Feature Configuration Guide for Cisco Unified Communications Manager, Release 10.5(2)

First Published: 2014-12-19

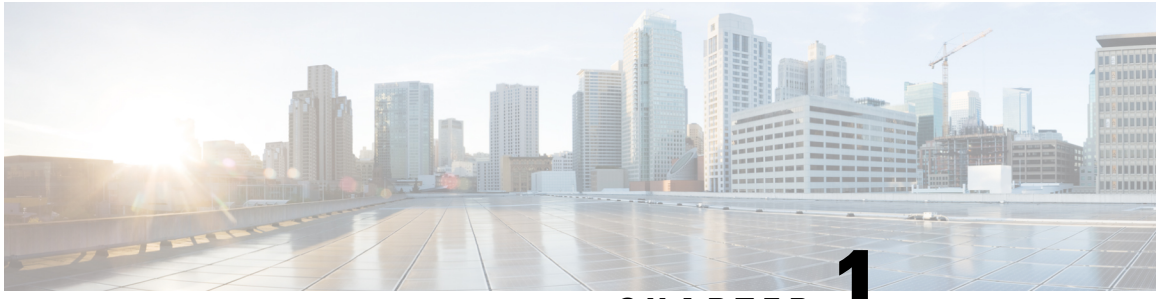
Last Modified: 2020-10-21

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

PART I

Getting Started



CHAPTER 1

Configuration Tools

About the Feature Configuration Guide

This guide provides information about the tasks that you need to complete in order to configure features on the Unified Communications Manager system. Use this guide after you have configured the call control system, which includes "day 1" configurations such as inbound and outbound calling, dial plans, and network resources. For information about configuring the call control system, see System Configuration Guide for Cisco Unified Communications Manager.

Configuration Tools Overview

The procedures in this guide require you to use the following two configuration tools:

- Cisco Unified Communications Manager Administration
- Cisco Unified Serviceability

This chapter provides a brief description of the tools and how to access them.

Cisco Unified Communications Manager Administration

Cisco Unified Communications Manager Administration Administration is a web-based application that allows you to make individual, manual configuration changes to the Unified Communications Manager nodes. The procedures in this guide describe how to configure features using this application.

If you need to perform bulk configuration tasks and want to automate the configuration process, you can use the Unified Communications Manager Bulk Administration Tool (BAT) to make a large number of configuration changes at the same time. For more information, see Bulk Administration Guide for Cisco Unified Communications Manager.

Log In to Cisco Unified CM Administration

Use the following procedure to log in to Cisco Unified Communications Manager Administration. After you log in to Cisco Unified Communications Manager Administration, messages may display that indicate the current state of licenses for Unified Communications Manager in the main window. For example, Unified Communications Manager may identify the following situations:

- Unified Communications Manager currently operates with starter (demo) licenses, so upload the appropriate license files.
- Unified Communications Manager currently operates with an insufficient number of licenses, so upload additional license files.
- Unified Communications Manager does not currently use the correct software feature license. In this case, the Cisco CallManager service stops and does not start until you upload the appropriate software version license and restart the Cisco CallManager service.

Use the following procedure to browse into the server and log in to Cisco Unified CM Administration.

Procedure

Step 1 Start your preferred operating system browser.

Step 2 In the address bar of the web browser, enter the following case-sensitive URL:

```
https://<Unified CM-server-name>:{8443}/ccmadmin/showHome.do
```

where: `<Unified CM-server-name>` equals the name or IP address of the server

Note You can optionally specify a port number.

Step 3 A Security Alert dialog box displays. Click the appropriate button.

Step 4 At the main Cisco Unified CM Administration window, enter the username and password that you specified during Unified Communications Manager installation and click **Login**. (If you want to clear the content of both fields, click **Reset**.)

Note For security purposes, Cisco Unified Communications Manager Administration logs you out after 30 minutes of inactivity, and you must log back in.

Cisco Unified Communications Manager Serviceability

Some procedures in this guide require you to use the Cisco Unified Serviceability application to start or restart services on the Unified Communications Manager nodes.

Cisco Unified Serviceability is a web-based troubleshooting tool that provides the following functionality:

- Saves alarms and events for troubleshooting and provides alarm message definitions.
- Saves trace information to log files for troubleshooting.
- Monitors real-time behavior of components through the Cisco Unified Real-Time Monitoring Tool (Unified RTMT).

- Provides audit capability by logging configuration changes to the system by a user or due to result of the user action. This functionality supports the Information Assurance feature of Unified Communications Manager and Cisco Unity Connection.
- Provides feature services that you can activate, deactivate, and view through the **Service Activation** window.
- Generates and archives daily reports; for example, alert summary or server statistic reports.
- Allows Unified Communications Manager, IM and Presence Service and Cisco Unity Connection to work as a managed device for Simple Network Management Protocol (SNMP) remote management and troubleshooting.
- Monitors the disk usage of the log partition on a node (or all nodes in the cluster).
- Monitors the number of threads and processes in the system; uses cache to enhance the performance.
- **Unified Communications Manager only**: Generates Unified Communications Manager reports for Quality of Service, traffic, and billing information through Cisco Unified Communications Manager CDR Analysis and Reporting.

Log into Cisco Unified Communications Manager Serviceability

Use the following procedure to log in to Cisco Unified Serviceability.

Procedure

Step 1 Start your preferred operating system browser.

Step 2 In the address bar of the web browser, enter the following case-sensitive URL:

```
https://<Unified CM-server-name>:{8443}/ccmadmin/showHome.do
```

where: `<Unified CM-server-name>` equals the name or IP address of the server

Step 3 A Security Alert dialog box displays. Click the appropriate button.

Step 4 From Cisco Unified CM Administration, choose **Cisco Unified Serviceability** from the Navigation menu drop-down list and click **Go**.

Step 5 Enter the username and password that you specified during Unified Communications Manager installation and click **Login**.

Note For security purposes, the system logs you out after 30 minutes of inactivity, and you must log back in.

Generate a Phone Feature List

Generate a phone feature list report to determine which devices support the feature that you want to configure.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System Reports**.

Step 2 From the list of reports, click **Unified CM Phone Feature List**.

Step 3 Perform one of the following steps:

- Choose **Generate New Report** (the bar chart icon) to generate a new report.
- Choose **Unified CM Phone Feature List** if a report exists.

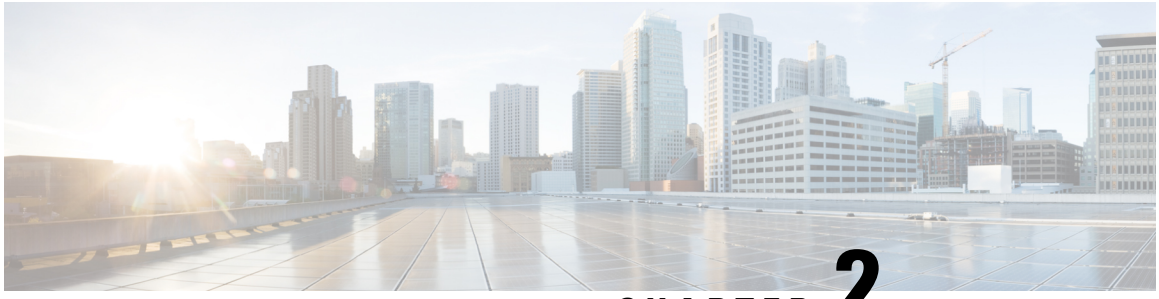
Step 4 From the **Product** drop-down list, choose **All**.

Step 5 Click the name of the feature that you want to configure.

Step 6 Click **Submit**, to generate the report.

PART II

Remote Worker Features



CHAPTER 2

Cisco Unified Mobility

Cisco Unified Mobility Overview

Cisco Unified Mobility offers a set of mobility-related features that allow users to interact with Unified Communications applications no matter where they may be, or which device they are using. Whether the device you are using is a home office phone, a dual-mode Cisco Jabber on iPhone or Android client over a WiFi connection, or a mobile phone from another cellular provider, you can still access Unified Communications features and have the call be anchored in the enterprise.

For example, you can answer a call that is directed to your enterprise number from any of your configured phones and then transfer the call to your mobile phone, allowing you to continue an in-progress conversation as you are leaving the office.

Benefits of Cisco Unified Mobility

Most of the mobility features offer call anchoring within the enterprise–even if the call is placed to or from a mobile device, the call is routed through an enterprise gateway.

This provides the following benefits:

- Single enterprise phone number and voicemail for all business calls, regardless of which device you are using, and whether you are in the office or out of the office.
- Ability to extend business calls to a mobile device and have the call still be handled as if it were your office phone.
- Calls placed from mobile devices are anchored to the enterprise and routed through an enterprise gateway. This provides access to UC mid-call features, centralized billing and call detail records, and potential cost savings from avoiding expensive cellular networks.
- Ability to roam from one network to another and have the call not be dropped.

Mobility Features

Cisco Unified Mobility offers the following mobility-related features:

Mobility Feature	Description
Single Number Reach	Provides you with a single enterprise phone number and voicemail by which you can be reached, regardless of whether you are in the office or outside the office. When someone dials your enterprise number, you can answer the call from your deskphone, or from any of your configured remote destinations (for example, a home office phone, a dual-mode Cisco Jabber on iPhone or Android client, and even a mobile phone from another provider) .
Move to Mobile	Allows you to transfer an active call from your desk-phone to a mobile device that is configured as a remote destination by pressing the **Mobility** soft-key on your Cisco IP Phone. It is associated with Single Number Reach as a part of the Remote Destination configuration. Similar to the **Move to Mobile** option is the **Desk Pickup** option, which fits the example where you are on a mobile call and are just arriving at the office. You can hang up on the call on your mobile device and immediately resume the call by picking up your deskphone before the **Maximum Wait Time for Desk Pickup** timer expires (the default is 10 seconds). This option is enabled as part of your Single Number Reach configuration. **Note** You can also use the `Enterprise Feature Access` code and the `Session Handoff` codes to transfer calls between your remote destinations and desk phone.
Mobile Voice Access	Allows you to place calls from any remote phone and have the call be anchored in the enterprise and presented to the called party as if you had called from your office phone. When using this feature, you must dial in to a system IVR from your mobile device. After authenticating you, and prompting you for the call destination, the system places the call as if you had called from your enterprise phone. You can also use **Mobile Voice Access** prompts to enable or disable **Single Number Reach** for a remote destination.
Enterprise Feature Access .	Provides two-stage dialing from a configured remote destination and have the call that is presented to the called party as if it originated from your desk phone. Unlike **Mobile Voice Access**, to use **Enterprise Feature Access**, you must be dialing from one of your configured remote destinations. **Enterprise Feature Access** also allows you to access mid-call features while on a call from a remote destination. You can access mid-call features by sending DTMF digits that represent the codes for the various features such as Hold, Exclusive Hold, Transfer.

Mobility Feature	Description
Intelligent Session Control	Enables automatic call anchoring for enterprise-originated calls that are placed directly to configured remote destination numbers (for example, an enterprise-originated call to a cell phone number that is configured as a remote destination). By configuring a service parameter, you can have the system redirect those calls automatically to the associated enterprise number, providing cost savings and added UC functionality.
Dual-Mode Phones	Cisco Jabber on iPhone and Android clients can be provisioned as dual-mode devices. **Dual-Mode phones** have the capability of connecting over Wifi or through cellular networks. When the client is within the enterprise network, Cisco Jabber can register to Unified Communications Manager over Wifi, and has UC calling and instant messaging functionality. If you configure a mobile identity with the phone number of the mobile device, allowing the call to be transferred from Jabber to the cellular device when leaving the enterprise network.

Cisco Unified Mobility Prerequisites

Refer to the following prerequisites:

- Enabling Mobility features requires proper planning to ensure that your dial plan and call routing configuration can handle the deployment needs. For more information, see "*Mobile Collaboration*" section in the *Cisco Collaboration System Solution Reference Network Designs* guide.
- For information on which Cisco IP Phones support Mobility feature, see Generate a Phone Feature List, on page 3.
  - For a list of Cisco IP Phones that support the Mobility softkey, run a report for the **Mobility** feature.
  - For a list of supported dual-mode phones, run a report for the **Dual-Mode** feature.
- If you are deploying Mobile Voice Access and you want to make additional locales available to your system (if you want to use non-English phone locales or country-specific tones), you can download the locale installers from cisco.com and install them through the Cisco Unified OS Administration interface. For more information on installing locales, see Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service.
- Configure Self-Provisioning so that phone users can provision their own Cisco Jabber clients and remote destinations. For more information, see "*Configure Self Provisioning*" and "*Provisioning End Users*" section in the System Configuration Guide for Cisco Unified Communications Manager.

Caution The Cisco mobility solution is verified with only Cisco equipment. This solution may also work with other third-party PSTN gateways and Session Border Controllers (SBCs), but the features might not work as described here. If you are using this solution with third-party PSTN gateways or SBCs, Cisco technical support may not be able to resolve problems that you encounter.

Cisco Unified Mobility Configuration Task Flow

Complete these tasks to configure Mobility features for your deployment.

Procedure

	Command or Action	Purpose
Step 1	Perform one of the following: • Configure a Mobility User, on page 11 • Configure Mobility Users through Bulk Administration, on page 11 • Provision Mobility Users Through LDAP, on page 12	Adds mobility features for an individual end user. Configures Mobility features for a large number of existing end users, use the Bulk Administration Tool. Provisions new users with mobility functionality, you can use a feature group template and LDAP sync.
Step 2	Configure Mobility for IP Phones, on page 13	Configures Cisco IP Phones for Mobility including setting up the Single Number Reach (SNR) and Move to Mobile features. This allows enterprise phone users to extend enterprise calls to a wide range of mobile devices, including a home office phone or a mobile phone.
Step 3	Configure Mobile Voice Access, on page 18	**Optional**. Provides a system IVR so that mobile users can call from any mobile device and have the call that is presented to the called party as if the caller were dialing from their enterprise desk phone.
Step 4	Configure Enterprise Feature Access, on page 25	**Optional**. Provides two-stage dialing from a configured remote destination and have the call that is presented to the called party as if it originated from a desk phone. This feature also allows you to access mid-call features while on a call from a remote destination.
Step 5	Configure Intelligent Session Control, on page 26	Configure the system so that inbound calls to a remote destination are rerouted to an associated enterprise, if one is available. This provides automatic call anchoring within the enterprise for mobility calls, providing cost savings and added Unified Communications functionality.
Step 6	Configure Mobility Service Parameters, on page 26	**Optional**. Configure optional mobility-related service parameters if you want to change the behavior of Cisco Unified Mobility.

	Command or Action	Purpose
Step 7	Configure Cisco Jabber Dual-Mode, on page 27	Configure Cisco Jabber for mobility so your users can access enterprise communications features through a Jabber client on their smartphone.
Step 8	Configure Other Dual-Mode Devices, on page 27	Complete this task flow if you want to deploy other dual-mode devices, such as FMC or IMS clients that can connect through Wi-Fi.

Configure a Mobility User

Use this procedure to configure an end user with the mobility feature.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **End User**.

Step 2 In **Find and List Users** window, perform one of the following tasks:

- Click **Find** and select an existing user to modify the settings.
- Click **Add New** to configure a new user.

Step 3 Configure values for the following fields:

- **User ID**
- **Last Name**

Step 4 In the **Mobility Information** section, complete the following fields:

a) Check the **Enable Mobility** check box.

b) **Optional**. Check the **Enable Mobile Voice Access** check box to allow this user to use Mobile Voice Access.

c) In the **Maximum Wait Time for Desk Pickup** field, enter a value in milliseconds. After hanging up a call from a remote destination, this timer represents the amount of time where the user still has the option of resuming the call from a deskphone.

d) In the **Remote Destination Limit** field, enter the number of remote destinations that a user is permitted to have for single number reach (SNR) targets.

Step 5 Complete the remaining fields in the **End User Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 6 Click **Save**.

Configure Mobility Users through Bulk Administration

Use this procedure to use Bulk Administration's **Update Users** menu to add the Mobility feature to existing end users by bulk.

Note Bulk Administration contains other features that allow you to update existing users by bulk. For example, you can use the Export and Import functions to import a CSV file with the new Mobility settings. For more information, see the Bulk Administration Guide for Cisco Unified Communications Manager.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Bulk Administration** > **Users** > **Update Users** > **Query**.

Step 2 Apply the filter and click **Find** to select the users whom you want to assign as mobility users.

Step 3 Click **Next**.

Step 4 In the **Mobility Information** section, modify the following four fields by first checking the check box on the far left to indicate that this field is to be updated, and then configuring the setting on the right as follows:

- **Enable Mobility**—Check this check box to enable the users provisioned with this template for Mobility features.
- **Enable Mobile Voice Access**—Check this check box for provisioned users to be able to use Mobile Voice Access.
- **Maximum Wait Time for Desk Pickup**—This field represents the amount of time, after hanging up a call on a mobile phone, that you have to resume the call on your deskphone.
- **Remote Destination Limit**—This field represents the number of Remote Destinations and Mobile Identities that you can assign to users whom are provisioned through this template.

Step 5 Under **Job Information**, check **Run Immediately**.

Step 6 Click **Submit**.

Provision Mobility Users Through LDAP

If you have not yet synced your LDAP directory, you can use this procedure to configure synced end users with mobility capability through the Feature Group Template configuration. Newly synced users inherit the mobility settings from the template.

Note This method works only if you have not yet synced your LDAP directory. You cannot assign new feature group template configurations to an LDAP directory sync after the initial sync has occurred.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Feature Group Template**.

Step 2 In the **Find and List Feature Group Templates** window, perform one of the following:

- Click **Add New** to configure a new template.
- Click **Find** and select an existing template to configure.

Step 3 Assign a **Name** to the template.

Step 4 Configure the following Mobility fields:

- **Enable Mobility**—Check this check box to enable the users provisioned with this template for Mobility features.
- **Enable Mobile Voice Access**—Check this check box for provisioned users to be able to use Mobile Voice Access.
- **Maximum Wait Time for Desk Pickup**—This field represents the amount of time in milliseconds, after hanging up a call on a mobile phone, that you have to resume the call on your deskphone.
- **Remote Destination Limit**—This field represents the number of Remote Destinations and Mobile Identities that you can assign to users whom are provisioned through this template.

Step 5 Configure the remaining fields in the **Feature Group Template Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 6 Click **Save**.

Note Assign the configured Feature Group Template to an LDAP Directory that has not yet been synced. Newly synced users have Mobility enabled. For more information, on provisioning users through LDAP see "*Provisioning End Users*" chapter in System Configuration Guide for Cisco Unified Communications Manager.

Configure Mobility for IP Phones

Complete these tasks to configure mobility features for Cisco IP Phones. This includes setting up Single Number Reach (SNR) and the Move To Mobile feature. This provides users with a single enterprise number that rings all their devices, in addition to an enterprise-level voicemail that can be reached no matter which device rings. And also, users are able to transfer active calls between their deskphone and mobile device.

Procedure

	Command or Action	Purpose
Step 1	Configure Softkey Template for Mobility, on page 14	Configures a mobility softkey template for Cisco IP Phones that includes the Mobility softkey. Users can transfer calls from their deskphone to a mobile phone by pressing the softkey.
Step 2	Configure IP Phone for Mobility, on page 15	Configures an IP phone for mobility so that incoming calls to an enterprise number are extended to remote destinations.
Step 3	Configure a Remote Destination Profile, on page 16	Configures common settings that you want to apply to all the remote destination numbers for a user.
Step 4	Configure a Remote Destination, on page 16	Configures a remote destination that is a virtual device that represents a mobile device where the user can be reached (for example, a home office phone, or a mobile phone on a cellular

	Command or Action	Purpose
		network). The remote destination carries many of the same settings as the user's desk phone.
Step 5	Configure an Access List, on page 17	**Optional**. Controls which calls can ring which remote destinations, and at which times of day. The access list filters callers based on the Caller ID and can either allow calls or block calls from the caller during that remote destination's ring schedule.

Configure Softkey Template for Mobility

Use this procedure to configure a softkey template that includes the **Mobility** softkey. The softkey will be enabled for all phones that use this template.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Softkey Template**.

Step 2 To create a new softkey template do the following. Otherwise, proceed to the next step.

a) Click **Add New**.
b) Select a default template and click **Copy**.
c) In the **Softkey Template Name** field, enter a new name for the template.
d) Click **Save**.

Step 3 To add mobility softkeys to an existing template.

a) Enter search criteria and click **Find**.
b) Choose an existing template.

Step 4 (Optional) Check the **Default Softkey Template** check box if you want to designate this softkey template as the default softkey template.

Note If you designate a softkey template as the default softkey template, you cannot delete it unless you first remove the default designation.

Step 5 Click **Save**.

Step 6 From the **Related Links** drop-down list, choose **Configure Softkey Layout** and click **Go**.

Step 7 From the **Select a Call State to Configure** drop-down list, choose the call state for which you want to add the softkey. Typically, you will want to add the softkey for both the **OnHook** and **Connected** call states.

Step 8 From the **Unselected Softkeys** list, choose the **Mobility** softkey and use the arrows to move the softkey to the **Selected Softkeys** list. Use the up and down arrows to change the position of the new softkey.

Step 9 To display the softkey in additional call states, repeat the previous step.

Step 10 Click **Save**.

Note If you created a new softkey template, you can assign the template to a phone through the **Phone Configuration** window or to a group of phones through Bulk Administration's **Update Phones** menu.

There are several methods to assign softkey template to phones during provisioning. For example, you can use the **Universal Device Template** configuration, or you can assign it as the default device profile for a specific model.

Enable Mobility within Feature Control Policy

If you have configured feature control policies to enable or disable features for Cisco IP Phones, then you will also have to enable Mobility within the policy that is used by your Cisco IP Phones. If the feature is disabled within the feature control policy configuration that is used by your phones, then the Mobility softkey will be disabled for all Cisco IP Phones that use that policy.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Feature Control Policy**.

Step 2 Click **Find** and choose the applicable policy.

Note You can also choose **Add New** if you want to create a new feature control policy that you will assign to your phones to enable mobility, along with other associated features. You can assign the policy to phones through the **Phone Configuration** window, or to a set of phones through the **Common Phone Profile Configuration**. You can also assign the policy to a universal device template to assign the policy to phones as they are provisioned.

Step 3 In the **Name** field, enter a name for the feature control policy. The name can include up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each feature control policy name is unique to the system.

Step 4 In the **Description** field, enter a brief description for the feature control policy. The description can include up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_).

Step 5 In the **Feature Control** Section, check both the **Override Default** check box and the **Enable Setting** check box that corresponde to the Mobility softkey.

Step 6 Click **Save**.

Configure IP Phone for Mobility

If you have Single Number Reach or Move to Mobility configured, use this procedure to configure your deskphone with the Mobility feature so that enterprise calls can be redirected to a remote destination.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Perform one of the following tasks:

- Click **Find** and select an existing phone to modify the settings.
- Click **Add New** and choose a phone from the **Phone type** drop-down list to add a new phone.

Step 3 Click **Next**.

Step 4 From the **SoftKey Template** drop-down list, choose the mobility softkey template that you configured.

Step 5 From the **Owner User ID** drop-down list, choose the user account on which you enabled mobility.

Step 6 (Optional) If you are using a **Feature Control Policy** to enable features, select the policy from the drop-down list.

Step 7 Click **Save**.

Configure a Remote Destination Profile

Configures common settings that you want to apply to all the remote destination numbers for a user.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Profile** > **Remote Destination Profile**.

Step 2 Click **Add New**.

Step 3 Enter a **Name** for the profile.

Step 4 From the **User ID** drop-down list, select the end user to whom this profile applies.

Step 5 From the **Device Pool** drop-down list, select the device pool where this profile should reside.

Step 6 Configure the remaining fields in the **Remote Destination Profile Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 7 Click **Save**.

Step 8 Under **Association Information**, click **Add a New DN**.

Step 9 In the **Directory Number** field, add the directory number of the user's desk phone.

Configure a Remote Destination

A remote destination is a virtual device that represents a mobile device where the user can be reached (for example, a home office phone, a mobile phone on a cellular network, or a PSTN phone). The remote destination carries many of the same settings as the user's desk phone.

Note

- When an enterprise user initiates a call from a remote destination to Cisco Jabber, Unified Communications Manager tries to establish a data call with Cisco Jabber by sending an INVITE message to Cisco TelePresence Video Communication Server (VCS). The call is established regardless of receiving a response from VCS.
- If you have Self-Provisioning enabled, your end users can provision their own phones from the Self-Care Portal. Refer to the System Configuration Guide for Cisco Unified Communications Manager and the "*Configure Self-Provisioning*" chapter for details on configuring the system for self-provisioning and the "*Provisioning End Users*" part for details on enabling self--provisioning for users as a part of a User Profile.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Remote Destination**.

Step 2 Click **Add New**.

Step 3 In the **Destination** field, enter the number of the remote destination. For example, this could be a cellular number or PSTN number.

Step 4 From the **Mobility User ID** field, select the mobility-enabled end user who uses this remote destination.

Step 5 Check the **Enable Unified Mobility** features check box.

Step 6 From the **Remote Destination Profile** drop-down list, select the profile that you set up for the user who owns this remote destination.

Step 7 From the **Single Number Reach Voicemail Policy** drop-down list, configure the voicemail policy.

a) From the **Single Number Reach Voicemail Policy** drop-down list, configure the voicemail policy.

b) Check the **Enable Single Number Reach** checkbox.

Step 8 Check the **Move to Mobile** check box to include this remote destination to the list of available destinations when the user hits the **Mobility** softkey on their desk phone.

Step 9 (Optional) Configure a **Ring Schedule** if you want to limit enterprise calls to this remote destination to just specific days such as office hours.

Step 10 In the **When receiving a call during the above ring schedule** area, apply the list configured for this remote destination.

Step 11 Configure the remaining fields on the **Remote Destination Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 12 Click **Save**.

Configure an Access List

An access list is an optional remote destination configuration if you want to control which calls can ring which remote destinations, and at which times of day. The access list filters callers based on the Caller ID and can either allow calls or block calls during that remote destination's ring schedule.

Note Phone users can configure their own access lists through the Self-Care Portal.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Access List**.

Step 2 Click **Add New** to create an access list.

Step 3 Enter a name and description to identify the new access list.

Step 4 Associate the access list to a user by choosing an ID from the **Owner** drop-down list.

Step 5 Choose one of the following options:

- **Allowed**—All numbers in the access list are allowed.
- **Blocked**—All numbers in the access list are blocked.

Step 6 Click **Save**.

Step 7 From the **Filter Mask** drop-down list, choose the filters that you want to apply to the access list:

- **Not Available**—All callers that advertise a not available status are added to the access list.
- **Private**—All callers that advertise a private status are added to the access list.
- **Directory Number**—All directory numbers or directory strings that you specify are added to the access list. If you choose this option, add a number or number string in the **DN Mask** field.

Step 8 Choose **Save**.

Step 9 Apply the access list to a remote destination:

a) From Cisco Unified CM Administration, choose **Device** > **Remote Destination** and reopen the remote destination that you created.

b) Configure the **Ring Schedule** for this access list and do either of the following:

- If you created an allowed access list, click the **Ring this destination only if caller is in** radio button and choose the access list that you created from the drop-down list.
- If you created a blocked access list, click the **Do not ring this destination if caller is in** radio button and choose the access list that you created from the drop-down list.

c) Click **Save**.

Configure Mobile Voice Access

Complete the following tasks to configure the system for Mobile Voice Access, which lets users place enterprise-anchored calls from any device. Users dial a system IVR for authentication, following which the call is sent out as an enterprise call that will appear to the end user as if the call were sent from the office phone.

Before you begin

To use Mobile Voice Access:

- Users must be enabled as mobility users with the **Enable Mobile Voice Access** option checked within **End User Configuration** For details, see Configure a Mobility User, on page 11.
- Interactive Voice Response service must be active, and included in a Media Resource Group List that the trunk uses.

