

Step 2 Mount the ISO image for the software to the virtual machine.

Step 3 Select the virtual machine and power it on, and open the console.

Step 4 Follow the Install wizard, making selections as follows:

a) In the **Disk Found** screen, click **OK** to begin the verification of the media integrity.
b) In the **Success** screen, select **OK**.
c) In the **Product Deployment Selection** screen:

- For the Progger (Lab only) or 2000 agent reference design, choose the coresident deployment option **Cisco Unified Intelligence Center with Live Data and IdS**, and then select **OK**. The **Cisco Unified Intelligence Center with Live Data and IdS** option installs Cisco Unified Intelligence Center, Live Data, and Cisco Identity Service (IdS) on the same server.
- For all other deployments, select one of the standalone install options. For example, select **Cisco Unified Intelligence Center**, **Live Data**, or **Cisco Identity Service (IdS)**. Then select **OK**.

Step 5 Follow the Install wizard, making selections as follows:

a) In the **Proceed with Install** screen, select **Yes**.
b) In the **Platform Installation Wizard** screen, select **Proceed**.
c) In the **Apply Patch** screen, select **No**.
d) In the **Basic Install** screen, select **Continue**.
e) In the **Timezone Configuration** screen, use the down arrow to choose the local time zone that most closely matches where your server is located. Select **OK**.

Note For Live Data servers, use the same timezone for all the nodes.

f) In the **Auto Negotiation Configuration** screen, select **Continue**.
g) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units.
h) In the **DHCP Configuration** screen, select **No**.
i) In the **Static Network Configuration** screen, enter static configuration values. Select **OK**.
j) In the **DNS Client Configuration** screen, click **Yes** to enable DNS client.
k) In the **Administrator Login Configuration** screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.
l) In the **Certificate Information** screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.
m) In the **First Node Configuration** screen, select **No**.
n) In the warning screen, select **OK**.
o) In the **Network Connectivity Test Configuration** screen, select **No**.
p) In the **First Node Access Configuration** screen, enter the host name and IP address of the first node. Enter and confirm the security password. Select **OK**.
q) In the **SMTP Host Configuration** screen, select **No**.
r) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and runs unattended.

- There is a reboot in the middle of the installation.

- The installation ends at a sign-in prompt.

Step 6 Unmount the ISO image.

Install VMware Tools for VOS

To install or upgrade VMware Tools using VOS, perform the following steps:

Procedure

Step 1 Ensure that your virtual machine is powered on.

Step 2 Right-click the VM menu. Select **Guest** > **Install / Upgrade VMware tools** .

Step 3 Choose the interactive tools update and press **OK**.

Step 4 Open the console and log in at the command prompt.

Step 5 Enter the command **utils vmtools refresh** and confirm.
The server automatically reboots twice.

Step 6 After reboot, check the **Summary** tab for the VM to verify that the VMware Tools version is current. If it is not current, reboot the VM and check the version again.

The process takes a few minutes. After the process completes, the tools are listed as Running (Current) on the VM's Summary tab in vSphere.

Install Coresident Deployment (Cisco Unified Intelligence Center with Live Data and IdS)

Follow this sequence of tasks to install the coresident deployment (Cisco Unified Intelligence Center with Live Data and IdS).

Sequence	Task
1	Set Deployment Type in Unified CCE Administration Configuration, on page 137
2	Install IdS publisher node. See Install Publishers/Primary Nodes of VOS-Based Contact Center Applications, on page 137
3	Install IdS subscriber node. See Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 138
4	Add Coresident (Cisco Unified Intelligence Center with Live Data and IdS) Machine Type to the System Inventory, on page 140
5	Upgrade VMware Tools. See Install VMware Tools, on page 140

Set Deployment Type in Unified CCE Administration Configuration

Before you install or upgrade IdS you must set the deployment type.

Procedure

Step 1 Navigate to **Unified CCE Administration** > **System** > **Deployment**.

Step 2 Select your deployment from the drop-down menu and click **Next**.

Install Publishers/Primary Nodes of VOS-Based Contact Center Applications

Before you begin

DNS Configuration is mandatory for installation of Cisco Unified Communications Manager, Cisco Unified Intelligence Center, Cisco Finesse and Cisco Identity Service (IdS). To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

Procedure

Step 1 Create a virtual machine for your VOS-based contact center application using the OVA.

Step 2 Mount the ISO image for the software to the virtual machine.

Step 3 Select the virtual machine, power it on, and open the console.

Step 4 Follow the Install wizard, making selections as follows:

a) In the **Disk Found** screen, click **OK** to begin the verification of the media integrity.

b) In the **Success** screen, select **OK**.

c) In the **Product Deployment Selection** screen:

- For the Progger (Lab only) or 2000 agent reference design, choose the coresident deployment option **Cisco Unified Intelligence Center with Live Data and IdS**, and then select **OK**. The **Cisco Unified Intelligence Center with Live Data and IdS** option installs Cisco Unified Intelligence Center with Live Data and Cisco Identity Service (IdS) on the same server.
- For all other deployments, select one of the standalone install options. For example, select **Cisco Unified Intelligence Center**, **Live Data**, or **Cisco Identity Service (IdS)**. Then select **OK**.

d) In the **Proceed with Install** screen, select **Yes**.

e) In the **Platform Installation Wizard** screen, select **Proceed**.

f) In the **Apply Patch** screen, select **No**.

g) In the **Basic Install** screen, select **Continue**.

h) In the **Timezone Configuration** screen, use the down arrow to choose the local time zone that most closely matches where your server is located. Select **OK**.

Note For Live Data servers, use the same timezone for all the nodes.

i) In the **Auto Negotiation Configuration** screen, select **Continue**.

j) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units.
k) In the **DHCP Configuration** screen, select **No**.
l) In the **Static Network Configuration** screen, enter static configuration values. Select **OK**.
m) In the **DNS Client Configuration** screen, click **Yes** to enable DNS client.
n) Enter your DNS client configuration. Select **OK**.
o) In the **Administrator Login Configuration** screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.
p) In the **Certificate Information** screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.
q) In the **First Node Configuration** screen, select **Yes**.
r) In the **Network Time Protocol Client Configuration** screen, enter a valid NTP server IP address and select **OK**.
s) In the **Security Configuration** screen, enter the security password and select **OK**.
t) In the **SMTP Host Configuration** screen, select **No**.
u) In the **Application User Configuration** screen, enter the application username. Enter, and confirm the application user password. Select **OK**.
v) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and runs unattended.

- There is a reboot in the middle of the installation.
- The installation ends at a sign-in prompt.

Step 5 Unmount the ISO image.

Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications

Note This task is required for installation of the subscriber/secondary nodes of the three VOS-based contact center applications: Cisco Finesse, Cisco Unified Communications Manager, and Cisco Unified Intelligence Center.

Before you begin

DNS Configuration is mandatory for installation of Cisco Unified Communications Manager, Cisco Unified Intelligence Center, and Cisco Finesse. To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

Before you install the subscriber/secondary nodes, you must install the publisher/primary nodes and configure the clusters.

Procedure

Step 1 Create a virtual machine for your VOS-based contact center application using the OVA.
Step 2 Mount the ISO image for the software to the virtual machine.
Step 3 Select the virtual machine and power it on, and open the console.

Step 4 Follow the Install wizard, making selections as follows:

a) In the **Disk Found** screen, click **OK** to begin the verification of the media integrity.
b) In the **Success** screen, select **OK**.
c) In the **Product Deployment Selection** screen:

- For the Progger (Lab only) or 2000 agent reference design, choose the coresident deployment option **Cisco Unified Intelligence Center with Live Data and IdS**, and then select **OK**. The **Cisco Unified Intelligence Center with Live Data and IdS** option installs Cisco Unified Intelligence Center, Live Data, and Cisco Identity Service (IdS) on the same server.
- For all other deployments, select one of the standalone install options. For example, select **Cisco Unified Intelligence Center**, **Live Data**, or **Cisco Identity Service (IdS)**. Then select **OK**.

Step 5 Follow the Install wizard, making selections as follows:

a) In the **Proceed with Install** screen, select **Yes**.
b) In the **Platform Installation Wizard** screen, select **Proceed**.
c) In the **Apply Patch** screen, select **No**.
d) In the **Basic Install** screen, select **Continue**.
e) In the **Timezone Configuration** screen, use the down arrow to choose the local time zone that most closely matches where your server is located. Select **OK**.

Note For Live Data servers, use the same timezone for all the nodes.

f) In the **Auto Negotiation Configuration** screen, select **Continue**.
g) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units.
h) In the **DHCP Configuration** screen, select **No**.
i) In the **Static Network Configuration** screen, enter static configuration values. Select **OK**.
j) In the **DNS Client Configuration** screen, click **Yes** to enable DNS client.
k) In the **Administrator Login Configuration** screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.
l) In the **Certificate Information** screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.
m) In the **First Node Configuration** screen, select **No**.
n) In the warning screen, select **OK**.
o) In the **Network Connectivity Test Configuration** screen, select **No**.
p) In the **First Node Access Configuration** screen, enter the host name and IP address of the first node. Enter and confirm the security password. Select **OK**.
q) In the **SMTP Host Configuration** screen, select **No**.
r) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and runs unattended.

- There is a reboot in the middle of the installation.
- The installation ends at a sign-in prompt.

Step 6 Unmount the ISO image.

Add Coresident (Cisco Unified Intelligence Center with Live Data and IdS) Machine Type to the System Inventory

Procedure

Step 1 In Unified CCE Administration, navigate to **System** > **Deployment**.

Step 2 Add the new machine to the System Inventory:

a) Click **Add**.

The **Add Machine** popup window opens.

b) From the Type drop-down menu, select the following machine type:

CUIC_LD_IdS Publisher, for the coresident Unified Intelligence Center, Live Data, and Identity Service machine available in the 2000 agent reference design.

c) In the **Hostname** field, enter the FQDN, hostname, or IP address of the machine.

The system attempts to convert the value you enter to FQDN.

d) Enter the machine's Administration credentials.

e) Click **Save**.

The machine and its related Subscriber or Secondary machine are added to the System Inventory.

What to do next

If you remove a component from your deployment, delete it from your System Inventory. If you add the component again, or add more components, add those components to the System Inventory.

Install VMware Tools

To install or upgrade using VOS, for Cisco Unified Communications Manager:

1. Ensure that your virtual machine is powered on.
2. Right-click the VM menu. Select **Guest** > **Install / Upgrade VMware tools**
3. Choose the interactive tools update and press **OK**.
4. Open the console and log in at the command prompt.
5. Enter the command **utils vmtools refresh** and confirm.

   The server automatically reboots twice.
6. After reboot, check the **Summary** tab for the VM to verify that the VMware Tools version is current. If it is not current, reboot the VM and check the version again.

The process takes a few minutes. After the process is complete, the tools are listed as Running (Current) on the VM's Summary tab in vSphere.

Configure the Cisco Identity Service

The Cisco Identity Service (Cisco IdS) provides authorization between the Identity Provider (IdP) and applications.

When you configure the Cisco IdS, you set up a metadata exchange between the Cisco IdS and the IdP. This exchange establishes a trust relationship that then allows applications to use the Cisco IdS for single sign-on. You establish the trust relationship by downloading a metadata file from the Cisco IdS and uploading it to the IdP. You can then select settings related to security, identify clients of the Cisco IdS service, and set log levels and, if desired, enable Syslog format.

Note If you are working with a Cisco IdS cluster, perform these steps on the Cisco IdS primary publisher node.

Be sure that the Principal AW is configured and functional before using the **Features** > **Single Sign-On** tool in Unified CCE Administration.

Procedure

Step 1 In Unified CCE Administration, navigate to **Features** > **Single Sign-On**.

Note Use a log in name in the format *username@FQDN* to log in to the Unified CCE Administration.

Step 2 Click **Identity Service Management**.

Result:

The Cisco Identity Service Management window opens:

Step 3 Enter your user name, and then click **Next**.

Step 4 Enter your password, and then click **Sign In**.

The Cisco Identity Service Management page opens, showing the **Nodes**, **Settings**, and **Clients** icons in the left pane.

Step 5 Click **Nodes**.

The **Nodes** page opens to the overall Node level view and identifies which nodes are in service. The page also provides the **SAML Certificate Expiry** details for each node, indicating when the certificate is due to expire. The node **Status** options are **Not Configured**, **In Service**, **Partial Service**, and **Out of Service**. Click a status to see more information. The star to the right of one of the Node names identifies the node that is the primary publisher.

Step 6 Click **Settings**.

Step 7 Click **IdS Trust**.

Step 8 To begin the Cisco IdS trust relationship setup between the Cisco IdS and the IdP, click **Download Metadata File** to download the file from the Cisco IdS Server.

Step 9 Click **Next**.

Step 10 To upload the trusted metadata file from your IdP, browse to locate the file.

The **Upload IdP Metadata** page opens and includes the path to the IdP. When the file upload finishes, you receive a notification message. The metadata exchange is now complete, and the trust relationship is in place.

Step 11 Clear the browser cache.

Step 12 Enter the valid credentials, when page is redirected to IdP.

Step 13 Click **Next**.
The **Test SSO Setup** page opens.

Step 14 Click **Test SSO Setup**.
A message appears telling you that the Cisco IdS configuration has succeeded.

Step 15 Click **Settings**.

Step 16 Click **Security**.

Step 17 Click **Tokens**.
Enter the duration for the following settings:

- **Refresh Token Expiry** -- The default value is 10 hours. The minimum value is 2 hours. The maximum is 24 hours.
- **Authorization Code Expiry** -- The default value is 1 minute, which is also the minimum. The maximum is 10 minutes.
- **Access Token Expiry** -- The default value is 60 minutes. The minimum value is 5 minutes. The maximum is 120 minutes.

Step 18 Set the **Encrypt Token** (optional); the default setting is **On**.

Step 19 Click **Save**.

Step 20 Click **Keys and Certificates**.
The **Generate Keys and SAML Certificate** page opens and allows you to:

- Regenerate the **Encryption/Signature key** by clicking **Regenerate**. A message appears to say that the Token Registration is successful and advises you to restart the system to complete the configuration.
- Regenerate the **SAML Certificate** by clicking **Regenerate**. A message appears to say that the SAML certificate regeneration is successful.

Step 21 Click **Save**.

Step 22 Click **Clients**.
The **Clients** page identifies the existing Cisco IdS clients, providing the client name, the client ID, and a redirect URL. To search for a particular client, click the Search icon above the list of names and type the client's name.

Step 23 To add a client:

a) Click **Add Client**.
b) Enter the client's name.
c) Enter the Redirect URL. To add more than one URL, click the plus icon.
d) Click **Add** (or click **Clear** and then click the X to close the page without adding the client).

Step 24 To edit or delete a client, highlight the client row and click the ellipses under **Actions**. Then:

- Click **Edit** to edit the client's name, ID, or redirect URL. On the **Edit Client** page, make changes and click **Save** (or click **Clear** and then click the X to close the page without saving edits).
- Click **Delete** to delete the client.

Step 25 Click **Settings**.

Step 26 From the **Settings** page, click **Troubleshooting** to perform some optional troubleshooting.

Step 27 Set the local log level by choosing from **Error**, **Warning**, **Info** (the default), **Debug**, or **Trace**.

Step 28 To receive errors in Syslog format, enter the name of the Remote Syslog Server in the Host (Optional) field.

Step 29 Click **Save**.

You can now:

- Register components with the Cisco IdS.
- Enable (or disable) SSO for the entire deployment.

Related Topics

Configure the Identity Provider in Your Environment
Register Components and Set Single Sign-On Mode, on page 155

Establish Trust Relationship

To enable applications to use Cisco Identity Service (Cisco IdS) for Single Sign-On, perform the metadata exchange between the Cisco IdS and the Identity Provider (IdP).

- Download the SAML SP Metadata file, `sp.xml`, on the Cisco IdS publisher primary node.
  1. Open Identity Service Management by doing either of the following:
     - Open the Identity Service Management window: `https://<Cisco IdS server address>:8553/idsadmin`.
     - In Unified CCE Administration, navigate to **Features** > **Single Sign-On** and click **Identity Service Management**.
  2. On the **Settings** > **IdS Trust** tab, download the SAML SP Metadata file, `sp.xml`.
- Download the Identity Provider Metadata file, federationmetadata.xml, from the IdP. For example,
  1. For AD FS, download the Identity Provider Metadata file from the IdP at the location:

     `https://<ADFSServer FQDN>/federationmetadata/2007-06/federationmetadata.xml`.
  2. On the **Identity Service Management** page, upload the Identity Provider Metadata file that was downloaded in the previous step.

The SAML SSO uses trust authentication certificates to exchange authentication and authorization details between the IdP (such as AD FS) and the Cisco IdS. This secures the communication between the servers.

Note Cisco IdS supports SAML self-signed certificates for authorization and authentication.

Integrate Cisco IdS to the AD FS

Procedure

Step 1 In AD FS, be sure that the default Authentication Type is set to Forms. (Cisco Identity Service requires the Identity Provider to provide form-based authentication.) See the Microsoft AD FS documentation for details.

Step 2 In AD FS server, open **AD FS Management**.

Step 3 Right-click **AD FS** -> **Trust Relationships** -> **Relying Party Trust**.

Step 4 From the menu, choose **Add Relying Party Trust** to launch the **Add Relying Party Trust Wizard**.

Step 5 In the **Select Data Source** step, choose the option **Import data about the relying party from a file**.

Step 6 **Browse** to the `sp.xml` file that you downloaded from Cisco Identity Server and complete the import to establish the relying party trust.

Step 7 Select the step **Specify Display Name**, and add a significant name you can use to identify the Relying Party Trust.

Step 8 For AD FS in Windows Server, select the option **I do not want to configure multi-factor authentication settings for the relying party at this time** in the Step **Configure Multi-factor Authentication Now**.

This step does not appear in AD FS 2.0 or 2.1. Continue with the next step.

Step 9 In the Step Choose Issuance Authorization Rules, select the option **Permit all users to access this relying party** and click **Next**.

Step 10 Click **Next** again to finish adding the relying party.

Step 11 Right-click on the **Relying Party Trust** and click **Properties**. Select the **Identifiers** tab.

Step 12 On the Identifiers tab, Set **Display name** to the name you specified when creating the Relying Party Trust, and set the **Relying party identifier** to the **fully qualified hostname** of the Cisco Identity Server from which `sp.xml` was downloaded.

Step 13 Still in **Properties**, select the **Advanced** tab.

Step 14 Select **secure hash algorithm** as **SHA-1** and then click **OK**.

Note In the following steps, you configure two claim rules to specify the claims that are sent from AD FS to Cisco Identity Service as part of a successful SAML assertion:

- A claim rule with the following custom claims, as AttributeStatements, in the assertion:
  - **uid** - Identifies the authenticated user in the claim sent to the applications.
  - **user_principal** - Identifies the authentication realm of the user in the assertion sent to Cisco Identity Service.
- A second claim rule that is a NameID custom claim rule specifying the fully qualified domain name of the AD FS server and the Cisco IdS server.

Follow the steps to configure these rules.

Step 15 In **Relying Party Trusts**, right-click on the Relying Party Trust you created, and click **Edit Claim Rules**.

Step 16 Follow these steps to add a rule with **Send LDAP Attributes as Claims** as the Claim rule template.

a) In the **Issuance Transform Rules** tab, click **Add Rule**.
b) In the Step **Choose Rule Type**, select the claim rule template **Send LDAP Attributes as Claims** and click **Next**.
c) In the **Configure Claim Rule** step, in the **Claim rule name** field, enter **NameID**.

d) Set the **Attribute store** drop-down to **Active Directory**.
e) Set the table **Mapping of LDAP attributes to outgoing claim types** to the appropriate **LDAP Attributes** and the corresponding **Outgoing Claim Type** for the type of user identifier you are using:

- When the identifier is stored as a **SAM-Account-Name** attribute:
  1. Select an **LDAP Attribute**of **SAM-Account-Name**, and set the corresponding **Outgoing Claim Type** to **uid** (lowercase).
  2. Select a second **LDAP Attribute** of **User-Principal-Name** and set the corresponding **Outgoing Claim Type** to **user_principal** (lowercase).
- When the identifier is a UPN:
  1. Select an **LDAP Attribute**of **User-Principal-Name**, and set the corresponding **Outgoing Claim Type** to **uid** (lowercase).
  2. Select a second **LDAP Attribute** of **User-Principal-Name** and set the corresponding **Outgoing Claim Type** to **user_principal** (lowercase).

Note The SAM-Account-Name or UPN choice is based on the User ID configured in the AW.

Step 17 Follow these steps to add a second rule with the template **custom claim rule**.

a) Select **Add Rule** on the **Edit Claim Rules** window.
b) Select **Send Claims Using Custom Rule**.
c) Set the name of rule to the **fully qualified domain name (FQDN)** of the Cisco Identity Server publisher (primary) node.
d) Add the following rule text:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
 =>
 issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
 Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType,
 Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
 "urn:oasis:names:tc:SAML:2.0:nameid-format:transient",

Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"]
 =
 "http://<AD FS Server FQDN>/adfs/services/trust",

Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"]
 =
 "<fully qualified domain name of Cisco IdS>");
```

e) Edit the script as follows:

- Replace **<ADFS Server FQDN>** to match exactly (including case) the ADFS server FQDN (fully qualified domain name.)
- Replace **<Cisco IdS server FQDN>** to match exactly (including case) the Cisco Identity Server FQDN.

Step 18 Add the following rules for Federated Scenario:

a) Add the rule for Name ID:

- In the **Issuance Transform Rules** tab, click **Add**.
- Select the claim rule template as **Pass Through or Filter an Incoming Claim**.
- In the **Configure Claim Rule** field, enter the claim rule name.
- Select **Incoming Claim type** to **Name ID**.
- Select Incoming name_ID format to Transient Identifier, then click **Finish**.

b) Add the rule for uid:

- In the **Issuance Transform Rules** tab, click **Add**.
- Select the claim rule template as **Pass Through or Filter an Incoming Claim**.
- In the **Configure Claim Rule** field, enter the claim rule name.
- In the **Incoming Claim type** field, enter **`uid`**, then click **Finish**.

c) Add the rule for user_principal:

- In the **Issuance Transform Rules** tab, click **Add**.
- Select the claim rule template as **Pass Through or Filter an Incoming Claim**.
- In the **Configure Claim Rule** field, enter the claim rule name.
- In the **Incoming Claim type** field, enter **`user_principal`**, then click **Finish**.

Step 19 Click **OK**.

Configure an Identity Provider (IdP)

To support SSO for the contact center solution, configure an Identity Provider (IdP) that is compliant with the Security Assertion Markup Language 2.0 (SAML v2) Oasis standard. The IdP stores user profiles and provides authentication services to the contact center solution.

This section provides sample configuration information for Microsoft AD FS.

Follow this sequence of tasks to configure the Identity Provider.

Sequence	Task
1	Install and Configure Active Directory Federation Services, on page 147
2	Set Authentication Type. See Authentication Types, on page 147.
4	Enable Signed SAML Assertions, on page 147
5	Optionally Customize the AD FS Sign-In Page in Windows Server to Allow User ID, on page 148

Install and Configure Active Directory Federation Services

Follow Microsoft instructions and guidelines to install Microsoft Active Directory Federation Services (AD FS).

For example, see *Active Directory Federation Services Overview* at https://technet.microsoft.com/en-us/library/hh831502(v=ws.11).aspx

- For AD FS 2.0, see *AD FS Content Map* at http://aka.ms/adfscontentmap.
- For AD FS in Windows Server, see *AD FS Technical Reference* at https://docs.microsoft.com/en-us/windows-server/identity/active-directory-federation-services.

Note SSO for Unified CCE supports IdPs other than MS, and AD FS. For the list of supported IdPs see the Compatibility matrix https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html

Note The certificate trust between the IdP and the Cisco Identity Service (Cisco IdS) requires SHA-1. (Certificate trust between Cisco IdS and the application browsers uses SHA-256.)

Note Cisco IdS does not support AD FS Automatic Certificate Rollover. If the AD FS certificate gets rolled over, then re-establish the trust relationship between the IdS and AD FS.

Authentication Types

Cisco Identity Service supports form-based authentication and Kerberos windows authentication of the Identity Provider.

For information on enabling form-based authentication in ADFS, see Microsoft documentation:

- For ADFS 2.0 see https://social.technet.microsoft.com/wiki/contents/articles/1600.ad-fs-2-0-how-to-change-the-local-authentication-type.aspx
- For ADFS 3.0 see https://blogs.msdn.microsoft.com/josrod/2014/10/15/enabled-forms-based-authentication-in-adfs-3-0/

For Kerberos authentication to work, ensure to disable the form-based authentication and follow the steps provided in the section *Kerberos Authentication (Integrated Windows Authentication)* at https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/200612-Configure-the-Identity-Provider-for-UCCX.html#anc19.

Enable Signed SAML Assertions

Enable Signed SAML Assertions for the Relying Party Trust (Cisco Identity Service).

Procedure

Step 1 Click **Start** and type **powershell** in the Search field to display the Windows Powershell icon.

Step 2 Right-click on the Windows Powershell program icon and select **Run as administrator**

Note All PowerShell commands in this procedure must be run in Administrator mode.

Step 3 Run the command, **Set-ADFSRelyingPartyTrust -TargetName <Relying Party Trust Display Name> -SamlResponseSignature "MessageAndAssertion"**.

Note Set <Relying Party Trust Display Name> to exactly match (including case) the Identifier tab of the Relying Party Trust properties.

For example:

```
Set-ADFSRelyingPartyTrust -TargetName CUICPub.PCCERCDN.cisco.com
-SamlResponseSignature "MessageAndAssertion".
```

Step 4 Navigate back to the Cisco Identity Service Management window.

Step 5 Click **Settings**.
By default **IdS Trust** tab is displayed.

Step 6 Click **Next** as you have already downloaded the required metadata.

Step 7 Click **Next** as you have already established trust relationship between IdP and IdS.

The configured IdP Entity ID is listed.

Note If reverse-proxy is configured for IdP, the IdP proxy url is listed at the bottom of the page.

Step 8 Click **Test SSO Setup** to test the required entity where the **SSO Status** displays **Needs Validation**.
SSO Status can be **Successful**, **Unsuccessful**, or **Needs Validation**.

Note If **Unsuccessful**, ensure that the claim you created on the AD FS is enabled or the rule has the correct names for IdS and AD FS.

Administrator client machine requires connectivity to reverse-proxy nodes for validating SSO connection with reverse-proxy.

Optionally Customize the AD FS Sign-In Page in Windows Server to Allow User ID

By default, the sign-in page presented to SSO users by AD FS in Windows Server requires a username that is a UPN. Usually this is an email format, for example, user@cisco.com. If your contact center solution is in a single domain, you can modify the sign-in page to allow your users to provide a simple User ID that does not include a domain name as part of the user name.

There are several methods you can use to customize the AD FS sign-in page. Look in the Microsoft AD FS in Windows Server documentation for details and procedures to configure alternate login IDs and customize the AD FS sign-in pages.

The following procedure is an example of one solution.

Procedure

Step 1 In the AD FS **Relying Party Trust**, change the NameID claim rule to map the chosen LDAP attribute to **uid**.

Step 2 Click the Windows **Start** control and type **powershell** in the Search field to display the Windows Powershell icon.

Step 3 Right-click on the Windows Powershell program icon and select **Run as administrator**

All PowerShell commands in this procedure must be run in Administrator mode.

Step 4 To allow sign-ins to AD FS using the sAMAccountName, run the following Powershell command:

```
Set-AdfsClaimsProviderTrust -TargetIdentifier "AD AUTHORITY" -AlternateLoginID sAMAccountName
-LookupForests myDomain.com
```

In the LookupForests parameter, replace `myDomain.com` with the forest DNS that your users belong to.

Step 5 Run the following commands to export a theme:

```
mkdir C:\themeExport-AdfsWebTheme –Name default –DirectoryPath c:\theme
```

Step 6 Edit `onload.js` in `C:\theme\script` and add the following code at the bottom of the file. This code changes the theme so that the AD FS sign-in page does not require a domain name or an ampersand, "@", in the username.

