Cisco Packaged Contact Center Enterprise Features Guide, Release 12.5(1)

First Published: 2020-02-05

Last Modified: 2021-07-29

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

Change	See	Date
Edge Chromium (Microsoft Edge) updates	Browser Settings and Single Sign-On	December, 2020
Initial Release of Document for Release 12.5		February, 2020
Overview of Avaya Support.	Avaya Support chapter	
Overview of ICM-to-ICM Gateway Support.	ICM-to-ICM Gateway Support chapter	
Information on how to configure Cisco Webex Experience Management	Webex Experience Management Integration chapter	
Information on how to configure Customer Virtual Assistant feature	Customer Virtual Assistant chapter	

About This Guide

This document explains the features you can enable after your Packaged CCE system is installed, configured, and operational. For each feature, there is a description, procedures for initial setup, and details on the functionality the feature provides.

Audience

This document is prepared for:

- Contact center administrators who configure and run the contact center, manage agents and supervisors, and address operational issues.
- Contact center supervisors, who lead agent teams and are responsible for team performance.

This document is written with the understanding that your system has been deployed by a partner or service provider who has validated the deployment type, virtual machines, and database and has verified that your contact center can receive and send calls.

Related Documents

Subject	Link
Cisco Packaged Contact Center Enterprise (Packaged CCE)	https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/tsd-products-support-series-home.html
Contact Center Enterprise Compatibility Matrix	https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html
Virtualization for Cisco Packaged CCE	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html
Cisco Unified Communications Manager	https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html
Cisco Unified Intelligence Center	https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/tsd-products-support-series-home.html
Cisco Finesse	https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/tsd-products-support-series-home.html
Cisco Unified Customer Voice Portal (Unified CVP)	https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html
Cisco Remote Expert Mobile	https://www.cisco.com/c/en/us/support/customer-collaboration/remote-expert-mobile/tsd-products-support-series-home.html
Cisco Customer Collaboration Platform	https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/tsd-products-support-series-home.html
Enterprise Chat and Email	https://www.cisco.com/c/en/us/support/customer-collaboration/unified-email-interaction-manager/tsd-products-support-series-home.html

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

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

Optional Features in Packaged CCE

Feature Descriptions

You can choose to enable these features at any time after your Packaged CCE system is installed, configured, and operational.

Agent Greeting

Agent Greeting manages the recording and playing of greeting messages from agents. An agent's recorded greeting plays automatically to callers when they connect to that agent. Agents can set up different greetings for different types of callers, if the call center supports that option.

Agent Request

Agent Request allows a customer to make request on the web to receive a return call from an agent. The request is initiated by a Customer Collaboration Platform callback feed.

Courtesy Callback

Courtesy Callback offers customers the option to hang up and then receive a callback when an agent is close to being available, rather than having to wait for an extended time on hold. Customers do not lose their place in the queue. The system collects callback information from the caller, monitors agent availability, and calls the customer when the agent is close to available.

Enterprise Chat and Email

Enterprise Chat and Email (ECE) is an optional feature that provides chat and email functionality to the contact center. The ECE server routes chat and email contacts to agents on their Cisco Finesse desktops. The ECE server can be installed on the Packaged CCE Side B host or on an external server.

ECE includes the following features:

- Email—Email is supported by ECE to create a communication channel between a customer and an agent. There are various steps involved in efficiently responding to emails from customers. Emails are first retrieved into the system and routed to appropriate users or queues. After a response is created, it is processed through the system and sent to the customer.
- Chat—A chat is a real-time interaction between an agent and a customer during which they exchange text messages. As part of a chat, agents can also push web pages to customers. Based on how chat

activities are routed to agents, they can be categorized as standalone chats or integrated chats. An integrated chat is routed to an integrated queue and a message is sent to Packaged CCE. The system processes the activity and assigns the chat to an available agent.

- Web Callback—The Web Callback feature allows the user to request a callback by submitting a form on a website. ECE processes the submitted information and connects the user with an agent. ECE then sends a request to Packaged CCE to route the callback request to the agent.
- Delayed Callback—The Delayed Callback feature is similar to Web Callback, but when ECE receives the delayed callback request, it adds the request in the Delayed Callback table. ECE sends the HTML page to the customer, indicating that the customer will receive a callback within a specified time. When the specified time arrives, ECE moves the request to the Packaged CCE queue for routing to Unified CCE.

For more information about this feature, see the Enterprise Chat and Email documentation at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/tsd-products-support-series-home.html.

Extension Mobility and Extension Mobility Cross Cluster

Extension Mobility and Extension Mobility Cross Cluster are Cisco Unified Communications Manager features that allow agents to temporarily access their Cisco Unified IP Phone configuration, such as line appearances, services, and speed dials, from other Unified IP Phones.

Extension Mobility works on phones that are located within the same Unified Communications Manager cluster. Extension Mobility Cross Cluster works on phones that are located in different Unified Communications Manager clusters.

As part of the configuration in **Unified Communications Manager Administration**, you create a device profile for each agent that will use Extension Mobility, and associate each device profile with the appropriate agent. You can add either all of the device profiles to the pguser, or all of the phones that the agents use to the pguser. You do not need to add both the profiles and phones to the pguser.

For more information, see the Extension Mobility section of the *Feature Configuration Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Mobile Agent

Mobile Agent supports call center agents who are using phones that are not directly controlled by Packaged CCE. A mobile agent can be located outside of the contact center, using an analog phone or a mobile phone. Mobile agents may also be located in the contact center using an IP phone connection that is not controlled by Packaged CCE. All mobile agents use broadband connection to access the same Agent desktop and agent state controls as non-mobile agents.

Packaged CCE supports both Call by Call and Nailed Connection mode.

Outbound Option

Outbound Option manages and performs outbound dialing campaigns. You configure the system to automatically dial numbers using imported contact lists and filtering rules. When a call connects to a live person, the system transfers the call to an agent skilled in handling that calling campaign.

Post-Call Survey

Post-Call Survey sends a caller to an automated survey after the agent disconnects. A Post-Call Survey is typically used to determine whether customers are satisfied with their call center experiences.

Single Sign-On

Single sign-on (SSO) is an authentication and authorization process. (Authentication proves you are the user you say that you are, and authorization verifies that you are allowed to do what you are trying to do.) SSO allows users 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 to 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.

Task Routing for Third-Party Multichannel Applications

Task Routing application programming interfaces (APIs) provide a standard way to request, queue, route, and handle third-party multichannel tasks in CCE.

Contact Center customers or partners must develop Customer Collaboration Platform and Finesse applications using these APIs to use the Task Routing feature. The Customer Collaboration Platform application submits nonvoice task requests to CCE. The Finesse application enables agents to sign in to different types of media and handle the tasks. Agents log in to and manage their state in each media independently.

Whisper Announcement

Whisper Announcement plays a brief message to an agent before connecting a caller to the agent. The message may include information about the caller or choices the caller made from menu options.

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.

Avaya Support

Support for Avaya integration has been provided in Packaged CCE 4000 and 12000 Agent deployments. You can maintain an Avaya Peripheral Gateway (PG) in a Packaged CCE environment and use its intelligent contact center routing capability to route calls to geographically distributed contact center sites.

ICM-to-ICM Gateway Support

Support for ICM-to-ICM Gateway has been provided in Packaged CCE 4000 and 12000 Agent deployments. ICM-to-ICM Gateway extends the ICM software capability by allowing agents to simultaneously pre-route/post-route calls, and supply additional call-related information to a second agent on a different ICM. This enables the initial agent to pass on gathered information without the customer’s needing to repeat it to the second agent.

Integrations with Other Cisco Products

You can extend Packaged CCE functionality by integrating it with other Cisco products.

Cisco Silent Monitoring

Silent monitoring allows a supervisor to listen in on agent calls for quality control and performance evaluation. Packaged CCE supports Unified CM-based silent monitoring.

Supervisors can start Unified CM-based silent monitor sessions by selecting an agent on the Team Performance page on their Cisco Finesse desktops and clicking **Start Monitoring**. They can then click **End** to end the session.

Cisco Customer Collaboration Platform

Cisco Customer Collaboration Platform is a customer-care system that provides capture, filtering, workflow, queuing, and reporting for social media engagement teams. Internet postings captured by Customer Collaboration Platform are referred to as Social Contacts. Customer Collaboration Platform stores the social contacts and groups them into user-defined Campaigns. Each Campaign obtains social contacts from one or more Feeds. Customer Collaboration Platform presents the social contacts to social media customer care personnel who can search, review, categorize, and respond to the postings. Customer Collaboration Platform also produces reporting metrics on the handling of the social contacts.

Customer Collaboration Platform is also used for the following contact center features:

- Agent Request
- Task Routing

For information about Customer Collaboration Platform, see https://www.cisco.com/en/US/products/ps11349/index.html.

Assumptions for Proceeding with Optional Features

This document makes the following assumptions about the state of your Packaged CCE system and the system administrator's knowledge of Packaged CCE:

- Your Packaged CCE system must be installed, configured, and operational.
- System administrators must have access to the following interfaces:
  - Cisco Packaged Contact Center Enterprise (CCE) Administration
  - Script Editor
  - Cisco Customer Collaboration Platform
  - Cisco Finesse
  - Cisco Unified Communications Manager (CUCM) reporting interface
  - Enterprise Chat and Email
- System administrators must be familiar with the following procedures or have access to the Cisco documentation that describes them:
  - Expanded call variables—Know how to use Unified CCE Administration to set variable values and add new variables.
  - Scripting—Know how to use the Script Editor to create new Packaged CCE call routing scripts and modify existing scripts. Understand the scripting technology.
  - CVP scripting—Know how to use the CVP Script Editor to create new or modify existing voice scripts.

The *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* describes all of the above procedures. This guide is available at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

CHAPTER 2

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/packaged-contact-center-enterprise/products-device-support-tables-list.html for the list of supported Packaged CCE 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 217

Initial Setup

This section is intended for system administrators responsible for installing and configuring Packaged 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 Defaul Administration, select **Device** > **Phone** > **Built in Bridge**.

Where	What
Unified CCE	Agent Greeting is supported with Type 10 Network VRUs only. (Type 10 is required to al 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: application; the second time is to tell the recording application where to save greetin Use the Unified CCE Administration tool to ensure this variable includes these setti • user.microapp.app_media_lib:This is required in Agent Greeting record and play scr greeting audio files are stored. Maximum Length - 100 and Enabled. • user.microapp.input_type: This is required in Agent Greeting record scripts to limit th No other ECC (Expanded Call Variable) are needed if you serve your files from the Unif default locale directory ("<*web_server_root*>\en-us\app"). However, if you store your fil the ECC in the next row in your scripts.
Unified CCE (optional variables, used to override defaults)	To make these variables available to your script authors, confirm that they are defined in ECC variables for CVP, see the *Administration Guide for Cisco Unified Customer Voice Po* 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 o • user.microapp.locale: Use to specify the name of the locale directory on the media s • user.microapp.UseVXMLParams: Required in your record script if you include the recording script to use the name/value pair of the application that you pass in the us
Unified CVP	Unified CVP Server must be installed and configured, as described in the *Cisco Package* https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-

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.

For more information, see *Setup Unified CVP Media Server IIS* section in 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.

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

For more information, see *Set Up IVR Service* section in 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/products-maintenance-guides-list.html.

Step 4 Configure a Unified CVP media server, if you have not already done so. See Media Server, on page 73.

Step 5 Set the cache size on the VXML Gateway. See Set Cache Size on VXML Gateway, on page 11.

Step 6 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 11.

Step 7 Configure call types to record and play agent greetings. See Configure Call Types, on page 12.

Step 8 Configure dialed numbers to record and play agent greetings. See Configure Dialed Numbers, on page 12.

Step 9 Schedule the Script, on page 13.

Step 10 Define Network VRU Scripts for Agent Greeting, on page 13.

Step 11 In Script Editor:

- To use the installed scripts to record and play agent greetings, see Import Example Agent Greeting Scripts, on page 14.
- To create your own scripts, see Agent Greeting Scripts, on page 17.

Step 12 Modify the Unified CCE call routing scripts to use Play Agent Greeting script, on page 16.

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 17.
  - 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.

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 end the call or return to the main menu

The built-in prompts are installed on each server at <*CCE_root*>`\wav` and are referenced in the example recording script that is included with Packaged CCE. To deploy the example script, copy the audio prompts to the <*web_server_root*>`\en-us\app` directory on your media server.

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.

Configure Call Types

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

Procedure

Step 1 In Unified CCE Administration, choose **Overview** > **Call Settings** > **Route Settings**.

Step 2 Click the **Call Type** tab.

Step 3 Click **New** to open the **New Call Type** window.

Step 4 Complete the fields to create a call type to record agent greetings. For **Name**, enter **`RecordAgentGreeting`**.

Step 5 Click **Save**.

Step 6 Repeat this procedure to create a call type to play agent greetings. For **Name**, enter **`PlayAgentGreeting`**

Configure Dialed Numbers

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

Procedure

Step 1 In Unified CCE Administration, choose **Overview** > **Call Settings** > **Route Settings**.

Step 2 Click the **Dialed Number** tab.

Step 3 Click **New** to open the **New Dialed Number** window.

Step 4 Complete the fields to create a dialed number to record agent greetings, as follows:

- **Dialed Number String:** RecordAgentGreeting

  The name must match exactly and is case-sensitive.

- **Routing Type:** Internal Voice
- **Call Type:** RecordAgentGreeting (the call type that you created for recording agent greetings)

Step 5 Click **Save**.

Step 6 Repeat this procedure to create a dialed number to play agent greetings. Complete the **New Dialed Number** fields as follows:

- **Dialed Number String:** PlayAgentGreeting

  The name must match exactly and is case-sensitive.

- **Routing Type:** Internal Voice
- **Call Type:** PlayAgentGreeting (the call type that you created for playing agent greetings)

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, log into Packaged CCE Administration and select **Overview** > **Call Settings** > **IVR Settings** > **Network VRU Scripts**.

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.

Table 2: 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.
`GreetingReview` `PM,-a,A`	`Y`	Y	This script allows the agent to review the recorded greeting audio file.

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 Unified CCE AW-HDS-DDS.

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 13) 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 runs the script. It requires that you define an AgentGreeting VRU script, described in Define Network VRU Scripts for Agent Greeting, on page 13.
- **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 13.
- **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 13) 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.

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.

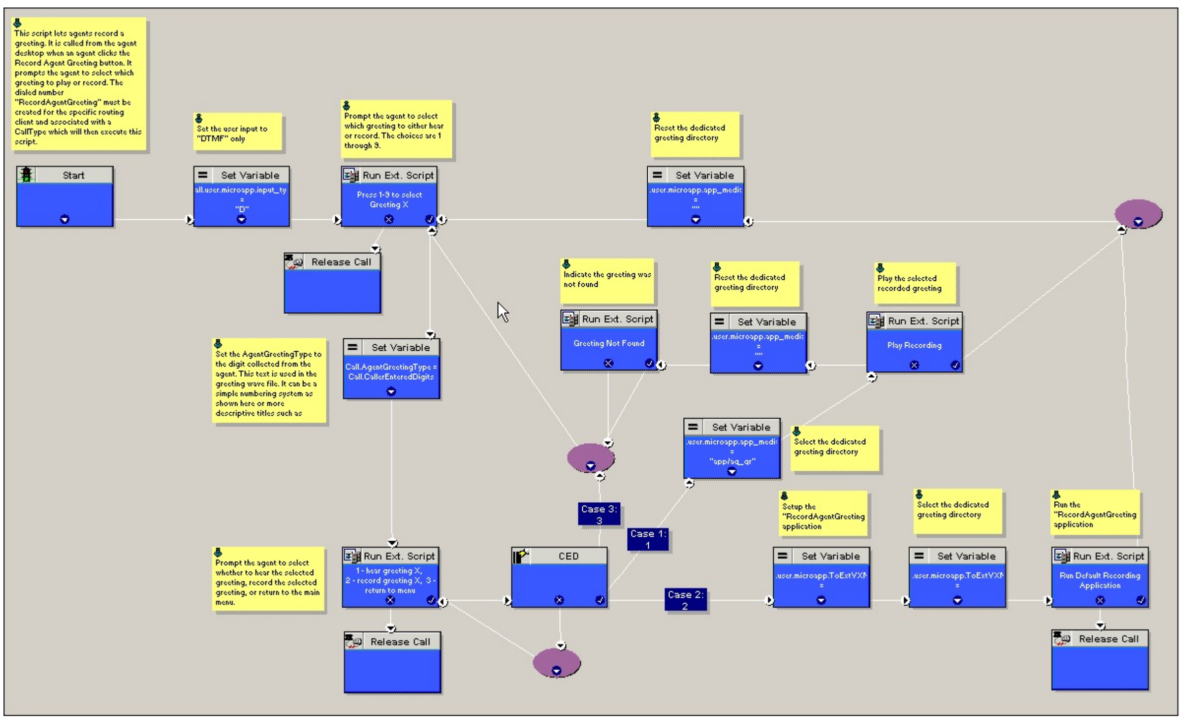
Agent Greeting Recording Script

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 1: Agent Greeting Record Script



302476

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 3: 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.
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 CVP Server uses to write greeting files to the media server. 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.
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 CVP Server.

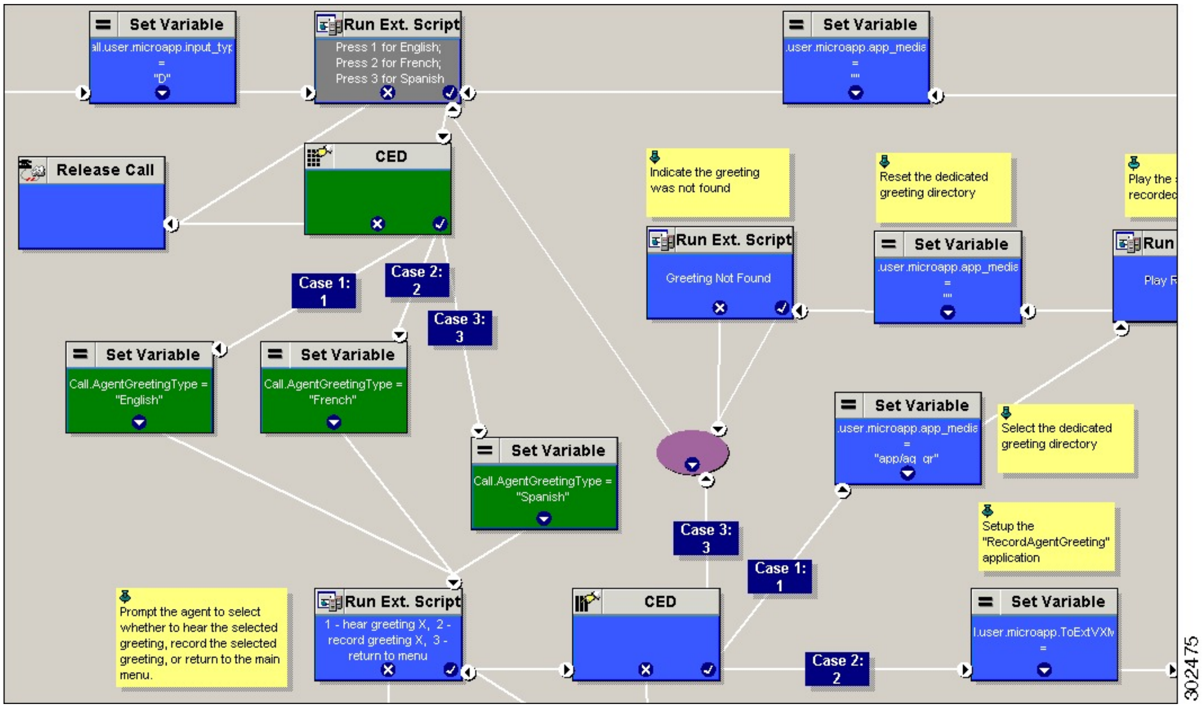
Descriptive Agent Greeting Type Strings

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 2: 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:

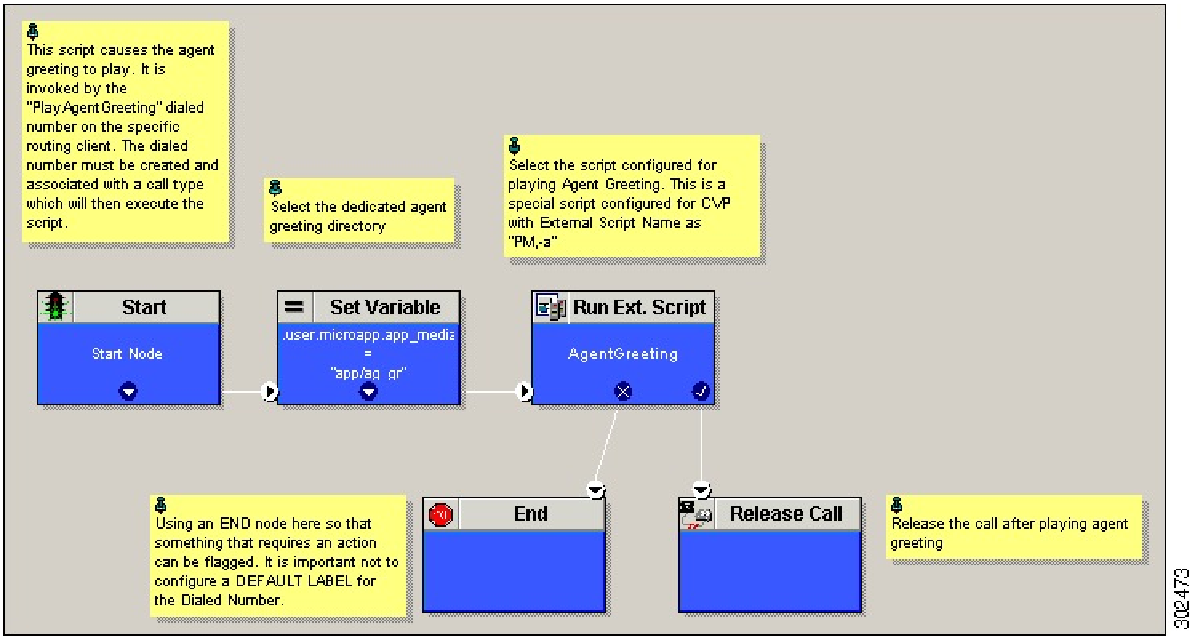
- A Run External Script node that calls the VRU script that plays the greeting.
- A Set Variable node that sets the directory path to your greeting files.

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 3: 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.

Administration and Usage

Use Agent Greeting with Your Finesse Desktop

Configure Custom Dialed Number for Finesse Agent Greeting Record

To record Agent Greetings with Finesse, create your own custom dialed number for recording. You may want to create different dialed numbers for different customers.

To record the greeting, your agents can enter the record dialed number using the dial pad on their desktops.

Use the following steps to create a custom dialed number for Finesse Agent Greeting Record:

1. Create a CTI Route Point in Unified CM and associate it with an Application User (PG User).
2. Create a Dialed Number in Unified ICM for the CTI Route Point created in Unified CM.

3. Create a Call Type for the Custom Dialed Number.
4. Associate the Call Type and Dialed Number with the Record Agent Greeting Script.
5. Create a Phonebook Entry in Finesse for the agent to dial the Custom Dialed Number.

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.

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 without the Agent Greeting.

CHAPTER 3

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.

Cisco Customer Collaboration Platform works in a Contact Center Enterprise (CCE) solution to process the request from its inception through the delivery of the callback.

Note Enterprise Chat and Email also offers callback and delayed callback. You can use Agent Request , Enterprise Chat and Email, or both.

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 Customer Collaboration Platform.

Customer Collaboration Platform and Agent Request

Customer Collaboration Platform 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 Customer Collaboration Platform 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 CCE using a notification mechanism (the Connection to 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.

Note Customer Collaboration Platform supports scalar ECC variables only.

CCE and Agent Request

CCE services in the Agent Request solution:

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

Agent Request Prerequisites

Install and configure Customer Collaboration Platform before implementing Agent Request. Customer Collaboration Platform must be geographically colocated with the Unified CCE PG on one side.

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 33.

Customer Collaboration Platform 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 27.

Agent Request Call Flow

The flow proceeds as follows:

1. The customer application initiates an agent request by requesting a callback.
2. Customer Collaboration Platform sends the request to the Unified CCE PG.
3. The Unified CCE PG sends the request to the agent.
4. 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 4: 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 Packaged CCE for Agent Request

Set up the Media Routing PG and PIM

Procedure

Step 1 Navigate to **Unified CCE Administration** > **Overview** > **Infrastructure Settings** > **Peripheral Gateways**. Determine the Peripheral ID for a Multichannel peripheral for the customer collaboration platform, as mentioned in the *Cisco Packaged Contact Center Enterprise Administration and Configuration guide*.

Note In Packaged CCE 4000 and 12000 Agents deployment, fetch the Peripheral ID from the PG Explorer tool using Configuration Manager.

Step 2 From Cisco Unified CCE Tools, select **Peripheral Gateway Setup**.

Step 3 On the Components Setup screen, in the Instance Components panel, select the PG Instance component. Click **Edit**.

Step 4 In the Peripheral Gateways Properties screen, click **Media Routing**. Click **Next**.

Step 5 Click **Yes** at the prompt to stop the service.

Step 6 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 for the unused Multichannel peripheral that you identified in Step 1.
d) For **Application Hostname (1)**, enter the hostname or IP address of Customer Collaboration Platform.

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.

e) By default, Customer Collaboration Platform accepts the MR connection on **Application Connection Port** 38001. The Application Connection Port setting on Customer Collaboration Platform 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 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 Customer Collaboration Platform as an external machine.

a) Click **Add Machine**.
b) Select Customer Collaboration Platform 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 Customer Collaboration Platform Administration, including the **Application Connection Port** you specified.

Unified CCE Administration Tools

This topic explains the Unified CCE Administration tools you use to configure Agent Request.

Before you begin

For details on the procedures for steps 2 to 5, refer to the Unified CCE Administration online help or to the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/en/US/products/ps12586/prod_maintenance_guides_list.html.

Procedure

Step 1 Sign in to Unified CCE Administration.

Step 2 **Call Type**: Create a call type for Agent Request.

Step 3 **Dialed Number**: Create a dialed number for Agent Request. You use this number when you configure the notification in Customer Collaboration Platform.

a) For **Routing Type**, select Customer Collaboration Platform.
b) For **Media Routing Domain**, select **Cisco_Voice**.
c) For **Call Type**, select the call type that you created in Step 2.

Step 4 **Expanded Call Variable**: You can use an existing Expanded Call Variable, or you can create an expanded call variable for Agent 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 Unified CVP, Finesse, and Customer Collaboration Platform.

Step 5 Create a **Network VRU Script**.

This network VRU script does not refer to a script that you create on a peripheral. This script satisfies a configuration requirement and provides a messaging vehicle to get the value of the estimated wait time to Customer Collaboration Platform using the MR PIM to fulfill the API call.

Use the Manage Network VRU Scripts gadget to create the new network VRU script. Choose a name (for example, VoiceCallback) and enter that name in both Name fields.

No configuration parameters are required for the network VRU script. Optionally, enter a description. In the remaining fields, leave the default values. You reference this configuration object when you configure the Run External Script node in the routing script.

Related Topics

Create Script for Agent Request, on page 31

Configure Customer Collaboration Platform for a Voice Callback Agent Request

To support a callback request, Customer Collaboration Platform 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 Customer Collaboration Platform.

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 Customer Collaboration Platform.

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 Customer Collaboration Platform.

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**.

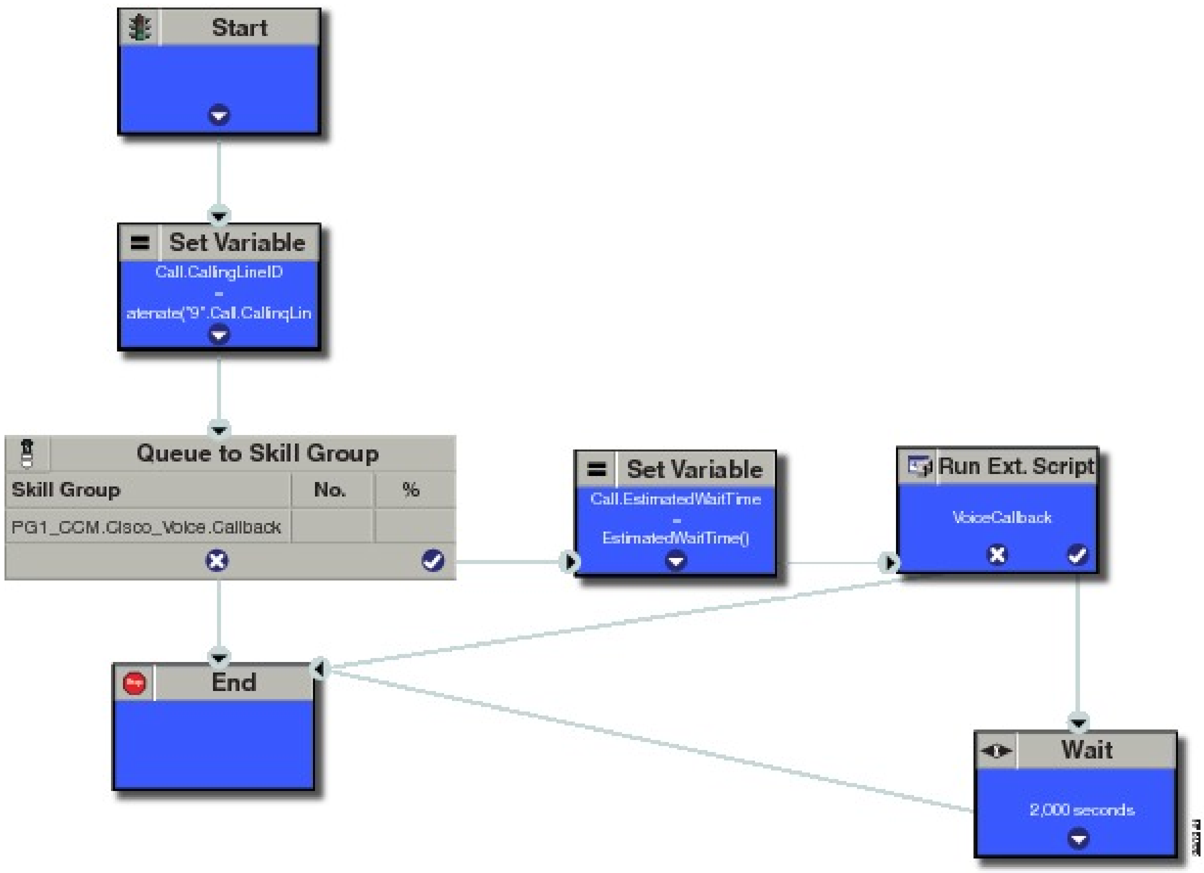
Step 9 In the **Dialed Number/Script Selector** field, enter the dialed number string that you have configured.

See Unified CCE Administration Tools, on page 28.

Step 10 Click **Save**.

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 Customer Collaboration Platform.

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

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

Related Topics

Unified CCE Administration Tools, on page 28

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 Customer Collaboration Platform Developer Guide.

Procedure

Step 1 Retrieve the feed id by entering this URL in a browser: **https://<Customer Collaboration Platform_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 Customer Collaboration Platform 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 4

Application Gateway

About Application Gateways

An application gateway is an optional Packaged CCE feature that allows you to invoke an external application from within a script (using a Gateway node). You can pass data to the application and receive data in return, which you can then examine and use for routing decisions.

Before you can use these nodes in a script, you must first configure the gateways.

The application gateway requires connection information to communicate with the external application. You perform this task using the Unified CCE Administration interface.

Configuring Application Gateways

Configure a application gateway for an application you want to access, from within the scripts.

Configuration information includes data such as:

- Type of application the gateway interacts with-a non-Packaged CCE application or an application on another Packaged CCE system
- Form of connection the gateway uses-duplex or simplex
- Fault tolerance strategy for the gateway-described in the following table.

Table 4: Application Gateway Fault Tolerance Strategies

Fault Tolerance Strategy	Description
Duplicate Request	Packaged CCE, both side A and B, connects to separate application gateway hosts. They send simultaneous requests. Each request is sent to both the sides of the gateway. The response that comes back first, is used by both the sides of A and B of ICM.

Fault Tolerance Strategy	Description
Alternate Request	Packaged CCE, Side A and Side B connects to separate application gateway hosts. All requests are sent alternatively to A and B.
Hot Standby	Each router manages a connection to a different host. All requests are directed to the designated primary host. If either host (or connection) fails then all requests are directed to the backup host. This results in the loss of some requests on failures.
None	The application gateway is not duplexed.

Once you specify the configuration information, you can define the connection information for the gateway. For example, the network address of the port, through which the system software communicates with the application.

If your Central Controller is duplexed, you can define separate connection information for each side of the Central Controller. This allows each side to communicate with a local copy of the external application.

Add and Maintain Application Gateways

You can create custom application gateways in Packaged CCE deployment.

Procedure

Step 1 In Unified CCE Administration, navigate to **System** > **Application Gateway**.

Step 2 In Unified CCE Administration, choose **Overview** > **Infrastructure Settings** > **Application Gateways**.

Step 3 To add a new gateway, click **New**.
The **New Application Gateway** page displays.

Step 4 Enter a name for the new application gateway. Maximum length is 32 characters. Valid characters are alphanumeric, period (.), and underscore (_). The first character must be alphanumeric.

Step 5 Enter a description.

Step 6 Select one of the options from the **Encryption** drop-down list.

- **None**: Selected by default. Indicates that the requests are not encrypted.
- **Private Key**: Indicates that the requests are encrypted using a private key.
- **TLS**: Indicates that the requests are encrypted using the TLS protocol.

Step 7 Select one of the options from the **Connection Type** drop-down list.

a) If you select **Duplex**, you can enter data in all the subsequent fields.
b) If you select **Simplex A**, the **Preferred Side** is set to **Side A**, **Fault Tolerance** is set to **None**, and the **Side B** box is disabled.
c) If you select **Simplex B**, the **Preferred Side** is set to **Side B**, **Fault Tolerance** is set to **None**, and the **Side A** box is disabled.

Step 8 Select a side from the **Preferred Side** drop-down list.

Step 9 Select one of the options from the **Fault Tolerance** drop-down list.

- **Alternate Request**: Each router manages connections with different hosts. The routers take turns to send half the request to the host connected to Side A and the other half to the host connected to Side B. If one host fails, the entire load is directed to the surviving host.
- **Duplicate Request**: Each router manages connections with different hosts. Each time a script initiates a request, both the routers communicate with their corresponding hosts. The routers process the response from the host that responds first.
- **Hot Standby**: Each router manages connections with different hosts. All the requests are directed to the designated primary host. If the host or the connection fails, all the requests are directed to the backup host.

Step 10 Enter the following server details in the **Side A** and **Side B** boxes as applicable:

- **In Service**: This option is enabled by default. If you uncheck the **In Service** check box, the connection is no more in service and the router does not send application gateway requests to that connection.
- **Hostname/IP Address**: Enter the IP address, hostname of the server, or fully qualified domain name (FQDN).
- **Port**: Enter the port number.
- **Initialization Data**: This information passes to the Application Gateway host at the time of initialization.

Step 11 Click **Advanced Settings** on Side A or Side B to open the respective **Advanced Settings** dialog box. The following parameters with default values appear:

- **Max Errors**: Indicates the number of consecutive errors that cause the software to declare the host unavailable.
- **Timeouts**
    - **Request**: Indicates the number of milliseconds the Router waits before timing out a request.
    - **Abandon**: Indicates the number of milliseconds the Router waits for a response before considering it as late.
    - **Late**: An internal timeout in milliseconds to communicate between the Router and the Application Gateway interface process.
- **Heartbeats**
    - **Request Timeout**: Indicates the number of milliseconds the Router waits for a response to a heartbeat before considering it as a failure.
    - **Retry Timeout**: Indicates the number of milliseconds the Router waits before retrying a missed heartbeat.
    - **Retry Limit**: Indicates the number of consecutive unanswered heartbeats after which the Router ends the connection.
    - **Interval**: Indicates the number of milliseconds the Router waits between successful heartbeats.
- **Sessions**
    - **Retry Timeout**: Indicates the number of milliseconds the Router waits before trying to reconnect after a connection terminates or a connection attempt fails.
    - **Retry Limit**: Indicates the number of times the Router tries to establish the connection before it quits.

- **Open Timeout**: Indicates the number of milliseconds the Router waits for a response to an open or close request. If it receives no response within this time, the Router assumes that the request failed.

Step 12 Edit the advanced settings parameters as applicable and click **OK**.

Note Click the **Restore Defaults** button to restore the default values.

Step 13 Click **Save**.

CHAPTER 5

Business Hours

Business Hours Overview

Business hours are the working hours during which you conduct business. You can create and modify business hours and set weekly and daily schedules for each business hour. You can create different business hour schedules for regular working days and holidays. You can also open or close the business hours if there is an emergency.

You can define the status reasons for business hours and assign codes for each status reason. Status reason is required when you force open or force close a business hour, and when you add special hours and holidays.

Contact Center Enterprise Reference Design Support for Business Hours

Packaged CCE supports Business Hours for these reference designs:

- 2000 Agents
- 4000 Agents
- 12000 Agents

Business Hours Use Cases

Use the Business Hours feature to manage the incoming customer calls or digital channel communications, by routing these contacts based on the Business Hours you configure.

Use the Business Hour status in an IF node in scripts to control the call and digital channel contacts, such as email and chat, and notify the customers accordingly.

You can have Business Hours scripts for the following treatments:

- When the business is open, route calls and digital contacts to the applicable skill groups and precision queues.

- When the business is closed, play the message for the closed status with the appropriate Status Reason and terminate the call. Route the digital contacts to the appropriate queues.
- When the business is not open 24x7, route the calls to skill groups and precision queues for after-hours support or play the after-hours message.
- When the business is open 24x7, at a predefined time before the end of each shift, route the calls and digital contacts to the appropriate queues for the next shift.
- When the business is closed for an emergency on a working day, notify the customers contacting your contact center appropriately about the emergency closing.

Based on reason code and status, the customers will hear appropriate prompts on the call.

Set the Principal AW for Business Hours

You must specify and set the Principal AW before configuring the Business Hours.

The Principal AW (Admin Workstation) is responsible for managing background tasks that are run periodically to sync configuration with other solution components, such as SSO management, Smart Licensing, etc.

Procedure

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

Step 2 Click the AW that you want to set as **Principal AW**.
The Edit CCE AW window opens.

Step 3 Select the **Principal AW** check box.