Procedure

	Command or Action	Purpose
Step 1	Activate the Cisco Unified Mobile Voice Access Service, on page 19	In Cisco Unified Serviceability, make sure that the Cisco Unified Mobile Voice Access feature service is activated.
Step 2	Enable Mobile Voice Access, on page 20	Enable the Mobile Voice Access feature and specify a directory number that users can dial to reach the enterprise.

	Command or Action	Purpose
Step 3	Configure Directory Number for Mobile Voice Access, on page 20	Configure mobile voice access (MVA) to assign sets of localized prompts for users who dial in from outside the enterprise. After the gateway collects the required digits from the user to make a call, the call is transferred to the DNA that is configured in this window. This DN can be internal. You must configure a dial-peer so that the MVA service can transfer the call from the gateway to this DN. This DN should be also be placed in a partition where the inbound calling search space (CSS) of the gateway or the remote destination profile CSS can reach the DN.
Step 4	Configure a gateway for MVA or enterprise feature access (EFA) by performing one of the following tasks: • Configure an Existing H.323 or SIP Gateway for Remote Access, on page 21 • Configure a New H.323 Gateway for Remote Access, on page 23	Depending on your system requirements, you can add a new gateway or configure an existing gateway to handle calls that come from outside the enterprise through MVA or EFA. If you have an existing H.323 or SIP PSTN gateway in your system, you can configure it for MVA. This function is accessed by calling a system-configured DID number that is answered and handled by an H.323 or SIP VoiceXML (VXML) gateway. After you configure your gateway, it uses a vxml script on the publisher node to pull the interactive voice response (IVR) prompts that are played to the MVA users. These prompts request user authentication and input of a number that users must dial on their phone keypad. If you do not have an existing H.323 or SIP PSTN gateway and you want to configure mobile voice access, you must add a new H.323 gateway and configure it for MVA functionality by using the hairpinning method. From a technical standpoint, this method refers to using a second gateway to receive the inbound call, apply the MVA service and then the inbound call leg returns to the PSTN gateway (original source) after the system applies the MVA service.

Activate the Cisco Unified Mobile Voice Access Service

Use the following procedure to activate this service in your publisher node.

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Service Activation**.

Step 2 From the **Server** drop-down list, choose the publisher node.

Step 3 Click **Go**.

Step 4 Under **CM Services**, check the **Cisco Unified Mobile Voice Access Service** check box.

Step 5 Click **Save**.

Enable Mobile Voice Access

Configure service parameters to enable Mobile Voice Access (MVA) and to specify the directory number or PSTN DID number that users can dial in order to reach the IVR.

Before you begin

The Cisco Unified Mobile Voice Access feature service must be activated for Mobile Voice Access to work.

Procedure

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

Step 2 From the **Server** drop-down list, choose publisher node.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.

Step 4 Configure the following service parameters:

- **Enable Mobile Voice Access**—Set this parameter to **True**.
- **Mobile Voice Access Number**—Enter the access number that you want users to dial when they access the enterprise.

Step 5 Click **Save**.

Configure Directory Number for Mobile Voice Access

Configure mobile voice access (MVA) to assign sets of localized prompts for users who dial in from outside the enterprise. After the gateway collects the required digits from the user to make a call, the call is transferred to the DNA that is configured in this window. This DN can be internal. You must configure a dial-peer so that the MVA service can transfer the call from the gateway to this DN. This DN should be also be placed in a partition where the inbound calling search space (CSS) of the gateway or the remote destination profile CSS can reach the DN.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **Mobile Voice Access**.

Step 2 In the **Mobile Voice Access Directory Number**, enter the internal directory number (DN) to receive Mobile Voice Access calls from the gateway.

Enter a value between 1-24 digits in length. Valid values are 0-9.

Step 3 In the **Localization** pane, use the arrows to move the locales that you want to select to or from this pane.

Note Mobile Voice Access uses the first locale that appears in the Selected Locales pane in the **Mobile Voice Access** window. For example, if English United States appears first in the Selected Locales pane, the Cisco Unified Mobility user hears English when the IVR is used during a call.

Step 4 Click **Save**.

What to do next

Perform one of the following tasks:

- Configure an Existing H.323 or SIP Gateway for Remote Access, on page 21
- Configure a New H.323 Gateway for Remote Access, on page 23

Configure an Existing H.323 or SIP Gateway for Remote Access

If you have an existing H.323 or SIP PSTN gateway in your system, you can configure it for MVA. This function is accessed by calling a system-configured DID number that is answered and handled by an H.323 or SIP VoiceXML (VXML) gateway. After you configure your gateway, it uses a vxml script on the publisher node to pull the interactive voice response (IVR) prompts that are played to the MVA users. These prompts request user authentication and input of a number that users must dial on their phone keypad.

Before you begin

Configure Directory Number for Mobile Voice Access, on page 20

Procedure

Step 1 Configure the T1/E1 controller for PRI from the PSTN.

Example:

```
controller T1 1/0
framing esf
linecode b8zs
pri-group timeslots 1-24
```

Step 2 Configure the serial interface for the PRI (T1/E1).

Example:

```
interface Serial 1/0:23
ip address none
logging event link-status none
isdn switch-type primary 4ess
isdn incoming-voice voice
isdn bchan-number-order ascending
no cdp enable
```

Step 3 Load the VXML application from the publisher node.

Example:

Sample configuration for IOS Version 12.3 (13) and later:

```
application service CCM
http://<Unified CM Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml
```

Example:

Sample configuration before IOS Version 12.3(12):

```
call application voice Unified CCM
http://<Unified CM Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml
```

Caution Although VXML was added in Version 12.2(11), other versions such as 12.3(8), 12.3(9), 12.3(14)T1, and 12.2(15) have VXML issues.

Step 4 Configure the dial peer to associate the Cisco Unified Mobility application with system remote access.

Example:

Sample configuration for IOS 12.3(13) and later:

```
dial-peer voice 58888 pots
service CCM (Cisco Unified Mobility VXML application)
incoming called-number 58888
```

Example:

Sample configuration for IOS 12.3(12) and earlier:

```
dial-peer voice 100 pots
application CCM (Cisco Unified Mobility VXML application)
incoming called-number 58888
```

(58888 represents the mobile voice access (MVA) number)

Step 5 Add a dial peer to transfer the calls to the MVA DN.

Example:

Sample configuration for primary Unified Communications Manager:

```
dial-peer voice 101 voip
preference 1
destination-pattern <Mobile Voice Access DN>
session target ipv4:10.1.30.3
codec g711ulaw
dtmf-relay h245-alphanumeric
no vad
```

Example:

Sample configuration for secondary Unified Communications Manager (if needed):

```
dial-peer voice 102 voip
preference 2
destination-pattern <Mobile Voice Access DN>
session target ipv4:10.1.30.4
codec g711ulaw
dtmf-relay h245-alphanumeric
no vad
```

Note If a generic dial peer is already configured to terminate the calls and is consistent with the MVA DN, you do not need to perform this step.

Example:

Sample configuration for SIP gateway VoIP dial-peer:

```
dial-peer voice 80 voip
destination-pattern <Mobile Voice Access DN>
rtp payload-type nse 99
session protocol sipv2
session target ipv4:10.194.107.80
incoming called-number .T
dtmf-relay rtp-nte
codec g711ulaw
```

Configure a New H.323 Gateway for Remote Access

If you do not have an existing H.323 or SIP PSTN gateway and you want to configure mobile voice access, you must add a new H.323 gateway and configure it for MVA functionality by using the hairpinning method. From a technical standpoint, this method refers to using a second gateway to receive the inbound call, apply the MVA service and then the inbound call leg returns to the PSTN gateway (original source) after the system applies the MVA service.

Note If you use Mobile Voice Access with hairpinning, users calling into your system will not be identified automatically by their caller ID. Instead, users must enter their remote destination number manually before they enter their PIN. The reason is that the PSTN gateway must first route the call to Unified Communications Manager to reach the hairpinned Mobile Voice Access gateway. Because of this route path, the conversion of the calling number from a mobile number to an enterprise directory number occurs before the Mobile Voice Access gateway handles the call. As a result, the gateway is unable to match the calling number with a configured remote destination, and therefore the system prompts users to enter their remote destination number.

Before you begin

Configure Directory Number for Mobile Voice Access, on page 20

Procedure

Step 1 Load the VXML application from the publisher node.

Example:

Sample configuration for IOS Version 12.3 (13) and later:

```
application service CCM
http://<Unified CM Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml
```

Example:

Sample configuration before IOS Version 12.3(12):

```
call application voice CCM
http://<Unified CM Publisher IP Addr>:8080/ccmivr/pages/IVRMainpage.vxml
```

Caution Although VXML was added in Version 12.2(11), other versions such as 12.3(8), 12.3(9), 12.3(14)T1, and 12.2(15) have VXML issues.

Step 2 Configure the dial-peer to associate the Cisco Unified Mobility application with system remote access.

Example:

Sample configuration for IOS 12.3(13) and later:

```
dial-peer voice 1234567 voip
service CCM
incoming called-number 1234567
codec g711u
session target ipv4:<ip_address of call manager>
```

Example:

Sample configuration for IOS 12.3(12) and earlier:

```
dial-peer voice 1234567 voip
application CCM
incoming called-number 1234567
codec g711u
session target ipv4:<ip_address of call manager>
```

Step 3 Add a dial-peer for transferring calls to the Mobile Voice Access (MVA) DN.

Example:

Sample configuration for primary Unified Communications Manager:

```
dial-peer voice 101 voip
preference 1
destination-pattern <Mobile Voice Access DN>
session target ipv4:10.1.30.3
voice-class h323 1
codec g711ulaw
dtmf-relay h245-alphanumeric
novad
```

Example:

Sample configuration for secondary Unified Communications Manager (if needed):

```
dial-peer voice 102 voip
preference 2
destination-pattern <Mobile Voice Access DN>
session target ipv4:10.1.30.4
voice-class h323 1
codec g711ulaw
dtmf-relay h245-alphanumeric
novad
```

Note If a generic dial peer is already configured to terminate the calls and is consistent with the MVA DN, you do not need to perform this step.

Step 4 Configure hairpin.

```
voice service voip
allow-connections h323 to h323
```

Step 5 On the Unified Communications Manager, create a new route pattern to redirect the incoming MVA number to the H.323 gateway that has the vxml script loaded. Ensure that the incoming CSS of the gateway can access the partition in which the new route pattern is created.

Configure Enterprise Feature Access

Use the following procedure to configure Enterprise Feature Access from a remote destination for:

- Two-stage dialing to place enterprise calls from a configured remote destination. Calls appear to the called party as if they were placed from an associated desk phone.
- Remote destination access to mid-call features through EFA codes that are sent using DTMF digits sent from the remote destination.

Note Unlike Mobile Voice Access, with Enterprise Feature Access you must be calling from a configured remote destination.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Mobility** > **Enterprise Feature Access Number Configuration**.

Step 2 In the **Number** field, enter the unique DID number that mobile users will dial from a remote destination in order to access the Enterprise Feature Access feature.

Step 3 From the **Route Partition** drop-down list, choose the partition where the DID resides.

Step 4 (Optional) Check the **Default Enterprise Feature Access Number** check box to make this EFA number the default for this system.

Step 5 Click **Save**.

Step 6 Configure the Enteprise Feature Access service parameters:

a) From Cisco Unified CM Administration, choose **System** > **Service Parameters**.
b) From the **Server** drop-down list, choose the publisher node.
c) From the **Service** drop-down list, choose **Cisco CallManager**.
d) Set the **Enable Enterprise Feature Access** service parameter to **True**.
e) (Optional) In the **Clusterwide Parameters (System - Mobility)** area, edit the DTMF digits that you must enter to access midcall features through Enterprise Feature Access. For example, you could edit the **Enterprise Feature Access Code for Hold** service parameter, which has a default value of ***81**. The default values are as follows:

- Hold: *81
- Exclusive Hold: *82
- Resume: *83
- Transfer: *84
- Conference: *85
- Session Handoff: *74
- Starting Selective Recording: *86
- Stopping Selective Recording: *87

- Hunt group login—enter a new code
- Hunt group logout—enter a new code

f) Click **Save**.

Configure Intelligent Session Control

Configure the system so that inbound calls to a remote destination are rerouted to an associated enterprise number, if one is available. This provides automatic call anchoring within the enterprise for mobility calls, providing cost savings and added Unified Communications functionality.

Procedure

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

Step 2 From the **Server** drop-down list, choose a Cisco Unified Communications Manager node.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.

Step 4 Under **Clusterwide Parameters (Feature - Reroute Remote Desination Calls to Enterprise Number)** set the following service parameters:

- **Reroute Remote Destination Calls to Enterprise Number**—To enable Intelligent Session Control, set this parameter to **True**.
- **Ring All Share Lines**—Set the value of the parameter to **True**. If Intelligent Session Control is enabled, and this service parameter is also enabled, the system anchor calls to remote destinations within the enterprise, and will also ring all the user's shared lines.
- **Ignore Call Forward All on Enterprise DN**—This parameter applies only to outgoing calls to a remote destination when Intelligent Session Control is enabled. By default, this parameter is set to **True**.

Step 5 Click **Save**.

Configure Mobility Service Parameters

Use this procedure to configure optional Mobility-related service parameters.

Procedure

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

Step 2 From the **Server** drop-down list, choose the publisher node.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.

Step 4 Configure any service parameters that you want to edit. The Mobility-related parameters are listed under the following headings. For help descriptions, click the parameter name:

- **Clusterwide Parameters (System - Mobility)**

- **Clusterwide Parameters (System - Mobility Single Number Reach Voicemail)**
- **Clusterwide Parameters (Feature - Reroute Remote Destination Calls to Enterprise Number)**

Step 5 Click **Save**.

Dual-Mode Devices

The task in this section describe how to configure dual-mode devices that can connect over enterprise wi-fi and over remote mobile or cellular networks.

Configure Cisco Jabber Dual-Mode

Complete these tasks to configure Cisco Jabber on iPhone or Android as dual-mode mobile devices that can connect over WiFi. Cisco Jabber registers to Unified Communications Manager over WiFi and can be reached through an enterprise number if Single Number Reach is enabled in the user's mobile identity.

Procedure

	Command or Action	Purpose
Step 1	Configure a Mobility Profile, on page 28	Configure a mobility profile to send consistent caller ID to Jabber mobile clients that are placing Dial through Office calls.
Step 2	Add a Dual-Mode Device for Cisco Jabber, on page 28	Configure a dual-mode device type for Cisco Jabber on iPhone or Android clients.
Step 3	Configure a Mobility Identity, on page 31	Add a Mobility Identity to the Jabber mobile client that points to the device phone number (that is, the iPhone number) to provide calling when Jabber roams out of WiFi range. Enable Single Number Reach destination for the Mobile Identity.
Step 4	Required: Configure Handoff Number, on page 31	Configure a handoff number for dual-mode devices that are leaving enterprise. Even when the device disconnects from the enterprise WiFi network the call can be maintained without interruption by reconnecting to a remote mobile or cellular network.

Configure Other Dual-Mode Devices

Complete these tasks to configure other dual-mode mobile devices that can place calls over the cellular network and can also connect over WiFi. For example:

- Carrier-Integrated Mobile Devices that connect over Fixed Mobile Convergence (FMC) networks.
- IMS-integrated Mobile Devices over IP Multimedia networks

Procedure

	Command or Action	Purpose
Step 1	Add a Dual-Mode Device for Cisco Jabber, on page 28	Configure an IMS or FMC dual-mode device.
Step 2	Configure a Mobility Identity, on page 31	Add a Mobility Identity that points to the phone number of the actual device.
Step 3	Required: Configure Handoff Number, on page 31	Configure a handoff number for dual-mode devices that are leaving the enterprise. Even when the device disconnects from the enterprise WiFi network the call can be maintained without interruption by reconnecting to a remote mobile or cellular network.

Configure a Mobility Profile

Configure a mobility profile for dual-mode Cisco Jabber on iPhone and Android clients. The profile configures the client with a consistent caller ID for dial via office calls.

Note From a technical standpoint, this caller ID is sent during the dial via office reverse (DVO-R) callback portion of a call to the mobility identity or alternate callback number. If no mobility profile is assigned to the mobility identity or if the Callback Caller ID field is left blank, the system sends the default enterprise feature access number.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Mobility** > **Mobility Profile**.

Step 2 Click **Add New**.

Step 3 Enter a **Name** for the profile.

Step 4 From the **Mobile Client Calling Option** drop-down list, select Dial via Office Reverse.

Note Despite the field options, Dial via Office Forward is not available.

Step 5 Configure a **Callback Caller ID** for Dial-via-Office Reverse.

Step 6 Configure the fields in the **Mobility Profile Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 7 Click **Save**.

Add a Dual-Mode Device for Cisco Jabber

Use the following procedure to configure a dual-mode device type for Cisco Jabber on iPhone or Android clients.

Before you begin

Make sure that your end users are mobility-enabled. Also, if you want to add remote destinations to your Jabber client, make sure that you have a softkey template that includes the Mobility softkey.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Perform one of the following:

- Click **Find** to edit an existing device.
- Click **Add New** and select either **Cisco Dual Mode for Android** or **Cisco Dual Mode for iPhone** as the phone model, to add a new device. **Click Next**.

Step 3 Configure the fields in the **Phone Configuration** window.

For detailed information about product specific configuration layout fields, see your Jabber client documentation at http://www.cisco.com/go/jabber.

Step 4 Configure the following mandatory fields:

- Device Name
- Device Pool
- Softkey Template
- Owner User ID—The user must have mobility enabled.
- Mobility User ID—The user must have mobility enabled.
- Device Security Profile
- SIP Profile

Step 5 Click **Save**.

Step 6 Add a directory number:

a) In the left Association area, click **Add a New DN**.
b) Enter a new **Directory Number** and click **Save**.
c) Complete any fields that you want in the **Directory Number Configuration** window and click **Save**. For more information on the fields and their configuration options, see Online Help.
d) Click **Associate End Users** .
e) Click **Find** and select the mobility-enabled end user whom owns this DN.
f) Click **Add Selected**.
g) Click **Save**.

What to do next

Add a Mobility Identity that points to the phone number of the iPhone or Android device. This allows you to transfer the call to the phone if you move out of Wi-Fi range. You can also add the device as a Single Number Reach destination. For details, Configure a Mobility Identity, on page 31.

Optionally, add Remote Destinations and Single Number Reach to your Cisco Jabber client. When someone calls the Jabber client, the remote destination rings as well. Configure a Remote Destination, on page 16.

Dual-Mode Device Configuration Fields

Table 1: Dual-Mode Device Configuration Fields

Field	Description
Softkey Template	Choose the Mobility Softkey template.
Owner User ID	Choose the user ID of the assigned phone user. The user ID is recorded in the call detail record (CDR) for all calls made from this device.
Mobility User ID	Choose the user ID of the person to whom this dual-mode phone is assigned.
Device Security Profile	Choose the security profile to apply to the device. You must apply a security profile to all phones that are configured in Cisco Unified Communications Manager Administration. To enable security features for a phone, you must configure a new security profile for the device type and protocol, and then apply it to the phone.
Rerouting Calling Search Space	Choose a calling search space for routing calls to configured remote destinations and mobility identities that are configured for this device.
SIP Profile	Choose **Standard SIP Profile for Mobile Device**.

Add Other Dual-Mode Device

Use this procedure to add another dual-mode device (for example, a **Carrier-integrated Mobile Device** for network-based FMC, or an **IMS-integrated Mobile Device**.

Before you begin

Make sure that your end users are mobility-enabled. Refer to topics earlier in this chapter for details on how to enable mobility for users.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Add New**.

Step 3 From the **Phone Model** drop-down list **Carrier-integrated Mobile Device** or **IMS-integrated Mobile Device**.

Step 4 Configure the following mandatory fields:

- Device Name
- Device Pool
- Owner User ID—The user must have mobility enabled.
- Mobility User ID—The user must have mobility enabled.

Step 5 Configure the remaining fields in the **Phone Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 6 Click **Save**.

Step 7 Add a directory number:

a) In the left Association area, click **Add a New DN**.
b) Enter a new **Directory Number** and click **Save**.
c) Complete any fields that you want in the **Directory Number Configuration** window and click **Save**. For more information on the fields and their configuration options, see Online Help.
d) Click **Associate End Users**.
e) Click **Find** and select the mobility-enabled end user whom owns this DN.
f) Click **Add Selected**.
g) Click **Save**.

Configure a Mobility Identity

Add a Mobility Identity that points to the phone number of the device if you want to enable the device as a Single Number Reach that can be reached through the enterprise number.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Enter search criteria if needed, click **Find**, and choose the dual-mode device that you created.

Step 3 Click **Add New Mobility Identity**.

Step 4 In the **Destination** field, enter the phone number of the mobile device. For example, for a Cisco Jabber on iPhone client, this would be the phone number of the iPhone.

Step 5 Cisco Jabber only. Select the **Mobility Profile** that you configured.

Step 6 If you want to make this Mobile Identity available from an enteprise phone number:
a) Check the **Enable Single Number Reach** check box.
b) Configure a **Single Number Reach Voicemail** policy

Step 7 Configure a **Dial-via-Office Reverse Voicemail** policy.

Step 8 Configure the fields on the **Mobility Identity Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 9 Click **Save**.

Note If you want to apply a Ring Schedule and access list to limit calls to this mobile identity to specific times and users, Configure an Access List, on page 17.

Configure Handoff Number

Configure handoff mobility for dual-mode phones if you want your system to preserve a call while the user moves out of the enterprise. Even when a user's device disconnects from the enterprise WiFi network and reconnects to the mobile voice or cellular network, an in-progress call is maintained without interruption.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Mobility** > **Handoff Configuration**.

Step 2 In the **Handoff Number** field, enter the direct inward dialing (DID) number for handoff between the Wi-Fi and mobile voice or cellular network.

For numbers that start with the international escape character (+), you must precede the + with a backslash (\). Example: \+15551234.

Step 3 From the **Route Partition** drop-down list, choose the partition to which the handoff DID number belongs.

Step 4 Click **Save**.

Cisco Unified Mobility Interactions and Restrictions

Cisco Unified Mobility Interactions

Table 2: Cisco Unified Mobility Interactions

Feature	Interaction
Auto Call Pickup	Cisco Unified Mobility interacts with auto call pickup depending on how you configured the service parameter. When the **Auto Call Pickup Enabled** service parameter is set to **True**, users must press only the **PickUp** softkey to pick up a call. If the service parameter is set to **False**, users must press the **PickUp**, **GPickUp**, or **OPickUp** softkey and then the Answer softkey.
Automatic Alternate Routing	Cisco Unified Mobility supports automatic alternate routing (AAR) as follows: • If a rejection occurs because of a lack of bandwidth for the location-based service, the rejection triggers AAR and reroutes the call through the PSTN so the caller does not need to hang up and redial. • If a rejection occurs because of resource reservation protocol (RSVP), however, AAR is not triggered for calls to remote destinations and the call stops.
Extend and Connect	Users who need the capabilities of both Cisco Unified Mobility and Extend and Connect can configure the same remote destination on the remote device profile and CTI remote device types when the owner ID of both device types is the same. This configuration allows Cisco Unified Mobility features to be used concurrently with Extend and Connect. For more information, see the “Extend and Connect” chapter.

Feature	Interaction
External Call Control	If external call control is configured, Unified Communications Manager follows the route decision from the adjunct route server for these Cisco Unified Mobility features: • Cisco Unified Mobility • Mobile voice access • Enterprise feature access • Dial via office Unified Communications Manager does not send a routing query for the following Cisco Unified Mobility features: • Cell pickup • Desk pickup • Session handoff
Intelligent Session Control and Session Handoff	For direct calls to remote destinations that are anchored to the enterprise number, mobile users can use the session handoff feature to hand off the call to their deskphones. You must enable Cisco Unified Mobility before you implement intelligent session control.
Licensing	Cisco Unified Mobility is included in all user-based licenses from basic to professional.
Local Route Groups	For single number reach calls to a remote destination, the device pool of the originating calling party determines the selection of the standard local route group.
Number of Supported Calls	Each remote destination supports a maximum of six active calls. However, the number of supported calls depends on the Unified Communications Manager configuration. For example, the Cisco Unified Mobility user receives a call while the user already has six calls for the remote destination or while the user is using DTMF to transfer or conference a call from the remote destination. The received call is sent to the enterprise voice mail when: • The number of calls with user exceeds Busy trigger configuration • CFB is configured • All shared lines are busy **Note** The calls sent to the enterprise voice mail is not based on the maximum supported calls.
SIP Trunks with Cisco Unified Border Element	Cisco Unified Mobility supports the Cisco Unified Mobility feature without midcall features over SIP trunks with Cisco Unified Border Element (CUBE).

Cisco Unified Mobility Restrictions

Table 3: Cisco Unified Mobility Interactions

Restriction	Description
Auto Answer	A remote destination call does not work when auto answer is enabled.
Call Forwarding Unregistered	Call Forward Unregistered (CFUR) support for Cisco Jabber on iPhone and Android is as follows: • CFUR is supported if Cisco Jabber on iPhone or Android does not have either a mobile identity or remote destination configured. • CFUR is not supported, and will not work, if a Remote Destination is configured • CFUR is not supported, and will not work, if a Mobile Identity is configured with a mobile phone number and Single Number Reach is enabled. If you have a mobile identity or remote destination configured, use Call Forward Busy and Call Forward No Answer instead.
Call Queuing	Unified Communications Manager does not support call queuing with Cisco Unified Mobility.
Conferencing	Users cannot initiate a meet-me conference as conference controller by using mobile voice access, but they can join a meet-me conference. If an existing conference call is initiated from a shared-line IP phone or dual-mode phone or smartphone that is a remote destination, no new conference party can be added to the existing conference after the call is sent to a mobile phone or a dual-mode handoff action occurs. To permit the addition of new conference parties, use the **Advanced Ad Hoc Conference Enabled** service parameter.
Dialing + Character from Mobile Phones	Users can dial a + sign through dual-tone multifrequency (DTMF) on a mobile phone to specify the international escape character. Cisco Unified Mobility does not support + dialing through DTMF for IVR to make an outgoing call from a mobile phone to an enterprise IP phone for which the directory number contains the + character. Cisco Unified Mobility does not support + dialing through DTMF for two-stage dialing to make an outgoing call from a mobile phone to an enterprise IP phone for which the directory number contains the + character.

Restriction	Description
Do Not Disturb on the Desk Phone and Direct Calls to Remote Destination	If do not disturb (DND) is enabled on a desk phone, the desk phone cannot be placed in the remote In use state and the call is not anchored in the following scenarios: • DND is enabled with the call reject option. • DND is activated by pressing the DND softkey on the desk phone. If DND is enabled with the ring off option, however, the call is anchored.
Dual-Mode Phones	**Dual-Mode Handoff and Caller ID** The handoff DN method of dual-mode handoff requires a caller ID in the cellular network. The mobility softkey method does not require caller ID. **Dual-Mode Phones and CTI Applications** While a dual-mode phone is in Wi-Fi enterprise mode, no CTI applications control it nor monitor it. The **In Use Remote** indicator for dual-mode phones on a shared line call in the WLAN disappears if the dual-mode phone goes out of WLAN range. **Dual-Mode Phones and SIP Registration Period** For dual-mode phones, Unified Communications Manager determines the registration period by using the value in the **Timer Register Expires (seconds)** field of the SIP profile that associates with the phone, not the value that the **SIP Station KeepAlive Interval** service parameter specifies. The standard SIP profile for mobile devices determines the registration period as defined by the **Time Register Expires** field in that profile.
Enterprise Features From Cellular Networks	Enterprise features from cellular networks require out-of-band DTMF. When using intercluster DNs as remote destinations for an IP phone over a SIP trunk (either intercluster trunk or gateway), check the **Require DTMF Reception** check box when configuring the IP phone. This allows DTMF digits to be received out of band, which is crucial for enterprise feature access midcall features.
Gateways and Ports	Both H.323 and SIP VoIP gateways are supported for mobile voice access. Cisco Unified Mobility features are not supported for T1 CAS, FXO, FXS and BRI.
Jabber Devices	When initially configured, Jabber devices count as registered devices. These devices increase the count of registered devices in a node, set by the **Maximum Number of Registered Devices** service parameter.
Locales	Cisco Unified Mobility supports a maximum of nine locales. If more than nine locales are installed, they appear in the Available Locales pane, but you can only save up to nine locales in the Selected Locales pane. If you attempt to configure more than nine locales for Cisco Unified Mobility, the following message appears: “Update failed. Check constraint (informix.cc_ivruserlocale_orderindex) failed.”