```
// Update the placeholder text to not include the domain
var userNameInput = document.getElementById("userNameInput");
if (userNameInput) {
 userNameInput.setAttribute("placeholder", "Username");
}

// Override submitLoginRequest to not have the "@" check
Login.submitLoginRequest = function () {
 var u = new InputUtil();
 var e = new LoginErrors();
 var userName = document.getElementById(Login.userNameInput);
 var password = document.getElementById(Login.passwordInput);
 if (!userName.value) {
  u.setError(userName, e.userNameFormatError);
  return false;
 }
 if (!password.value) {
  u.setError(password, e.passwordEmpty);
  return false;
 }
 document.forms['loginForm'].submit();
 return false;
};
```

Step 7 In Windows PowerShell, run the following commands to update the theme and make it active:

```
Set-AdfsWebTheme -TargetName custom -AdditionalFileResource
@{Uri='/adfs/portal/script/onload.js';path="c:\theme\script\onload.js"}

Set-AdfsWebConfig -ActiveThemeName custom
```

Federation between Identity Provider(IdP)

Add Claim Description for AD FS 1

Procedure

Step 1 Open **AD FS Management Console**, select **Service** > **Claim Descriptions**.

Step 2 Right click **Claim Descriptions** and select **Add Claim Descriptions**.

Step 3 Create uid claim description:

a) Enter the display name as **`uid`**.
b) Enter the claim identifier as **`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/uid`**.
c) Check the **Publish this claim description in federation metadata as a claim type that this Federation Service can accept** check box.
d) Check the **Publish this claim description in federation metadata as a claim type that this Federation Service can send** check box, then click **OK**.

Step 4 Create user_principal claim description:

a) Enter the display name as **`user_principal`**.
b) Enter the claim identifier as **`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/user_principal`**.
c) Check the **Publish this claim description in federation metadata as a claim type that this Federation Service can accept** check box.
d) Check the **Publish this claim description in federation metadata as a claim type that this Federation Service can send** check box, then click **OK**.

Important After creating claim descriptions, update federation metadata of the claim provider trust in Hosted AD FS.

Add Claim Rules for Relying Party Trust in the AD FS 1

Use this procedure to add the Claim rules for the Relying Party Trust in the Customer AD FS:

Procedure

Step 1 Open **AD FS Management Console**.

Step 2 Select **Trust Relationships** > **Relying Party Trusts**.

Step 3 Select and right click the appropriate Relying party trust, then select **Edit Claim Rules**.

Step 4 Add a rule with **Send LDAP Attributes as Claims** as the Claim rule template.

a) In the **Issuance Transform Rules** tab, click **Add Rule**. Select the claim rule template **Send LDAP Attributes as Claims**.
b) For **Configure Claim Rule**, set the rule name as **NameID**.
c) Select **Attribute store** to **Active Directory**.
d) Map the LDAP attribute **User-Principal-Name** to the **Outgoing Claim Type** of **user_principal** (lowercase).
e) Select one of the possible LDAP attributes that identifies application users and map it to **uid** (lowercase).

Note The rule that you create can use one of several possible LDAP attributes to identify the user. The exact mapping depends on which attribute the rule uses:

- When the identifier is stored as a **SAMAccountName** attribute:
  - The Outgoing Claim Type **uid** maps to the LDAP attribute **SAM-Account-Name**.
  - The Outgoing Claim Type **user_principal** maps to the LDAP attribute **User-Principal-Name**.
- When the identifier is a UPN:
  - The Outgoing Claim Type **uid** maps to the LDAP attribute **User-Principal-Name**.
  - The Outgoing Claim Type **user_principal** maps to the LDAP attribute **User-Principal-Name**.

Step 5 Add another rule with the template **custom claim rule**.

a) Select **Add Rule** on the **Edit Claim Rules** window.
b) Select **Send Claims Using Custom Rule**.
c) Set the name of rule to the **fully qualified domain name (FQDN)** of the Cisco Identity Server publisher (primary) node.
d) Add the following rule text:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
 =>
 issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
 Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType,
 Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
 "urn:oasis:names:tc:SAML:2.0:nameid-format:transient",

Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"]
 =
 "http://<AD FS Server FQDN>/adfs/services/trust",

Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"]
 =
 "<fully qualified domain name of Cisco IdS>");
```

- Set **<AD FS Server FQDN>** to match exactly (including case) the AD FS FQDN.
- Set **<fully qualified domain name of Cisco IdS>** to match exactly (including case) the Cisco Identity Server FQDN.

Step 6 Click **OK**.

Add Claim Rules for Claim Provider Trust in the AD FS 2

Note Add the claim rules for Claim Provider Trust in the ADFS where Cisco IDS is registered.

Procedure

Step 1 Open **AD FS Management Console**.

Step 2 Select **Trust Relationships** > **Claim Provider Trusts**.

Step 3 Select and right click the appropriate Claims provider trust, then select **Edit Claim Rules**.

Step 4 In the **Acceptance Transform Rules** tab, click **Add**.

Step 5 Add the rule for Name ID:

a) Select the claim rule template as **Pass Through or Filter an Incoming Claim**.
b) In the **Configure Claim Rule** field, enter the claim rule name.
c) Select **Incoming Claim type** to **Name ID**.
d) Select Incoming name_ID format to Transient Identifier, then click **Finish**.

Step 6 Add the rule for uid:

a) Select the claim rule template as **Transform an Incoming Claim**.
b) In the **Configure Claim Rule** field, enter the claim rule name.
c) Select **Incoming Claim type** to **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/uid**.
d) Select **Outgoing Claim type** to **`uid`**, then click **Finish**.

Step 7 Add the rule for user_principal:

a) Select the claim rule template as **Transform an Incoming Claim**.
b) In the **Configure Claim Rule** field, enter the claim rule name.
c) Select **Incoming Claim type** to **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/user_principal**.
d) Select **Outgoing Claim type** to **`user_principal`**, then click **Finish**.

Set up the System Inventory for Single Sign-On

Set up the System Inventory before configuring the Cisco Identity Service (Cisco IdS) and the components for single sign-on.

By default, the System Inventory displays a list of all of the AWs, Routers, and Peripheral Gateways in the deployment. Select the Principal AW to manage registering the components with the Cisco IdS and enabling them for SSO. Add the remaining SSO-capable machines to the System Inventory, and select the default Cisco IdS for each of the SSO-capable machines.

Procedure

Step 1 In Unified CCE Administration, navigate to **Features** > **Single Sign-On**.

Step 2 Set the Principal AW:

a) Click the AW that you want to be the Principal AW.

Note If the AW is coresident with the Router, you can set the Principal AW on the Router.

You can only specify one Principal AW for each Unified CCE system.

The **Edit AW** popup window opens.

b) Check the **Principal AW** check box on the General tab.

c) Enter the Unified CCE Diagnostic Framework Service domain, username, and password.

These credentials must be for a domain user who is a member of the Config security group for the instance. These credentials must be valid on all CCE components in your deployment (Routers, PGs, AWs, and so on).

d) Click **Save**.

Step 3 Add the SSO-capable machines to the System Inventory:

a) Click **New**.
The **Add Machine** popup window opens.

b) From the **Type** drop-down list, select one of the following types of machines:

- **Finesse Primary**
- **CUIC, LD, IdS Publisher**, for the coresident Unified Intelligence Center, Live Data, and Cisco IdS machine available in the 2000 agent or Progger (Lab only) reference design
- **Unified Intelligence Center Publisher**, if you are using a standalone Unified Intelligence Center
- **Identity Service Primary**, if you are using a standalone Cisco IdS

c) In the **Hostname** field, enter the FQDN, IP address, or hostname of the machine.

Note If you do not enter the FQDN, the system converts the value you enter to FQDN.

d) Enter the machine's Administration credentials.

e) Click **Save**.
The machine and its related Subscriber or Secondary machine are added to the System Inventory.

f) Repeat this procedure to add all of the SSO-capable machines in the deployment.

Step 4 Select the default Identity Service for each of the following machines:

- All Unified CCE AW servers
- Finesse Primary and Secondary
- Unified Intelligence Center Publisher and Subscriber

Note If you are using a coresident CUIC, LD, Ids Publisher and Subscriber, you do not need to set the default Cisco IdS for those machines.

In a standalone deployment, select the Cisco IdS that is deployed on the same Data Center Side (A or B) as the machine you are configuring. For example, in the Reference Deployment:

- Select the Identity Service Publisher (IdS A) for AW-HDS-DDS 1, AW-HDS 3, Finesse 1 Pub, Finesse 2 Pub, CUIC Pub, and CUIC Sub 1.
- Select the Identity Service Subscriber (Ids B) for AW-HDS-DDS 2, AW-HDS 4, Finesse 1 Sub, Finesse 2 Sub, CUIC Sub 2, and CUIC Sub 3.

For details on the Reference Deployment, see *Solution Design Guide for Cisco Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html.

a) Click a machine to open the **Edit Machine** popup window.
b) Click the Search icon next to **Default Identity Service** to open the **Select Identity Service** popup window.
c) Enter the machine name for the Cisco IdS in the Search field and choose the Cisco IdS from the list.
d) Click **Save**.

What to do next

Be sure to update the System Inventory if you change your deployment:

- If you add or remove contact center solution components from your deployment, make the corresponding changes in the System Inventory.
- If you add or remove Cisco Identity Service machines or coresident CUIC-LD-IdS machines, update the System Inventory appropriately and reconfigure the Cisco IdS. Re-associate the components with a default Cisco IdS.

Reset Live Data Streaming Data Source After Upgrade and Migration

If you upgrade from Packaged CCE 11.0 to 11.5(1), and then switch from Packaged CCE to a Unified CCE: 4000 Agents Rogger deployment in which Unified Intelligence Center is installed coresident with Live Data and Cisco IdS, you must reset the Live Data Streaming Data Source.

In this situation, when you set up the coresident machine in the system inventory, the system generates a new username and password for the Live Data API service that does not match the existing credentials for the Live Data Streaming Data Source. As a result, the Live Data Streaming Data Source is no longer online.

Perform the following procedure to reset the Live Data Streaming Data Source:

Procedure

- After you add the coresident CUIC, LD, IdS machine to the system inventory, access the Live Data CLI and run the following command:

  set live-data cuic-datasource

Note For more information about Live Data CLI, see the Live Data CLI Commands section of the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Register Components and Set Single Sign-On Mode

If you add any SSO-compatible machines to the System Inventory after you register components with the Cisco IdS, those machines are registered automatically.

Before you begin

- Configure the Cisco Identity Service (Cisco IdS).
- Disable popup blockers. It enables viewing all test results correctly.
- If you are using Internet Explorer, verify that:
  - It is not in the Compatibility Mode.
  - You are using the fully qualified domain name of AW to access the CCE Administration (for example, **https://<FQDN>/cceadmin**).

Procedure

Step 1 In the Unified CCE Administration, navigate to **Features** > **Single Sign-On**.

Step 2 Click the **Register** button to register all SSO-compatible components with the Cisco IdS.

The component status table displays the registration status of each component.

If a component fails to register, correct the error and click **Retry**.

Step 3 Click the **Test** button. When the new browser tab opens, you may be prompted to accept a certificate. In order for the page to load, accept any certificates. Then, when presented with a log in dialog, log in as a user with SSO credentials.

The test process verifies that each component has been configured correctly to reach the Identity Provider, and that the Cisco IdS successfully generates access tokens. Each component that you are setting up for SSO is tested.

The component status table displays the status of testing each component.

If a test is unsuccessful, correct the error, and then click **Test** again.

Test results are not saved. If you refresh the page, run the test again before enabling SSO.

Step 4 Select the SSO mode for the system from the **Set Mode** drop-down menu:

- Non-SSO: This mode disables SSO for all agents and supervisors. Users log in using existing Active Directory-based local authentication.
- Hybrid: This mode allows you to enable agents and supervisors selectively for SSO.

- SSO: This mode enables SSO for all agents and supervisors.

The component status table displays the status of setting the SSO mode on each component.

If the SSO mode fails to be set on a component, correct the error, and then select the mode again.

Migration Considerations Before Enabling Single Sign-On

Administrator User and Single Sign-On in Unified Intelligence Center

During installation, Cisco Unified Intelligence Center creates an administrator user. This user is not enabled for SSO, as the user is known only to Unified Intelligence Center.

When you enable SSO, this administrator user is no longer able to log in to the Unified Intelligence Center and perform administrative tasks. These tasks include configuring datasources and setting permissions for other users, for example. To avoid this situation, perform the following steps before enabling SSO.

1. Create a new SSO user who has the same roles and permissions as those of the administrator user.
2. Log in to the CLI.
3. Run the following command:

   utils cuic user make-admin *username*

in which the user name is the complete name of the new user, including the authenticator prefix as shown on the Unified Intelligence Center User List page.

The command, when executed, provides all the roles to the new user and copies all permissions from the administrator user to this new user.

Note

- The administrator's group memberships are not copied to the new user by this CLI command and must be manually updated. The new user, now a Security Administrator, can set up the group memberships.
- For any entity (for example, reports or report definitions), if this new user's permissions provide higher privileges than the administrator, the privileges are left intact. The privileges are not overwritten by the execution of this CLI command.

Browser Settings and Single Sign-On

If you have enabled single sign-on and are using Internet Explorer, Chrome, or Firefox, verify that the browser options are set as shown in the following table. These settings specify that you do not want a new session of the browser to reopen tabs from a previous session. No changes are required for Internet Explorer.

Browser	Browser options to verify when using SSO
Internet Explorer	1. Open Internet Explorer. 2. Click the **Tools (Alt+X)** icon, and then click **Internet options**. 3. In the **General** tab, click **Tabs**. 4. From the **When a new tab is opened, open:** drop-down list, verify that the **Your first home page** option is selected.
Chrome	1. Open Chrome. 2. Click the **Customize and control Google Chrome** icon. 3. Click **Settings**. 4. In the **On startup** section of the **Settings** page, verify that the **Open the New Tab page** option is selected.
Firefox	1. Open Firefox. 2. Click the **Open menu** icon. 3. Click **Options**. 4. In the **Startup** section of the **General** page, verify that either the home page or a blank page is chosen in the **When Firefox starts** drop-down list.

Migrate Agents and Supervisors to Single Sign-On Accounts

If you are enabling SSO in an existing deployment, you can set the SSO state to hybrid to support a mix of SSO and non-SSO users. In hybrid mode, you can enable agents and supervisors selectively for SSO making it possible for you to transition your system to SSO in phases.

Use the procedures in this section to migrate groups of agents and supervisors to SSO accounts using the SSO Migration content file in the Unified CCE Administration Bulk Jobs tool. You use the Administration Bulk Jobs tool to download a content file containing records for agents and supervisors who have not migrated to SSO accounts. You modify the content file locally to specify SSO usernames for the existing agents and supervisors. Using the Administration Bulk Jobs tool again, you upload the content file to update the agents and supervisors usernames; the users are also automatically enabled for SSO.

The content file returns the first 12,000 agents and supervisors who have not been migrated to SSO accounts. After you run the bulk job to update users from that group of records, you can download the SSO Migration content file again to update additional agent and supervisor records.

If you do not want to migrate a user, delete the row for that user.

For instructions on how to setup SSO for Agent or Supervisor login, see the Configure the Cisco Identity Service, on page 141.

Important While the Finesse agent is logged in, changing the login name prevents the agent from answering or placing calls. In this situation, the agent can still change between *ready* and *not_ready* state. This affects all active agents, independent of whether SSO is enabled or disabled. Should you need to modify a login name, do so only after the corresponding agent is logged out. Note too that SSO migration (moving a non-SSO agent to be SSO-enabled, by either hybrid mode or global SSO mode) should not be done when the agent is logged in.

Procedure

Step 1 In Unified CCE Administration, navigate to **Manage** > **Bulk Jobs**.

Step 2 Download the SSO Migration bulk job content file.

a) Click **Templates.**

The **Download Templates** popup window opens.

b) Click the **Download** icon for the SSO Migration template.

c) Click **OK** to close the **Download Templates** popup window.

Step 3 Enter the SSO usernames in the SSO Migration content file.

a) Open the template in Microsoft Excel. Update the **newUserName** field for the agents and supervisors whom you want to migrate to SSO accounts.

The content file for the SSO migration bulk job contains these fields:

Field	Required?	Description
userName	Yes	The user's non-SSO username.
firstName	No	The user's first name.
lastName	No	The user's last name.
newUserName	No	The user's new SSO username. Enter up to 255 ASCII characters. If you want to enable a user for SSO, but keep the current username, leave **newUserName** blank, or copy the value of **userName** into **newUserName**.

b) Save the populated file locally.

Step 4 Create a bulk job to update the usernames in the database.

a) Click **New** to open the **New Bulk Job** window.

b) Enter an optional **Description** for the job.

c) In the **Content File** field, browse to the SSO Migration content file you completed.

The content file is validated before the bulk job is created.

d) Click **Save**.

The new bulk job appears in the list of bulk jobs. Optionally, click the bulk job to review the details and status for the bulk job. You can also download the log file for a bulk job.

When the bulk job completes, the agents and supervisors are enabled for SSO and their usernames are updated. You can open an individual user's record to see the changes.

Step 5 Repeat this procedure, if needed, to migrate additional agents and supervisors to SSO usernames.

What to do next

After all of the agents and supervisors in your deployment are migrated to SSO accounts, you can enable SSO globally in your deployment.

Single Sign-On Migration and the Configuration Manager

When the global SSO-enabled setting is Hybrid, you can use several of the existing Unified CCE Configuration Manager tools to either:

- Enable (or disable) users individually for single sign-on
- Prevent changes to system configuration information access

Tool	General description	New functionality specific to single sign-on
Agent Explorer (in Explorer Tools)	Allows you to view, and (if you have maintenance privileges) define, delete, or edit agent records, routes, peripheral targets, labels, and their relationships. You can also designate an agent as a supervisor.	Includes an **Enable single sign-on (SSO)** option. Check the check box to require a selected agent to sign in with SSO authentication. Uncheck the check box to require Unified CCE authentication. **Note** The check box is disabled when the global SSO-enabled setting is enabled or disabled.

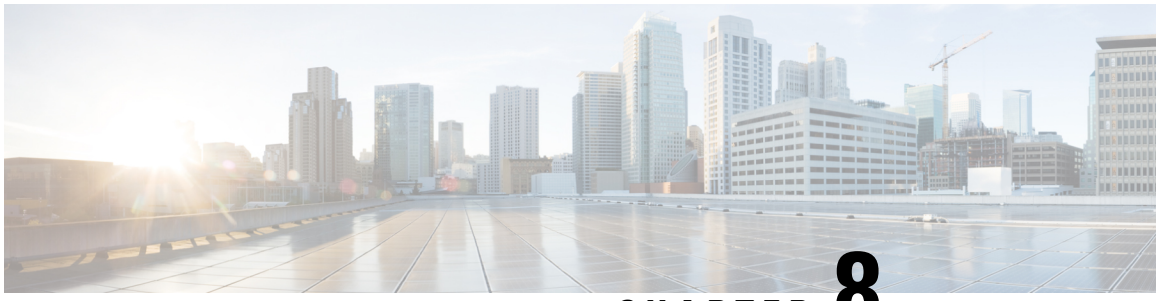
Tool	General description	New functionality specific to single sign-on
Person Bulk Insert and Person Bulk Edit (in Bulk Configuration Tools)	Allow you to insert and update multiple configuration records in a single transaction from a single screen.	Allows you to view or change the person's SSO status. If the global SSO setting is hybrid, the person's SSO enabled setting is either: • **Yes** if the person uses SSO authentication • **No** if the person uses non-SSO authentication. (If global SSO is *enabled*, the person's SSO setting is ignored. All agents use SSO authentication. If global SSO is *disabled*, the person's SSO setting is ignored. All agents use non-SSO authentication.) **Note** In Import or Export files, the Person SSO Enabled setting is recorded in the file as a number: Yes = 1, No = 0.
Person List (in List Tools)	Allows you to list the persons currently defined in the database, to define new persons, and to view, edit, or delete the records of existing persons.	Includes an **Enable single sign-on (SSO)** option. Check the check box to require an agent associated with a selected Person to sign in with SSO authentication. Uncheck the check box to require Unified CCE authentication. **Note** The check box is disabled when the global SSO-enabled setting is enabled or disabled.
User List (in List Tools)	Allows you to list the users currently defined, associate new users with their Active Directory account, and view, edit, or delete the records of existing (nonsupervisor) users.	Prevents changes to Configuration Security Group membership or system information read-only access for SSO-enabled supervisors.

For more information, see the Explorer Tools online help, the Bulk Configuration Tools online help, or the List Tools online help.

Related Documentation

Refer to the following documents and other resources for more details about single sign-on.

See this information	Located here	For these details
Solution Design Guide for Cisco Unified Contact Center Enterprise	https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html	Design considerations and guidelines for deploying the Cisco Unified CCE System.
Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise	https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html	How to monitor and manage Unified Contact Center Enterprise (Unified CCE) and Cisco Unified Intelligent Contact Management Enterprise (Unified ICM).
Release Notes for Cisco Unified Contact Center Enterprise Solutions	https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-release-notes-list.html	New features and changes for this release of the Unified CCE solution.
Virtualization for Unified Contact Center Enterprise	https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html	Information about deploying Unified CCE (including single sign-on) on VMware.
Contact Center Enterprise Compatibility Matrix	https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html	Unified CCE requirements.
Configuration Manager: • Explorer Tools • List Tools	Online help	Changes to support single sign-on.
Unified CCE Administration Single Sign-On Tool	Online help	Changes to support single sign-on.
System Inventory Tool	This guide.	Information related to adding SSO-compatible components to the inventory.



CHAPTER 8

Task Routing

Task Routing

Task Routing describes the system's ability to route requests from different media channels to any agents in a contact center.

You can configure agents to handle a combination of voice calls, emails, chats, and so on. For example, you can configure an agent as a member of skill groups or precision queues in three different Media Routing Domains (MRD) if the agent handles voice, e-mail, and chat. You can design routing scripts to send requests to these agents based on business rules, regardless of the media. Agents signed into multiple MRDs may switch media on a task-by-task basis.

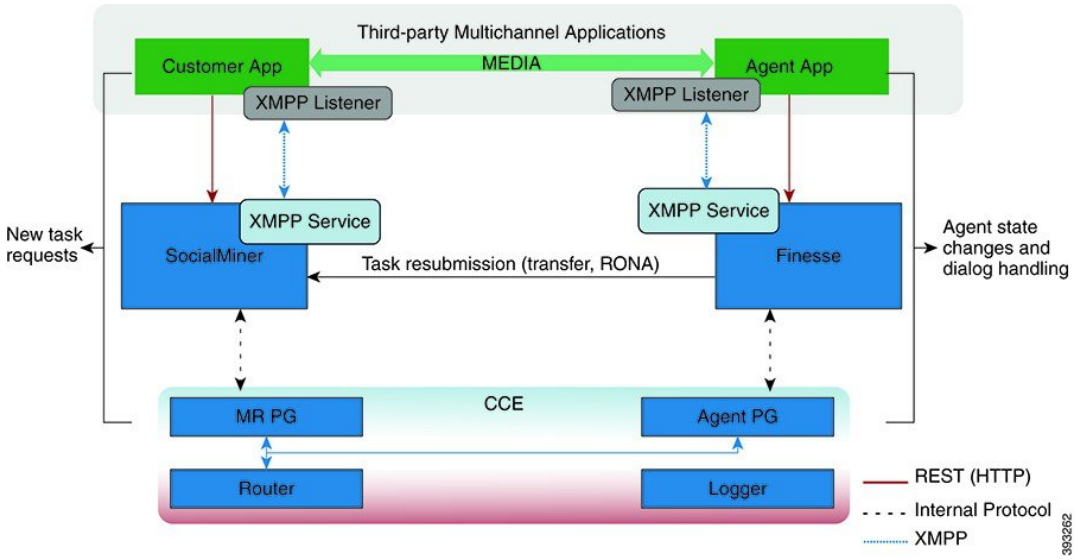
Enterprise Chat and Email provides universal queue out of the box. Third-party multichannel applications can use the universal queue by integrating with CCE through the Task Routing APIs.