Step 4 Enter the Unified CCE Diagnostic Framework Service domain, username, and password.

The credential must be of a domain user who is a member of the local administrator group if `ADSecurityGroupUpdate` registry key in AW is zero. If `ADSecurityGroupUpdate` registry key is set to 1, then the user must be available in the Config security group under the instance OU. These credentials must be valid on all CCE components in your deployment (routers, PGs, AWs, and so on).

Note Every time the Active Directory credentials are updated, the credentials configured here must be updated as well.

Step 5 Click **Save**.

Step 6 Restart Tomcat service on **Principal AW** machine.

Business Hours Set Up Workflow

This section provides information necessary to set up the Business Hours feature.

Table 5: Business Hours Set Up Workflow

Tasks	Documentation
Scripting for Business Hours	*Business Hours Variables* and *Dynamic Formula for Business Hours* in 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
Business Hours Configuration	Cisco Packaged Contact Center Enterprise Administration and Configuration Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html

Scripting for Business Hours

To enable scripting for Business Hours, use the following variables:

- Business Hour Status—The real time status based on the configured Business Hours.
- Reason Code— The reason code associated with the current status.

These variables must be used in the CCE script IF node to route the customer contacts.

Business Hours Configuration

Business hours can be configured by defining the following:

- **Default Open/Close (as per Business Calendar)**: The status of the regular hours.
- **Force Open**: Force the status of Business Hours to Open with a reason code.
- **Force Closed**: Force the status of Business Hours to Closed with a reason code.
- **24x7** setting: Set the schedules for 24x7 working. Status is Always Open.
- **Special Hours & Holiday**: Configure a holiday or special day. On a holiday, you can close the Business Hours for the whole day or open it for specific hours. On a special day, you can configure extra working hours (in cases where 24x7 working is not set), the evaluation stops when the Special Hours & Holiday step is evaluated and the status is derived from this step. Further Business Hours setting for that day will not be evaluated.
- **Custom**: Configure the regular working hours for a weekday and, if necessary, specify the working hours for each day in a week.

The following variables control this feature:

- **Time Zone**: The line of Business or team's operational time zone.
- **Reason Code**: Reason code for special days and Force Open/Close status.

  Apply the appropriate reason codes when you configure a Business Hour with **Force Open**, **Force Close**, and **Special Hours & Holidays**. When these Business Hour schedules are in effect, the associated reason code is available in the scripting environment and the real time reports. **Reason Code** configuration is not available for regular weekdays. In such cases, the system reports the default open and default close reason codes.

- **Department**: Associate the business hours to a department so that the change to business hours is restricted to only the user of that department.

Configure Yearly Schedules

You can configure and maintain a Business hours calendar for the whole year.

- Configure the regular working hours for weekdays.
- Configure **Special Hours & Holidays** schedules for whole year by doing the following:
  - Add the **Special Hours & Holidays** details for all the special hours and holidays for the whole year into the CSV template file.
  - On the **Import Special Hours & Holidays** page, click **Choose File** and browse to the special hours and holidays file.

    Click **Import** to upload the file.

    After you import the configuration file, the configurations are loaded on the Business Hours page. Validate the configurations.
  - Click **Save**.

Note When you update the configured Business Hours, remove any elapsed schedules and then update the new schedules for any new special hours or holidays in a Business Hour configuration.

Daylight Saving Time

The Business Hours feature uses **`Time Zone`** to determine the status based on the Business Hours configured. **`Time Zone`** is set based on the local time. When the daylight saving time (DST) settings are applicable to any **`Time Zone`**, the status is automatically adjusted for DST.

Note In case, any new Timezone definition is added or updated at the Windows Operating System (OS) through patch, apply that OS patch at both Side A and Side B at the same time.

Business Hours Status Evaluation

The status is evaluated using the following order of the configured Business Hour settings:

1. Force Open or Close
2. Special Hours and Holiday schedule
3. Open/Close as per Business Calendar

The evaluation terminates at the step at which the status is determined.

For example, if **Special Hours & Holidays** is configured, the evaluation stops when the **Special Hours & Holiday** step is evaluated and the status is derived from this step.

If any configuration is changed, the status is re-evaluated and updated to reflect the change.

CHAPTER 6

Courtesy Callback

Capabilities

Courtesy Callback reduces the time callers have to physically wait on hold or in a queue. The feature enables your system to offer callers (who meet your criteria) the option to receive a courtesy callback by the system instead of waiting on the phone for an agent. The caller who has been queued by Unified CVP can hang up and subsequently be called back when an agent is close to becoming available (preemptive callback).

Preemptive callback does not change the time a customer must wait to be connected to an agent, but rather enables the caller to hang up and not be required to remain in queue listening to music. Callers who have remained in queue or have undergone the callback treatment appears the same to agents answering the call.

If the caller decides to be called back by the system, they leave their name and phone number. Their request remains in the system and when the system determines that an agent will be available soon (or is available), then the system places a call back to the caller. The caller answers the call and confirms that they are the original caller and the system connects the caller to the agent after a brief wait.

In the event that the caller cannot be reached after a configurable max number and frequency of retries, the callback is aborted and the database status is updated appropriately. You can run reports to determine if any manual callbacks are necessary based on your business rules.

Note that you cannot schedule a callback for a specific time.

Note There are a number of prerequisites and design considerations for using this feature. See the Cisco Unified Customer Voice Portal Release Solution Reference Network Design (SRND) guide.

Note The Cisco Unified Customer Voice Portal Release Solution Reference Network Design (SRND) guide also describes how the system determines customer wait time and when to call the customer for the callback.

Callback Criteria

In your callback script, you can establish criteria for offering a caller a courtesy callback. Examples of callback criteria include:

- Number of minutes a customer is expected to be waiting *in queue* that exceeds a maximum number of minutes (based on your average call handling time per customer)

Note The included example scripts use this method for determining callback eligibility.

- Assigned status of a customer (*gold* customers may be offered the opportunity to be called back instead of remaining on the line)
- The service a customer has requested (sales calls, or system upgrades, for example, may be established as callback criteria)

Sample Scripts and Audio Files for Courtesy Callback

The courtesy callback feature is implemented using Unified CCE scripts. The installation provides a set of modifiable example CCE scripts, call studio scripts, and audio files to get you started. You can use these scripts in your implementation after making a few required changes.

Related Topics

CCE Script for Courtesy Callback, on page 58

Typical Use Scenario

If the caller decides to be called back by the system, they leave their name and phone number. Their request remains in the system and the EWT fires when the system places a callback to the caller. The caller answers the call and confirms that they are the original caller, and the system connects the caller to the agent after a short wait.

Note Courtesy Callback is supported for IP originated calls as well.

A typical use of the Courtesy Callback feature follows this pattern:

1. The caller arrives at Unified CVP and the call is treated in the IVR environment.
2. The Call Studio and Packaged CCE Courtesy Callback scripts determine if the caller is eligible for a callback based on the rules of your organization (such as in the prior list of conditions).
3. If a courtesy callback can be offered, the system tells the caller the approximate wait time and offers to call the customer back when an agent is available.
4. If the caller chooses not to use the callback feature, queuing continues as usual.

   Otherwise, the call continues as indicated in the remaining steps.

5. If the caller chooses to receive a callback, the system prompts the caller to record their name and to key in their phone number.
6. The system writes a database record to log the callback information.

Note If the database is not accessible, then the caller is not offered a callback and they are placed in queue.

7. The caller is disconnected from the TDM side of the call. However, the IP side of the call in Unified CVP and Packaged CCEis still active. This keeps the call in the same queue position. No queue music is played, so Voice XML gateway resources used during this time are less than if the caller had actually been in queue.
8. When an agent in the service/skill category the caller is waiting for is close to being available (as determined by your callback scripts), then the system calls the person back. The recorded name is announced when the callback is made to insure the correct person accepts the call.
9. The system asks the caller, through an IVR session, to confirm that they are the person who was waiting for the call and that they are ready for the callback.

   If the system cannot reach the callback number provided by the caller (for example, the line is busy, RNA, network problems, etc.) or if the caller do not confirm they are the caller, then the call is not sent to an agent. The agent is always guaranteed that someone is there waiting when they take the call. The system assumes that the caller is already on the line by the time the agent gets the call.

   This feature is called preemptive callback as the system assumes that the caller is already on the line by the time the agent gets the call and that the caller has to wait minimal time in queue before speaking to an agent.
10. The system presents the call context on the agent screen-pop, as usual.

In the event that the caller cannot be reached after a configurable maximum number and frequency of retries, the callback is stopped and the database status is updated appropriately. You can run reports to determine if any manual callbacks are necessary based on your business rules.

See the *Configuration and Administration Guide for Cisco Unified Customer Voice Portal* http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products_installation_and_configuration_guides_list.html guide which provides a call flow description of the function of the scripts that provide the Courtesy Callback feature.

Initial Setup

The Courtesy Callback feature must be configured on the following servers/gateways:

- Ingress Gateway (IOS configuration)
- VXML Gateway (IOS configuration)
- Virtualized Voice Browser (no special configuration is required if you use VVB instead of VXML Gateway)
- Reporting Server (through the PCCE Administration Tool)
- Media Server (upload of Courtesy Callback media files)

- Unified CVP VXML Server (upload of Call Studio Scripts)
- Packaged CCE

Courtesy Callback Design Considerations

The following design considerations apply for Courtesy Callback feature:

- During Courtesy Callback, callback is made using the same Ingress Gateway through which the call arrived.

Note In Courtesy Callback, outbound calls cannot be made using any other Egress Gateway.

- Calls that allow Callback must be queued using a Unified CVP VXML Server.
- The Unified CVP Reporting Server is a prerequisite for Courtesy Callback.
- Answering machine detection is not available for this feature. During the callback, the best that can be done is to prompt the caller with a brief IVR session and acknowledge with DTMF that they are ready to take the call.
- Calls that are transferred to agents using DTMF *8, TBCT, or hookflash cannot use the Courtesy Callback feature.
- Callbacks are a best-effort function. After a limited number of attempts to reach a caller during a callback, the callback is terminated and marked as failed.
- Customers must configure the allowed or blocked numbers that Callback is allowed to place calls through the Unified CVP Operations Console.
- Media inactivity detection feature on the VXML Gateway can impact waiting callback calls. For more information, see the *Configuration Guide for Cisco Unified Customer Voice Portal (CVP)*.
- Courtesy Callback requires an accurate EWT calculation for its optimal behavior.

  Consider the following recommendations to optimize the EWT, when using Precision Queues for Courtesy Callback :

  - Queue the calls to a single Precision Queue
  - Do not include a `Consider If` expression when you configure a step.
  - Do not include a wait time between steps or use only one step in the Precision Queue.

Configure the Ingress Gateway for Courtesy Callback

The ingress gateway where the call arrives is the gateway that processes the preemptive callback for the call, if the caller elects to receive a callback.

Note A sip-profile configuration is needed on ISR for the courtesy callback feature, only when deploying an IOS-XE version affected by CSCts00930. For more information on the defect, access the Bug Search Tool at https://sso.cisco.com/autho/forms/CDClogin.html.

For more information about sip-profile configuration, see *Design Guide for Cisco Unified Customer Voice Portal*, at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-implementation-design-guides-list.html.

Procedure

Step 1 Download the **survivability.tcl** file from DevNet: https://developer.cisco.com/site/customer-voice-portal/downloads/courtesy-callback-scripts/

Step 2 Copy the survivability.tcl file to the flash memory of the Ingress gateway.

Step 3 Log in to the ingress gateway.

Step 4 If survivability is not already configured, configure it as described in the "Call Survivability" section of the *Configuration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html.

Step 5 To add services to the gateway, you must be in enabled-config application mode. Type these commands at the gateway console:

```
GW81#en
GW81#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
GW81(config)#application
GW81(config-app)#
```

Step 6 Add the following to the survivability service:

```
param ccb id:<host name or ip of this gateway>;loc:<location name>;trunks:<number of callback
trunks>
```

Where the definitions of the preceding fields are:

- *id*: A unique identifier for this gateway and is logged to the database to show which gateway processed the original callback request.
- *loc*: An arbitrary location name specifying the location of this gateway.
- *trunks*: The number of DS0's reserved for callbacks on this gateway. Limit the number of T1/E1 trunks to enable the system to limit the resources allowed for callbacks.

The following example shows a basic configuration:

```
service cvp-survivability flash:survivability.tcl
param ccb id:10.86.132.177;loc:doclab;trunks:1
!
```

If you are updating the survivability service, or if this is the first time you created the survivability service, remember to load the application using the command:

```
call application voice load cvp-survivability
```

Step 7 Create the incoming dial peer, or verify that the survivability service is being used on your incoming dial peer. For example:

```
dial-peer voice 978555 pots
service cvp-survivability
incoming called-number 9785551234
direct-inward-dial
!
```

Note: We support both POTS and VoIP dial peers that point to a service provider.

Step 8 Create outgoing dial peers for the callbacks. These dial peers place the actual callback out to the PSTN. For example:

```
dial-peer voice 978554 pots
destination-pattern 978554....
no digit-strip
port 0/0/1:23
!
```

Step 9 Use the following configuration to ensure that SIP is set up to forward SIP INFO messaging:

```
voice service voip
signaling forward unconditional
```

Step 10 Save your changes.

Configure the VXML Gateway for Courtesy Callback

To configure the VXML gateway for Courtesy Callback:

Procedure

Step 1 Download the **cvp_ccb_vxml.tcl** file from DevNet: https://developer.cisco.com/site/customer-voice-portal/downloads/courtesy-callback-scripts/

Step 2 Copy the **cvp_ccb_vxml.tcl** to the flash memory of the VXML gateway.

Step 3 To add services to the gateway, you must be in enabled-config application mode. Type these commands at the gateway console:

```
GW81#en
GW81#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
GW81(config)#application
GW81(config-app)#
```

Step 4 Add the cvp_cc service to the configuration:

```
service cvp_cc flash:cvp_ccb_vxml.tcl
```

The service does not require any parameters.

Load the application with the command:

```
call application voice load cvp_cc
```

Note The media-inactivity detection feature must be turned off in the VXML Gateway to successfully call back the caller. With media-inactivity enabled on the VXML Gateway, the cvp_cc service will disconnect the waiting callback calls after 'ip rtcp report interval' * 1000-milliseconds interval. This configuration becomes important in a colocated Ingress/VXML setup where media inactivity timers are always enabled. In such scenarios, the 'ip rtcp report interval' must be increased to support the maximum allowable waiting for a callback call as defined by the solution requirements.

Step 5 On the VoIP dial-peer that defines the VRU leg from Packaged CCE, verify that the codec can be used for recording. The following example shows that g711ulaw can be used for recording in Courtesy Callback:

```
dial-peer voice 123 voip
service bootstrap
incoming called-number 123T
dtmf-relay rtp-nte
codec g711ulaw
no vad
!
```

In other words, this example shows the g711ulaw codec set on the 123 voip dial-peer. The codec must be specified explicitly. A codec class cannot be used because recording will not work.

Step 6 Use the following configuration to ensure that SIP is set up to forward SIP INFO messaging:

```
voice service voip
signaling forward unconditional
```

Step 7 VXML 2.0 is required to play the beep to prompt the caller to record their name in the BillingQueue example script. Add the following text to the configuration so the VXML Server uses VXML 2.0:

```
vxml version 2.0
```

Note Whenever vxml version 2.0 is enabled on the gateway,vxml audioerror is off by default. When an audio file cannot be played, error.badfetch will *not* generate an audio error event. To have the gateway generate an error.badfetch event when a file cannot be played, enable vxml audioerror in your gateway configuration. The following example uses config terminal mode to add both commands:

```
config t
vxml version 2.0
vxml audioerror
exit
```

Step 8 Save your changes.

Configure the Reporting Server for Courtesy Callback

Before you begin

A Reporting Server is required for the Courtesy Callback feature. The Reporting Server must be installed prior to completing the following task. For instructions, 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.

Procedure

Step 1 Log in to PCCE Administration Tool.

Step 2 In **Unified CCE Administration**, choose **Overview** > **Features** > **Courtesy Callback**.

Step 3 From the **Site** drop-down list, choose a site for which you want configure the Courtesy Callback feature. By default, it is 'Main'.

Step 4 From the **CVP Reporting Server** drop-down list, choose a Reporting Server to use for storing Courtesy Callback data.

Note The list includes all the Reporting Servers configured for the site.

If you leave the selection blank, no Reporting Server is associated with the Courtesy Callback deployment.

Step 5 In the **Dialed Number Configuration** section, complete the following:

Fields	Required?	Description
Maximum Callbacks per Dialed Number	Yes	By default, the **Unlimited** option is selected, which is equivalent to an unlimited number of callbacks offered per calling number. The maximum value is 1000. To limit the number of calls, from the same calling number that are eligible to receive a callback: **a.** Select the **Limited** option. **b.** Enter a postive number in the text field to allow Courtesy Callback to validate and allow the specified number of callbacks per calling number.
Allow unmatched Dialed Numbers	Yes	Check the **Allow unmatched Dialed Numbers** check box to allow callbacks to the dialed numbers that are not available in the **Allowed Dialed Number Patterns** list. **Note** If no dialed numbers are present in the **Allowed Dialed Number Patterns** list, then Courtesy Callback does not allow any callbacks.

Fields	Required?	Description
Allowed Dialed Number Patterns	No	The list of allowed dialed numbers to which callbacks can be se By default, the list includes preconfigured allowed dialed numb patterns. To add a dialed number pattern: **a.** Click the '+' icon and enter a dialed number pattern. **b.** Click **Add**. To remove a dialed number pattern, click the 'x' icon associated the number in the list.
Denied Dialed Number Patterns	No	The list of denied dialed numbers to which callbacks are never s By default, the list includes preconfigured denied dialed number patterns. To add a dialed number pattern: **a.** Click the '+' icon and enter a dialed number pattern. **b.** Click **Add**. To remove a dialed number pattern, click the 'x' icon associated the number in the list. Denied numbers takes precedence over allowed numbers. • Wildcarded DN patterns can contain "." and "X" in any posi to match a single wildcard character • Any of the wildcard characters in the set ">*!T" will match multiple characters but can only be used trailing values bec they will always match all remaining characters in the strin • The highest precedence of pattern matching is an exact mat followed by the most specific wildcard match. • When the number of characters are matched equally by wildcarded patterns in both the Allowed Dialed Numbers a Denied Dialed Numbers lists, precedence is given to the on the Denied Dialed Numbers list.

Step 6 Click **Save**.

Configure the Media Server for Courtesy Callback

Several Courtesy-Callback-specific media files are included with the sample scripts for Courtesy Callback.

You can download the Courtesy Callback specific sample media files and scripts (CCBAudioFiles.zip) from DevNet **Customer Voice Portal (CVP)** > **Downloads** > **Courtesy Callback Sample Scripts** at https://developer.cisco.com/site/customer-voice-portal/downloads/courtesy-callback-scripts/

The special audio files should be unzipped and copied to your media server.

CCBAudioFiles.zip has callback-specific application media files under `C:\inetpub\wwwroot\en-us\app` and media files for Say It Smart under `C:\inetpub\wwwroot\en-us\sys`.

Note If you selected the Media File installation option, during the Unified CVP install, the audio files were unzipped and copied to `C:\inetpub\wwwroot\en-us\app` on the installation server.

Note CCBAudioFiles.zip also contains media files for Say It Smart. During installation, these files are copied to `C:\inetpub\wwwroot\en-us\sys`. Copy these files to your media server, if you do not have them there already.

Note The sample scripts are set up to use the default location of `http://<server>:<port>/en-us/app` for the audio files. Later in this configuration process you will change the <server> and <port> parameters in the default location of the audio files in the example scripts to be your media server IP address and port number.

Configure Call Studio Scripts for Courtesy Callback

The Courtesy Callback feature is controlled by a combination of Call Studio scripts and ICM scripts. Refer to the *Solution Design Guide for Cisco Unified Contact Center Enterprise* (formerly the *Cisco Unified Customer Voice Portal Solution Reference Network Design*) at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-implementation-design-guides-list.html for a discussion of the script logic.

To configure the Call Studio scripts, perform the following procedure:

Note This example follows the BillingQueue example application.

Procedure

Step 1 Extract the example Call Studio Courtesy Callback scripts contained in CourtesyCallbackStudioScripts.zip to a folder of your choice on the computer running Call Studio.

You can access the .zip file from the following two locations:

- From the Unified CVP install media in \CVP\Downloads and Samples\Studio Samples\CourtesyCallbackStudioScripts
- From DevNet (**Customer Voice Portal (CVP)** > **Downloads** > **Courtesy Callback Sample Scripts**) at https://developer.cisco.com/site/customer-voice-portal/downloads/courtesy-callback-scripts/

Step 2 Each folder contains a Call Studio project having the same name as the folder. The five individual projects comprise the Courtesy Callback feature.

Do *not* modify the following scripts:

- CallbackEngine: Keeps the VoIP leg of the call alive when the caller elects to receive the callback (and ends the call) and when the caller actually receives the callback. Do **not** modify this script.
- CallbackQueue: Handles the keepalive mechanism for the call when callers are in queue and listening to the music played by BillingQueue.

Modify the following scripts to suit your business needs:

- BillingQueue: Determines the queue music played to callers.
- CallbackEntry: Modify the initial IVR treatment a caller receives when entering the system and is presented with an opportunity for a callback.
- CallbackWait: Modify the IVR treatment a caller receives when they respond to the callback.

Note Do not change the CCB application names.

Step 3 Start Call Studio by selecting **Start** > **Programs** > **Cisco** > **Cisco Unified Call Studio**.

Step 4 In Call Studio, select **File** > **Import**.

Step 5 In the Import dialog box, expand the Call Studio folder and select **Existing Call Studio Project Into Workspace** .

Step 6 Click **Next**.

Step 7 In the Import Call Studio Project From File System dialog, browse to the location where you extracted the call studio projects. For each of the folders that were unzipped, select the folder (for example BillingQueue) and click **Finish**.

The project is imported into Call Studio. Repeat this action for each of the five folders.

When you are finished importing the five folders, you should see five projects in the *Navigator* window in the upper left.

Step 8 Update the Default Audio Path URI field in Call Studio to contain the IP address and port value for your media server.

For each of the Call Studio projects previously unzipped, complete the following steps:

a) Select the project in the Navigator window of Call Studio.
b) Click **Project** > **Properties** > **Call Studio** > **Audio Settings**.
c) On the Audio Settings window, modify the Default Audio Path URI field by supplying your server IP address and port number for the <*Server*> and <*Port*> placeholders.
d) Click **Apply**, and then click **OK**.

Step 9 Billing Queue Project: If desired, change the music played to the caller while on hold.

You can also create multiple instances of this project if you want to have different hold music for different clients, for example, BillingQueue with music for people waiting for billing, and SalesQueue with music for people waiting for sales. You also need to point to the proper version (BillingQueue or SalesQueue) in the ICM script. In the ICM script, the parameter queueapp=BillingQueue would also have a counterpart, queueapp=SalesQueue.

The CallbackEntry Project (in the following step) contains a node called SetQueueDefaults. This node contains the value Keepalive Interval which must be *greater* than the length of the queue music you use. Refer to the Keepalive Interval in the next step for details.

Step 10 Callback Entry Project: If desired, in the CallbackEntry project, modify the caller interaction settings in the SetQueueDefaults node.

This step defines values for the default queue. You can insert multiple SetQueueDefaults elements here for each queue name, if it is necessary to customize configuration values for a particular queue. If you do not have a SetQueueDefaults element for a given queue, the configuration values in the default queue are used.

Note You can define a Callback_Set_Queue_Defaults node with **Queue Name** parameter set to default. Configuration defined in this default node will be picked whenever a queue type is encountered for which there are no explicitly defined values.

a) In the Call Studio Navigator panel, open the CallBackEntry project and double click **app.callflow** to display the application elements in the script window.
b) Open the Start of Call page of the script using the tab at the bottom of the script display window.
c) Select the SetQueueDefaults node.
d) In the **Element Configuration panel**, select the Setting tab and modify the following default settings as desired:

   For the SetQueueDefaults element, the caller interaction values in the Start of Call and the Wants Callback elements, may be edited.

Step 11 Perform the following steps.

a. Set the path for the storage of recorded caller names.

b. Select app.callflow.

c. In the CallbackEntry project, on the Wants Callback page, highlight the Record Name node and click the **Settings** tab in the Element Configuration window of Call Studio.

d. In the Path setting, change the path to the location where you want to store the recorded names of the callers.

By default, Call Studio saves the path string in your VXML Server audio folder. If you are using the default path, you can create a new folder called recordings in the `%CVP_HOME%\VXMLServer\Tomcat\webapps\CVP\audio\` folder on the VXML Server. If you are using IIS as your media server, create a new folder called recordings under `C:\Inetpub\wwwroot\en-us\app` and set that as the path for recordings.

Step 12 Set the name of the Record name file.

From the CallbackEntry project on the Wants Callback page, highlight the **Add Callback to DB** node and select the **Settings** tab in the Element Configuration window of Call Studio.

Change the **Recorded name file** setting to match the location of the recording folder you created.

This setting references the URL of the recordings folder, whereas the Path setting references the file system path.

The AddCallback element setting in the CallbackEntry project is configured to do automatic recorded file deletions. If automatic recorded file deletion is not desired, then remove the value of the Recorded name path setting in the AddCallback element. This removal action assumes that you will be doing the deletion or management of the recorded file yourself.

Step 13 In the CallbackEntry project on the Callback_Set_Queue_Defaults node, be sure the keepalive value (in seconds) is greater than the length of the queue music being played. The default is 120 seconds.

Step 14 Save the **CallbackEntry** project.

Step 15 CallbackWait Project: Modifying values in the CallbackWait application.

In this application, you can change the IVR interaction that the caller receives at the time of the actual callback. The caller interaction elements in **CallbackWait** > **AskIfCallerReady (page)** may be modified. Save the project after you modify it. The WaitLoop retry count can also be modified from the default of six retries in the Check Retry element. This will allow a larger window of time to pass before the call is dropped from the application. It is used in a failure scenario when the CallbackServlet on the reporting server cannot be reached. For instance, in a reboot or a service restart, this allows more time for the reporting server to reload the entry from the database when it is initializing. If the reporting server is not online within the retry window, then the entry will not be called back.

Step 16 Validate each of the five projects associated with the Courtesy Callback feature by right-clicking each Courtesy Callback project in the Navigator window and selecting **Validate**.

Deploy VXML Application to VXML Server

You can deploy a VXML application to the VXML Server using the File Transfer feature in Packaged CCE Administration web application.

Procedure

Step 1 After validating and saving your applications, in the navigator panel of Call Studio (top left), right-click and select all the applications you want to deploy.

Step 2 Click **Deploy**.

Step 3 In the Deploy Destination area, select **Archive File** and click **Browse**.

Step 4 Navigate to the archive folder that you have set up; for example, `C:\Users\Administrator\Desktop\Sample`.

Step 5 Enter the name of the file; for example, **Samplefile.zip**.

Step 6 Click **Save**.

Step 7 In the Deploy Destination area, click **Finish**.

Step 8 Log in to the Packaged CCE Administration web application from the principal AW machine.

Step 9 Choose **Overview** > **Call Settings** > **IVR Settings** > **File Transfers**.

Step 10 Click **New** to open the **New File Transfer** page.

Step 11 Click **Add to Server** to open the **Upload File** pop-up.

Note You can upload one file at a time.

Step 12 Click **Click to select** and select a zip file to upload.

Step 13 Click **Upload**.

The file is uploaded to AW and listed under **Available Files in the Server**.

Note You can hover over a row and click the **x** icon to delete a file from the server.

Step 14 Select one or more sites for the file transfer.

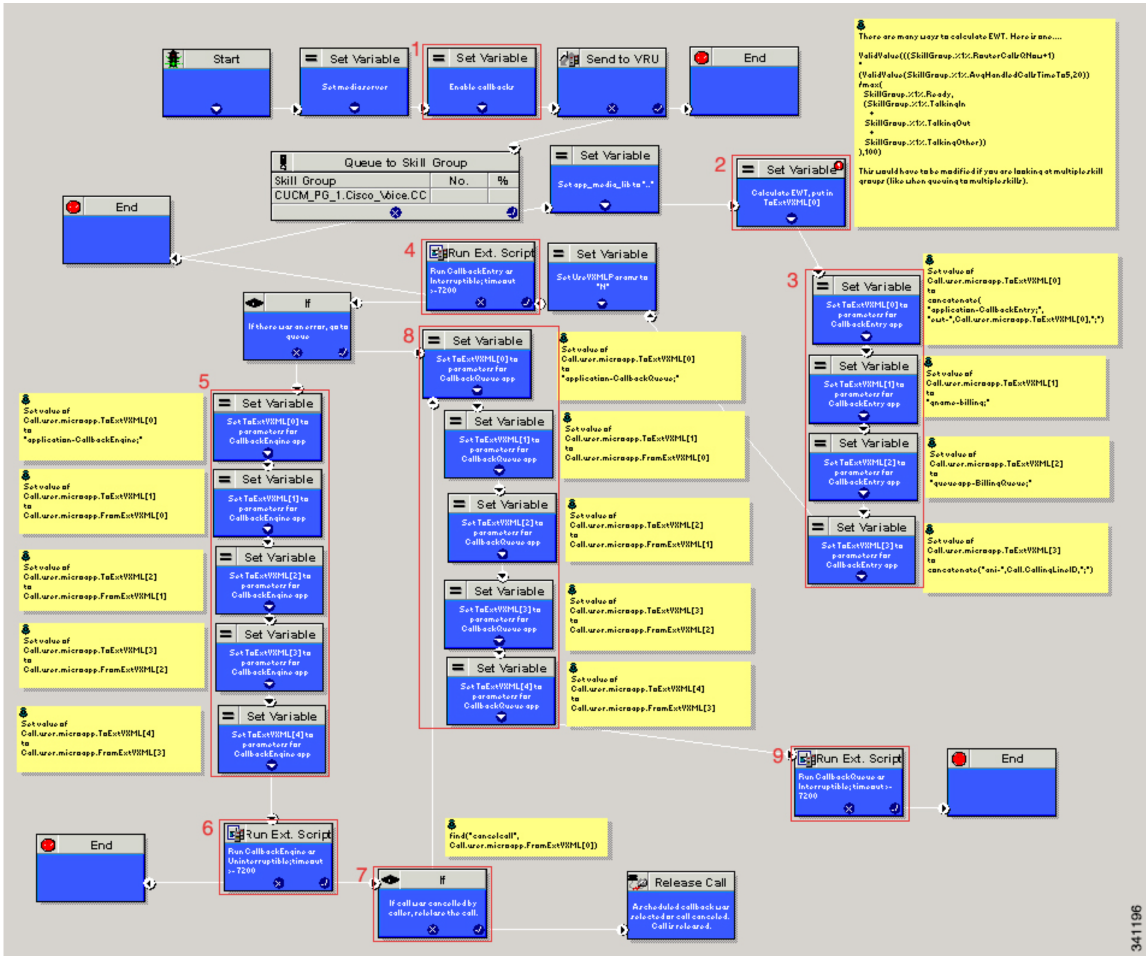
Step 15 On the **Available Files in the Server** list, select the files that you want to transfer and click **Save**. This initiates the transfer of the selected files to VXML Server of the selected sites.

CCE Script for Courtesy Callback

The following discussion provides an overview of the scripts used for the courtesy callback feature. There are nine numbered blocks, or sets of blocks, identified in the following figure.

Note In the following example, the yellow comment blocks describe first the value being set and then the place where the value is being sent.

Figure 5: Setting Value for Courtesy Callback



The following bullets provide descriptions for the numbered blocks in the preceding graphic:

- Block 1: Enable callback or shut it off.
- Block 2: Compute average wait time. Once the caller is *in queue*, calculate the Estimated Wait Time (EWT) for that queue and place the value in ToExtVXML[0].

  If there is poor statistical sampling because of sparse queues and the wait time cannot be calculated in the VXML Server, use the ICM-calculated estimated wait time.

  One method of calculating EWT (the method used in this example) is:

```
ValidValue(((SkillGroup.%1%.RouterCallsQNow+1)
*
(ValidValue(SkillGroup.%1%.AvgHandledCallsTimeTo5,20))
/max(
SkillGroup.%1%.Ready,
(SkillGroup.%1%.TalkingIn
+
SkillGroup.%1%.TalkingOut
+
SkillGroup.%1%.TalkingOther))
),100)
```

Modify this method if you are looking at multiple skill groups (when queuing to multiple skills).

- Block 3: Set up parameters to be passed.
- Block 4: Run this block and prompt the caller. If the caller does not accept the offer for a callback, keep the caller in the queue and provide queue music.
- Block 5: Set up variables. Call flow returns to this block if the caller elects to receive a callback. Otherwise, the call remains queuing in the queuing application (BillingQueue in this example) on the VXML Server.
- Block 6: Run external to Callback engine to keep the call alive. If the agent becomes available and there is no caller, then agent can't interrupt (do not want an agent to pick up and have no one there).
- Block 7: Has the caller rejected the callback call? If no, then go to block 8.
- Block 8: Compute average wait time, as in block 2.
- Block 9: Set up variables.
- Block 10: Put caller briefly into queue (after caller accepts the actual callback call).

Modifiable Example Scripts and Sample Audio Files

The courtesy callback feature is implemented using Unified CCE scripts. Modifiable example scripts are provided. These scripts determine whether or not to offer the caller a callback, depending on the callback criteria (previously described). Sample audio files are also provided.

The example scripts and audio files are located on the CVP installation media in the `\CVP\Downloads and Samples\` folder.

The files provided are:

- `CourtesyCallback.ICMS`, the ICM script, in the `ICMDownloads` subfolder
- `CourtesyCallbackStudioScripts.zip`, a collection of Call Studio scripts, in the `helloStudio` Samples subfolder.

  The following example scripts are provided:

  - BillingQueue: Plays queue music to callers. Can be customized.
  - Callback Engine: Keeps the VoIP leg of the call alive when the caller elects to receive the callback (and ends the call) and when the caller actually receives the callback. *Do not* modify this script.
  - CallbackEntry: Initial IVR when caller enters the system and is presented with opportunity for a callback. Can be customized.
  - CallbackQueue: Handles the keepalive mechanism for the call when callers are in queue. Do *not* modify this script.
  - CallbackWait: Handles IVR portion of call when caller is called back. Can be customized.

- `CCBAudioFiles.zip` contains sample audio files that accompany the sample studio scripts.

  If you use `CCBAudioFiles.zip`, unzip the contents onto the media server. `CCBAudioFiles.zip` has Courtesy Callback-specific application media files under `en-us\app` and media files for **Say It**

Smart under `en-us\sys`. If you already have media files for **Say It Smart** on your media server, then you only require the media files under `en-us\app`.

> **Note** The Courtesy Callback sample files and scripts are also available on DevNet (**Customer Voice Portal (CVP)** > **Downloads** > **Courtesy Callback Sample Scripts**) at https://developer.cisco.com/site/customer-voice-portal/downloads/courtesy-callback-scripts/.

Overview of CCE Script Configuration for Courtesy Callback

The provided CCE script for Courtesy Callback contains the necessary sample elements for the Courtesy Callback feature. However, you must merge this script into your existing CCE scripts.

As a starting point and to run a simple test, import the script into the CCE script editor, validate it with the CCE script editor validation tool to locate nodes that need extra configuration (such as for Network VRU scripts and expanded call variables), and then modify the script according to your existing CCE environment.

The general process is as follows:

1. Locate each queue point in every CCE script. For example: Queue To Skill Group, Queue to Enterprise Skill Group, Queue to Scheduled Target or Queue to Agent.
2. Categorize each queue point according to the pool of resources that it is queuing for. Each unique pool of resources will ultimately require a queue in VXML Server if Courtesy Callback is going to be offered for that resource pool. For example, using the following example, QueueToSkill X and QueueToSkill Z are queuing for the exact same resource pool (despite the different queuing order). Queue to Skill Y, however, is queuing to a different pool because it includes Skill Group D.
   - QueueToSkillGroup X is queuing for Skill Group A, B, C in that order.
   - QueueToSkillGroup Y is queuing for Skill Group A, C and D in that order.
   - QueueToSkillGroup Z is queuing for Skill Group C, B, A in that order.
3. Assign a unique name to each unique resource pool. In the above example, we can use names ABC and ACD as example names.
4. For each resource pool, decide whether callbacks will be allowed in that resource pool. If yes, then every occurrence of that resource pool in all ICM scripts must be set up to use VXML Server for queuing. This is to ensure that the Courtesy Callback mechanism in the VXML Server gets a full, accurate picture of each resource pool's queue.
5. For any queue point where Courtesy Callback will be offered, modify all CCE scripts that contain this queue point according to the guidelines in the following CCE script examples.

Configure the CCE Script for Courtesy Callback

Many of the following configuration items relate to the numbered blocks in the diagram and provide understanding for CCE Script for Courtesy Callback (for more information, see CCE Script for Courtesy Callback, on page 58). Steps that refer to specific blocks are noted at the beginning of each step.

To configure CCE to use the sample Courtesy Callback CCE script, perform the following steps:

Procedure

Step 1 Copy the CCE example script, **CourtesyCallback.ICMS** to the CCE Admin Workstation.

The example CCE script is available in the following locations:

- On the CVP install media in `\CVP\Downloads and Samples\`.
- On DevNet (**Customer Voice Portal (CVP)** > **Downloads** > **Courtesy Callback Sample Scripts**) at https://developer.cisco.com/site/customer-voice-portal/downloads/courtesy-callback-scripts/

Step 2 Perform these steps:

a) Enable the user.CourtesyCallbackEnabled ECC variable.
b) Enable the user.microapp.ToExtVXML ECC variable and verify that it is set up as an array with a maximum array size of 5 elements.
c) Enable the user.microapp.FromExtVXML ECC variable and verify that it is set up as an array with a maximum array size of 4 elements.

Step 3 Make sure the VXML_Server_Interruptible and the VXML_Server_Noninterruptible Network VRU scripts exist.

Step 4 Once the script is open in Script Editor, open the **Set media server** node and specify the URL for your VXML Server.

For example: **http://10.86.132.139:7000/CVP**

With the current implementation of CVP, you do not have to specify the VXML Server URL. You do, however, have to enter *some* numeric value; for example "1" (with quotes).

Step 5 Map the route and skill group to the route and skill group available for courtesy callback.

a) In Script Editor, select **File** > **Import Script...**.
b) In the script location dialog, select the **CourtesyCallback.ICMS** script and click **Open**.
c) In the Import Script - Manual Object Mapping window, map the route and skill group to the route and skill group available for courtesy callback (identified previously).