Restriction	Description
Maximum Wait Timer for Desktop Call Pickup	If a user presses the *81 DTMF code from a remote destination (either a smartphone or any other phone) to put a call on hold, the user desk phone displays the **Resume** softkey. However, the desk phone does not apply a timer for Desktop Call Pickup. The **Resume** key continues to be displayed even after the timeout that is configured for the end user to pick up the call elapses and the call is not dropped. Instead, users should hang up the call on the remote phone, which triggers the desk phone to apply the timer for desktop call pickup. (Use the **Maximum Wait Time for Desk Pickup** field on the **End User Configuration** window to change this setting.)
Multilevel Precedence and Preemption	Cisco Unified Mobility does not work with multilevel precedence and preemption (MLPP). If a call is preempted with MLPP, Cisco Unified Mobility features are disabled for that call.
Overlap Sending	Overlap sending patterns are not supported for the Intelligent Session Control feature.
Q Signaling	Mobility does not support Q signaling (QSIG).
QSIG Path Replacement	QSIG path replacement is not supported.
Service Parameters	Enterprise feature access service parameters apply to standard phones and smartphones; however, smartphones generally use one-touch keys to send the appropriate codes. You must configure any smartphones that will be used with Cisco Unified Mobility to use either the default codes for enterprise feature access or the codes that are specified in the smartphone documentation.
Session Handoff	The following limitations apply to the session handoff feature: • Session handoff can take place only from mobile phone to desk phone. For session handoff from desk phone to mobile phone, the current remote destination pickup method specifies that you must use send call to mobile phone. • Only audio call session handoff is supported.
Single Number Reach with Hunt Groups	If you have a hunt group configured and one or more of the directory numbers that the hunt group points toward also has Single Number Reach (SNR) enabled, the call does not extend to the SNR remote destinations unless all devices in the hunt group are logged in. For each device within the hunt group, the **Logged Into Hunt Group** check box must be checked within the **Phone Configuration** window for that device.
SIP Trunks	The Cisco Unified Mobility feature is supported only for primary rate interface (PRI) public switched telephone network (PSTN) connections. For SIP trunks, Cisco Unified Mobility is supported over IOS gateways or intercluster trunks.

Restriction	Description
SIP URI and Direct Calls to Remote Destination	The Intelligent session control feature does not support direct URI dialing. Therefore, calls that are made to a SIP URI cannot be anchored to an enterprise number.
Unified Communications Manager publisher dependent features	In a cluster environment, the publisher must be reachable in order to enable or disable Single Number Reach. Some features may not function if the publisher is not actively running. Mobile voice access is not available when the publisher node is not reachable; IVR prompts for Mobile Voice Access are stored only on the publisher.
Video Calls	Cisco Unified Mobility services do not extend to video calls. A video call that is received at the desk phone cannot be picked up on the mobile phone.
Mobile Voice Access (MVA)	Cisco 4000 Series Integrated Services Routers do not support Voice XML (VXML). Hence, when these routers function as Unified Communications gateways with Cisco Unified Communications Manager, they do not support Mobile Voice Access (MVA) application.

Related Topics

Ad Hoc Conferencing Service Parameters, on page 188

Cisco Unified Mobility Troubleshooting

Cannot Resume Call on Desktop Phone

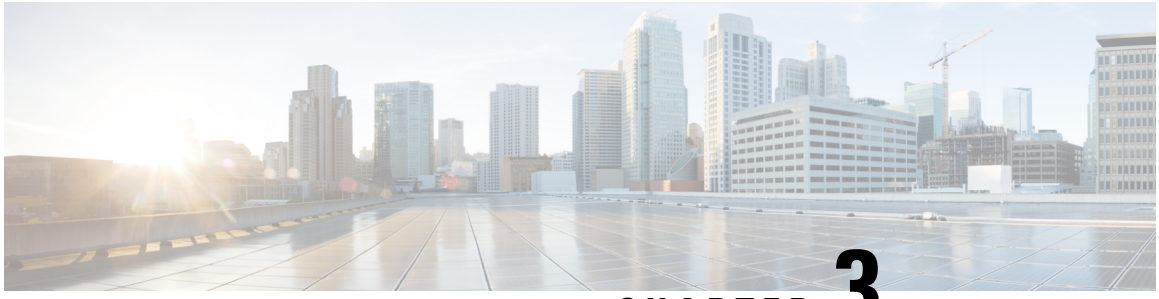
Problem When a remote destination (mobile phone) is not a smartphone and a call to this mobile phone is anchored through Cisco Unified Communications Manager, the user can hang up the mobile phone and expect to see a **Resume** softkey on the user desktop phone to resume the call. The user cannot resume this call on the user desktop phone.

Possible Cause If the calling party receives a busy, reorder, or disconnect tone when the mobile phone hangs up, the mobile phone provider probably did not disconnect the media. No disconnect signals came from the provider. To verify this possibility, let the calling party wait for 45 seconds. After this wait, the service provider will time out and send disconnect signals, at which time Cisco Unified Communications Manager can provide a **Resume** softkey to resume the call.

- Add the following command to the gateway:

```
voice call disc-pi-off
```

- For the Cisco CallManager service, set the **Retain Media on Disconnect with PI for Active Call** service parameter to **False**.



CHAPTER 3

Device Mobility

Device Mobility Overview

Device mobility allows devices to assume settings based on their location. Your system uses the device IP subnets to determine the exact location of the device. By enabling device mobility within a cluster, you allow mobile users to roam from one site to another and acquire the site-specific settings. Your system then uses these dynamically allocated settings for functions such as call routing, codec selection, and media resource selection.

Device Mobility Prerequisites

- The phone must have a dynamic IP address to use device mobility. If a phone with a static IP address roams, Unified Communications Manager uses the configuration settings from its home location.
- The Device Mobility feature requires you to set up device pools with site-specific settings. This chapter describes only the device pool settings that relate to device mobility. For more detailed information on configuring device pools, see the "*Configure Device Pools*" chapter in the System Configuration Guide for Cisco Unified Communications Manager.
- Cisco Database Layer Monitor service must be running on the same node as the Cisco CallManager service.
- Cisco TFTP service must be running on at least one node in the cluster.
- Cisco Unified Communications Manager Locale Installer (if you want to use non-English phone locales or country-specific tones).
- Any phone that runs either SCCP or SIP.

Device Mobility Configuration Task Flow

Before you begin

- Review Device Mobility Prerequisites, on page 39.

Procedure

	Command or Action	Purpose
Step 1	To Enable Device Mobility, on page 41, perform one or both of the following subtasks: • Enable Device Mobility Clusterwide, on page 41 • Enable Device Mobility for Individual Devices, on page 42	Perform these procedures as needed for your configuration. You can configure Device Mobility to be enabled across your cluster, for individual devices, or a combination of enabled and disabled for devices.
Step 2	Configure a Physical Location, on page 42	Configure the geographic location so that your system can determine which network resources to assign to a device. If a user moves away from the home location, the system ensures that the device uses local media resources and the correct bandwidth for the call.
Step 3	Configure a Device Mobility Group, on page 43	Configure the device mobility group to define a logical group of sites with similar dialing patterns (for example, US_dmg and EUR_dmg). Depending on the network size and scope, your device mobility groups can represent countries, regions, states, provinces, or cities. For example, an enterprise with a worldwide network can choose device mobility groups that represent individual countries, whereas an enterprise with a national or regional network can define device mobility groups that represent states, provinces, or cities.
Step 4	Configure Device Mobility Information, on page 43	Configure device mobility information such as the subnets and device pools that are used for device mobility. When a phone registers, your system compares the IP address of the device to the subnets that are configured device mobility in the **Device Mobility Info Configuration** window. The best match uses the largest number of bits in the IP subnet mask (longest match rule). For example, the IP address 9.9.8.2 matches the subnet 9.9.8.0/24 rather than the subnet 9.9.0.0/16.

	Command or Action	Purpose
Step 5	Configure a Device Pool for Device Mobility, on page 44	Unified Communications Manager assigns a device pool to an IP phone based on the device's IP subnet. The following steps describe the behavior: • The IP phone tries to register to Unified Communications Manager by sending its IP address in the registration message. • Unified Communications Manager derives the device's IP subnet and matches it with the subnet configured as part of the device mobility information. • If the subnet matches, Unified Communications Manager provides the device with a new configuration based on the device pool configuration.
Step 6	(Optional) View Roaming Device Pool Parameters, on page 46	Follow this procedure if you want to view and verify the current device mobility settings for a device.

Enable Device Mobility

Perform these procedures as needed for your configuration. You can configure Device Mobility to be enabled across your cluster, for individual devices, or a combination of enabled and disabled for devices.

Procedure

	Command or Action	Purpose
Step 1	Enable Device Mobility Clusterwide, on page 41	Activate a service parameter if you want to enable device mobility on all devices in the cluster.
Step 2	Enable Device Mobility for Individual Devices, on page 42	Follow this procedure if you want to enable device mobility for an individual device or if you want to specify a different value for individual devices.

Enable Device Mobility Clusterwide

Use the following procedure to configure a service parameter that sets the default device mobility setting to **On** for all phones clusterwide except where there is an overriding configuration in that phone's **Phone Configuration**.

Procedure

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

Step 2 From the **Server** drop-down list, choose the node that is running the Cisco CallManager service.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager Service**.

Step 4 Under **Clusterwide Parameters (Device - Phone)**, set the **Device Mobility Mode** service parameter to **On**.

Step 5 Click **Save**.

For devices that are already registered, you must restart the **Cisco CallManager** service for this new setting to be enabled.

What to do next

If you want to configure device mobility settings for an individual device, go to Enable Device Mobility for Individual Devices, on page 42.

Otherwise, you can begin configuring the system for device mobility. Go to Configure a Physical Location, on page 42.

Enable Device Mobility for Individual Devices

Use this procedure to enable device mobility for an individual device. This configuration overrides the setting of the **Device Mobility Mode** clusterwide service parameter.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select the device that you want to configure.

Step 3 From the **Device Mobility Mode** drop-down list, choose one of the following:

- **On**—Device mobility is enabled for this device.
- **Off**—Device mobility is disabled for this device.
- **Default**—The device uses the setting of the **Device Mobility Mode** clusterwide service parameter. This is the default setting.

Step 4 Click **Save**.

Configure a Physical Location

Use this procedure to configure a physical location that you will assign to a device pool. Device Mobility uses the location of the device registration to assign an appropriate device pool.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Physical Location**.

Step 2 Click **Add New**.

Step 3 Enter a **Name** for the location.

Step 4 Enter a **Description** for the location.

Step 5 Click **Save**.

Configure a Device Mobility Group

Use the following procedure to configure device mobility group is a logical grouping of sites with similar dialing patterns. For example, a company with a worldwide network may want to set up device mobility groups that represent individual countries.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Device Mobility** > **Device Mobility Group**.

Step 2 Click **Add New**.

Step 3 Enter a **Name** for the device mobility group.

Step 4 Enter a **Description** for the device mobility group.

Step 5 Click **Save**.

Configure Device Mobility Information

Use this procedure to configure Device Mobility Info, representing the IP subnets to which roaming devices can register and the corresponding device pools that the system can assign to roaming devices.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Device Mobility** > **Device Mobility Info**.

Step 2 Click **Add New**.

Step 3 Enter a **Name** for the Device Mobibility Info.

Step 4 Enter the IP subnet details for roaming device registrations.

- If you are using IPv4 addresses for your mobile devices, complete the IPv4 subnet details.
- If you are using IPv6 addresses for your mobile devices, complete the IPv6 subnet details.

Step 5 Select the device pools that you want the system to assign for roaming devices that register to one of these subnets. Use the arrows to move the appropriate device pools from the **Selected Device Pools** list box to the **Available Device Pools**s list box.

Step 6 Click **Save**.

For more information on the fields and their configuration options, see Online Help.

Configure a Device Pool for Device Mobility

Use this procedure to set up a device pool with parameters that you configured for device mobility.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Device Pool**.

Step 2 Do either of the following:

- Click **Find** and select an existing device pool.
- Click **Add New** to create a new device pool.

Step 3 Under **Roaming Sensitive Settings**, assign the parameters that you set up in the previous device mobility tasks:

- **Physical Location**—From the drop-down list, select the physical location that you set up for this device pool. Device mobility uses this location to assign a device pool for a roaming device.
- **Device Mobility Group**—From the drop-down list, select the device mobility group that you set up for this device pool.

Step 4 Under **Device Mobility Related Information**, configure the following device mobility-related fields. For more information on the fields and their configuration options, see Online Help.

- **Device Mobility Calling Search Space**—Select the CSS to be used by a roaming device that uses this device pool.
- **AAR Calling Search Space**—Select the calling search space for the device to use when automated alternate routing (AAR) is performed.
- **AAR Group**—If AAR is configured, select the AAR Group for this device.
- **Calling Party Transformation CSS**—Select the calling party transformation CSS for roaming devices that use this device pool.

Note
- The **Calling Party Transformation CSS** overrides the device level configuration for roaming devices, even if the **Use Device Pool Calling Party Transformation CSS** check box is unchecked in the **Phone Configuration** window.
- **The Called Party Transformation CSS** setting is applied to the gateway rather than to the roaming device.

Step 5 Configure any remaining fields in the **Device Pool Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 6 Click **Save**.

Device Pool Fields for Device Mobility

The following table contains the settings in the **Device Pool Configuration** window that are relevant to setting up device mobility.

Field	Description
Roaming Sensitive Settings	
Physical Location	From the drop-down list, choose the physical location for this device pool. The system uses physical location with the Device Mobility feature to identify the parameters that relate to a specific geographical location.
Device Mobility Group	From the drop-down list, choose the device mobility group.
Device Mobility Related Information	
Device Mobility Calling Search Space	From the drop-down list, choose the calling search space to be used as the device calling search space when the device is roaming and in same device mobility group.
AAR Calling Search Space	From the drop-down list, choose the calling search space for the device to use when automated alternate routing (AAR) is performed. The AAR calling search space is the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth.
AAR Group	From the drop-down list, choose the AAR group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of **None** specifies that no rerouting of blocked calls is attempted.

Field	Description
Calling Party Transformation CSS	This setting allows you to localize the calling party number on the device. Ensure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device pool. **Note** Before the call occurs, the device must apply the transformation by using digit analysis. If you choose **None** and you check the **Use Device Pool Calling Party Transformation CSS** check box in the device configuration window, the transformation does not match and is not applied. Ensure that you configure the calling party transformation pattern in a partition that is not used for routing.
Called Party Transformation CSS	This setting allows you to localize the called party number on the device. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device pool. **Note** If you choose **None**, the transformation does not match and is not applied. Ensure that you configure the called party transformation pattern in a partition that is not used for routing.

View Roaming Device Pool Parameters

Use the following procedure to view and verify the current device mobility settings for a device.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Enter search criteria and click **Find** to find the device with device mobility mode enabled.

Step 3 Click **View Current Device Mobility Settings** next to the **Device Mobility Mode** field.

The roaming device pool settings appear. If the device is not roaming, the home location settings appear.

Device Mobility Interactions and Restrictions

Device Mobility Interactions

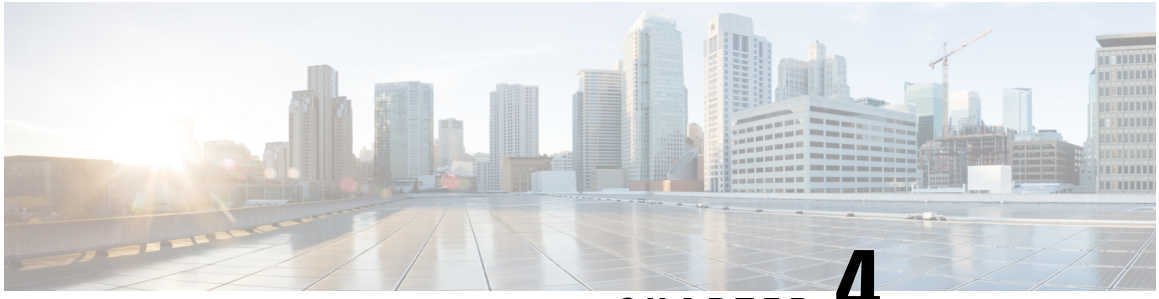
Table 4: Device Mobility Interactions

Feature	Interaction
Calling Party Normalization	Calling party normalization enhances the dialing capabilities of some phones and improves call-back functionality when a call is routed to multiple geographical locations; that is, the feature ensures that the called party can return a call without the need to modify the directory number in the call log directories on the phone. Additionally, calling party normalization allows you to globalize and localize phone numbers, so the appropriate calling number presentation is displayed on the phone.
Roaming	When a device is roaming in the same device mobility group, Unified Communications Manager uses the device mobility CSS to reach the local gateway. If a user sets call forward all (CFA) at the phone, the CFA CSS is set to None, and the CFA CSS activation policy is set to With Activating Device/Line CSS, then the following behaviors will occur, depending on the device location: • The Device CSS and Line CSS are used as the CFA CSS when the device is in its home location. • If the device is roaming within the same device mobility group, the device mobility CSS from the roaming device pool and the line CSS are used as the CFA CSS. • If the device is roaming within a different device mobility group, the Device CSS and Line CSS are used as the CFA CSS.

Device Mobility Restrictions

Table 5: Device Mobility Restrictions

Restriction	Description
IP Address	The device mobility feature depends on the IPv4 address of the device that registers with Unified Communications Manager. • The phone must have a dynamic IPv4 address to use the device mobility. • If the device is assigned an IP address by using network address translation (NAT) or port address translation (PAT), the IP address that is provided during registration may not match the actual IP address of the device.
IPv6	Device mobility supports only IPv4 addresses, so you cannot use phones with an IP addressing mode of IPv6 only with the device mobility.



CHAPTER 4

Extend and Connect

Extend and Connect Overview

The Extend and Connect feature allows administrators to deploy Unified Communications Manager (UC) Computer Telephony Integration (CTI) applications that interoperate with any endpoint. With Extend and Connect, users can access UC applications from any location using any device.

The Extend and Connect feature for Unified Communications Manager provides the following UC features:

- Receive incoming enterprise calls
- Make Call
- Disconnect
- Hold and Retrieve
- Redirect and Forward
- Call Forward All
- Do Not Disturb
- Play Dual Tone Multi Frequency (DTMF) (out-of-band and in-band)
- Consult Transfer, Conference
- Add, edit, and delete remote destinations
- Set remote destination as Active or Inactive
- Persistent Connection
- Play Whisper Announcement

Extend and Connect Prerequisites

- Cisco Jabber, Release 9.1(1) or later
- Cisco Unified Workspace License (CUWL) Standard, CUWL Professional, or Cisco User Connect License (UCL) - Enhanced

Extend and Connect Configuration Task Flow

This section describes the procedures that you must complete to provision Unified Communications Manager users with Extend and Connect capabilities. For information about provisioning Cisco Jabber for Windows users with Extend and Connect, see the Cisco Jabber for Windows Installation and Configuration Guide.

Before you begin

Procedure

	Command or Action	Purpose
Step 1	Configure User Account, on page 50	Enable mobility for users so that they can use CTI remote devices. CTI devices are off-cluster phones that work with Cisco UC applications.
Step 2	Add User Permissions, on page 51	Add access control group permissions.
Step 3	Create CTI Remote Devices, on page 52	Configure off-cluster phones that users can use with Cisco UC applications.
Step 4	Add Directory Number to a Device, on page 52	Associate a directory number with the CTI remote device.
Step 5	Add Remote Destination, on page 53	Add a numerical address or directory URI that represents the other phones that the user owns.
Step 6	Verify Remote Destination, on page 54	Verify if the remote destination is successfully added for a user.
Step 7	Associate User with Device, on page 54	Associate an end user account to the CTI remote device.

Configure User Account

Use the following procedure to configure a new or existing user in Unified Communications Manager, you must enable user mobility so that they can use CTI remote devices. If you do not enable mobility for users, you cannot assign those users as owners of CTI remote devices.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **End User**.

Step 2 Perform either of the following:

- Click **Add New**, to configure a new user.
- Apply the filters using the **Find User Where** field and click **Find** to retrieve a list of users.

Note You may add the new end user account through LDAP integration or local configuration.

Step 3 Locate the **Mobility Information** section.

Step 4 Check the **Enable Mobility** check box.

Step 5 Click **Save**.

Add User Permissions

After the end user is active in Unified Communications Manager, add access control group permissions.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **End User**.

Step 2 Specify the appropriate filters in the **Find User Where** field, and then select **Find** to retrieve a list of users.

Step 3 Select the user from the list.

Step 4 Locate the **Permissions Information** section.

Step 5 Click **Add to Access Control Group**.

The **Find and List Access Control Groups** window appears.

Step 6 Click **Find**.

The Access Control Group list for Standard Users appears.

Step 7 Check the check boxes next to the following permissions:

- Standard CCM End-Users
- Standard CTI Enabled

Step 8 Click **Add Selected**.

Step 9 Click **Save**.

Create CTI Remote Devices

Use the following procedure to create a CTI remote device is a device type that represents off-cluster phones that users can use with Cisco UC applications. The device type is configured with one or more lines (directory numbers) and one or more remote destinations.

Unified Communications Manager provides Extend and Connect capabilities to control calls on devices such as public switched telephone network (PSTN) phones and private branch exchange (PBX) devices.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Add New**.

Step 3 Select **CTI Remote Device** from the **Phone Type** drop-down list and then click **Next**.

Step 4 Select the appropriate user ID from the **Owner User ID** drop-down list.

Note Only users for whom you enable mobility are available from the **Owner User ID** drop-down list.

Unified Communications Manager populates the **Device Name** field with the user ID and a CTRID prefix, for example, *CTRIDusername*.

Step 5 Edit the default value in the **Device Name** field, if appropriate.

Step 6 Enter a meaningful description in the **Description** field.

Note Cisco Jabber displays device descriptions to users. If Cisco Jabber users have multiple devices of the same model, the descriptions from Unified Communications Manager help users tell the difference between them.

Step 7 Ensure that you select an appropriate option from the **Rerouting Calling Search Space** drop-down list in the **Protocol Specific Information** section.

The **Rerouting Calling Search Space** drop-down list defines the calling search space for rerouting and ensures that users can send and receive calls from the CTI remote device.

Step 8 Configure the remaining fields in the **Phone Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 9 Click **Save**.

The fields to associate directory numbers and add remote destinations are displayed in the **Phone Configuration** window.

Add Directory Number to a Device

A directory number (DN) is a numerical address that is configured as a line on the CTI remote device. A DN typically represents the primary work number of a user (for example, 2000 or +1 408 200 2000).

Note

- The Calling Search Space (CSS) and partition of DN are mandatory on devices.
- The CTI Remote Device should not block its own DN. The CSS is important for the CTIRD device to reach its own DN.

Follow these steps to add a directory number to a CTI remote device.

Procedure

Step 1 Locate the **Association Information** section in the **Phone Configuration** window.

Step 2 Click **Add a new DN**.

Step 3 Specify a directory number in the **Directory Number** field.

Step 4 Configure all other required fields. For more information on the fields and their configuration options, see Online Help.

Step 5 Click **Save**.

Add Remote Destination

Use the following procedure to add a remote destination is a numerical address or directory URI that represents the other phones that the user owns (for example, a home office line or other PBX phone). A remote destination may be any off-cluster device. Unified Communications Manager automatically applies application dial rules to all remote destination numbers for CTI remote devices. By default, four remote destinations are supported per device. You can set the maximum number to 10 remote destinations per device in **End User Configuration** window.

Note You can determine which remote destination the Jabber client has set as Active by opening the **Phone Configuration** window from the Cisco Unified Communications Manager Administration interface.

Note Unified Communications Manager users can add remote destinations through the Cisco Jabber interface. For more information, see the Cisco Jabber for Windows Installation and Configuration Guide.

- Unified Communications Manager automatically verifies whether it can route calls to remote destinations that Cisco Jabber users add through the client interface.
- Unified Communications Manager does not verify whether it can route calls to remote destinations that you add through the Cisco Unified Communications Manager Administration interface.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Specify the appropriate filters in the **Find Phone Where** field to and then click **Find** to retrieve a list of phones.

Step 3 Select the CTI remote device from the list.

Step 4 Locate the **Associated Remote Destinations** section.

Step 5 Click **Add a New Remote Destination**.

Step 6 Enter the destination number in the **Destination Number** field.

To use the remote destination with Cisco Jabber clients, you must configure the destination name as *JabberRD*.

Step 7 Configure the remaining fields in the **Remote Destination Information** window. For more information on the fields and their configuration options, see Online Help.

Step 8 Click **Save**.

Verify Remote Destination

Perform these steps to verify if the remote destination is successfully added for a user.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Specify the appropriate filters in the **Find Phone Where** field to and then click **Find** to retrieve a list of phones.

Step 3 Select the CTI remote device from the list.

Step 4 Locate the **Associated Remote Destinations** section and verify that the remote destination is available.

Step 5 Click **Apply Config**.

Note The Device Information section on the **Phone Configuration** window indicates when a remote destination is active or controlled by Cisco Jabber.

Associate User with Device

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **End User**.

Step 2 Specify the appropriate filters in the **Find User Where** field to and then click **Find** to retrieve a list of users.

Step 3 Select the user from the list.

Step 4 Locate the **Device Information** section.

Step 5 Click **Device Association**.

Step 6 Find and select the CTI remote device.

Step 7 To complete the association, click **Save Selected/Changes**.

Step 8 From **Related Links** drop-down list, choose **Back to User**, and then click **Go**.
The **End User Configuration** window appears, and the associated device that you chose appears in the **Controlled Devices** pane.

Extend and Connect Interactions and Restrictions

Extend and Connect Interactions

Table 6: Extend and Connect Interactions

Feature	Interaction
Directory URI Dialing	Configure a Directory URI as the DN, remote destination, or both for the CTI remote device.
Unified Mobility	Extend and Support does not support moving active calls between a Cisco Unified IP Phone and a remote destination. If you want the capabilities of both Unified Mobility and Extend and Connect, you can configure the same remote destination on the Remote Device Profile and CTI Remote Device types when the Owner ID of both device types is the same. This configuration allows Cisco Mobility features to be used concurrently with Extend and Connect. The ability to configure the same remote destination on both device types is supported using Cisco Unified Communications Manager Release 10.0(1) or later. Do not configure remote destinations that are used with the Cisco Extend and Connect feature on Cisco Dual-mode for iPhone, Cisco Dual-mode for Android, and Carrier-integrated Mobile device types. Do not use prefixes to differentiate the same remote destination address. For example, 91-4085555555 and +1-4085555555 are treated as the same number.
Hunt List	The Extend and Connect feature allows users to receive hunt calls on remote destination phones under the following conditions: • The user has a Cisco Unified IP Phone. • The Cisco Unified P Phone is available to answer hunt calls (logged-in/HLog). • Cisco Jabber is running in Extend and Connect mode.