Task Routing APIs provide a standard way to request, queue, route, and handle third-party multichannel tasks in CCE.

Contact Center customers or partners can develop applications using SocialMiner and Finesse APIs in order to use Task Routing. The SocialMiner Task API enables applications to submit nonvoice task requests to CCE. The Finesse APIs enable agents to sign into different types of media and handle the tasks. Agents sign into and manage their state in each media independently.

Cisco partners can use the sample code available on Cisco DevNet as a guide for building these applications (https://developer.cisco.com/site/task-routing/).

Figure 18: Task Routing for Third-party Multichannel Applications Solution Components



SocialMiner and Task Routing

Third-party multichannel applications use SocialMiner'sTask API to submit nonvoice tasks to CCE.

The API works in conjunction with SocialMiner task feeds, campaigns, and notifications to pass task requests to the contact center for routing.

The Task API supports the use of Call variables and ECC variables for task requests. Use these variables to send customer-specific information with the request, including attributes of the media such as the chat room URL or the email handle.

Note CCE solutions support only the Latin 1 character set for Expanded Call Context variables and Call variables when used with Finesse and SocialMiner. Arrays are not supported.

CCE and Task Routing

CCE provides the following functionality as part of Task Routing:

- Processes the task request.
- Provides estimated wait time for the task request.
- Notifies SocialMiner when an agent has been selected.
- Routes the task request to an agent, using either skill group or precision queue based routing.
- Reports on contact center activity across media.

Finesse and Task Routing

Finesse provides Task Routing functionality via the Media API and Dialog API.

With the Media API, agents using third-party multichannel applications can:

- Sign into different MRDs.
- Change state in different MRDs.

With the Dialog API, agents using third-party multichannel applications can handle tasks from different MRDs.

Task Routing Deployment Requirements

Task Routing for third-party multichannel applications deployment requirements:

- Finesse and SocialMiner are required. Install and configure Finesse and SocialMiner before configuring the system for Task Routing.

  See the Finesse documentation at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/tsd-products-support-series-home.html.

  See the SocialMiner documentation at https://www.cisco.com/c/en/us/support/customer-collaboration/socialminer/tsd-products-support-series-home.html.

  By default, access to the Social Miner administration user interface is restricted. Administrator can provide access by unblocking the IP addresses of the clients. For more details, see the *Control Social Miner Application Access* topic in the *Cisco Social Miner Installation and Upgrade Guide* guide at https://www.cisco.com/c/en/us/support/customer-collaboration/socialminer/products-installation-guides-list.html.

- You can install only one SocialMiner machine in the deployment.
- SocialMiner must be geographically colocated with one side of the Media Routing Peripheral Gateway (MR PG).
- Install SocialMiner in a location from which CCE, Finesse, and the third-party multichannel SocialMiner Task Routing application can access it over the network.

  If you install SocialMiner in the DMZ, open a port for CCE and Finesse to connect to it. The default port for CCE to connect to SocialMiner is port 38001. Finesse connects to SocialMiner over HTTPS, port 443.

  Install the third-party multichannel application locally with SocialMiner, or open a port on the SocialMiner server for the application to connect to it.

Supported Functionality for Third-Party Multichannel Tasks

Blind transfer is supported for third-party multichannel tasks submitted through the Task Routing APIs.

We do not support the following functionality for these types of tasks:

- Agent-initiated tasks.
- Direct transfer.

- Consult and conference.

Plan Task Routing Media Routing Domains

Media Routing Domains (MRDs) organize how requests for each communication medium, such as voice and email, are routed to agents. You configure an MRD for each media channel in your deployment.

Finesse agents can sign in to any of the multichannel MRDs you create for Task Routing.

Important factors to consider when planning your MRDs include the following:

- Whether the MRD is interactive.
- The maximum number of concurrent tasks that an agent can handle in an MRD.
- Whether the MRDs are interruptible.
- For interruptible MRDs, whether Finesse accepts or ignores interrupt events.

To configure the settings and parameters described in the following sections, see the following documents:

- *Cisco SocialMiner Developer Guide* at https://developer.cisco.com/site/socialminer/documentation/
- *Cisco Finesse Web Services Developer Guide* at https://developer.cisco.com/site/finesse/documents/
- Unified CCE Administration and Configuration Manager Tools, on page 187

Interactive and Non-interactive MRDs

Interactive tasks are tasks in which an agent and customer communicate in real time with each other, such as chats and SMS messages. The customer usually engages with the agent through an application, like a chat window, and leaves this application open while waiting to be connected to an agent. Non-interactive tasks are asynchronous, such as email. The customer submits the request and then may close the application, checking later for a response from an agent.

API Parameter or Setting	API/Tool	Possible Values	
		Interactive Task/MRD	Non-interactive Task/MRD
requeueOnRecovery Whether SocialMiner re-queues or discards the task when SocialMiner recovers from a failure. Set this parameter when submitting a task request.	SocialMiner Task Submission API	**False** - customers are waiting at an interface for an agent and can be notified if there is a problem. You don't need to resubmit these tasks.	**True** - customers are not waiting at an interface for an agent, and there is no way to alert them that there was a problem. You need to resubmit these tasks.

API Parameter or Setting	API/Tool	Possible Values	
		Interactive Task/MRD	Non-interactive Task/MRD
dialogLogoutAction Whether active tasks are closed or transferred when an agent signs out or loses presence. Set this parameter when an agent signs in to a Media Routing Domain.	Finesse Media Sign In API	**Close**- customers are engaged with an agent, and can be notified that the task has ended.	**Transfer** - customers are not engaged with an agent, and there is no way to alert them that the task has ended.
Start Timeout The amount of time that the system waits for an agent to accept an offered task. When this time is reached, the system makes the agent not routable and re-queues the task. Set this parameter when configuring an MRD.	Media Routing Domains tool in Unified CCE Administration	**Shorter duration** - customer is waiting at an interface for the agent	**Longer duration** - customer is not waiting at an interface for an agent
Monitoring status of submitted tasks You can monitor status of submitted and queued tasks using either the SocialMiner Task API to poll for status or SocialMiner XMPP BOSH eventing.	SocialMiner Task API or XMPP BOSH eventing	Use SocialMiner Task API status polling for MRDs when you want to monitor the status of a single contact/task.	Use SocialMiner XMPP BOSH eventing to receive updates on all contacts/tasks in the campaign supporting Universal Queue over one channel.

Maximum Concurrent Tasks Per Agent

Specify the maximum number of concurrent tasks for an agent in an MRD when an agent signs into the Finesse application, using the **maxDialogLimit** parameter in the **Finesse Media - Sign In API**.

See the *Solution Design Guide for Cisco Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html for the maximum number of tasks supported within an MRD and across MRDs for a single agent.

For agents handling interactive tasks, consider how many concurrent tasks an agent can handle reasonably. How many simultaneous chat sessions, for example, can an agent handle and provide good customer care? If you are using precision queue routing, keep in mind that CCE assigns tasks to agents who match attributes for step one, **up to their task limit**, until all of those agents are busy. CCE then assigns tasks to agents who match attributes for step two, up to their task limit, and so on.

Interruptible and Non-Interruptible MRDs

When you create an MRD in the Unified CCE Administration Media Routing Domains tool, you select whether the MRD is interruptible.

- **Interruptible:** Agents handling tasks in the MRD can be interrupted by tasks from other MRDs. Non-interactive MRDs, such as an email MRD, are typically interruptible.
- **Non-interruptible:** Agents handling tasks in the MRD cannot be interrupted by tasks from other MRDs. The agents can be assigned tasks in the same MRD, up to their maximum task limits. For example, an agent can handle up to three non-interruptible chat tasks; if the agent is currently handling two chat tasks, CCE can assign the agent another chat, but cannot interrupt the agent with a voice call. Interactive MRDs, such as a chat MRD, are typically non-interruptible. Voice is non-interruptible.

When an agent is working on a non-interruptible task, CCE does not assign a task in any other MRD to the agent. Any application handling the non-voice MRDs must follow the same rule. In certain cases, it is possible that a task from another media routing domain gets assigned to an agent who is working on a non-interruptible task in an MRD.

For example, if an agent is working on a non-interruptible chat MRD and makes an outbound call (internal or external) using the desktop or phone, CCE cannot prevent the agent from making that call. Instead, the system handles this situation differently. CCE marks the agent temp not routable across all media domains until the agent has completed all non-interruptible tasks the agent is currently working on. Because of this designation, the agent is not assigned any new tasks from any MRDs until finishing all current tasks. Even if the agent tries to go ready or routable, the agent's temp not routable status is cleared only after all tasks are complete.

Note If you change the MRD from interruptible to non-interruptible or vice versa, the change takes effect once the agent logs out and then logs back in on that MRD.

Accept and Ignore Interrupts

Specify whether an MRD accepts or ignores interrupt events when an agent signs into the Finesse application, using the **interruptAction** parameter in the **Finesse Media - Sign In API**. This setting controls the agent's state in an interrupted MRD and ability to work on interrupted tasks. The setting applies only when a task from a non-interruptible MRD interrupts the agent.

- **Accept:** When an agent is interrupted by a task from a non-interruptible MRD while working on a task in an interruptible MRD, Finesse accepts the interrupt event.

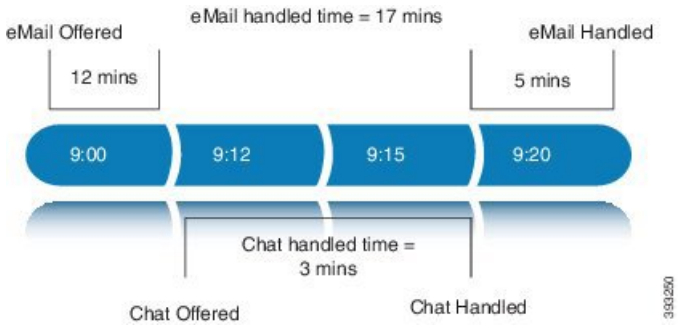
  The agent, CCE task, and Finesse dialog state in the interrupted MRD change to INTERRUPTED.

  The agent cannot perform dialog actions while a task is interrupted.

Important The application is responsible for disabling all dialog-related activities in the interface when an agent's state changes to INTERRUPTED.

  The agent's time on task stops while the agent is interrupted.

  Example: An agent has an email task for 20 minutes, and is interrupted for 3 of those minutes with a chat task. The handled time for the email task is 17 minutes, and the handled time for the chat task is 3 minutes.

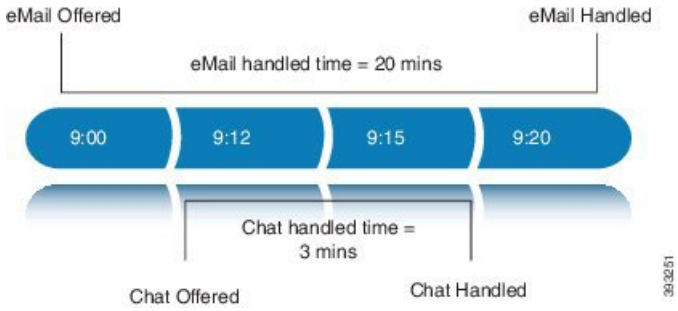


- **Ignore:** When an agent is interrupted by another task while working on a task in an interruptible MRD, Finesse ignores the interrupt event.

  The new task does not affect any of the agent's other assigned tasks. The agent, CCE task, and Finesse dialog state in the interrupted MRDs do not change.

  The agent can perform dialog actions on original task and the interrupting task at the same time. The agent's time on the original task does not stop while the agent is handling the interrupting task.

  Example: An agent has an email task for 20 minutes, and is interrupted for 3 of those minutes with a chat task. The handled time for the email task is 20 minutes, and the handled time for the chat task is 3 minutes. This means that during a 20-minute interval, the agent handled tasks for 23 minutes.



If an agent is working on a task in an interruptible MRD and is routed a task in another interruptible MRD, CCE does not send an interrupt event. Therefore, interruptAction setting does not apply.

Plan Dialed Numbers

Dialed numbers, also called script selectors, are the strings or numbers submitted with Task Routing task requests through SocialMiner. Each dialed number is associated with a call type, and determines which routing script CCE uses to route the request to an agent.

Dialed numbers are media-specific; you associate each one with a Media Routing Domain.

For Task Routing, plan which dialed numbers the custom SocialMiner application will use when submitting new task requests. Consider whether you will use the same dialed numbers for transfer and tasks that are requeued on RONA, or if you need more dialed numbers.

Important You must associate each Task Routing dialed number with a call type. The default call type is not supported for Task Routing.

Skill Group and Precision Queue Routing for Nonvoice Tasks

Routing to skill groups and precision queues is largely the same for voice calls and nonvoice tasks. However, the way that contact center enterprise distributes tasks has the following implications for agents who can handle multiple concurrent tasks:

- **Precision queues**—In precision queue routing, Unified CCE assigns tasks to agents in order of the precision queue steps. Unified CCE assigns tasks to agents who match the attributes for step one, up to their task limit, until all those agents are busy. Unified CCE then assigns tasks to agents who match attributes for step two, and so on. If you configure agents to handle three concurrent tasks, Unified CCE assigns three tasks to each agent in the first step. It then moves on to the second step and assigns any remaining tasks to those agents.
- **Overflow skill groups**—Routing scripts can specify a preferred skill group and an overflow skill group. Unified CCE assigns tasks to all agents in the preferred skill group, up to their task limit, before assigning any tasks in the overflow skill group. If you configure agents to handle three concurrent tasks, Unified CCE assigns three tasks to each agent in the preferred skill group. It then moves on to the overflow skill group and assigns any remaining tasks to those agents.

Note The number of available slots is an important factor in the Longest Available Agent (LAA) calculation.

The number of available slots = The maximum concurrent task limit for the MRD that an Agent has logged into - Current tasks being handled by the Agent or routed to the Agent.

If there are multiple skill groups that are part of the queue node, then the skill group that has the higher LAA is picked. Then, the agents within the picked skill group (or the Precision Queue) who have the highest number of available slots for non-voice tasks get prioritised.

Agents with the same number of available slots get prioritized based on the time in the available state or the LAA mechanism.

Agent State and Agent Mode

An agent's state and routable mode in an MRD work together to determine whether CCE routes tasks to the agent in that MRD.

Agent Routable Mode

The agent's routable mode controls whether CCE can assign the agent tasks in that MRD. If the agent is routable, CCE can assign tasks to the agent. If the agent is not routable, CCE cannot assign tasks to the agent.

The agent changes to routable/not routable through Finesse Media - Change Agent to Routable/Not Routable API calls.

Agent State

The agent's state in an MRD indicates the agent's current status and whether the agent is available to handle a task:

- Ready: The agent is available to handle a task.
- Reserved/Active/Paused/Work Ready/Interrupted: The agent is available to handle a task if the agent has not reached their maximum task limit in the MRD.
- Not Ready: The agent is not available to handle a task.

The agent changes to Ready and Not Ready through calls to the Finesse Media - Change Agent State API. The agent's state while working on a task depends on the actions the agent performs on the Finesse dialog related to the task, through calls to the Finesse Dialog - Take Action on Participant API.

How Mode and State Work Together to Determine if an Agent Receives Tasks

CCE will route an agent a task in the MRD if ALL of the following are true:

- The agent's mode is routable, and
- The agent is in any state other than NOT_READY, and
- The agent has not reached the maximum task limit in the MRD, and
- The agent is not working on a task in a different and non-interruptible MRD.

CCE will NOT route an agent a task in the MRD if ANY of the following are true:

- The agent's mode is not routable, or
- The agent is NOT_READY, or
- The agent has reached the maximum task limit in the MRD, or
- The agent is working on a task in a different and non-interruptible MRD.

Why Change the Agent's Mode to Not Routable?

By changing the agent's mode to not routable, you stop sending tasks to the agent without changing the agent's state to Not Ready. You may want to make an agent not routable if the agent is close to ending the shift, and needs to complete in progress tasks before signing out.

If an agent changes to Not Ready state while still working on tasks, CCE reports show those tasks as ended; time spent working on the tasks after going Not Ready is not counted. By making the agent not routable instead of Not Ready, the agent's time on task continues to be counted.

In RONA situations, in which agents do not accept tasks within the Start Timeout threshold for the MRD, Finesse automatically makes agents not routable. Finesse resubmits the tasks through for routing through SocialMiner. The application must make the agent routable in order for the agent to receive tasks again.

SocialMiner and Finesse Task States

In most cases, SocialMiner social contact states do not map directly to Finesse dialog states. For SocialMiner, social contacts are created when the customer submits a task request. For Finesse, the dialog with which the agent engages with the customer is created when the task is routed to the agent.

This table shows the relationships between SocialMiner social contact task states and Finesse dialog states.

SocialMiner Social Contact Task State	Finesse Dialog State
Unread: The task request has not been submitted to the contact center.	None
Queued: The task request is successfully submitted to the contact center as a result of creating a new task or resubmitting a task due to agent transfer, automatic transfer on agent logout, or automatic transfer for RONA.	None
Reserved: The task is assigned to an agent. This state includes all work on a task.	**Offered:** The dialog is being offered to the agent.
	Accepted: The agent accepted the dialog but has not started working on it.
	Active: The agent is working on the dialog.
	Paused: The agent paused the dialog.
	Wrapping Up: The agent is performing wrap up activity on the dialog.
	Interrupted: The agent is interrupted with a task from a non-interruptible Media Routing Domain. The agent cannot work on this task until the interrupting task is complete.
Handled: SocialMiner receives a handled notification from Finesse indicating that the task ended.	**Closed:** The agent ended the task. Finesse sends a handled notification to SocialMiner.

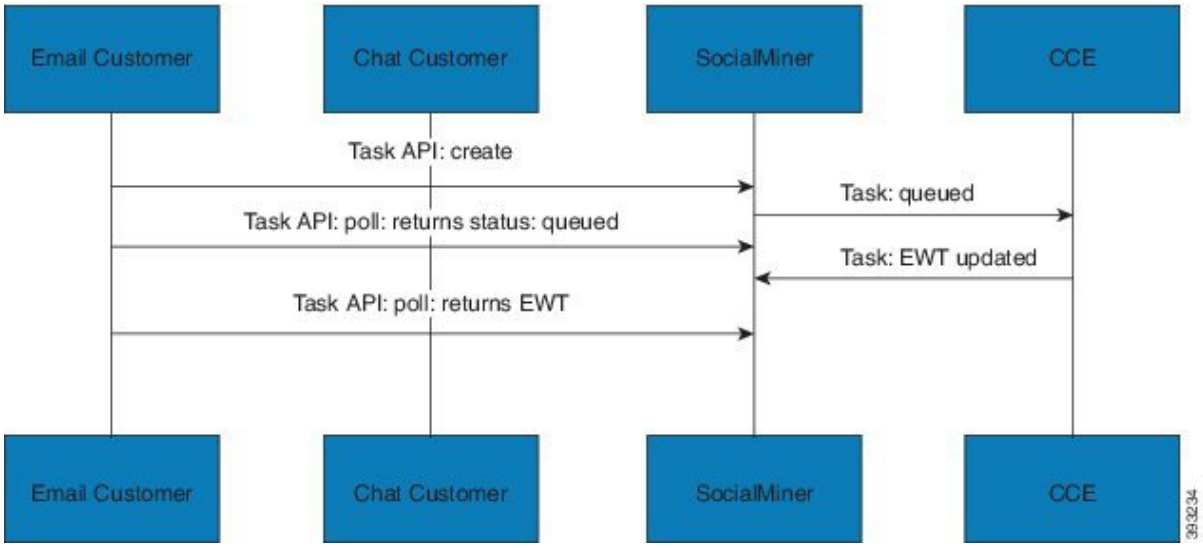
Task Routing API Request Flows

Task Routing API Basic Task Flow

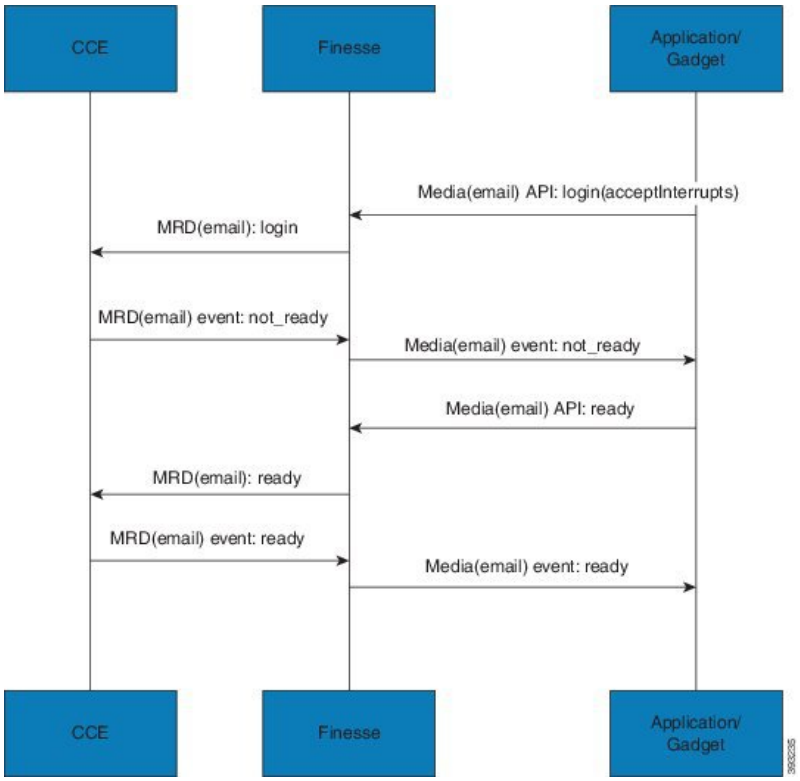
This topic provides the SocialMiner and Finesse API calls and events when an active email task is interrupted by a chat request.

In this scenario, the email MRD is interruptible. When the agent signs into the email MRD, the application uses the Finesse Media API to accept interrupts. The chat MRD is non-interruptible.

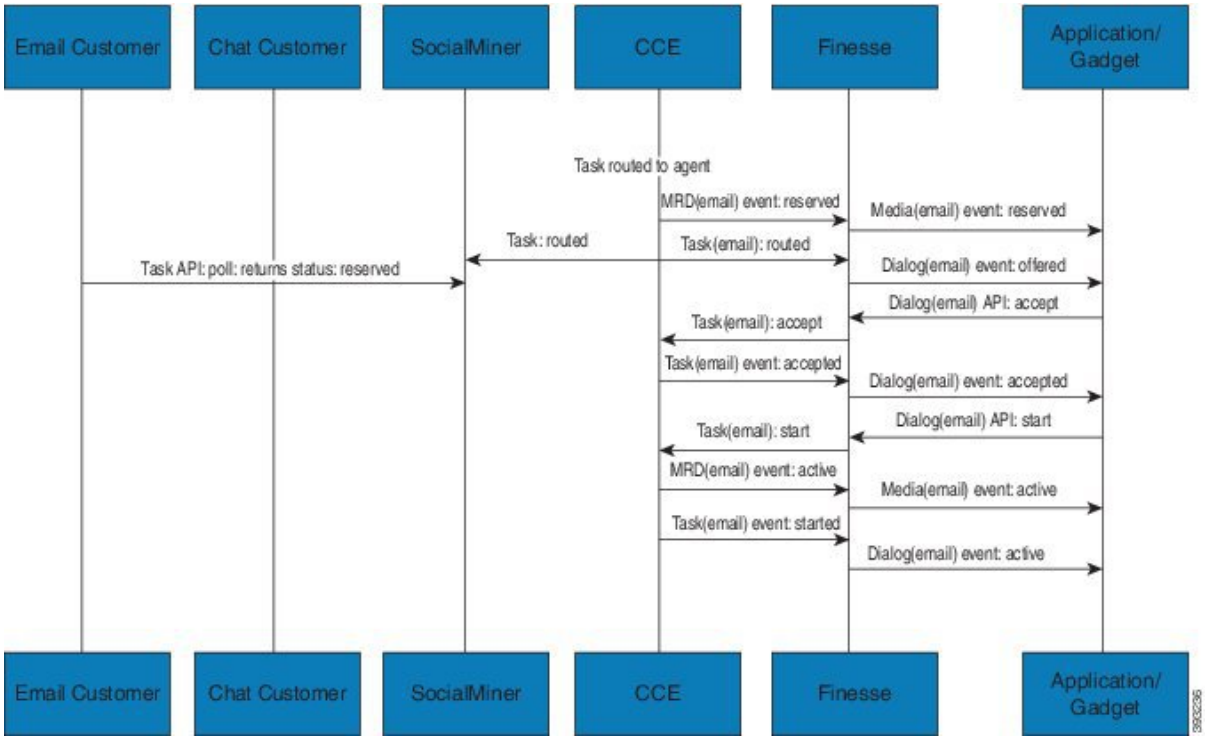
1. The email application submits a new email task request to CCE, and polls for status and Estimated Wait Time (EWT).