In Packaged CCE deployments, the route tool does not exist. Routes have one-on-one mappings with skill groups, so when you create a skill group, a route is created with the same name.

Step 6 **Block #2:** If you wish to use a different estimated wait time (EWT), modify the calculation in block #2. You must do this if you use a different method for calculating EWT or if you are queuing to multiple skill groups.

Step 7 **Block #3:** Set up the parameters to be passed to CallbackEntry (VXML application).

Note This step assumes that you have already configured the CCE and expanded call variables not related to Courtesy Callback.

Variable values specific to Courtesy callback include:

ToExtVXML[0] = concatenate("application=CallbackEntry",";ewt=",Call.user.microapp.ToExtVXML[0])

ToExtVXML[1] = "qname=billing";

ToExtVXML[2] = "queueapp=BillingQueue;"

ToExtVXML[3] = concatenate("ani=",Call.CallingLineID,";");

Definitions related to these variables are:

- CallbackEntry is the name of the VXML Server application that is run.
- ewt is calculated in **Block #2**.
- qname is the name of the VXML Server queue into which the call is placed. There must be a unique qname for each unique resource pool queue.
- queueapp is the name of the VXML Server queuing application that is run for this queue.
- ani is the caller's calling Line Identifier.

Step 8 Verify that you have at least one available skill group to map to the skill group in the example script.

Step 9 Save the script, then associate the call type and schedule the script.

For information about scheduling scripts, 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/products-maintenance-guides-list.html.

Administration and Usage

Element Specifications for Courtesy Callback

The example IVR scripts provided for Courtesy Callback work as installed. To change how Courtesy Callback works, you can change the configuration of Courtesy Callback elements. This section lists the elements associated with Courtesy Callback and briefly describes the purpose of each one.

Callback_Add

The `Callback_Add` element is used to add a callback object to the database after all the callback information has been collected from the caller. In addition, it can be optionally configured to automatically delete old recorded files at specified intervals. These recorded files are the files produced by the Record element when the user records their name if they want a call back in the CallbackEntry application.

Callback_Disconnect_Caller

The `Callback_Disconnect_Caller` element is responsible for disconnecting the caller's leg of the call. The IP leg of the call for Unified CVP is preserved to hold the caller's *place in line* until the callback is made back to the caller.

Callback_Enter_Queue

The `Callback_Enter_Queue` element is responsible for adding a new caller to the queue. This element must be run for all callers even if the caller may not be offered a callback.

Callback_Get_Status

The `Callback_Get_Status` element is responsible for retrieving all information about the callback related to the current call (if a callback exists).

Callback_Reconnect

The `Callback_Reconnect` element is responsible for reconnecting the caller's leg of the call.

Callback_Set_Queue_Defaults

The `Callback_Set_Queue_Defaults` element is responsible for updating the DBServlet with the values that should be used for each queue. There is always a *default* queue type. The values are used whenever a queue type is encountered for which there are no explicitly defined values. For example, if an administrator has defined values for a *billing* and *default* queues, but the caller is queued for *mortgages*. In that case, the application uses the values from `Callback_Set_Queue_Defaults`.

Note When the DBServlet is not reachable to check the callback status for the duration of keepalive interval, the callback entry in the Reporting Server gets marked as a stale cached entry and subsequently gets cleared. As a result, a callback is not initiated.

Callback_Update_Status

The `Callback_Update_Status` element is responsible for updating the database after a callback disconnect or reconnect.

Callback_Validate

The `Callback_Validate` element is responsible for verifying whether or not a callback can be offered to the caller during this call. Depending on the outcome of the validation, the Validate element exits with one of four states.

Callback_Wait

The `Callback_Wait` element is responsible for *sleeping* the application for X seconds. The application hands control back to cvp_ccb_vxml.tcl with the parameter wait=X.

CHAPTER 7

Customer Virtual Assistant

Feature Overview

Customer Virtual Assistant (CVA) feature enables the IVR platform to integrate with cloud-based speech services. This feature supports human-like interactions that enable customers to resolve issues quickly and more efficiently within the IVR, thereby, reducing the calls directed towards agents.

Note The Dialogflow ES GCP project trial version should not be used in a production environment.

In a traditional IVR, customers can interact with the IVR in the following ways:

- **VVB Media Services-Based Interaction**: Prompts are played locally by VVB by downloading WAV files. User inputs are captured using DTMF grammar.
- **ASR-Based and TTS-Based Interactions**: Prompts are played by the external media server over MRCP Synthesis command for Text-to-Speech (TTS) functionality. The responses are recognized by external media server based on predefined grammar provided by Asynchronous Speech Recognition (ASR).

CVA-based IVR enables a new mechanism to leverage cloud-based-AI-enabled speech services. CVA provides the following speech services:

- **Text-to-Speech**: Integration with cloud-based TTS services in your application for Speech Synthesis operations. CVA currently supports Google Text to Speech service.
- **Speech-to-Text**: Integration with cloud-based ASR services in your application for Speech Recognition operations. CVA currently supports Google Speech to Text service.
- **Speech-to-Intent**: CVA provides capability of identifying the intent of customer utterances by processing the text received from Speech-to-Text operations. CVA offers this service by using cloud-based Natural Language Understanding (NLU) services. CVA currently supports Google Dialogflow service.

> **Note**
>
> - You can configure the Customer Virtual Assistant (CVA) feature of VVB 12.5(1) keeping the Unified CCE Controller in 12.0 version (as in multi-stage upgrade). However, in this case, the configuration user interface for CVA service account will not be available in the Unified CCE Administration. So, System Administrators can use the *Command Execution Pane* for such configurations.
>
>   For more information, see the *Command Execution Pane* section in 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/products-maintenance-guides-list.html.

Getting Started

This section explains the prerequisites and the documentation resources for CVA.

Prerequisites

- CVP 12.5(1) and VVB 12.5(1).
- CVP/VVB configuration:
  - Enable access to cloud-based services from CVP and VVB directly or via proxy.

    For details, see the *Cisco Unified Customer Voice Portal > Operations Console (NOAMP) > Integration > Cloud Connect > Configure CVP or VVB Devices for Cloud Connect* section in the *Administration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html.
  - Synchronize the date/time in CVP, VVB, and proxy with a common NTP server.
  - Configure access to DNS server in CVP/VVB.

  For more information on NTP and DNS server configurations in CVP, refer to the Microsoft Windows platform documentation.

  For more information on NTP and DNS server configurations in VVB, refer to the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.
- Non-OEM users must enable speech services and generate JSON key. To know more about enabling speech services, see Enable Speech Services (For Non-OEM Users), on page 67. To know more about generating JSON key, see Generate JSON Key (for Non-OEM Users), on page 67.
- OEM users must provision Google Contact Center AI (CCAI) for Cisco Contact Center Enterprise. To know more about provisioning Google CCAI, see Provision Google CCAI with Unified Contact Center Enterprise (for OEM Users), on page 67.

Enable Speech Services (For Non-OEM Users)

To enable speech services, follow these steps:

1. Log in to your Dialogflow account at https://dialogflow.cloud.google.com/.
2. Scroll down on the homepage and click **Project ID** of your Dialogflow agent.

   This takes you to the Google Cloud Platform (GCP) homepage.
3. Select **APIs & Services** from the left pane (through the hamburger menu).
4. Select the API services (such as Cloud Text-to-Speech, Cloud Speech-to-Text, and Dialogflow) to be enabled.
5. Click **Enable** to enable the selected API for the given Project ID.

Generate JSON Key (for Non-OEM Users)

To generate the JSON key, follow these steps:

1. In the GCP homepage, select **IAM & Admin** from the left pane (through the hamburger menu).
2. Select **Service accounts** which shows the list of your enabled services.
3. Select the service for which the JSON key is to be generated.
4. Click the ellipsis menu on the right and click **+Create Key**.
5. Select JSON as **Key type** and then click **Create**.

   The key is downloaded.

For best results:

- Migrate your Dialogflow Agent to Enterprise Essential (**Console Left Bar** > **Migrate from Standard to Enterprise Essential**).
- Enable the enhanced Speech Model in Dialogflow console (**Settings** > **Speech** > **Enable Enhanced Speech Model and Data Logging**).

If this option is enabled, speech recognition data is shared with Google. For more information see https://cloud.google.com/speech-to-text/docs/enhanced-models.

Provision Google CCAI with Unified Contact Center Enterprise (for OEM Users)

To provision Google CCAI with Cisco Unified Contact Center Enterprise, follow these steps:

Procedure

Step 1 Log in to the Cisco Commerce Workspace (CCW) portal https://apps.cisco.com/Commerce/ using your Cisco ID and place the order for Google CCAI.

Step 2 Complete the CCAI provisioning form and submit to get a CCAI account with Cisco.

Note When the CCAI provisioning request is approved, an email (*CCAI Onboarding Provision Status Update*) is triggered to the user. This email includes the account details and the *CCAI Provisioning Document* which explains the steps to configure the CCAI account and services.

Step 3 Configure the CCAI account and integrate the CCAI services with the Contact Center application by following the *CCAI Provisioning Document*. For any further assistance, contact the Cisco CCAI onboarding team or send an email to: cisco-ccai-onboarding@cisco.com.

The service account provided by Cisco allows the CCAI customers to leverage the following APIs to integrate with the Contact Center applications:

- Dialogflow API
- Text-to-Speech API
- Speech-to-Text API

Documentation Resources

The following table lists the reference documents for CVA.

Information	Resource
Sample CVA Application	See https://github.com/CiscoDevNet/cvp-sample-code/tree/master/CustomerVirtualAssistant.
Design Considerations	*Design Considerations for Integrated Features > Customer Virtual Assistant Considerations* section in *Solution Design Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html.
CVA configuration in PCCE Deployment	*Customer Virtual Assistant* section in *PCCE Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.
TTS Prompt Cache Management and proxy setting for Speech Server	*VVB Operations Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/virtualized-voice-browser/products-maintenance-guides-list.html.
Proxy settings for VXML Server	See the *VXML Server Configuration > Proxy Settings in VXML Server for Customer Virtual Assistant* section in *CVP Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html.
Configuration of Call Studio elements for CVA	The following chapters in *CVP Element Specification Guide* at https://www.cisco.com/c/en/us/support/

Information	Resource
	customer-collaboration/unified-customer-voice-portal/products-programming-reference-guides-list.html: • *Dialogflow Element* • *DialogflowIntent Element* • *DialogflowParam Element* • *Transcribe Element*
CVA Speech Configuration APIs	See *CVA Speech Configuration* section in *VVB Developer Guide* at https://developer.cisco.com/site/customer-voice-portal/documents/virtual-voice-browser/.

Feature Overview

Customer Virtual Assistant (CVA) feature enables the IVR platform to integrate with cloud-based speech services. This feature supports human-like interactions that enable customers to resolve issues quickly and more efficiently within the IVR, thereby, reducing the calls directed towards agents.

Note The Dialogflow ES GCP project trial version should not be used in a production environment.

In a traditional IVR, customers can interact with the IVR in the following ways:

- **VVB Media Services-Based Interaction**: Prompts are played locally by VVB by downloading WAV files. User inputs are captured using DTMF grammar.
- **ASR-Based and TTS-Based Interactions**: Prompts are played by the external media server over MRCP Synthesis command for Text-to-Speech (TTS) functionality. The responses are recognized by external media server based on predefined grammar provided by Asynchronous Speech Recognition (ASR).

CVA-based IVR enables a new mechanism to leverage cloud-based-AI-enabled speech services. CVA provides the following speech services:

- **Text-to-Speech**: Integration with cloud-based TTS services in your application for Speech Synthesis operations. CVA currently supports Google Text to Speech service.
- **Speech-to-Text**: Integration with cloud-based ASR services in your application for Speech Recognition operations. CVA currently supports Google Speech to Text service.
- **Speech-to-Intent**: CVA provides capability of identifying the intent of customer utterances by processing the text received from Speech-to-Text operations. CVA offers this service by using cloud-based Natural Language Understanding (NLU) services. CVA currently supports Google Dialogflow service.

Note

- You can configure the Customer Virtual Assistant (CVA) feature of VVB 12.5(1) keeping the Unified CCE Controller in 12.0 version (as in multi-stage upgrade). However, in this case, the configuration user interface for CVA service account will not be available in the Unified CCE Administration. So, System Administrators can use the *Command Execution Pane* for such configurations.

  For more information, see the *Command Execution Pane* section in 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/products-maintenance-guides-list.html.

Getting Started

This section explains the prerequisites and the documentation resources for CVA.

Prerequisites

- CVP 12.5(1) and VVB 12.5(1).
- CVP/VVB configuration:
  - Enable access to cloud-based services from CVP and VVB directly or via proxy.

    For details, see the *Cisco Unified Customer Voice Portal > Operations Console (NOAMP) > Integration > Cloud Connect > Configure CVP or VVB Devices for Cloud Connect* section in the *Administration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html.
  - Synchronize the date/time in CVP, VVB, and proxy with a common NTP server.
  - Configure access to DNS server in CVP/VVB.

  For more information on NTP and DNS server configurations in CVP, refer to the Microsoft Windows platform documentation.

  For more information on NTP and DNS server configurations in VVB, refer to the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.
- Non-OEM users must enable speech services and generate JSON key. To know more about enabling speech services, see Enable Speech Services (For Non-OEM Users), on page 67. To know more about generating JSON key, see Generate JSON Key (for Non-OEM Users), on page 67.
- OEM users must provision Google Contact Center AI (CCAI) for Cisco Contact Center Enterprise. To know more about provisioning Google CCAI, see Provision Google CCAI with Unified Contact Center Enterprise (for OEM Users), on page 67.

Documentation Resources

The following table lists the reference documents for CVA.

Information	Resource
Sample CVA Application	See https://github.com/CiscoDevNet/cvp-sample-code/tree/master/CustomerVirtualAssistant.
Design Considerations	*Design Considerations for Integrated Features > Customer Virtual Assistant Considerations* section in *Solution Design Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html.
CVA configuration in PCCE Deployment	*Customer Virtual Assistant* section in *PCCE Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.
TTS Prompt Cache Management and proxy setting for Speech Server	*VVB Operations Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/virtualized-voice-browser/products-maintenance-guides-list.html.
Proxy settings for VXML Server	See the *VXML Server Configuration > Proxy Settings in VXML Server for Customer Virtual Assistant* section in *CVP Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html.
Configuration of Call Studio elements for CVA	The following chapters in *CVP Element Specification Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-programming-reference-guides-list.html: • *Dialogflow Element* • *DialogflowIntent Element* • *DialogflowParam Element* • *Transcribe Element*
CVA Speech Configuration APIs	See *CVA Speech Configuration* section in *VVB Developer Guide* at https://developer.cisco.com/site/customer-voice-portal/documents/virtual-voice-browser/.

CHAPTER 8

Media Server

About Media Server

Many of the optional features in Packaged CCE require a Cisco Unified Customer Voice Portal (CVP) media server to store and serve supporting `.wav` files. This chapter describes how to set up a CVP media server. It also describes expanded call variable settings that are related to the media server and requirements for accessing a media server in call routing scripts.

The features that require a CVP media server include Agent Greeting, Courtesy Callback, Post-Call Survey, and Whisper Announcement.

Prepare a Media Server

A media server is installed by default on each of the CVP servers in a Packaged CCE deployment.

Procedure

Step 1 Ensure that IIS is properly configured and running on the server. It must be listening on port 80. To validate proper configuration of the media server, launch a browser from a remote machine that is able to ping the CVP server and attempt to access and play one of the default media files installed during the CVP installation such as **http://<cvp_ip>/en-us/app/en_1.wav**. If the file is accessible, the media server is installed correctly.

Note Use Microsoft IIS with Unified CVP. This component is automatically installed as part of the CVP server package installation.

Step 2 Ensure the server is accessible to CVP, Unified CCE, and your agent desktops.

Step 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, and specify to start immediately.
k) On the FTP SSL Settings, select **Allow SSL Connections**.
l) On the **Authentication and Authorization** section select the type of authentication required. If using basic, note the name and password of the account.
m) Select the authorization; for anonymous select **Anonymous users**.
n) Set the read and write permissions.

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

Step 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.

Step 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 expanded call variable **call.user.microapp.ToExtVXML** to send the ftpPath parameter to the recording application. Make sure the expanded call variable length is long enough, or it may get truncated and fail.

Step 6 To allow 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, configure a cache expiration value in IIS Manager. 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.

To configure a cache expiration value in IIS Manager:

a) Find the site you are using, go to the agent greeting folder you created (ag_gr), and then select **HTTP Response Headers**.
b) Click **Set Common Headers** on Actions panel.
c) Select **Expire Web Content** and set the desired value.

What to do next

- 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. Reset the gateway to clear the cache.

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 VXML Gateway is 30 seconds.

- Add Media Servers in the **Unified CCE Administration** > **Infrastructure** > **Inventory** page. For more information, 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/products-maintenance-guides-list.html.

Reference a Media Server in CCE Scripts

Specify Media Server in Routing Scripts

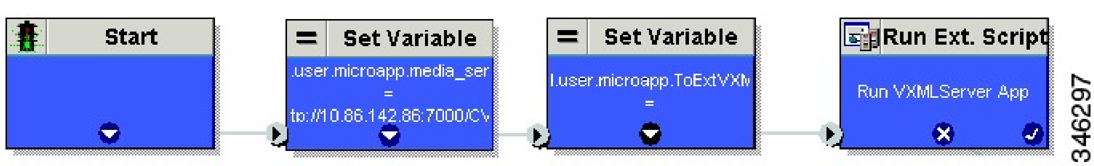
When you configure media servers in CVP, you can specify a default media server. The benefit to specifying a default media server is that your scripts do not need a Set Variable node to access the default media server. For this to work, you must make sure that the files a script requests are stored on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

See the following example.



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`. The physical location of the default storage directory is `c:\inetpub\wwwroot\en-us\app`. To take advantage of this, Packaged 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 Unified CCE Administration, navigate to **Overview** > **Call Settings** > **Route Settings** > **Expanded Call Variables**.

CHAPTER 9

Mobile Agent

Capabilities

Cisco Unified Mobile Agent Description

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 Packaged 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.

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 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.

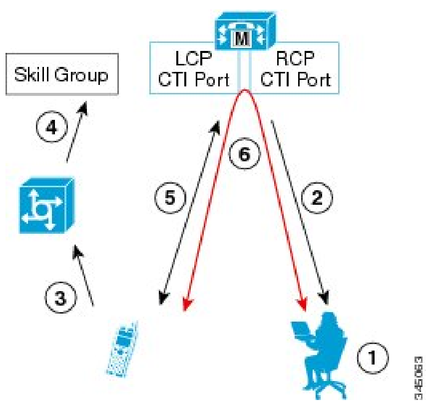
Note To configure Mobile Agent in call by call delivery mode, you must set the wrap-up timer to at least one second using the Agent Desktop Settings List tool in the Configuration Manager.

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.

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 6: Nailed Connection Call Flow



The nailed connection call flow works as follows:

1. At login, the agent enters the directory number of the local CTI port (LCP) and the remote phone number in the Desktop.

   The remote phone number can be any phone number reachable by Unified CM.

   When the agent clicks the Login button, a call is initiated to the agent's remote CTI port (RCP) and the agent's remote phone rings.

2. When the agent answers the call, the call is then *nailed up*. This means that the agent will remain on this call until the agent logs out or ends the call.

3. A customer's call arrives in the system and, through Packaged CCE configuration and scripting, is queued for a skill group/precision queue. (This is no different than existing processing for local agents.)

4. When the agent clicks the Answer button, the voice path between the agent and the customer phone is established, and the two parties can talk.

5. When the system assigns an agent to the call, the call is routed to the agent's LCP port. The agent then hears the connect tone on the headset.

6. When the call ends, the customer connection is terminated and the agent state returns 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.

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 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 93

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.

- 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 ends the call 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.

For more information about Agent Greeting, see Capabilities, on page 7.

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

Phone Requirements

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

> **Note** When Unified Mobile Agent phones are located on a cluster and a SIP Trunk is used to connect the cluster to another cluster under Packaged CCE control, you must either use SIP phones as Mobile Agent phones or select **mtp required** on the Packaged CCE cluster to allow Mobile Agent calls to work.

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 88.

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.
- Packaged CCE intercepts the call arriving on the CTI Port and directs Unified CM to connect the call to the Mobile Agent.

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 Packaged CCE application. The ports are recognized by Packaged CCE 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.

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

- For the total number of supported Unified Mobile Agents and more information about Unified Mobile Agent capability, see *Solution Design Guide for Cisco Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html.
- Because Unified Mobile Agent adds processing steps to Unified CCE 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 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 makes these connections.

Codec

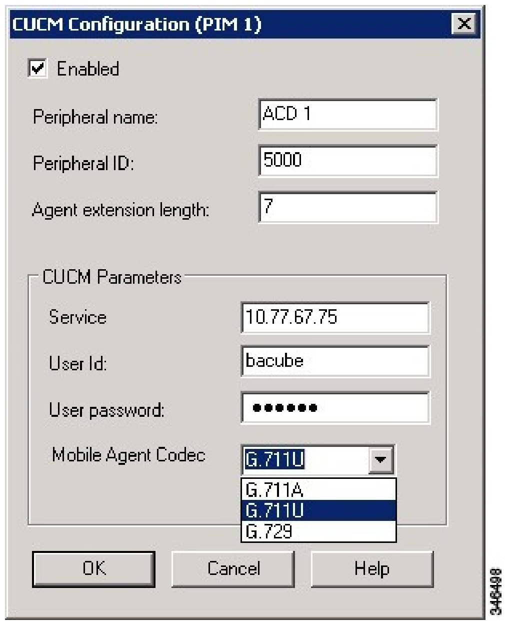
The codec settings on the Peripheral Gateway and Voice Gateway must match. Perform the following procedure:

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 7: Mobile Agent Codec Selection



Unsupported Features

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

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

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.

> **Note** The service level for Unified Mobile Agent calls might be different than the service level for 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 Packaged CCE 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.

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 84
Configure Unified CM Call Duration Timer	Maximum Call Duration Timer configuration, on page 87
Configure Agent Desk Settings	Agent Desk Setting Configuration for Unified Mobile Agent, on page 87
Configure Media Termination Points	Media Termination Points Configuration, on page 88

Unified CM CTI Port Configuration and Mapping for Unified Mobile Agent

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.

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. 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. You must disable the hold tone.

Perform the following steps to disable the hold tone:

1. Log in to Unified CM Administration and navigate to **System > Service Parameters**.
2. Scroll down to the **Tone on Hold Time** field and set the value to **0**.
3. Click **Save**.

Note Because Tone on Hold Time is a cluster-wide setting, it will be applied to all nodes, not just the currently selected node.

Configure Unified CM CTI Ports 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 name; click **OK** when finished.

Using the naming convention format LCP*yyyy*:

- LCP identifies the CTI Port as a local device.
- *yyyy* is the local CTI Port.

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 where you want to assign the network CTI port. Do not select Default. (The device pool defines sets of common characteristics for devices.)

Step 8 For Device Security Profile, select **Cisco CTI Port - Standard SCCP Non-Secure Profile**.

Step 9 Click **Save**.

Step 10 Click **Apply config**.

Step 11 In the Association section, select **Add a New DN**.

Step 12 Add a unique directory number for the CTI port you just created.

Step 13 In Maximum Number of Calls, enter **2**.

Step 14 In Busy Trigger, enter **1**.

Step 15 When finished, click **Save**, and click **Apply config**.

Step 16 Repeat the preceding steps to configure the network CTI port.

In Device Name, using the naming convention format RCP*yyyy*, 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.
- *yyyy* is the network CTI port.

The name RCP0000 represents the local port.

Note The port number for both LCP and RCP must be the same even though the directory numbers are different.

Step 17 In Description, enter text that identifies the network CTI port.

Step 18 Use the **Device Pool** drop-down list to choose where you want to assign the network CTI port. Do not select Default.. (The device pool defines sets of common characteristics for devices.)

Step 19 Click **Save**.

Step 20 In the Association Information section, select **Add a New DN**.

Step 21 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 22 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**.

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 Unified Mobile Agent will be logged in *longer than* 12 hours, use the following instructions to either one of the following:

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

If your Mobile Agent deployment uses intercluster trunks between your CTI ports and your mobile agent's phone, you must set these service parameters on both the local and remote 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 **Cisco CallManager Service**.

The **Service Parameters Configuration** page appears.

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

Step 5 Click **Save**.

Agent Desk Setting Configuration for Unified Mobile Agent

You can configure Agent Desk Settings through the PCCE Administration tool.

Configure Desk Settings with Unified CCE Administration

This section describes how to configure Desk Settings in Unified CCE Administration to accommodate Unified Mobile Agent features.

The following procedure describes how to configure one desk setting. Repeat this process for each different desk setting in your deployment.

Procedure

Step 1 In Unified CCE Administration, choose **Overview** > **Desktop Settings** > **Desk Settings**.

Step 2 Click **New** to create a new desk setting or click the name of an existing desk setting to edit it.

Step 3 Complete the required fields.

Step 4 From the Mobile Agent drop-down list, select one of the following options:

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

Step 5 Click **Save**.

Associate Desk Setting with a Mobile Agent

After you have configured agent desk settings, you need to associate the desk setting with a mobile agent.

Procedure

Step 1 Access Unified CCE Administration.

Step 2 Select **Overview** > **User Setup** > **Agents**.

The List of Agents window appears.

Step 3 Select the agent that you want to associate.

The Edit <agent> window appears.

Step 4 In the Desk Settings box, select the desk setting that has the Mobile Agent enabled.

Step 5 Click **Save**.

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 thcce-in10360-01-pcceucceipv6support-1101em. 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.

The following table lists the steps in configuring MTPs in Unified CM. Make sure you have completed the tasks in the checklist.

Table 7: Checklist for Unified CM SIP Trunk Configuration

Check when done	Task
	Add MTP resources to Unified CM, on page 90

Check when done	Task
	Configure MTP resources in Unified CM , on page 90
	Associate a Media Resource Group List with Device Pools, on page 91
	Quarantine Unified CM software-based resources, on page 91
	Configure MTPs with SIP Trunks, on page 91
	Enable Call Progress Tones for Agent-Initiated Calls, on page 92
	Verify MTP Resource Utilization, on page 92

Add MTP resources to Unified CM

Perform these steps to add 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 configuration 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 that 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 Cisco Call Manager server group you configured on each of your gateways.

Configure MTP resources in Unified CM

The following 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 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 a Media Resource Group List with Device Pools

The following procedure shows how to associate a media resource group list (MRGL) 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.

Configure MTPs with SIP Trunks

If you use SIP trunks, you must configure MTPs. 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.

At a minimum all trunks whose destination is unified CVP need to have this configuration. This requirement also applies to all TDM trunks that are used to connect to Mobile Agent phones through service providers.

Step 3 Depending on the scenario listed below, perform the corresponding step. Note that if you configure trunk groups to dynamically insert MTPs, only the calls that require MTPs use them.

- Insert MTPs for inbound and outbound calls through a given trunk: In the Trunk Configuration settings, check the **Media Termination Point Required** check box.
- Dynamically allocate MTPs when Cisco Unified Intelligent Contact Management detects media or signaling incompatibility between the caller and called endpoints: In the Trunk Group Configuration settings, for the DTMF Signaling Method, select **RFC2833**.

Enable Call Progress Tones for Agent-Initiated Calls

For an agent to hear call progress tones for agent-initiated calls, additional configuration is required if **MTP Required** is not enabled. If instead you have dynamic MTP allocation by forcing mismatched DTMF settings, then you should configure the Unified CM to enable Early Offer.

For information on configuring the Unified CM, see the Unified CM product documentation at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html. Ringback and other call progress tones are not generated by the Cisco Annunciator, as is the case for regular phones and softphones. Instead, Mobile Agent relies on these tones being generated by the called party (and the Early Offer setting triggers these tones to be sent to the agent).

Note This selection does not affect MTP sizing for IP phones and other endpoints that support RFC 2833 signaling, as is the case for many Cisco phones (including the 6900 series and the 794x and 796x phones).

Verify MTP Resource Utilization

Because Unified CM comes preconfigured with software MTP resources, these resources may sometimes be used to provide MTP for Unified Mobile Agent calls without proper configuration. Cisco does not support the use of Unified CM-based software MTPs. You can quarantine the Unified CM-based MTPs. (See Quarantine Unified CM software-based resources, on page 91.) To ensure that the IOS-based MTPs are being used for Unified Mobile Agents, perform the following verification steps:

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 nodes 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 only the IOS-based resources are active during the Mobile Agent phone call. Also, ensure that all Unified UC-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 Packaged 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 following URL in your browser: 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*>:8445/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.

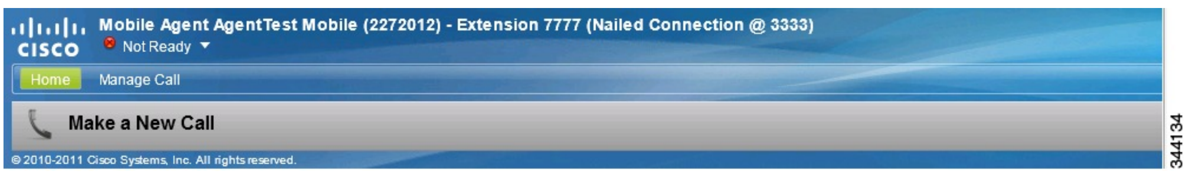
In Call by Call mode, the dial number provided is not verified. To ensure that the number is correct, verify the number in the header on the Agent Desktop after sign-in is complete.

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 21.

CHAPTER 10

Outbound Option

Capabilities

Features

Outbound Option enables call centers to manage outbound calls. With Outbound Option, you can configure a contact center to automatically dial customer contacts from imported lists and direct a call to an available agent. This application transfers a call to an agent only if a live contact is reached.

A summary of major features in Outbound Option follows:

Automated dialing

The dialer automatically dials contact numbers, screens for busy signals, no answers, and answering machines, and transfers calls to agents. The dialer transfers a call to an available agent only when it reaches a live contact.

Campaigns

Users create calling campaigns using a set of tabs in a graphical user interface (GUI). A campaign is a set of numbers that will be automatically dialed and a set of agents who will talk to contacted customers.

More specifically, a campaign consists of imported contact lists and agent skill groups.

Imported contact lists and Do Not Call lists

You can import lists of customers you want to call and lists of customers who you do not want to call. You can configure Outbound Option to import both types of lists either by continuously polling or at scheduled intervals. You can also specify whether imported lists will replace existing lists or be appended to them.

Agent skill groups

You assign agents to campaigns by using skill groups. A skill group defines a set of agents with specific capabilities, such as language skills, product knowledge, or training that is associated with a campaign. Agents might belong to multiple skill groups and thus be part of multiple campaigns.

Campaign management

Outbound Option uses a dialing list that is associated with a campaign and directs dialers to place calls to customers. The dialer then directs contacted customers to agents.

Choice of dialing modes

Outbound Option supports the following dialing modes:

- Preview mode lets the agent preview the contact information on the desktop and decide whether the SIP dialer should dial a contact.
- Direct Preview mode is similar to Preview mode; however, the dialer places the calls from the agent's phone. This mode prevents abandoned calls and false positive detection of answering machines.
- Progressive mode dials a configured number of calls per available agent.
- Predictive mode adjusts the number of calls dialed per agent based on the current abandon rate.

Callbacks

If a customer requests a callback for a later date and time, the agent can enter the request in the system, and the dialer schedules the call appropriately. The following callback types are supported:

- Personal callbacks specify that the customer receive a callback from the same agent who made the initial contact.
- Regular callbacks are handled by any available agent.

Call analysis

The Call Progress Analysis (CPA) feature uses a combination of call signaling and media stream analysis to identify different types of calls, such as faxes and modems, answering machines, and operator intercepts.

Sequential dialing

The sequential dialing feature allows up to ten phone numbers per customer record.

Abandoned and retry calls

You can configure campaigns to retry abandoned calls.

Campaign prefix digits for dialed numbers

You can configure a prefix for customer number, which can be used to identify specific campaigns.

Activity reports

Outbound Option reporting features include agent, campaign, dialer, and skill groups report templates.

Two-Way Replication

If you choose to enable Outbound Option, you can also enable Outbound Option High Availability. Outbound Option High Availability supports two-way replication between the Outbound Option database on Logger Side A and the Outbound Option database on Logger Side B.

Outbound API

Outbound API allows you to use REST APIs to create, modify, and delete Outbound Option campaigns.

Outbound API provides a streamlined mechanism for creating campaigns with a single preconfigured query rule and import rule.

Administrative scripts are not required for Outbound Option campaigns created with the Outbound API. If an administrative script is provided, the information in the script overrides the information defined in the API.

Outbound API consists of the following APIs:

- Outbound Campaign API: Use this API to define new Outbound Option campaigns, and to view, edit, or delete existing campaigns. You can also use this API to disable all campaigns at once (emergency stop).
- Do Not Call API: Use this API to set the Do Not Call (DNC) import rule configuration for Outbound Option. This prevents the Dialer from dialing the numbers on the DNC list.
- Import API: Use this API to import customer contact information for an Outbound Option campaign.
- Time Zone API: Use this API to list all available time zones and to get information for a specified time zone. You also use this API with the Outbound Campaign API to set the default time zone for an Outbound Option campaign.
- Campaign Status API: Use this API to get the real-time status of running Outbound Option campaigns.
- Personal Callback (PCB) API: Use this API to configure your Outbound Option campaign to handle personal callbacks. You can create personal callback records individually or in bulk. You can also use this API to update or delete personal callback records.

For more information about Outbound API, see the *Cisco Packaged Contact Center Enterprise Developer Reference Guide* at https://developer.cisco.com/site/packaged-contact-center/documentation/.

Dialing Modes

Outbound Option supports various dialing modes, described in the following sections.

Note All dialing modes reserve an agent at the beginning of every Outbound Option call cycle by sending a reservation call to the agent.

Predictive Dialing

In predictive dialing, the dialer determines the number of customers to dial per agent based on the number of lines available per agent and the configured maximum abandon rate. The agent must take the call if that agent is logged in to a campaign skill group.

A Predictive Dialer is designed to increase the resource utilization in a call center. It is designed to dial several customers per agent. After reaching a live contact, the Predictive Dialer transfers the customer to a live agent along with a screen pop to the agent's desktop. The Predictive Dialer determines the number of lines to dial per available agent based on the target abandoned percentage.

Outbound Option predictive dialing works by keeping outbound dialing at a level where the abandon rate is below the maximum allowed abandon rate. Each campaign is configured with a maximum allowed abandon rate. In Predictive mode, the dialer continuously increments the number of lines it dials per agent until the abandon rate approaches the configured maximum abandon rate. The dialer lowers the lines per agent until the abandon rate goes below the configured maximum. In this way, the dialer stays just below the configured maximum abandon rate. Under ideal circumstances, the dialer internally targets an abandon rate of 85% of the configured maximum abandon rate. Due to the random nature of outbound dialing, the actual attainable abandon rate at any point in time may vary for your dialer.

Preview Dialing

Preview dialing reserves an agent before initiating an outbound call and presents the agent with a popup window. The agent can then Accept or Reject the call with the following results:

- **Accept**: The customer is dialed and transferred to the agent.
- **Reject**: The agent is released. The system then delivers another call to the agent, either another Preview outbound call, or a new inbound call.
- **Rejects-Close**: The agent is released and the record is closed so it is not called again. The system then delivers another call to the agent, either another Preview outbound call or a new inbound call.

Direct Preview Dialing

The Direct Preview mode is similar to the Preview mode, except that the dialer automatically places the call from the agent's phone after the agent accepts. Because the call is initiated from the agent's phone, the agent hears the ringing, and there is no delay when the customer answers. However, in this mode, the agent must deal with answering machines and other results that the Dialer Call Progress Analysis (CPA) handles for other campaign dialing modes.

Note

- A *zip tone* is a tone that announces incoming calls. There is no zip tone in Direct Preview mode.
- If you select *personal callback* as the callback option for a Direct Preview mode campaign, a *personal callback* is dialed in Preview mode. The *personal callback* is processed like a call in the Preview mode.

Progressive Dialing

Progressive Dialing is similar to predictive dialing (see Predictive Dialing, on page 99). The only difference is that in Progressive Dialing mode, Outbound Option does not calculate the number of lines to dial per agent, but allows users to configure a fixed number of lines that will always be dialed per available agent.

Note In the Outbound dialer log, the Progressive dialing mode is also logged as Predictive.

Initial Setup and Maintenance

This section is intended for system administrators who install and configure Packaged CCE. It describes the one-time tasks required to set up Outbound Option. It also discusses occasional upgrade and maintenance tasks. It contains the following topics:

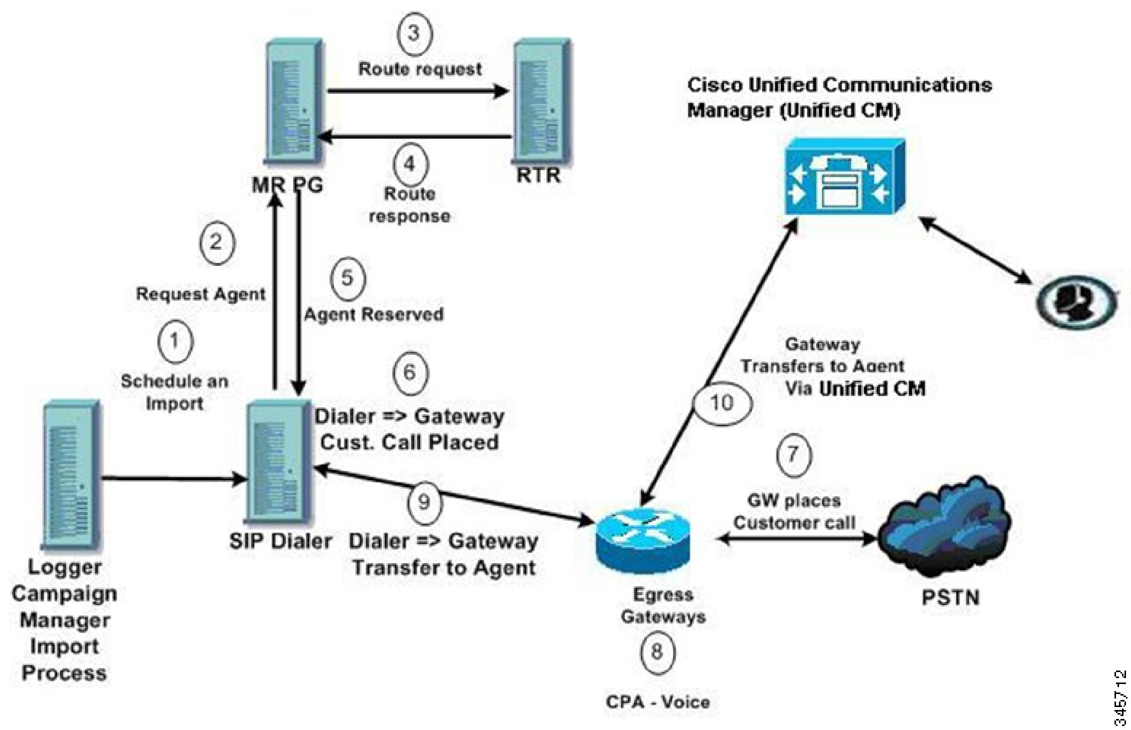
• Unified Communications Manager and Gateway Configuration, on page 104
• Outbound Option Software Installation Steps, on page 111
• Maintenance Considerations, on page 119

Outbound SIP Dialer Call Flows

Call Flow Diagram for Packaged CCE

This figure illustrates a transfer to agent call flow for a SIP dialer Outbound Option campaign.