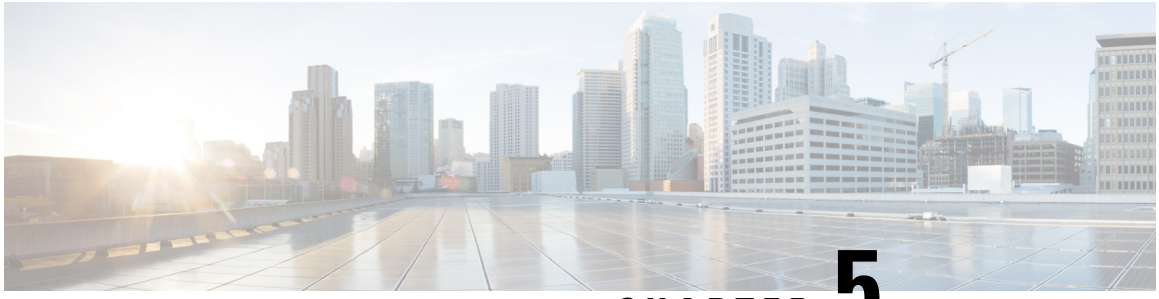
Feature	Interaction
CallerID Information	• The incoming caller ID information (name and number) is displayed on the Jabber client. • This information may also be displayed on the device, depending on your carrier and trunk configuration. • Outbound Dial Via Office calls to the remote destination display *Voice Connect* as the name and the trunk DID as the number. • Configure the trunk DID in the Unified CM Trunk Pattern, Route Pattern, or Cisco Gateway. This configuration may also be assigned by the carrier. The number field may display as blank if the trunk DID is not configured. • Outbound calls to the desired party display the CTI Remote Device Display Name and Directory Number (DN) as configured in Unified Communications Manager. • Remote destination numbers are never displayed to the called party.

Extend and Connect Restrictions

Table 7: Extend and Connect Restrictions

Restriction	Description
Maximum number of remote destinations	You can configure up to ten remote destinations for each CTI remote device. **Note** By default, four remote destinations are supported per device. You can set the maximum number to 10 remote destinations per device.
Off-cluster devices	• Remote destination numbers must represent off-cluster devices. • Remote destinations can be off-cluster URIs.
Directory numbers	You cannot configure directory numbers as remote destination numbers.
Cisco Jabber	Before you save the remote destinations that are configured using Cisco Jabber, verify if the remote destinations can be routed by the configured dial plan.
Application dial rules	Application Dial Rules are applied to all remote destinations that are configured on the CTI remote device through the Cisco Unified Communications Manager Administration interface and Cisco Jabber. **Note** Advise end users which number formats the Application Dial Rules are configured to support (for example, nn-nnn-nnnn, E.164, both).
Remote destination number	Each remote destination number must be unique within the cluster. **Note** The same remote destination number cannot be used by two or more users.

Restriction	Description
Remote destination validation	• Remote destination numbers are validated using the CTI remote device reroute calling search space. • Remote destinations that are configured using the Cisco Unified Communications Manager Administration interface and AXL interface are not validated.



CHAPTER 5

Remote Worker Emergency Calling

Remote Worker Emergency Calling Overview

The Remote Worker Emergency Calling feature enables customers to provide reliable emergency calling support to remote workers by using remote Virtual Private Network (VPN) connections. Emergency calls from off-premises users are routed to the Public Safety Answering Point (PSAP), and user-provided location information is delivered with each call.

To use this feature, remote workers must confirm or update their location whenever their device registration is interrupted. A customizable disclaimer notice is first displayed on the devices that are designated for off-premises (connected remotely to the customer network), which advises the users to provide correct location information. After the location information is provided, the off-premises location that is currently associated with the designated device is displayed. Users can confirm their current location or select another previously stored location from their device display; if their location is new, they are directed to the Cisco Emergency Responder Off-Premises User web page to create a new location.

Before completing this process, the administrator may restrict the device to calling a single configured destination. This action ensures that the device user has acknowledged the disclaimer and provided current location information before the device is enabled for normal use.

Remote Worker Emergency Calling Prerequisites

You must configure Intrado (a third party application) on the Cisco Emergency Responder before you configure the Remote Worker Emergency Calling feature. For information about configuring Intrado on the Cisco Emergency Responder, see Cisco Emergency Responder Administration Guide

Remote Worker Emergency Calling Configuration Task Flow

Before you begin

Procedure

	Command or Action	Purpose
Step 1	Configure User As a Remote Worker, on page 60	Associate the off-premises device with the owner of the device.
Step 2	Specify Alternate Routing for Emergency Calling, on page 61	These parameters specify the calling search space and destination number that are used to restrict the routing of any call that is made from a registered off-premises device where the user chose not to set a location. If these parameters are not configured, calls are routed normally.
Step 3	Configure the Application Server, on page 61	Direct end users to the application server where they enter the location of the device.
Step 4	Configure E911 Messages, on page 61	Configure the E911 messages that appear on an off-premises end-user phone.

Configure User As a Remote Worker

Before you begin

Ensure that you have configured Intrado on the Cisco Emergency Responder. For more information about configuring Intrado on the Cisco Emergency Responder, see Cisco Emergency Responder Administration Guide.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Enter the appropriate search criteria to find the phone and click **Find**.
A list of phones that match the search criteria is displayed.

Step 3 Choose the phone for which you want to configure Remote Worker Emergency Calling.
The **Phone Configuration** window is displayed.

Step 4 From the **Device Information** section, select the appropriate user ID from the **Owner User ID** drop-down list and check the **Remote Device** check box.

Step 5 Click **Save**.

Specify Alternate Routing for Emergency Calling

Perform the following steps to configure calling search space and destination number. These parameters are used to restrict the routing of any call made from a registered off-premises device where the user has not set a location. If you do not configure these parameters, the calls are routed normally.

Procedure

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

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

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.
The **Service Parameter Configuration** window appeares.

Step 4 In the **Clusterwide Parameters (Emergency Calling for Required Off-premise Location)** section, specify **Alternate Destination for Emergency Call**.

Step 5 Specify **Alternate Calling Search Space for Emergency Call**.

Step 6 Click **Save**.

Configure the Application Server

You must configure the application server to enable the E911 Proxy to communicate with the Cisco Emergency Responder. E911 proxy is used to direct the users to the application server where they enter the location of the device.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Application Server**.

Step 2 Click **Add New**.
The **Application Server** window appears.

Step 3 From the **Application Server Type** drop-down list, select **CER Location Management**.

Step 4 Click **Next**.

Step 5 In the **Name** field, specify a name to identify the application server that you are configuring.

Step 6 In the **IP address** field, specify the IP address of the server that you are configuring.

Step 7 From the list of **Available Application Users**, select the application user and click the **Down** arrow.

Step 8 In the **End User URL** field, enter a URL for the end users that are associated with this application server.

Step 9 Click **Save**.

Configure E911 Messages

Use the following procedure to select and edit E911 messages for off-premises devices.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **E911 Messages**.

Step 2 Select the required language link of the E911 messages.

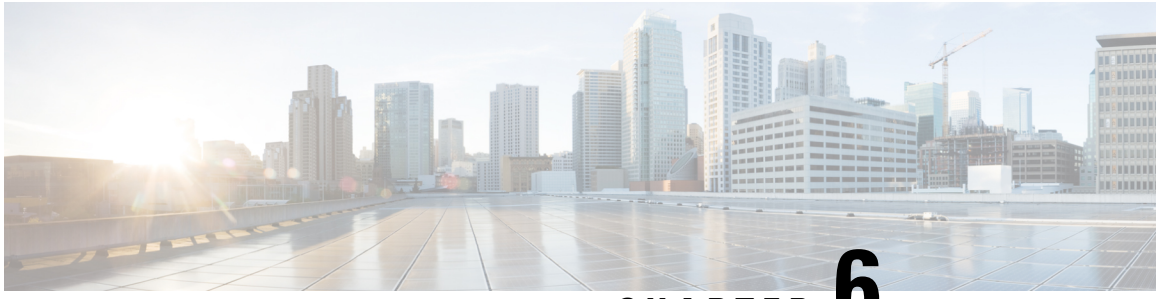
The **E911 Messages Configuration** page displays the Agreement, Disclaimer, and Error messages.

Step 3 (Optional) Edit the E911 messages to be displayed on off-premises devices.

Step 4 Click **Save**.

PART III

Remote Network Access



CHAPTER 6

Wireless LAN

Wireless LAN Overview

This feature removes the need for users to configure WiFi parameters on their phones. You can configure WiFi profiles for them. Devices can then automatically download and apply the WiFi configuration from your system. You can configure a network access profile, which contains further security layers that are related to VPN connectivity and HTTP proxy settings.

Wireless LAN Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Generate a Phone Feature List, on page 3	Generate a report to identify devices that wireless LAN profiles.
Step 2	Configure a Network Access Profile, on page 66	**Optional:** Configure a network access profile if you want to configure VPN and HTTP proxy settings that you can link to a wireless LAN profile.
Step 3	Configure a Wireless LAN Profile, on page 66	Configure a wireless LAN profile with common WiFi settings to apply to devices or device pools in the enterprise.
Step 4	Configure a Wireless LAN Profile Group, on page 66	Group wireless LAN profiles together.
Step 5	To Link a Wireless LAN Profile Group to a Device or Device Pool, on page 67, perform one of the following subtasks:	After you complete the device link, TFTP adds the wireless LAN profile group to the existing device configuration file, which the device (or

	Command or Action	Purpose
	• Link a Wireless LAN Profile Group to a Device, on page 67 • Link a Wireless LAN Profile Group to a Device Pool, on page 67	devices that are tied to a device pool) proceeds to download.

Configure a Network Access Profile

Configure a network access profile if you want to configure VPN and HTTP proxy settings that you can link to a wireless LAN profile.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Network Access Profile**

Step 2 Click **Add New**.

Step 3 Configure the fields in the **Network Access Profile Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 4 Click **Save**.

Configure a Wireless LAN Profile

Configure a wireless LAN profile with common WiFi settings to apply to devices or device pools in enterprise.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Wireless LAN Profile**

Step 2 Click **Add New**.

Step 3 Configure the fields in the **Wireless LAN Profile Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 4 Click **Save**.

Configure a Wireless LAN Profile Group

Group your wireless LAN profiles.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Wireless LAN Profile Group**.

Step 2 Click **Add New**.

Step 3 Configure the fields in the **Wireless LAN Profile Group Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 4 Click **Save**.

Link a Wireless LAN Profile Group to a Device or Device Pool

After you complete the device link, TFTP adds the wireless LAN profile group to the existing device configuration file, which the device (or devices tied to a device pool) proceeds to download.

Procedure

	Command or Action	Purpose
Step 1	Link a Wireless LAN Profile Group to a Device, on page 67	
Step 2	Link a Wireless LAN Profile Group to a Device Pool, on page 67	

Link a Wireless LAN Profile Group to a Device

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Perform one of the following tasks:

- Click **Find** to enter search criteria and choose an existing device from the resulting list.
- Click **Add New**, and choose the device type from the **Phone Type** drop-down list.

Step 3 From the **Wireless LAN Profile Group** drop-down list, choose a wireless LAN profile group that you created.

Step 4 Click **Save**.

Link a Wireless LAN Profile Group to a Device Pool

If you link a wireless LAN profile group at the device and device pool level, your system uses the device pool setting.

Procedure

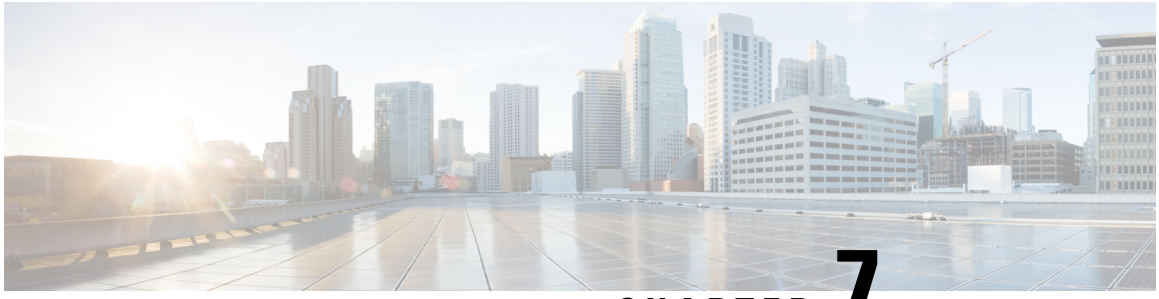
Step 1 From Cisco Unified CM Administration, choose **System** > **Device Pool**.

Step 2 Perform one of the following tasks:

- Click **Find** to enter search criteria and choose an existing device pool from the resulting list.
- Click **Add New**.

Step 3 From the **Wireless LAN Profile Group** drop-down list, choose a wireless LAN profile group that you created.

Step 4 Click **Save**.



CHAPTER 7

VPN Client

VPN Client Overview

The Cisco VPN Client for Cisco Unified IP Phone creates a secure VPN connection for employees who telecommute. All settings of the Cisco VPN Client are configured through Cisco Unified Communications Manager Administration. After the phone is configured within the Enterprise, the users can plug it into their broadband router for instant connectivity.

Note The VPN menu and its options are not available in the U.S. export unrestricted version of Unified Communications Manager.

VPN Client Configuration Task Flow

Pre-provision the phone and establish the initial connection inside the corporate network to retrieve the phone configuration. You can make subsequent connections using VPN, as the configuration is already retrieved on the phone.

Procedure

	Command or Action	Purpose
Step 1	Complete Cisco IOS Prerequisites, on page 70	Complete Cisco IOS prerequisites. Perform this action if you want to configure Cisco IOS VPN.
Step 2	Configure Cisco IOS SSL VPN to Support IP Phones , on page 71	Configure Cisco IOS for VPN client on an IP Phone. Perform this action if you want to configure Cisco IOS VPN.
Step 3	Complete ASA Prerequisites for AnyConnect, on page 72	Complete ASA prerequisites for AnyConnect. Perform this action if you want to configure ASA VPN.

	Command or Action	Purpose
Step 4	Configure ASA for VPN Client on IP Phone, on page 73	Configure ASA for VPN client on an IP Phone. Perform this action if you want to configure ASA VPN.
Step 5	Configure the VPN concentrators for each VPN Gateway.	To avoid long delays when the user upgrades the firmware or configuration information on a remote phone, set up the VPN concentrator close in the network to the TFTP or Unified Communications Manager server. If this is not feasible in your network, you can set up an alternate TFTP or load server that is next to the VPN concentrator.
Step 6	Upload VPN Concentrator Certificates, on page 75	Upload the VPN concentrator certificates.
Step 7	Configure VPN Gateway, on page 76	Configure the VPN gateways.
Step 8	Configure VPN Group, on page 77	After you create a VPN group, you can add one of the VPN gateways that you just configured to it.
Step 9	Perform one of the following: • Configure VPN Profile, on page 78 • Configure VPN Feature Parameters, on page 79	You must configure a VPN profile only if you have multiple VPN groups. The VPN Profile fields take precedence over the VPN Feature Configuration fields.
Step 10	Add VPN Details to Common Phone Profile, on page 81	Add the VPN Group and VPN Profile to a Common Phone Profile.
Step 11	Upgrade the firmware for Cisco Unified IP Phone to a version that supports VPN.	To run the Cisco VPN client, a supported Cisco Unified IP Phone must be running firmware release 9.0(2) or higher. For more information about upgrading the firmware, see *Cisco Unified IP Phone Administration Guide* for Unified Communications Manager for yourCisco Unified IP Phone model.
Step 12	Using a supported Cisco Unified IP Phone, establish the VPN connection.	Connect your Cisco Unified IP Phone to a VPN.

Complete Cisco IOS Prerequisites

Use this procedure to complete Cisco IOS Prerequisites.

Procedure

Step 1 Install Cisco IOS Software version 15.1(2)T or later.

Feature Set/License: Universal (Data & Security & UC) for IOS ISR-G2 and ISR-G3

Feature Set/License: Advanced Security for IOS ISR

Step 2 Activate the SSL VPN License.

Configure Cisco IOS SSL VPN to Support IP Phones

Use this procedure to complete Cisco IOS SSL VPN to Support IP Phones.

Procedure

Step 1 Configure Cisco IOS locally.

a) Configure the Network Interface.

Example:

```
router(config)# interface GigabitEthernet0/0
router(config-if)# description "outside interface"
router(config-if)# ip address 10.1.1.1 255.255.255.0
router(config-if)# duplex auto
router(config-if)# speed auto
router(config-if)# no shutdown
router#show ip interface brief (shows interfaces summary)
```

b) Configure static and default routes by using this command:

router(config)# **ip route** <*dest_ip*> < *mask*> < *gateway_ip*>

Example:

```
router(config)# ip route 10.10.10.0 255.255.255.0 192.168.1.1
```

Step 2 Generate and register the CAPF certificate to authenticate the IP phones with an LSC.

Step 3 Import the CAPF certificate from Unified Communications Manager.

a) From the Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Note This location changes based on the Unified Communications Manager version.

b) Find the Cisco_Manufacturing_CA and CAPF certificates. Download the .pem file and save as .txt file.

c) Create trustpoint on the Cisco IOS software.

```
hostname(config)# crypto pki trustpoint trustpoint_name
hostname(config-ca-trustpoint)# enrollment terminal
hostname(config)# crypto pki authenticate trustpoint
```

When prompted for the base 64-encoded CA certificate, copy and paste the text in the downloaded .pem file along with the BEGIN and END lines. Repeat the procedure for the other certificates.

d) Generate the following Cisco IOS self-signed certificates and register them with Unified Communications Manager, or replace with a certificate that you import from a CA.

- Generate a self-signed certificate.

```
Router> enable
Router# configure terminal
Router(config)# crypto key generate rsa general-keys label <name>
<exportable -optional>Router(config)# crypto pki trustpoint <name>
```

```
Router(ca-trustpoint)# enrollment selfsigned
Router(ca-trustpoint)# rsakeypair <name> 2048 2048
Router(ca-trustpoint)#authorization username subjectname commonname
Router(ca-trustpoint)# crypto pki enroll <name>
Router(ca-trustpoint)# end
```

- Generate a self-signed certificate with Host-id check enabled on the VPN profile in Unified Communications Manager.

  Example:

```
Router> enable
Router# configure terminal
Router(config)# crypto key generate rsa general-keys label <name>
<exportable -optional>Router(config)# crypto pki trustpoint <name>
Router(ca-trustpoint)# enrollment selfsigned
Router(config-ca-trustpoint)# fqdn <full domain
name>Router(config-ca-trustpoint)# subject-name CN=<full domain
name>, CN=<IP>Router(ca-trustpoint)#authorization username
subjectname commonname
Router(ca-trustpoint)# crypto pki enroll <name>
Router(ca-trustpoint)# end
```

- Register the generated certificate with Unified Communications Manager.

  Example:

```
Router(config)# crypto pki export <name> pem terminal
```

  Copy the text from the terminal and save it as a .pem file and upload it to the Unified Communications Manager using the Cisco Unified OS Administration.

Step 4 Install AnyConnect on Cisco IOS.

Download the Anyconnect package from cisco.com and install to flash.

Example:

```
router(config)#webvpn install svc
flash:/webvpn/anyconnect-win-2.3.2016-k9.pkg
```

Step 5 Configure the VPN feature.

Note To use the phone with both certificate and password authentication, create a user with the phone MAC address. Username matching is case sensitive. For example:

```
username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9 encrypted
```

Complete ASA Prerequisites for AnyConnect

Use this procedure to complete ASA Prerequisites for AnyConnect.

Procedure

Step 1 Install ASA software (version 8.0.4 or later) and a compatible ASDM.

Step 2 Install a compatible AnyConnect package.

Step 3 Activate License.

a) Check features of the current license using the following command:

show activation-key detail

b) If necessary, obtain a new license with additional SSL VPN sessions and enable the Linksys phone.

Step 4 Make sure that you configure a tunnel-group with a non-default URL as follows:

```
tunnel-group phonevpn type remote-access
tunnel-group phonevpn general-attribute
  address-pool vpnpool
tunnel-group phonevpn webvpn-attributes
  group-url https://172.18.254.172/phonevpn enable
```

Consider the following when configuring non-default URL:

- If the IP address of the ASA has a public DNS entry, you can replace it with a Fully Qualified Domain Name (FQDN).
- You can only use a single URL (FQDN or IP address) on the VPN gateway in Unified Communications Manager.
- It is preferred to have the certificate CN or subject alternate name match the FQDN or IP address in the group-url.
- If the ASA certificate CN or SAN does not match with the FQDN or IP address, uncheck the host ID check box in the Unified Communications Manager.

Configure ASA for VPN Client on IP Phone

Use this procedure to configure ASA for VPN Client on IP Phone.

Note Replacing ASA certificates results in non-availability of Unified Communications Manager.

Procedure

Step 1 Local configuration

a) Configure network interface.

Example:

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.89.79.135 255.255.255.0
ciscoasa(config-if)# duplex auto
ciscoasa(config-if)# speed auto
ciscoasa(config-if)# no shutdown
ciscoasa#show interface ip brief (shows interfaces summary)
```

b) Configure static routes and default routes.

ciscoasa(config)# **route** <interface_name> <ip_address> <netmask> <gateway_ip>

Example:

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 10.89.79.129
```

c) Configure the DNS.

Example:

```
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67 209.165.201.6
```

Step 2 Generate and register the necessary certificates for Unified Communications Manager and ASA.

Import the following certificates from the Unified Communications Manager.

- CallManager - Authenticating the Cisco UCM during TLS handshake (Only required for mixed-mode clusters).
- Cisco_Manufacturing_CA - Authenticating IP phones with a Manufacturer Installed Certificate (MIC).
- CAPF - Authenticating IP phones with an LSC.

To import these Unified Communications Manager certificates, do the following:

a) From the Cisco Unified OS Administration, choose **Security** > **Certificate Management**.
b) Locate the certificates Cisco_Manufacturing_CA and CAPF. Download the `.pem` file and save as a `.txt` file.
c) Create trustpoint on the ASA.

Example:

```
ciscoasa(config)# crypto ca trustpoint trustpoint_name
ciscoasa(ca-trustpoint)# enrollment terminal
ciscoasa(config)# crypto ca authenticate trustpoint_name
```

When prompted for base 64 encoded CA Certificate, copy-paste the text in the downloaded `.pem` file along with the BEGIN and END lines. Repeat the procedure for the other certificates.

d) Generate the following ASA self-signed certificates and register them with Unified Communications Manager, or replace with a certificate that you import from a CA.

- Generate a self-signed certificate.

  Example:

```
ciscoasa> enable
ciscoasa# configure terminal
ciscoasa(config)# crypto key generate rsa general-keys label <name>
ciscoasa(config)# crypto ca trustpoint <name>
ciscoasa(ca-trustpoint)# enrollment self
ciscoasa(ca-trustpoint)# keypair <name>
ciscoasa(config)# crypto ca enroll <name>
ciscoasa(config)# end
```

- Generate a self-signed certificate with Host-id check enabled on the VPN profile in Unified Communications Manager.

  Example:

```
ciscoasa> enable
ciscoasa# configure terminal
ciscoasa(config)# crypto key generate rsa general-keys label <name>
ciscoasa(config)# crypto ca trustpoint <name>
ciscoasa(ca-trustpoint)# enrollment self
ciscoasa(ca-trustpoint)# fqdn <full domain name>
ciscoasa(config-ca-trustpoint)# subject-name CN=<full domain name>,CN=<IP>
ciscoasa(config)# crypto ca enroll <name>
ciscoasa(config)# end
```

- Register the generated certificate with Unified Communications Manager.

  Example:

  ```
  ciscoasa(config)# crypto ca export <name> identity-certificate
  ```

  Copy the text from the terminal and save it as a .pem file and upload it to Unified Communications Manager.

Step 3 Configure the VPN feature. You can use the Sample ASA configuration summary below to guide you with the configuration.

Note To use the phone with both certificate and password authentication, create a user with the phone MAC address. Username matching is case sensitive. For example:

```
ciscoasa(config)# username CP-7975G-SEP001AE2BC16CB password klkLGQIoxyCO4ti9
encrypted
ciscoasa(config)# username CP-7975G-SEP001AE2BC16CB attributes
ciscoasa(config-username)# vpn-group-policy GroupPhoneWebvpn
ciscoasa(config-username)#service-type remote-access
```

ASA Certificate Configuration

For more information on *ASA certificate configuration*, see Configure AnyConnect VPN Phone with Certificate Authentication on an ASA

Upload VPN Concentrator Certificates

Generate a certificate on the ASA when you set it up to support the VPN feature. Download the generated certificate to your PC or workstation and then upload it to Unified Communications Manager using the procedure in this section. Unified Communications Manager saves the certificate in the Phone-VPN-trust list.

The ASA sends this certificate during the SSL handshake, and the Cisco Unified IP Phone compares it against the values stored in the Phone-VPN-trust list.

If a Locally Significant Certificate (LSC) is installed on the Cisco Unified IP Phone, it will send its LSC by default.

To use device level certificate authentication, install the root MIC or CAPF certificate in the ASA, so that the Cisco Unified IP Phone are trusted.

To upload certificates to Unified Communications Manager, use the Cisco Unified OS Administration.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Click **Upload Certificate**.

Step 3 From the **Certificate Purpose** drop-down list, choose **Phone-VPN-trust**.

Step 4 Click **Browse** to choose the file that you want to upload.

Step 5 Click **Upload File**.

Configure VPN Gateway

Ensure that you have configured VPN concentrators for each VPN gateway. After configuring the VPN concentrators, upload the VPN concentrator certificates. For more information, see Upload VPN Concentrator Certificates, on page 75.

Use this procedure to configure the VPN Gateway.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advanced Features** > **VPN** > **VPN Gateway**.

Step 2 Perform one of the following tasks:

a) Click **Add New** to configure new profile.

b) Click the **Copy** next to the VPN gateway that you want to copy.

c) Locate the appropriate VPN gateway and modify the settings to update an existing profile.

Step 3 Configure the fields in the **VPN Gateway Configuration** window. For more information, see VPN Gateway Fields for VPN Client, on page 76.

Step 4 Click **Save**.

VPN Gateway Fields for VPN Client

The table describes the VPN Gateway fields for VPN Client.

Table 8: VPN Gateway Fields for VPN Client

Field	Description
VPN Gateway Name	Enter the name of the VPN gateway.
VPN Gateway Description	Enter a description of the VPN gateway.

Field	Description
VPN Gateway URL	Enter the URL for the main VPN concentrator in the gateway. **Note** You must configure the VPN concentrator with a group URL and use this URL as the gateway URL. For configuration information, refer to the documentation for the VPN concentrator, such as the following: • *SSL VPN Client (SVC) on ASA with ASDM Configuration Example*
VPN Certificates in this Gateway	Use the up and down arrow keys to assign certificates to the gateway. If you do not assign a certificate for the gateway, the VPN client fails to connect to that concentrator. **Note** You can assign up to 10 certificates to a VPN gateway, and you must assign at least one certificate to each gateway. Only certificates that are associated with the Phone-VPN-trust role appear in the available VPN certificates list.

Configure VPN Group

Use this procedure to configure VPN Group.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advanced Features** > **VPN** > **VPN Group**.

Step 2 Perform one of the following tasks:

a) Click **Add New** to configure new profile.
b) Click **Copy** next to the VPN group that you want to copy an existing VPN group.
c) Locate the appropriate VPN group and modify the settings to update an existing profile.

Step 3 Configure the fields in the **VPN Group Configuration** window. For more information, see VPN Gateway Fields for VPN Client, on page 76 for the field description details.

Step 4 Click **Save**.

VPN Group Fields for VPN Client

The table describes the VPN Group Fields for VPN Client.

Table 9: VPN Group Fields for VPN Client

Field	Definition
VPN Group Name	Enter the name of the VPN group.
VPN Group Description	Enter a description of the VPN group.

Field	Definition
All Available VPN Gateways	Scroll to see all available VPN gateways.
Selected VPN Gateways in this VPN Group	Use the up and down arrow buttons to move available VPN gateways into and out of this VPN group. If the VPN client encounters critical error and cannot connect to a particular VPN gateway, it will attempt to move to the next VPN gateway in the list. **Note** You can add up to a maximum of three VPN gateways to a VPN group. Also, the total number of certificates in the VPN group cannot exceed 10.

Configure VPN Profile

Use this procedure to configure the VPN Profile.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advanced Features** > **VPN** > **VPN Profile**.

Step 2 Perform one of the following tasks:

a) Click **Add New** to configure new profle.

b) Click **Copy** next to the VPN profile that you want to copy an existing profile.

c) To update an existing profile, specify the appropriate filters in the **Find VPN Profile Where**, click **Find**, and modify the settings.

Step 3 Configure the fields in the **VPN Profile Configuration** window. For more information, see VPN Profile Fields for VPN Client, on page 78 for the field description details.