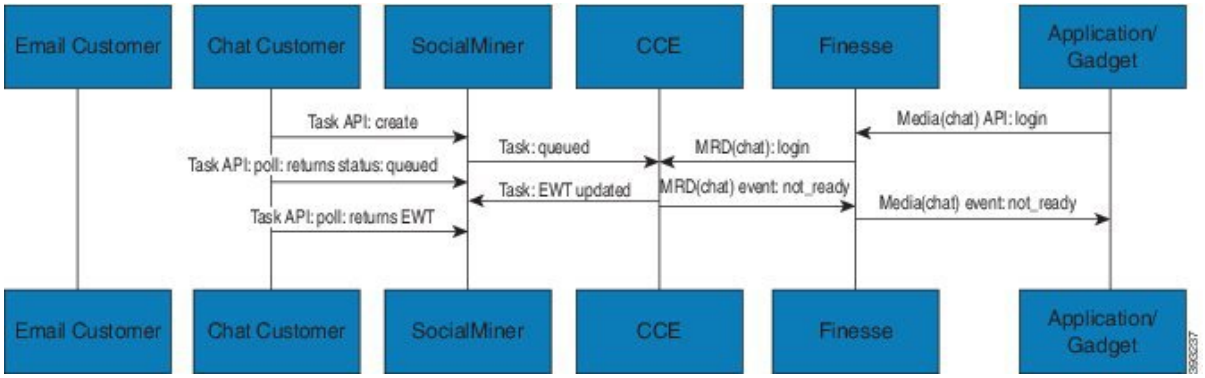
2. An agent signs in to the email MRD and changes state to Ready.



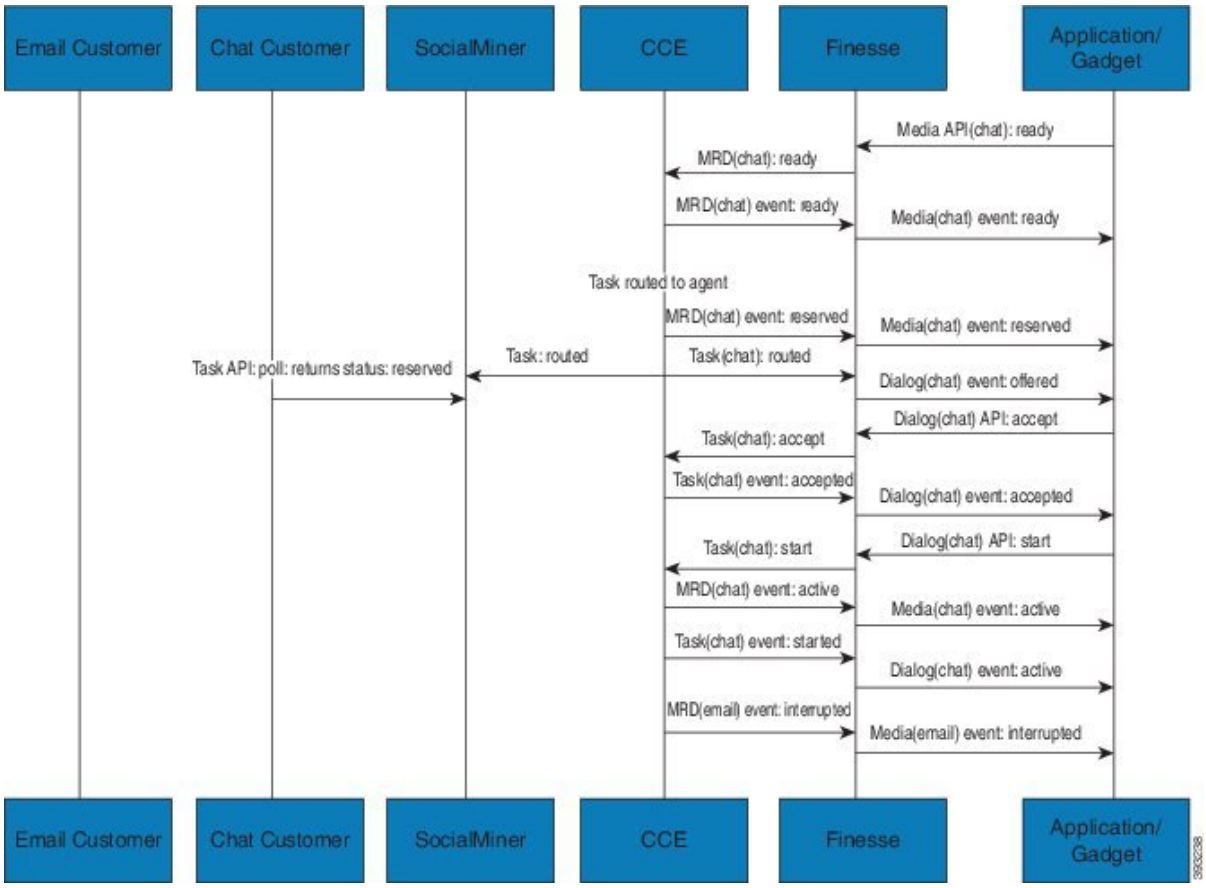
3. CCE assigns the agent the email task. The Call and ECC variables used to create the task are included in the dialog's media properties, and contain information such as the handle to the email. The variables can be used to reply to the email. The agent starts work on the email dialog in Finesse.



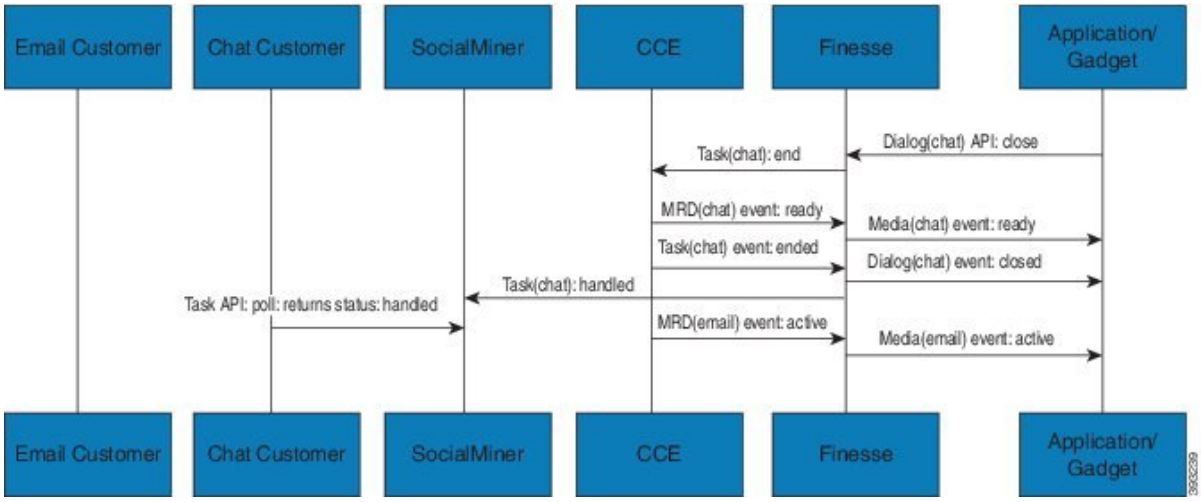
4. The chat application submits a new chat request, and polls for status and EWT. The same agent logs into the chat MRD.



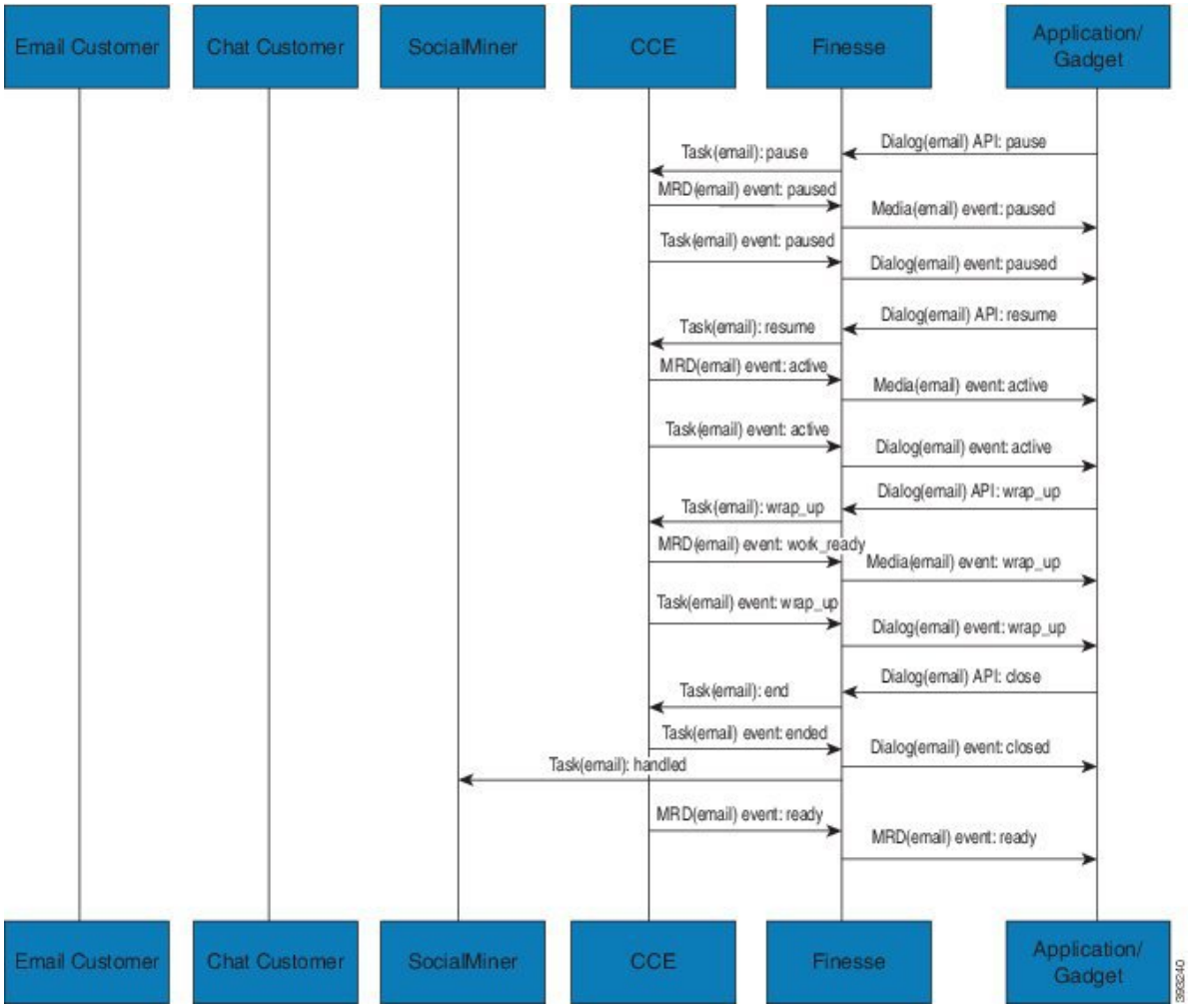
5. The agent changes state to Ready in the chat MRD. CCE assigns the chat task to the agent. The Call and ECC variables used to create the task are included in the dialog's media properties, and contain information such as the chat room URL. The variables can be used to join the chat room with the customer. The agent starts the chat dialog in Finesse. The Email dialog is interrupted.



6. The agent completes work on the chat dialog and closes the dialog. Finesse sends a handled event to SocialMiner for the chat task. The application is responsible for closing the chat room. The agent is not handling other non-interruptible dialogs, and the email dialog becomes active.

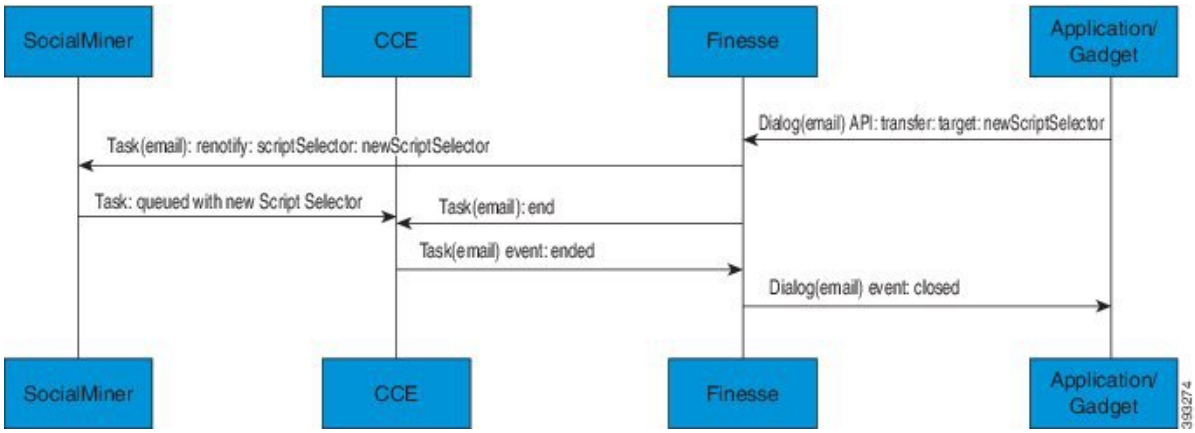


7. The agent continues working on the email dialog, including pausing, resuming, and wrapping up the dialog. The agent closes the dialog. Finesse sends a handle event to SocialMiner for the email task. The application is responsible for sending the email reply to the customer.



Task Routing API Agent Transfer Flow

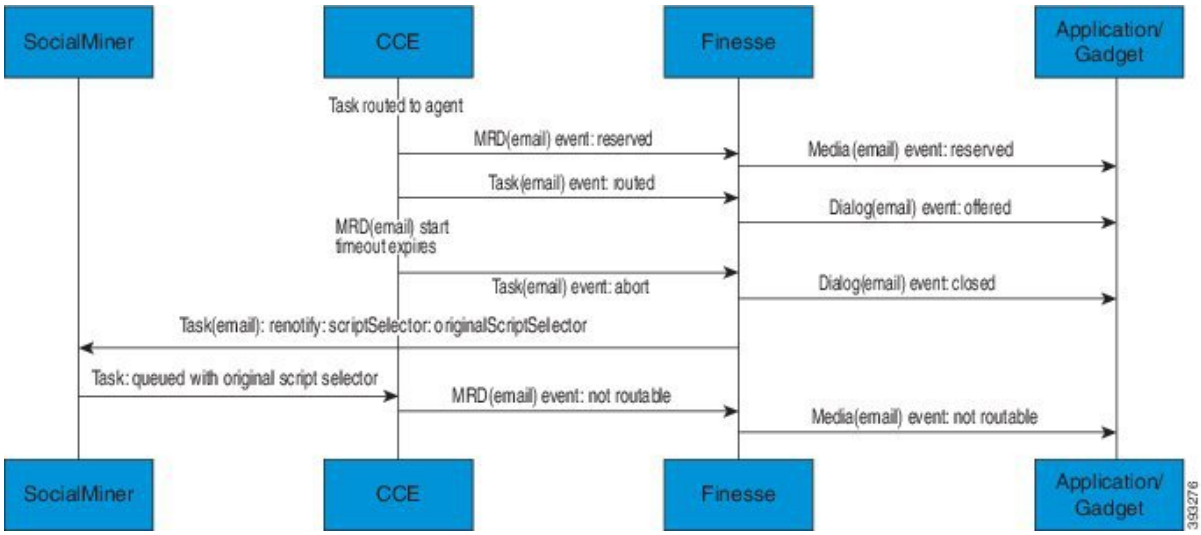
This illustration provides the SocialMiner and Finesse API calls and events when an agent transfers a task.



1. The agent transfers the dialog from the Finesse application, selecting the script selector to which to transfer the task.
2. Finesse resubmits the task to SocialMiner, and the task is queued to the script selector as a new task.
3. Finesse puts the original dialog in the CLOSED state, with the disposition code CD_TASK_TRANSFERRED. Finesse does not send a handled notification to SocialMiner.

Task Routing API RONA Flow

This illustration provides the SocialMiner and Finesse API calls and events in a RONA scenario, in which an agent does not accept an offered task within the Start Timeout threshold for the MRD.



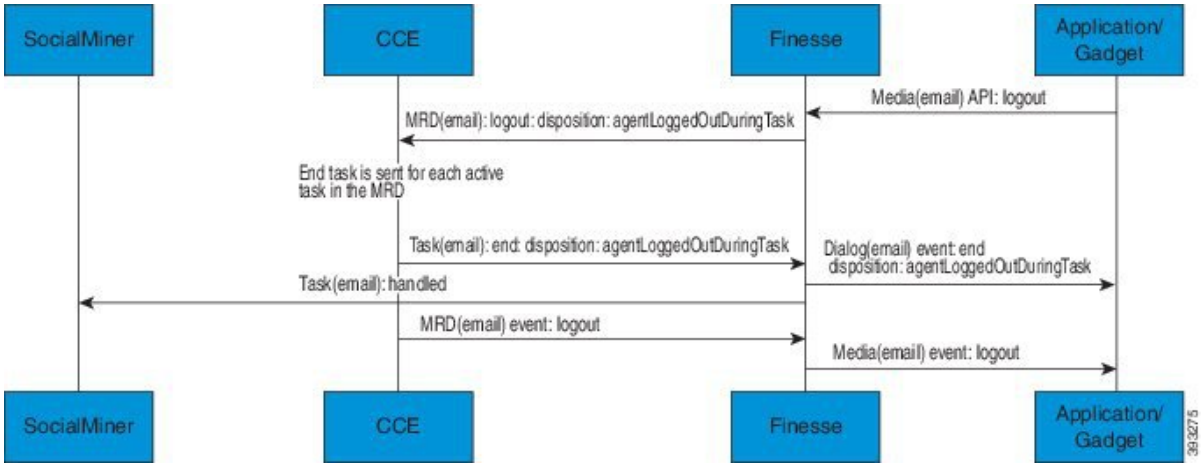
1. The task is routed to an agent, and the dialog is offered to the agent.
2. The Media Routing Domain's Start Timeout threshold expires.
3. CCE instructs Finesse to end the dialog. Finesse puts the dialog in the CLOSED state, with the disposition code CD_RING_NO_ANSWER. Finesse does not send a handled notification to SocialMiner.
4. The Finesse server on which the agent was last signed in resubmits the task to SocialMiner with the original script selector. The task is queued to the script selector as a new task.
5. CCE instructs Finesse to make the agent not routable in that Media Routing Domain, so that the agent is not routed more tasks.

Task Routing API Agent Sign Out with Tasks Flows

The Finesse Media - Sign Out API allows agents to sign out with assigned tasks. The dialogLogoutAction parameter set by the Media - Sign In API determines whether those tasks are closed or transferred when the agent signs out.

Close Tasks on Sign Out

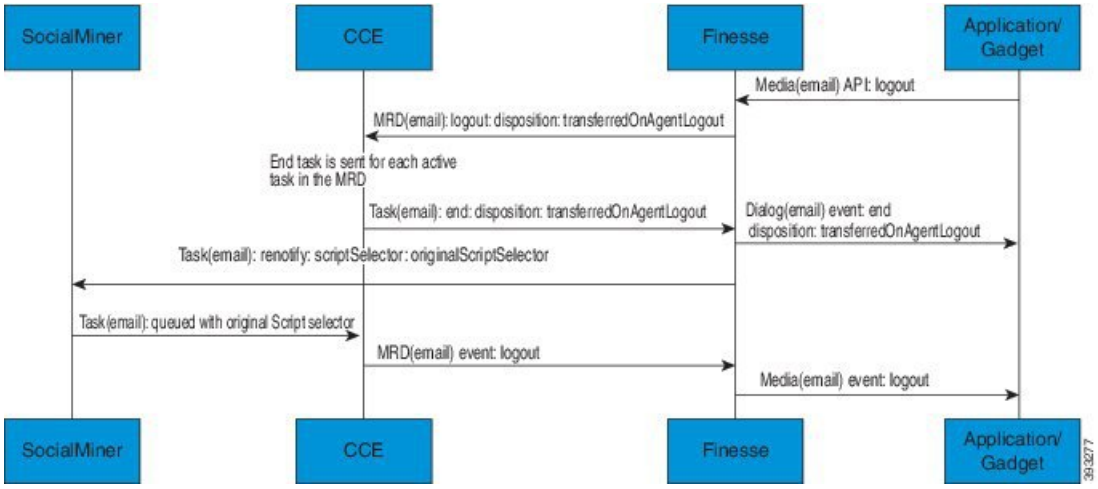
This illustration provides the SocialMiner and Finesse API calls and events when agents are set to have assigned tasks closed on sign out.



1. The agent requests to sign out of the MRD with an active task.
2. CCE instructs Finesse to end the task. Finesse puts the dialog in CLOSED state, with the disposition code CD_AGENT_LOGGED_OUT_DURING_DIALOG.
3. The agent is signed out of the MRD.

Transfer Tasks on Sign Out

This illustration provides the SocialMiner and Finesse API calls and events when agents are set to have assigned tasks transferred on sign out.



1. The agent requests to sign out of the MRD with an active task.
2. CCE instructs Finesse to end the dialog. Finesse puts the dialog in the CLOSED state, with the disposition code CD_TASK_TRANSFERRED_ON_AGENT_LOGOUT. Finesse does not send a handled notification to SocialMiner.

3. The Finesse server on which the agent was signed in resubmits the task to SocialMiner with the original script selector. The task is queued to the script selector as a new task.
4. The agent is signed out of the MRD.

Failover and Failure Recovery

Component	Failover/Failure Scenario	New Task Request Impact	Queued, Offered, and Active Task Impact
SocialMiner	MR connection fails. For example, there is a networking problem, the PG loses connection, or SocialMiner loses connection. Finesse loses connection with SocialMiner.	**New task requests from SocialMiner application**: New task requests fail, and the failures are delivered back to the application. Details of these failures are described in the next column. **Automatic transfer request from Finesse** (for transfer on sign out or RONA): Results in a lost transfer request. **Agent transfer request:** The request fails, and Finesse sends an error back to the application. Finesse retains the task.	**Queued tasks:** When tasks are submitted, they can be set to requeue on recovery. Typically, non-interactive tasks, such as email, are set to requeue on recovery because there is not a way to alert the customer that there was a problem while in queue. Interactive tasks, such as chat, are set not to requeue on recovery because the customer is waiting at an interface for an agent, and there is a way to alert the customer that there is a problem. If tasks are set to requeue on recovery, the task is resubmitted when the MR connection is reestablished. The status and statusReason of the contact does not change. If tasks are set NOT to requeue on recovery, the task's contact's status is marked discarded. The task's contact's statusReason is marked as follows: **SocialMiner failure:** NOTIFICATION_CCE_SOCIALMINER_SYSTEM_FAILURE **MR connection failure:** NOTIFICATION_CCE_CONNECTION_LOST **Offered and active tasks:** No impact.

Component	Failover/Failure Scenario	New Task Request Impact	Queued, Offered, and Active Task Impact
SocialMiner	SocialMiner overruns the new task queue limit. See the *Cisco SocialMiner Developer Guide* for the limit (https://developer.cisco.com/site/socialminer/documentation/).	**New task requests from SocialMiner application:** New task requests are discarded with the statusReason NOTIFICATION_RATE_LIMITED. **Automatic or agent transfer requests:** No impact	**Queued, offered, and active tasks:** No impact.
Finesse	Finesse loses connection with Agent PG or CTI Server	**New task request from SocialMiner application:** No impact **Automatic transfer requests from Finesse** (for transfer on logout or RONA): Automatic transfers are initiated on the Finesse server on which the agent was signed in. Any outage on that Finesse server can result in lost transfer requests. **Agent transfer request:** The request fails because Finesse is out of service, and Finesse retains the task.	Agents signed into media on the failed Finesse server are put into WORK_NOT_READY state and made not routable. Tasks on that server are preserved in their current state, and time continues to accrue towards the maximum task lifetime. The agent fails over to the secondary Finesse server, and must sign in to the media again. The agent is put into the previous state. If the agent doesn't have tasks, the agent is put in NOT_READY state. **Queued tasks:** No impact. **Offered tasks:** These tasks RONA because the agent cannot accept them. **Active tasks:** These tasks fail over to the other Finesse server and are recovered on that server. **Note** Any active tasks that were in INTERRUPTED state at the time of the lost connection change are recovered. However, these tasks change to the UNKNOWN state when the task is no longer INTERRUPTED. The agent can only close tasks when they are in the UNKNOWN state.

Component	Failover/Failure Scenario	New Task Request Impact	Queued, Offered, and Active Task Impact
Finesse	Agent logs out, or presence is lost while agent has active tasks	**New task request from SocialMiner application:** No impact **Automatic or agent transfer requests:** No impact	**Queued tasks:** No impact. **Offered tasks:** These tasks fail over to the other Finesse server and are recovered on that server. If a task's Start Timeout threshold is exceeded during failover, the task RONAs. **Active tasks:** If an agent logs out with active tasks, or agent presence is lost with active tasks, the tasks are either closed or transferred to the original script selector depending on how the agent was configured when signing into the MRD. If the tasks are transferred, the disposition code is CD_TASK_TRANSFERRED_AGENT_LOGOUT. If the tasks are closed, the disposition code is CD_AGENT_LOGGED_OUT_DURING_DIALOG.
Finesse application	Finesse application fails	**New task request from SocialMiner application:** No impact **Automatic or agent transfer requests:** No impact	**Queued tasks:** No impact. **Offered tasks:** These tasks may RONA depending on how the application is structured. A Task Routing application may prevent an agent from accepting a dialog when the application down because the agent cannot handle the dialog while the application is down. In this case, the dialog RONAs. **Active tasks:** Varies by application. Applications are responsible for managing the tasks while the application is down. Finesse retains the tasks, and the tasks are recovered once the application is restored.