Figure 8: SIP Dialer Agent Campaign Call Flow



The call flow works as follows:

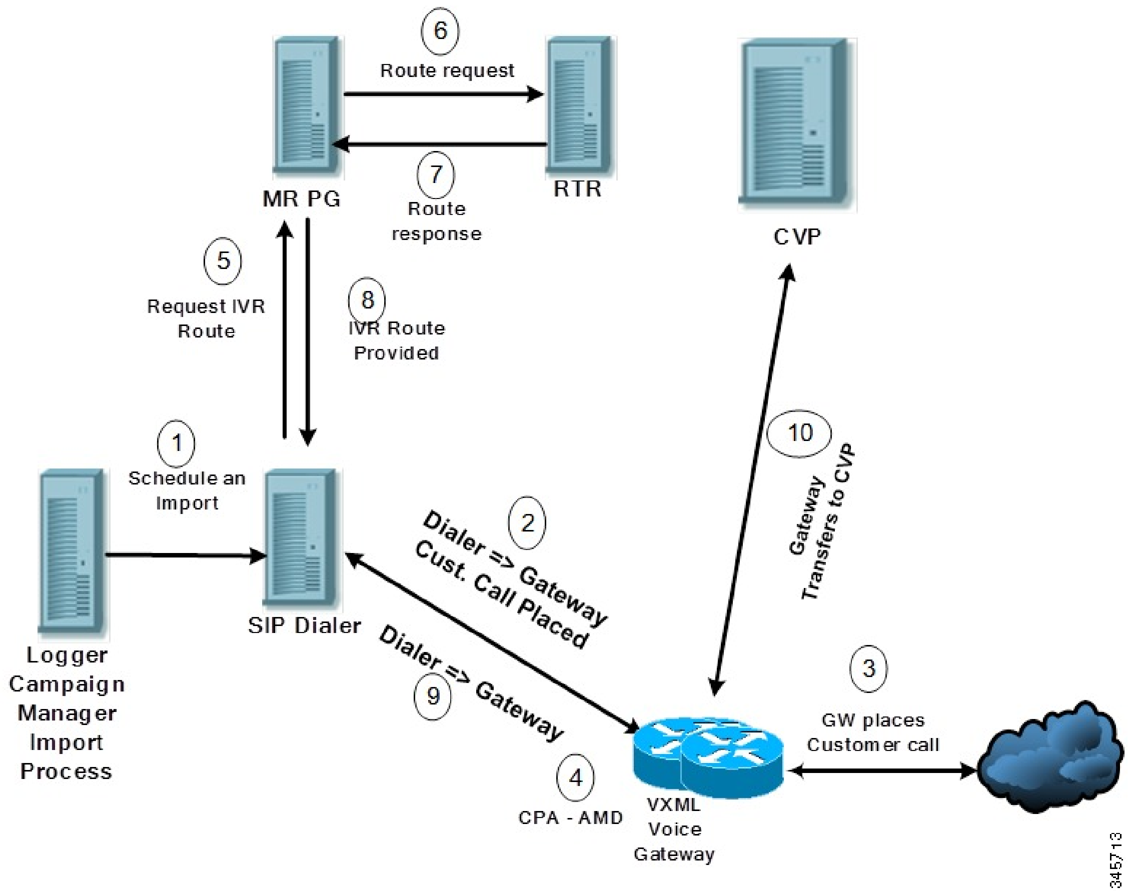
1. You schedule the import and the campaign starts. Records are delivered to the dialer.
2. The dialer looks for an available agent through the media routing interface.
3. The media routing peripheral gateway (MR PG) forwards the request to the router.
4. The routing script identifies an agent and responds to the MR PG.
5. The MR peripheral interface manager (PIM) notifies the dialer that the agent is reserved.
6. The dialer signals the gateway to call the customer.
7. The gateway calls the customer and notifies the dialer of the attempted call.

8. Call Progress Analysis (CPA) is done at the gateway. When voice is detected, the gateway notifies the dialer.
9. The dialer directs the voice gateway to transfer the call to the reserved agent by the agent extension.
10. The gateway directs the call to the agent through Unified Communications Manager (using dial peer configuration to locate the Unified Communications Manager). Media are set up between the gateway and the agent's phone.

Unattended VRU Call Flow Diagram for Packaged CCE

This figure illustrates a transfer-to-VRU call flow for a SIP dialer Outbound Option campaign.

Figure 9: SIP Dialer Unattended IVR Campaign Call Flow



The call flow works as follows:

1. An unattended VRU campaign starts and schedules an import. Records are delivered to the dialer.
2. The dialer sends a SIP INVITE to the voice gateway to call a customer.
3. The gateway calls the customer.
4. Call Progress Analysis (CPA) detects an answering machine (AMD) and notifies the dialer.
5. The dialer sends a VRU route request to the MR PG.

6. The MR PG forwards the route request to the router which invokes the routing script.
7. The router sends the route response with the network VRU label to the MR PG.
8. The MR PG forwards the route response to the dialer.
9. The dialer sends a SIP REFER request for the label to the voice gateway.
10. The voice gateway transfers the call to Unified CVP.

Unified CVP then takes control of the call.

Unified CCE Configuration for Outbound Option

This section provides procedures for configuring Unified CCE for Outbound Option.

Configure the Dialer Component

You deploy the Dialer as a single redundant pair for each Agent PG with agents who handle Outbound Option calls.

Procedure

Step 1 Make sure that all Packaged CCE services are running.

Step 2 In the **Unified CCE Configuration Manager**, expand **Outbound Option Option** and double-click **Dialer** to display the **Outbound Option Option Dialer configuration** window.

Step 3 Click **Retrieve**.

Step 4 Click **Add** to add a new dialer.

Step 5 Enter the required information on the **Dialer General Tab**. See the *Configuration Manager Online Help* for details of these fields.

Step 6 Click **Save**.

Step 7 Select the **Port Map Selection** tab to display the port map configuration. See the *Configuration Manager Online Help* for details of configuring these mappings.

Step 8 Click **Add**

Step 9 Configure a set of ports and their associated extensions.

A Dialer can support 3000 ports. The allowed **Telephony Port** range is from 0 to 2999.

Step 10 Click **OK**. The port mappings appear on the **Port Map Selection** tab.

Step 11 Click **Save** to save all the configuration information.

Configure System Options

Procedure

Step 1 In **Unified CCE Administration**, choose **Organization** > **Campaigns** to open the Campaigns page.

Step 2 Define the dialing time range to use for all your Outbound Option campaigns.

For more information on campaign configuration, refer the **Manage Campaigns** section in 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/products-maintenance-guides-list.html.

Enable Expanded Call Context Variables

Perform the following steps to enable the expanded call context variables.

Procedure

Step 1 In **Unified CCE Administration**, click **Overview** > **Call Settings** > **Route Settings** > **Expanded Call Variables**.

Step 2 Enable all BAxxxx variables (BAAccountNumber, BABuddyName, BACampaign, BADialedListID, BAResponse, BAStatus, and BATimezone).

What to do next

By default, the solution includes the predefined BAxxxx ECC variables in the "Default" ECC payload. You can also create a custom ECC payload for your Outbound Option call flows. Always remember that you cannot use an ECC variable unless it exists in one of the ECC payloads that you use for a call flow.

Packet Capture for Troubleshooting

For the SIP Dialer to capture data, ensure that the dialer on the Unified CCE PG machine uses the active interface from the Ethernet Interface list. You can determine the active interface with a network protocol analyzer tool such as Wireshark, which you can download from www.wireshark.org. The interface with network packets is the active interface.

You can change the SIP Dialer packet capture parameters to use the active interface from the Windows Registry Editor. Change the interface name option (-i) in the `CaptureOptions` key to the number of the active interface. For example, to use the third interface, set the value for -i to `-i 3`.

Capture files are in the `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\`<*customer instance*>`\Dialer` registry key location.

Unified Communications Manager and Gateway Configuration

In the next phase of Outbound Option installation, you set up Unified Communications Manager and its related gateway.

The following table lists the steps that comprise Unified CM setup.

Table 8: Unified CM Configuration Steps for Deployments with SIP Dialer

Step Number	Procedure
1	Disable Ringback During Transfer to Agent for SIP, on page 105

Step Number	Procedure
2	Configuration of Voice Gateways, on page 107
3	Configure SIP Trunks, on page 110

Disable Ringback During Transfer to Agent for SIP

The voice gateway generates a ringback tone to the customer. To prevent the gateway from generating a ringback, apply a SIP normalization script to the Unified Communications Manager SIP trunk.

Apply this SIP normalization script only to the SIP trunk that handles the inbound call from the voice gateway for agent transfer.

- If your deployment uses the same gateway for both PSTN calls and the dialer, complete all steps, 1 to 13, to create a dedicated SIP trunk and apply the normalization script.

Note The trunk for PSTN calls still needs a 180 RINGING SIP message for inbound calls to trigger the gateway to play ringback to the PSTN.

For more information, see the TechNote *Disable Ringback During Transfer to Agent for SIP* at https://www.cisco.com/c/en/us/support/docs/customer-collaboration/packaged-contact-center-enterprise/200323-Cisco-Packaged-Contact-Center-Enterprise.html.

- If your deployment has a dedicated SIP trunk to handle the agent transfer dialer, complete steps 1 to 2 and 8 to 13 to apply the normalization script to your SIP trunk.

Procedure

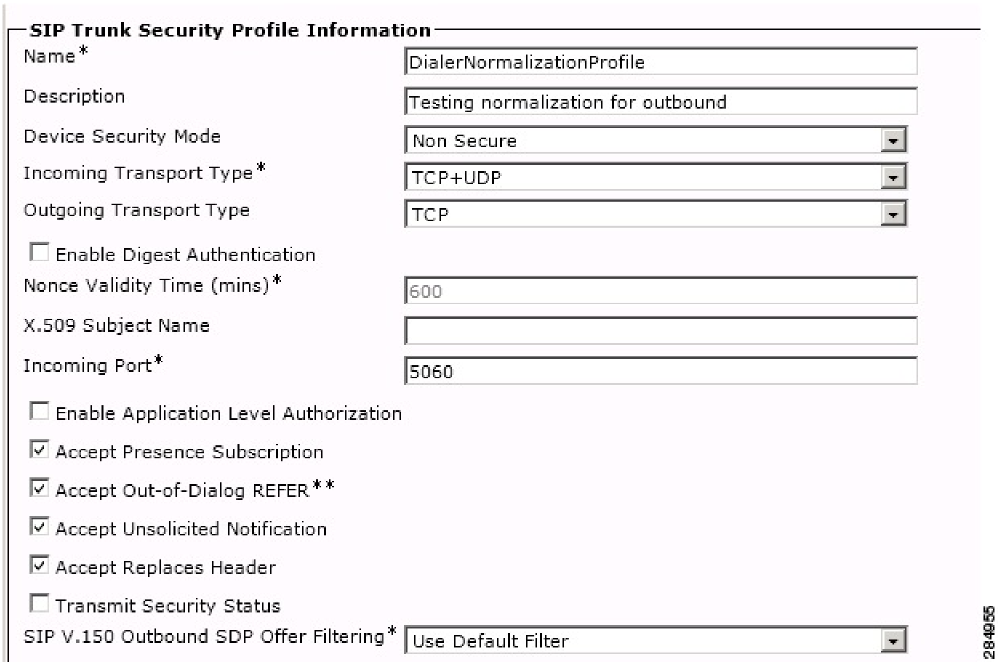
Step 1 Navigate to `https://<IP_address>:8443` where *`<IP_address>`* identifies the Unified Communications Manager server.

Step 2 Sign in to Unified Communications Manager.

Step 3 To create a SIP trunk security profile in Unified Communications Manager, select **Communications Manager GUI** > **System** > **Security** > **SIP Trunk Security Profile** > **[Add New]**.

The default port is 5060.

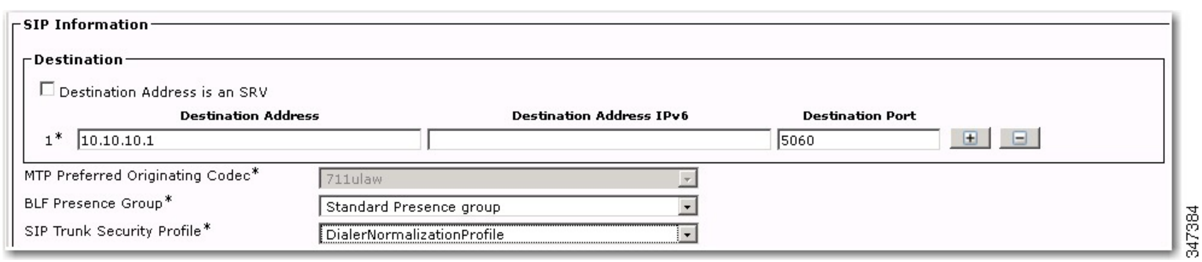
Figure 10: SIP Security Profile



Step 4 Click **Save**.

Step 5 Create a new SIP trunk and add the new SIP Trunk Security Profile.

Figure 11: Create a New SIP Trunk



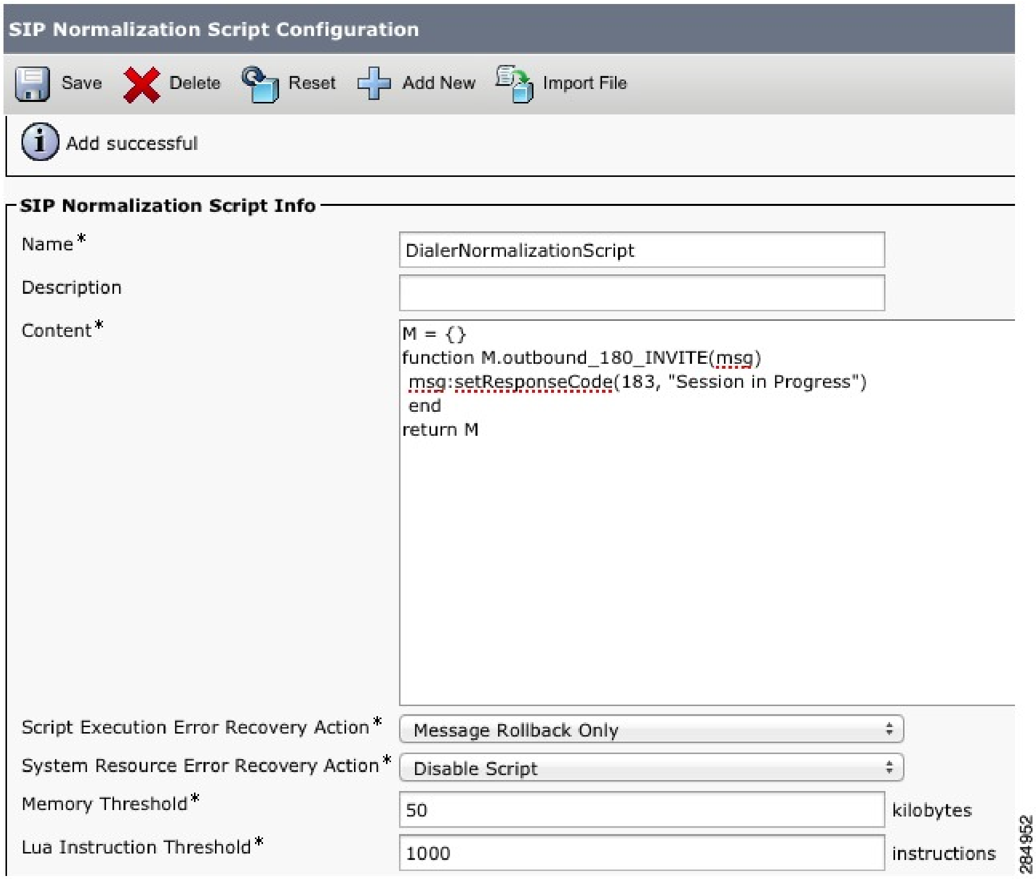
Step 6 Click **Save**.

Step 7 Click **Reset**.

Step 8 In **Communications Manager GUI** > **Devices** > **Device Settings** > **SIP Normalization Scripts** > **[Create New]**, enter the following SIP normalization script into the content field. All other values remain set to default.

```
M = {}
function M.outbound_180_INVITE(msg)
msg:setResponseCode(183, "Session in Progress")
end
return M
```

Figure 12: Add Normalization Script



Step 9 Click **Save**.

Step 10 Associate the new normalization script with the SIP trunk.

Figure 13: Associate Script with Trunk

Step 11 Click **Save**.

Step 12 Click **Reset**.

Configuration of Voice Gateways

Telecom carriers sometimes send an ISDN alerting message without a progress indicator. This situation causes the voice gateway to send a SIP 180 Ringing message, instead of a SIP 183 Session In Progress message, to the SIP dialer. The SIP dialer can process provisional messages such as 180, 181, 182, and 183 with or without Session Description Protocol (SDP). When the SIP dialer receives these provisional messages without SDP, the dialer does not perform Call Progress Analysis (CPA) and the Record CPA feature is disabled.

To enable the SIP dialer to perform CPA, add the following configuration to the POTS dial-peer of the voice gateway: "`progress_ind alert enable 8`". This code sends a SIP 183 message to the SIP dialer.

Telecom carriers sometimes send an ISDN alerting message without a progress indicator. This situation causes the voice gateway to send a SIP 180 Ringing message, instead of a SIP 183 Session In Progress message, to the SIP dialer. The SIP dialer can process provisional messages such as 180, 181, 182, and 183 with or without Session Description Protocol (SDP). The SIP Dialer processes the CPA information along with the SDP information because the SDP information is part of these provisional messages. But if the dialer receives these provisional messages without SDP, the dialer does not perform Call Progress Analysis (CPA) and the Record CPA feature is disabled. If the next provisional message changes the SDP information, the dialer processes the SDP information.

Enable 100rel for Outbound Option. Otherwise, Outbound calls from the SIP Dialer fail. The following two sections provide examples of voice gateway configuration from the command line.

Configure Rel1xx Supported for Dial-Peer for the SIP Dialer

The following example shows how to enable rel1xx on a voice dial-peer for the SIP dialer. It uses 8989 for the tag of the voice dial-peer.

```
GW(config)#config t
GW(config-dial-peer)#dial-peer voice 8989 voip
GW(config-dial-peer)#voice-class sip rel1xx supported 100rel
GW(config-dial-peer)#exit
GW(config)#exit
GW#wr
```

This short procedure results in the following dial-peer configuration. (Only the bolded line is relevant to this discussion.)

```
dial-peer voice 8989 voip
incoming called-number 978T
voice-class sip rel1xx supported "100rel"
dtmf-relay rtp-nte h245-signal h245-alphanumeric
codec g711ulaw
```

Configure Outgoing Dial-Peer for a Dialing Customer

The following example shows how to configure an outgoing dial-peer for a dialing customer.

```
GW(config)#config t
GW(config-dial-peer)#dial-peer voice 97810 voip
GW(config-dial-peer)#destination-pattern 97810[1-9]
GW(config-dial-peer)#port 1/0:23
GW(config-dial-peer)#forward-digits all
GW(config-dial-peer)#exit
GW(config)#exit
GW#wr
```

This short procedure results in the following dial-peer configuration for a dialing customer.

```
dial-peer voice 97810 pots
destination-pattern 97810[1-9]
port 1/0:23
forward-digits all
```

Configure Rel1xx Disable for Unified CVP Voice Dial-Peer

The following example shows how to disable rel1xx for a Unified CVP voice dial-peer. It uses 8989 for the tag of the voice dial-peer.

```
GW(config)#config t
GW(config-dial-peer)#dial-peer voice 8989 voip
GW(config-dial-peer)#voice-class sip rel1xx disable
GW(config-dial-peer)#exit
GW(config)#exit
GW#wr
```

This short procedure results in the following dial-peer configuration. (Only the bolded line is relevant to this discussion.)

```
dial-peer voice 8989 voip
description CVP SIP ringtone dial-peer
service ringtone
incoming called-number 9191T
voice-class sip rel1xx disable
dtmf-relay rtp-nte h245-signal h245-alphanumeric
codec g711ulaw
no vad
```

Configure an Outgoing Dial-Peer for Transferring Call to Agent

The following example shows the outgoing dial-peer configuration for transferring calls to agents.

```
dial-peer voice 11000 voip
 destination-pattern 11T
 session protocol sipv2
 session target ipv4:10.10.10.31(this is Call Manager's IP address)
 voice-class codec 1
 voice-class sip rel1xx supported "100rel"
 dtmf-relay rtp-nte h245-signal h245-alphanumeric
 no vad
```

Note In a SIP Dialer with Unified CVP VRU deployment, dialer-related call flows do not invoke call-survivability scripts that are enabled on an incoming POTS dial-peer in the Ingress gateway. However, enabling a call-survivability script on an Inbound POTS dial-peer does not negatively affect dialer-related call flows.

Configure Transcoding Profile for Cisco Unified Border Element

The following example shows the transcoding profile for Cisco UBE.

Note Transcoding impacts port density.

```
dspfarm profile 4 transcode universal
     codec g729r8
     codec g711ulaw
     codec g711alaw
     codec g729ar8
     codec g729abr8
     maximum sessions 250
     associate application CUBE
     !
```

Configure Cisco Unified Border Element

While configuring Cisco UBE, ensure that you:

- Configure the three dial-peers in the Cisco UBE.

  The dial-peers are used for:

  - Incoming calls from the dialer.
  - Outgoing calls to the terminating network from the Cisco UBE.
  - Calls to be routed to the Cisco Unified Communications Manager.

- Issue the following commands globally to configure the Cisco UBE:

  - **no supplementary-service sip refer**
  - **supplementary-service media-renegotiate**

Note Virtual CUBE does not support CPA. Use a dedicated physical gateway if your solution needs CPA.

Configure SIP Trunks

Unified CM is connected to the voice gateway by SIP Trunks, which you configure on Unified CM. Set up route patterns for the Dialer which are appropriate for your dial pattern.

See the *System Configuration Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html for instructions on how to configure SIP trunks. For information about logging in to Ingress or VXML gateways, refer to the sections on configuring gateways for Courtesy Callback in the *Configuration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html.

Procedure

Configure a SIP trunk on Unified CM from Unified CM to the voice gateway. Specify the IP address of the voice gateway in the **Destination** field.

Configure E1 R2 Signaling

The Outbound Option Dialer may be configured with systems using the E1 R2 signaling protocol. E1 R2 signaling is a channel associated signaling (CAS) international standard that is used with E1 networks in Europe, Latin America, Australia, and Asia. For more information, see E1 R2 Signaling Theory

The high-level procedure for configuring an E1 R2 controller for use with the Outbound dialer is summarized below. For full configuration details, see E1 R2 Signaling Configuration and Troubleshooting.

Procedure

Step 1 Set up an E1 controller connected to the private automatic branch exchange (PBX) or switch. Ensure that the framing and linecoding of the E1 are properly set for your environment.

Step 2 For E1 framing, choose either **CRC** or **non-CRC**.

Step 3 For E1 linecoding, choose either **HDB3** or **AMI**.

Step 4 For the E1 clock source, choose either **internal** or **line**. Keep in mind that different PBX's may have different requirements for their clock source.

Step 5 Configure line signaling.

Step 6 Configure interregister signaling.

Step 7 Customize the configuration with the **cas-custom** command.

Example E1 R2 Settings

```
controller E1 0/0/0
  framing NO-CRC4
  ds0-group 1 timeslots 1-15,17-31 type r2-digital r2-compelled ani
  cas-custom 1
  country telmex
  category 2
  answer-signal group-b 1
  caller-digits 4
  dnis-digits min 4 max 13
  dnis-complete
  timer interdigit incoming 1000
  groupa-callerid-end
```

Outbound Option Software Installation Steps

This section discusses the tasks that are associated with installing Outbound Option and related components. Before proceeding, navigate to the Side A Unified CCE AW-HDS-DDS and stop all ICM services there. Then perform the steps in the following sections.

Software and Database Creation

In the next phase, you install the Outbound Option component software and create its database. The following table lists the steps that comprise software installation and database creation.

Table 9: Software Installation and Database Creation Steps

Step	Procedure
1	Configure the Logger for Outbound Option, on page 114
2	Create Outbound Option Database, on page 113
3	Add MR PIM for Outbound, on page 116
4	Install Dialer Component on the PG Virtual Machine, on page 117

Outbound Option Database

Outbound Option uses a dedicated SQL database on the Logger. The installation includes creating this database. The installer collects some business-related data to properly create the database.

If you enable Outbound Option High Availability, ensure that the Logger virtual machine datastore is large enough to accommodate both the Logger database and the Outbound Option database on Logger Side A and Logger Side B.

Consider these guidelines when determining minimum drive size:

- For a 4000 (or smaller) Agent Reference Design solution, add an extra 500 GB of disk space for the Outbound Option database.
- For a 12000 Agent Reference Design solution, add an extra 1 TB of disk space for the Outbound Option database.

Note When using Outbound Option High Availability on a Packaged CCE system, the maximum number of records that can be imported without adding any extra disk space to the Rogger VM is one million.

Outbound Option for High Availability: Preliminary Two-Way Replication Requirements

If you plan to set up Outbound Option for High Availability two-way replication, there are several preliminary requirements.

Create an Outbound Option Database on Logger Side A and Side B

If you have enabled Outbound Option on Logger Side A in a previous release, you must:

- Stop all Logger services on Logger Side A.
- Perform a full database backup for the Outbound Option database on Logger Side A and restore it to Logger Side B. Use SQL Server Management Studio (SSMS) to complete this task.

If you have not enabled Outbound Option in a previous release, you must create an Outbound Option database on Logger Side A and Logger Side B. Use the ICMDBA utility to complete this task.

Note If the database replication fails and it is resolved, the Outbound Option HA must be enabled again. In such a case, you must again synchronize the databases on the Active and Standby sides. Perform a full database backup for the Outbound Option database on Active side and restore it to the Standby side.

Define Logger Public Interface Hostname on Logger Side A and Logger Side B

As you configure Outbound Option for High Availability, you must define the Logger Public Interface Hostname on both sides of the Logger. IP addresses are not allowed.

Make Campaign Manager and Dialer Registry Setting Customizations on Both Side A and Side B

If you customize any Campaign Manager and Dialer registry settings on one side, you must make the same updates for the registry settings on the other side.

Stop the Logger Service Before Enabling or Disabling Outbound Option High Availability

Before you enable or disable Outbound Option High Availability, stop the Logger service on the applicable side or sides.

Create Outbound Option Database

Before you use Outbound Option, estimate the size for the Outbound Option database.

Procedure

Step 1 Collect the following information:

- The size, in bytes, of each customer record in the import file. If the size is less than 128 bytes, use 128. (RecordSize)
- The number of records that are imported. (RecordCount)
- Do the records from new imports replace or append to records that are already in the database?

Step 2 Estimate the contact table size as follows:

- If imports overwrite existing records: Do not change record count.
- If imports append to existing records: RecordCount = total number of rows kept in a customer table at a time.
- contact-table-size = RecordSize * RecordCount * 1.18

Step 3 Estimate the dialing list table size as follows:

- If imports overwrite existing records: RecordCount = number of rows imported * 1.5. (50% more rows are inserted into the dialing list than are imported.)
- If imports append existing records: RecordCount = total number of rows kept in customer table at a time * 1.5
- dialing-list-table-size = rows in dialing list * 128 bytes * 4.63

Step 4 Calculate the database size using this formula:

```
(Number of rows in all DL tables * (size of one row + size of index) ) +
(Number of rows in personal call back table * (size of one row + size of index) ) +
(Number of rows in Contact List table * (size of one row + size of index))
```

Step 5 Start ICMDBA by entering **ICMDBA** in the Microsoft Windows **Run** dialog box or command window.

Step 6 Select the **Logger**. Then, select **Database** > **Create**.

Step 7 In the **Create Database** window, specify the Outbound Option database type.

Step 8 Click **Add**. The **Add Device** window appears.

Use this window to create a new data device and log device for the Outbound Option database. Specify the disk drive letter and size in megabytes for each new device.

Step 9 Click **OK** to create the device.

Step 10 Click **Create**, and then click **Start**.

Step 11 Click **Close**.

If necessary, you can later edit the device to change storage size, or remove a device, using the **Database** > **Expand** option.

Caution You cannot make manual changes to the contents of the Outbound Option database. Do not use triggers in the Outbound Option database. Do not add or modify triggers for the dialing lists or personal callback list. The Dialer_Detail table in the logger or HDS contains the information that custom applications require. Extract that information from the historical database server (HDS) to a separate server where the custom application can process the data without impacting the HDS.

Note If you have used the ICMDBA tool to create an Outbound Option database on Side B of Unified CCE Rogger and you later uninstall Packaged CCE, you can manually delete the database after the uninstallation by using SQL Server Management Studio (SSMS).

Note When you use the **Append** option to import records to the **Outbound Contact Table**, the size of the Blended Agent (BA) database keeps increasing and it occupies all the available space in the disk. Hence, you must manually purge the **Outbound Contact Table** to create more space on the disk.

What to do next

You must enable autogrowth on the Outbound Option database. For details, refer to the section about verifying database configuration in the *Outbound Option Guide for Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html.

Configure the Logger for Outbound Option

Use this procedure to configure the Logger for Outbound Option.

You can (optionally) configure the Logger to enable Outbound Option and Outbound Option High Availability. Outbound Option High Availability facilitates two-way replication between the Outbound Option database on Logger Side A and the Outbound Option database on Logger Side B. Use the ICMDBA tool to create an outbound database on Side A and Side B; then set up the replication by using Web Setup.

Perform the following procedure on both the Side A and Side B Loggers to configure Outbound Option or Outbound Option High Availability. Both Logger machines must be up and operational.

Important Before you configure the Logger for Outbound Option High Availability:

- Confirm that an Outbound Option database exists on Logger Side A and Logger Side B.

Procedure

Step 1 Open the Web Setup tool.

Step 2 Choose **Component Management** > **Loggers**.

Step 3 Choose the Logger that you want to configure, and click **Edit**.

Step 4 Click **Next** twice.

Step 5 On the Additional Options page, click the **Enable Outbound Option** check box.

Step 6 Click the **Enable High Availability** check box to enable Outbound Option High Availability on the Logger. Checking this check box enables High Availability two-way replication between the Outbound Option database on Logger Side A and the Outbound Option database on Logger Side B. Two-way replication requires that you check this check box on the Additional Options page for both Logger Side A and Side B. If you disable two-way replication on one side, you must also disable it on the other side.

You must enable Outbound Option in order to enable Outbound Option High Availability. Similarly, if you have enabled High Availability, you must disable High Availability (uncheck the **Enable High Availability** check box) before you can disable Outbound Option (uncheck the **Enable Outbound Option** check box).

Step 7 If you enable High Availability, enter a valid public server hostname address for **Logger Side A** and **Logger Side B**. Entering a server IP address instead of a server name is not allowed.

Step 8 If you enable High Availability, enter the **Active Directory Account Name** that the opposite side Logger runs under or a security group that includes that account.

Note While using Outbound Option High Availability, if you want to change the **Logger Public Interface** or **Active Directory Account Name**, you must disable Outbound Option High Availability using logger setup. Only after disabling Outbound Option HA, change the **Logger Public Interfaces** or **Active Directory Account Name**, then re-enable Outbound Option High Availability to update the new **Logger Public Interface** or **Active Directory Account Name**.

Step 9 Select the **Syslog** box to enable the Syslog event feed process (cw2kfeed.exe).

Note The event feed is processed and sent to the Syslog collector only if the Syslog collector is configured. For more information about the Syslog event feed process, see the *Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Step 10 Click **Next**.

Step 11 Review the Summary page, and click **Finish**.

Additional Two-Way Outbound Option Database Replication Consideration

Keep in mind the following consideration when setting up two-way replication.

Import to Active Side

Importing a local file succeeds only if you import it to the active side. To avoid having to identify which side is active, you can use any of the following methods:

- Create a Microsoft Windows file share that is accessible to both sides with the same mapping; for example, //<machine_name>/drive/file, viewable from both sides.

- Use Microsoft Windows Distributed File System (DFS). With DFS, you can set up a local drive that DFS updates for you. DFS also makes sure that operations are replicated. For more information, see your Microsoft documentation.
- For campaigns created by using the Outbound API, you can use the Import API to import contacts without identifying the active side. For more information, see the *Cisco Packaged Contact Center Enterprise Developer Reference* at https://developer.cisco.com/site/packaged-contact-center/documentation/.

Add MR PIM for Outbound

Procedure

Step 1 Access the Unified CCE PG on Side A.

Step 2 From **Cisco Unified CCE Tools**, select **Peripheral Gateway Setup**.

Step 3 In the Instance Components panel of the **Components Setup** screen, select the **PG2A Instance** component for Side A. (Select **PG2B** for Side B.) Then click **Edit**.

Step 4 In the **Peripheral Gateways Properties** screen, click **Media Routing**. Then click **Next**.

Step 5 Click **Yes** at the prompt to stop the service.

Step 6 From the **Peripheral Gateway Component Properties** screen, click **Add** and select **PIM2**.

Note Select **PIM2** and **peripheralID 5003** even if you are not using PIM1 for another machine.

Step 7 Configure with the client type of Media Routing as follows:

a) Check **Enabled**.
b) Enter `MR2` or a name of your choice for the **Peripheral name**.
c) Enter `5003` for the **Peripheral ID**.
d) Enter `Unified CCE PG Side A IP` (Side B IP for **PG2B**) for the **Application Hostname(1)**.
e) Retain the default value for the **Application Connection port (1)**.
f) Enter `Unified CCE PG Side B IP` (Side A IP for **PG2B**) for the **Application Hostname(2)**.
g) Retain the default value for the **Application Connection port (2)**.
h) Enter `5` for the **Heartbeat interval (sec)**.
i) Enter `10` for the **Reconnect interval (sec)**.
j) Check the **Enable Secured Connection** option.

   This establishes a secured connectionbetween MR PIM and Application Server.

   Ensure that you provide the correct information in the Application Hostname (1) and Application Connection Port (1) fields.

k) Click **OK**.

Step 8 Accept defaults and click **Next** until the **Setup Complete** screen opens.

Step 9 At the **Setup Complete** screen, check **Yes** to start the service. Then click **Finish**.

Step 10 Click **Exit Setup**.

Step 11 Repeat from Step 1 for the Unified CCE PG on Side B.

Install Dialer Component on the PG Virtual Machine

Procedure

Step 1 Stop all Packaged CCE Services.

Step 2 On both the Side A and Side B PGs, run Peripheral Gateway Setup. Select **Start** > **All Programs** > **Cisco Unified CCE Tools** > **Peripheral Gateway Setup**.

Step 3 In the **Cisco Unified ICM/Contact Center Enterprise & Hosted Components Setup** dialog, select an instance from the left column under **Instances**.

Step 4 Click **Add** in the **Instance Components** section.

The **ICM Component Selection** dialog opens.

Step 5 Click **Outbound Option Dialer**.

The **Outbound Option Dialer Properties** dialog opens.

Step 6 Check **Production mode** and **Auto start at system startup**. These options set the Dialer Service startup type to Automatic, so the dialer starts automatically when the machine starts up.

The **SIP (Session Initiation Protocol)** Dialer Type is automatically selected.

Step 7 Click **Next**.

Step 8 Supply the following information on this page:

- In the **SIP Dialer Name** field, enter the name of the SIP dialer. For example, `Dialer_for_Premium_Calling_List`. There's a 32-character limit. The name entered here must match the name that is configured in Configuration Manager.
- For **SIP Server Type**, select Cisco voice gateway .
- In the **SIP Server** field, enter the hostname or IP address of the Cisco voice gateway.

  Note The **SIP Server** hostnames are restricted to a maximum of 16 characters.

- In the **SIP Server Port** field, enter the port number of the SIP Server port. Default is 5060.

Click **Next**.

Step 9 On the **Outbound Option Dialer Properties** dialog, specify the following information:

- **Campaign Manager server**—The hostname or IP address of the Outbound Option server (the hostname or IP address of Unified CCE Rogger Side A) in Packaged CCE.
- **Campaign Manager server A**—If the Campaign Manager is set up as duplex, enter the hostname or IP address of the machine where the Side A Campaign Manager is located. If the Campaign Manager is set up as simplex, enter the same hostname or IP address in this field and the **Campaign Manager server B** field. You must supply a value in this field.
- **Campaign Manager server B**—If the Campaign Manager is set up as duplex, enter the hostname or IP address of the machine where the Side B Campaign Manager is located. If the Campaign Manager is set up as simplex, enter the same hostname or IP address in this field and the **Campaign Manager server A** field. You must supply a value in this field.

In simplex mode, make sure not to provide same port number in server Side B and Side A. For more information about port ranges, see the *Port Utilization Guide*.

- **Enable Secured Connection**— Allows you to establish secured connection between the following:
  - CTI server and dialer
  - MR PIM and dialer

  Check the **Enable Secured Connection** check box to enable secured connection.

  Note Before you enable secured connection between the components, ensure to complete the security certificate management process.

  For more information, see the *Security Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

- **CTI server A**—The hostname or IP address of Unified CCE PG Side A.
- **CTI server port A**—The port number that the dialer uses to create an interface with CTI server-Side A. The default is 42027.
- **CTI server B**—The hostname or IP address of Unified CCE PG Side B.
- **CTI server port B**—The port number that the dialer uses to create an interface with CTI server-Side B. The default is 43027.
- **Heart beat**—The interval between dialer checks for the connection to the CTI server, in milliseconds. The default value is 500.
- **Media routing port**—The port number that the dialer uses to create an interface with the Media Routing PIM on the Media Routing PG. The default is 38001. Make sure the Media routing port matches that of the MR PG configuration.