Step 4 Click **Save**.

VPN Profile Fields for VPN Client

The table describes the VPN profile field details.

Table 10: VPN Profile Field Details

Field	Definition
Name	Enter a name for the VPN profile.
Description	Enter a description for the VPN profile.
Enable Auto Network Detect	When you check this check box, the VPN client can only run when it detects that it is out of the corporate network. Default: Disabled.

Field	Definition
MTU	Enter the size, in bytes, for the Maximum Transmission Unit (MTU). Default: 1290 bytes.
Fail to Connect	This field specifies the amount of time to wait for login or connect operations to complete while the system creates the VPN tunnel. Default: 30 seconds
Enable Host ID Check	When you check this check box, the gateway certificate subjectAltName or CN must match the URL to which the VPN client is connected. Default: Enabled
Client Authentication Method	From the drop-down list, choose the client authentication method: • User and password • Password only • Certificate (LSC or MIC)
Enable Password Persistence	When you check this check box, a user password gets saved in the phone until either a failed log in attempt occurs, a user manually clears the password, or the phone resets or loses power.

Configure VPN Feature Parameters

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advanced Features** > **VPN** > **VPN Feature Configuration**.

Step 2 Configure the fields in the **VPN Feature Configuration** window. For more information, see VPN Feature Parameters, on page 79.

Step 3 Click **Save**.

Perform the following tasks:

- Upgrade the firmware for Cisco Unified IP Phones to a version that supports VPN. For more information about upgrading the firmware, see *Cisco Unified IP Phone Administration Guide* for your Cisco Unified IP Phone model.
- Using a supported Cisco Unified IP Phone, establish the VPN connection.

VPN Feature Parameters

The table describes the VPN feature parameters.

Table 11: VPN Feature Parameters

Field	Default
Enable Auto Network Detect	When True, the VPN client can only run when it detects that it is out of the corporate network. Default: False
MTU	This field specifies the maximum transmission unit: Default: 1290 bytes Minimum: 256 bytes Maximum: 1406 bytes
Keep Alive	This field specifies the rate at which the system sends the keep alive message. **Note** If it is non zero and less than the value specified in Unified Communications Manager, the keep alive setting in the VPN concentrator overwrites this setting. Default: 60 seconds Minimum: 0 Maximum: 120 seconds
Fail to Connect	This field specifies the amount of time to wait for login or connect operations to complete while the system creates the VPN tunnel. Default: 30 seconds Minimum: 0 Maximum: 600 seconds
Client Authentication Method	From the drop-down list, choose the client authentication method: • User and password • Password only • Certificate (LSC or MIC) Default: User And Password
Enable Password Persistence	When True, a user password gets saved in the phone until either a failed login attempt occurs, a user manually clears the password, or the phone resets or loses power. Default: False
Enable Host ID Check	When True, the gateway certificate subjectAltName or CN must match the URL to which the VPN client is connected. Default: True

Add VPN Details to Common Phone Profile

Use this procedure to add VPN details to common phone profile.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Common Phone Profile**.

Step 2 Click **Find** and choose common phone profile to which you want to add the VPN details.

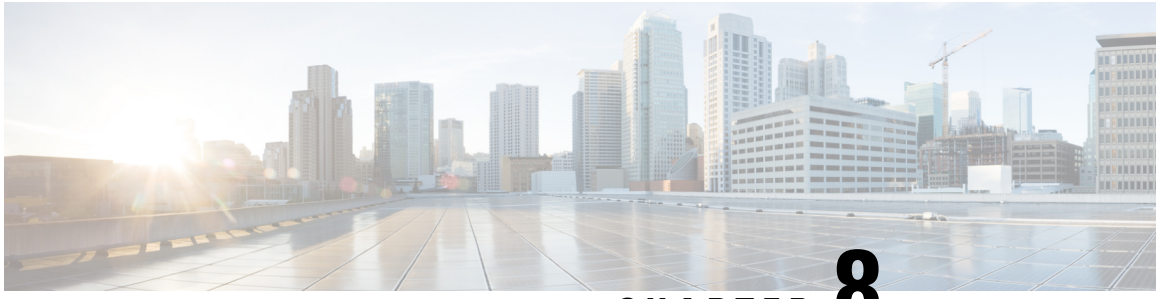
Step 3 In the **VPN Information** section, choose the appropriate **VPN Group** and **VPN Profile**.

Step 4 Click **Save** and then **Apply Config**.

Step 5 Click **OK** in apply configuration window.

PART IV

Monitoring and Recording



CHAPTER 8

Silent Monitoring

Silent Monitoring Overview

Silent call monitoring allows a supervisor to eavesdrop on a phone conversation. The most common scenario is in a call center where a call agent is speaking with a customer. Call centers need to be able to guarantee the quality of customer service that an agent in a call center provides. With silent monitoring, the supervisor can hear both call participants, but neither of the call participants can hear the supervisor.

Silent monitoring can only be invoked by a CTI application through the JTAPI or TAPI interfaces. Many Cisco applications, such as Cisco Unified Contact Center Enterprise and Cisco Unified Contact Center Express have the ability to use silent monitoring. Any CTI application that monitors calls must have the corresponding monitoring privileges that are enabled for the application-user or end-user account.

Silent monitoring is call based. When a supervisor invokes a silent monitoring session, the following occurs:

- The supervisor selects a specific call to be monitored.
- The start-monitoring request from the application triggers the supervisor phone to go off hook and automatically triggers a monitoring call to the agent.
- The agent phone automatically answers the monitoring call. The monitoring call does not get presented to the agent.

Secure Silent Monitoring

You can also configure secure silent monitoring. Secure silent monitoring allows encrypted media (sRTP) calls to be monitored. Monitoring calls are always established using the highest level of security that is determined by the capabilities of the agent phone regardless of the security status of the call being observed. The highest level of security is maintained by exchanging the secure media key in any call between the customer, agent, and supervisor. Monitoring calls using secured media carries approximately 4000 bits per second of additional bandwidth overhead, same as standard secure media (sRTP) calls.

If the agent phone has encryption that is enabled, the supervisor phone must also have encryption enabled in order to allow secure silent monitoring. If the agent phone has encryption that is enabled, but the supervisor phone does not, the monitoring request fails.

Whisper Coaching

Unified Communications Manager also supports whisper coaching, a CTI enhancement on silent monitoring whereby a supervisor can speak to the agent while the monitoring session is underway without the customer hearing. Whisper coaching can only be initiated by a CTI application. If silent monitoring is already configured, then no additional configuration of Unified Communications Manager is required for whisper coaching.

Silent Monitoring Prerequisites

Silent monitoring can only be invoked by an external CTI application. Cisco applications such as Cisco Unified Contact Center Enterprise or Cisco Unified Contact Center Express can initiate silent monitoring sessions. For details, see the following:

- Cisco Unified Contact Center Enterprise—For details on how to set up silent monitoring in Cisco Unified Contact Center Enterprise, see Cisco Remote Silent Monitoring Installation and Administration Guide.
- Cisco Unified Contact Center Express—This chapter contains a sample configuration to set up Silent Monitoring for Unified Contact Center Express via Cisco Finesse. For additional documentation that is related to your Cisco Unified Contact Center Express deployment, go to https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/tsd-products-support-series-home.html.

Configure Silent Monitoring Task Flow

This task flow describes the tasks that you must perform within Unified Communications Manager to allow CTI applications to use the monitoring feature.

Before you begin

- Determine which phones support silent monitoring by running a phone feature list report. For more information,Generate a Phone Feature List, on page 3

Procedure

	Command or Action	Purpose
Step 1	Perform one of the following procedures: • Enable Built in Bridge for Phones Clusterwide, on page 87 • Enable Built in Bridge for a Phone, on page 87	Turn on the Built in Bridge on agent phones. You can use a service parameter to configure the clusterwide default setting or you can enable the Built in Bridge for individual phones. **Note** The Built in Bridge setting on individual phones overrides the clusterwide default setting.

	Command or Action	Purpose
Step 2	Enable Monitoring Privileges for Supervisor, on page 88	Add the supervisor to a group that allows silent monitoring.
Step 3	Assign a Monitoring Calling Search Space, on page 88	Set up the monitoring calling search space for the supervisor phone.
Step 4	Configure Silent Monitoring Notification Tones, on page 89	Configure whether you want to play notification tones to the call participants.
Step 5	Configure Secure Silent Monitoring, on page 89	**Optional**. If your calls are encrypted, configure secure silent monitoring.
Step 6	Configure Silent Monitoring for Unified Contact Center Express, on page 90	For Unified Contact Center Express deployments, configure Silent Monitoring via Cisco Finesse.

Enable Built in Bridge for Phones Clusterwide

When you set the Built-in-Bridge clusterwide service parameter to enable, the Built-in-Bridge default setting for all phones in the cluster is changed to enabled. However, the Built-in-Bridge setting in the Phone Configuration window for individual phones overrides the clusterwide service parameter.

Procedure

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

Step 2 From the **Server** drop-down list, choose the server on which the CallManager service is running.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.

Step 4 Set the **Builtin Bridge Enable** service parameter to **On**.

Step 5 Click **Save**.

Enable Built in Bridge for a Phone

Use this procedure to enable the Built in Bridge on an individual phone. The Built in Bridge setting on an individual phone overrides the clusterwide service parameter.

Before you begin

Use a service parameter to set the Built in Bridge defaults for all phones in the cluster. For details, see Enable Built in Bridge for Phones Clusterwide, on page 87.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** to select the agent phone.

Step 3 From the **Built in Bridge** drop-down list, choose one of the following options:

- **On**—The Built in Bridge is enabled.
- **Off**—The Built in Bridge is disabled.
- **Default**—The setting of the clusterwide **Builtin Bridge Enable** service parameter is used.

Step 4 Click **Save**.

Enable Monitoring Privileges for Supervisor

In order for a supervisor to be able to monitor agent conversations, the supervisor must be part of a group that allows monitoring.

Before you begin

Perform one of the following procedures to enable the Built in Bridge on agent phones:

- Enable Built in Bridge for Phones Clusterwide, on page 87
- Enable Built in Bridge for a Phone, on page 87

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **End User**.

Step 2 Select the supervisor from the list of users.

Step 3 In the **Permissions Information** section, click **Add to Access Control Group**.

Step 4 Add the **Standard CTI Allow Call Monitoring** and **Standard CTI Enabled** user groups.

Step 5 Click **Save**.

Assign a Monitoring Calling Search Space

For monitoring to work, you must assign a Monitoring Calling Search Space to the supervisor phone line. The Monitoring Calling Search Space must include both the supervisor phone line and the agent phone line.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select the supervisor phone.
The left navigation pane displays the available phone lines for the supervisor's phone.

Step 3 Perform the following steps for each of the supervisor's phone lines that are used for monitoring:

a) Click the phone line. The **Directory Number Configuration** window displays configuration information for that phone line.

b) From the **Monitoring Calling Search Space** drop-down list, choose a calling search space that includes both the supervisor phone line and the agent phone line.

c) Click **Save**.

Configure Silent Monitoring Notification Tones

In certain jurisdictions, a notification tone must be played to either the agent, the customer, or both, that indicates that the call is being monitored. By default, Unified Communications Manager does not play notification tones. You must configure a service parameter to allow notification tones.

Procedure

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

Step 2 From the **Server** drop-down list, choose the server one which the CallManager service is running.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.

Step 4 Configure values for the following service parameters:

- If you want to play a notification tone to the agent, change the value of the **Play Monitoring Notification Tone To Observed Target** service parameter to **True**.
- If you want to play a notification tone to the customer, change the value of the **Play Monitoring Notification Tone To Observed Connected Parties** service parameter to **True**.

Step 5 Click **Save**.

Step 6 Reset the agent phone, if you changed the service parameter configuration.

Configure Secure Silent Monitoring

To configure secure silent monitoring using sRTP, you must configure phone security profiles that include encryption and apply them to the supervisor phone and to any agent phones that are being monitored.

Procedure

	Command or Action	Purpose
Step 1	Configure an Encrypted Phone Security Profile , on page 89	Configure phone security profiles that include encryption for the agent phone and supervisor phone.
Step 2	Assign Security Profile to Phone, on page 90	Apply the encrypted phone security profile to the agent phone and the supervisor phone.

Configure an Encrypted Phone Security Profile

To configure secure silent monitoring, you must configure the phone security profile for your supervisor phone and any agent phones to specify **Encrypted** as the **Device Security Mode**.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Security** > **Phone Security Profile**.

Step 2 Perform either of the following steps:

- Click **Add New** to create a new phone security profile.
- Click **Find** and select an existing phone security profile.

Step 3 If you have created a new phone security profile, select your phone model from the **Phone Security Profile Type** drop-down list.

Step 4 Enter a **Name** for the Phone Security Profile.

Step 5 From the **Device Security Mode** drop-down list, choose **Encrypted**.

Step 6 Click **Save**.

Step 7 Repeat the above steps to configure phone security profiles for your supervisor phone and any agent phones.

Assign Security Profile to Phone

Perform the following steps to assign a phone security profile to a phone. For secure silent monitoring to work, you must assign the phone security profile to both the agent phone and the supervisor phone.

Procedure

Step 1 From Cisco Unified CM Administration, chooseI **Device** > **Phone**.

Step 2 Click **Find** and select the agent phone on which you want to configure a phone security profile.

Step 3 From the **Device Security Profile** drop-down list, choose the phone security profile that you have set up.

Step 4 Click **Save**.

Step 5 Repeat the previous steps for the supervisor phone.

Configure Silent Monitoring for Unified Contact Center Express

The following steps contain a sample Silent Monitoring for Cisco Unified Contact Center Express configuration via Cisco Finesse.

Before you begin

Make sure that both the agent and supervisor phone are compatibile for Cisco Finesse. Refer to the *Unified CCX Software Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html.

Procedure

Step 1 Configure a test agent and supervisor on Unified Contact Center Express.

Note The IP Contact Center (IPCC) Extension for the Agents and Supervisors must be unique. This can be verified from Cisco Unified Communications Manager under **Call Routing** > **Route Plan Report**.

Step 2 Ensure that the agent phone has the Built in Bridge (BIB) On. This can be done on the phone or at the Cluster level (Set the Default Service Parameter to On).

Step 3 Log in to Finesse as an Agent.

Step 4 Log in to Finesse as a Supervisor and ensure that the supervisor is in NOT READY State.

Step 5 Ensure that the Resource Manager Contact Manager (RMCM) user has the required roles for Call Monitoring and Call Recording -- Standard Computer Telephony Integration (CTI) Allow Call Monitoring and Recording.

Note This is automatically done by Unified Contact Center Express at the initial setup of the RMCM user. Ensure the roles exist on the **Application User** window of Cisco Unified Communications Manager.

Step 6 Assign the Monitoring CSS (Calling Search Space) on the Supervisor Phone to contain the Partition of the agent line.

Step 7 Place a call to Unified Contact Center Express so that the call is routed to the agent logged in. Once the agent is in the TALKING state, from the supervisor, start the Silent Monitoring. The supervisor will then be able to hear the conversation between the agent and the caller

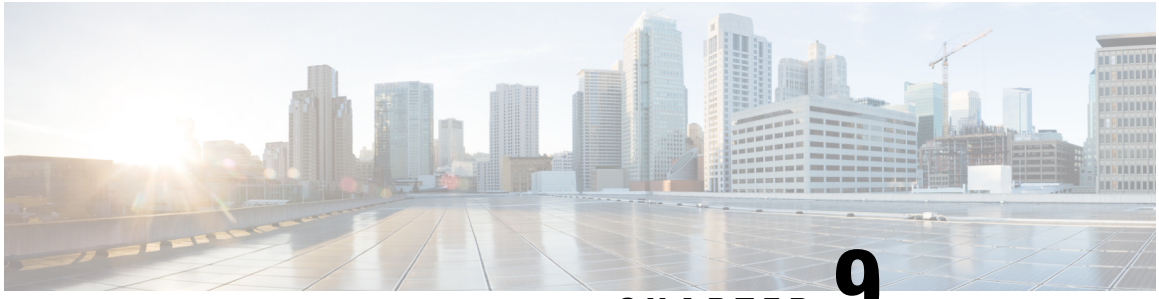
Silent Monitoring Interactions and Restrictions

Silent Monitoring Interactions

Feature	Interaction
Call preservation	If the agent call that is being monitored goes to call preservation, Unified Communications Manager also puts the monitoring call into call preservation mode.
Transfer of secure monitoring call	Unified Communications Manager supports transferring a secure monitoring session so long as the destination supervisor device exceeds the security capabilities of the agent that is being monitored.
Recording Tones	Recording Tones take precedence over Monitoring Tones for calls that are both recorded and monitored. If a call is recorded and monitored, only the recording tone plays.
Secure Tones	If Secure Tones are configured and the call is secured, the secure tone plays to both call participants at the outset of the call irrespective of whether Monitoring Tones are configured. If Secure Tones and Monitoring Tones are both configured, the secure tone plays once, followed by the monitoring tones. If Secure Tones, Monitoring Tones, and Recording Tones are all configured, and the call is recorded and monitored, the secure tone plays once followed by the recording tone. The monitoring tone does not play.

Silent Monitoring Restrictions

Feature	Restriction
Barge	Unified Communications Manager does not support barge with silent monitoring. If an agent call is being monitored, the barge-in call from a shared line fails. If the agent call has already been barged, the monitoring call fails.
Transfer of Secure Silent Monitoring over an intercluster trunk	Unified Communications Manager does not support transferring Secure Silent Monitoring calls over an intercluster trunk.



CHAPTER 9

Recording

Recording Overview

Call recording is a Unified Communications Manager feature that enables a recording server to archive agent conversations. Call recording is one of the essential features in call centers, financial institutions and other enterprises. The call recording feature sends copies of the agent and the end-user media streams to the recording server over a SIP trunk. Each media stream is sent separately in an effort to best support a wide range of voice analytic applications.

Unified Communications Manager offers IP phone-based or network-based recording.

- In IP phone based recording, recording media is sourced from the phone. The phone forks two media streams to the recording server.
- In network-based recording, recording media can be sourced from either the phone or the gateway. When you implement network-based recording, the gateway in your network must connect to Unified Communications Manager over a SIP trunk.

Unified Communications Manager supports call recording in both single cluster and multi-cluster environments and offers three different recording modes:

- **Automatic Silent Recording**—Automatic silent recording records all calls on a line appearance automatically. Unified Communications Manager invokes the recording session automatically with no visual indication on the phone that an active recording session is established.
- **Selective Silent Recording**—A supervisor can start or stop the recording session via CTI-enabled desktop. Alternatively, a recording server can invoke the session based on predefined business rules and events. There is no visual indication on the phone that an active recording session is established.
- **Selective User Call Recording**—An agent can choose which calls to record. The agent invokes the recording session through CTI-enabled desktop, or by a softkey or programmable line key. When selective user call recording is used, the Cisco IP phone displays recording session status messages.

Recording Media Source Selection

When you configure network-based recording, you must configure either the phone or the gateway as your preferred source of recording media for the agent phone line. However, depending on your deployment, Unified Communications Manager may not select your preferred choice as the recording media source. The following table displays the logic Unified Communications Manager uses to select the recording media source.

Table 12: Recording Media Source Selection

Preferred Media Source	Media Type	Gateway in call path?	Selected Media Source
Gateway	Unsecure (RTP)	Yes	Gateway
		No	Phone
	Secure (sRTP)	Yes	Phone
		No	Phone
Phone	Unsecure (RTP)	Yes	Phone
		No	Phone
	Secure (sRTP)	Yes	Phone
		No	Phone

Alternate Recording Media Source if the First Choice is Unavailable

If the recording media source that Unified Communications Manager selects is unavailable, Unified Communications Manager attempts to use an alternate source. The following table shows the logic Unified Communications Manager uses to select an alternate source for recording media.

Table 13: Alternate Recording Media Source if First Choice is Unavailable

Selected Media Source	Gateway Preferred	Phone Preferred
First attempt	First gateway in call path	Phone
Second attempt	Last gateway in call path	First gateway in call path
Third attempt	Phone	Last gateway in call path

Recording Prerequisites

- Cisco Unified IP Phone support—To view a list of the Cisco Unified IP Phone that support recording, log in to Cisco Unified Reporting and run the Unified CM Phone Feature List report, selecting **Record** as the feature. For a detailed procedure, see Generate a Phone Feature List, on page 3.
- Gateway support—For details on which gateways support recording, see https://developer.cisco.com/web/sip/wiki/-/wiki/Main/Unified+CM+Recording+Gateway+Requirements.

Recording Configuration Task Flow

Before you begin

Procedure

	Command or Action	Purpose
Step 1	Create a Recording Profile, on page 96	Create a recording profile.
Step 2	Configure SIP Profile for Recording, on page 96	**Optional**. Configure the SIP Profile if you want to deliver the Conference Bridge Identifier to the recorder.
Step 3	Configure SIP Trunks for Recording, on page 96	Configure the recorder server as a SIP trunk device.
Step 4	Configure Route Pattern for Recording, on page 97	Create a route pattern that routes to the recorder server .
Step 5	Configure Agent Phone Line for Recording, on page 97	Configure the agent phone line for recording.
Step 6	Enable the built in bridge for your agent phones. Perform one of the following tasks to enable the built-in-bridge for recording: • Enable Built in Bridge for Cluster , on page 98 • Enable Built in Bridge for a Phone, on page 98	To use the agent phone as the recording media source you must enable the phone's built in bridge for recording. You can use a service parameter to set the built in bridge defaults across the cluster, or enable the built in bridge on an individual phone. **Note** The Built in Bridge setting on individual phones overrides the clusterwide defaults.
Step 7	Enable Gateway for Recording, on page 99	Configure Unified Communications services on the gateway.
Step 8	Configure Recording Notification Tones, on page 99	Configure whether you want a notification tone to play when calls are recorded.
Step 9	Configure Recording Redundancy Using Route Groups, on page 100	**Optional**.Configure redundancy for your recording servers. There are many methods for configuring redundancy for the servers. For the preferred redundancy method for your deployment, refer to your vendor.
Step 10	Perform one of the following procedures, depending on whether your phone uses feature buttons or softkeys: • Configure a Record Feature Button, on page 101 • Configure a Record Softkey, on page 102	Configure a Record feature button or softkey for your phone.

Create a Recording Profile

Use this procedure to create a recording profile.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Recording Profile**.

Step 2 Click **Add New**.

Step 3 In the **Name** field, enter a name for your recording profile.

Step 4 In the **Recording Calling Search Space** field, select the calling search space that contains the partition with the route pattern that is configured for the recording server.

Step 5 In the **Recording Destination Address** field, enter the directory number or the URL of the recording server or the URL of the CUBE Media Proxy server.

Step 6 Click **Save**.

Configure SIP Profile for Recording

Use this procedure to deliver the conference bridge identifier to the recorder and configure the SIP Profile.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **SIP Profile**.

Step 2 Select the SIP profile that you want to use for your network.

Step 3 Check the **Deliver Conference Bridge Identifier** check box.

Step 4 Click **Save**.

Configure SIP Trunks for Recording

Use this procedure to assign the recording server information in the **SIP Trunk Configuration** window.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Trunk**.

Step 2 Click **Add New**.

Step 3 From the **Trunk Type** drop-down list, choose **SIP Trunk**.

Device Protocol is auto-populated to **SIP**, which is the only available option.

Step 4 From the **Trunk Service Type** drop-down list, choose the service type that you want to use in your network. The default value is **None**.

Step 5 Click **Next**.

Step 6 In the **Destination Address** field of the **SIP Information** pane, enter an IP address, fully qualified domain name, or DNS SRV of the recording server or CUBE Media proxy.

Step 7 From the **SIP Profile** drop-down list in the **SIP Information** pane, choose the SIP profile that you want to use in your network.

Step 8 From the **Recording Information** pane, select one of the following options:

- None—This trunk is not used for recording.
- This trunk connects to a recording-enabled gateway.
- This trunk connects to other clusters with recording-enabled gateways.

Step 9 Click **Save**.

What to do next

Perform one of the following procedures, depending on whether you are configuring your main recording server, or multiple recording servers for redundancy:

- Add Recording Servers to Route Group, on page 100

Configure Route Pattern for Recording

Use this procedure to describe the route pattern configurations that are specific to recorders. You must configure a route pattern that routes to the recording server or CUBE Media Proxy server.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Route/Hunt** > **Route Pattern**.

Step 2 Click **Add New** to create a new route pattern.

Step 3 Complete the fields in the **Route Pattern Configuration** window.For more information on the fields and their configuration options, see Online Help.

Step 4 For call recording, complete the following fields:

- **Pattern**—Enter a pattern that matches the recording destination address from the recording profile.
- **Gateway/Route List**—Choose the SIP trunk or route list that points to the recording server.

Step 5 Click **Save**.

Configure Agent Phone Line for Recording

Use this procedure to configure the agent phone line for recording.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find**.

Step 3 Select the agent's phone.

Step 4 In the left Association pane, click the phone line for the agent to view the settings.

Step 5 From the **Recording Option** drop-down list, choose one of the following options:

- **Call Recording Disabled**—Calls on this phone line are not recorded.
- **Automatic Call Recording Enabled**—All calls on this phone line are recorded.
- **Selective Call Recording Enabled**—Only selected calls on this phone line are recorded.

Step 6 From the **Recording Profile** drop-down list, choose the recording profile that is configured for the agent.

Step 7 From the **Recording Media Source** drop-down list, choose whether you want to use the gateway or the phone as the preferred source of recording media.

Step 8 Set the **Busy Trigger** field to a minimum of **3** if you also have Multilevel Precedence and Preemption (MLPP) configured.

Step 9 Click **Save**.

Enable Built in Bridge for Cluster

Use this procedure to enable the phone's built in bridge for recording to use the agent phone as the recording media source.

When you set the Built-in-Bridge clusterwide service parameter to enable, the Built-in-Bridge default setting for all phones in the cluster is changed to enabled. However, the Built-in-Bridge setting in the **Phone Configuration** window for an individual phone overrides the clusterwide service parameter setting if the default option is not selected for that phone.

Procedure

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

Step 2 From the **Server** drop-down list, choose the server on which the CallManager service is running.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.

Step 4 Set the **Builtin Bridge Enable** service parameter to **On**.

Step 5 Click **Save**.

Enable Built in Bridge for a Phone

Use this procedure to enable the Built in Bridge for an individual phone. If the default option is not selected, the Built in Bridge setting in the **Phone Configuration** window overrides the clusterwide service parameter.

Optionally, use a service parameter to set the Built in Bridge defaults across the cluster. For more information, see Enable Built in Bridge for Cluster , on page 98.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** to select the agent phone.

Step 3 From the **Built in Bridge** drop-down list, choose one of the following options:

- **On**—The Built in Bridge is enabled.
- **Off**—The Built in Bridge is disabled.
- **Default**—The setting of the clusterwide **Builtin Bridge Enable** service parameter is used.

Step 4 Click **Save**.

Enable Gateway for Recording

Use this procedure to configure the gateway for recording. You must enable Unified Communications Gateway Services. The following task flow contains the high-level process to enable Unified Communications Gateway Services.

Procedure

Step 1 Configure Unified Communications Manager IOS Services on the Device.

Step 2 Configure the XMF Provider.

Step 3 Verify Unified Communications Gateway Services.

For detailed configuration steps, including examples, refer to the Cisco Unified Communications Gateway Services chapter for either of the following documents:

- For more information, see ASR routers Cisco Unified Border Element (Enterprise) Protocol-Independent Features and Setup Configuration Guide. Cisco IOS XE Release 35.
- For more information, see ISR routers Cisco Unified Border Element Protocol-Independent Features and Setup Configuration Guide, Cisco IOS Release 15M&T.

Configure Recording Notification Tones

Use this procedure to configure notification tone to play when calls are recorded. For legal compliance, an explicit notification in the form of a periodic tone can be made audible to the agent, the caller, or both, to indicate that a recording session is in progress. This tone can also be disabled.

Note Recording tone settings override monitoring tone settings when both are enabled for the same call.

Procedure

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

Step 2 From the **Server** drop-down list, choose the server on which the Cisco CallManager service is running.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.