Component	Failover/Failure Scenario	New Task Request Impact	Queued, Offered, and Active Task Impact
CTI Server or OPC	One CTI Server or one OPC fails	**New task request from SocialMiner application:** No impact **Automatic transfer requests from Finesse** (for transfer on logout or RONA): Results in lost transfer requests. **Agent transfer request:** The request fails, and Finesse retains the task.	**Queued tasks:** No impact. **Offered tasks:** These tasks fail over to the other Finesse server and are recovered on that server. If a task's Start Timeout threshold is exceeded during failover, the task RONAs. **Active tasks:** These tasks fail over to the other Finesse server and are recovered on that server. **Note** Any active tasks that were in INTERRUPTED state at the time of the lost connection change are also recovered. However, these tasks change to the UNKNOWN state when the task is no longer INTERRUPTED. The agent only can only close tasks when they are in the UNKNOWN state.
OPC	Both OPCs fail	**New task request from SocialMiner application:** No impact **Automatic or agent transfer requests:** Results in lost transfers.	**Queued tasks:** No impact **Offered and active tasks:** These tasks are lost

Task Routing Setup

Initial Setup

Step	Task	Notes
Set up CCE		
1	Configure Finesse with the AW, so that Finesse can access SocialMiner connection information. See Configure Finesse with the AW, on page 184.	

Step	Task	Notes
2	Configure a Network VRU and Network VRU scripts. See Configure Network VRU and Network VRU Scripts, on page 185.	
3	Configure the MR PG and PIM See Configure the Media Routing PG and PIM, on page 185.	
4	Set up the MR PG and PIM for SocialMiner. See Set up the Media Routing PG and PIM, on page 186.	
5	Add SocialMiner as an External Machine in the System Inventory. See Add SocialMiner as an External Machine, on page 186.	The system configures the following settings automatically in SocialMiner Administration: • Enables and configures the **CCE Multichannel Routing settings**. • Configures the Task feed and the associated campaign and Connection to CCE notification needed for the Task Routing feature.
6	Configure the following in Unified CCE Administration or Configuration Manager: • Media Routing Domains • Call types • Dialed numbers • Skill groups or precision queues • ECC variables • Agent desk settings See Unified CCE Administration and Configuration Manager Tools, on page 187.	
7	Increase the TCDTimeout registry key value, if you are using precision queues and will be submitting potentially long tasks, like email. See Increase TCDTimeout Value, on page 189.	
9	Create routing scripts See Create Routing Scripts for Task Routing, on page 190.	
Create SocialMiner and Finesse Applications		

Step	Task	Notes
10	Create the SocialMiner multichannel application to begin task requests. See Sample SocialMiner HTML Task Application, on page 191.	
11	Create the Finesse applications to manage nonvoice agent and dialog states. See Sample Finesse Code for Task Routing, on page 191.	
Set up Finesse		
12	Upload the Finesse desktop gadgets to the desktop layout (optional). See the *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-list.html.	

Configure Finesse with the AW

Finesse connects to SocialMiner to transfer Task Routing tasks and resubmit tasks for RONA. The Finesse AWDB user requires special database permissions to access SocialMiner connection information. Map the user to the Side A, AWDB, and primary databases. In these databases, give the user the db_datareader and public roles.

Before you begin

Configure the Contact Center Administration and Data Server Connection Settings on Finesse. You need the Finesse AWDB username to complete this procedure.

See the *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-list.html.

Procedure

Step 1 Determine whether the Finesse AWDB user is a domain user or a SQL user. If the user is a domain user, proceed to the last step in the procedure (step 7). Otherwise, complete all of the steps.

Step 2 Launch Microsoft SQL Server Management Studio on the Unified CCE Administration Client workstation.

Step 3 Connect to the Side A Logger using the default credentials.

Step 4 Navigate to **Security** > **Logins**. Right-click the Finesse AWDB username.
The Login Properties screen opens.

Step 5 Select the **User Mapping** page, and perform the following:

a) Verify that the databases associated with Side A and AWdb are checked.
b) Check the master database.
c) Select the Side A database. In the **Database role membership for** section, check the **db_datareader** and **public** roles.

Repeat this step for the AWdb and master databases.

d) Click **OK**.

Step 6 Repeat these steps on the Side B Logger.

Step 7 Execute the following SQL queries as the SQL administrative user "sa" or as a user with sysadmin privileges.

For <user>, enter the Finesse AWDB username. If the Finesse AWDB user is a domain user, rather than a SQL user, use the <domain\user> format.

```
USE master
GO
GRANT CONTROL ON CERTIFICATE :: UCCESymmetricKeyCertificate TO "<user>"
GRANT VIEW DEFINITION ON SYMMETRIC KEY :: UCCESymmetricKey TO "<user>"
```

Configure Network VRU and Network VRU Scripts

The Network VRU is used to queue nonvoice tasks if an agent is not available to handle them. The Network VRU Script is used to return estimated wait time to customers. For more information on writing routing scripts that return estimated wait time, see the *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html.

When you configure the Network VRU Script, you specify whether it is interruptible. The **Interruptible** setting for the Network VRU Script controls whether the script can be interrupted (for example if an agent becomes available). This setting is not related to the Media Routing Domain **Interruptible** setting, which controls whether an agent working on a task in that MRD can be interrupted by a task from a non-interruptible MRD.

Procedure

Step 1 In Configuration Manager, use the **Network VRU Explorer** tool to configure and save a type 2 VRU.

Step 2 Use the **Network VRU Script List** tool to add a Network VRU Script that references this Network VRU.

You can accept the default values.

Configure the Media Routing PG and PIM

Procedure

Step 1 In Configuration Manager, open the PG Explorer tool to configure a media routing PG.

Step 2 Create a media routing PIM and routing client for SocialMiner.

Write down the Logical Controller ID and the Peripheral ID. You will use them when you set up the PG.

Step 3 On the Peripheral tab in the PG Explorer tool, check the **Enable post routing** check box.

Step 4 On the Routing Client tab in the PG Explorer tool, select the **Multichannel** option from the **Routing Type** drop-down list box.

Note The **Default call type** setting is not supported for tasks submitted through the Task Routing APIs.

Step 5 On the Advanced tab in the PG Explorer tool, select the type 2 Network VRU that you created.

Set up the Media Routing PG and PIM

Set up the Media Routing PG and PIM

Procedure

Step 1 From Cisco Unified CCE Tools, select **Peripheral Gateway Setup**.

Step 2 On the Components Setup screen, in the Instance Components panel, select the PG Instance component. If the PG does not exist, click **Add**. If it exists, click **Edit**.

Step 3 In the Peripheral Gateways Properties screen, click **Media Routing**. Click **Next**.

Step 4 Click **Yes** at the prompt to stop the service.

Step 5 From the Peripheral Gateway Component Properties screen, click **Add**, select the next PIM, and configure with the Client Type of Media Routing as follows.

a) Check **Enabled**.
b) In the **Peripheral Name** field, enter `MR`.
c) In the **Peripheral ID** field, enter the Peripheral ID that you recorded when you configured the Media Routing PG and PIM.
d) For **Application Hostname (1)**, enter the hostname or IP address of SocialMiner.
e) By default, SocialMiner accepts the MR connection on **Application Connection Port** 38001. The Application Connection Port setting on SocialMiner must match the setting on the MR PG. If you change the port on one side of the connection, you must change it on the other side.
f) Leave the **Application Hostname (2)**, field blank.
g) Keep all other values.
h) Click **OK**.

Step 6 On the Peripheral Gateway Component Properties screen, enter the Logical Controller ID that you recorded when you configured the Media Routing PG and PIM.

Step 7 Accept defaults and click **Next** until the Setup Complete screen opens.

Step 8 At the Setup Complete screen, check **Yes** to start the service. Click **Finish**.

Step 9 Click **Exit Setup**.

Step 10 Repeat this procedure for Side B.

Add SocialMiner as an External Machine

When you add SocialMiner as an External Machine in the Unified CCE Administration System Inventory, the system automatically performs the following SocialMiner configuration:

- Enables and completes the **CCE Configuration for Multichannel Routing** settings in SocialMiner Administration.

  These settings include the hostnames of the MR PGs and the Application Connection Port you specified when setting up the MR PG and PIM.

- Configures the Task feed and the associated campaign and Connection to CCE notification needed for the Task Routing feature, with the following names:
  - **Task feed:** Cisco_Default_Task_Feed
  - **Campaign:** Cisco_Default_Task_Campaign
  - **Notification:** Cisco_Default_Task_Notification
  - **Tag:** cisco_task_tag

Note If the Task feed has been configured to use a different tag, the Connection to CCE notification is configured to use that tag.

Procedure

Step 1 Navigate to **Unified CCE Administration** > **Infrastructure** > **Inventory**.

Step 2 Click Add.

Step 3 Select SocialMiner from the drop-down list.

Step 4 Enter the fully qualified domain name (FQDN), hostname or IP address in the **Hostname** field.

Note The system attempts to convert the value you enter to FQDN.

Step 5 Enter the SocialMiner Administration username and password.

Step 6 Select the **Side A** and **Side B** Media Routing PGs.

Step 7 Enter the Application Port you specified when setting up the MR PG and PIM. The default value is 38001.

Step 8 Click **Save**.

Unified CCE Administration and Configuration Manager Tools

This topic explains the Unified CCE Administration and Configuration Manager tools you need to configure Task Routing.

Before you begin

For details on the procedures for these steps, refer to the Unified CCE Administration online help and the Configuration Manager online help.

Procedure

Step 1 Sign in to Unified CCE Administration.

Step 2 From the **Manage** menu, configure the following:

Item to Configure	Details
Media Routing Domains	Create an MRD for each type of task that the third-party multichannel application submits to CCE (email, chat, and so on).
Precision Queues	Configure either skill groups or precision queues. If you configure precision queues: • For **Media Routing Domain**, select one of the Task Routing MRDs you created. • Associate agents with attributes that are part of the precision queue steps.

Step 3 Launch Configuration Manager.

Step 4 Configure the following:

Item to Configure	Details
Call Types	Create call types for Task Routing.
Dialed Numbers	Create dialed numbers for Task Routing. Add the numbers or strings that the custom application will use when submitting task requests. • On the **Attributes** tab, select a Task Routing MRD from the **Media routing domain** drop-down list box. • On the **Dialed Number Mapping** tab, map the script selector to a call type you created for Task Routing. **Important** Each dialed number must be associated with a call type. Default call type is not supported for tasks submitted with Task Routing APIs.
Skill Groups	Configure either skill groups or precision queues. If you configure skill groups: • For **Media Routing Domain**, select one of the Task Routing MRDs you created. • Assign agents to the skill group.

Item to Configure	Details
Expanded Call Variable	You can use an existing Expanded Call Variable, or you can create an Expanded Call Variable for Task Routing, depending on the needs of your third-party multichannel application. **Note** Arrays are not supported with the Task Routing feature. CCE solutions support the Latin 1 character set only for Expanded Call Context variables and Call variables when used with Finesse and SocialMiner.
Agent Desk Settings	If agents will use a Task Routing gadget in the Finesse desktop, leave the **Logout inactivity time** setting for those agents blank, or remove the existing value. Otherwise, if the agent exceeds the **Logout inactivity time** in the voice MRD, the agent is logged out of the Cisco Finesse desktop, even if the agent is actively working on tasks from nonvoice MRDs. The agent needs log into the desktop again to continue working on the nonvoice tasks.

Increase TCDTimeout Value

Complete this procedure only if you are using precision queues and routing tasks with potentially long durations, like emails.

Several precision queue fields in the Termination_Call_Detail record are not completed until the end of a task. These precision queue fields are blank for tasks whose durations exceed the TCDTimeout registry key value. The default value of theTCDTimeout registry key is 9,000 seconds (2.5 hours).

If you are configuring a system to handle email or other long tasks, you can increase the TCDTimeout registry key value to a maximum of 86,400 seconds (24 hours).

Change the registry key on either the Side A or B Router.

Procedure

Modify the following registry key: `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Icm\<instance name>\Router<A/B>\Router\CurrentVersion\Configuration\Global\TCDTimeout`.

Context Service

Cisco Context Service is a cloud-based omnichannel solution for Cisco Contact Center Enterprise Solutions. It enables you to capture your customer's interaction history by providing flexible storage of customer-interaction data across any channel.

Various components in the CCE Solution provide out of the box integration with Context Service. Context Service also provides an API for integration with your own applications or third-party applications to capture end-to-end customer-interaction data.

For more information about Context Service and to check service availability, see https://cisco.com/go/contextservice.

For information on Context Service setup, the the "Context Service" chapter.

Related Topics

Context Service , on page 59

Context Service for Task Routing Tasks

Context Service can store data for Task Routing task contacts. When Context Service is enabled, SocialMiner selects pieces of data from an incoming task request and saves it as an activity in the cloud.

You can specify the media type of the request in the task request. If you don't specify the media type, then the media type defaults to “event”.

If you have already saved the task request information in request and include its reference URL in the task request, SocialMiner doesn't create a new activity. SocialMiner passes the existing Request ID directly to Unified CCE for use by the Finesse clients.

When creating a new contact, SocialMiner looks up the customer by the author field of the SocialMiner social contact. The results of the lookup determine whether the contact includes a customer reference, as follows:

- If zero or many customers are returned, the contact doesn't include a customer reference.
- If one customer is returned, the contact includes that customer reference.

SocialMiner populates the following fields from the Context Service cisco.base.pod field set for Task Routing task contacts:

- **Context_Notes:** This field is populated with the value of SocialContact.description.
- **Context_POD_Source_Cust_Name:** This field is populated with the value of SocialContact.author.
- **Context_POD_Source_Email:** To populate this field, SocialMiner looks up the email address using the SocialContact.author field.

Create Routing Scripts for Task Routing

For complete multichannel scripting information, see the *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html.

Important Ensure that the routing scripts include skill groups or precision queues from the appropriate Media Routing Domains to handle all of the types of tasks that can be routed with the scripts. For example, if a script is used to route email tasks, be sure that the script includes skill groups or precision queues from an email MRD.

Sample Code for Task Routing

Cisco Systems has made sample Task Routing application code for SocialMiner and Finesse available to use as baselines in building your own applications.

Sample SocialMiner HTML Task Application

The sample SocialMiner HTML Task application:

- Submits task requests to CCE.
- Retrieves and displays the estimated wait time, if it has been configured in CCE.

Note You cannot copy and paste this code to achieve a working application. It is only a guideline.

The sample application uses the Task API. For more information about how to use the Task API, see the *Cisco SocialMiner Developer Guide* at https://developer.cisco.com/site/socialminer/documentation/.

Procedure

Step 1 Download the sample HTML Task application from DevNet: https://developer.cisco.com/site/task-routing/.

Step 2 Read the sample application's **readme.txt** file to complete the prerequisites and use the sample application.

Sample Finesse Code for Task Routing

The Finesse sample Task Management Gadget application lets agents perform the following actions in individual nonvoice Media Routing Domains:

- Sign in and out.
- Change state.
- Handle tasks.

The sample gadget also signals the Customer Context gadget to display a customer record.

Note You cannot copy and paste this code to achieve a working application. It is only a guideline.

For more information about how to use the APIs available for Task Routing, see the *Cisco Finesse Web Services Developer Guide* at https://developer.cisco.com/site/finesse/.

Procedure

Step 1 Download the sample Task Management Gadget application (TaskManagementGadget-x.x.zip) from DevNet: https://developer.cisco.com/site/task-routing/.

Step 2 Read the sample application's **readme.txt** file to complete the prerequisites and use the sample application.

For more information about uploading third-party gadgets to the Finesse server, see the "Third Party Gadgets" chapter in the *Cisco Finesse Web Services Developer Guide* at https://developer.cisco.com/site/finesse/.

For more information about adding third-party gadgets to the Finesse desktop, see the "Manage Third-Party Gadgets" chapter in the *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/tsd-products-support-series-home.html.

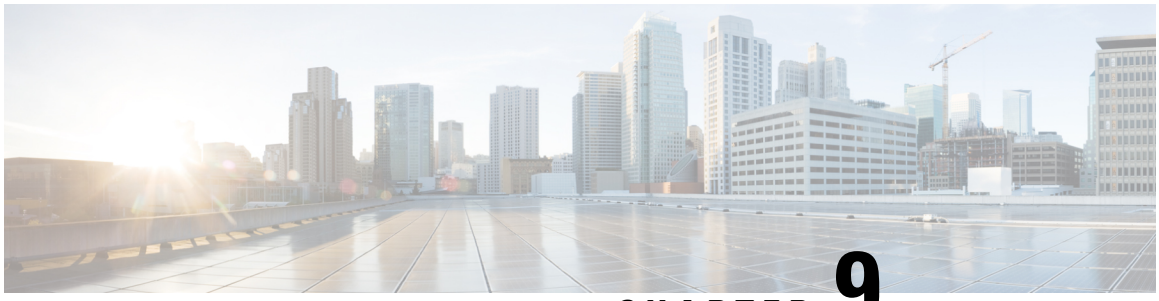
Task Routing Reporting

Cisco Unified Intelligence Center CCE reports include data for voice calls and nonvoice Task Routing tasks.

You can filter these All Fields and Live Data report templates by Media Routing Domain:

- Agent Real Time
- Agent Skill Group Real Time
- Enterprise Skill Group Real Time
- Peripheral Skill Group Real Time All Fields
- Precision Queue Real Time All Fields
- Agent Precision Queue Historical All Fields
- Agent Skill Group Historical All Fields
- Peripheral Skill Group Historical All Fields
- Precision Queue Abandon Answer Distribution Historical
- Precision Queue Interval All Fields
- Skill Group Abandon-Answer Distribution Historical
- Precision Queue - Live Data
- Skill Group - Live Data

See the *Reporting Concepts for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html for information about multichannel reporting data.



CHAPTER 9

Unified Communications Manager Extension Mobility

Capabilities

Extension Mobility is a Unified Communications Manager feature that you can use in Unified CCE. The feature enables users to temporarily configure a phone as their own by logging in to that phone. Once a user logs in, the phone adopts the individual user device profile information, including line numbers, speed dials, services links, and other user-specific properties of a phone.

Cisco Extension Mobility (EM) works on phones that are located within the same Cisco Unified Communications Manager cluster. Cisco Extension Mobility Cross Cluster (EMCC) works on phones that are located in different Cisco Unified Communications Manager clusters.

The main documentation on this feature is in the Unified Communications Manager documentation. For more information, see the following sources:

Information Type	Sources
Design considerations	*Cisco Collaboration System Solution Reference Network Designs* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html
Feature description and configuration	*Feature Configuration Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html
Extension Mobility API	https://developer.cisco.com/site/extension-mobility/

Configuration

You configure EM and EMCC in the Cisco Unified Communications Manager. Take into account the following interactions between Unified CCE and Unified Communications Manager for successful implementation of EM and EMCC within a Unified CCE solution:

- For Unified CCE configurations with multiline agent phone line control on the PG, configure all directory numbers for the user profile in Cisco Unified Communications Manager as follows:

Setting	Value
Maximum Number of Calls	2
Busy Trigger	1

- For Unified CCE configurations with single-line agent phone line control on the PG, configure the secondary lines (but not the primary ACD line) for the directory number of the user profile in Cisco Unified Communications Manager as follows:

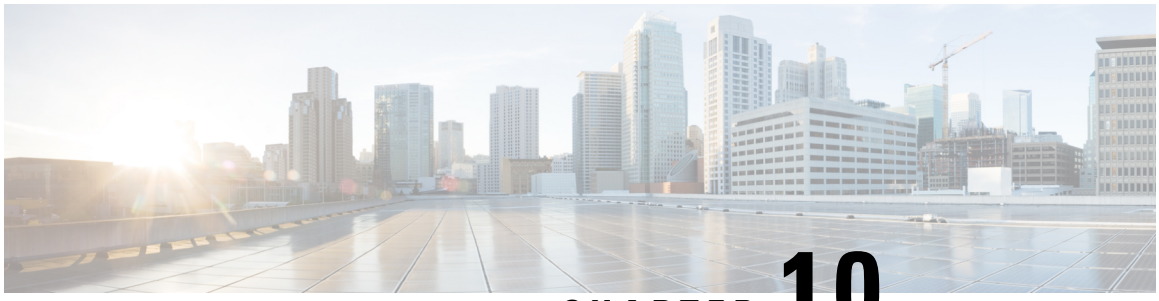
Setting	Value
Maximum Number of Calls	4
Busy Trigger	2

- You cannot use phones with an **IP Addressing Mode** of **IPv6 Only** for Cisco Extension Mobility. If you want to use Cisco Extension Mobility with the phone, you must configure the phone with an **IP Addressing Mode** of **IPv4 Only** or **IPv4 and IPv6**.
- Agents can log in to multiple devices, depending on the **Intra-cluster Multiple Login Behavior** service parameter. You can set this parameter for EM implementations. EMCC implementations require that you set this parameter for multiple logins.

  If an agent fails to log out of a device, another agent who attempts to access that device gets a "shared line" error. Follow these Unified Communications Manager configuration guidelines to avoid shared line errors:

  - For EM implementations with hard phones, set the **Intra-cluster Multiple Login Behavior** Extension Mobility service parameter to "Auto Logout".
  - For EM implementations with a mix of hard and IP phones and for all EMCC implementations, limit the time that an agent can remain logged in to a device. Set the **Intra-cluster Maximum LoginTime** service parameter to the typical time that an agent remains logged in to a device during a shift.

For more information on Extension Mobility with Unified CCE, see *UCCE Integration with CM Configuration Example* at https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-enterprise/117777-config-ucce-00.html.



CHAPTER 10

Whisper Announcement

Capabilities

Whisper Announcement plays a brief, prerecorded message to an agent just before the agent connects with each caller. The announcement plays only to the agent; the caller hears ringing (based on existing ring tone patterns) while the announcement plays.

The content of the announcement can contain information about the caller that helps prepare the agent to handle the call. The information can include caller language preference, choices the caller made from a menu (Sales, Service), customer status (Platinum, Gold, Regular), and so on.

After Whisper Announcement is enabled, the played announcements are specified in the call routing scripts. The determination of which announcement to play is controlled in the script and is based on various inputs, such as the dialed number, a customer ID look up in your customer database, or selections you made from a VRU menu.

Functional Limitations

Whisper Announcement is subject to these limitations:

- Announcements do not play for outbound calls made by an agent. The announcement plays for inbound calls only.
- For Whisper Announcement to work with agent-to-agent calls, use the SendToVRU or TranslationRouteToVRU node before you transfer the call to the agent. Transfer the call to Unified CVP before you transfer the call to another agent. Then, Unified CVP can control the call and play the announcement, regardless of which node transfers the call to Unified CVP.
- Announcements do not play when the router selects the agent through a label node.
- CVP Refer Transfers do not support Whisper Announcement.
- Whisper Announcement supports Silent Monitoring with this exception: For Unified Communications Manager-based Silent Monitoring, supervisors cannot hear the announcements themselves. The supervisor desktop dims the Silent Monitor button while an announcement plays.

- Only one announcement can play for each call. While an announcement plays, you cannot put the call on hold, transfer, or conference; release the call; or request supervisor assistance. These features become available again after the announcement completes.
- The codec settings for Whisper Announcement recording and the agent's phone must match. For example, if Whisper Announcement is recorded in G.711 ALAW, the phone must also be at G.711 ALAW. If Whisper Announcement is recorded in G.729, the phone must support or connect using G.729.
- Forking happens in Gateway in NBR only when a caller is connected to the agent (with two-way audio). Whisper announcement is played only with one way audio with agent (before connecting to the caller).
- In an IPv6-enabled environment, Whisper Announcement might require extra Media Termination Points (MTPs).

Deployment Tasks

The following list shows the high-level tasks that are required to deploy Whisper Announcement. Individual steps are covered in more detail in later sections.

1. Ensure your deployment meets the baseline requirements for software, hardware, and configuration described in the System Requirements and Limitations section. See the *Solution Design Guide for Cisco Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html.
2. Create Whisper Announcement Audio Files, on page 196.
3. Deploy Whisper Announcement Audio Files to Media Server, on page 197.
4. Configure Whisper Service Dialed Numbers, on page 197.
5. Add Whisper Announcement to Routing Scripts, on page 199.
6. Fail-Safe Timeout for Whisper Announcement in Unified CCE, on page 201.

Example scripts that enable Whisper Announcement are installed with your system. For information about these scripts and how to access them, see Whisper Announcement Sample Scripts, on page 202.

Create Whisper Announcement Audio Files

You must create audio files for each different Whisper Announcement you want to use on your system; for example, “Sales, English” or “Soporte Técnico en Español.” Create the files using the recording tool of your choice.

When recording your files, follow these rules:

- The media files must be in wave (.wav) format. Your wave files must match Unified CVP encoding and format requirements (G729, CCITT G.711 A-Law and U-law 8 kHz, 8 bit, mono).
- To avoid cutting off files when they are played, make sure they do not exceed the Whisper Announcement play limit (15 seconds).
- Test your audio files. Ensure that they are not cut off and that they are consistent in volume and tone.

- To reduce the likelihood of scripting errors, decide ahead of time on a file-naming convention that is easy for you and others to remember. For example, en_sales.wav, sp_support.wav.