Step 10 Click **Next**. A **Summary** screen appears.

Step 11 Click **Next** to begin the dialer installation.

Optional - Edit Dialer Registry Value for Auto-Answer

If you enable auto answer in the CallManager with a zip tone, you must disable auto answer in the Dialer or Dialers, if there are more than one. A zip tone is a tone sent to the agent's phone to signal that a customer is about to be connected.

To disable auto answer in the Dialer, after the Dialer process runs for the first time, change the value of the following registry key to 0:

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<*instance_name*>
\Dialer\AutoAnswerCall

Auto Answer Configuration on Agent Phones

The dialer component is preconfigured during installation to auto answer Outbound Option related calls to the Outbound Option agent. However, this default configuration does not provide a zip tone to the agent (which notifies of incoming calls), so agents must monitor the agent application for incoming customer calls.

To enable zip tone, enable auto-answer on the agent's phone configuration in Unified CM. This solution adds about a second onto the transfer time. This solution is identical to the solution that is used for Unified CCE.

For Mobile Agents using the nailed connection, the Unified CM auto answer setting does not provide a zip tone, but contact center enterprise does provide an option for playing a notification tone to the agent using the agent desk settings.

Enabling auto answer in the agent desk settings or in the dialer component in conjunction with the Unified CM can be problematic. Therefore, disable the auto answer option in the dialer component, and enable it either in the agent desk settings or in Unified CM.

Verify connections

The Diagnostic Framework Portico provides details about the health of the installation even before any campaign configuration is initiated or before any call is placed. The interface contains the following details about the dialer status.

Procedure

Step 1 Navigate to the Outbound Option Dialer component in the Diagnostic Framework Portico.

The Node Name is Dialer. The Process name is BADialer.

Step 2 Verify that the Campaign Manager (CM) has a status of Active (A).

Step 3 Verify that the CTI Server (CTI) has a status of Active (A).

Step 4 Verify that the number of Configured Ports equals the number of Ready Ports.

Step 5 Verify that the MR has a status of Active (A).

Maintenance Considerations

This section contains information about maintaining the Outbound Option application.

SIP Dialer Voice Gateway Over-capacity Errors

If your network monitoring tool receives an alarm in the SIP dialer about being over capacity, you can ignore the alarm unless it becomes an ongoing issue. This section describes the source of the alarm and remedial actions associated.

If the Voice Gateway in a SIP dialer implementation is over capacity, the SIP Dialer receives the following message: `SIP 503 messages if the SIP Dialer is deployed with Voice Gateway only`

If the percentage of SIP 503 messages reaches 1% of all messages, the SIP dialer raises an alarm.

Use one of the following measures to attempt to remedy the problem if Voice Gateway capacity becomes an ongoing issue:

- Check the Voice Gateway configuration. If there are errors, fix them and reset Port Throttle to its original value. Port Throttle (the calls-per-second rate at which the dialer dials outbound calls) is set on the Dialer General tab in the Configuration Manager.
- Check the sizing information. Adjust the value of Port Throttle according to the documented guidelines.
- Enable the auto-throttle mechanism by setting the Dialer registry setting **EnableThrottleDown** to 1.

  To set **EnableThrottleDown**, open the Registry Editor (regedit.exe) on the PG machine and navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<customerinstance>\Dialer`.

The SIP dialer performs an automatic throttle down when the percentage of SIP 503 messages reaches 2% of all messages, if the auto-throttle mechanism is enabled. This throttle down means that the SIP dialer decreases the configured value of Port Throttle by approximately 10%.

If one throttle down does not correct the problem, the SIP dialer performs more throttle downs until either the problem is corrected or the value of Port Throttle is throttled down to 50% of the originally configured value.

For each automatic throttle down, alarm and trace messages clearly provide detailed information about the adjusted port throttle value, configured port throttle value, and time duration.

Even after the problem is corrected, the dialer does not automatically throttle back to the configured value. To increase the throttle back to the configured value, run the **updateportthrottle /portthrottle <configured value>** command using the process monitoring tool Procmon.

Update the North American Numbering Plan Data

The Regional Prefix Update Tool (RPUT) is used to update the Packaged CCE database to the latest North American Local Exchange NPA NXX Database (NALENND).

You can use this tool only if Packaged CCE is using the North American Numbering Plan.

The RPUT is composed of the following two files (installed in the `ICM\bin` directory on the Unified CCE AW-HDS-DDS server):

- region_prefix_data.txt (or the <DatafileName>)

  Contains the data this tool uses to update the region prefix table in the Packaged CCE database. Note that you should change paths to the `ICM\bin` directory.

- regionfix.exe

  This executable reads the region_prefix_data.txt data file and updates the region prefix table.

The RPUT is run from the command line as described in the following procedure.

Procedure

Step 1 Open a command prompt (Select **Start** > **Run**, and enter **cmd**, then click **OK**).

Step 2 Change the path to `ICM\bin`.

Step 3 Enter the following at the prompt: `regionfix.exe <DatafileName>` (where *<DatafileName>* is the name of the data file).

The Regional Prefix Update Tool then shows the version of the input data file and asks if you want to proceed. If you proceed, the tool connects to the Packaged CCE database. The number of records that are to be updated, deleted, and inserted appear. These records are put into three different files:

- region_prefix_update.txt (which includes preserved Custom Region Prefixes)
- region_prefix_new.txt
- region_prefix_delete.txt

Step 4 You can either delete or retain the entries present in the region_prefix_delete.txt file while performing the insertions and updates. To retain the entries, type **No** when the tool prompts you to delete the entries. Type **Yes** to delete the entries.

Step 5 Check the contents of the files before proceeding.

Step 6 Answer **Yes** to proceed with the update.

When the update is complete, the tool displays the following message:

```
Your region prefix table has been successfully updated.
```

Administration and Usage

Campaign configuration

Campaign Task List

The following table lists the steps that are required to create both an agent and IVR campaign, and the location of the instructions for the task.

Table 10: Steps for Creating a Campaign

Step Number	Task	Where Discussed
1	Create one or more skill groups for the campaign.	Configure Skill Group, on page 122
2	Configure the call type using the Packaged CCE Call Type gadget.	Create a Call Type, on page 122
3	Create a dialed number on the MR client using the Packaged CCE Dialed Number gadget. This dialed number is for agent reservation.	Configure Dialed Numbers, on page 122
4	Create DN for Abandon to IVR on the MR PG for the SIP dialer.	Configure Dialed Numbers, on page 122
5	Create DN for AMD to IVR on the MR PG for the SIP dialer.	Configure Dialed Numbers, on page 122

Step Number	Task	Where Discussed
6	Configure a campaign using the Outbound Option Campaign tool.	Create a Campaign, on page 122
7	Configure a routing script using the Script Editor.	Set Up Routing Scripts, on page 129
8	Configure an administrative script using the Script Editor.	Set Up Administrative Scripts, on page 125
9	Voice gateway configuration.	Voice Gateway and Unified CVP Configuration for a VRU Campaign, on page 123

Configure Skill Group

Add at least one skill group. For an agent campaign, add at least one agent to the skill group. Log the agent in to the skill group, and make the agent ready for the agent campaign. You do not need to add an agent for a VRU campaign skill group. For information about configuring skill groups, 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/products-maintenance-guides-list.html.

Create a Call Type

The dialed numbers and routing scripts that you will create will reference *call types*, so you should create them as needed. For information about creating call types, 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/products-maintenance-guides-list.html. For example, you can create one call type for an agent campaign and another for a VRU campaign. You need to associate the call types with the dialed numbers you created earlier.

Configure Dialed Numbers

Configure at least two dialed numbers on the outbound routing client: one for the agent campaign and one for the VRU campaign. 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/products-maintenance-guides-list.html for information about configuring dialed numbers.

Create a Campaign

The Campaign feature in the Packaged CCE webadmin is used to add, delete, and modify Outbound Option campaigns.

Before you create a campaign, first configure the following information:

- At least one skill group
- The following dialed numbers with Routing Type set to Outbound Voice:
    - One for accessing the agent reservation script (not required for transfer to VRU campaigns).

- One for transferring the call to the VRU for abandon treatment when no agents are available. This number must be different from the previous number.
- One for transferring the call to the VRU for answering machine detection (AMD) or transfer to VRU campaign treatment. This number can be the same as the previous number, but different from the first number.

For more information, refer the **Manage Campaign** section in 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/products-maintenance-guides-list.html.

Notes on Editing a Campaign in Progress

You can edit most campaign configuration settings while a campaign is running. The changes take effect with new calls after the setting has been changed. However, do not edit the following settings while a campaign is in progress:

- Do not modify the **Maximum Attempts**value. Modifying this value while a campaign is in progress can cause a long delay in record retrieval and longer agent idle times.
- Do not delete a skill group while a campaign is in progress.

(Optional) Configure Personal Callbacks

PersonalizedCallback is an optional feature in Outbound Option. Personal Callback enables an agent to schedule a callback to a customer for a specific date and time. A personal callback connects the agent who originally spoke to the customer back to the customer at the customer-requested time.

When you create campaigns, you enable the callback feature individually for each campaign.

For more information, refer the **Manage Campaign** section in 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/products-maintenance-guides-list.html.

Voice Gateway and Unified CVP Configuration for a VRU Campaign

For a VRU campaign, you need to configure a dial-peer in the voice gateway. This dial peer is used to instruct the voice gateway to transfer the call to Unified CVP. It must match the Network VRU label that is configured on the MR routing client with type 10 Unified CVP network VRU.

In base configuration, this label is preconfigured with default value 66611110000. Follow the steps in this example.

Procedure

Step 1 Add a dial-peer to match the network VRU label in the outbound routing client.

Example:

```
dial-peer voice 6661111 voip
description ******To CVP1*****
destination-pattern 6661111T
session protocol sipv2
session target ipv4:10.10.10.10
voice-class codec 1
```

```
voice-class sip rel1xx supported "100rel"
dtmf-relay rtp-nte h245-signal h245-alphanumeric
no vad
```

Note The call can be transferred to only one Unified CVP; in the above example, the call is transferred to CVP1.

Step 2 Configure a dial-peer for the VRU leg. This is the same dial-peer as the inbound call flow whose call is transferred to Unified CVP.

Example:

```
dial-peer voice 777111 voip
description Used for VRU leg
service bootstrap
incoming called-number 7771111T
voice-class sip rel1xx disable
dtmf-relay rtp-nte h245-signal h245-alphanumeric
codec g711ulaw
no vad
```

Step 3 A Routingpattern needs to be configured on Unified CCE Administration so that Unified CVP can route the call to the VXML gateway after it receives the run script request from the router. This dialed pattern is the same one as the inbound call flow that transfers a call to VRU. If the base configuration has not been changed, the pattern is 777111*.

Note It is possible that the procedures in Steps 2 and 3 may have been done already during installation. For more information, 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/products-maintenance-guides-list.html

Outbound Option Scripting

Outbound Option uses Packaged CCE scripting configured on the Administrative Workstation to manage campaigns.

There are two types of scripts:

- Administrative Scripts
- Agent Reservation Routing Scripts

Administrative Scripts for Outbound Option

Outbound Option administrative scripts enable, disable, or throttle campaign skill groups for outbound campaigns. The scripts can also automatically close out a skill group for a specific campaign. The administrative scripts can use time or any other conditional factor that the script can access to close a skill group. You can perform this scripting at the skill group level to provide more flexibility for managing larger campaigns with multiple skill groups.

Enable a campaign skill group by setting the campaign mode to one of the available modes: Preview, Direct Preview, Progressive, or Predictive. Schedule an administrative script to run at regular intervals. Disable the campaign skill group in the administrative script by creating a script node to change the campaign mode to inbound for that skill group.

An administrative script controls a campaign skill group. You can only map a campaign skill group to one campaign at a time. Multiple administrative scripts controlling the same skill group can result in conflicting campaign mode requests.

Note Both the Outbound API and administrative scripts can set the dialing mode for a campaign. The value set by the administrative script takes precedence over the value set by the API.

You can also use administrative scripts to control the percentage of agents that a campaign skill group can use. A script can also set whether to use a skill group for other campaigns or inbound calls.

Note To allow the outbound control and percent configured values from Campaign Skill group (set by either the Configuration Manager Campaign Skill Group tab or the Campaign API) to apply without restarting the router. If you use an administrative script to set the outbound control and percent variables in operation and if you want to employ these configured value on the Campaign Skillgroup, set the outbound control and percent variable to -1 in the administrative script accordingly.

Set Up Administrative Scripts

Use the Script Editor application to create an administrative script for each skill group to set the OutboundControl variable and the skill group reservation percentage. The Outbound Option Dialer uses the value of this variable to determine which mode each skill group uses.

Note

- If the OutboundControl variable is not set, the skill group defaults to inbound. See chapter 1, "Outbound Business Concepts" for detailed information about Outbound Option outbound dialing modes.
- Make sure that the routing client for the translation route labels is Unified CM, which makes the outgoing call.

Perform the following steps to create the administrative script:

Procedure

Step 1 Open the Script Editor application.

Step 2 Select **File > New > Administrative Script**.

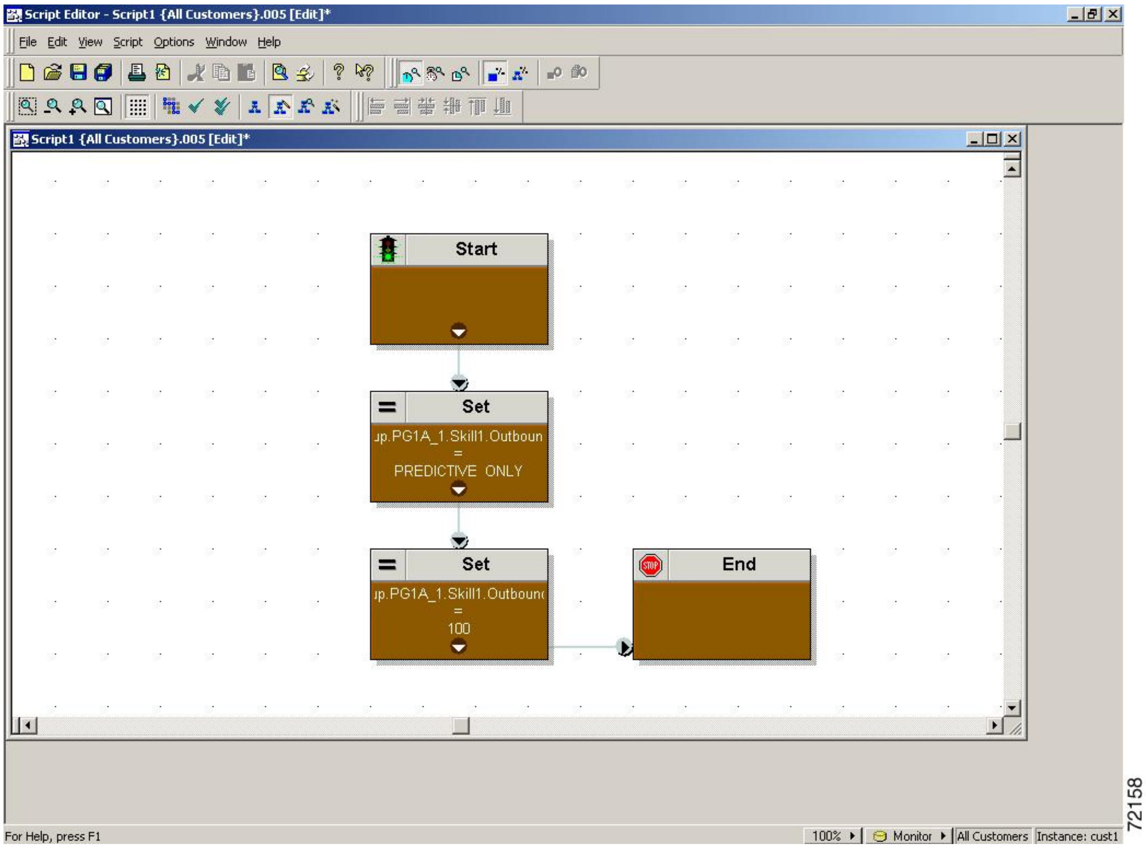
Step 3 Create an administrative script.

One script can be used to control all Outbound Option skill groups or multiple scripts can control multiple Outbound Option skill groups. For example, if you want to control skill groups at different times of the day, you need multiple administrative scripts; however, if you are going to initialize the groups all in the same way, you need only one script (with additional Set nodes).

Step 4 Set up the script with the following nodes (required): Start, Set Variable, and End.

The following diagram displays a simple administrative script where both the OutboundControl variable and the outbound percentage are set for a skill group. A script in a production call center is typically more complex, perhaps changing these variables according to time of day or service level.

Figure 14: Sample Administrative Script



Note The Transfer to VRU feature requires an IF node in the administrative script to disable it if the VRU is not available. Also, to ensure timely responses to VRU outages, set the administrative script to run every minute.

Step 5 Set the OutboundControl variable. Setting this variable enables contact center managers to control the agent mode.

Right-click on the work space and select **NEW** > **Object** > **Set Variable** to open the Set Properties window.

- For Object Type, select a skill group.
- For variable, select **OutboundControl**.

Set this variable to one of the values listed in the following table.

Table 11: OutboundControl Variable Values

Value String	Description
INBOUND	Agents take inbound calls only. Outbound dialing is disabled for the skill group.

Value String	Description
PREDICTIVE_ONLY	Agents in the skill group are dedicated for outbound Predictive calls only.
PREVIEW_ONLY	Agents in the skill group are dedicated for outbound Preview calls only.
PROGRESSIVE_ONLY	Agents in the skill group are dedicated for outbound Progressive calls only.
PREVIEW_DIRECT_ONLY	Agents only place outbound calls and hear ringtones, such as phone ringing or busy signal.

Note If the administrative script is changed and the SET variable is removed, the value of the OutboundControl variable is the same as it was the last time the script was run. However, if the Central Controller is restarted, the value resets to INBOUND.

Step 6 Right-click on the work space and select **NEW** > **Object** > **Set Variable** to open the Set Properties window.

- For Object Type, select a skill group.
- For variable, select **OutboundControl**.

Step 7 Set the OutboundPercent variable in the same administrative script; for example, select the OutboundPercent variable in the Set Properties window and enter the agent percentage in the Value field. This variable controls the percentage of agents, which are logged in to a particular skill group, used for outbound dialing. For example, if 100 agents are logged in to a skill group, and the OutboundPercent variable is set to 50%, 50 agents are allocated for outbound dialing for this campaign skill group. This setup allows the rest of the agents to be used for inbound or other active campaigns. The default is 100%.

Note This variable does not allocate specific agents for outbound dialing, just a total percentage. The default is 100%.

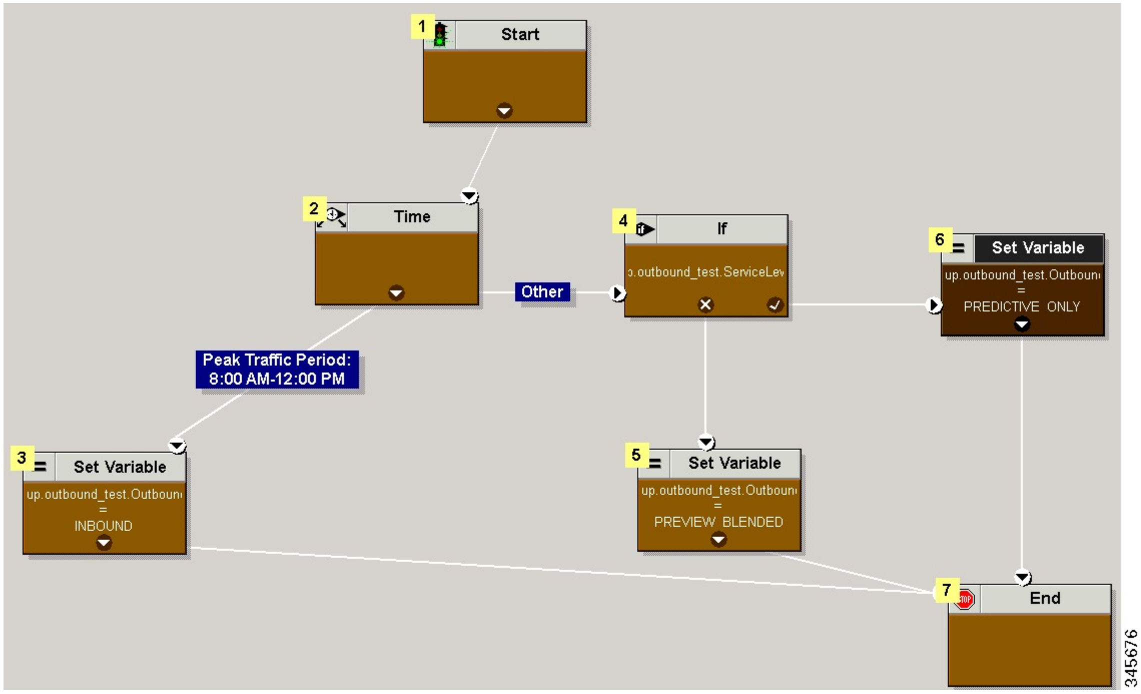
Step 8 Schedule the script.

a) Select **Script** > **Administrative Manager**. An Administrative Manager dialog box appears.
b) Click **Add**.
c) On the Script tab, select the administrative script.
d) On the Period tab, specify the run frequency of the script. (For example, every minute of every day.)
e) (Optional) Enter a description on the Description tab.
f) Click **OK** to close the Add Administrative Schedule dialog box.
g) Click **OK** to close the Administrative Manager.

Sample Administrative Script: ServiceLevelControl

The following figure demonstrates how to control skill group modes based on "Service Level," which maximizes the resource utilization in a call center and maintains an acceptable service level at the same time.

Figure 15: ServiceLevelControl Script



This script divides the day into two parts:

- **Peak Traffic Period (8:00 a.m. to 12:00 p.m.)**: During this period, the OutboundControl variable is set to INBOUND only, because more agents are required to handle inbound calls.
- **Other Periods**: During all other time periods, the OutboundControl variable is set according to the service level in the past half hour. If the skill group service level in the past half-hour period is over 85%, the OutboundControl variable gets set to PREDICTIVE_ONLY, which maximizes the efficiency of outbound campaigns. If during any half-hour period the skill group service level drops below 85%, the OutboundControl variable is switched to PREVIEW_BLENDED, so that the agents in the skill group can accept inbound calls to improve the service level. When the agents are not in an inbound call, Outbound Option presents the agents with a Preview outbound call, maximizing the resource utilization for the call center at the same time.

Add the IF Node

To add the IF node, follow these steps:

Procedure

Step 1 Select ObjectType as Skillgroup.

Step 2 Select the skill group that was created for outbound as the Object.

Step 3 Select ServiceLevelHalf as the variable.

Routing Scripts for Outbound Option

Two types of routing scripts are described later in this document. One is for Agent Campaign and one is for VRU Campaign.

Set Up Routing Scripts

Use the Script Editor application to create a reservation script that uses the dialed number for the Outbound Routing Type and routes through one of the following methods:

- Using a Select node to the previously configured skill group.
- Using Dynamic Route Target by ID in the Skill Group node.

Before beginning this procedure, you must create and configure a skill group. For information about creating skill groups, see the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/en/US/products/ps12586/tsd_products_support_series_home.html.

The following sections contain diagrams displaying sample routing scripts.

Script for Agent Campaign Without Personal Callback

The following steps and accompanying diagrams provide an example of how to create a script for an agent campaign without personal callback.

Procedure

Step 1 Using the **Dialed Number** tool, associate the Outbound Voice dialed numbers with the configured call type.

Step 2 Using the **Call Type Manager** in **Script Editor**, associate the MR dialed numbers with the configured call type and newly created reservation script.

Figure 16: Sample Script for Agent Campaign Without Personal Callback (Using Select Node)

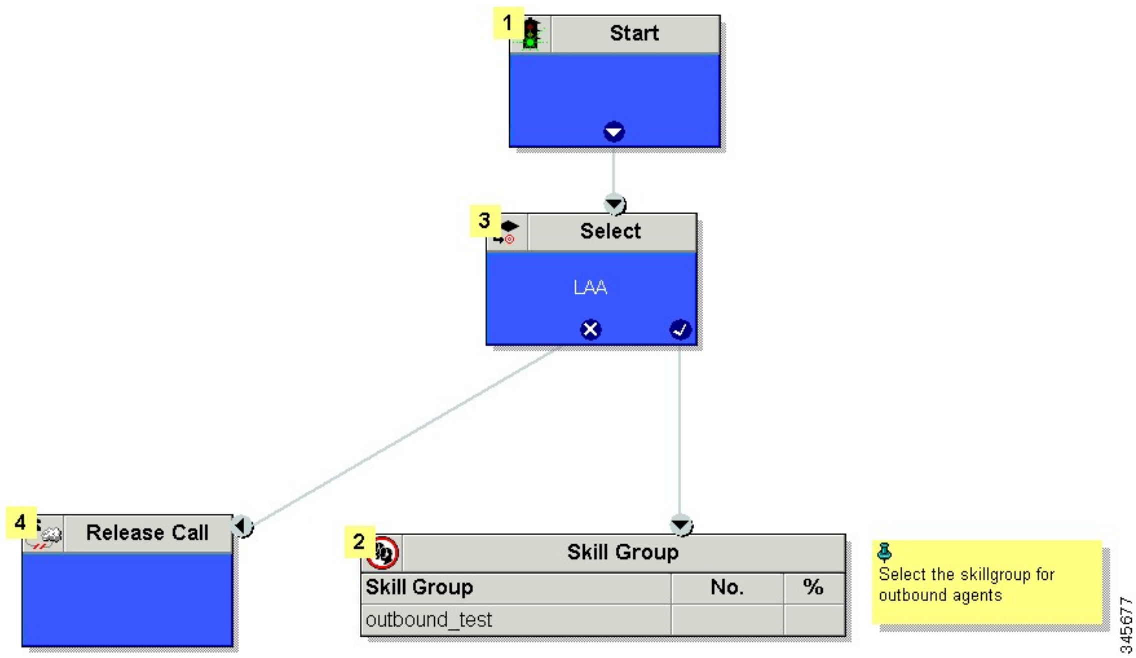
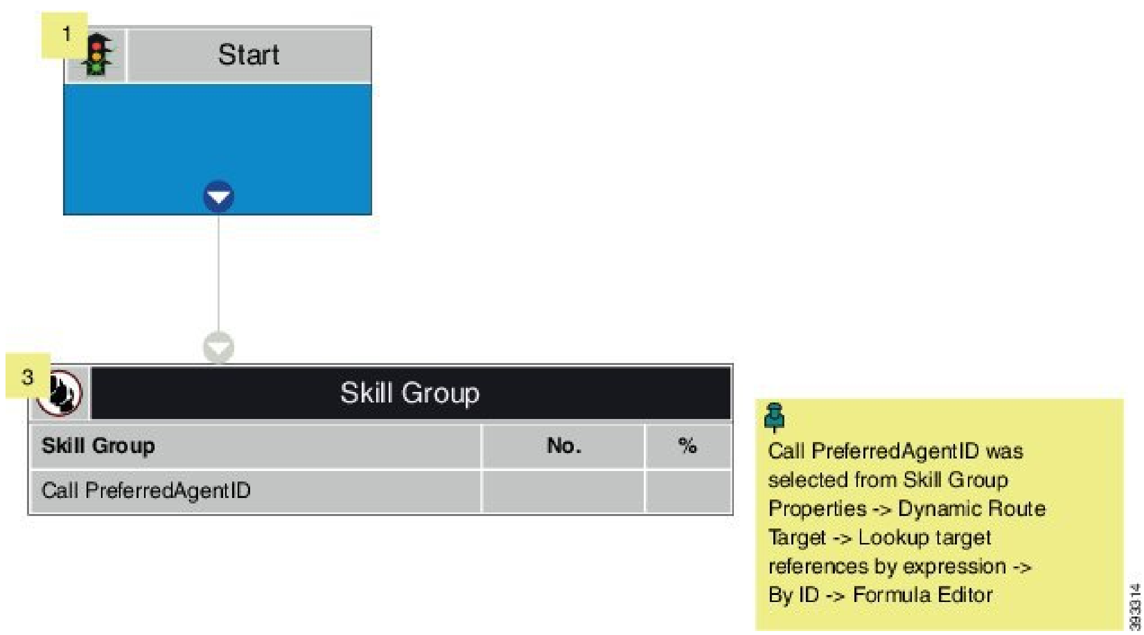


Figure 17: Sample Script for Agent Campaign Without Personal Callback (Using Dynamic Route Target by ID)



Script for Agent Campaign with Personal Callback

The following steps and accompanying diagram provide an example of how to create a script for an agent campaign with personal callback.

Include the following nodes:

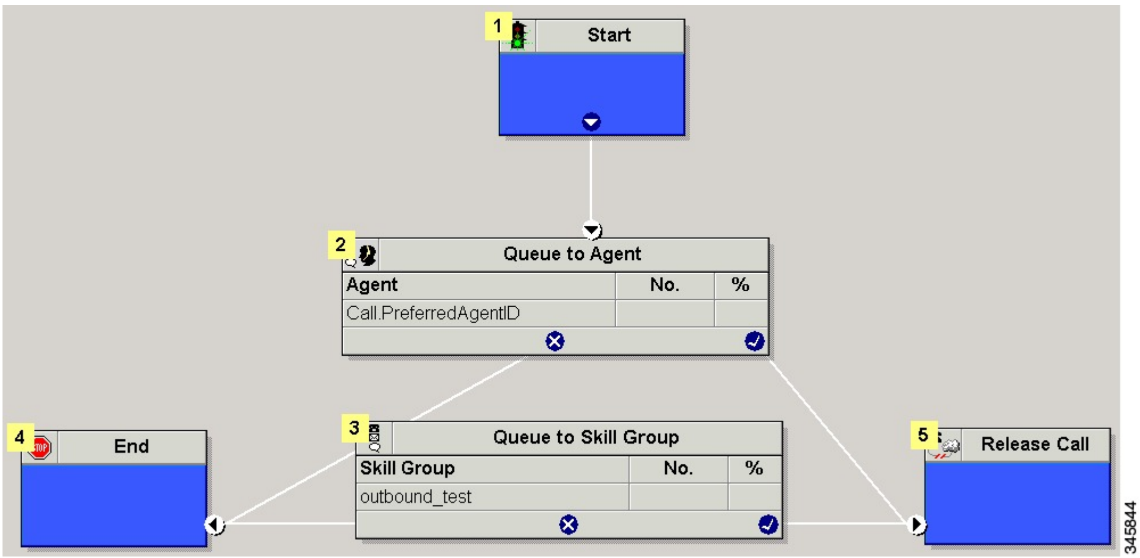
- Add a queue-to-agent node.
- Add a Queue to Skill Group Node after the Queue to Agent Node. Use a skill group that handles outbound calls.
- End the script in a release call node for a successful case; otherwise end the script with the END node.

Procedure

Step 1 Using the Dialed Number tool, associate the Outbound Voice dialed numbers and Personal Callback dialed numbers with the configured call type.

Step 2 Using the Script Editor Call Type Manager, associate the call type with the newly created reservation script.

Figure 18: Sample Script for Agent Campaign with Personal Callback



Configure Queue to Agent Node

Procedure

Step 1 In **Script Editor**, double-click the **Queue to Agent** node.

Step 2 In the **Agent Expression** column, enter `Call.PreferredAgentID`.

Step 3 Confirm that the **Peripheral** column is left blank.

Step 4 Click **OK** to save the **Queue to Agent** node.

Step 5 Save and then schedule the script. When scheduling the script, use the call type that is configured for personal callback.

For more information about script scheduling, see the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/en/US/products/ps12586/tsd_products_support_series_home.html.

Script for VRU Campaign

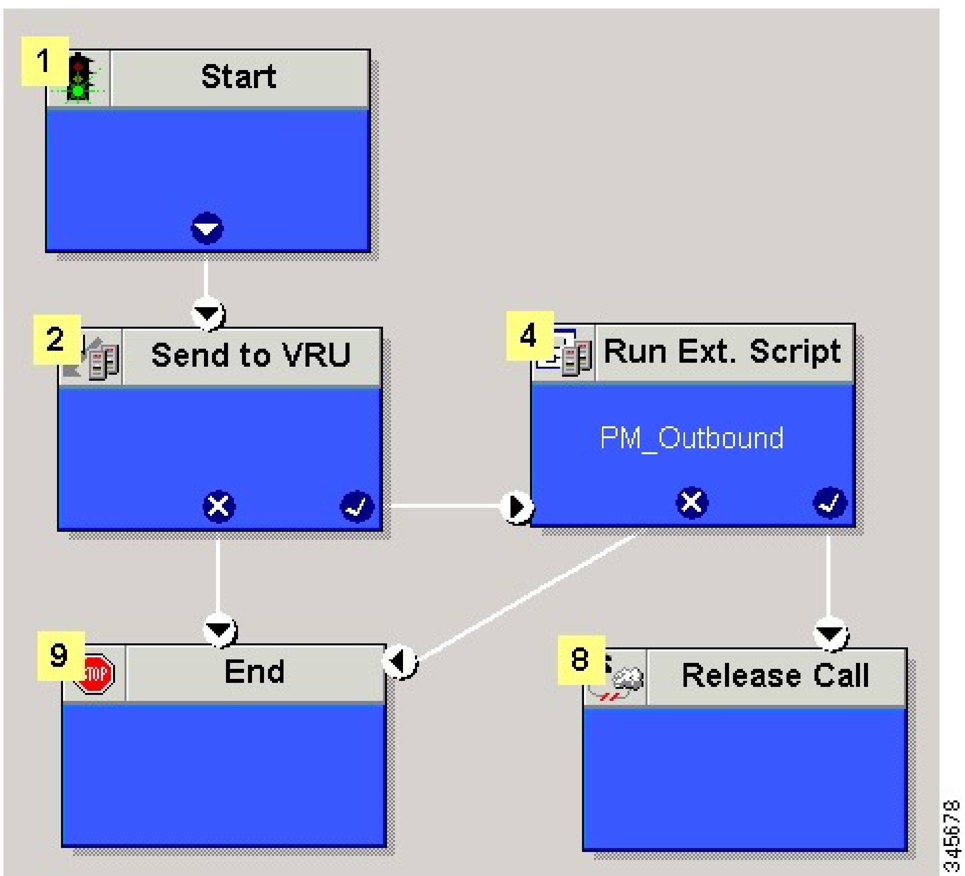
The following steps and accompanying diagram provide an example of how to create a script for a VRU campaign.

Procedure

Step 1 Using the Dialed Number tool, associate the Outbound Voice dialed numbers with the configured call type.

Step 2 Using the Script Editor Call Type Manager, associate the call type with the newly created reservation script.

Figure 19: Sample Script for VRU Campaign



SIP Dialer Recording Parameters Configuration

When recording is enabled in a campaign, the number of recording files that result can be large. The following table lists registry settings that you can adjust to regulate the number of recording sessions and the maximum recording file size.

Registry Setting	Default Setting	Description
MaxAllRecordFiles	500,000,000	The maximum recording file size (in bytes) of all recording files.
MaxMediaTerminationSessions	200	The maximum number of media termination sessions if recording is enabled in the Campaign configuration.
MaxPurgeRecordFiles	100,000,000	The maximum recording file size (in bytes) when the total recording file size, MaxAllRecordFiles, is reached.
MaxRecordingSessions	100	The maximum number of recording sessions if recording is enabled in the Campaign configuration.

Recording files are in the `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\`*`<customer instance>`*`\Dialer directory`.

Note Only the G.711 codec is supported for recording. To record outbound calls, configure the G.711 on the voice gateway.

Verification of Dialed Number

Outbound Option places agents in the Reserved state before using them for an outbound call. The dialer uses the dialed number to route to an agent. The following procedure describes how to verify that this mechanism works properly.

Verify DN Configuration

When an Outbound Option Dialer is installed in a Unified CCE environment, the dialer uses the dialed number to make routing requests through the Media Routing (MR) Peripheral Gateway. The following verification steps assume that you have completed all the applicable configuration and reservation script generation.

Procedure

Step 1 Log in an agent to a skill group participating in an outbound campaign, and make the agent available. (Note the dialed number, which was configured in the Skill Group Selection tab in the Campaign component.) If a different dialed number is used for predictive and preview calls, make sure to verify both dialed numbers.

Step 2 Run the Script Editor application and select the **Call Tracer** utility from the **Script** > **Call Tracer** menu. Select the routing client that is associated with the MR PG and select the Dialed Number.

Step 3 Press **Send Call** to simulate a route request and note the results. If a label was returned for the agent who was logged in above, the reservation script is working properly and the dialer can reserve agents through this script.

Verify Campaign Configuration

As a final step to verify that you configured your Outbound Option campaign correctly, create a small campaign of one or two entries that dial work phones or your mobile phone.

Campaign Management

Single Campaign Versus Multiple Campaigns

You might choose to run multiple campaigns because of different calling policies (for example, time rules) or to run different outbound modes simultaneously.

From the perspective of dialer port allocation, running fewer campaigns with a larger agent pool is more efficient. Dialer ports are allocated based on the number of agents assigned and the current number of lines per agent to dial. The more campaigns you have that are active, the more the ports are distributed across the campaigns, which affects overall efficiency.

Results from Individual Customers

After running a campaign, you can generate a list of customers who were reached, not reached, or have invalid phone numbers.

Interpret Information from Dialer_Detail Table

The Dialer_Detail table is a single table that contains the customer call results for all campaigns. When you view the Dialer_Detail table, note that each attempted Outbound Option call is recorded as an entry in the table. Each entry lists the number called and which numbers are invalid.

For more information, see the appendix on the Dialer Detail Table.

Management of Campaign Manager Database Tables

The Campaign Manager tables, Dialing_List and Personal_Callback_List can grow to be large. If the database size grows too large, Campaign Manager performance can significantly slow down. To limit the size of the Outbound Option database, a stored procedure is run daily at midnight to purge records that are no longer needed.

By default, records are removed from the Personal_Callback_List table when the record's **CallStatus** is either C, M, or D, and the **CallbackDateTime** for the record is more than five days old. In the Dialing_List table, records are removed by default when **CallStatusZone1** has a value of either C, M, or D, and **ImportRuleDate** is more than five days old.

You can change the status and age of the records to be removed by modifying the Campaign Manager registry values on the Logger machine. The registry settings are located in HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\LoggerA\BlendedAgent\CurrentVersion in the Outbound Option registry.

- To specify the records to remove from the Personal_Callback_List table, set **PersonalCallbackCallStatusToPurge** and **PersonalCallbackDaysToPurgeOldRecords**.