Step 4 If you want a notification tone to be played to the agent, set the **Play Recording Notification Tone to Observed Target (agent)** service parameter to **True**.

Step 5 If you want a notification tone to be played to the customer, set the value of the **Play Recording Notification Tone To Observed Connected Parties (customer)** service parameter to **True**.

Step 6 Click **Save**.

Configure Recording Redundancy Using Route Groups

This task flow describes how to configure recording redundancy using route groups. For the preferred method of configuring recording redundancy for your deployment, refer to your vendor.

Procedure

	Command or Action	Purpose
Step 1	Configure SIP Trunks for Recording, on page 96	Configure a separate SIP trunk for each recording server.
Step 2	Add Recording Servers to Route Group, on page 100	Add your recording SIP trunks to a route group.
Step 3	Add Route Group to Route List, on page 101	Add your recording route group to a route list.
Step 4	Configure Route Pattern for Recording, on page 97	Configure a route pattern that routes recording calls to your route list.

Add Recording Servers to Route Group

Configure SIP Trunks for Recording, on page 96

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Route** > **Route Hunt/List** > **Route Group**.

Step 2 Perform one of the following steps:

- Click **Find** and select an existing route group.
- Click **Add New** to create a new route group.

Step 3 Complete the fields in the Route Group Configuration window. For more information on the fields and their configuration options, see Online Help.

Step 4 In the Available Devices pane, for each SIP trunk on which you configured a recording server, select the SIP trunk and click **Add to Route Group** until each recording server appears in the Selected Devices pane.

Step 5 Use the up and down arrows to adjust the priority setting for each recording server.

Step 6 Click **Save**.

Add Route Group to Route List

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Route/Hunt** > **Route List**.

Step 2 Perform one of the following options:

- Click **Find** and select an existing route list.
- Click **Add New** to create a new route list.

Step 3 Click **Add Route Group**.
The Route List Details Configuration window opens.

Step 4 From the Route Group drop-down list, select the route group that you created for your recording servers.

Step 5 Click **Save**.

Step 6 Complete the remaining fields in the Route List Configuration window. For more information on the fields and their configuration options, see Online Help.

Step 7 Click **Save**.

Configure a Record Feature Button

Use this procedure to assign the Record feature button to your phone if your phone uses feature buttons.

Procedure

	Command or Action	Purpose
Step 1	Configure a Phone Button Template for Recording, on page 101	Configure a phone button template that includes the Record button.
Step 2	Associate a Phone Button Template with a Phone, on page 102	Associate the phone button template that you set up for recording to the phone.

Configure a Phone Button Template for Recording

Use this procedure to create a phone button template that includes the Record feature button.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Phone Button Template**.

Step 2 Click **Find** to display list of supported phone templates.

Step 3 Perform the following steps if you want to create a new phone button template; otherwise, proceed to the next step.

a) Select a default template for the model of phone and click **Copy**.
b) In the **Phone Button Template Information** field, enter a new name for the template.
c) Click **Save**.

Step 4 Perform the following steps if you want to add phone buttons to an existing template.

a) Click **Find** and enter the search criteria.
b) Choose an existing template.

Step 5 From the **Line** drop-down list, choose feature that you want to add to the template.

Step 6 Click **Save**.

Step 7 Perform one of the following tasks:

- Click **Apply Config** if you modified a template that is already associated with devices to restart the devices.
- If you created a new softkey template, associate the template with the devices and then restart them.

Associate a Phone Button Template with a Phone

Use this procedure to associate the phone button template that you created for the Record button of the phone.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** to display the list of configured phones.

Step 3 Choose the phone to which you want to add the phone button template.

Step 4 In the **Phone Button Template** drop-down list, choose the phone button template that contains the new feature button.

Step 5 Click **Save**.
A dialog box is displayed with a message to press **Reset** to update the phone settings.

Configure a Record Softkey

Use this procedure to add a Record softkey to the phone, if your phone uses softkeys. The Record softkey is only available in the Connected call state for the Cisco Chaperone Phone with Feature Hardkeys template.

Procedure

	Command or Action	Purpose
Step 1	Configure a Softkey Template for Recording, on page 103	Configure a softkey template that includes the Record softkey.

	Command or Action	Purpose
Step 2	Perform one of the following procedure: • Associate a Softkey Template with a Phone, on page 104 • Associate a Softkey Template with a Common Device Configuration, on page 104	Associate the softkey template to a phone directly, or to a Common Device Configuration. You can then associate the Common Device Configuration to a group of phones.

Configure a Softkey Template for Recording

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Softkey Template**.

Step 2 Perform the following steps to create a new softkey template; otherwise, proceed to the next step.

a) Click **Add New**.
b) Select a default template and click **Copy**.
c) Enter a new name for the template in the **Softkey Template Name** field.
d) Click **Save**.

Step 3 Perform the following steps to add softkeys to an existing template.

a) Click **Find** and enter the search criteria.
b) Select the required existing template.

Step 4 Check the **Default Softkey Template** check box to designate this softkey template as the default softkey template.

Note If you designate a softkey template as the default softkey template, you cannot delete it unless you first remove the default designation.

Step 5 Choose **Configure Softkey Layout** from the **Related Links** drop-down list in the upper right corner and click **Go**.

Step 6 From the **Select a Call State to Configure** drop-down list, choose the call state for which you want the softkey to display.

Step 7 From the **Unselected Softkeys** list, choose the softkey to add and click the right arrow to move the softkey to the **Selected Softkeys** list. Use the up and down arrows to change the position of the new softkey.

Step 8 Repeat the previous step to display the softkey in additional call states.

Step 9 Click **Save**.

Step 10 Perform one of the following tasks:

- Click **Apply Config** if you modified a template that is already associated with devices to restart the devices.
- If you created a new softkey template, associate the template with the devices and then restart them. For more information, see *Add a Softkey Template to a Common Device Configuration* and *Associate a Softkey Template with a Phone* sections.

Associate a Softkey Template with a Phone

Use this procedure to assign the Record softkey to the phone by associating the softkey template that includes the Record softkey directly to a phone.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** to select the phone to add the softkey template.

Step 3 From the **Softkey Template** drop-down list, choose the template that contains the new softkey.

Step 4 Click **Save**.

Step 5 Press **Reset** to update the phone settings.

Associate a Softkey Template with a Common Device Configuration

Use this procedure to add a Record softkey to the phone by associating the softkey template to a Common Device Configuration.

Procedure

	Command or Action	Purpose
Step 1	Add a Softkey Template to the Common Device Configuration, on page 104	
Step 2	Add Common Device Configuration to Phone, on page 105	

Add a Softkey Template to the Common Device Configuration

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Common Device Configuration**.

Step 2 Perform the following steps to create a new Common Device Configuration and associate the softkey template with it; otherwise, proceed to the next step.

a) Click **Add New**.
b) Enter a name for the Common Device Configuration in the **Name** field.
c) Click **Save**.

Step 3 Perform the following steps to add the softkey template to an existing Common Device Configuration.

a) Click **Find** and enter the search criteria.
b) Click an existing Common Device Configuration.

Step 4 In the **Softkey Template** drop-down list, choose the softkey template that contains the softkey that you want to make available.

Step 5 Click **Save**.

Step 6 Perform one of the following tasks:

- If you modified a Common Device Configuration that is already associated with devices, click **Apply Config** to restart the devices.
- If you created a new Common Device Configuration, associate the configuration with devices and then restart them.

Add Common Device Configuration to Phone

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select the phone device to add the softkey template.

Step 3 From the **Common Device Configuration** drop-down list, choose the common device configuration that contains the new softkey template.

Step 4 Click **Save**.

Step 5 Click **Reset** to update the phone settings.

Recording Call Flow Examples

For call flow examples for both network-based call recording and IP phone-based call recording use cases, refer to *Call Recording Examples for Network-Based and Phone-Based Recording* at the following URL:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/configExamples/cucm_b_recording-use-cases.html

Recording Interactions and Restrictions

Feature	Interactions and Restrictions
Monitoring Tones	Recording Tones take precedence over Monitoring Tones for calls that are both recorded and monitored. If both are configured, and a call is both recorded and monitored, only the recording tone plays.
Multilevel Precedence and Preemption	If you also have Multilevel Precedence and Preemption (MLPP) configured, the **Busy Trigger** setting on the agent phone line that you are recording must be set to a minimum of 3.

Feature	Interactions and Restrictions
Secure Tones	If Secure Tones are configured, the secure tone plays to both call participants at the outset of a secure call, irrespective of whether Recording Tones are configured. If Secure Tones and Recording Tones are both configured and the call is secure, the secure tone plays once at the outset of the call followed by the recording tone. If Secure Tones, Recording Tones, and Monitoring Tones are all configured, and the call is secured, recorded, and monitored, the secure tone plays once followed by the recording tone. The monitoring tone does not play.
Customer Voice Portal	Agent - customer calls that are routed through the Customer Voice Portal may be recorded using the agent phone as the recording source.
SIP Proxy Servers	If you are using the gateway as your recording source, you cannot place SIP proxy servers between Unified Communications Manager and the gateway.
Busy Hour Call Completion Rate	Each recording session adds two calls to the Busy Hour Call Completion (BHCC) rate with a minimal impact on CTI resources.
Selective Recording with Media Sense	When Selective Recording is configured, the Media Sense server does not record the consult call during a transfer. For example, if a call between an agent and a customer is being recorded and the agent initiates a transfer to a second agent, the consult call that takes place between the two agents, prior to the call being transferred, is not recorded. To ensure that the consult call is recorded, the agent must press the ‘Record’ softkey when the consult call starts.
Recording on authenticated phones	The system does not support recording on authenticated phones.
Codec locking for auto recording calls in select and join conference	Skinny Client Control Protocol (SCCP) phone adversities one single codec when recording is enabled and there is a select and join conference performed in Unified Communications Manager.

PART V

Call Center Features

CHAPTER 10

Agent Greeting

Agent Greeting Overview

Agent Greeting enables Unified Communications Manager to automatically play a prerecorded announcement following a successful media connection to the agent device. Agent Greeting is audible for the agent and the customer.

The process of recording a greeting is similar to recording a message for voicemail. Depending on how your contact center is set up, you can record different greetings that play for different types of callers (for example, an English greeting for English speakers or an Italian greeting for Italian speakers).

By default, agent greeting is enabled when you log in to your agent desktop but you can turn it off and on as necessary.

Agent Greeting Prerequisites

- Install Cisco Unified Contact Center Enterprise. See Cisco Unified Contact Center Enterprise Installation and Upgrade Guide.
- Install Cisco Unified Customer Voice Portal. See Installation and Upgrade Guide for Cisco Unified Customer Voice Portal .
- Ensure that you enable Built In Bridge. To view the details, see Configure Built In Bridge, on page 111.

Agent Greeting Configuration Task Flow

Agent Greeting configuration tasks are completed in Cisco Unified Contact Center Enterprise (Unified CCE) and Cisco Unified Customer Voice Portal (Unified CVP). To view detailed steps for the following tasks, see the Agent Greeting section in the Cisco Unified Contact Center Enterprise Features Guide.

Before you begin

- Review Agent Greeting Prerequisites, on page 109

Procedure

	Command or Action	Purpose
Step 1	Configure a media server for Agent Greeting. • Configure a server to act as a media server. • Add the media server in Unified CVP. • Configure the media server to write files.	Agent Greeting uses the Unified CVP media server to store and serve prompt and greeting files.
Step 2	Republish .tcl scripts to Voice Extensible Markup Language (VXML) Gateway.	The .tcl script files that ship with Unified CVP Release 9.0(1) include updates to support Agent Greeting. You must republish these updated files to your VXML Gateway. Republishing scripts to the VXML Gateways is a standard task in Unified CVP upgrades. If you did not upgrade Unified CVP and republish the scripts, you must republish the scripts before you can use Agent Greeting.
Step 3	Set the cache size on the 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.
Step 4	Create voice prompts to record greetings.	Create audio files for each of the voice prompts that agents hear as they record a greeting.
Step 5	Configure call types.	Complete to record and play agent greetings.
Step 6	Configure a dialed number.	Complete to record and play agent greetings.
Step 7	Schedule the script.	
Step 8	Define network VRU scripts.	For Agent Greeting record and play scripts to interact with Unified CVP, Network VRU scripts are required.
Step 9	(Optional) Import sample Agent Greeting scripts.	
Step 10	Modify the Unified CCE call routing scripts.	Modify the Unified CCE call routing scripts to use the Play Agent Greeting script.

Configure Built In Bridge

The **Built in Bridge** field setting in the **Phone Configuration** window for an individual phone overrides the setting for the **Builtin Bridge Enable** clusterwide service parameter.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** to select the agent phone.

Step 3 From the **Built in Bridge** drop-down list, choose one of the following options:

- **On**—The Built in Bridge is enabled.
- **Off**—The Built in Bridge is disabled.
- **Default**—The setting of the clusterwide **Builtin Bridge Enable** service parameter is used.

Step 4 Click **Save**.

Agent Greeting Troubleshooting

For information about how to troubleshoot Agent Greeting issues, see "Troubleshooting Agent Greeting" chapter in the Agent Greeting and Whisper Announcement Feature Guide for Cisco Unified Contact Center Enterprise guide.

CHAPTER 11

Auto-Attendant

Auto-Attendant Overview

Auto-Attendant allows callers to locate people in your organization without talking to a receptionist. You can customize the prompts that are played for the caller.

Auto-Attendant works with Unified Communications Manager to receive calls on specific telephone extensions. The software interacts with the caller and allows the caller to search for and select the extension of the party (in your organization) that the caller is trying to reach.

Auto-Attendant provides the following functions:

- Answers a call
- Plays a user-configurable welcome prompt
- Plays a main menu prompt that asks the caller to perform one of three actions:
  - Press 0 for the operator
  - Press 1 to enter an extension number
  - Press 2 to spell by name

    If the caller chooses to spell by name (by pressing 2), the system compares the letters that are entered with the names that are configured to the available extensions. One of the following results can occur:

    - If a match exists, the system announces a transfer to the matched user and waits for up to 2 seconds for the caller to press any Dual Tone Multifrequency (DTMF) key to stop the transfer. If the caller does not stop the transfer, the system performs an explicit confirmation: it prompts the user for confirmation of the name and transfers the call to the primary extension of that user.
    - If more than one match occurs, the system prompts the caller to choose the correct extension.
    - If too many matches occur, the system prompts the caller to enter more characters.

- If no match occurs, that is, if the user presses wrong options, the system prompts that the user pressed the wrong options and prompts the user to press the correct options.

- When the caller specifies the destination, the system transfers the call.
- If the line is busy or not in service, the system informs the caller accordingly and replays the main menu prompt.

Auto-Attendant solution can be deployed in three different ways as follows using different Cisco products that can provide interactive voice response functionality.

- Auto-Attendant using Cisco Unity Connection (CUC); the most widely used Auto-Attendant solution configuration by customers
- Auto-Attendant using Cisco Unified Contact Center Express (Unified CCX)
- Auto-Attendant using Cisco Unity Express (CUE)

Cisco Unity Connection Configuration

The Cisco Unity Connection server provides Automated-Attendant functionality for both external and internal callers. An Auto-Attendant allows callers to be automatically transferred to an extension without the intervention of an operator or receptionist.

Auto-Attendants offer a menu system; it may also allow a caller to reach a live operator by dialing a number, usually “0”. Multiple Auto-Attendants may be implemented to support individual site locations. Within Cisco Unity Connection, an Auto-Attendant is a customized application tree structure that is built by creating and linking multiple Call Handlers together. The Auto-Attendant is defined by entry and exit points, and intermediate routing decisions based on the callers DTMF input choices.

For more information about Auto-Attendant default behavior and examples, see System Administration Guide for Cisco Unity Connection.

Cisco Unity Connection Configuration Task Flow

You can use this task flow to configure auto-attendant using Cisco Unity Connection:

Procedure

	Command or Action	Purpose
Step 1	Configure CTI Route Point, on page 115	Perform this task on the Cisco Unified CM Administration. Create a CTI Route Point which maps to the Direct-Inward Dial (DID) number of the company (board number).
Step 2	Configure Auto-Attendant System Call Handler, on page 116	Call handlers answer calls, greet callers with recorded prompts, provide callers with information and options, route calls, and take messages.

	Command or Action	Purpose
		Note You can customize the greeting for the AutoAttendant Call Handler by choosing **Edit** > **Greetings**. For more information about customizing greetings, see System Administration Guide for Cisco Unity Connection.
Step 3	Configure Caller Input Option, on page 116	Caller input option enables you to designate a single digit to represent a user extension, alternate contact number, call handler, interview handler, or directory handler. The caller presses a single key during a call handler greeting instead of entering the full extension, and Cisco Unity Connection responds accordingly. Several different keys configured as caller input options offers the callers a menu of choices in the call handler greeting.
Step 4	Configure Extension for Operator Call Handler, on page 117	Configure an extension for the operator to allow callers to speak to an operator during a call handler greeting.
Step 5	Modify Standard Call Transfer Rule for Operator, on page 117	Modify the Standard Call Transfer Rule to enable the call to be transferred to the operator when the caller presses 0 to speak to an operator.
Step 6	Update Default System Transfer Restriction Table, on page 117	Update the Default System Transfer restriction table. The Default System Transfer restriction table restricts numbers that can be used for Caller system transfers, which allow unidentified callers to transfer to a number that they specify.

Configure CTI Route Point

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **CTI Route Point**.

Step 2 Click **Add New**.

Step 3 In the **Device Name** field, enter a device name for the route point.

Step 4 From the **Device Pool** drop-down list, choose **Default**.

Step 5 Click **Save**.
The `Add successful` message is displayed.

Step 6 From the **Association** area, click **Line [1] - Add a new DN**.
The **Directory Number Configuration** window is displayed.

Step 7 In the **Directory Number** field, enter the directory number that matches with the DID of the company.

Step 8 From the **Route Partition** drop-down list, choose the required route partition.

Step 9 From the **Call Forward and Call Pickup Settings** area, for **Forward All**, choose the appropriate calling search space and check the **Voice Mail** check box.

Step 10 Click **Save**.

Configure Auto-Attendant System Call Handler

Procedure

Step 1 From Cisco Unity Connection Administration, from the Cisco Unity Connection tree on the left, navigate to **Call Management** and choose **System Call Handlers**.

Step 2 Click **Add New**.
The **New Call Handler** window is displayed.

Step 3 In the **Display Name** field, enter **AutoAttendant**.

Step 4 In the **Extension** field, enter the same extension that you provided for the CTI Route Point.

Step 5 Click **Save**.
The **Edit Call Handler Basics (AutoAttendant)** window is displayed.

Step 6 Edit the required fields and click **Save**.

Configure Caller Input Option

Procedure

Step 1 From Cisco Unity Connection Administration, from the Cisco Unity Connection tree on the left, navigate to **Call Management** and choose **System Call Handlers**.

Step 2 Click **AutoAttendant**.
The **Edit Call Handler Basics (AutoAttendant)** window is displayed.

Step 3 Choose **Edit** > **Caller Inputs**.
The **Caller Input** window is displayed.

Step 4 In the **Key** column, click **0**.
The **Edit Caller Input (0)** window is displayed.

Step 5 Click the **Call Handler** radio button, choose **Operator** from the drop-down list, and click the **Attempt Transfer** radio button.

Step 6 Click **Save**.
The `Updated Caller Input` status message is displayed.

Step 7 Choose **Edit** > **Caller Inputs**.
The **Caller Input** window is displayed.

Step 8 In the **Key** column, click **1**.
The **Edit Caller Input (0)** window is displayed.

Step 9 In the **Conversation** radio button, choose **Caller System Transfer** from the drop-down list.

Step 10 Click **Save**.

The `Updated Caller Input` status message is displayed.

Configure Extension for Operator Call Handler

Procedure

Step 1 From Cisco Unity Connection Administration, from the Cisco Unity Connection tree on the left, navigate to **Call Management** and choose **System Call Handlers**.

Step 2 Click **Operator**.
The **Edit Call Handler Basics (Operator)** window is displayed.

Step 3 Enter the extension of the operator in the **Extension** field and click **Save**.
The `Updated Caller Input` status message is displayed.

Modify Standard Call Transfer Rule for Operator

Procedure

Step 1 From Cisco Unity Connection Administration, from the Cisco Unity Connection tree on the left, navigate to **Call Management** and choose **System Call Handlers**.

Step 2 Click **Operator**.
The **Edit Call Handler Basics (Operator)** window is displayed.

Step 3 From the **Edit** menu, choose **Transfer Rules**.
The **Transfer Rules** window is displayed.

Step 4 Click **Standard**.
The **Edit Transfer Rule (Standard)** window is displayed.

Step 5 In the **Transfer Calls to** option, click the **Extension** radio button and enter the configured operator extension number.

Step 6 Click **Save**.

Update Default System Transfer Restriction Table

Procedure

Step 1 From Cisco Unity Connection Administration, from the Cisco Unity Connection tree on the left, navigate to **System Settings** and choose **Restriction Tables**.

Step 2 Click **Default System Transfer**.
The **Edit Restriction Table Basics (Default System Transfer)** window is displayed.

Step 3 Uncheck the check box in the **Blocked** column for 6 in the **Order** column.

Step 4 Click **Save**.

Cisco Unity Connection Auto-Attendant Troubleshooting

For information about troubleshooting Auto-Attendant using Cisco Unity Connection, see the following:

- http://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-callmanager/107517-calltrf.html
- http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/8x/troubleshooting/guide/8xcuctsgx/8xcuctsg110.html
- http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/8x/troubleshooting/guide/8xcuctsgx/8xcuctsg040.html
- http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/8x/troubleshooting/guide/8xcuctsgx/8xcuctsg180.html

Cisco Unified CCX Configuration

Auto-Attendant comes standard with the five-seat bundle of Cisco Unified Contact Center Express (Unified CCX).

Note For information about the supported versions of Cisco Unified CCX with Unified Communications Manager, see Cisco Collaboration Systems Release Summary Matrix for IP Telephony.

For information about getting started with scripts, see the Cisco Unified Contact Center Express Getting Started with Scripts.

Cisco Unified CCX Prerequisites

- Install and configure Cisco Unified CCX before you can use Auto-Attendant. Cisco Unified CCX controls the software and its connection to the telephony system.
- Configure users on Unified Communications Manager.

Cisco Unified CCX Auto-Attendant Task Flow

Auto-Attendant configuration tasks are completed in Cisco Unified Contact Center Express (Unified CCX). To view detailed steps for the following tasks, see Cisco Unified CCX Administration Guide and the Cisco Unified Contact Center Express Getting Started with Scripts respectively.

Before you begin

- Learn more about the Auto-Attendant feature by reviewing Auto-Attendant Overview, on page 113.

- Learn more about Cisco UCCX with Auto-Attendant functionality by reviewing Cisco Unified CCX Configuration, on page 118
- Review Cisco Unified CCX Prerequisites, on page 118.

Procedure

	Command or Action	Purpose
Step 1	Configure Unified CM Telephony call control groups.	The Unified CCX system uses Unified CM Telephony call control groups to pool together a series of CTI ports, which the system uses to serve calls as they arrive or depart from the Unified CCX server.
Step 2	Add a Cisco Media Termination (CMT) dialog control group.	The Cisco Media subsystem is a subsystem of the Unified CCX Engine. The Cisco Media subsystem manages the CMT media resource. CMT channels are required for Unified CCX to be able to play or record media. The Cisco Media subsystem uses dialog groups to organize and share resources among applications. A dialog group is a pool of dialog channels in which each channel is used to perform dialog interactions with a caller, during which the caller responds to automated prompts by pressing buttons on a touch-tone phone. **Caution** All media termination strings begin with “auto” and contain the same ID as the call control group—not the CMT dialog group. Perform this procedure if the default media termination is configured and the ID differs.
Step 3	Configure a Cisco script application.	The Unified CCX script applications are applications that are based on scripts created in the Unified CCX Editor. These applications come with every Unified CCX system and executes scripts that are created in the Unified CCX Editor.
Step 4	Provision a Unified CM Telephony trigger.	A Unified CM Telephony trigger responds to calls that arrive on a specific route point by selecting telephony and media resources to serve the call and invoking an application script to handle the call.
Step 5	Customize Auto-Attendant. • Modify an existing Auto-Attendant instance	The Cisco Unified CCX Administration page allows you to modify any existing Auto-Attendant instance as necessary.

	Command or Action	Purpose
	• Configure the Auto-Attendant prompts	Cisco Unified CCX allows you to customize the Auto-Attendant prompts from the Cisco Unified CCX Administration Media Configuration window. It allows you to record the welcome prompt, configure the welcome prompt, and upload a spoken name.

Cisco Unified CCX Auto-Attendant Troubleshooting

For information about troubleshooting Auto-Attendant using Cisco Unified CCX, see http://docwiki.cisco.com/wiki/List_of_Troubleshooting_Tips_for_Unified_CCX_7.0#Cisco_Unified_Communications_Manager_Automated_Attendant (applicable only for Windows version).

Cisco Unity Express Configuration

For information about Auto-Attendant Configuration using Cisco Unity Express, see the "Configuring Auto Attendants" chapter in Cisco Unity Express VoiceMail and Auto Attendant CLI Administrator Guide for 3.0 and Later Versions.

For information about deploying a sample Auto-Attendant script, see "Deployment of sample script aa.aef" chapter in the Getting Started with Cisco Unified IP IVR.

For information about an Auto-Attendant example, see "Auto Attendant Script Example" chapter in the Cisco Unity Express Guide to Writing and Editing Scripts for 7.0 and Later Versions.

For information about Auto-Attendant design considerations, see "Auto Attendant Design Considerations" chapter in the Cisco Unity Express Design Guide.

Cisco Unity Express Auto-Attendant Troubleshooting

For information about Auto-Attendant troubleshooting using Cisco Unity Connection, see the "Troubleshooting Cisco Unity Express Automated Attendant" in Excerpts from Cisco IP Communications Express: CallManager Express with Cisco Unity Express.

CHAPTER 12

Manager Assistant

Cisco Unified Communications Manager Assistant Overview

The Unified Communications Manager Assistant feature is a plug-in that an assistant can use to handle calls on behalf of a manager, intercept manager calls, and route them appropriately.

Manager Assistant supports up to 3500 managers and 3500 assistants. To accommodate this number of users, you can configure up to three Manager Assistant applications in one Unified Communications Manager cluster and assign managers and assistants to each instance of the application.

Manager Assistant supports shared line support and proxy line support.

Manager Assistant Architecture

The Manager Assistant architecture comprises the following:

- **Cisco IP Manager Assistant service**—After you install Unified Communications Manager, activate this service from the Cisco Unified Serviceability interface.
- **Assistant Console interface**—Allows assistants to access the Manager Assistant features on their computer to handle calls for managers. The Manager Assistant handles calls for an assistant and for as many as 33 managers.
- **Cisco Unified IP Phone interface:** Managers and assistants use softkeys and the Cisco Unified IP Phone Services button to access the Manager Assistant features.

For more information, see chapter Manager Assistant, in Feature Configuration Guide for Cisco Unified Communications Manager.

Manager Assistant Database Access Architecture

The database stores all Manager Assistant configuration information. When the manager or assistant logs in, the Cisco IP Manager Assistant service retrieves all data that is related to the manager or assistant from the database and stores it in memory. The database includes two interfaces:

- **Manager interface**—The manager phone makes available the manager features except Manager Configuration. Manager Assistant automatically logs in a manager in to the Cisco IP Manager Assistant service when the Cisco IP Manager Assistant service starts.

  Note Managers also have access to Unified Communications Manager features such as Do Not Disturb and Immediate Divert.

- **Assistant interface**—The assistant accesses the Manager Assistant features by using the Assistant Console application and the Cisco Unified IP Phone. The Assistant Console, an application, provides call-control functions such as answer, divert, transfer, and hold. The assistant uses the Assistant Console to log in and log out, to set up assistant preferences, and to display the **Manager Configuration** window that is used to configure manager preferences.

For more information, see chapter Manager Assistant, in Feature Configuration Guide for Cisco Unified Communications Manager.