Deploy Whisper Announcement Audio Files to Media Server

Deploy your whisper audio files to your Unified CVP media server using whatever file-transfer method you prefer. The most important consideration is where on the server to place the files. HTTP requests for media server audio files are constructed as

`http://<media_server>/<locale_directory>/<application_directory>/<file_name>.`

The CVP defaults for the locale and application directories are `en-us/app`. Unified CCE automatically adds `en-us/app` to the server name when making HTTP requests for media files.

For example, if:

- The script node that defines the media server has a value of `http://myserver.mydomain.com` and
- The script node that defines the audio file to play has a value of `en_sales.wav`

Then the HTTP request for the file is automatically constructed as

`http://myserver.mydomain.com/en-us/app/en_sales.wav`

If you store your files in a different locale and application directory, your routing scripts must include variable nodes that define those alternate locations. Make note of the directories in which you place your files and communicate the locations to your script authors.

Make sure that the directories in which you deploy your files have the appropriate permissions to allow Read access.

CVP with the Streaming Audio (Helix) and Whisper Announcement

You must set the **user.microapp.media_server** variable, to point to the whisper announcement .wav file, for the CVP Whisper Announcement feature to work while Streaming Audio feature (using Helix) is also on. This is achieved by setting the **Call.WhisperAnnouncement** variable to the complete URL of the whisper announcement wav file. The **Call.WhisperAnnouncement** variable should be put in using the `http://<VXMLserverip>:7000/CVP/audio/XXX.wav` URL format.

Using a Default Media Server

Optionally, CVP lets you define a default media server. (You do this in the CVP Operations Console; see your CVP documentation for more information.) If a default media server is defined in CVP, script authors need not identify the media server in their call routing scripts provided the files that they request are available from that server.

Configure Whisper Service Dialed Numbers

For Whisper Announcement, Unified CVP uses two different dialed numbers when transferring a call to an agent:

- The first number calls the ringtone service that the caller hears while the whisper plays to the agent. The CVP default for this number is 91919191.
- The second number calls the whisper itself. The Unified CVP default for this number is 9191919100.

Note Whisper Announcement dialed number is always an extension of the Ringtone dialed number with an extra two zeros at the end.

For Whisper Announcement to work, your dial plan must include both of these numbers. The easiest way to ensure coverage is through the use of wild cards such as 9191*.

Configure Dialed Numbers

You configure the dialed numbers for Whisper Announcement in the Unified CVP Operations Console at **System** > **Dialed Number Pattern** > **Add new**. For the Dialed Number Pattern Types, select **Enable Local Static Route**. Once **Enable Local Static Route** is checked, select either **Route to Device** or **Route to SIP Server Group** for VXML gateways. Then save and deploy the dialed number.

It may be necessary to override the dialed number plan for the default Whisper DN, if the default DN conflicts with the overall dial number plan.

Change the Whisper Announcement Default Dialed Number

To override the DN pattern from the SIP subsystem level in CVP OAMP:

Procedure

Step 1 Select **Device Management > Unified CVP Server**.

Step 2 Select the Call Server on which to override the default whisper DN.

Step 3 Select the SIP tab.

Step 4 Override the default value of 91919191 configured under the **DN on the Gateway to play the ringtone** field.

Step 5 Click **Save & Deploy**.

Configure Ringtone Dialed Number

To configure the Ringtone dialed number in the CVP Operations Console:

1. Select **Device Management** > **Unified CVP Server**.
2. Select the Call Server on which you want to configure the settings.
3. Select the SIP tab.
4. In the **DN on the Gateway to play the ringtone** field, configure the default Ringtone dialed number Pattern.

Dialed Number in the Dial-Peer

In addition to configuring the dial plan in Unified CVP, examine your IOS dial-peer. Make sure that the dialed number setting in your dial-peer configuration accommodates both of the whisper service dialed numbers.

Add Whisper Announcement to Routing Scripts

To enable Whisper Announcements, use the Script Editor to modify your routing scripts as follows:

- Specify the WhisperAnnouncement call variable
- Specify the Unified CVP media server and location of whisper audio files
- Specify other required variables

For more information, see Whisper Announcement Sample Scripts, on page 202.

Specify WhisperAnnouncement Call Variable

To include Whisper Announcement in a script, insert a Set Variable node that references the WhisperAnnouncement call variable. The WhisperAnnouncement variable causes a whisper to play and specifies the audio file it should use. Typically, you use a single whisper prompt for a single call type. As a result, you use only one WhisperAnnouncement set node for each script. However, as needed, you can set the variable at multiple places in your scripts to allow different announcements to play for different endpoints. For example, for skills-based routing, you can specify the variable at each decision point used to select a particular skill group or Precision Queue.

Note Only one Whisper Announcement can play for each call. If a script references and sets the WhisperAnnouncement variable more than once in a single path through a script, the last value to be set is the one that plays.

Use these settings in the Set Variable node for Whisper Announcement:

- Object Type: Call.
- Variable: Must use the WhisperAnnouncement variable.
- Value: Specify the filename of the whisper file. For example: “my_whisper.wav” or “my_whisper”.
  - Specify the filename only, not its path.
  - You must enclose the filename in quotation marks.
  - The filename is not case sensitive.
  - The filename cannot include spaces or characters that require URL encoding.
  - The .wav extension is optional. If you omit it, Unified CVP adds it automatically in the HTTP request.

Specify Unified CVP Media Server Information

If you define a default media server in your CVP Operations Console and it is the server from which you serve your whisper files, then you need not specify the media server in your routing scripts. However, if you do not define a default media server, or if you store your whisper file on a server other than the default, then your scripts must include a Set Variable node that identifies that server.

To specify your media server, use the following settings in the Set Variable node:

- Object Type: Call.
- Variable: Must use the user.microapp.media_server ECC variable.
- Value: Specify the HTTP path to the server. For example: “http://myserver.mydomain.net.” You must enclose the path in quotes.
- Alternately you can specify an IP address in place of a DNS. Include the listening port number if the media server web server listens on a port other than 80 (for HTTP) or 443 (for HTTPS).

Specify Whisper File Locale and Application Directories

CVP uses a default storage directory for media files: <web_server_root>/en-us/app. To take advantage of this, Unified CCE call routing scripts automatically add “en-us/app,” to the server name when constructing HTTP requests for media files. For example:

- If the script node that defines the media server has a value of “http://myserver.mydomain.com” and...
- The script node that defines which audio file to play has a value of “en_sales.wav,” then...
- The HTTP request for the file is automatically constructed as

http://myserver.mydomain.com/en-us/app/en_sales.wav

If your whisper audio files are stored in a different locale directory, you must add a Set Variable node to your script that identifies the locale directory. Similarly, if your whisper files are stored in a different application directory, you must add a Set Variable node that identifies that directory.

Specify Locale Directory

Use these settings in the Set Variable node to specify your locale directory:

- Object Type: Call.
- Variable: Must use the user.microapp.locale ECC variable.
- Value: Specify the directory name. For example: “pt-br,” You must enclose the path in quotes.

Specify Application Directory

Use these settings in the Set Variable node to specify your application directory:

- Object Type: Call.
- Variable: Must use the user.microapp.app_media_lib ECC variable.
- Value: Specify the directory name. For example: to use a directory “wav_files” in place of the default directory “app,” enter “wav_files.” To use a sub-directory “wav_files” “app,” enter “app/wav_files.” You must enclose the path in quotes.

Variable Length for Media Server Locale and Application Directory Variables

If you do include Set Variable nodes for the media server, locale, or application directories, ensure that the values you set for them do not exceed the Maximum Length settings for their corresponding ECC variables.

For example, if you include a Set Variable node for the media server with a value of “http://mysubdomain.mydomain.co.uk,” the string is 33 characters long. Therefore, the Maximum Length setting for the user.microapp.media_server ECC variable must be 33 or greater. If it is not, you must increase

the Maximum Length setting. Otherwise, the server name is truncated in the HTTP request for the file and the file is not found. You configure ECC variables in the Unified CCE Configuration Manager at List Tools > Expanded Call Variables List.

Test Whisper Announcement File Path

To test the path to the whisper file that you defined in you script variables, enter the complete URL into a browser. The .wav file should play. For example:

- If your script includes: default media server + default locale + default application directory + whisper.wav, then the path is “http://<default_media_server>/en-us/app/whisper.wav”
- If your script includes: http://my_server.my_domain.com + default locale + “app/wav_files” + whisper.wav, then the path is “http://my_server.my_domain.com/en-us/app/wav_files/whisper.wav”

Other Script Settings That Are Required for Whisper Announcement

These additional settings are required for Whisper Announcement to work:

- Enable Target Requery on all script nodes that follow the WhisperAnnouncement variable and target an agent. These include Queue (to Skill Group or Precision Queue), Queue Agent, Route Select, and Select. If Target Requery is not enabled, the Whisper Announcement does not play.
- When you run an agent transfer or a conference script, use a SendToVRU, a TranslationToVRU, or a Run Script Request node before you target an agent.

Fail-Safe Timeout for Whisper Announcement in Unified CCE

Unified CVP sends one message to Unified CCE each time a Whisper Announcement begins and a second message when the announcement ends. The time stamps from these messages are used to calculate Whisper Announcement data in Unified CCE reports.

If Unified CVP fails to send a Whisper Announcement end message toUnified CCE, the following occurs:

- Unified CCE cannot accurately calculate the whisper length, thus skewing report data.
- The agent cannot control the call (for example, put it on hold or transfer it) because these controls are disabled while a Whisper Announcement is playing.

To prevent this, Unified CCE has a Whisper Announcement timeout setting. The value for this setting represents the maximum Whisper Announcement play time that Unified CCE uses to calculate its report data.

The default is 20 seconds. This default is based on the default Whisper Announcement play time (specified in Unified CVP) of 15 seconds. The extra 5 seconds in the Unified CCE fail-safe timeout is a buffer against latency. If you modify the maximum Whisper Announcement play time in Unified CVP, modify the Unified CCE Whisper Announcement fail-safe timeout accordingly.

The Unified CCE Whisper Announcement fail-safe timeout value should be equal to or greater than the maximum Whisper Announcement play time setting in Unified CVP. Otherwise, Whisper Announcement play time in Unified CCE reports are under-reported.

To change the fail-safe timeout value, complete the following steps for theUnified CCE peripheral by using the PG explorer tool:

Procedure

Step 1 In Unified CCE Configuration, select **Tools** > **Explorer Tools** > **PG Explorer**.

Step 2 Click **Retrieve** to return a list of PGs (Peripheral Gateways).

Step 3 Double-click the agent PG to expand it, and select the peripheral with client type **CUCM** or **UCCE system**.

Step 4 On the **Peripheral** tab, enter the following text in the **Configuration Parameters** field:

```
/WHSTMOUT <value in seconds>
```

Step 5 Once you are finished, click **Save**.

Whisper Announcement Sample Scripts

Unified CCE includes sample routing scripts that demonstrate Whisper Announcement. You can use them as learning tools and as models for your own Whisper Announcement scripts. They are the following:

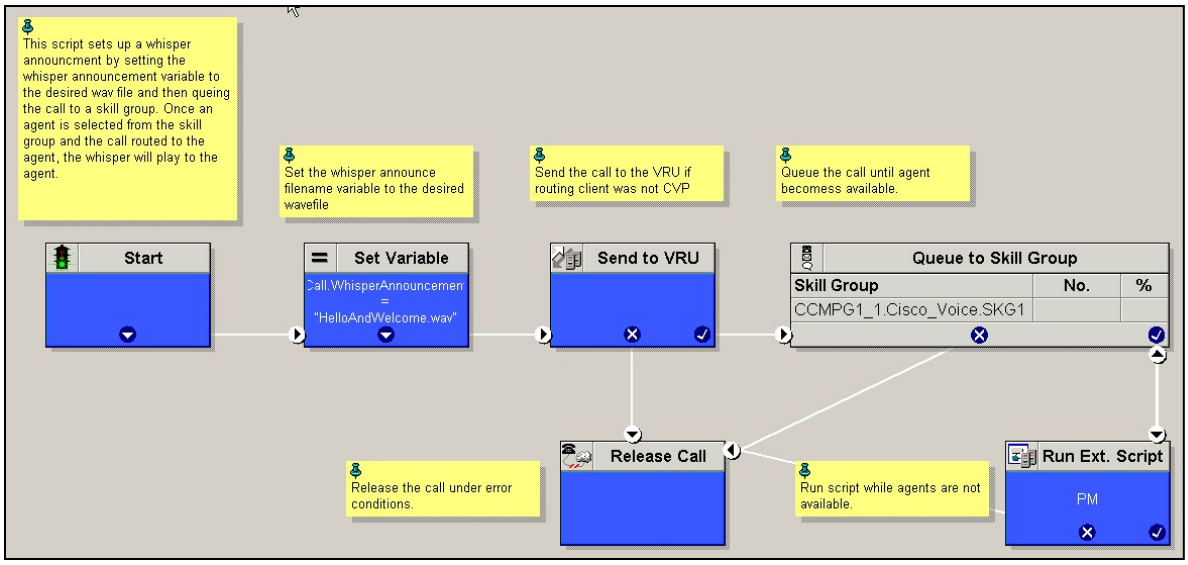
- **WA.ICMS**—This script plays a Whisper Announcement.
- **WA_AG.ICMS—**This script plays both a Whisper Announcement and an Agent Greeting to play on the same call flow.

The script files are located in the `c:\icm\bin` directory. In Unified CCE Script Editor, they are installed to the application root directory.

Note To use these scripts you must have a default media server configured in Unified CVP, and have the Whisper file stored in the default location on the media server. For that reason, they do not include variables that specify the media server, locale, or application directories.

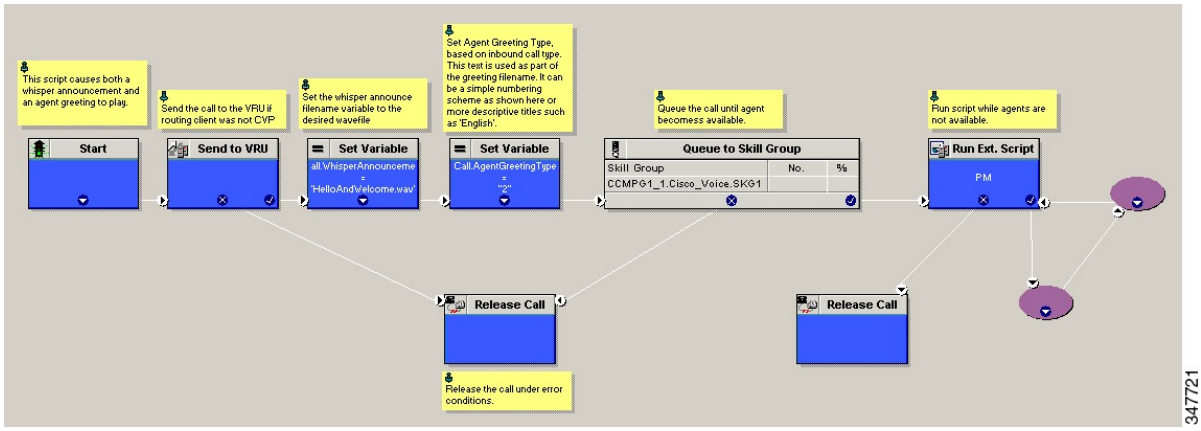
WA.ICMS Script

This script sets up a Whisper Announcement by setting the Whisper Announcement variable to the desired wave file and then queuing the call to a skill group or Precision Queue. After an agent is selected from the skill group or Precision Queue and the call routed to the agent, the whisper plays to the agent.



WA_AG.ICMS Script

This script causes both a Whisper Announcement and an Agent Greeting to play.



Import Sample Whisper Announcement Scripts

To view or use the sample Whisper Announcement scripts, you must first import them into Unified CCE Script Editor. Follow this procedure to import the scripts:

Procedure

Step 1 Open Script Editor.

Step 2 Select **File** > **Import Script** and select the first of the two scripts to import.

In addition to importing the script, Script Editor tries to map imported objects. Some objects that are referenced in the sample scripts, such as the external Network VRU scripts or the skill groups or Precision Queues, do not map successfully. You must create these maps manually or change these references to point to existing Network VRU scripts, skill groups, and Precision Queues in your system.

Step 3 Repeat steps 2 and 3 for the remaining script.

How Whisper Announcement Works

Whisper Announcement Audio File

You store and serve your Whisper Announcement audio files from the Cisco Unified Contact Center Enterprise (Unified CCE) media server. This feature supports only the wave (`.wav`) file type. The maximum play time for a Whisper Announcement is subject to a timeout. Playback terminates at the timeout regardless of the actual length of the audio file. The default timeout is 15 seconds. In practice, you may want your messages to be much shorter than that, 5 seconds or less, to shorten your call-handling time.

While a Whisper Announcement Is Playing

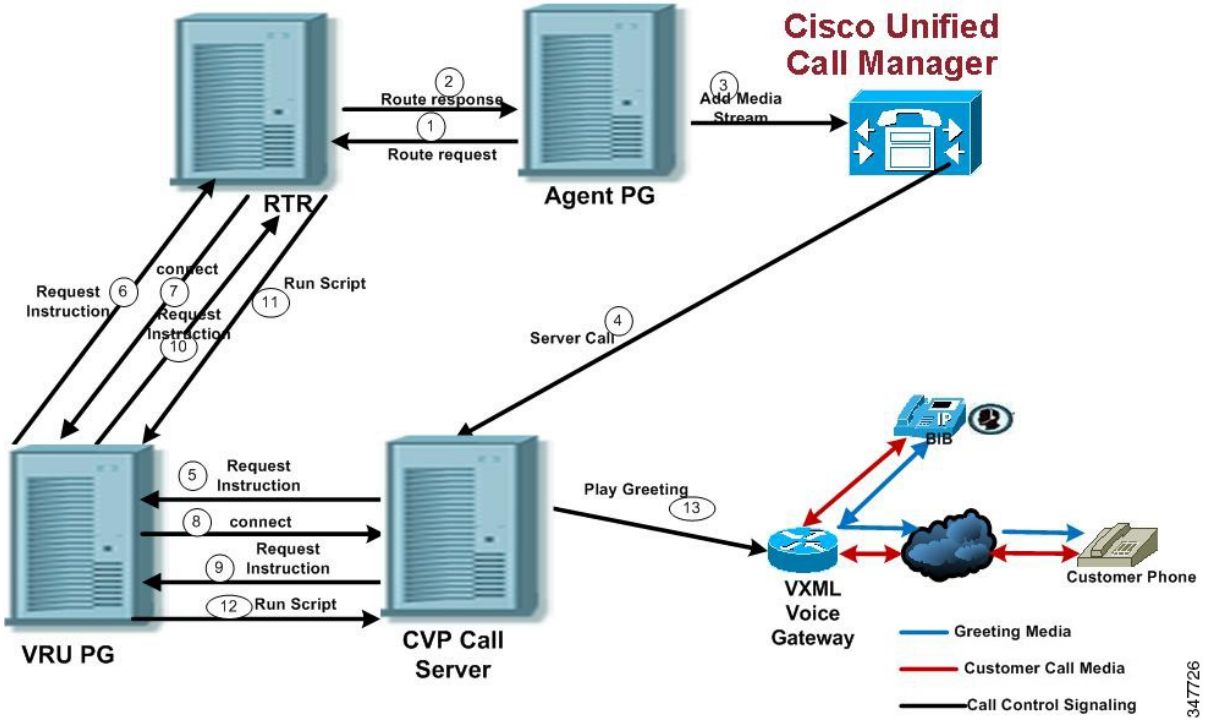
Only one Whisper Announcement can play for each call. While a Whisper Announcement is playing, you cannot put the call on hold, transfer, conference, or release the call, or request supervisor assistance. These features become available again after the whisper is complete.

Whisper Announcement with Transfers and Conference Calls

When an agent transfers or initiates a conference call to another agent, the second agent hears an announcement if the second agent's number supports Whisper Announcement. In the case of consultative transfers or conferences, while the whisper plays, the caller hears whatever normally plays during hold. The first agent hears ringing. In the case of blind transfers, the caller hears ringing while the whisper announcement plays.

Whisper Announcement Call Flow

Following is a Whisper Announcement call flow diagram accompanied by a description of the steps.



1. CVP receives a new call from the PSTN.

2 - 3. CVP sends the new call to the VRU PIM and the VRU PIM sends the new call to the Unified CCE router.

4. If an agent is available, the router reserves the agent.

5 - 6. The router sends a label with a whisper prompt to CVP.

7. CVP sends the call to Unified CM.

8 - 9. The agent receives and answers the call.

10. Unified CM sends the established event to the agent PIM. The agent PIM holds the event until the Whisper Announcement is done playing.

11. CVP tells the VXML gateway to play ringback to the caller and the Whisper Announcement to the agent. After the Whisper Announcement plays, CVP connects the agent to the customer and notifies Unified CCE.

12. The agent PIM gets notification that Whisper Announcement is complete and sends the established event to the agent desktop.

Reporting and Serviceability

Whisper time is not specifically broken out in Unified CCE reports. In agent, skill group, and Precision Queue reports, the period during which the announcement plays is reported as Reserved agent state time. In the Termination Call Detail records, it is treated as Ring Time.

Serviceability for Whisper Announcement includes system events to indicate reasons for Whisper Announcement failures and counters to track the number of failed whisper events.

Component Failure and Whisper Announcement

Failure to Access CVP Media Server

If the connection to the CVP media server fails, or if a requested whisper audio file cannot be found, the call proceeds normally without Whisper Announcement.

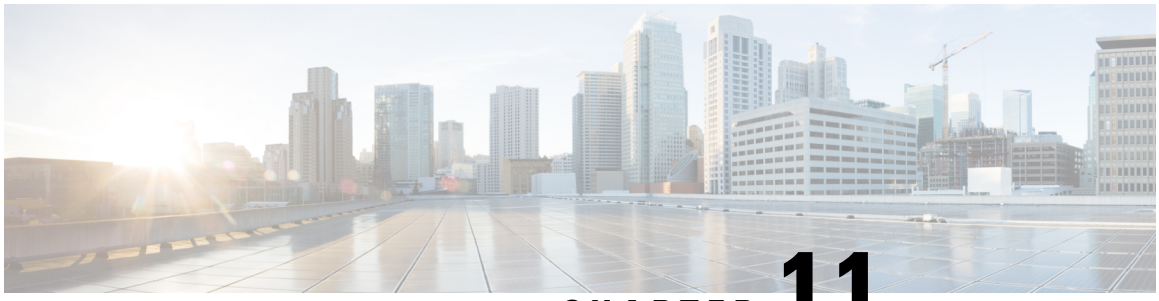
Whisper Announcement in Agent Desktop Software

No configuration is needed to integrate Whisper Announcement with agent desktop software. While a whisper is playing, software on the agent desktop shows the call in the Ring state. Desk phones show the call in the Talking state.

Using Agent Greeting with Whisper Announcement

You can use Agent Greeting along with the Whisper Announcement feature. Consider the following when you use them together:

- On the call, the Whisper Announcement always plays first before the greeting.
- To shorten your call-handling time, you may want to use shorter whispers and greetings than you might if you were using either feature by itself. A long whisper followed by a long greeting means a long wait before an agent handles a call.
- Usually, agents that use Whisper Announcement handle different types of calls: for example, "English, Gold Member, Activate Card, Spanish, Gold Member, Report Lost Card, English, Platinum Member, Account Inquiry." Ensure the greetings your agents record are generic enough to cover the range of customer calls they handle.



CHAPTER 11

Video Contact Center

Video Contact Center

Video Contact Center provides high-quality video collaboration between customers and agents. Depending on how Video Contact Center is deployed, customers may connect with agents either from within the enterprise network or from devices outside the enterprise.

Packaged Contact Center supports the following Video Contact Center capabilities:

- Video communication between agents and callers
- Video on Hold - Videos are played to callers when they are placed on hold by an agent.
- Video-in-Queue - Video-in-Queue can play videos before and while a caller is in queue. This feature presents high-definition video prompts that allow callers to navigate a video menu using DTMF keys.
- Cisco MediaSense recording - Cisco MediaSense can record both the video and audio parts of a video call, or the audio only.

Packaged CCE supports two Video Contact Center deployments:

1. Video Contact Center for enterprise callers
2. Video Contact Center with Jabber Guest

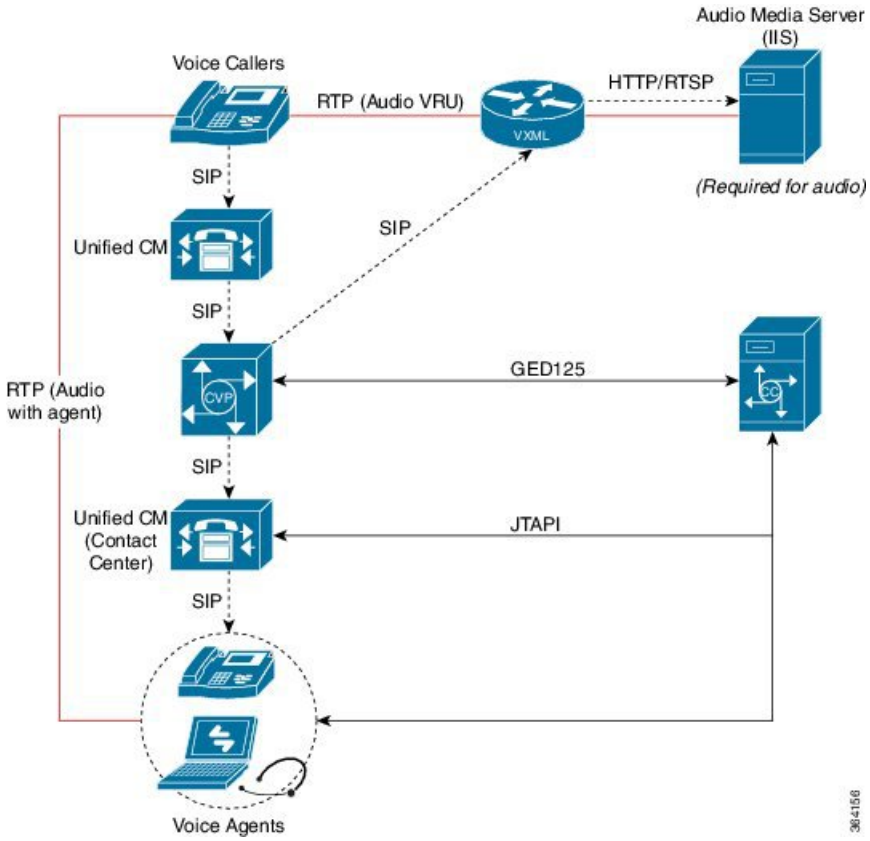
1. Video Contact Center for Enterprise Callers

You can deploy Video Contact Center so that only callers within the enterprise network can engage in video calls with agents. These callers use endpoints that are registered to the Cisco Unified Communications Manager. For example, company employees can have a video call with your IT help desk.