> **Note** **PersonalCallbackCallStatusToPurge** is not added by default. To change the call status of the records to remove, create this registry setting manually.

- To specify the records to remove from the Dialing_List table, set **DialingListCallStatusToPurge** and **DialingListDaysToPurgeOldRecords**.

> **Note** **DialingListCallStatusToPurge** is not added by default. To change the call status of the records to remove, create this registry setting manually.

To specify the age of the records to be removed, set **PersonalCallbackDaysToPurgeOldRecords** or **DialingListDaysToPurgeOldRecords** to specify the number of days to keep the record before it is removed. For the Personal Callback list, this value is the number of days after the personal callback is scheduled (CallbackDateTime). For the Dialing List, this value is the number of days after the record is imported (ImportRuleDate). The default is 5. The valid range is 1 to 30. If the value is not set or set to 0, the automated purge is disabled.

To set the call status of the records to be removed, set **PersonalCallbackCallStatusToPurge** or **DialingListCallStatusToPurge** to a string containing the call status types to apply when purging personal callback or dialing list records. For example, if the string contains "C,M,F,L,I," all records with these call statuses, that are also older than the number of days specified by **PersonalCallbackDaysToPurgeOldRecords** or **DialingListDaysToPurgeOldRecords**, are removed from the database.

You can specify the following call status values:

Value	Description
U	Unknown
F	Fax
I	Invalid Number
O	Operator
L	Not Allocated
X	Agent Not Available
C	Closed
M	Max Calls
D	Dialed

Management of Predictive Campaigns

The following sections provide guidelines to follow when working with predictive campaigns.

Initial Values for Lines per Agent

Determining the initial value for the number of lines per agent is not as simple as inverting the hit rate. If a campaign has a 20% hit rate, you cannot assume that five lines per agent is the applicable initial value for the campaign if you are targeting a 3% abandon rate. The opportunity for abandoned calls increases geometrically as the lines per agent increases; therefore, set the initial value conservatively in the campaign configuration.

If the reports show that the abandon rate is below target and does not come back in line very quickly, modify the initial value in the campaign configuration to immediately correct the lines per agent being dialed.

End-of-Day Calculation for Abandon Rate

It is not unusual for a campaign to be over the abandon rate target for any given 30 minute period. The dialer examines the end-of-day rate when managing the abandon rate. If the overall abandon rate is over target for the day, the system targets a lower abandon rate for remaining calls until the average abandon rate falls into line. This end-of-day calculation cannot work until after the campaign has been running for one hour. Small sample sizes due to short campaigns or campaigns with fewer agents might not give the dialer enough time to recover from an initial value that is too high.

Similarly, if the campaign is significantly under the target abandon rate, it might begin dialing more frequently with an abandon rate over target for a while to compensate in the abandon rate.

Transfer of Answering Machine Detection Calls to Agents

When enabling the Transfer AMD (Answering Machine Detection) to agent option for an agent campaign or enabling the Transfer AMD to IVR option for an IVR campaign, consider the increase in calls to the target resources (agents or IVR) when determining the initial value. If the expectation is that the AMD rate and the live voice rate are over 50%, perhaps start out with an initial value of 1.1 or even one line per agent to stay under a 3% abandon rate.

Management of Agent Idle Time

One of the key reporting metrics for administrators managing campaigns is the amount of time agents spend idle between calls.

There are many possible reasons for longer idle times, such as a combination of one or more of the following:

- A dialing list with a low hit rate. The solution is to create an improved list.
- A small agent pool results in fewer calls, resulting in slower adjustments. One solution is to add more agents to the pool.
- Shorter average handle times means agents become available more frequently. A shorter handle time means that the agent idle time percentage will climb.
- Not enough dialer ports deployed or too many agents. Deploy more ports or use fewer agents.
- A large number of retry attempts at the beginning of a day when running with append imports resulting in lower hit rates. Prioritize pending over retries.
- Modifying the maximum number of attempts up or down in an active campaign. This activity can interrupt the Campaign Manager’s processing of dialer requests for records, as mentioned earlier in this chapter. One solution is to perform the activity during off hours.
- Running out of records to dial. Import new records.

Sources of Higher Idle Times in Reports

The following Outbound Option reports provide information regarding sources of higher idle times:

- Campaign Consolidated Reports: These reports provide a very useful overview of a campaign by combining campaign and agent skill group statistics into a single report. They provide average idle time, campaign hit rate, the number of agents working on the campaign, as well as their Average Handle Time per call. Low hit rates and low average handle times result in more work for the dialer to keep those agents busy.

- Dialer Capacity Reports: These reports show how busy the dialers are and how much time was spent at full capacity when the dialer was out of ports. They also provide the average reservation call time as well as the average time each dialer port spent contacting customers.

Dialer Saturation

If both Dialers have relatively low idle times and high all ports busy times, then it is likely the Dialers have been oversubscribed. The combination of number of agents, Dialing List hit rate, and average handle time are likely more than the deployed number of ports the Dialer can handle.

To solve this problem, perform one of the following actions:

- Reduce the number of agents working on the campaign.
- Add more Dialer ports to the solution.

Few Available Records

Call Summary Count reports show how many records in the aggregate campaign dialing lists have been closed and how many are still available to dial.

Reports

This section provides an overview of the Outbound Option reports available in the Cisco Unified Intelligence Center.

For detailed report template descriptions, see the *Cisco Packaged Contact Center Enterprise Reporting User Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

For directions on importing report templates into Cisco Unified Intelligence Center and configuring Cisco Unified Intelligence Center data sources for Packaged CCE, 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.

Outbound Option Reports

This section describes the Outbound Option reports, created using the Unified Intelligence Center.

- Outbound Historical Reports Bundle, on page 138
- Outbound Realtime Reports Bundle, on page 139
- Agent Reports, on page 139
- Campaign and Dialer Reports, on page 140
- Skill Group Reports, on page 141

Additionally, sample custom report templates are available from the Cisco Developer Network (https://developer.cisco.com/web/ccr/documentation.)

Note Call Type reporting can be used on Outbound Option reservation calls and transfer to VRU calls. Call Type reporting is not applicable for outbound customer calls because a routing script is not used.

Outbound Historical Reports Bundle

The Outbound Options Historical reports receive data from the historical data source. Reports are populated with interval data that has a default refresh rate of 15 minutes.

Half-hour/Daily: Provides statistics for each half-hour period. Many of the half-hour reports are also available in a daily report format.

The Outbound Historical bundle contains the following reports:

Report	Description
Attempts per Campaign Daily	Shows the status (summary and percentage) of each campaign for the selected time period and the breakdown of attempts (in percentage) of each campaign for the selected time period.
Campaign Consolidated Daily	Shows the daily activity and performance of the selected campaigns and their skill groups for the selected time period and provides analysis of the actual customer calls (outbound calls which reached live voice, inbound calls, or calls transferred to the campaign's skill group) for the selected campaigns and their skill groups for the selected time period.
Campaign Consolidated Half Hour	Shows the list of Consolidated Calls and Agent Statistics per Campaign by Half Hour and Breakdown of completed calls.
Campaign Half Hour Summary	Shows the status for all campaigns for the selected time period, the status (summary and percentage) of each campaign for the selected time period and the breakdown of attempts (in percentage) of each campaign for the selected time period.
Dialer Call Result Summary Half Hour Dialer Capacity Daily Dialer Capacity Half Hour	Shows the status of each dialer for the selected time period.
Import Rule	Shows the status of imported records for the selected time period.
Query Rule Within Campaign Daily	Shows the breakdown of attempts (in percentage) of each campaign for the selected time period and the status (summary and percentage) of each campaign for the selected time period.

Outbound Realtime Reports Bundle

The Outbound Option Real Time reports display current information about a system entity; for example, the number of tasks an agent is currently working on or the number of agents currently logged in to a skill group. By default, the reports automatically query the Admin Workstation database on the distributor every 15 seconds. The data is written to the database by the Router almost every 10 seconds.

The Outbound Real Time Reports Bundle contains the following reports:

Report	Description
Call Summary Count per Campaign Real Time	Shows status of all campaign records, and the currently valid campaign dialing times.
Dialer Real Time	Shows the status of each dialer, including the number of contacts dialed today and the result of each attempt.
Import Status Real Time	Shows the status of Outbound Option import records.

Agent Reports

In addition to the reports contained in the Outbound Reports bundles, other Agent reports also provide information about Outbound activities:

Report	Outbound Option Fields
Agent Queue Real-Time Agent Real-Time Agent Skill Group Real-Time Agent Team Real-Time	The **Direction** field indicates the direction of the call that the agent is currently working on including Other Out/Outbound Direct Preview, Outbound Reserve, Outbound Preview, or Outbound Predictive/Progressive. The **Destination** field indicates the type of outbound task on which the agent is currently working.
Agent Team State Counts	The **Active Out** field shows the number of agents currently working on outbound tasks.
Agent State Real Time Graph	For agents handling Outbound Option calls, the **Hold** state indicates that the agent has been reserved for a call. The Outbound Dialer puts the agent on hold while connecting the call.

Interpreting agent data for Outbound Option tasks, requires understanding how Outbound Option reserves agents, reports calls that are connected to agents, and handles calls that are dropped by customers before the calls are connected.

The Outbound Option Dialer assigns and connects calls differently than regular contact center enterprise routing. Report data for agents handling Outbound Option calls therefore differs from data for agents handling typical voice calls and multichannel tasks.

When the Outbound Dialer calls a customer, it reserves the agent to handle the call. The Dialer places a reservation call to the agent and changes the agent's state to Hold. This reservation call is reported as a Direct In call to the agent.

For typical calls, the agent is placed into Reserved state when the contact center reserves the agent to handle a call. For Outbound Option calls, reports show the agent in Hold state when reserved for a call and the time that agent spends reserved is reported as Hold Time.

When the customer answers the call, the Outbound Option Dialer transfers the call to an agent. The call is now reported as a Transfer In call to the agent. When the customer call is transferred to the agent, the Dialer drops the reservation call and classifies it as Abandon on Hold.

The abandoned call wait time, set in the Campaign Configuration screen, determines how calls are reported if the caller ends the call. Calls are counted in the Customer Abandon field in both Real Time and Historical campaign query templates only if the customer ends the call before the abandoned call wait time is reached.

For agent reporting per campaign, Outbound Option provides reports that accurately represent the Outbound Option agent activity for a contact center, including information grouped by skill group.

The following list describes the data that are presented in the agent reports.

- A real-time table that shows Outbound Option agent activity that is related to Outbound Option calls.
- A historical table that shows agent daily performance for Outbound Option predictive calls, by skill group.
- A historical table that shows agent daily performance for Outbound Option preview calls, by skill group.
- A historical table that shows agent daily performance for Outbound Option reservation calls, by skill group.

Campaign and Dialer Reports

Outbound Option provides a campaign report template that describes the effectiveness of a campaign and the dialer. This list can be used for Agent and VRU campaigns.

Observe the following guidelines when using the campaign reports:

- Campaign Real Time reports describe how many records are left in the campaign dialing list.
- Both Campaign and Dialer Half Hour reports provide the call result counts.

Note Campaign Real Time reports capture call results since the last Campaign Manager restart only. If the Campaign Manager restarts, data collected before the restart is lost.

Note When the active Campaign Manager fails over, partial campaign interval reports are generated for the relevant interval based on the data that was available after failover. Some of the campaign statistics collected prior to failover will be missing.

The campaign interval tables used in Reporting are impacted due to this scenario.

The following list describes the data that is presented in the campaign reports.

- A summary of call results for query rules within a campaign since the beginning of the day.
- A summary of call results for a campaign since the beginning of the day. It includes a summary of all query rules within the campaign.

- A view of what is configured for valid campaign calling times for zone1 and zone2 for selected campaigns. The times are relative to the customer's time zone.
- A view of what is configured for valid campaign calling times for zone1 and zone2 for selected campaign query rules. The zone times are relative to the customer's time zone. The query rule start and stop times are relative to the Central Controller time.
- How many records for selected query rules have been dialed to completion, and how many records remain.
- How many records for selected campaigns have been dialed to completion, and how many records remain.
- A summary of call results for selected campaign query rules for selected half-hour intervals.
- A summary of call results for all query rules for selected campaigns for selected half-hour intervals.
- A historical table by half-hour/daily report that shows the status (summary and percentage) of each campaign for the selected time period.
- A historical table by breakdown of attempts (in percentage) of each campaign for the selected time period.
- A historical table by half-hour/daily report that shows the status (summary and percentage) per query rule of each campaign for the selected time period.
- A historical table by breakdown of attempts (in percentage) per query rule of each campaign for the selected time period.
- A summary half-hour/daily report that shows activity and performance of the selected campaigns and their skill group for the selected time period, including abandon rate, hit rate, and agent idle times.
- A historical table by breakdown of actual customer calls (outbound calls which reached live voice, inbound calls, or calls transferred to the campaign skill group) for the selected campaigns and their skill groups for the selected time period.

Dialer Reports

The Outbound Option Dialer reports provide information about the dialer. These reports include information about performance andresource usage. The templates also enable you to determine whether you need more dialer ports to support more outbound calls.

The following list describes the data presented in the Outbound Option Dialer reports:

- A real-time table that shows contact, busy, voice, answering machine, and special information tone (SIT) detection for each dialer. A SIT consists of three rising tones indicating a call has failed.
- An historical table that records contact, busy, voice, answering machine, and SIT Tone detection for each dialer by half-hour intervals.
- Displays information about the amount of time the dialer was idle or had all ports busy.
- Displays Dialer status on a port-by-port basis used for troubleshooting. If this report does not display any records, then the data feed is disabled by default. It is only enabled for troubleshooting purposes.

Skill Group Reports

For skill group reporting per campaign, Outbound Option provides reports that represent the skill group activity for a contact center.

The following list describes the data presented in the skill group reports:

- A real-time table that shows all skill groups and their associated Outbound Option status.
- A historical table that records Outbound Option counts for the agent states *signed on*, *handle*, *talk*, and *hold* by half-hour intervals.

CHAPTER 11

Post Call Survey

Capabilities

A Post Call Survey takes place after usual call treatment. It is typically used to determine whether customers are satisfied with their call center experiences. This feature lets you configure a call flow that, after the agent disconnects from the caller, optionally sends the call to a Dialed Number configured for a Post Call Survey.

The Unified CCE script can enable and disable Post Call Survey on a per-call basis by testing for conditions and setting an expanded call variable that controls post call survey. For example, the script can invoke a prompt that asks callers whether they want to participate in a survey. Based on the caller's response, the script can set the expanded call variable that controls whether the call gets transferred to the Post Call Survey dialed number.

The Post Call Survey call works just like a regular call from the Unified CCE point of view. Scripts can be invoked and the customer can use the keypad on a touch tone phone and/or voice with ASR/TTS to respond to questions asked during the survey. During Post Call Survey, the call context information is retrieved from the original customer call.

Note The call context for the post call survey includes all context up to the point where the call is transferred to the agent. Context that the agent creates after the transfer is not included in the post call survey context.

Design Considerations

Observe the following conditions when designing the Post Call Survey feature:

- A Post Call Survey is triggered by the hang-up event from the last agent. When the agent ends the call, the call routing script launches a survey script.
- The mapping of a dialed number pattern to a Post Call Survey number enables the Post Call Survey feature for the call.

- The value of the expanded call variable **user.microapp.isPostCallSurvey** controls whether the call is transferred to the Post Call Survey number.
    - If **user.microapp.isPostCallSurvey** is set to **y** (the implied default), the call is transferred to the mapped post call survey number.
    - If **user.microapp.isPostCallSurvey** is set to **n**, the call ends.
    - To route all calls in the dialed number pattern to the survey, your script does not have to set the **user.microapp.isPostCallSurvey** variable. The variable is set to **y** by default.
- REFER call flows are not supported with Post Call Survey. The two features conflict: REFER call flows remove Unified CVP from the call and Post Call Survey needs Unified CVP because the agent has already disconnected.
- For Unified CCE reporting purposes, when a survey is initiated, the call context of the customer call that was just transferred to the agent is replicated into the call context of the Post Call Survey call.

Initial Setup

To set up the Post Call Survey feature:

Procedure

Step 1 Create one or more survey scripts and add the files to the CVP media servers. See Create a Survey Script, on page 144.

Step 2 Configure Unified CCE for Post Call Survey. This step adds a required expanded call context variable, adds a new call type for Post Call Survey, maps incoming dialed number to a survey dialed number pattern, and associates your survey dialed number patterns to the survey call type. See Configure Packaged CCE for Post Call Survey, on page 145.

Step 3 Modify your Unified CCE call routing scripts to launch the survey scripts. See Modify CCE Scripts for Post Call Survey, on page 147.

The scripts can optionally contain nodes that test for conditions and dynamically control whether a call is transferred to the survey.

Create a Survey Script

To create a survey script or application that queries the caller for information, use the CVP Call Studio tool. For more information on Unified CVP Call Studio, see User Guide for Cisco Unified CVP VXML Server and Unified Call Studio.

What to do next

Map CVP dialed number patterns to the survey script numbers.

Configure Packaged CCE for Post Call Survey

You can enable and disable Post Call Survey within a CCE routing script by using the ECC variable **variableuser.microapp.isPostCallSurvey**. A value of *n* or *y* disables and enables the feature. (The value is case-insensitive.)

Configure the ECC variable to a value of n or y before either the label node or the Queue to Skillgroup node. This configuration sends the correct value to Unified CVP before the agent transfer. This ECC variable is not needed to initiate a Post Call Survey call, but you can use it to control the feature once Post Call Survey is configured in the Unified CCE Administration. Dialed Number is mapped to the Post Call Survey Dialed Number patter to automatically transfer the call.

Note

- The Post Call Survey DN is called if the Unified CVP has received at least one CONNECT message from CCE (either from the VRU leg or from the Agent leg). Use the END node in your CCE routing script if the Post Call Survey is not required for the calls disconnected from the IVR.
- If Router Requery is configured incorrectly and the Ring-No-Answer timeout expires, the caller is still transferred to the Post Call Survey DN. This can occur if a Queue node is used and Enable target requery is not checked.

Procedure

Step 1 In Unified CCE Administration, navigate to **Overview** > **Call Settings** > **Route Settings** > **Expanded Call Variables**.

Step 2 Click **New** to open the **New Expanded Call Variable** window.

Step 3 Create a new ECC variable with **Name:**`user.microapp.isPostCallSurvey`.

Step 4 Set **Max Length:** to 1.

Step 5 Check the **Enabled** checkbox. Then click **Save**.

In your CCE routing scripts, remember that, at script start, the default behavior of Post Call Survey equals **enabled**, even if **user.microapp.isPostCallSurvey** has not yet been set in the script. You can turn **off** Post Call Survey in the script by setting **user.microapp.isPostCallSurvey** to *n*. You can later enable Post Call Survey in the same path of the script by setting this variable to *y*.

Step 6 Navigate to **Overview** > **Call Settings** > **Route Settings** > **Call Types**.

Step 7 Add the call type for Post Call Survey, and click **Save**.

Step 8 Navigate to **Overview** > **Call Settings** > **Route Settings** > **Dialed Numbers**.

Step 9 Click **New** and complete the following fields:

Field	Required?	Description
Dialed Number String	yes	The value used to route the call, which is the Post Call Survey Dialed Number. Enter a string value that is unique for the routing type, maximum of 25 characters. **Note** The **External Voice** and **Post Call Survey** routing types must not have the same dialed number strings for the same site.

Field	Required?	Description
Description	no	Enter a maximum of 255 characters to describe the dialed number string.
Department	yes (for departmental administrators)	A departmental administrator must select one department from the popup list to associate with this dialed number. The list shows all this administrator's departments. When a departmental administrator selects a department for the dialed number, the popup list for call type includes global call types and call types in the same department as the dialed number. A global administrator can leave this field as Global (the default), which sets the dialed number as global (belonging to no departments). A global administrator can also select a department for this Dialed Number. When an administrator changes the department, selections for call type are cleared if the selections do not belong to the new department or the global department.
Routing Type	yes	From the drop-down menu, select **Post Call Survey:** . **Post Call Survey:** Select this option for Post Call Survey dialed number strings that apply to voice calls coming from Cisco Unified Customer Voice Portal (CVP). This option is similar to External Voice where the calls comes from outside of the enterprise through a gateway. However, Unified CVP directs the calls internally to Post Call Survey after agent ends the call. This option allows you to enter the Post Call Survey Dialed Number and associate the Dialed Number Patterns to the Post Call Survey Dialed Number. For remote sites, the **Post Call Survey** option is available if the site is configured to VRU PG.
Media Routing Domain	no	The Media Routing Domain associated with the dialed number. Media Routing Domains (MRDs) organize how requests for media are routed. The system routes calls to agents who are associated with a particular communication medium; for example, voice or email. The selection of Routing Type determines what appears in this field. • If the Routing Type is External Voice, Internal Voice, or Outbound Voice, the Media Routing Domain is Cisco_Voice and you cannot change it. • If the Routing Type is Multichannel, click the **magnifying glass** icon to display the **Select Media Routing Domain** popup window.
Call Type	no	Use the drop-down menu to select the call type that you created for Post Call Survey.

Field	Required?	Description
PCS Enabled Dialed Number Patterns	no	**Note** The **PCS Enabled Dialed Number Patterns** field appears if the **Routing Type** is **Post Call Survey**. Enter one or more dialed number patterns that allow calls to transfer to the Post Call Survey dialed number entered in the **Dialed Number String** field. The field allows maximum of 512 characters that can have the comma separated list without any spaces. Both alphanumeric and special characters are supported.
Ringtone Media File	no	**Note** The **Ringtone Media File** field appears if the **Routing Type** is **External Voice**. Enter filename of the custom ringtone - maximum of 256 characters without any spaces.

Step 10 Click **Save**.

Step 11 Restart the active generic PG (side A or B) to register the new ECC variable.

If the ECC variable already existed, you can skip this step.

Note The **user.microapp.isPostCallSurvey** setting takes effect on Unified CVP only when it receives a connect or temporary connect message. Therefore, if you do not want the survey to run, without first reaching an agent (such as 'after hours of treatment'), you must set the isPostCallSurvey to *n* before the initial 'Run script request'.

Modify CCE Scripts for Post Call Survey

In Script Editor, modify your CCE call routing scripts for incoming calls as follows:

- Add nodes to invoke the call studio survey script, if needed. The following notes explain when you might need to explicitly add nodes to call the survey script.

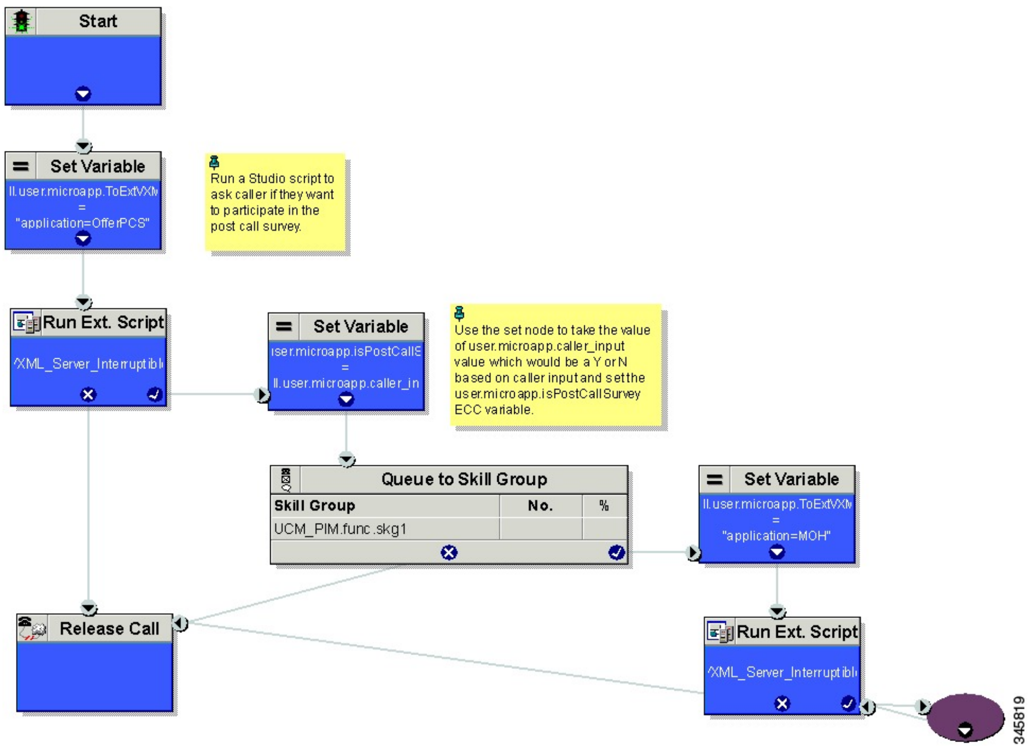
  If a DN is mapped for Post Call Survey, the call is automatically transferred to the configured Post Call Survey dialed number.

  Note The Post Call Survey dialed number is only called if the script ends with a call to an agent. If the script completes without going to an agent then the call is not directed to the Post Call Survey dialed number . In these cases, you can, for example, use a *Send to Script* node in your Unified CCE script to direct the call to the Post Call Survey script.

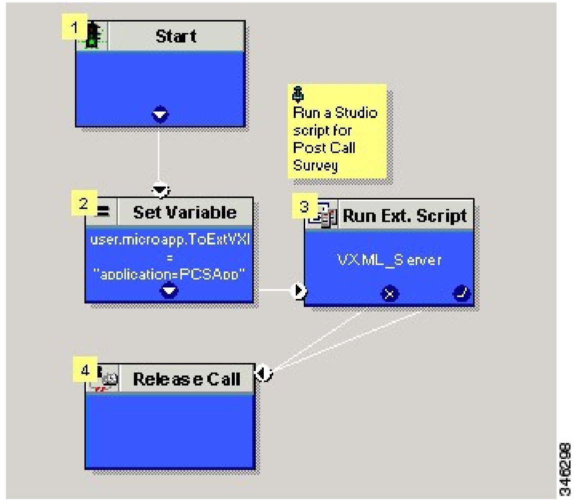
- Optionally, you can add nodes in the script to test for conditions for which you want to turn the survey off.

- To dynamically control whether the survey is offered to callers, you must explicitly set the **user.microapp.isPostCallSurvey** expanded call context variable to **y** and **n**.
- To offer the survey to all callers, you do not need to set the variable in the script. It is set to **y** by default.
- Configure the expanded call context variable to a value of *n* or *y* before the Queue to Skillgroup node. This sends the correct value to Unified CVP before the agent transfer.

The following example calls a script that asks callers if they want to participate in a survey. The script then sets the **user.microapp.isPostCallSurvey** variable according to the caller's response.



Create a routing script for the Post Call Survey Call Type to play your survey script or application to the caller. The following script is an example:



Administration and Usage

Get Survey Results

For reporting purposes, in both the CVP and the CCE databases, a post call survey call has the same RouterCallKey, Call GUID, and call context as the original inbound call.

To obtain survey results, you query or create a report that gathers survey data from the CVP database.

For more information on how to configure a Data Source, 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.

Procedure

Step 1 In Cisco Unified Intelligence Center Reporting tool, connect to the CVP database.

Step 2 Create a query that identifies survey calls, gathers call information from those calls, and extracts data related to specific survey dialed numbers:

a) In the Call_Type table, test for Event_Type = Post_Call_Survey.
b) If true, use that entry's call information to query the VXML_Element table and get the VXML data for the call.
c) In the VXML data, you can identify the exact survey that a caller participated in from the dialed number used to place the Post Call Survey.

Step 3 To report on the results of a particular survey, collate the VXML data for all calls with that survey's dialed number.

Step 4 To identify answers to survey questions, in the CauseRef table, the CauseID is 20, and the Cause is Post Call Answer.

CHAPTER 12

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 Packaged 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.

This is only applicable for Unified CCE deployment.

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

Packaged CCE supports single sign-on for these reference designs:

- 2000 Agents
- 4000 Agents
- 12000 Agents

Coresidency of Cisco Identity Service by Reference Design

Reference Design	Packaged CCE Solution
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

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.
- 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 12: 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
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

Operation	Allowed on Publisher	Allowed on Subscriber
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 Flow

Single sign-on (SSO) configuration by an administrator follows this flow:

Procedure

Step 1 Install the appropriate release of Packaged CCE. For more information, see 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

Step 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

For Packaged CCE deployments, the Cisco IdS is installed as a service on the Unified Intelligence Center VMs.

Step 3 Install and configure the Identity Provider (IdP).

Step 4 Configure System Inventory.

Step 5 Configure the Cisco IdS.

Step 6 Register and test SSO-compatible components with the Cisco IdS.

Step 7 Choose the SSO mode.

Step 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.

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.

Note For a current list of supported Identity Provider products and versions, see the *Contact Center Enterprise Compatibility Matrix*.

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 155
2	Set Authentication Type. See Authentication Types, on page 156.
3	Configure an Identity Provider (IdP), on page 155
4	Enable Signed SAML Assertions, on page 159
5	Optionally Customize the AD FS Sign-In Page in Windows Server to Allow User ID, on page 159

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

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.

Note The Secure Hash Algorithm (SHA) used for signature verification between:

- IdP and Cisco IdS: SHA-1, SHA-256
- Cisco IdS and the application browsers: SHA-256

Configure SAML Certificate Secure Hash Algorithm from SHA-1 to SHA-256

This procedure is useful for upgrades from version 11.x where the only Secure Hash Algorithm supported was SHA-1.

.

Perform this procedure after the upgrade has completed successfully.

Procedure

Step 1 From browser in AD FS Server, login to Cisco IdS admin interface `https://<Cisco IdS server address>:8553/idsadmin`.

Step 2 Click **Settings**.

Step 3 Click **Security** tab.

Step 4 Click **Keys and Certificates**.

Note After this step, Single Sign On will stop working until you complete Step 8.

Step 5 Regenerate SAML Certificate with SHA-256 Secure Hash Algorithm. In the SAML Certificate section, change Secure Hash algorithm dropdown menu to SHA-256 and then click **Regenerate** button

Step 6 Download new metadata file. Click on **IdS Trust** tab and then click download button.

Step 7 Change Secure Hash Algorithm in AD FS Relaying Party Trust configuration. In AD FS server, open AD FS Management. Go to **ADFS** ->**Trust Relationships**->**Relying Party Trusts**, right click on existing Relying Party Trust for Cisco IdS and then click on Properties. In the Advanced Tab, change the Secure Hash Algorithm to **SHA-256.** Click **Apply**.

Step 8 Update Relying party trust on AD FS. From AD FS Server, run the following Powershell command:

```
Update-AdfsRelyingPartyTrust -MetadataFile <path to Step 6 new MetaData File> -TargetName
        <Relying Party Trust Display Name>
```

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 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.

Integrate Cisco IdS to the Shared Management 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**.

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, configure the following:

Field	Description
Display name	The unique name of the identifier.
Relying party identifier	FQDN of the publisher node of Cisco Identity Server from which you downloaded the Cisco IdS metadata file.
	FQDN of the subscriber node of Cisco Identity Server.

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 Click **OK**.

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 On the Download SAML SP Metadata and Upload IdP Metadata windows, click Next as you have already established trust relationship between IdP and IdS.

Step 7 On the AD FS authentication window, provide the login credentials.

Step 8 On successful SSO setup, the message "SSO Configuration is tested successfully" is displayed.

Note If you receive the error message "An error occurred", ensure that the claim you created on the AD FS is enabled.

If you receive the error message "IdP configuration error: SAML processing failed", ensure that the rule has the correct names for Ids and AD FS.