Softkeys

Manager Assistant supports the following softkeys:

- Redirect
- Transfer to VoiceMail
- Do Not Disturb

Manager Assistant supports the following softkey templates:

- Standard Manager—Supports manager for proxy mode
- Standard Shared Mode Manager—Supports manager for shared mode
- Standard Assistant—Supports assistant in proxy or shared mode
- Standard User—The system makes call-processing (such as Hold and Dial) softkeys available with the Standard User template.

Manager Assistant Shared Line Overview

When you configure Manager Assistant in shared line mode, the manager and assistant share a directory number, for example, 8001. The assistant handles calls for a manager on the shared directory number. When a manager receives a call on 8001, both the manager phone and the assistant phone ring.

The Manager Assistant features that do not apply to shared line mode include Default Assistant Selection, Assistant Watch, Call Filtering, and Divert All Calls. An assistant cannot see or access these features on the Assistant Console application.

Manager Assistant Proxy Line Overview

When you configure Manager Assistant in proxy line mode, the assistant handles calls for a manager using a proxy number. The proxy number is not the directory number for the manager, but is an alternate number chosen by the system that an assistant uses to handle manager calls. In proxy line mode, a manager and an assistant have access to all features that are available in Manager Assistant, which include Default Assistant Selection, Assistant Watch, Call Filtering, and Divert All Calls.

Manager Assistant Prerequisites

- From Release 12.0(1)SU4 onwards, the user should install JRE on 32 or 64-bit Windows platform before the user upgrades the Manager Assistant client to a newer version.

  Note Before you perform the upgrade, ensure that you uninstall the Cisco Unified Communications Manager Assistant client that is currently installed on your machine.

- Manager Assistant supports the following browsers and platform:
  - Unified Communications Manager Assistant Administration and the Assistant Console are supported on Internet Explorer 11 with Windows 10 (64 bit) or later, Firefox with Windows 10 (64 bit) or later, and Safari with MacOS (10.x) or later.
  - On a computer running Windows 10 or Apple MAC OS X, customers can open one of the browsers specified above.
- To display Manager Assistant features in other languages, install the locale installer before you configure the Manager Assistant.
- The Assistant Console application is supported on computers that run Windows 10, or later.
- You must configure the phones and users, and associated the devices to the users. In addition, for shared line appearances between managers and assistants, you must configure the same directory number on the manager primary line and assistant secondary line.
- To add managers and assistants in bulk, install the Cisco Unified Communications Manager Bulk Administration Tool. For more information, see the *Bulk Administration Guide*.

Manager Assistant Task Flow for Proxy Lines

Before you begin

- Review Manager Assistant Prerequisites, on page 123.

Procedure

	Command or Action	Purpose
Step 1	Run the Cisco Unified CM Assistant Configuration Wizard, on page 124	
Step 2	Configure Manager And Assign Assistant For Proxy Line, on page 131	
Step 3	Configure Assistant Line Appearances for Proxy Line, on page 133	
Step 4	Install Assistant Console Plugin, on page 151	The assistant accesses the Unified Communications Manager Assistant features by using the Assistant Console application and the Cisco Unified IP Phone. The Assistant Console provides call-control functions such as answer, divert, transfer, and hold.
Step 5	Configure the manager and Assistant Console applications.	See Cisco Unified Communications Manager Assistant User Guide for Cisco Unified Communications Manager.

Run the Cisco Unified CM Assistant Configuration Wizard

You can run the Cisco Unified CM Assistant Configuration Wizard to automatically create partitions, calling search spaces, and route points. The wizard also creates Bulk Administration Tool (BAT) templates for the manager phones, the assistant phones, and all other user phones. You can use the BAT templates to configure the managers, assistants, and all other users. For more information about BAT, see Bulk Administration Guide for Cisco Unified Communications Manager .

Before you begin

Ensure that the configuration wizard runs on the same server (the Unified Communications Manager server) as the Bulk Administration Tool.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Application** > **Cisco Unified CM Assistant Configuration Wizard**.

Step 2 Click **Next** to begin the Cisco Unified CM Assistant Configuration wizard process.

Step 3 In the **Partition for Managers** window, enter a name, provide a description, and then click **Next**. Alternatively, you can accept the default partition name and description.

Step 4 In the **Partition for CTI Route Point** window, enter a name, provide a description, and then click **Next**. Alternatively, you can accept the default CTI route point name.

Step 5 In the **Partition for All Users** window, enter a name, provide a description and then click **Next**. Alternatively, you can accept the default partition name and description for all users.

Step 6 In the **Intercom Partition** window, enter a name, provide a description, and then click **Next**. Alternatively, you can accept the default intercom partition name.

Step 7 In the **Assistant Calling Search Space** window, enter a name, and provide a description. Alternatively, you can use the default calling search space name and description.
The Available Partitions and Selected Partitions boxes under the Route Partitions for this Calling Search Space automatically list Partitions for the Assistant Calling Search Space. You can accept the default values or you can choose the applicable partition from the Available Partitions box. Use the up and down arrows to move partitions from one box to the other.

Step 8 Click **Next**.

Step 9 In the **Everyone Calling Search Space** window, enter a name, and provide a description. Alternatively, you can accept the default calling search space name and description for everyone.
The Available Partitions and Selected Partitions boxes under the Route Partitions for this Calling Search Space automatically list Partitions for the Assistant Calling Search Space. You can accept the default values or you can choose the applicable partition from the Available Partitions box. Use the up and down arrows to move partitions from one box to the other.

Step 10 Click **Next**.
If you have existing calling search spaces that are configured on the system, the **Existing Calling Search Spaces** window is displayed; otherwise, proceed to the next step.

Manager Assistant requires that the existing calling search spaces add the prefix **Generated_Route Point** and **Generated_Everyone** partitions. The Available Calling Search Spaces and Selected Calling Search Spaces boxes automatically list these partitions. Use the up and down arrows to move partitions from one box to the other.

Note The prefix that is added to the existing calling search spaces may change if the administrator has changed the names of the partitions.

Step 11 Click **Next**.

Step 12 In the **CTI Route Point** window, enter a name in the CTI route point name field; otherwise, use the default CTI route point name.

Step 13 From the drop-down list, choose the appropriate device pool.

Step 14 Enter a route point directory number; otherwise, use the default route point directory number.

Step 15 From the drop-down list, choose the appropriate numbering plan and then click **Next**.

Step 16 In the **Phone Services** window, enter the primary phone service name; otherwise, use the default Phone Service name.

Step 17 From the drop-down list, choose the primary Cisco Unified Communications Manager Assistant server or enter a server name or IP address.

Step 18 Enter the secondary phone service name; otherwise, use the default phone service name.

Step 19 From the drop-down list, choose the secondary Cisco Unified Communications Manager Assistant server or enter a server name or IP address and then click **Next**.
The **Confirmation** window is displayed. It provides all the information that you chose. If the information is not correct, you can cancel the configuration process or return to the previous configuration windows.

Step 20 Click **Finish**.
Upon completion, a final status window is displayed.

Any errors that the configuration wizard generates is sent to a trace file. Access this file by using the following CLI command: **`file get activelog tomcat/logs/ccmadmin/log4j`**

What to do next

The Cisco Unified CM Assistant Configuration Wizard only creates the Cisco IP Manager Assistant service parameters. You must enter the remaining service parameters manually. For service parameter information, see Manager Assistant Service Parameters for Proxy Line, on page 126.

Manager Assistant Service Parameters for Proxy Line

From Cisco Unified CM Administration, choose **System** > **Service Parameters**. Choose the server on which the Cisco IP Manager Assistant service is active and click **?** for detailed descriptions.

Setting	Description
Cisco IP Manager Assistant (Active) Parameters	
CTIManager (Primary) IP Address	This parameter specifies the IP address of the primary CTIManager that this Cisco IPMA server uses to process calls. No default value.
CTIManager (Backup) IP Address	This parameter specifies the IP address of the backup CTIManager that this Cisco IPMA server uses to process calls when primary CTIManager is down. No default value.
Route Point Device Name for Proxy Mode	This parameter specifies the device name of the CTI route point that this Cisco IPMA server uses to intercept all calls to managers' primary lines for intelligent call routing. Cisco recommends that you use same CTI route point device for all servers running the IPMA service. You must configure the CTI route point device name if any manager or assistant will be configured to use proxy mode.
CAPF Profile Instance Id for Secure Connection to CTIManager	This service parameter specifies the Instance ID of the Application CAPF Profile for the application user **IPMASecureSysUser** that this Manager Assistant will use to open a secure connection to CTIManager. Configure this parameter if **CTIManager Connection Security Flag** is enabled.
Clusterwide Parameters (Parameters that apply to all servers) **Important** Click **Advanced** to view the hidden parameters.	
Cisco IPMA Server (Primary) IP Address	This parameter specifies the IP address of the primary Cisco IPMA server. No default value.

Setting	Description
Cisco IPMA Server (Backup) IP Address	This parameter specifies the IP address of the backup Cisco IPMA server. The backup server provides IPMA service when the primary IPMA server fails. No default value.
Cisco IPMA Server Port	This parameter specifies the TCP/IP port on the Cisco IPMA servers to which the IPMA Assistant Consoles will open socket connections. You may change the parameter if a port conflict exists. Default value: 2912
Cisco IPMA Assistant Console Heartbeat Interval	This parameter specifies the interval, in seconds, at which the Cisco IPMA server sends keepalive messages (commonly referred to as heartbeat) to the IPMA Assistant Consoles. The IPMA Assistant Consoles initiate failover when they fail to receive heartbeat from the server before the time that is specified in this parameter expires. Default value: 30 seconds
Cisco IPMA Assistant Console Request Timeout	This parameter specifies the time, in seconds, that the IPMA Assistant Consoles wait to receive a response from the Cisco IPMA server. Default value: 30 seconds
Cisco IPMA RNA Forward Calls	This parameter determines whether Cisco IPMA Ring No Answer (RNA) forwarding is enabled. Valid values are **True** (Cisco IPMA forwards unanswered calls to next available assistant) or **False** (Cisco IPMA does not forward calls). This parameter works in conjunction with the **Cisco IPMA RNA Timeout** parameter; calls are forwarded after the time that is specified in the **Cisco IPMA RNA Timeout** parameter. If a voicemail profile is specified for the line, unanswered calls that cannot be forwarded to an assistant are sent to voicemail when this timer expires. Default value: False
Alpha Numeric UserID	This parameter determines whether Cisco IPMA Assistant Phone uses an alphanumeric user ID or a numeric user ID. Default value: True

Setting	Description
Cisco IPMA RNA Timeout	This parameter specifies the time, in seconds, that the Cisco IPMA server waits before forwarding an unanswered call to the next available assistant. This parameter works in conjunction with the **Cisco IPMA RNA Forward Calls** parameter; forwarding occurs only if the **Cisco IPMA RNA Forward Calls** parameter is set to **True**. Default value: 10 seconds
CTIManager Connection Security Flag	This parameter determines whether security for the Cisco IP Manager Assistant service CTIManager connection is enabled. If it is enabled, Cisco IPMA opens a secure connection to CTIManager using the CAPF profile that is configured for the instance ID (as specified in the **CAPF Profile Instance ID for Secure Connection to CTIManager** service parameter) for the application user **IPMASecureSysUser**. Default value: Non Secure To enable security, you must select an instance ID in the **CAPF Profile Instance ID for Secure Connection to CTIManager** service parameter.
Redirect call to Manager upon failure to reach Assistant	This parameter determines whether the Cisco Unified IP Manager Assistant application redirects the call back to the intended manager if the call fails to reach the selected proxy assistant. Default value: False
Advanced Clusterwide parameters **Important** Configure unique IP addresses for each pool so that the same Cisco IPMA server IP address does not appear in more than one pool.	
Enable Multiple Active Mode	This parameter determines whether multiple instances of the Cisco IP Manager Assistant service must be run for scalability. If it is enabled, Cisco IPMA can run on the other nodes as configured in the Pool 2 and Pool 3 parameters. To enable multiple active mode, you must enter the IP addresses of the nodes on which you want to run the additional instances of Cisco IPMA. Configure the Cisco IP Manager Assistant service parameters on those nodes. Default value: False

Setting	Description
Pool 2: Cisco IPMA Server (Primary) IP Address	If multiple active mode is enabled, this parameter specifies the IP address of the primary Cisco IPMA server of the second instance of Cisco IPMA. Configure the Cisco IP Manager Assistant service parameters on this node.
Pool 2: Cisco IPMA Server (Backup) IP Address	If multiple active mode is enabled, this parameter specifies the IP address of the backup Cisco IPMA server of the second instance of Cisco IPMA. The backup server provides IPMA service when the primary IPMA server fails. Configure the Cisco IP Manager Assistant service parameters on this node.
Pool 3: Cisco IPMA Server (Primary) IP Address	If multiple active mode is enabled, this parameter specifies the IP address of the primary Cisco IPMA server of the third instance of Cisco IPMA. Configure the Cisco IP Manager Assistant service parameters on this node.
Pool 3: Cisco IPMA Server (Backup) IP Address	If multiple active mode is enabled, this parameter specifies the IP address of the primary Cisco IPMA server of the third instance of Cisco IPMA. The backup server provides IPMA service when the primary IPMA server fails. Configure the Cisco IP Manager Assistant service parameters on this node.
Clusterwide Parameters (Softkey Templates) **Important** Configure these parameters if you want to use the Manager Assistant automatic configuration for managers and assistants.	
Assistant Softkey Template	This parameter specifies the assistant softkey template that is assigned to assistant devices during Automatic Configuration. The value that is specified in this parameter is used when the **Automatic Configuration** check box is checked on the **Cisco IPMA Assistant Configuration** page.
Manager Softkey Template for Proxy Mode	This parameter specifies the manager softkey template for proxy mode that is assigned to manager devices during Automatic Configuration. This parameter applies only for managers that use proxy mode.
Clusterwide Parameters (IPMA Device Configuration Defaults for Proxy Mode)	

Setting	Description
Manager Partition	This parameter defines the partition that is assigned to manager lines that IPMA handles on manager devices during Automatic Configuration. Make sure the partition you want to use has already been added to Cisco Unified CM Administration. If the **Cisco IPMA Configuration Wizard** is run, it will populate this value. This parameter applies only for managers that use proxy mode.
All User Partition	This parameter specifies the partition that is configured on all proxy lines and the intercom line on assistant devices, as well as the intercom line on manager devices, during Automatic Configuration. Make sure the partition you want to use has already been added to Cisco Unified CM Administration. If the **Cisco IPMA Configuration Wizard** is run, it will populate this value. This parameter applies only for managers or assistants that use proxy mode.
IPMA Calling Search Space	This parameter specifies the calling search space that is configured for manager lines on manager devices that IPMA handles and the intercom line, as well as the assistant intercom line on assistant devices during Automatic Configuration. Make sure the calling search space you want to use has already been added to Cisco Unified CM Administration. If **Cisco IPMA Configuration Wizard** is run, it will populate this value. This parameter applies only for managers or assistants that use proxy mode.
Manager Calling Search Space	This parameter defines the manager calling search space that is configured on proxy lines on assistant devices during Automatic Configuration. This calling search space must be a calling search space that already exists in the system. If **Cisco IPMA Configuration Wizard** is run, it will populate this value. This parameter applies only for assistants that use proxy mode.
Cisco IPMA Primary Phone Service	This parameter defines the IP phone service to which manager/assistant devices will be subscribed during Automatic Configuration. If **Cisco IPMA Configuration Wizard** is run, it will populate this value. This parameter applies only for managers or assistants that use proxy mode.

Setting	Description
Cisco IPMA Secondary Phone Service	This parameter defines the secondary IP phone service to which manager or assistant devices will be subscribed during Automatic Configuration. If **Cisco IPMA Configuration Wizard** is run, it will populate this value. This parameter applies only for managers or assistants that use proxy mode.
Clusterwide Parameters (Proxy Directory Number Range for Proxy Mode)	
Starting Directory Number	This parameter specifies the starting directory number that is used as the starting number for automatic generation of proxy directory numbers during IPMA assistant configuration. After an auto-generated proxy line number is used for an assistant, the next number will be generated for the next assistant, and so on. This parameter applies only for assistants that use proxy mode.
Ending Directory Number	This parameter specifies the ending directory number for automatic generation of proxy directory numbers during IPMA assistant configuration. Configuration will stop at this number. This parameter applies only for assistants that use proxy mode.
Clusterwide Parameters (Proxy Directory Number Range for Proxy Mode)	
Number of Characters to be Stripped from Manager DN	This parameter specifies the number of characters to be stripped from the manager directory number (DN) in the process of generating the proxy DN. Generating a proxy DN may involve stripping some number of digits and adding a prefix. Digits are stripped starting from the left. This parameter applies only for assistants that use proxy mode.
Prefix for Manager DN	This parameter specifies the prefix to be added to a manager DN in the process of generating the proxy DN. Generating a proxy DN may involve some stripping of digits and adding a prefix. This parameter applies only for assistants that use proxy mode.

Configure Manager And Assign Assistant For Proxy Line

For information about configuring a new user and associating a device to the user, see Administration Guide for Cisco Unified Communications Manager.

Note Make sure you configure manager information before you configure assistant information for an assistant.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **End User**.

Step 2 Click **Find**.
The search result displays all the end users that are configured in Unified Communications Manager.

Step 3 From the **Related Links** drop-down list, choose **Manager Configuration** and click **Go**.

Tip To view existing assistant configuration information, click the assistant name in the Associated Assistants list and click **View Details**. The **Cisco Unified CM Assistant - Assistant Configuration** window is displayed. To return to the manager configuration information, click the manager name in the Associated Managers list and click **View Details**.

The **Cisco Unified CM Assistant - Manager Configuration** window is displayed.

Step 4 From the **Device Name/Profile** drop-down list, choose the device name or device profile to associate a device name or device profile with a manager. For more information about Extension Mobility with Manager Assistant, see Manager Assistant Interactions, on page 152.

Note If the manager telecommutes, click the **Mobile Manager** check box and optionally choose a device profile from the **Device Name/Profile** drop-down list. After you choose a device profile, the manager must log in to the phone by using extension mobility before accessing Manager Assistant.

Step 5 From the **Intercom Line** drop-down list, choose the intercom line appearance for the manager, if applicable.

Note The chosen intercom line applies to the Manager Assistant and Unified Communications Manager intercom features.

Step 6 From the **Assistant Pool** drop-down list, choose the appropriate pool number (1 to 3).

Step 7 From the **Available Lines** selection box, choose a line that you want Manager Assistant to control and click the down arrow to make the line display in the Selected Lines selection box. Configure up to five Manager Assistant—controlled lines.

Tip To remove a line from the Selected Lines selection box and from Manager Assistant control, click the up arrow.

Step 8 Check the **Automatic Configuration** check box to automatically configure the softkey template, subscribe to the Manager Assistant phone service, calling search space, and partition for Manager Assistant—Controlled selected lines and intercom line; and Auto Answer with Speakerphone for intercom line for the manager phone based on the Cisco IP Manager Assistant service parameters.

Note Automatic Configuration for intercom applies only when using the Manager Assistant intercom feature for the Cisco Unified IP Phones 7940 and 7960.

Step 9 Click **Save**.
If you checked the **Automatic Configuration** check box and the service parameters are invalid, a message displays. Ensure that the service parameters are valid. Upon successful completion of the automatic configuration, the manager device resets. If you configured a device profile, the manager must log out and log in to the device for settings to take effect.

Configure Assistant Line Appearances for Proxy Line

A proxy line specifies a phone line that appears on the assistant Cisco Unified IP Phone. Manager Assistant uses proxy lines to manage calls that are intended for a manager. The administrators can manually configure a line on the assistant phone to serve as the proxy line, or you can enable the **Automatic Configuration** check box to generate a DN and to add the line to the assistant phone.

Note

1. Make sure that you configure manager information and assign an assistant to the manager before you configure assistant information for an assistant.
2. If you want to automatically configure proxy line on the assistant phone, configure the service parameters in **Proxy Directory Number Range** and **Proxy Directory Number Prefix** sections.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **End User**.

Step 2 Click **Find**.

Step 3 Click on the user name to display user information for the chosen assistant
The **End User Configuration** window is displayed.

Step 4 From the **Related Links** drop-down list, choose **Assistant Configuration** and click **Go**.

Note The system automatically sets the softkey template and intercom line on the basis of the Cisco IP Manager Assistant service parameter settings when the **Automatic Configuration** check box is checked. In addition, the system also sets Auto Answer with Speakerphone for intercom line.

The **Assistant Configuration** window is displayed.

Step 5 From the **Device Name** drop-down list, choose the device name to associate with the assistant.

Step 6 From the **Intercom Line** drop-down list, choose the incoming intercom line appearance for the assistant.

Step 7 From the **Primary Line** drop-down list, choose the primary line for the assistant.

Step 8 To associate the manager line to the assistant line, perform the following steps from the Manager Association to Assistant Line selection box:

a) From the **Available Lines** drop-down list, choose the assistant line that will be associated with the manager line.
b) From the **Manager Names** drop-down list, choose the preconfigured manager name for whom this proxy line will apply.
c) From the **Manager Lines** drop-down list, choose the manager line for which this proxy line will apply.

Step 9 Click **Save**.
The update takes effect immediately. If you chose **Automatic Configuration**, the assistant device automatically resets.

Manager Assistant Task Flow for Shared Lines

Before you begin

- Review Manager Assistant Prerequisites, on page 123.

Procedure

	Command or Action	Purpose
Step 1	Configure Partitions for Manager Assistant Shared Line Support, on page 135	Configure a partition for lines that is used by Manager Assistant.
Step 2	Configure Calling Search Spaces for Manager Assistant Shared Line Support, on page 136	Configure calling search spaces for manager and assistant lines.
Step 3	Configure Cisco IP Manager Assistant Service Parameters, on page 137	Configure these parameters to use automatic configuration for managers and assistants.
Step 4	Configure Intercom Settings • Configure an Intercom Partition, on page 138 • Configure an Intercom Calling Search Space, on page 278 • Configure an Intercom Directory Number, on page 286 • Configure an Intercom Translation Pattern, on page 279	
Step 5	Configure Multiple Manager Assistant Pool, on page 140	Configure multiple pools if you need to support a large number of managers and assistants. You can configure up to three active Cisco IP Manager Assistant servers, with each managing up to 2500 pairs of managers and assistants.
Step 6	Configure Secure TLS Connection to CTI for Manager Assistant • Configure IPMASecureSysUser Application User, on page 141 • Configure CAPF Profile, on page 141 • Configure Cisco IP Manager Assistant, on page 143	Follow these procedures if your system is running in mixed mode.
Step 7	Configure CTI Route Point, on page 144	Cisco Unified Communications Manager Assistant requires creation of CTI route point to intercept and route calls from managers.
Step 8	Configure IP Phone Services for Manager and Assistant, on page 144	

	Command or Action	Purpose
Step 9	Configure Phone Button Templates for Manager, Assistant, and Everyone, on page 147	
Step 10	Configure Manager and Assign Assistant for Shared Line Mode, on page 149	
Step 11	Configure Assistant Line Appearances for Shared Line, on page 150	
Step 12	Install Assistant Console Plugin, on page 151	The assistant accesses the Cisco Unified Communications Manager Assistant features by using the Assistant Console application and the Cisco Unified IP Phone. The Assistant Console provides call-control functions such as answer, divert, transfer, and hold.
Step 13	Configure the manager and assistant console applications.	See Cisco Unified Communications Manager Assistant User Guide for Cisco Unified Communications Manager.

Configure Partitions for Manager Assistant Shared Line Support

You must create three partitions: Generated_Everyone, Generated_Managers, and Generated_Route_Point.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Partition**.

Step 2 Click **Add New** to create a new partition.

Step 3 In the **Partition Name, Description** field, enter a name for the partition that is unique to the route plan.

Partition names can contain alphanumeric characters, as well as spaces, hyphens (-), and underscore characters (_). See the online help for guidelines about partition names.

Step 4 Enter a comma (,) after the partition name and enter a description of the partition on the same line.

The description can contain up to 50 characters in any language, but it cannot include double quotes ("), percentage sign (%), ampersand (&), backslash (\), angle brackets (<>), or square brackets ([ ]).

If you do not enter a description, Cisco Unified Communications Manager automatically enters the partition name in this field.

Step 5 To create multiple partitions, use one line for each partition entry.

Step 6 From the **Time Schedule** drop-down list, choose a time schedule to associate with this partition.

The time schedule specifies when the partition is available to receive incoming calls. If you choose **None**, the partition remains active at all times.

Step 7 Select one of the following radio buttons to configure the **Time Zone**:

- **Originating Device**—When you select this radio button, the system compares the time zone of the calling device to the **Time Schedule** to determine whether the partition is available is available to receive an incoming call.

- **Specific Time Zone**—After you select this radio button, choose a time zone from the drop-down list. The system compares the chosen time zone to the **Time Schedule** to determine whether the partition is available is available to receive an incoming call.

Step 8 Click **Save**.

Partition Name Guidelines for Manager Assistant Shared Line Support

The list of partitions in a calling search space is limited to a maximum of 1024 characters. This means that the maximum number of partitions in a CSS varies depending on the length of the partition names. Use the following table to determine the maximum number of partitions that you can add to a calling search space if partition names are of fixed length.

Table 14: Partition Name Guidelines

Partition Name Length	Maximum Number of Partitions
2 characters	340
3 characters	256
4 characters	204
5 characters	172
. . .	. . .
10 characters	92
15 characters	64

Configure Calling Search Spaces for Manager Assistant Shared Line Support

A calling search space is an ordered list of route partitions that are typically assigned to devices. Calling search spaces determine the partitions that calling devices can search when they are attempting to complete a call.

You must create two calling search spaces: Generated_CSS_I_E and Generated_CSS_M_E.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Calling Search Space**.

Step 2 Click **Add New**.

Step 3 In the **Name** field, enter a name.

Ensure that each calling search space name is unique to the system. The name can include up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_).

Step 4 In the **Description** field, enter a description.

The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).

Step 5 From the **Available Partitions** drop-down list, perform one of the following steps:

- For a single partition, select that partition.
- For multiple partitions, hold down the **Control (CTRL)** key, then select the appropriate partitions.

Step 6 Select the down arrow between the boxes to move the partitions to the **Selected Partitions** field.

Step 7 (Optional) Change the priority of selected partitions by using the arrow keys to the right of the **Selected Partitions** box.

Step 8 Click **Save**.

Configure Cisco IP Manager Assistant Service Parameters

Configure Cisco IP Manager Assistant service parameters if you want to use the Manager Assistant automatic configuration for managers and assistants. You must specify the cluster-wide parameters once for all Cisco IP Manager Assistant services and general parameters for each Cisco IP Manager Assistant service that is installed.

Procedure

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

Step 2 From the **Server** drop-down list, choose the server on which the Cisco IP Manager Assistant service is active.

Step 3 From the **Service** drop-down list, choose **Cisco IP Manager Assistant** service.
The **Service Parameter Configuration** window, which lists the parameters, is displayed.

Step 4 Configure the **Cisco IP Manager Assistant Parameters**, **Clusterwide Parameters (Parameters that apply to all servers)**, and **Clusterwide Parameters (Softkey Templates)**.

click ? for detailed descriptions.

Step 5 Click **Save**.

Configure Intercom Settings

Procedure

	Command or Action	Purpose
Step 1	Configure an Intercom Partition, on page 138	
Step 2	Configure an Intercom Calling Search Space, on page 138	
Step 3	Configure an Intercom Directory Number, on page 139	
Step 4	Configure an Intercom Translation Pattern, on page 139	

Configure an Intercom Partition

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Intercom** > **Intercom Route Partition**.

The **Find and List Intercom Partitions** window appears.

Step 2 Click **Add New**.

An **Add New Intercom Partition** window appears.

Step 3 Under the **Intercom Partition Information** section, in the **Name** box, enter the name and description of the intercom partition that you want to add.