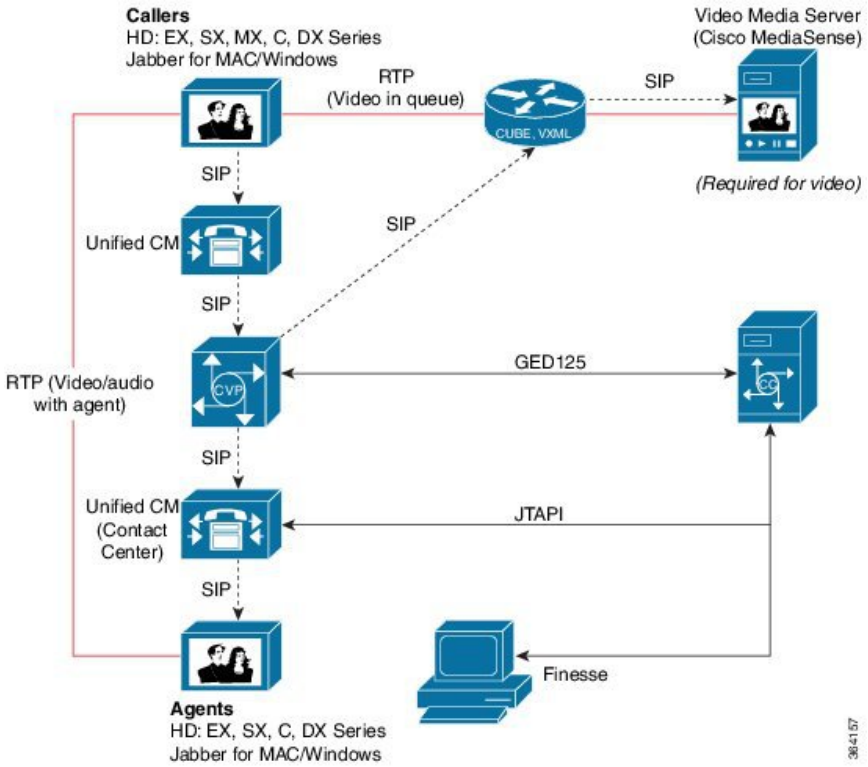
To transition from a voice contact center to a Video Contact Center for enterprise callers, Packaged CCE requires the following components:

- Cisco MediaSense to store, stream, and play video content. MediaSense can also record video calls.
- Telepresence MCU Video Conference Bridge to facilitate multi-party video conferences.
- Cisco Unified Border Element (Cisco UBE) that connects video calls from Unified CVP to Cisco MediaSense to queue the calls or play video prompts.
- Video endpoints for agents and callers

For example, this is a traditional voice deployment:



After the transition to Video Contact Center for enterprise callers, the deployment looks like this:



See the *Solution Design Guide for Cisco Packaged Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html for the supported versions of these components.

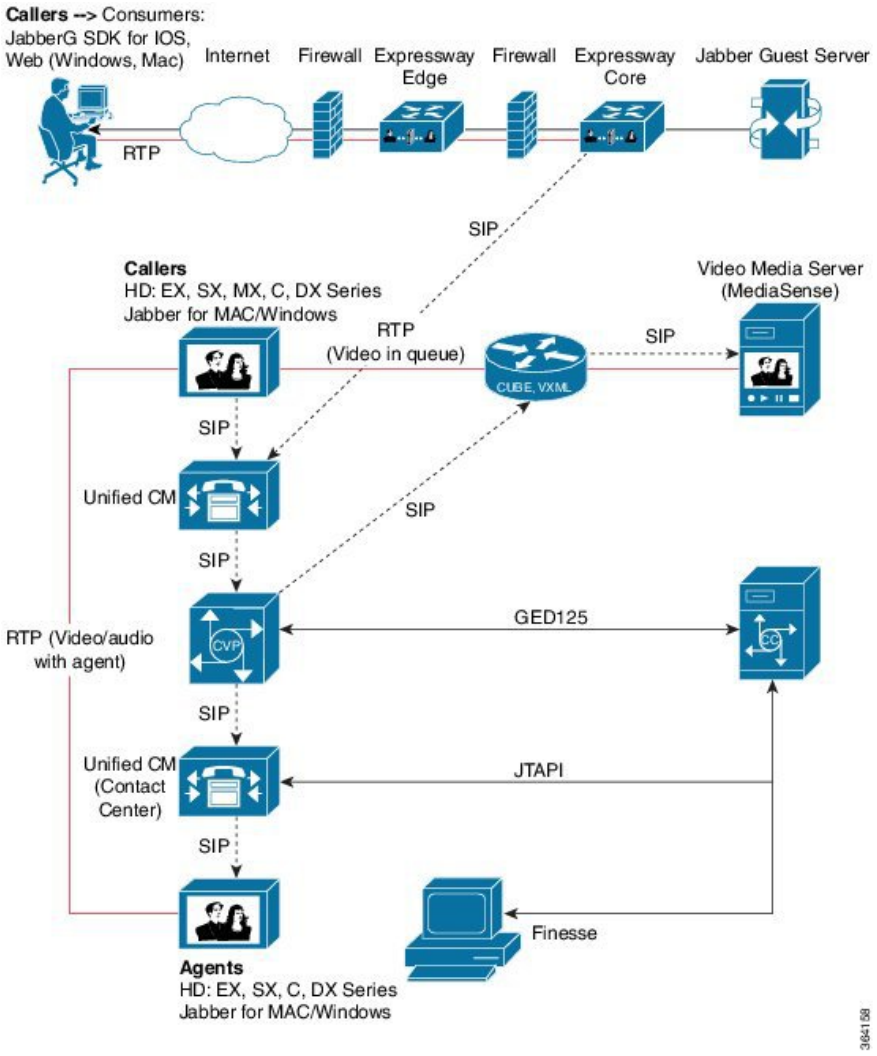
2. Video Contact Center with Jabber Guest

Packaged Contact Center Enterprise supports **Video Contact Center with Jabber Guest** as an add-on to Video Contact Center. In Video Contact Center with Jabber Guest, callers outside the enterprise network use a Cisco Jabber application or browser client for video calls with agents.

In addition to the components required for enterprise callers, Video Contact Center with Jabber Guest deployments also requires these components:

- Cisco Jabber Guest Server, to connect Jabber client video callers with agents.
- Cisco Expressway Edge and Core, to enable Jabber client traffic to reach the Jabber Guest Server through the enterprise's firewall.

After the transition to Video Contact Center with Jabber Guest, the deployment looks like this:



See the *Solution Design Guide for Cisco Packaged Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html, for the supported versions of these components.

Video Prerequisites

Licenses

Before installing Video Contact Center solutions, acquire the necessary licenses for these products:

- Cisco Telepresence MCU video conference bridge
- Cisco MediaSense
- Cisco Unified Border Element
- Cisco Jabber Guest Server - Video Contact Center with Jabber Guest deployments only

- Expressway Edge and Core - Video Contact Center with Jabber Guest deployments only

Cisco Telepresence MCU Video Conference Bridge License Requirements

For license requirements for the supported Cisco Telepresence MCU conference bridges, see the *Ordering Guide for Cisco Customer Contact Solutions* at this location on cisco.com.

Cisco MediaSense License Requirements

You need the following licenses to run Cisco MediaSense with Video Contact Center:

- Media Sense Base License for the number of concurrent non-redundant sessions required.
- Video Session Licenses for the number of concurrent non-redundant video sessions required.
- MediaSense Server Software Licenses for the Primary and Secondary servers that provide database and media operations.
- MediaSense Expansion Server Software Licences for servers that provide additional capacity for media operations.

Additional ordering and licensing information is available to Cisco Partners in the following documents:

- *Ordering Guide for Cisco Customer Contact Solutions* at https://www.cisco.com/c/en/us/products/customer-collaboration/mediasense/partner-resources-listing.html
- Cisco MediaSense Sizing Spreadsheet

Cisco Unified Border Element License Requirements

A software license is required to run Cisco Unified Border Element. If you have already deployed Cisco UBE, you can re-use the existing ports. However, if you need additional sessions to support Video Contact Center, you need to purchase additional Cisco UBE ports. See the *Cisco Unified Border Element and Gatekeeper Ordering Guide* at https://www.cisco.com/en/US/prod/collateral/voicesw/ps6790/gatecont/ps5640/order_guide_c07_462222.html.

Cisco Jabber Guest License Requirements - Video Contact Center with Jabber Guest Deployments Only

Cisco Jabber Guest is licensed and obtained through User Connect Licensing (UCL), Cisco Unified Workspace Licensing (CUWL), and other ordering mechanisms. Contact a sales representative from a Cisco partner or from Cisco for ordering details. No license keys are provided or required for the Cisco Jabber Guest software.

Cisco Expressway License Requirements - Video Contact Center with Jabber Guest Deployments Only

The following table describes the license requirements for using Cisco Expressway with Cisco Jabber Guest.

Table 8: License Requirements for Using Cisco Expressway with Cisco Jabber Guest

License	Requirement	Note
Rich Media Session licenses	2 Rich Media Session licenses are required per Cisco Jabber Guest session: • 1 Rich Media Session license on the Cisco Expressway-E for each Cisco Jabber Guest session • 1 Rich Media Session license on the Cisco Expressway-C for each Cisco Jabber Guest session	
TURN relay license	TURN licensed on Cisco Expressway	When you order Cisco Expressway, a TURN relay license is included.
Advanced Networking (AN) license	If Cisco Jabber Guest is installed in a dual-NIC deployment, an AN license is required on Cisco Expressway.	When you order Cisco Expressway, an AN license is included.

Video Contact Center Restrictions

Packaged CCE supports Video Contact Center solutions with the restrictions described in this table.

Note Packaged CCE Video Contact Center does not support any features that are not included in this document.

Restriction Type	Restriction
Packaged CCE features	Packaged CCE Video Contact Center solutions do not support the following features: • Agent Greeting • Whisper Announcement • Mobile Agent • Silent Monitor • Video on Hold (caller-initiated) • Outbound Dialer • Courtesy Callback

Restriction Type	Restriction
Jabber endpoints	Use Jabber as a video endpoint only. As for all endpoints, all call controls (except for answer, mute, and hangup) must be done via the agent desktop.
Audio codec	Cisco MediaSense does not support G.711 a-law codec for video playback.
Video resolution scaling	MediaSense does not support video resolution scaling. For example, a 320p video plays at 320p on every device, and a 1080p video plays at 1080p on every device. Supported devices properly handle any necessary up- or down-scaling themselves.
Agent and supervisor desktop features	Agent desktops support a limited set of features for video agents, as follows: • Standard actions — Agent log in, Agent State (Ready, Not Ready), Dial, Answer, Release, and CTI data. • Additional services — Hold, Retrieve, Alternate, Reconnect, and Blind/Consult Transfer/Conference. Agent desktops do not support these features for video agents: • Silent Monitor • Supervisor Barge-In • Intercept

Supported Video Formats and Codecs

Cisco MediaSense supports the following formats and codecs for uploaded videos:

- MP4 video with up to 1080p resolution
- H.264 video codec
- AAC-LD MP4A-LATM audio codec

Videos play back using the AAC-LD MP4A-LATM, G.711 mu-law, or G.722 codec, depending on the endpoint.

Set Up Video Contact Center Components

You must set up Cisco Packaged Contact Center Enterprise before installing and configuring additional Video Contact Center components.

See the *Cisco Packaged Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-installation-guides-list.html.

Video Contact Center

Install and configure these components for all Video Contact Center deployments. This table includes links to installation and configuration instructions for each component, and notes specific to Video Contact Center configuration.

Component Task	Related Document	Notes

Deploy Cisco UBE	Cisco IOS Voice Command Reference	Confirm that Cisco UBE is enabled on the system. In the terminal window, type:
		`show cube status`
		If Cisco UBE is disabled, type the following text to enable it:
		`Voice service voip`
		`Mode border-element`
		`Allow-connections sip to sip`

Install and configure Cisco MediaSense	*Installation and Administration Guide for Cisco MediaSense* at https://www.cisco.com/c/en/us/support/customer-collaboration/mediasense/tsd-products-support-series-home.html	The system default incoming call configuration in MediaSense is set to **Record Audio Only**. Change this setting to **Record Audio and Video** in order to record video calls. Follow the instructions to Edit the System Default Incoming Call Rule in the *Administer and Configure MediaSense* chapter to change this setting.
Integrate MediaSense and Cisco UBE	*Installation and Administration Guide for Cisco MediaSense* at https://www.cisco.com/c/en/us/support/customer-collaboration/mediasense/tsd-products-support-series-home.html	Follow the instructions for MediaSense Setup with Cisco Unified Border Element in the *Administer and Configure MediaSense* chapter. Be sure to add the username for the AXL Administrator to the Standard Unified Communications Manager Administrators group and Standard AXL API Access roles in Unified Communications Manager, if necessary.

Component Task	Related Document	Notes
Configure Unified Communications Manager for the Cisco Telepresence MCU conference bridge	*Cisco TelePresence MCU 45X0, 53X0 and MCU MSE 8510 Deployment Guide* at https://www.cisco.com/c/en/us/support/conferencing/telepresence-mcu-5300-series/products-installation-guides-list.html	Follow the instructions in the *Deploying an MCU as a Unified CM media resource* section.

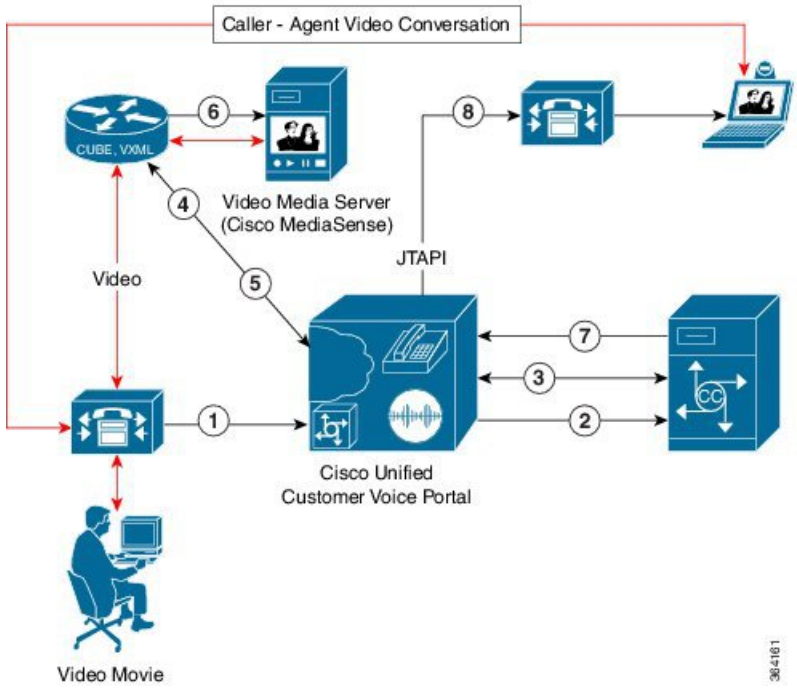
Video Contact Center with Jabber Guest

For Video Contact Center with Jabber Guest deployments, install and configure these additional components. This table includes links to installation and configuration instructions for each component, and notes specific to Video Contact Center with Jabber Guest configuration.

Component Task	Related Document	Installation and Configuration Notes
Deploy Cisco Expressway Edge and Expressway Core (Expressway-C and Expressway-E), including firewall configuration	*Cisco Expressway Basic Configuration Deployment Guide* at https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html *Cisco Expressway on Virtual Machine Installation Guide* at https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-guides-list.html	Deploy Expressway-C and Expressway-E before installing and configuring Cisco Jabber Guest Server. Once installed, confirm the configuration details using the appendices listed in the *Cisco Expressway Basic Configuration Deployment Guide*.
Install and Configure Cisco Jabber Guest Server	*Cisco Jabber Guest Installation and Administration Guide* at https://www.cisco.com/c/en/us/support/unified-communications/jabber-guest/tsd-products-support-install-and-upgrade.html	Follow the instructions for the **Dual NIC Deployment**. Skip any steps that you completed while setting up the Expressway components earlier. Review the instructions in the *Cisco Jabber Guest Installation and Administration Guide* to verify that you correctly configured the Expressway-E and Expressway-C.

Configure Video-in-Queue

Video-in-Queue (VIQ) is an optional feature in Unified CVP. Depending on configuration, the caller interacts through high-definition video prompt or navigates a video menu using DTMF keys. The following figure displays the topology and call flow for an enterprise deployment.



1. New call from Unified CM to Unified CVP.
2. New call to Packaged CCE from Unified CVP.
3. Play Unified CVP Studio video application.
4. Unified CVP sends the call to the Cisco UBE/VXML Gateway.
5. Unified CVP VXML Server application instructs VXML Gateway to connect to specific dialed number (DN).
6. Cisco UBE sends call to Video Media Server with that DN. Caller gets static video.
7. Agent is now available.
8. Unfied CVP sends call to an agent.

The Unified CVP Studio VideoConnect element plays a specific video prompt for video endpoints. VideoConnect also collects and integrates the DTMF input during video-prompt playback with the Unified Call Studio or Unified CCE scripting environment.

Note Video-in-Queue does not play during a Unified Communications Manager Failover.

Note When setting up the Video-in-Queue for Unified CVP, set the MediaSense **Incoming Call Configuration** > **Action** to play once.

Video-in-Queue Configuration Sequence

To set up Video-in-Queue, perform the following tasks:

Sequence	Task	Notes
Configure Cisco Unified Communications Manager		
1	Configure the SIP Trunk to MediaSense, on page 218	
2	Configure Video on Hold, on page 227	
Configure Cisco MediaSense		
3	Upload Video File, on page 220 to play to callers	
4	Associate the Dialed Number with the Video File, on page 220	The Dialed Number for the video must match the following settings on other components: • **VXML/Cisco UBE gateway dial peer configuration:** destination-pattern • **Unified CVP Call Studio Script:** VideoConnect element VideoMedia Server DN setting • **Packaged CCE routing script:** "video_id" value for the Set variable that points to the Unified CVP Studio script for Video-in-Queue
Configure Cisco UBE/VXML Gateway		
5	Configure Cisco Unified Border Element/VXML Gateway for Video, on page 221 to connect a dial-peer to MediaSense and configure video capabilities on the gateway.	The destination-pattern must match the pattern used for the Dialed Number that you associated with the uploaded video in MediaSense Administration.
Write the Cisco Unified CVP Call Studio Script		
6	Create Unified CVP Call Studio Script for Video-in-Queue, on page 221	
Write the Packaged CCE Routing Script		
7	If necessary, create a new dialed number and call type using Unified CCE Administration for the Video-in-Queue routing script you will create in the next step.	

Sequence	Task	Notes
8	Create Script Editor Routing Script for Video-in-Queue, on page 223 that invokes the Unified CVP Call Studio script.	The "application" value in the Set variable must be set to the name of the Unified CVP Call Studio script. The "video_id" value for the Set variable must the Dialed Number for the video in MediaSense Administration.

Configure Unified Communications Manager

After the postinstallation process for a Cisco MediaSense server, access your Unified CM server. In Unified CM Administration, configure the SIP Trunk and video endpoints.

Configure the SIP Trunk to MediaSense

Video Contact Center requires two Unified Communications Manager SIP Trunks:

- A SIP trunk to Unified CVP to handle the Contact Center routing and VXMLGW interactions. Video Contact Center uses the SIP trunk to Unified CVP that is already configured as part of Packaged CCE.
- A SIP trunk to MediaSense for forking calls via Cisco UBE.

You must set up the SIP trunk to MediaSense.

Procedure

Step 1 Login to Unified CM as an Administrator user.

Step 2 Click **Device** > **Trunk**.

Step 3 Click **Add New**.

Step 4 Select **SIP Trunk** from the **Trunk Type** drop-down menu.

Step 5 Leave the **Device Protocol** set to **SIP**.

Step 6 Select **None(Default)** from the **Trunk Service Type** drop-down menu.

Step 7 Click **Next**.

Step 8 Enter the **Device Name** and **Description** for the SIP trunk, and **Destination Address for MediaSense server**.

Step 9 Select a Device Pool from the **Device Pool** drop-down menu.

Step 10 In the **SIP Information** section, enter a destination address for the MediaSense server in the **Destination** field.

Step 11 Select **Non Secure SIP Trunk Profile** from the **SIP Trunk Security Profile** drop-down menu.

Step 12 Select the appropriate SIP profile for your deployment from the **SIP Profile** drop-down menu.

Step 13 Click **Save**.

Provision Video Endpoints

Provision your video endpoints by following the documentation for your endpoints and the *Cisco Unified Communications Manager Administration Guide* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

This section provides additional configuration necessary for video endpoints.

Configure Multiline Settings for Video Phones

You configure multiline settings for video phones in both Unified CCE Administration and Unified Communications Manager Administration. After changing the settings, you must restart the Peripheral Gateway services on the Side A and Side B Unified CCE Call Servers.

Procedure

Step 1 Log in to **Unified CCE Administration** as an Administrator, and perform the following steps:

a) Navigate to **System** > **Settings** > **Agent**.
b) Select **All Lines** from the **Agent Phone Line Control** drop-down menu.
c) Click **Save**.

Step 2 On the Unified Communications Manager publisher, log in to **Unified CM Administration** as an Administrator, and perform the following steps:

a) Navigate to **Cisco Unified Communications Manager Administration** > **Bulk Administration**.
b) Use the Unified Communications Bulk Administration Tool to modify the device profiles for all phones as follows:

- Set **Maximum Number of Calls** to 2. This value indicates that the phones do not allow multiple calls per line.
- Set **Busy Trigger** to 1. This value indicates that if the line is in use, other calls presented to that line are rejected with a busy cause.

For more information about the Unified Communications Manager Bulk Administration Tool, see the *Cisco Unified Communications Manager Bulk Administration Guide* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Step 3 Restart the Peripheral Gateway services as follows:

a) On the Side A Unified CCE Call Server, use the **Unified CCE Service Control** tool to restart PG1A and PG2A.
b) On the Side B Unified CCE Call Server, use the **Unified CCE Service Control** tool to restart PG1B and PG2B.

Set the Default Maximum Session Bit Rate for Video Calls

Unified Communications Manager Region settings are set by default to a maximum session bit rate of 384 kbps for video calls. This bit rate does not support HD video. You must change the default value to a value higher than 6000 kbps.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, navigate to **System** > **Region Information** > **Region**.

Step 2 Enter `Default` in the text field and click **Find**.

Step 3 Click **Default** in the results.

Step 4 In the **Modify Relationships to other Regions** > **Maximum Session Bit Rate for Video Calls** section, select the **kpbs** radio button and enter a value higher than 6000.

Step 5 Click **Save**.

Configure Cisco MediaSense

Use a Video Media Server to upload, store, and play back video prompts. Cisco MediaSense is the Video Media Server that provides network-based multimedia capture, streaming, and recording. Cisco MediaSense records conversations on the network rather than on a device. This process simplifies the architecture, lowers costs, provides optimum scalability, and facilitates use by analytics applications from Cisco technology partners.

Upload Video File

After installing Cisco MediaSense, upload a video MP4 file.

Procedure

Step 1 Go to **Administration** > **Media File Management** and click **Add**.

Step 2 Type in the **Title** (filename) and **Description**, and then browse to the location of the video MP4 file.

Step 3 Click **Save** to upload the video file to MediaSense server.

What to do next

Associate the file with a new dialed number.

Associate the Dialed Number with the Video File

Once you upload a video file, associate the file with a dialed number.

Procedure

Step 1 Go to **Administration** > **Incoming Call Configuration** and click **Add**.

Step 2 Click **Address**, and type the address of the appropriate dialed number.

Step 3 In the **Action** drop-down menu, choose **Play Once**.

Step 4 In the **Media File** drop-down menu, choose the appropriate video file.

The file is now associated with this dialed number.

Configure Cisco Unified Border Element/VXML Gateway for Video

This example Cisco Unified Border Element/VXML Gateway dial-peer code shows the configuration needed to connect a dial-peer to a Video Media Server:

```
application
service cvp_videoconnect flash:cvp_videoconnect.tcl

     voice service voip

allow-connections sip to sip
dial-peer voice 6000 voip
destination-pattern 6000T
session protocol sipv2
session target ipv4:10.78.26.142
voice-class sip midcall-signaling block
dtmf-relay rtp-nte
codec g711ulaw
video codec h264
no vad
```

The following code from the example connects Cisco UBE/VXML Gateway to MediaSense:

```
application
service cvp_videoconnect flash:cvp_videoconnect.tcl

voice service voip

     allow-connections sip to sip
```

Important You need to add the `destination-pattern` code to configure video capabilities on the gateway. The `destination-pattern` must match the pattern used for the Dialed Number that you associated with the uploaded video in MediaSense Administration.