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
```

Set the Principal AW for Single Sign On

Note This procedure is applicable only for Packaged CCE 4K or 12K agent reference design.

During deployment, the first SideA AW machine in the CSV file is the Principal AW.

The Principal AW (Admin Workstation) is responsible for managing background tasks that are run periodically to sync configuration with other solution components, such as SSO management, Smart Licensing, etc.

After deployment, you can change the Principal AW by selecting a different AW on the Inventory page. Set the AW on which you make most of your configuration changes as the Principal AW.

Procedure

Step 1 In Unified CCE Administration, choose **Inventory** to open the **Inventory** page.

Step 2 Set the Principal AW:

a) Click the AW that you want to be the Principal AW.

Note You can only specify one Principal AW for each Unified CCE system.

The Edit CCE AW window opens.

b) Check the **PrincipalAW** check box.

c) Enter the Unified CCE Diagnostic Framework Service domain, username, and password.

The credential must be of a domain user who is a member of the local administrator group if the `ADSecurityGroupUpdate` registry key in AW is zero. If the `ADSecurityGroupUpdate` registry key is set to 1, then the user must be available in the Config security group under the instance OU. These credentials must be valid on all CCE components in your deployment (routers, PGs, AWs, and so on).

Note Every time the Active Directory credentials are updated, the credentials configured here must be updated as well.

d) Click **Save**.

Set Up the External HDS for Single Sign-On

If you have an external HDS in 2000 Agent deployments, manually associate it with a default Cisco IdS by performing the following instructions.

Procedure

Step 1 In **Unified CCE Administration**, click **Infrastructure** > **Inventory** to open the **Inventory** page.

Step 2 Click the pencil icon for the External HDS to open the edit machine popup window.

Step 3 Click the Search icon next to **Default Identity Service**.
The **Select Identity Service** popup window opens.

Step 4 Enter the machine name for the Cisco IdS in the **Search** field or choose the Cisco IdS from the list.

Step 5 Click **Save**.

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 that are related to security, identify clients of the Cisco IdS service, and set log levels. If desired, enable Syslog format.

Note In Packaged CCE 4000 or 12000 Agent deployments:

- Unified CCE AW, Unified Intelligence Center, Finesse, and external HDS gets automatically associated with a default Cisco Identity Service (Cisco IdS).
- Make sure that the Principal AW is configured, and is functional before using the Single Sign-On tool in the Unified CCE Administration. Also, add the SSO-capable machines to the Inventory.

In Packaged CCE 2000 Agent deployments, you must manually associate an external HDS with a default Cisco Identity Service (Cisco IdS). For more information, see Set Up the External HDS for Single Sign-On, on page 161.

Procedure

Step 1 In the Unified CCE Administration, choose **Overview** > **Infrastructure Settings** > **Device Configuration** > **Identity Service**.

Note Use a log in name in the format *username@FQDN* to log in to the Unified CCE Administration.

The **Identity Service Nodes**, **Identity Service Settings**, and **Identity Service Clients** tabs appear.

Step 2 Click **Identity Service Nodes**.
You can view the overall Node level and identify which nodes are in service. You can also view 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 3 Click **Identity Service Settings**.

Step 4 Click **Security**.

Step 5 Click **Tokens**.
Enter the duration for the following settings:

- **Refresh Token Expiry** -- Refresh token is used to get new Access tokens. This parameter specifies the duration after which the Refresh token expires. The default value is 10 hours. The minimum value is 2 hours. The maximum is 24 hours.
- **Authorization Code Expiry** -- Authorization code is used to get Access tokens from Cisco IdS. This parameter specifies the duration after which the Authorization code expires. The default value is 1 minute, which is also the minimum. The maximum is 10 minutes.
- **Access Token Expiry** -- Access token contains security credentials used to authorize clients for accessing resource server. This parameter specifies the duration after which the Access token expires. The default value is 60 minutes. The minimum value is 5 minutes. The maximum is 120 minutes.

Step 6 Set the **Encrypt Token** (optional); the default setting is **On**. Use this configuration to secure the tokens as Cisco IdS issues tokens in both plain text or encrypted formats.

Step 7 Click **Save**.

Step 8 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. An Administrator regenerates the Encryption/Signature key when it is exposed or compromised.
- Regenerate the **SAML Certificate** by clicking **Regenerate**. A message appears to say that the SAML certificate regeneration is successful. SAML certificate is regenerated when it expires or when IdS relying party trust configuration on IdP is deleted.

Note Establish the trust relationship again whenever the Encryption keys or SAML certificates are regenerated.

Step 9 Click **Save**.

Step 10 Click **Identity Service Clients**.
On the **Identity Service Clients** tab, you can view the existing Cisco IdS clients, with the client name, client ID, and a redirect URL. To search for a particular client, click the Search icon above the list of names and type the name of client.

Step 11 To add a client on the **Identity Service Clients** tab:

a) Click **New**.
b) Enter the name of client.
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 12 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 13 Click **Identity Service Settings**.

Step 14 Click **Troubleshooting** to perform some optional troubleshooting.

Step 15 From the **Log Level** drop-down list, set the local log level by choosing **Error**, **Warning**, **Info** (the default), **Debug**, or **Trace**.

Step 16 To receive errors in Syslog format, enter the name of the Remote Syslog Server in the **Host** (Optional) field.

Step 17 Click **Save**.

You can now:

- Register components with the Cisco IdS.
- Enable (or disable) SSO for the entire deployment.

Note If SSO is enabled in the deployment, then import all the IdS server nodes certificate into Cisco Finesse, CUIC, and LiveData component trust store.

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-OnOverview** > **Infrastructure Settings** > **Device Configuration** > **Identity Service**.

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.

Single Sign-On and the Agent Tool

When the global SSO-enabled setting is Hybrid, you can use the Unified CCE Administration Agent Tool to enable agents individually for single sign-on.

In the tool, check the **Single Sign-On** check box to require a selected agent to sign in with SSO authentication. For supervisors and for agents with single sign-on (SSO) enabled, the username is the user's Active Directory or SSO account username.

Note The check box is disabled when the global SSO mode is set to SSO or non-SSO.

To update agent records in bulk, use the Bulk Jobs Agent content file.

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 performed, 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 this CLI command.

Browser Settings and Single Sign-On

If you have enabled single sign-on and are using Internet Explorer, Chrome, Edge Chromium (Microsoft Edge), 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.

Browser	Browser options to verify when using SSO
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.
Edge Chromium (Microsoft Edge)	1. Open Microsoft Edge. 2. Click the **Settings and more (Alt+F)** (...) icon. 3. Click **Settings**. 4. On the **Settings** page, click **On startup**, and verify that the **Open a new tab** radio button 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.

If you do not want to migrate a user, delete the row for that user.

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 **Overview** > **Bulk Import**.

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 in the Agent tool in Unified CCE Administration to see the changes.

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.

Globally Disable Single Sign-On

Follow these steps if you need to globally disable single sign-on from either SSO or Hybrid mode.

Important If you later want to migrate agents or supervisors from SSO-enabled to non-SSO:

- You must assign new passwords for agents (using the Unified CCE Administration Agent tool) when you disable the agents for SSO.
- If you change a Cisco Unified Intelligence Center supervisor who was created as SSO-enabled to non-SSO, a new, non-SSO user account is created for the supervisor after the next user synchronization. The older, SSO-enabled supervisor account (in the format SSO\<loginname>) still exists in Cisco Unified Intelligence Center, however, and you must delete it. You must reconfigure the new, non-SSO supervisor user account (that matches the supervisor's SAM account name in Active Directory) in Cisco Unified Intelligence Center Administration Console to set up the supervisor's reports and permissions.

Procedure

Step 1 If the system is in **SSO** mode, change the SSO mode to **Hybrid** in the Unified CCE Administration **Single Sign-On** tool.

Step 2 Disable agents for SSO, and assign the agents new passwords. This step allows the agents to sign into Finesse.

In Unified CCEAdministration, you can update individual agent records using the Agent tool, or update records in bulk using the Bulk Jobs Agent content file.

Step 3 Disable supervisors for SSO. This step allows the supervisors to sign in to Unified CCE Administration to reskill agents.

In Unified CCE Administration, you can update individual supervisor records using the Agent tool, or update records in bulk using the Bulk Jobs Agent content file.

Step 4 After you have updated all of the agent and supervisor records, change the SSO mode to **Non-SSO**.

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 Packaged Contact Center Enterprise	https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/tsd-products-support-series-home.html	Design considerations and guidelines for deploying the Cisco Packaged CCE system.
Virtualization for Cisco Packaged CCE	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html	Information about deploying Packaged CCE (including single sign-on) on VMware.
Release Notes for Cisco Packaged Contact Center Enterprise Solution	https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-release-notes-list.html	New features and changes for this release of the Packaged CCE solution.
Contact Center Enterprise Compatibility Matrix	https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html	Packaged CCE requirements.
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 13

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.

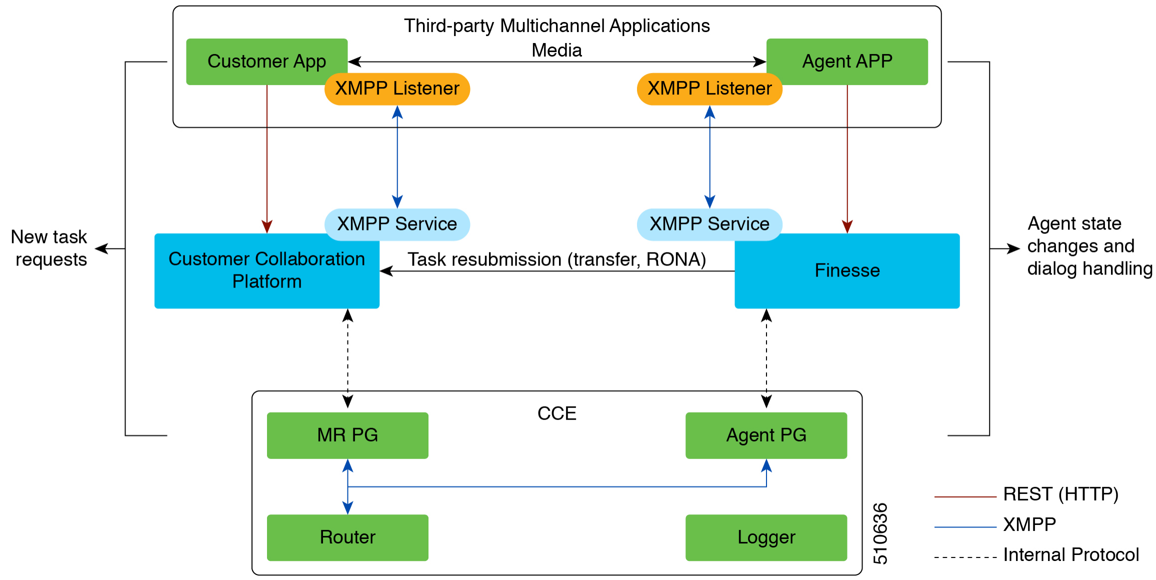
Enterprise Chat and Email provides universal queue out of the box. Third-party multichannel applications can use the universal queue by integrating with CCE through the Task Routing APIs.

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 Customer Collaboration Platform and Finesse APIs in order to use Task Routing. The Customer Collaboration Platform 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 20: Task Routing for Third-party Multichannel Applications Solution Components



Customer Collaboration Platform and Task Routing

Third-party multichannel applications use Customer Collaboration Platform'sTask API to submit nonvoice tasks to CCE.

The API works in conjunction with Customer Collaboration Platform 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 Customer Collaboration Platform. 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 Customer Collaboration Platform 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 Customer Collaboration Platform are required. Install and configure Finesse and Customer Collaboration Platform before configuring the system for Task Routing.

  See the Finesse documentation and Customer Collaboration Platform documentation.

  By default, access to the Customer Collaboration Platform administration user interface is restricted. Administrator can provide access by unblocking the IP addresses of the clients. For more details, see the *Control Customer Collaboration Platform Application Access* topic in the *Cisco Customer Collaboration Platform Installation and Upgrade Guide* guide.

- You can install only one Customer Collaboration Platform machine in the deployment.
- Customer Collaboration Platform must be geographically colocated with the Unified CCE PG on one side.
- Install Customer Collaboration Platform in a location from which CCE, Finesse, and the third-party multichannel Customer Collaboration Platform Task Routing application can access it over the network.

  If you install Customer Collaboration Platform in the DMZ, open a port for CCE and Finesse to connect to it. The default port for CCE to connect to Customer Collaboration Platform is port 38001. Finesse connects to Customer Collaboration Platform over HTTPS, port 443.

  Install the third-party multichannel application locally with Customer Collaboration Platform, or open a port on the Customer Collaboration Platform 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 Customer Collaboration Platform Developer Guide.
- Cisco Finesse Web Services Developer and JavaScript Guide
- Unified CCE Administration Tools, on page 194

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 Customer Collaboration Platform re-queues or discards the task when Customer Collaboration Platform recovers from a failure. Set this parameter when submitting a task request.	Customer Collaboration Platform 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.
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.

API Parameter or Setting	API/Tool	Possible Values	
		Interactive Task/MRD	Non-interactive Task/MRD
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 Customer Collaboration Platform Task API to poll for status or Customer Collaboration Platform XMPP BOSH eventing.	Customer Collaboration Platform Task API or XMPP BOSH eventing	Use Customer Collaboration Platform Task API status polling for MRDs when you want to monitor the status of a single contact/task.	Use Customer Collaboration Platform 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 Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-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.

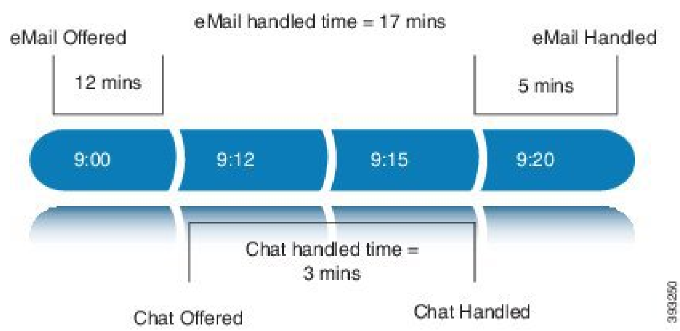
  The agent, CCE task, and Finesse dialog state in the interrupted MRD change to INTERRUPTED.

  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.

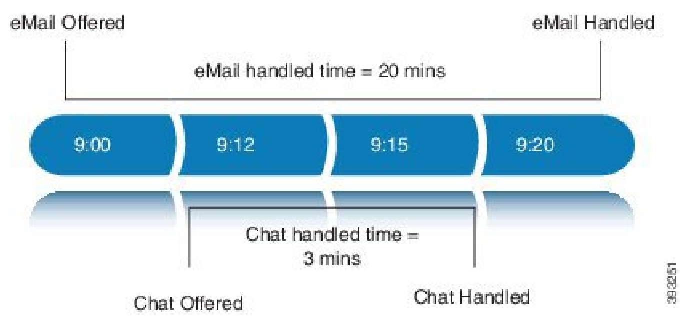


- **Ignore:** When an agent is interrupted by another task while working on a task in an interruptible MRD, Finesse ignores the interrupt event.

  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 Customer Collaboration Platform. 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 Customer Collaboration Platform 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 Customer Collaboration Platform. The application must make the agent routable in order for the agent to receive tasks again.

Customer Collaboration Platform and Finesse Task States

In most cases, Customer Collaboration Platform social contact states do not map directly to Finesse dialog states. For Customer Collaboration Platform, 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 Customer Collaboration Platform social contact task states and Finesse dialog states.

Customer Collaboration Platform 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: Customer Collaboration Platform receives a handled notification from Finesse indicating that the task ended.	**Closed:** The agent ended the task. Finesse sends a handled notification to Customer Collaboration Platform.

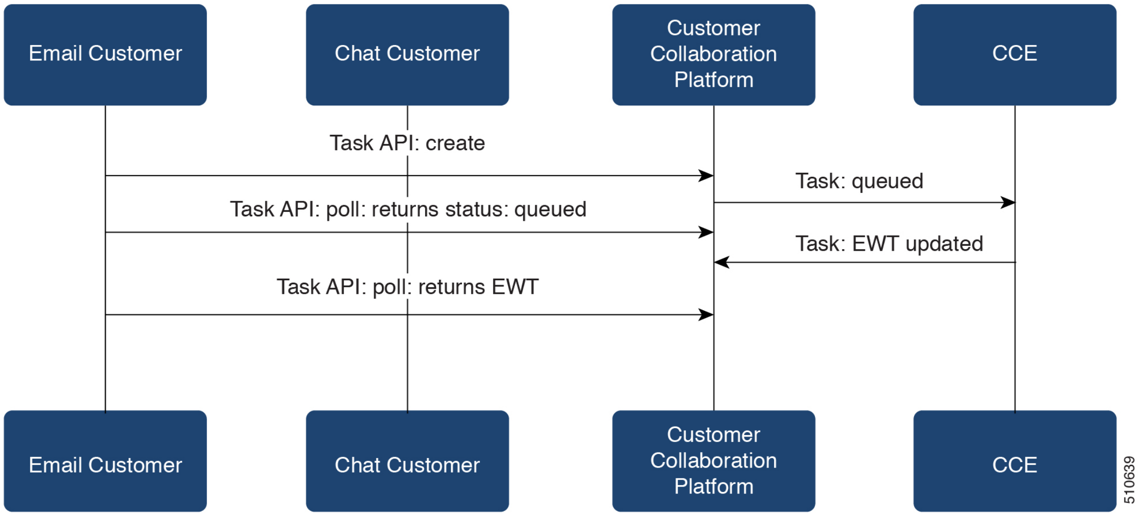
Task Routing API Request Flows

Task Routing API Basic Task Flow

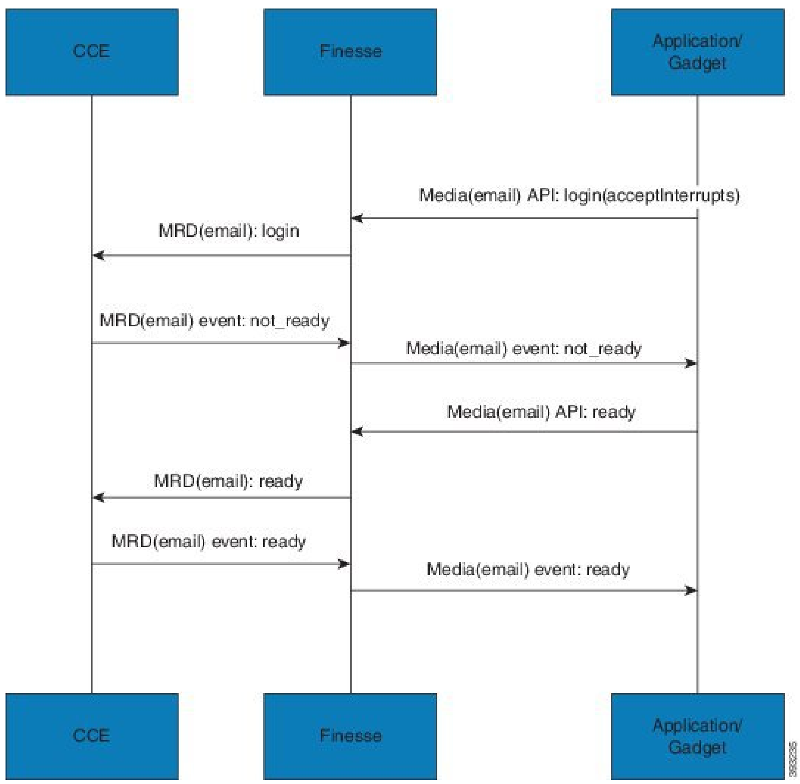
This topic provides the Customer Collaboration Platform and Finesse API calls and events when an active email task is interrupted by a chat request.

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.

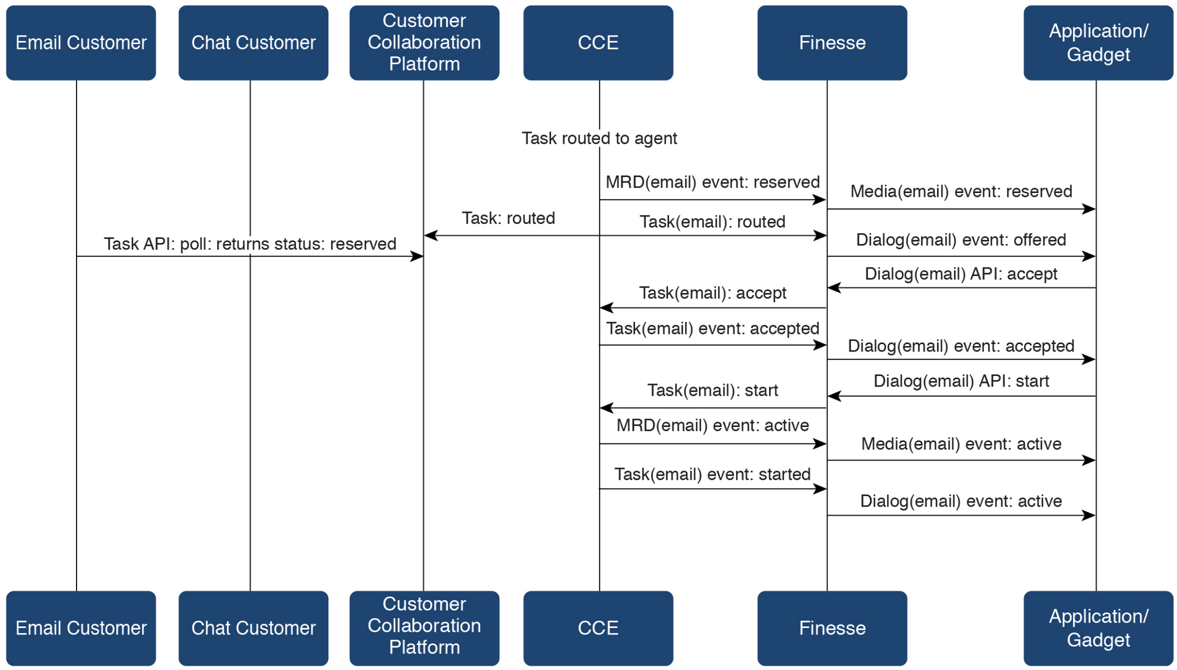
1. The email application submits a new email task request to CCE, and polls for status and Estimated Wait Time (EWT).



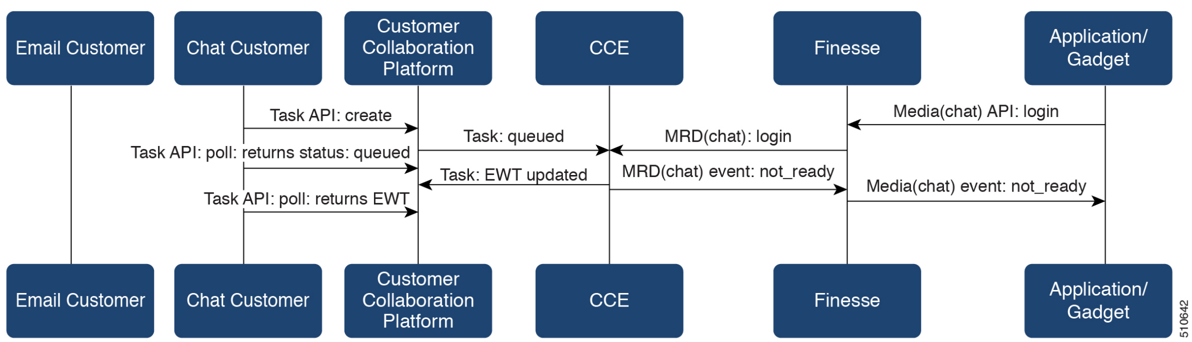
2. An agent signs in to the email MRD and changes state to Ready.



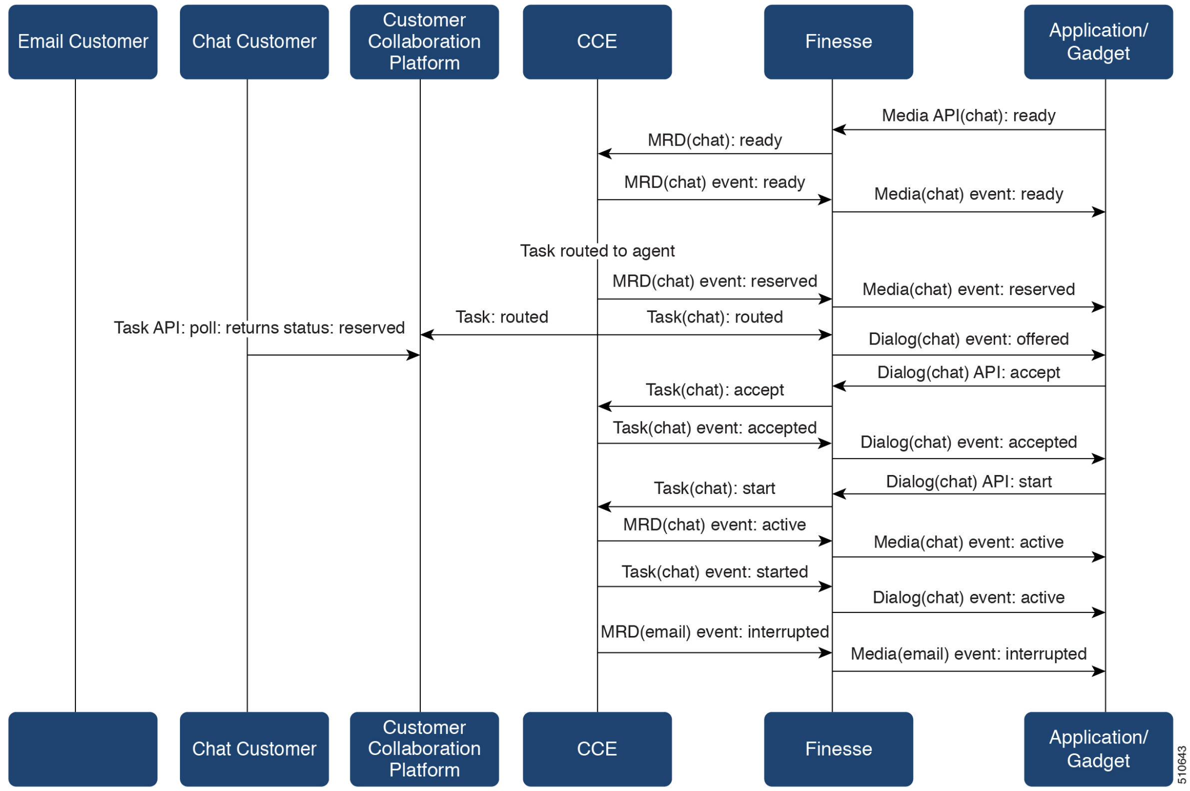
3. CCE assigns the agent the email task. The Call and ECC variables used to create the task are included in the dialog's media properties, and contain information such as the handle to the email. The variables can be used to reply to the email. The agent starts work on the email dialog in Finesse.



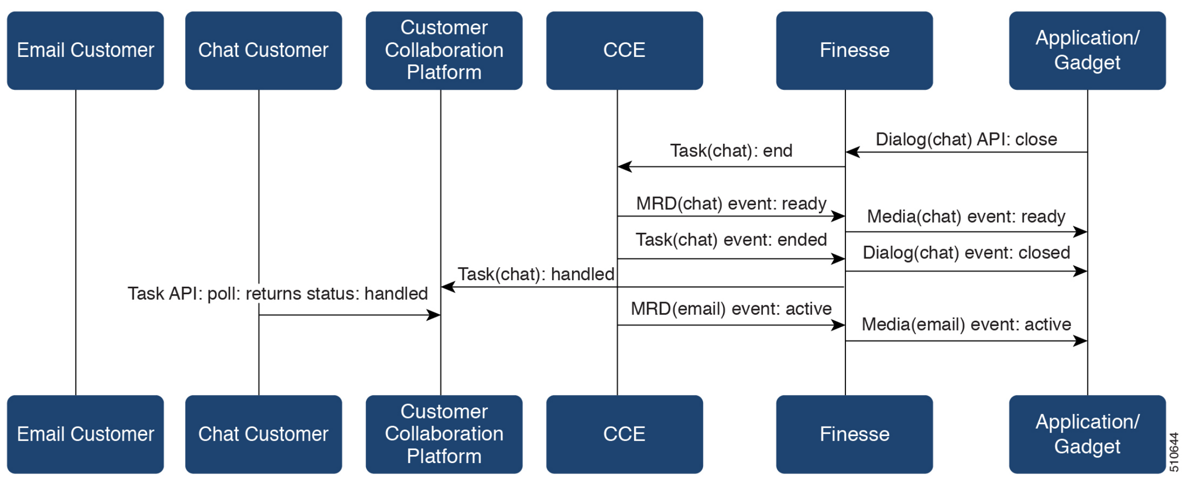
4. The chat application submits a new chat request, and polls for status and EWT. The same agent logs into the chat MRD.



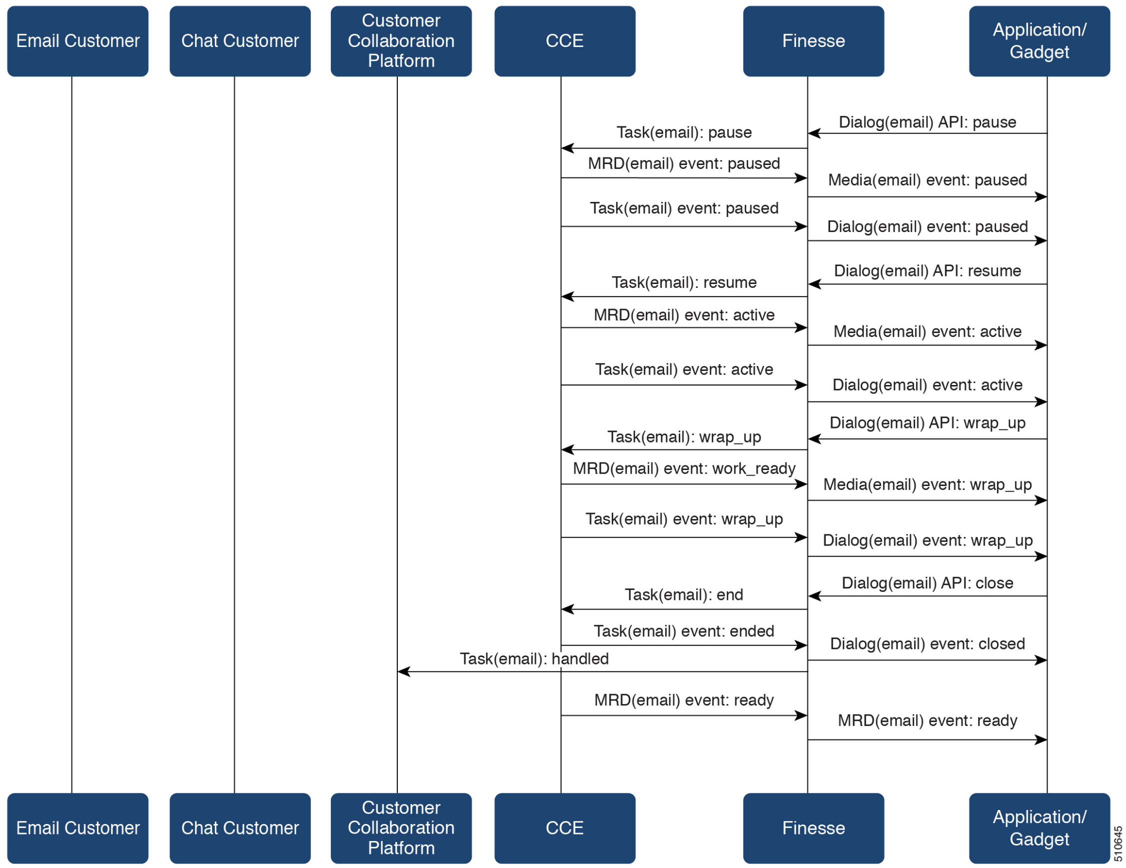
5. The agent changes state to Ready in the chat MRD. CCE assigns the chat task to the agent. The Call and ECC variables used to create the task are included in the dialog's media properties, and contain information such as the chat room URL. The variables can be used to join the chat room with the customer. 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 Customer Collaboration Platform 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.

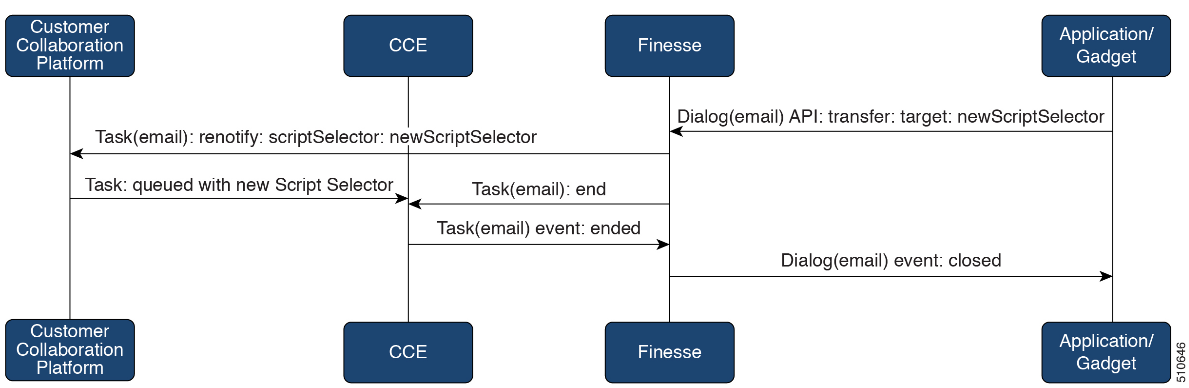


7. The agent continues working on the email dialog, including pausing, resuming, and wrapping up the dialog. The agent closes the dialog. Finesse sends a handle event to Customer Collaboration Platform for the email task. The application is responsible for sending the email reply to the customer.



Task Routing API Agent Transfer Flow

This illustration provides the Customer Collaboration Platform and Finesse API calls and events when an agent transfers a task.



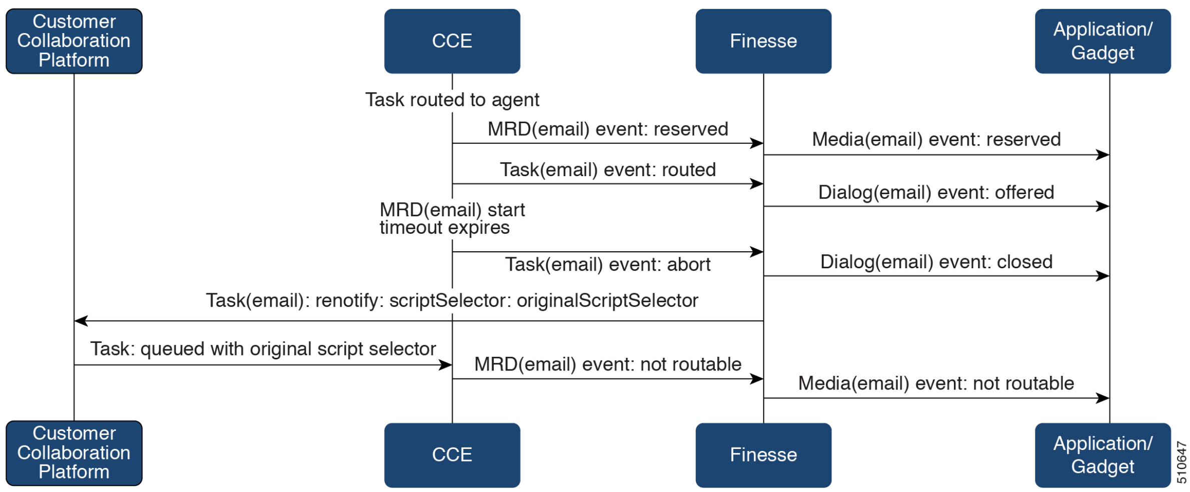
1. The agent transfers the dialog from the Finesse application, selecting the script selector to which to transfer the task.

2. Finesse resubmits the task to Customer Collaboration Platform, 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 Customer Collaboration Platform.

Task Routing API RONA Flow

This illustration provides the Customer Collaboration Platform 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 Customer Collaboration Platform.

4. The Finesse server on which the agent was last signed in resubmits the task to Customer Collaboration Platform with the original script selector. The task is queued to the script selector as a new task.

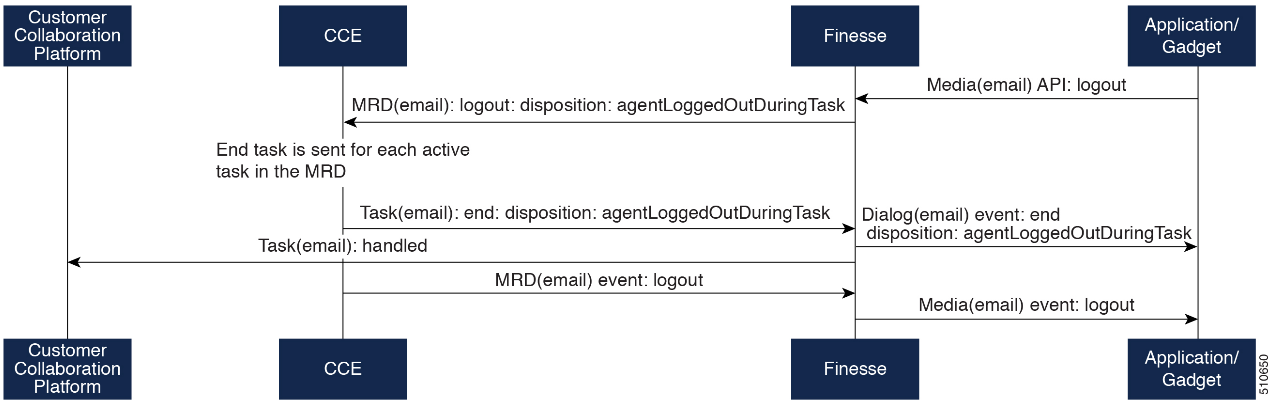
5. CCE instructs Finesse to make the agent not routable in that Media Routing Domain, so that the agent is not routed more tasks.

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

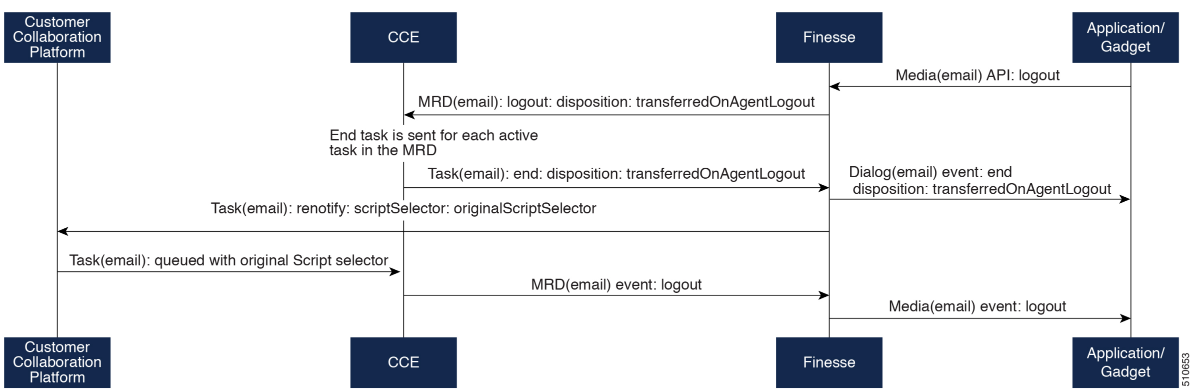
This illustration provides the Customer Collaboration Platform and Finesse API calls and events when agents are set to have assigned tasks closed on sign out.



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 Customer Collaboration Platform 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 Customer Collaboration Platform.
3. The Finesse server on which the agent was signed in resubmits the task to Customer Collaboration Platform 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
Customer Collaboration Platform	MR connection fails. For example, there is a networking problem, the PG loses connection, or Customer Collaboration Platform loses connection. Finesse loses connection with Customer Collaboration Platform.	**New task requests from Customer Collaboration Platform 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: **Customer Collaboration Platform failure:** NOTIFICATION_CCE_ CUSTOMERCOLLABORATIONPLATFORM_ SYSTEM_FAILURE **MR connection failure:** NOTIFICATION_CCE_CONNECTION_LOST **Offered and active tasks:** No impact.
Customer Collaboration Platform	Customer Collaboration Platform overruns the new task queue limit. For the limit, see the Cisco Customer Collaboration Platform Developer Guide.	**New task requests from Customer Collaboration Platform 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.

Component	Failover/Failure Scenario	New Task Request Impact	Queued, Offered, and Active Task Impact
Finesse	Finesse loses connection with Agent PG or CTI Server	**New task request from Customer Collaboration Platform 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 Customer Collaboration Platform 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 Customer Collaboration Platform 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 Customer Collaboration Platform 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 Customer Collaboration Platform 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	Set up the MR PG and PIM for Customer Collaboration Platform. See Set up the Media Routing PG and PIM, on page 192.	

Step	Task	Notes
2	Add Customer Collaboration Platform as an External Machine in the System Inventory. See Add Customer Collaboration Platform as an External Machine, on page 193.	The system configures the following settings automatically in Customer Collaboration Platform 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.
3	Configure the following in Unified CCE Administration: • Media Routing Domains • Call types • Dialed numbers • Skill groups or precision queues • ECC variables • Agent desk settings See Unified CCE Administration Tools, on page 194.	
4	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 195.	
5	Create routing scripts See Create Routing Scripts for Task Routing, on page 196.	
Create Custom Customer Collaboration Platform and Finesse Applications		
6	Create the Customer Collaboration Platform multichannel application to begin task requests. See Sample Customer Collaboration Platform HTML Task Application, on page 196.	
7	Create the Finesse applications to manage nonvoice agent and dialog states. See Sample Finesse Code for Task Routing, on page 197.	
Set up Finesse		

Step	Task	Notes
8	Upload the Finesse applications 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.	

Set up the Media Routing PG and PIM

Caution Before performing the step to enable the secured connection between the components, ensure that the security certificate management process is completed.

Set up the Media Routing PG and PIM

Procedure

Step 1 Navigate to **Unified CCE Administration** > **Overview** > **Infrastructure Settings** > **Peripheral Gateways**. Determine the Peripheral ID for a Multichannel peripheral that is unused.

Step 2 From Cisco Unified CCE Tools, select **Peripheral Gateway Setup**.

Step 3 On the Components Setup screen, in the Instance Components panel, select the PG Instance component. Click **Edit**.

Step 4 In the Peripheral Gateways Properties screen, click **Media Routing**. Click **Next**.

Step 5 Click **Yes** at the prompt to stop the service.

Step 6 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 for the unused Multichannel peripheral that you identified in Step 1.
d) For **Application Hostname (1)**, enter the hostname or IP address of Customer Collaboration Platform.
e) By default, Customer Collaboration Platform accepts the MR connection on **Application Connection Port** 38001. The Application Connection Port setting on Customer Collaboration Platform 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) Check the **Enable Secured Connection** option.

   This establishes a secured connectionbetween MR PIM and Application Server.

   Ensure that you provide the correct information in the Application Hostname (1) and Application Connection Port (1) fields.

i) Click **OK**.

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 Customer Collaboration Platform as an External Machine

When you add Customer Collaboration Platform as an External Machine in the Unified CCE Administration System Inventory, the system automatically performs the following Customer Collaboration Platform configuration:

- Enables and completes the **CCE Configuration for Multichannel Routing** settings in Customer Collaboration Platform Administration.

  These settings include the hostnames of the Unified CCE 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 In **Unified CCE Administration**, click **Inventory** from the left navigation.

Step 2 Select the main site or remote site and in the **External Machines** section, click the + icon.

Step 3 Click **Add Machine**.

Step 4 Select Customer Collaboration Platform from the drop-down list.

Step 5 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 6 Enter the Customer Collaboration Platform Administration username and password.

Step 7 Click **Save**.

Unified CCE Administration Tools

This topic explains the Unified CCE Administration tools you need to configure Task Routing.

For details on the procedures for these steps, refer to the Unified CCE Administration online help.

Procedure

Step 1 Sign in to Unified CCE Administration.

Step 2 Configure the following:

Item to Configure	Details
Media Routing Domains	Create an MRD for each type of task that the custom application submits to CCE (email, chat, and so on).
Call Types	Create call types for Task Routing.
Dialed Numbers	Create dialed numbers for Task Routing. Add the numbers or strings that the third-party multichannel application will use when submitting task requests. • For **Routing Type**, select Customer Collaboration Platform. • For **Media Routing Domain**, select one of the Task Routing MRDs you created. • For **Call Type**, select a call type that 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.
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.

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 Customer Collaboration Platform.
Network VRU Script	Create a Network VRU Script that references the Network VRU (MR_Network_VRU). The Network VRU Script is used to return estimated wait time to customers. You can accept the default values. 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. For more information on writing scripts to return estimated wait time, 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/products-maintenance-guides-list.html.
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 delete 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 to 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 Unified CCE Rogger.

Procedure

Modify the following registry key: `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Icm\<instance name>\Router<A/B>\Router\CurrentVersion\Configuration\Global\TCDTimeout`.

Create Routing Scripts for Task Routing

For complete multichannel scripting information, 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/products-maintenance-guides-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 Customer Collaboration Platform and Finesse available to use as baselines in building your own applications.

Sample Customer Collaboration Platform HTML Task Application

The sample Customer Collaboration Platform 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 Customer Collaboration Platform Developer Guide.

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
- 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 *Cisco Packaged Contact Center Enterprise Reporting User Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html for information about multichannel reporting data.

CHAPTER 14

Webex Experience Management

Experience Management Overview

Note To enable this feature in Packaged CCE, install the following patches:

- ICM 12.5(1)_ES7
- CVP 12.5(1)_ES6
- Cloud Connect 12.5(1)ES1
- Finesse 12.5(1)ES2

Cisco Webex Experience Management is a Customer Experience Management (CEM) platform that allows you to see your business from your customers' perspective. To know more about Webex Expereince Management, see https://xm.webex.com/docs/ccoverview/.

With Webex Experience Management, Packaged CCE supports:

- Customer experience surveys - Set up and send surveys to customers, after an interaction, to collect feedback about their interaction.
- Customer Experience Journey (CEJ) gadget - Displays all the past survey responses from a customer in a chronological list. The agent and supervisor use this gadget to gain context about the customers past experiences with the business and engage with them appropriately.

- Customer Experience Analytics (CEA) gadget - Displays the overall experience of the customer interaction with agents using industry-standard metrics such as NPS, CSAT, and CES or other KPIs tracked within Experience Management. This gadget is available for agents and supervisors.

Experience Management Survey

Experience Management post-call survey is used to determine whether the customers are satisfied with their voice call experiences. You can configure Experience Management to initiate this survey when an agent disconnects from the caller. The survey can be done in three modes—voice, SMS, or email.

The CCE script enables or disables voice call survey for each call by testing for conditions and setting an expanded call variable that controls Experience Management. For example, the script can invoke a prompt that asks callers whether they want to participate in a survey. Based on the caller's response, the script sets the expanded call variable that controls whether the call gets transferred to the voice call survey Dialed Number.

You can send post call survey links through email or SMS also. After every call, the customer is provided with a choice to participate in the survey and answer few questions over email or their phone. For more information on how to configure or to associate the survey, refer to the section Configure Packaged CCE for Experience Management Voice, SMS and Email Survey, on page 205 .

Note Experience Management supports G.711 u-law and G.711 a-law codecs.

Experience Management Task Flow

To enable Experience Management Post Call Survey in Cisco Packaged CCE, follow this task flow:

Procedure

Step 1 Contact your Cisco representative to purchase Experience Management license. After the purchase, you need to provide relevant information about your organization to Experience Management Activation Team. To know more about the information that will be collected, see Prerequisites.

Step 2 Experience Management Activation Team performs the following actions:

a. Creates accounts and provisions the same.

b. Creates default spaces and metric groups for your accounts. To know more about creating spaces, see Space Creation.

c. Creates standard questionnaires for Experience Management Post Call Survey and publishes the same. To know more about creating questionnaires, see Questionnaires.

Step 3 After creating and provisioning the account, you will receive handover emails from the Experience Management Activation Team. The email contains credentials and other essential information for your account. To know more about provisioning details, see Handover.

Step 4 Initially, Spaces and Widgets are created by the Experience Management provisioning team. To know more about the different default Widgets, how to export and derive meaningful insights from them, see Experience Management Gadgets.

To know how to configure additional Widgets in Experience Management, see Experience Management Gadgets.

Step 5 Ensure that the Cloud Connect publisher and subscriber are installed. For more information, see the *Create VM for Cloud Connect Publisher* and *Create VM for Cloud Connect Subscriber* sections in *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

Step 6 Provision Experience Management service using CLI on Cloud Connect. For more information, see Provision Experience Management Service on Cloud Connect, on page 201.

Step 7 Configure Cloud Connect in Unified CCE Admininstration. For details on how to do this, see *Configure Cloud Connect* section in *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

Step 8 Configure Packaged CCE for Post Call Survey. For more information, see Configure Packaged CCE for Post Call Survey, on page 145.

Step 9 Import the following certificates to the CVP Server:

- Cloud Connect certificate
- Experience Management certificate

For details, see the sections *Import Cloud Connect Certificate to Unified CVP Keystore* and *Import Experience Management Certificate to Unified CVP Call Server* in *Configuration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html.

Step 10 Ensure that the threshold properties (in *ivr.properties* and *sip.properties* files) and proxy settings are configured in CVP for Experience Management. For details, see the section *Webex Experience Management Configuration* in *Configuration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html.

Step 11 Configure Packaged CCE Experience Management. For more information, see the topic Configure Packaged CCE for Experience Management Voice, SMS and Email Survey, on page 205.

Step 12 Configure Dialed Number and Call Type for Incoming Call and Experience Management post call survey routing script. For more information, see Configure Dialed Number and Call Type, on page 207.

Step 13 Modify CCE scripts. For more information, see *Experience Management Scripting* in *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

Associate the CCE script with the Call Type created in the previous step.

Step 14 Add Experience Management gadgets into Finesse desktop layout. For more information, see Cisco Webex Experience Management Gadgets.

Provision Experience Management Service on Cloud Connect

Provision Experience Management service using the following CLI on Cloud Connect.

```
set cloudconnect cherrypoint config
```

Configure Cloud Connect in Packaged CCE Admininstration. For details on how to do this, see *Configure Cloud Connect* topic at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

The partner hosted module which is a part of Experience Management Invitations solution is required to send surveys to customers over emails and SMS.

For information about *Partner Hosted Module Architecture* refer to https://xm.webex.com/docs/cxsetup/guides/partnerarchitecture/

For information about how to provision the infrastructure required to deploy the partner hosted components of the Experience Management Invitations module, see https://xm.webex.com/docs/cxsetup/guides/partnerinfra/
.

For information about how to deploy the partner hosted components on the Experience Management Invitations module once the infrastructure is provisioned, see https://xm.webex.com/docs/cxsetup/guides/partnerdeployment/.

Configure Packaged CCE for Post Call Survey

You can enable and disable Post Call Survey within a CCE routing script by using the ECC variable **variableuser.microapp.isPostCallSurvey**. A value of *n* or *y* disables and enables the feature. (The value is case-insensitive.)

Configure the ECC variable to a value of n or y before either the label node or the Queue to Skillgroup node. This configuration sends the correct value to Unified CVP before the agent transfer. This ECC variable is not needed to initiate a Post Call Survey call, but you can use it to control the feature once Post Call Survey is configured in the Unified CCE Administration. Dialed Number is mapped to the Post Call Survey Dialed Number patter to automatically transfer the call.

Note

- The Post Call Survey DN is called if the Unified CVP has received at least one CONNECT message from CCE (either from the VRU leg or from the Agent leg). Use the END node in your CCE routing script if the Post Call Survey is not required for the calls disconnected from the IVR.
- If Router Requery is configured incorrectly and the Ring-No-Answer timeout expires, the caller is still transferred to the Post Call Survey DN. This can occur if a Queue node is used and Enable target requery is not checked.

Procedure

Step 1 In Unified CCE Administration, navigate to **Overview** > **Call Settings** > **Route Settings** > **Expanded Call Variables**.

Step 2 Click **New** to open the **New Expanded Call Variable** window.

Step 3 Create a new ECC variable with **Name:**`user.microapp.isPostCallSurvey`.

Step 4 Set **Max Length:** to 1.

Step 5 Check the **Enabled** checkbox. Then click **Save**.

In your CCE routing scripts, remember that, at script start, the default behavior of Post Call Survey equals **enabled**, even if **user.microapp.isPostCallSurvey** has not yet been set in the script. You can turn **off** Post Call Survey in the script by setting **user.microapp.isPostCallSurvey** to *n*. You can later enable Post Call Survey in the same path of the script by setting this variable to *y*.

Step 6 Navigate to **Overview** > **Call Settings** > **Route Settings** > **Call Types**.

Step 7 Add the call type for Post Call Survey, and click **Save**.

Step 8 Navigate to **Overview** > **Call Settings** > **Route Settings** > **Dialed Numbers**.

Step 9 Click **New** and complete the following fields:

Field	Required?	Description
Dialed Number String	yes	The value used to route the call, which is the Post Call Survey Dialed Number. Enter a string value that is unique for the routing type, maximum of 25 characters. **Note** The **External Voice** and **Post Call Survey** routing types must not have the same dialed number strings for the same site.
Description	no	Enter a maximum of 255 characters to describe the dialed number string.
Department	yes (for departmental administrators)	A departmental administrator must select one department from the popup list to associate with this dialed number. The list shows all this administrator's departments. When a departmental administrator selects a department for the dialed number, the popup list for call type includes global call types and call types in the same department as the dialed number. A global administrator can leave this field as Global (the default), which sets the dialed number as global (belonging to no departments). A global administrator can also select a department for this Dialed Number. When an administrator changes the department, selections for call type are cleared if the selections do not belong to the new department or the global department.
Routing Type	yes	From the drop-down menu, select **Post Call Survey:** . **Post Call Survey:** Select this option for Post Call Survey dialed number strings that apply to voice calls coming from Cisco Unified Customer Voice Portal (CVP). This option is similar to External Voice where the calls comes from outside of the enterprise through a gateway. However, Unified CVP directs the calls internally to Post Call Survey after agent ends the call. This option allows you to enter the Post Call Survey Dialed Number and associate the Dialed Number Patterns to the Post Call Survey Dialed Number. For remote sites, the **Post Call Survey** option is available if the site is configured to VRU PG.

<table>
<tr><th>Field</th><th>Required?</th><th>Description</th></tr>
<tr><td>Media Routing Domain</td><td>no</td><td>The Media Routing Domain associated with the dialed number. Media Routing Domains (MRDs) organize how requests for media are routed. The system routes calls to agents who are associated with a particular communication medium; for example, voice or email. The selection of Routing Type determines what appears in this field.
• If the Routing Type is External Voice, Internal Voice, or Outbound Voice, the Media Routing Domain is Cisco_Voice and you cannot change it.
• If the Routing Type is Multichannel, click the magnifying glass icon to display the Select Media Routing Domain popup window.</td></tr>
<tr><td>Call Type</td><td>no</td><td>Use the drop-down menu to select the call type that you created for Post Call Survey.</td></tr>
<tr><td>PCS Enabled Dialed Number Patterns</td><td>no</td><td>Note The PCS Enabled Dialed Number Patterns field appears if the Routing Type is Post Call Survey.
Enter one or more dialed number patterns that allow calls to transfer to the Post Call Survey dialed number entered in the Dialed Number String field.
The field allows maximum of 512 characters that can have the comma separated list without any spaces. Both alphanumeric and special characters are supported.</td></tr>
<tr><td>Ringtone Media File</td><td>no</td><td>Note The Ringtone Media File field appears if the Routing Type is External Voice.
Enter filename of the custom ringtone - maximum of 256 characters without any spaces.</td></tr>
</table>

Step 10 Click **Save**.

Step 11 Restart the active generic PG (side A or B) to register the new ECC variable.

If the ECC variable already existed, you can skip this step.

Note The **user.microapp.isPostCallSurvey** setting takes effect on Unified CVP only when it receives a connect or temporary connect message. Therefore, if you do not want the survey to run, without first reaching an agent (such as 'after hours of treatment'), you must set the isPostCallSurvey to *n* before the initial 'Run script request'.

Configure Packaged CCE for Experience Management Voice, SMS and Email Survey

Refer to the following procedures to enable the Experience Management voice, SMS and email survey:

- Configure Expanded Call Variables, on page 205
- Upload Audio Files for Questions in Experience Management, on page 207
- Configure Dialed Number and Call Type, on page 207
- Associate Survey to Call Type in Unified CCE Admin, on page 209

Configure Expanded Call Variables

Procedure

Step 1 In Unified CCE Administration, navigate to **Overview** > **Call Settings** > **Route Settings** > **Expanded Call Variables**.

Step 2 From the list of ECC variables, click on the `user.microapp.isPostCallSurvey` variable to open it.

a) Set **Max Length:** to 1.
b) Check the **Enabled** checkbox.
c) Click **Save**.

In your CCE routing scripts, remember that, at script start, the default behavior of Post Call Survey equals **enabled**, even if **user.microapp.isPostCallSurvey** has not yet been set in the script. You can turn **off** Post Call Survey in the script by setting **user.microapp.isPostCallSurvey** to *n*. You can later enable Post Call Survey in the same path of the script by setting this variable to *y*.

Step 3 Create a new ECC variable with **Name:**`user.CxSurveyInfo`.

a) Set **Max Length** to 120.
b) Check the **Enabled** check box.

Step 4 Click **Save**.

Note The newly created ECC variables are added to the default payload list. If you want to save the ECC variables to a different payload list, in the **Configuration Manager**, navigate to **Tools** > **List Tools** > **Expanded Call Variable Payload List** and add the ECC variables to the payload list of your choice.

Step 5 Populate the **POD. ID** variable.

For more information on populating this variable, refer to the topic Configure POD.ID.

Step 6 Restart the active VRU PG (side A or B) to register the new ECC variable.

If the ECC variable already exists, you can skip this step.

Note The **user.microapp.isPostCallSurvey** setting takes effect on Unified CVP only when it receives a **connect** or temporary connect message. If you do not want the survey to run, without first reaching an agent (such as 'after hours of treatment'), set the isPostCallSurvey to **`n`** before the initial 'Run script request'.

Configure POD.ID

Cisco provided variables are predefined, but for POD.ID, the maximum length should be set to 120.

You can modify the variables only if you have the edit access.

Populate the value in the script with multiple attributes in a key-value pair format. Each key-value pair is seperated with a semi-colon. The following table displays the supported attributes:

Table 13: Variables and their descriptions

Attribute	Description	Applicable
cc_CustomerId	Unique ID for a customer across multiple channels	Chat and Email surveys for Digital Channels
Email	Email ID of the caller for Email surveys	Email survey for voice channel
Mobile	Phone number for SMS surveys	SMS survey for voice channel
cc_language	Language of the survey For the list of supported languages, refer to the Webex Experience Management documentation at https://xm.webex.com/docs/user/getting-help/#cloudcherry-language-support	Email, SMS, and Voice surveys for voice channel
Optin	Whether to opt in or opt out of the survey	Email, SMS, and Voice surveys for voice channel

Example: `cc_CustomerId=xxx;Email=xx;Mobile=xxx;cc_langauge=xxx;Optin=yes/no`

For more information on **Expanded Call Context Variables**, see the chapter *Expanded Call Variables* in 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/products-maintenance-guides-list.html.

You can also configure POD.ID from CVP Call Studio. For more information, refer to the topic *Configure Call Studio App Data Format* in *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

Upload Audio Files for Questions in Experience Management

Experience Management allows you to upload the audio files for post call survey.

Note To run post-call voice survey, you must either configure *Text-To-Speech(TTS)* in the voice browser or upload audio prompts in Experience Management.

Create and configure the questionnaires in Experience Management for sending IVR surveys to the customer. For more information on Experience Management, refer to https://xm.webex.com/docs/ccoverview/

For more information on how to create and modify the questionnaires, refer to https://xm.webex.com/docs/cxsetup/questionnaires/.

Configure Dialed Number and Call Type

Procedure

Step 1 In **Unified CCE Administration**, navigate to **Overview** > **Call Settings** > **Route Settings** > **Call Types**.

Step 2 Click **New** to open the Call Type window.

Step 3 Enter the Name of the Call Type for Experience Management survey.

Step 4 Click **Save** You will be re-directed to the List window and the confirmation message is displayed.

Step 5 Navigate to **Overview** > **Call Settings** > **Route Settings** > **Dialed Numbers**.

Step 6 Click **New** and complete the following fields:

Field	Required?	Description
Dialed Number String	Yes	This value is used to route the call.
Description	No	Enter a maximum of 255 characters to describe the dialed number string.

Field	Required?	Description
Department	No (Yes for departmental administrators)	A departmental administrator must select one department from the pop-up list to associate with this dialed number. The list shows all this administrator's departments. When a departmental administrator selects a department for the dialed number, the pop-up list for call type includes global call types and call types in the same department as the dialed number. A global administrator can leave this field as Global (the default), which sets the dialed number as global (belonging to no departments). A global administrator can also select a department for this Dialed Number. When an administrator changes the department, selections for call type are cleared if the selections do not belong to the new department or the global department.
Site	Yes	The **Site** field displays Main by default for Packaged CCE 2000 Agents deployment. For Packaged CCE 4000 Agents and 12000 Agents deployments, **Site** is a mandatory field and has no default value. To add a site: **a.** Click the **magnifying glass** icon to display the list of sites. **b.** Select the site.
Peripheral Set	Yes	This field is available only in Packaged CCE 4000 Agents and 12000 Agents deployments. To add a peripheral set: **a.** Click the **magnifying glass** icon to display the list of peripheral sets configured for the selected **Site**. **b.** Select the peripheral set.
Routing Type	Yes	From the drop-down menu, select External Voice. These calls are referred to as external because they typically come from outside of the enterprise through a gateway. External Voice is the selection for calls that come in from customers and must be answered by agents or sent to the VRU.

Field	Required?	Description
Media Routing Domain	Yes	The Media Routing Domain associated with the dialed number. The selection of Routing Type determines what appears in this field. Because the **Routing Type** is **External Voice**, the Media Routing Domain is always Cisco_Voice.
Call Type	Yes	Click on the magnifying glass icon. From the **Select Call Type** pop-up window, enter or select the call type you created in step 3. Associating a dialed number with a call type ensures appropriate routing and affects reporting.
Ringtone Media File	No	This field appears when the **Routing Type** is **External Voice**. Enter file name of the custom ringtone for the user-defined Dialed Numbers, a maximum of 256 characters without any spaces.

Step 7 Click **Save**. You will be re-directed to the List window and the confirmation message is displayed.

Step 8 To create the PCS dialed number refer topic, Configure Packaged CCE for Post Call Survey, on page 145.

Associate Survey to Call Type in Unified CCE Admin

You can associate the Call Type to the survey only if you have added **Cloud Connect** in the **Inventory** page and configured the survey in **Webex Experience Management** portal.

Note Only one survey can be associated to a Call Type.

Procedure

Step 1 In **Unified CCE Administration**, navigate to **Overview** > **Call Settings** > **Route Settings** > **Call Types**.

The list of all the **Call Types** are displayed.

Step 2 Click on the **Call Type** which you want to associate to the Survey. Associate the survey with the last call type before the call is first connected to an agent.

Step 3 Select the **Enable Experience Management** check box to associate the **Webex Experience Management** survey.

The **Experience Management** tab is enabled with the following options:

- **Inline Survey** (post-call voice survey)
- **Deferred Survey** (post-call Email and SMS survey)

Step 4 Click on the **magnifying glass** icon, and the configured surveys will be populated in the pop-up window.

Step 5 Select the survey from the pop-up window and click **Save**.

CHAPTER 15

Webex Experience Management Digital Channel Survey

Overview

Note To enable this feature in Packaged CCE, install the following patches:

- ICM 12.5(1)_ES7
- Cloud Connect 12.5(1)ES1
- Finesse 12.5(1)ES3
- ECE 12.5(1) ES1

Digital Channel Survey is initiated when the agent responds to an email/chat from a customer using the Enterprise Chat and Email gadget. Cisco Webex Experience Management is a Customer Experience Management (CEM) platform that allows you to see the business from your customers perspective. It provides customer journey experience using the CEJ omni-channel gadget. To learn more about Webex Experience Management, see https://xm.webex.com/docs/ccoverview/.

With Webex Experience Management, Packaged CCE supports:

- Customer experience surveys - Set up and send surveys to customers, after an interaction, to collect feedback about their interaction.
- Customer Experience Journey (CEJ) gadget - Displays all the past survey responses from a customer in a chronological list. The agent and supervisor use this gadget to gain context about the customers past experiences with the business and engage with them appropriately.

- Customer Experience Analytics (CEA) gadget - Displays the overall experience of the customer interaction with agents using industry-standard metrics such as NPS, CSAT, and CES or other KPIs tracked within Experience Management. This gadget is available for agents and supervisors.

Digital Channel Survey

Email and chat inline surveys are used to determine whether customers are satisfied with their interaction with the agent in resolving their query over an email or chat. The feedback collected through the survey is used by the agents to gain context about the customer in their subsequent interactions and to also improve their own performance. You can configure Enterprise Chat and Email to initiate this survey when the agent sends an email or terminates a chat conversation with a customer. The survey is sent inline in the agents email response to customers who contact them via email, and within the chat window for customers who contact them via chat.

Digital Channel Survey Task Flow (Email/Chat)

To enable Experience Management inline surveys with Enterprise Email and Chat in Cisco Packaged CCE, perform the following procedure:

Procedure

Step 1 Contact your Cisco representative to purchase Experience Management license. Provide relevant information about your organization to Experience Management Activation Team. To know more about the information that will be collected, see Prerequisites.

Step 2 Experience Management Activation Team performs the following actions:

a) Creates account and provisions the same.
b) Creates default spaces and metric groups for your accounts. To know more about creating spaces, see Space Creation.
c) Creates default questionnaires in Expereince Management suited for inline email and chat survey. To know more about creating your own questionnaires or editing the default ones, see Questionnaires.

Step 3 After creating and provisioning the account, you will receive handover emails from the Experience Management Activation Team. The email contains credentials and other essential information for your account. To know more about provisioning details, see Handover.

Step 4 Initially, Spaces and Widgets are created by the Experience Management provisioning team. To know more about the different default Widgets and how to export and derive meaningful insights from them, see Cisco Webex Experience Management Gadgets.

To know how to configure other Widgets in Experience Management, see Basic Widget and Composite Widgets.

Step 5 Ensure that the Cloud Connect publisher and subscriber are installed. For more information, see the *Create VM for Cloud Connect Publisher* and *Create VM for Cloud Connect Subscriber* sections in *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

Step 6 Provision Experience Management service using CLI on Cloud Connect. For more information, see Provision Cloud Connect for Digital Channel Survey, on page 213.

Step 7 Ensure that the Enterprise Chat and Email (ECE) is installed and configured, see the *Webex Experience Manager Integration* in *Enterprise Chat and Email Administrator's Guide to Administration Console* at https://www.cisco.com/c/en/us/support/contact-center/enterprise-chat-email-12-5-1/model.html.

Step 8 Configure Packaged CCE Experience Management integration. For more information, see Configure Packaged CCE for Digital Channel Survey , on page 213.

Step 9 Configure Call Type and Dialed Number. For more information, see Configure Call Type, Dialed Number, and Survey Association, on page 215.

Step 10 Modify CCE Scripts. For more information, see *Scripts for Experience Management* in *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

Associate the CCE script with the Call Type created in the previous step.

Step 11 Add Experience Management gadgets into Finesse desktop layout. For more information, see Cisco Webex Experience Management Gadgets.

Provision Cloud Connect for Digital Channel Survey

Before provisioning Cloud Connect for Experience Management service, ensure to setup and enable Cloud Connect. For more information, see the *Cloud Connect Administration* section in *Administration Guide for Cisco Unified Contact Center Enterprise*

Note Ensure that you have installed the self-signed certificates for Cloud Connect. For more information, see the *Self-Signed Certificates* section in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*.

Provision Experience Management service using the following CLI on Cloud Connect.

```
set cloudconnect cherrypoint config
```

Configure Cloud Connect in Packaged CCE Admininstration. For details on how to do this, see *Configure Cloud Connect* topic at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

Configure Packaged CCE for Digital Channel Survey

Refer to the following procedures to enable the Experience Management email and chat survey:

- Configure Expanded Call Variables , on page 214
- Configure Call Type, Dialed Number, and Survey Association, on page 215
- Associate Survey to Call Type in Unified CCE Admin, on page 216

Configure Expanded Call Variables

Procedure

Step 1 In Unified CCE Administration, navigate to **Overview** > **Call Settings** > **Route Settings** > **Expanded Call Variable**.

Step 2 From the list of ECC variables, click on the `user.microapp.isPostCallSurvey` variable to open it.

a) Set **Max Length** to 1.
b) Check the **Enabled** check box.
c) Click **Save**.

When your CCE routing scripts starts, you can turn off Post Call Survey field in the script by setting *user.microapp.isPostCallSurvey* to *n*. You can later enable Post Call Survey in the same path of the script by setting this variable to *y*.

Note In the script, set the *user.microapp.isPostCallSurvey* before routing it to the agent.

Note To enable Experience Management, *user.microapp.isPostCallSurvey* must be set to *y*.

Step 3 Create a new ECC variable with **Name:**`user.CxSurveyInfo`.

a) Set **Max Length** to 80.
b) Check the **Enabled** check box.

Step 4 Click **Save**.

Note The newly created ECC variables are added to the default payload list. If you want to save the ECC variables to a different payload list, in the **Configuration Manager**, navigate to **Tools** > **List Tools** > **Expanded Call Variable Payload List** and add the ECC variables to the payload list of your choice.

Note You can use several ECC payloads in the same call flow, but only one ECC payload has scope at a given moment. For more information, see *ECC Payloads* sections in *Configuration Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html

Step 5 Populate the **POD. ID** variable.

For more information on populating this variable, refer to the topic Configure POD.ID , on page 214.

Configure POD.ID

Cisco provided variables are predefined, but for POD.ID, the maximum length should be set to 120. Enable the POD.ID variable to edit its length.

You can modify the variables only if you have the edit access.

Populate the value in the script with multiple attributes in a key-value pair format. Each key-value pair is seperated with a semi-colon. These attributes are sent to the Webex Experience Management as prefills when ECE initiates the survey. The following table displays the supported attributes:

Table 14: Variables and their descriptions

Attribute	Description	Applicable
cc_CustomerId	Unique ID for a customer across multiple channels	Chat and Email surveys for Digital Channels
Email	Email ID of the customer for Email survey across multiple channels	Chat and Email surveys for Digital Channels
Mobile	Phone number for Chat surveys	Chat and Email surveys for Digital Channels

Example: `cc_CustomerId=xxx;Email=xx;Mobile=xxx;`

For more information on setting the ECC variables used in the example, see *Modify CCE Scripts for Experience Management Digital Channel Surveys* in *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.

For more information on **Expanded Call Context Variables**, see the chapter *Expanded Call Variables* in 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/products-maintenance-guides-list.html.

Configure Call Type, Dialed Number, and Survey Association

Procedure

Step 1 In **Unified CCE Administration**, navigate to **Overview** > **Call Settings** > **Route Settings** > **Call Types** and click **New** to create a Call Type.

For more information on how to create Call Type, refer to the section *Call Type* in *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html

Step 2 Associate the survey with the last call type before the email/chat is handled by the agent.

For more information, refer to the topic Associate Survey to Call Type in Unified CCE Admin, on page 216.

Step 3 Navigate to **Overview** > **Call Settings** > **Route Settings** > **Dialed Numbers** and click **New** to create Dialed Number.

Note Select **Enterprise Chat and Email** as routing type for dialed number.

For more information on how to create Dialed Number, refer to the section *Dialed Number* in *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html

Step 4 Click **Save**. You will be re-directed to the List window and the confirmation message is displayed.

Associate Survey to Call Type in Unified CCE Admin

You can associate the survey to the Call Type only if you have added **Cloud Connect** to the **Inventory** page in **CCE Admin** and configured the survey in **Webex Experience Management** portal.

Note Only inline surveys can be associated to a Call Type associated with digital channels.

Procedure

Step 1 In **Unified CCE Administration**, navigate to **Overview** > **Call Settings** > **Route Settings** > **Call Type**.

The list of all the **Call Type** are displayed.

Step 2 Click on the **Call Type** which you want to associate to the Survey.

Step 3 Select the **Enable Experience Management** check box to associate the **Webex Experience Management** survey.

a) The Experience Management tab is enabled with the following options:

- Inline Survey
- Deferred Survey

Step 4 Select **Inline Survey** for email and chat.

- Click on the **magnifying glass** icon, and the configured surveys will be populated in the pop-up window.

Step 5 Select the survey from the pop-up window and click **Save**.

CHAPTER 16

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.

Whisper Announcement is supported for blended outbound agents when they receive inbound calls.

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 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.
- 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. Media Server, on page 73.
2. Create Whisper Announcement Audio Files, on page 218.
3. Deploy Whisper Announcement Audio Files to Media Server, on page 219.
4. Configure Whisper Service Dialed Numbers, on page 219.
5. Add Whisper Announcement to Routing Scripts, on page 220.
6. Fail-Safe Timeout for Whisper Announcement in Unified CCE, on page 221.

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 221.

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.

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*.

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 221.

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

Ensure that your call routing scripts can access the Whisper Announcement audio files that you stored on a CVP media server. If you configure a default media server, and you store the audio files on the default server, you may not have to add any additional nodes to the scripts. For more information, see . To test the access, see Test Whisper Announcement File Path, on page 221.

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 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 **value**. This value is 20 seconds and represents the maximum Whisper Announcement play time that Unified CCE uses to calculate its report data.

The value was chosen 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. While the value is configurable in Unified CCE, changing the value is not supported in Unified CCE.

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:

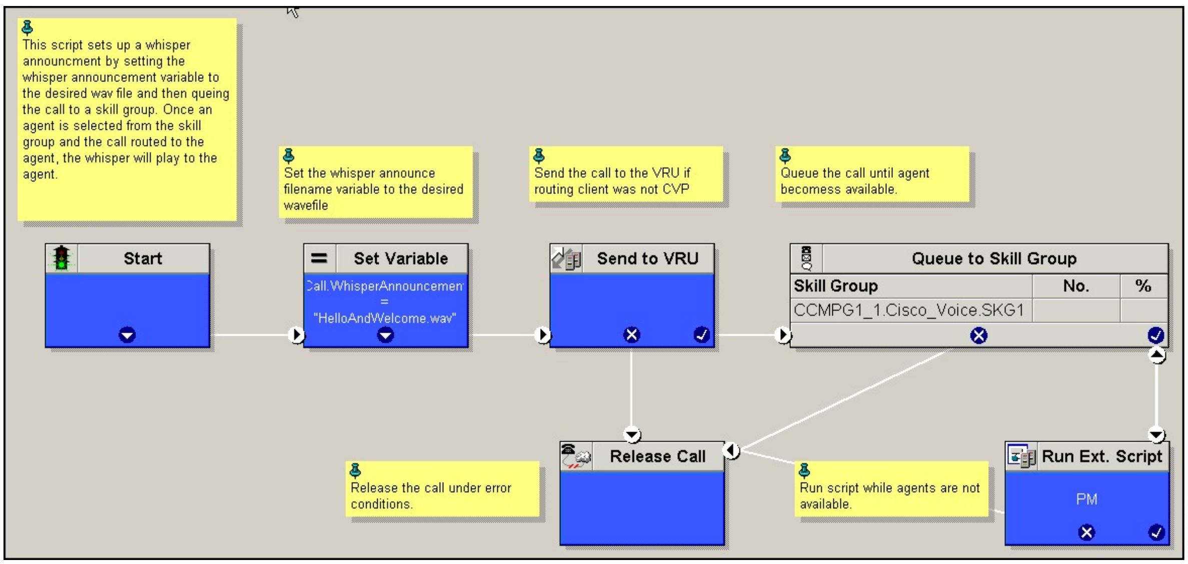
- **WA.ICMS**—This script plays a Whisper Announcement.
- **WA_AG.ICMS—**This script plays both a Whisper Announcement and an Agent Greeting to play on the same call flow.

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

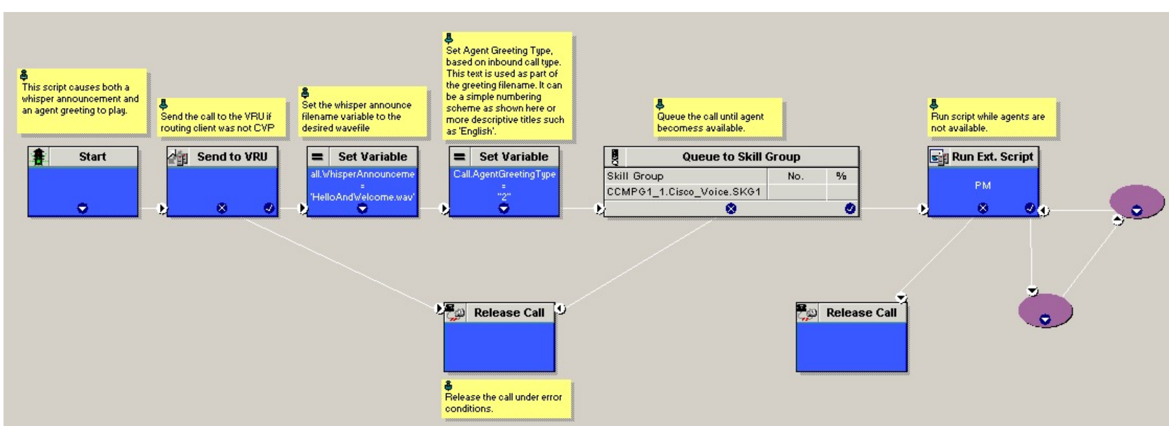
This script sets up a Whisper Announcement by setting the Whisper Announcement variable to the desired wave file and then queuing the call to a skill group or Precision Queue. After an agent is selected from the skill group or Precision Queue and the call routed to the agent, the whisper plays to the agent.



347723

WA_AG.ICMS Script

This script causes both a Whisper Announcement and an Agent Greeting to play.



347721

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.

Administration and Usage

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 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 generally plays during hold. The first agent hears ringing. In the case of blind transfers, the caller hears ringing while the whisper announcement plays.

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.

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.

APPENDIX **A**

Avaya Support

Avaya Support

Prerequisite

Make sure you have Avaya Automatic Call Distribution (ACD) versions that are compatible with Packaged CCE deployments. For more information, see the *Contact Center Enterprise Solution Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

Avaya Support Overview

Support for Avaya ACD int has been provided in Packaged CCE 4000 and 12000 Agent deployments. You can maintain an Avaya Peripheral Gateway (PG) in a Packaged CCE environment and use its intelligent contact center routing capability to route calls to geographically distributed contact center sites.

For detailed information about the required Avaya configurations, see chapter *Unified ICM Software Configuration* in the *Cisco Unified ICM ACD Supplement for Avaya Communication Manager Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-technical-reference-list.html.

Note Note that Avaya PG must be deployed on a separate VM. Also Avaya agents cannot be associated with a department.

Tools that Support Avaya Configurations

Configuration Manager Tools and nodes in the Script Editor have been enabled to facilitate the support for Avaya ACD in Packaged CCE 4000 and 12000 agent deployments. For the complete list of nodes and tools, 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/products-maintenance-guides-list.html.

The following restrictions apply to the tools that support Avaya PG configurations.

Table 15: Configuration Manager Tool Restrictions

Configuration Manager Tool	Restriction
Agent Explorer	• Only supports Avaya PG configurations • Does not support selecting persons who are already associated with the CUCM Peripheral agents
Person List	Does not list persons who are already associated with the CUCM peripheral agents
Dialed Number/Script Selector List	Supports addition of Dialed Numbers for Avaya Agents and NIC Routing Clients
Skill Group Explorer	Only supports Avaya PG configurations
Bulk Configuration Tools	The following bulk tools only support Avaya PG configurations. • Agent Bulk Insert • Dialed Number Bulk Insert • Skill Group Bulk Insert • Agent Bulk Edit • Dialed Number Bulk Edit • Skill Group Bulk Edit • Person Bulk Insert • Person Bulk Edit

For design details, scalability constraints and sizing factors, see the *Solution Design Guide for Cisco Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html.

You can also view historical and real-time stock reports for Avaya ACD. For more information, see the *Cisco Packaged Contact Center Enterprise Reporting User Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

APPENDIX B

Do Not Call Table

Do_Not_Call Table

The Do_Not_Call table includes all the phone numbers and extensions that, when matched exactly, are not dialed during an Outbound Option campaign.

The following table lists the Do_Not_Call table column names and provides their descriptions.

Column Name	Type	Description
Phone	VARCHAR(20)	The Do Not Call phone number.
PhoneExt	VARCHAR(8)	The extension for the Do Not Call phone number. **Note** Although the phone number extension is imported into the table, it is currently not used for any dialing operations.

Do Not Call Considerations

Consider the following for the Do Not Call feature:

- When you upgrade to or downgrade from Cisco Unified CCE, Release 11.6(1), the Do Not Call table is not available. Therefore, import the Do Not Call table again after upgrade or downgrade.
- Do not configure multiple Do Not Call import rules.
- A customer number is dialled even if the number is listed in the Do Not Call table. This occurs when:
  - the Campaign Manager restarts.
  - one of the routers is not available during the import of the Do Not Call records.
- Do not perform manual operations on database including database replication.

APPENDIX C

ICM to ICM Gateway Support

ICM to ICM Gateway Support

Prerequisite

Make sure you have ICM-to-ICM Gateway versions that are compatible with Packaged CCE deployments. For more information, see the *Contact Center Enterprise Solution Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

ICM-to-ICM Gateway Overview

Support for ICM-to-ICM Gateway has been provided in Packaged CCE 4000 and 12000 Agent deployments, where Packaged CCE can act as a client or a server. The call requests can be routed from Packaged CCE to remote Unified CCE/Unified ICM deployments and vice versa.

ICM-to-ICM Gateway extends the ICM software capability by allowing agents to simultaneously pre-route/post-route calls, and supply additional call-related information to a second agent on a different ICM. This enables the initial agent to pass on gathered information without the customer's needing to repeat it to the second agent.

Following are some business scenarios where ICM-to-ICM Gateway functionality can be useful.

- A customer calls the institutional department of a financial corporation for customer service assistance with a company-sponsored 401k. The customer then asks to be transferred to the retail department to obtain assistance with a personal account.
- Two corporations (for example, a bank and an insurance company), each of which has a contact center that uses an ICM, merge. It may often be desirable to transfer a call between the two companies; for example, to sell insurance to a bank customer.
- A customer calls a hotel to make a reservation. The hotel agent then asks the customer if he/she also needs to rent a car, and then transfers the customer to a car rental agent.
- A company uses an outsourcer to handle part of its overflow traffic. For example, the company service department handles paid support calls in-house but transfers warranty service requests to the outsourcer.

- A multi-national corporation encompasses several geographic regions; each geographic region has its own ICM.

In all these cases, ICM-to-ICM Gateway enables the call-related data to be transferred along with the call so the customer does not need to supply this information again.

For more information about ICM-to-ICM Gateway call flows and configuration, see the *ICM-to-ICM Gateway User Guide for Cisco Unified ICM Enterprise & Hosted Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html

Tools Supported for ICM-to-ICM Gateway

Configuration Manager Tools and nodes in the Script Editor have been enabled to facilitate the ICM-to-ICM Gateway capability in Packaged CCE 4000 and 12000 Agent deployments. For the complete list of nodes and tools, 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/products-maintenance-guides-list.html.

Note The **Application Gateway List** tool only supports remote ICM configuration.

For design details, scalability constraints and sizing factors, see the *Solution Design Guide for Cisco Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html.