Create Unified CVP Call Studio Script for Video-in-Queue

The CVP Studio VideoConnect element plays the specific video prompts for video endpoints. VideoConnect also collects and integrates the DTMF input during video prompt playback within a standard scripting environment.

The following graphic shows a sample CVP studio script:

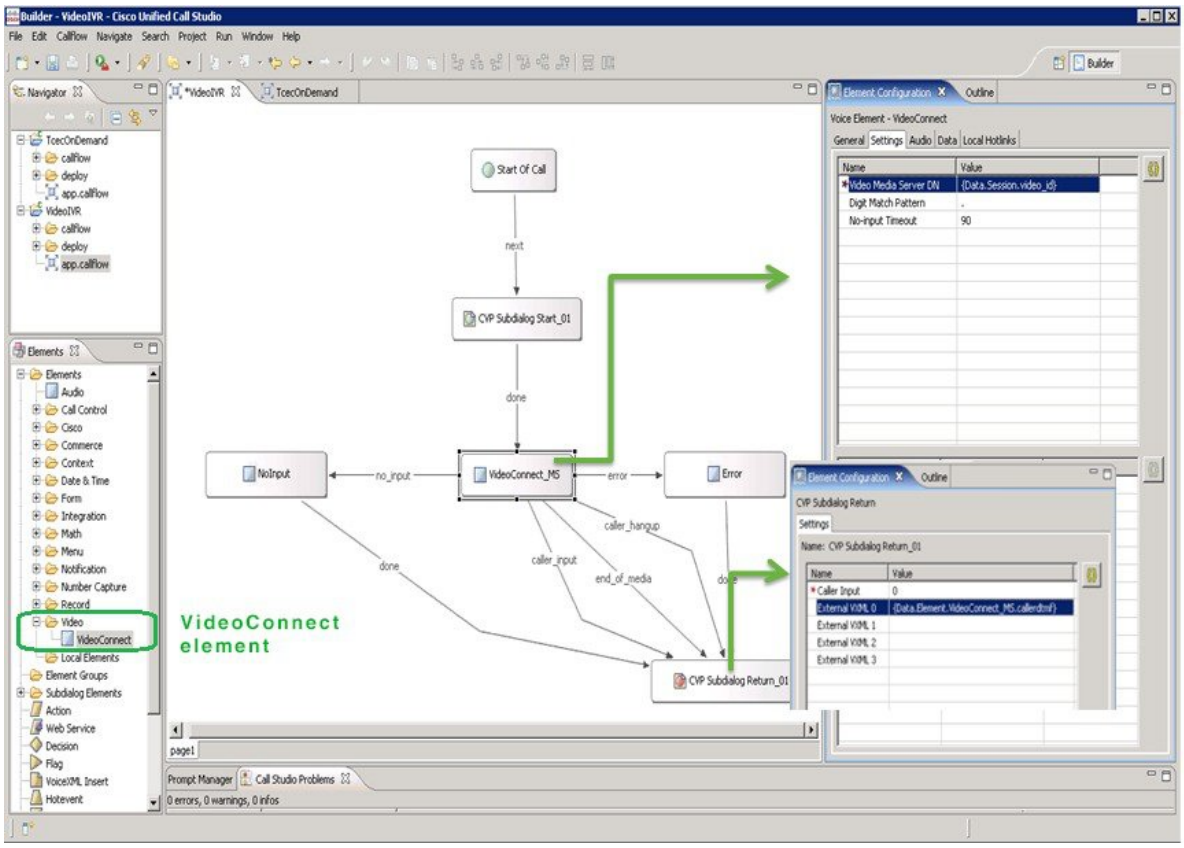


Table 9: Settings

Name (Label)	Required	Default	Notes
Video Media Server DN	Yes	None	Video Media Server Destination Number. Example: 5000. Must be a valid dialed number on Cisco Unified Border Element and Video Media Server.
Digit Match Pattern	No	None	Pattern to use for matching incoming digit collection. Leave blank for no digit collection. Example: 600. Must be a valid pattern for Cisco IOS gateway. The pattern format is the same as the destination-pattern format used in IOS gateway dial-peers.
No Input Timeout	No	No timeout	Maximum time (secs) to wait for caller input. Example: 15.

The following table describes the different ways a video call is completed/terminated:

Exit State	Notes
End_of_media	Video played to completion and the video server disconnected.
Caller_input	Caller entered a DTMF string that matched the specified digit collection pattern.
No_input	No input received before the input timeout expired on a digit collection pattern.
Error	An error or other unexpected termination occurred.
Caller_hangup	Caller disconnected while video in progress.

The following table describes element data that is created when one of these exit states is not completed:

Name	Type	Notes
callerdtmf	string	The digit string value captured.
result	string	Video call outcome.

Set Up Packaged CCE Routing Script for Video-in-Queue

To configure the Packaged CCE routing script for Video-in-Queue, complete these steps:

1. Create a new dialed number (if required) for the Video-in-Queue script.

   Complete this step using the **Dialed Number** tool in Unified CCE Administration. For instructions, see the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at

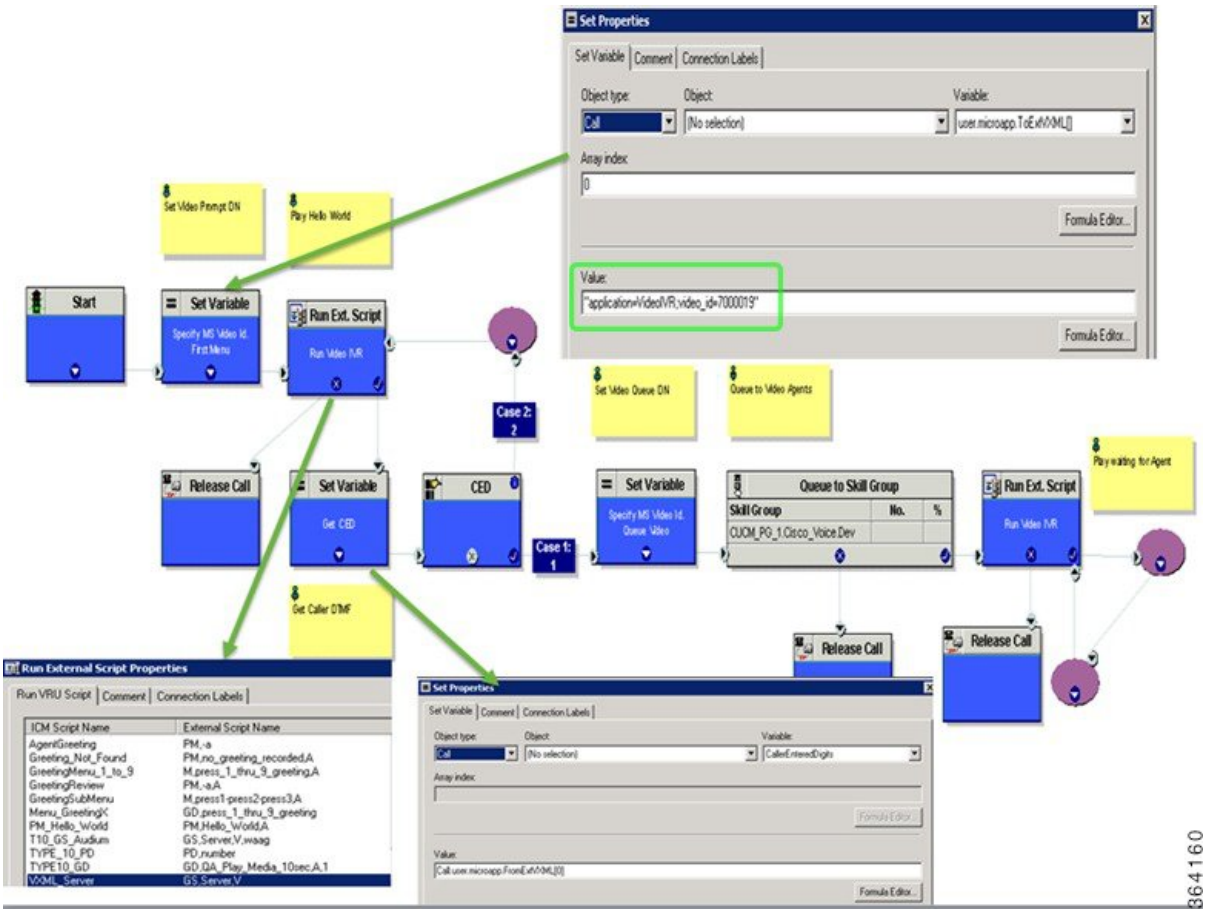
   https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/tsd-products-support-series-home.html.
2. Associate the dialed number with either a new or existing call type.

   Complete this step using the **Dialed Number** and **Call Type** tools in Unified CCE Administration. For instructions, see the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/tsd-products-support-series-home.html,
3. Create a routing script in Script Editor that invokes the Unified CVP Call Studio script that you created for Video-in-Queue.
4. Schedule the routing script for the call type in the Script Editor **Call Type Manager**.

Create Script Editor Routing Script for Video-in-Queue

The following illustration is a sample Script Editor script for Video-in-Queue. In this script:

- The Set variable is set to "application=VideoIVR;video_id=7000019" where **application** is the name of the Unified CVP Call Studio application, and **video_id** indicates the video to play. The **video_id** is the Dialed Number for the video in MediaSense Administration.
- The RunExtScript node uses the standard "GS,Server,V" to invoke the Unified CVP VXML application.
- You can receive the DTMF digits back from CVP Studio application in the "Call.user.microapp.FromExtVXML[0]".



After creating your script, schedule the routing script using Call Type Manager in Script Editor.

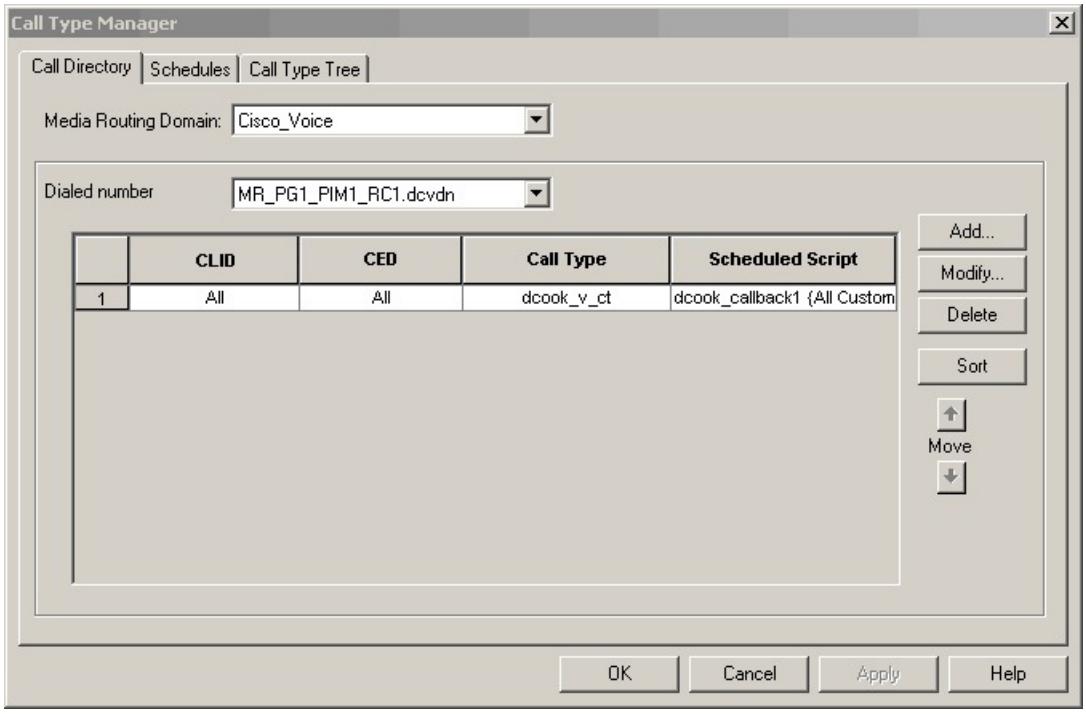
Schedule Routing Script

You schedule a script by associating it with a call type as follows:

Procedure

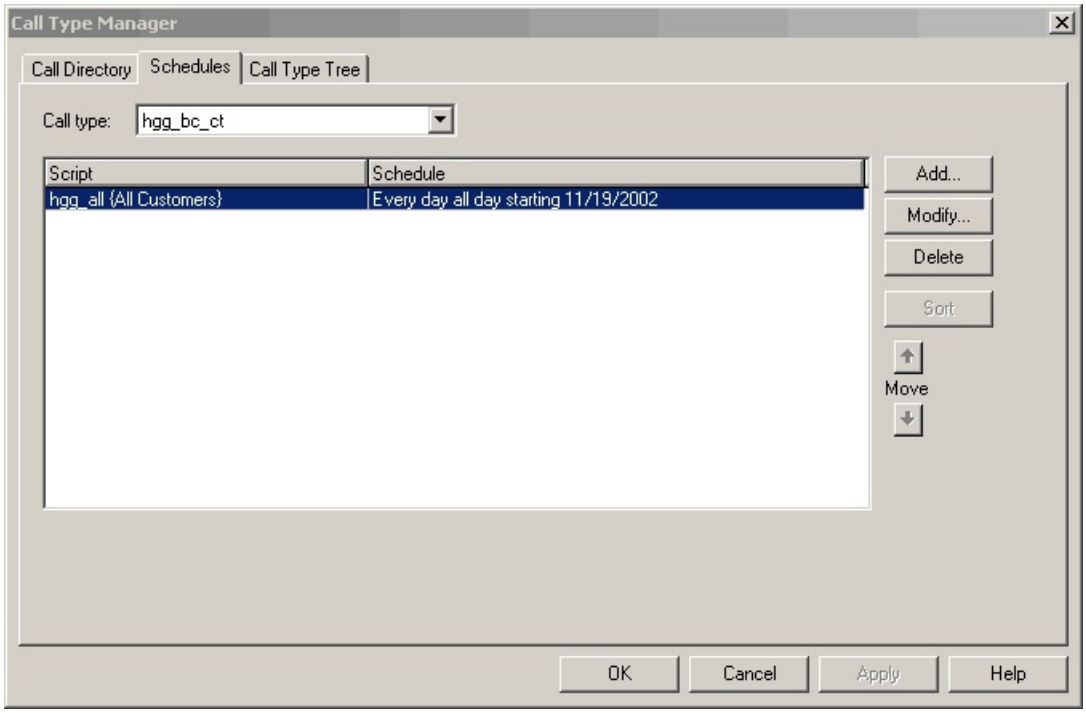
Step 1 Choose **Script > Call Type Manager**. The Call Type Manager dialog box opens.

Figure 19: Call Type Manager Dialog Box—Call Directory Tab



Step 2 Select the **Schedules** tab.

Figure 20: Call Type Manager Dialog Box - Schedules Tab

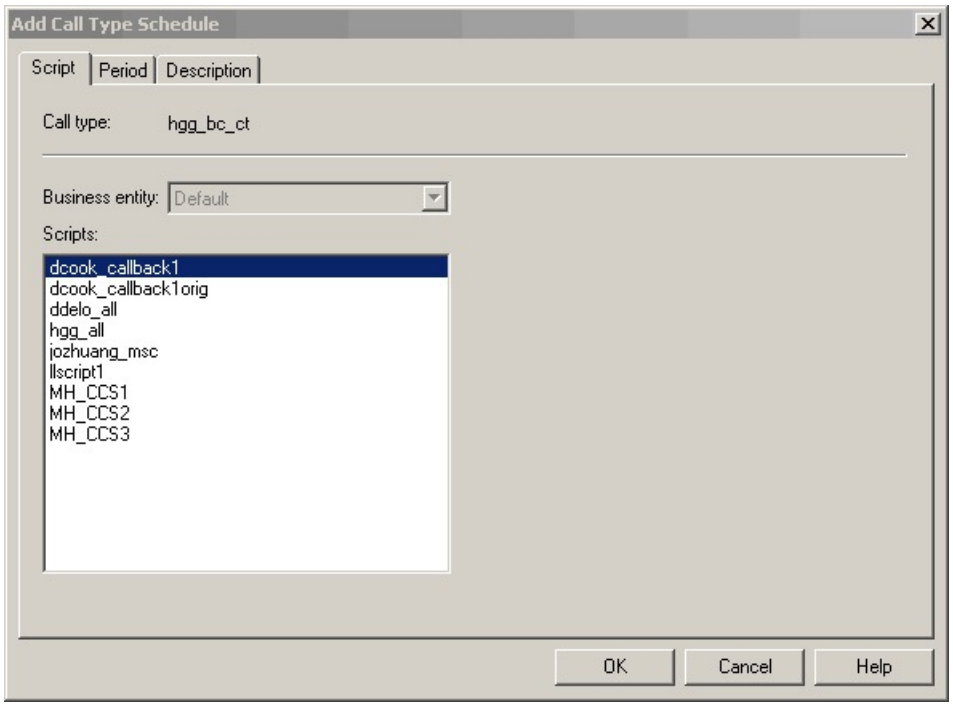


Step 3 Select the call type to associate with the script.

Step 4 Click **Add**. The Add Call Type Schedule dialog box opens.

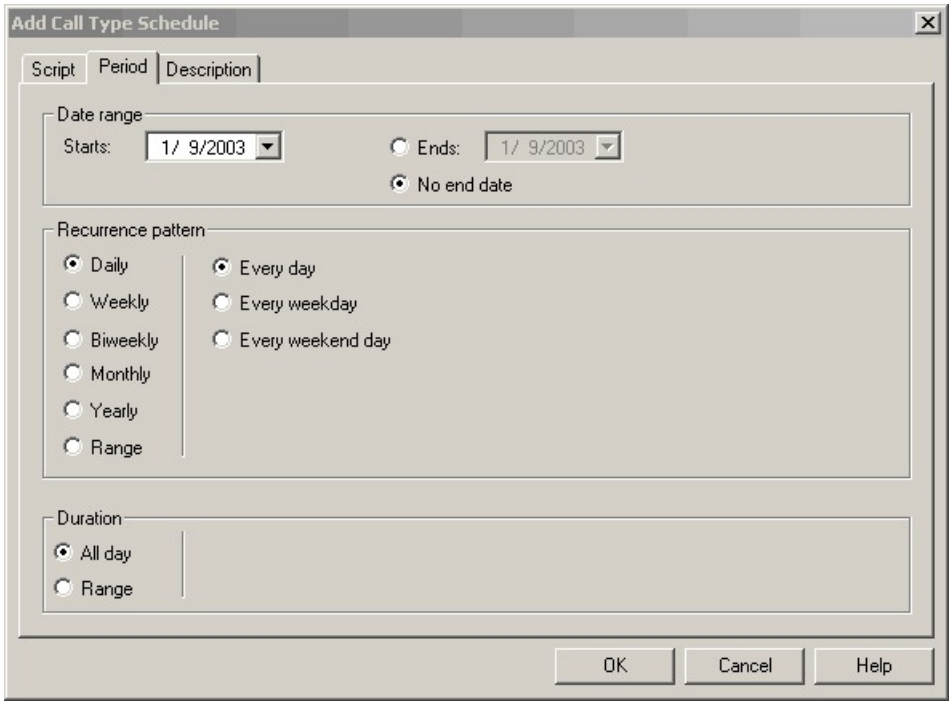
Step 5 In the Script tab, select the script to schedule:

Figure 21: Add Call Type Dialog Box - Script Tab



Step 6 In the **Period** tab, choose the information to define the period for which the schedule will be effective.

Figure 22: Add Call Type Schedule Dialog Box - Period Tab



Step 7 Optionally, in the **Description** tab, enter a description of the schedule.

Step 8 Click **OK** in the Add Call Type Schedule dialog box.

Step 9 Click **OK** in the Call Type Manager dialog box.

Note The schedule is not saved until you click **OK** in the Call Type Manager dialog box.

Configure Video on Hold

After configuring the Cisco MediaSense server, Video on Hold (VOH) is available. Once you configure video on hold, videos are played to callers when they are placed on hold by an agent.

To upload new video files for VOH, you must perform the steps in the following sections:

- Configure MediaSense for Video on Hold, on page 227
- Configure Unified CM for Video on Hold, on page 228

Configure MediaSense for Video on Hold

Follow these instructions to add the new media file to the Media Resource Group List (MRGL) in Cisco MediaSense.

Procedure

Step 1 Login to MediaSense as an Administrator user.
Step 2 Click **Administration** > **Media File Management**.
Step 3 Click **Add**.
Step 4 Enter the **Title**, **Description**, and **File**.
Step 5 Click **Save**.
Step 6 Click **Administration** > **Incoming Call Configuration**.
Step 7 Click **Add**.
Step 8 Enter the **Address** and **Action**, and then choose your recently added media file.
Step 9 Click **Save**.
Step 10 Login to Unified CM to apply this MRGL to the Device Pool of the client side video endpoints.

What to do next

Configure Unified CM for Video on Hold.

Configure Unified CM for Video on Hold

After you add your new media file to MediaSense, follow these instructions to add a SIP trunk to the MediaSense server and add the Video on Hold server to the Media Resource Group List.

Note In video conference use cases, the video conference bridge is a call leg on Cisco Unified Border Element. Ensure that you select the added Media Resource Group List (MRGL) on the SIP trunk to Cisco Unified Border Element.

Procedure

Step 1 Log in as an Administrator user.
Step 2 Click **Device** > **Trunk**.
Step 3 Click **Add New**.
Step 4 Click **Trunk Type** > **SIP Trunk**.
Step 5 Click **Next**.
Step 6 Enter the **Device Name**, **Description**, **Device Pool**, and **Destination Address** for the MediaSense server.
Step 7 Click **Save**.
Step 8 Click **Media Resources** > **Video On Hold Server**.
Step 9 Click **Add New**.
Step 10 Enter the **Name**, **Description**, **Default Video Content Identifier** (Address from previous section) and recently added SIP Trunk to the MediaSense server.

Alternatively, configure a call studio script to prompt the caller for a list of videos, and play the video matching the number the user selected.

Step 11 Click **Save**.

Step 12 Click **Device** > **Trunk** and select the trunk.

Step 13 Click **Reset**.

Step 14 Click **Media Resources** > **Media Resource Group (MRG)**.

Step 15 Click **Add New**.

Step 16 Enter the **Name** and **Description**, and then move the new Video on Hold server to **Selected Media Resources**.

Step 17 Click **Save**.

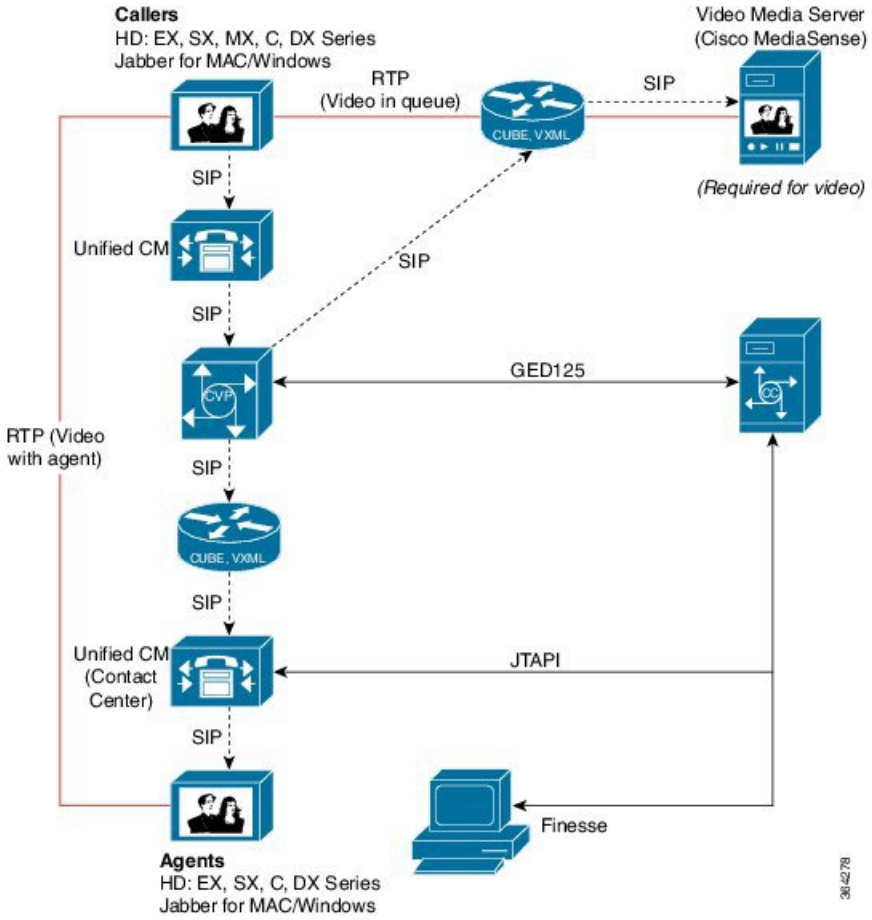
Step 18 Click **Media Resources** > **Media Resource Group List (MRGL)**.

Step 19 Click **Find** and then select an existing MRGL.

Step 20 Add the new MRG to the MRGL above the Music on Hold entry (for priority).

Record Video Calls

Recording can be performed using the phone or through the gateway. When recording through the gateway, an additional Cisco UBE is required, as shown in this configuration:



For more information on video recording, refer to the *Cisco MediaSense User Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/mediasense/tsd-products-support-series-home.html.