Note To enter multiple partitions, use one line for each partition entry. You can enter up to 75 partitions; the names and descriptions can have up to a total of 1475 characters. The partition name cannot exceed 50 characters. Use a comma (,) to separate the partition name and description on each line. If a description is not entered, Unified Communications Manager uses the partition name as the description.

Step 4 Click **Save**.

Step 5 Locate the partition that you want to configure.
Intercom Partition Configuration window is displayed

Step 6 Configure the fields in the Intercom Partition Configuration field area. See the online help for more information about the fields and their configuration options.

Step 7 Click **Save**.

The **Intercom Partition Configuration** window appears.

Step 8 Enter the appropriate settings. For detailed information about the Intercom Partition Configuration parameters, see online help.

Step 9 Click **Save**.

Step 10 Click **Apply Config**.

Configure an Intercom Calling Search Space

Procedure

Step 1 In the menu bar, choose **Call Routing** > **Intercom** > **Intercom Calling Search Space**.

Step 2 Click the **Add New**.

Step 3 Configure the fields in the Intercom Calling Search Space field area. For more information on the fields and their configuration options, see Online Help.

Step 4 Click **Save**.

Configure an Intercom Directory Number

Procedure

Step 1 Choose **Call Routing** > **Intercom** > **Intercom Directory Number**.

The **Find and List Intercom Directory Numbers** window is displayed.

Step 2 To locate a specific intercom directory number, enter search criteria and click **Find.**
A list of intercom directory numbers that match the search criteria displayed.

Step 3 Perform one of the followings tasks:

a) To add an intercom directory number, click **Add New**.
b) To update an intercom directory number, click the intercom directory number to update.

The **Intercom Directory Number Configuration** window displayed.

Step 4 Configure the fields in the Intercom Directory Number Configuration field area. For more information on the fields and their configuration options, see Online Help.

Step 5 Click **Save**.

Step 6 Click **Apply Config**.

Step 7 Click **Reset Phone**.

Step 8 Restart devices.

During the restart, the system may drop calls on gateways.

Configure an Intercom Translation Pattern

Procedure

Step 1 Choose **Call Routing** > **Intercom** > **Intercom Translation Pattern**.

The **Find and List Intercom Translation Patterns** window appears.

Step 2 Perform one of the followings tasks:

a) To copy an existing intercom translation pattern, locate the partition to configure, click **Copy** eside the intercom translation pattern to copy.
b) To add a new intercom translation pattern, click the **Add New**.

Step 3 Configure the fields in the Intercom Translation Pattern Configuration field area. For more information on the fields and their configuration options, see Online Help.

Step 4 Click **Save**.

Ensure that the intercom translation pattern that uses the selected partition, route filter, and numbering plan combination is unique. if you receive an error that indicates duplicate entries, check the route pattern or hunt pilot, translation pattern, directory number, call park number, call pickup number, or meet-me number configuration windows.

The **Intercom Translation Pattern Configuration** window displays the newly configured intercom translation pattern.

What to do next

Refer to the Manager Assistant Task Flow for Shared Lines, on page 134 to determine the next task to complete.

Configure Multiple Manager Assistant Pool

Procedure

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

Step 2 From the **Server** drop-down list, choose the server on which the Cisco IP Manager Assistant service is active.

Step 3 From the **Service** drop-down list, choose the **Cisco IP Manager Assistant** service.
The **Service Parameter Configuration** window, which lists the parameters, is displayed.

Step 4 Click **Advanced**.
The advanced parameters for **Clusterwide Parameters (Parameters that apply to all servers)** are displayed.

Step 5 Configure the following parameters to add multiple manager assistant pools in **Clusterwide Parameters (Parameters that apply to all servers)**:

a) **Enable Multiple Active Mode**—The default is False. When this parameter is set to True, the administrator can configure up to 7000 managers and assistants by using multiple pools.

b) **Pool 2: Cisco IPMA Server (Primary) IP Address**—No default. The administrator must manually enter this IP address. Administrator can assign up to 2500 managers and assistants to this address.

c) **Pool 2: Cisco IPMA Server (Backup) IP Address**—No default. The administrator must manually enter this IP address.

d) **Pool 3: Cisco IPMA Server (Primary) IP Address**—No default. The administrator must manually enter this IP address and can assign up to 2500 managers and assistants to this address.

e) **Pool 3: Cisco IPMA Server (Backup) IP Address**—No default. The administrator must manually enter this IP address.

click ? for detailed descriptions.

Step 6 Click **Save**.

What to do next

Refer to the Manager Assistant Task Flow for Shared Lines, on page 134 to determine the next task to complete.

Configure Secure TLS Connection to CTI for Manager Assistant

Manager Assistant uses WDSecureSysUser application user credentials to establish a secure TLS connection to CTI to make calls.

To configure the WDSecureSysUser application user to establish a secure TLS connection, complete the following tasks.

Before you begin

- Install and configure the Cisco CTL Client.

  For more information about CTL Client, see Security Guide for Cisco Unified Communications Manager.

- Verify that the **Cluster Security Mode** in the **Enterprise Parameters Configuration** window is **1** (mixed mode). Operating the system in mixed mode impacts other security functions in your system. If your system is not currently running in mixed mode, do not switch to mixed mode until you understand these interactions. For more information, see Security Guide for Cisco Unified Communications Manager.
-
- Activate the Cisco Certificate Authority Proxy Function (CAPF) service on the first node.

Procedure

	Command or Action	Purpose
Step 1	Configure IPMASecureSysUser Application User, on page 141	Configure IPMASecureSysUser Application User.
Step 2	Configure CAPF Profile, on page 141	Configure Certificate Authority Proxy Function (CAPF) Profile for the IPMASecureSysUser Application User.
Step 3	Configure Cisco IP Manager Assistant, on page 143	Configure service parameters for the Cisco IP Manager Assistant service.

Configure IPMASecureSysUser Application User

Use this procedure to configure IPMASecureSysUser application user.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **Application User**.

Step 2 Click **Find**.

Step 3 From the **Find and List Application Users Application** window, choose **WDSecureSysUser**.

Step 4 Configure the fields in the **Application User Configuration** window and click **Save**.

Configure CAPF Profile

Certificate Authority Proxy Function (CAPF) is a component that performs tasks to issue and authenticate security certificates. When you create an application user CAPF profile, the profile uses the configuration details to open secure connections for the application.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **Application User CAPF Profile**.

Step 2 Perform one of the following tasks:

- Click **Add New** in the **Find** window, to add a new CAPF profile.
- Click **Copy** for that record in the **Copy** column, to copy an existing profile, and locate the appropriate profile.

To update an existing entry, locate and display the appropriate profile.

Step 3 Configure or update the relevant CAPF profile fields. See the Related Topics section information about the fields and their configuration options.

Step 4 Click **Save**.

Step 5 Repeat the procedure for each application and end user that you want to use security.

CAPF Profile Settings

Setting	Description
Application User	From the drop-down list, choose the application user for the CAPF operation. This setting displays configured application users. This setting does not appear in the **End User CAPF Profile** window.
End User ID	From the drop-down list, choose the end user for the CAPF operation. This setting displays configured end users. This setting does not appear in the **Application User CAPF Profile** window.
Instance ID	Enter 1 to 128 alphanumeric characters (a-z, A-Z, 0-9). The Instance ID identifies the user for the certificate operation. You can configure multiple connections (instances) of an application. To secure the connection between the application and CTIManager, ensure that each instance that runs on the application PC (for end users) or server (for application users) has a unique certificate. This field relates to the CAPF Profile Instance ID for Secure Connection to CTIManager service parameter that supports web services and applications.
Certificate Operation	From the drop-down list, choose one of the following options: • **No Pending Operation**—This message is displayed when no certificate operation is occurring. (default setting) • **Install/Upgrade**—This option installs a new certificate or upgrades an existing locally significant certificate for the application.
Authentication Mode	The authentication mode for the Install/Upgrade certificate operation specifies By Authentication String, which means CAPF installs, upgrades, or troubleshoots a locally significant certificate only when the user or administrator enters the CAPF authentication string in the **JTAPI/TSP Preferences** window.

Setting	Description
Authentication String	To create your own authentication string, enter a unique string. Each string must contain 4 to 10 digits. To install or upgrade a locally significant certificate, the administrator must enter the authentication string in the JTAPI/TSP preferences GUI on the application PC. This string supports one-time use only; after you use the string for the instance, you cannot use it again.
Generate String	To automatically generate an authentication string, click this button. The 4-to10-digit authentication string appears in the **Authentication String** field.
Key Size (bits)	From the drop-down list, choose the key size for the certificate. The default setting is 1024. The other option for key size is 512. Key generation, which is set at low priority, allows the application to function while the action occurs. Key generation may take up to 30 or more minutes.
Operation Completes by	This field, which supports all certificate operations, specifies the date and time by which you must complete the operation. The values that are displayed apply for the first node. Use this setting with the **CAPF Operation Expires in (days)** enterprise parameter, which specifies the default number of days in which the certificate operation must be completed. You can update this parameter at any time.
Certificate Operation Status	This field displays the progress of the certificate operation, such as pending, failed, or successful. You cannot change the information that is displayed in this field.

Configure Cisco IP Manager Assistant

Procedure

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

Step 2 From the **Server** drop-down list, choose the server on which the Cisco IP Manager Assistantservice is active.

Step 3 From the **Service** drop-down list, choose the **Cisco IP Manager Assistant** service.
A list of parameters appears.

Step 4 Navigate to and update the CTIManager Connection Security Flag and CAPF Profile Instance ID for Secure Connection to CTIManager parameters.

To view parameter descriptions, click the parameter name link.

Step 5 Click **Save**.

Step 6 Repeat the procedure on each server on which the service is active.

What to do next

Refer to the Manager Assistant Task Flow for Shared Lines, on page 134 to determine the next task to complete.

Configure CTI Route Point

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **CTI Route Point**.

Step 2 Click **Add New**.
The **CTI Route Point Configuration** window is displayed.

Step 3 In the **Device Name** field, enter the device name.

Step 4 From the **Device Pool** drop-down list, choose **Default**.

Step 5 From the **Calling Search Space** drop-down list, choose **Generated_CSS_M_E**.

Step 6 Check the **Use Device Pool Calling Party Transformation CSS** check box.

Step 7 Click **Save**.
`Add successful` status message is displayed.

Step 8 From the Association area, click **Line [1] - Add a new DN**.
The **Directory Number Configuration** window is displayed.

Step 9 Enter a directory number in the **Directory Number** field.

Step 10 From the **Route Partition** drop-down list, choose **Generated_Route_Point**.

Step 11 Click **Save**.

Configure IP Phone Services for Manager and Assistant

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Phone Services**.

Step 2 Click **Add New**.
The **IP Phone Services Configuration** window is displayed.

Step 3 For each supported phone for managers and assistants, enter the required fields and click **Save**. See Cisco IP Phone Services Configuration Fields, on page 144 for more information about the fields and their configuration options.
The `Update successful` message is displayed.

Cisco IP Phone Services Configuration Fields

Field	Description
Service Information	

Field	Description
Service Name	Enter the name of the service. If the service is not marked as an enterprise subscription, the service name will display in areas where you can subscribe to a service, for example, under Cisco Unified Communications Self Care Portal. Enter up to 128 characters for the service name. For Java MIDlet services, the service name must exactly match the name that is defined in the Java Application Descriptor (JAD) file. **Note** Unified Communications Manager allows you to create two or more IP phone services with identical names. Cisco recommends that you do not do so unless most or all phone users are advanced, or unless an administrator always configures the IP phone services. Be aware that if AXL or any third-party tool accesses the list of IP phone services for configuration, you must use unique names for IP phone services. **Note** When the service URL points to an external customized URL, you cannot localize the service name according to the device locale of the phone. The service name gets displayed in English alphabets only.
ASCII Service Name	Enter the name of the service to display if the phone cannot display Unicode.
Service Description	Enter a description of the content that the service provides. The description can include up to 50 characters in any language, but it cannot include double quotation marks (") or single quotation marks ('). Service URL	Enter the URL of the server where the IP phone services application is located. Make sure that this server remains independent of the servers in your Unified Communications Manager cluster. Do not specify a Unified Communications Manager server or any server that is associated with Unified Communications Manager (such as a TFTP server or directory database publisher server). For the services to be available, the phones in the Unified Communications Manager cluster must have network connectivity to the server. For Cisco-signed Java MIDlets, enter the location where the JAD file can be downloaded; for example, a web server or the back-end application server to which the Java MIDlet communicates. For Cisco-provided default services, the service URL is displayed as `Application:Cisco/<name of service>` by default; for example, `Application:Cisco/CorporateDirectory`. If you modify the service URL for Cisco-provided default services, verify that you configured both for the **Service Provisioning** setting, which displays in the **Phone**, **Enterprise Parameter**, and **Common Phone Profile Configuration** windows. For example, you use a custom corporate directory, so you change `Application:Cisco/CorporateDirectory` to the external service URL for your custom directory; in this case, change the **Service Provisioning** value to **Both**.

Field	Description
Secure-Service URL	Enter the secure URL of the server where the Cisco Unified IP Phone services application is located. Make sure that this server remains independent of the servers in your Unified Communications Manager cluster. Do not specify a Unified Communications Manager server or any server that is associated with Unified Communications Manager (such as a TFTP server or publisher database server). For the services to be available, the phones in the Unified Communications Manager cluster must have network connectivity to the server. **Note** If you do not provide a Secure-Service URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities.
Service Category	Choose a service application type (XML or Java MIDlet). If you choose Java MIDlet, when the phone receives the updated configuration file, the phone retrieves the Cisco-signed MIDlet application (JAD and JAR) from the specified Service URL and installs the application.
Service Type	Choose whether the service is provisioned to the Services, Directories, or Messages button or option on the phone; that is, if the phone has these buttons or options. To determine whether your phone supports these buttons or options, see the *Cisco Unified IP Phone Administration Guide* that supports your phone model.
Service Vendor	Allows you to specify the vendor or manufacturer for the service. This field is optional for XML applications, but it is required for Cisco-signed Java MIDlets. For Cisco-signed Java MIDlets, the value that you enter in this field must exactly match the vendor that is defined in the MIDlet JAD file. This field displays as blank for Cisco-provided default services. You can enter up to 64 characters.

Field	Description
Service Version	Enter the version number for the application. For XML applications, this field is optional and is informational only. For Cisco-signed Java MIDlets, consider the following information: • If you enter a version, the service version must exactly match the version that is defined in the JAD file. If you enter a version, the phone attempts to upgrade or downgrade the MIDlet if the version is different than what is installed on the phone. • If the field is blank, the version gets retrieved from the **Service URL**. Leaving the field blank ensures that the phone attempts to download the JAD file every time that the phone reregisters to Unified Communications Manager as well as every time that the Cisco-signed Java MIDlet is launched; this ensures that the phone always runs the latest version of the Cisco-signed Java MIDlet without you having to manually update the **Service Version** field. This field displays as blank for Cisco-provided default services. You can enter numbers and periods in this field (up to 16 ASCII characters).
Enable	Allows you to enable or disable the service without removing the configuration from Cisco Unified CM Administration (and without removing the service from the database). Uncheck the check box to remove the service from the phone configuration file and the phone.
Service Parameter Information	
Parameters	Lists the service parameters that apply to this IP phone service. Use the following buttons to configure service parameters for this pane: • **New Parameter**—Click this button to display the **Configure Cisco Unified IP Phone Service Parameter** window, where you configure a new service parameter for this IP phone service. • **Edit Parameter**—Highlight a service parameter that is displayed in the **Parameters** pane, then click this button to display the **Configure Cisco Unified IP Phone Service Parameter** window, where you can edit the selected service parameter for this IP phone service. • **Delete Parameter**—Highlight a service parameter that is displayed in the **Parameters** pane, then click this button to delete a service parameter for this IP phone service. A popup window asks you to confirm deletion.

Configure Phone Button Templates for Manager, Assistant, and Everyone

The procedures in this section describe how to configure phone button for manager and assistant.

Procedure

	Command or Action	Purpose
Step 1	Configure a Phone Button Template for Manager Assistant, on page 148	Perform this step to assign manage and assistant button features to line or speed dial keys.
Step 2	Associate a Manager Assistant Button Template with a Phone, on page 148	Perform this step to configure the manager and assistant button for a phone.

Configure a Phone Button Template for Manager Assistant

Use this procedure to configure a phone button template for the Manager Assistant feature.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Phone Button Template**.

Step 2 Click **Find** to display list of supported phone templates.

Step 3 Perform the following steps if you want to create a new phone button template; otherwise, proceed to the next step.

a) Select a default template for the model of phone and click **Copy**.
b) In the **Phone Button Template Information** field, enter a new name for the template.
c) Click **Save**.

Step 4 Perform the following steps if you want to add phone buttons to an existing template.

a) Click **Find** and enter the search criteria.
b) Choose an existing template.

Step 5 From the **Line** drop-down list, choose feature that you want to add to the template.

Step 6 Click **Save**.

Step 7 Perform one of the following tasks:

- Click **Apply Config** if you modified a template that is already associated with devices to restart the devices.
- If you created a new softkey template, associate the template with the devices and then restart them.

Associate a Manager Assistant Button Template with a Phone

Before you begin

Configure a Phone Button Template for Manager Assistant, on page 148

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** to display the list of configured phones.

Step 3 Choose the phone to which you want to add the phone button template.

Step 4 In the **Phone Button Template** drop-down list, choose the phone button template that contains the new feature button.

Step 5 Click **Save**.
A dialog box is displayed with a message to press **Reset** to update the phone settings.

Configure Manager and Assign Assistant for Shared Line Mode

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **End User**.

Step 2 Click **Find**.
The search result displays all the end users that are configured in Unified Communications Manager.

Step 3 From the **Related Links** drop-down list, choose **Manager Configuration** and click **Go**.

Step 4 Check the **Automatic Configuration** check box to automatically configure the softkey template and Auto Answer with Speakerphone for intercom line for the manager phone based on the Cisco IP Manager Assistant service parameters.

Note **Automatic Configuration** for intercom applies only when the Unified Communications Manager Assistant intercom feature is used for the Cisco Unified IP Phones 7940 and 7960.

Step 5 Check **Uses Shared Lines** check box.

Step 6 From the **Device Name/Profile** drop-down list, choose the device name or device profile to associate a device name or device profile with a manager.

Note If the manager telecommutes, check the **Mobile Manager** check box and optionally choose a device profile from the **Device Name/Profile** drop-down list. When device profile is chosen, the manager must log in to the phone by using Cisco Extension Mobility before accessing Manager Assistant.

See the related topics for more information about Extension Mobility with Manager Assistant.

Step 7 From the **Intercom Line** drop-down list, choose the intercom line appearance for the manager, if applicable. The chosen intercom line applies to the Manager Assistant and Unified Communications Manager intercom features.

Step 8 From the **Assistant Pool** drop-down list, choose the appropriate pool number (1 to 3).

Step 9 Choose the name of the assistant from the Available Assistants selection box and move it to the Associated Assistants selection box by clicking the down arrow to assign an assistant to the manager.

You can go to the **Assistant Configuration** window by highlighting the assistant name and clicking the **View Details** link.

Step 10 Choose the appropriate line from the Available Lines list box and move it to the Selected Lines list box by clicking the down arrow to configure the Manager Assistant controlled lines.
Make sure that the controlled line is always the shared line DN.

Step 11 Click **Save**.
If you checked the **Automatic Configuration** check box and the service parameters are invalid, a message is displayed. Ensure that the service parameters are valid. After successful completion of the automatic

configuration, the manager device resets. If you configured a device profile, the manager must log out and log in to the device for the changes to take effect.

Configure Assistant Line Appearances for Shared Line

Administrators can set up one or more lines with a shared line appearance. The Unified Communications Manager system considers a directory number to be a shared line if it appears on more than one device in the same partition.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **End User**.

Step 2 Click **Find**.
The search result displays all the end users that are configured in Unified Communications Manager.

Step 3 Click on the username to display user information for the chosen assistant.
The **End User Configuration** window is displayed.

Step 4 From the **Related Links** drop-down list, choose **Assistant Configuration** and click **Go**.
The **Assistant Configuration** window is displayed. The system automatically sets the softkey template and intercom line on the basis of the Cisco IP Manager Assistant service parameter settings when you check the **Automatic Configuration** check box. In addition, the system also sets Auto Answer with Speakerphone for intercom line.

Step 5 From the **Device Name** drop-down list, choose the device name to associate with the assistant.

Step 6 From the **Intercom Line** drop-down list, choose the incoming intercom line appearance for the assistant.

Step 7 From the **Primary Line** drop-down list, choose the primary line for the assistant.

a) To view existing manager configuration information, highlight the manager name in the **Associated Managers** list and click **View Details**.
The **Manager Configuration** window is displayed.

b) To return to the **Assistant Configuration** window, highlight the assistant name and click **View Details** link in the **Manager Configuration** window.

In the **Associated Manager** selection list box, the name of the previously configured manager is displayed.

Step 8 To associate the manager line to the assistant line, perform the following steps from the Manager Association to Assistant Line selection box:

a) From the **Available Lines** drop-down list, choose the assistant line that will be associated with the manager line.

b) From the **Manager Names** drop-down list, choose the preconfigured manager name for whom this proxy line will apply.

c) From the **Manager Lines** drop-down list, choose the manager line for which this proxy line will apply.

Step 9 Click **Save**.
The update takes effect immediately. If you chose **Automatic Configuration**, the assistant device automatically resets.

Install Assistant Console Plugin

Procedure

Step 1 From Cisco Unified CM Administration, choose **Application** > **Plugins**.
The **Find and List Plugins** window is displayed.

Step 2 Click **Find**.
A list of installable application plug-ins is displayed.

Step 3 Click on the **Download** link for Cisco Unified CM Assistant Console and save the executable to a location.

Step 4 Run the executable file.

Note If you install the application on a Windows Vista PC, a security window may be displayed. Allow the installation to continue.

The **Cisco Unified CallManager Assistant Console** installation wizard is displayed.

Step 5 In the **Introduction** window, click **Next**.

Step 6 In the **License Agreement** window, click **Next**.

Step 7 Choose a location where you want the application to install and click **Next**.

Note By default, the application installs in `C:\Program Files\Cisco\ Unified CallManager Assistant Console`.

Step 8 In the **Pre-installation Summary** window, review the summary and click **Install**.
The installation begins.

Step 9 After the installation is complete, click **Finish**.

Step 10 Provide the assistant the username and password that is required to log in to the console.

Step 11 To launch the Assistant Console, click the desktop icon or choose **Cisco Unified Communications Manager Assistant** > **Assistant Console** from the **Start...Programs** menu.

Step 12 The **Advanced** tab in the **Cisco Unified Communications Manager Assistant Settings** window allows you to enable trace for the Assistant Console.

Step 13 Provide the assistant with the port number and the IP address or hostname of the Unified Communications Manager server on which the Cisco IP Manager Assistant service is active. The first time that the assistant logs in to the console, the assistant must enter the information in the **Cisco Unified Communications Manager Assistant Server Port** and the **Cisco Unified Communications Manager Assistant Server Hostname or IP Address** fields.

Manager Assistant Interactions and Restrictions

Manager Assistant Interactions

Feature	Interaction
Bulk Administration Tool	You can use the Bulk Administration Tool to add many users (managers and assistants) at once instead of adding users individually. The Bulk Administration Tool templates that the **Cisco Unified CM Assistant Configuration Wizard** creates for Cisco Unified IP Phones support only the Unified Communications Manager intercom lines. For more information, see the Bulk Administration Guide for Cisco Unified Communications Manager.
Calling Party Normalization	Manager Assistant automatically supports localized and globalized calls if you configure the Calling Party Normalization feature. Manager Assistant can display localized calling party numbers on the user interfaces. In addition, for an incoming call to the manager, Manager Assistant can display localized and globalized calling party numbers when filter pattern matching occurs.
Extension Mobility	You can simultaneously use Manager Assistant with the Cisco Extension Mobility feature. When you log in to the Cisco Unified IP Phone using Extension Mobility, the Cisco IP Manager Assistant service is automatically enabled on that phone. You can then access the Manager Assistant features. For more information about Cisco Extension Mobility, see Extension Mobility Overview, on page 381.
Internet Protocol Version 6 (IPv6)	Manager Assistant does not support IPv6, so you cannot use phones with an IP Addressing Mode of IPv6 Only with Manager Assistant. To use Manager Assistant with the phone, ensure that you configure the phone with an IP Addressing Mode of IPv4 Only or IPv4 and IPv6.

Feature	Interaction
Reporting tools	Manager Assistant provides statistical information in the CDR Analysis and Reporting (CAR) tool and provides a summary of changes to configurations in a change log. The administrator can view a summary of changes that are made to the Manager or Assistant Configurations in Unified CM AssistantChangeLog*.txt. A manager can change defaults by accessing the Manager Configuration from a URL. An assistant can change the manager defaults from the Assistant Console. For information about the URL and Manager Configuration, see the *Cisco Unified Communications Manager Assistant User Guide*. When the manager or assistant makes changes, the changes are sent to a log file called **ipma_changeLogxxx.log**. The log file resides on the server that runs the Cisco IP Manager Assistant service. Use the following command to obtain the log file: **file get activelog tomcat/logs/ipma/log4j/** For more information about downloading the log file, see the *Cisco Unified Real -Time Monitoring Tool Administration Guide*.
CDR Analysis and Reporting	Manager Assistant supports call-completion statistics and inventory reporting for managers and assistants. The CAR tool supports call-completion statistics. Cisco Unified Serviceability supports inventory reporting. For more information, see the following guides: • *Cisco Unified Serviceability Administration Guide* • Call Reporting and Billing Administration Guide for Cisco Unified Communications Manager
Multilevel Precedence and Preemption (MLPP)	The following points describe the interactions between Manager Assistant with shared line support and MLPP: • The system preserves call precedence in the handling of calls by Manager Assistant. For example, when an assistant diverts a call, the system preserves the precedence of the call. • Filtering of precedence calls occurs in the same manner as all other calls. The precedence of a call will not affect whether a call is filtered. • Because Manager Assistant does not have information about the precedence of a call, it does not provide any additional indication of the precedence of a call on the Assistant Console.

Feature	Interaction
Intercom	Manager Assistant supports the following two types of intercom: • Manager Assistant intercom (used with Cisco Unified IP Phones 7940 and 7960). You can configure this intercom feature using the DN configuration and end user (manager and assistant) configuration windows. • Unified Communications Manager intercom (used with Cisco Unified IP Phones 7940 and 7960). You can configure this intercom feature using the intercom partition, intercom calling search space, intercom directory number, intercom translation pattern, DN, and end user (manager and assistant) configuration windows.
Message Waiting Indicator	The Message Waiting Indicator feature interacts with proxy line support only. The Message Waiting Indicator (MWI) on and off numbers should have the partition of the manager line in their calling search space. The partition can exist in any order of priority within each calling search space.
Time-of-Day Routing	The Time-of-Day feature interacts with proxy line support only. Time-of-Day routing routes calls to different locations based on the time that the call gets made; for example, during business hours, calls get routed to a manager office, and after hours, the calls go directly to voicemail service. For more information about Time-of-Day Routing, see the System Configuration Guide for Cisco Unified Communications Manager.

Manager Assistant Restrictions

Feature	Restriction
Assistant Console Application	To install the Assistant Console application on a computer with Microsoft Internet Explorer 7 (or later), install the Microsoft Java Virtual Machine (JVM) before the Assistant Console installation.
Call Management features	The Assistant Console does not support hunt groups or queues, recording and monitoring, one-touch Call Pickup, and On-Hook transfer (the ability to transfer a call by pressing the Transfer softkey and going on hook to complete the transfer).

Feature	Restriction
Cisco IP Phones	Manager Assistant supports SIP on Cisco Unified IP Phones 7900 Series, except for Cisco Unified IP Phones 7940 and 7960. Manager Assistant supports up to 3500 managers and 3500 assistants by configuring multiple Cisco IP Manager Assistant servers (pools). When you enable multiple pools, the manager and all configured assistants for that manager should belong to the same pool. Cisco Unified IP Phones 7960 and 7940 support only the Unified Communications Manager Assistant Intercom lines feature. Cisco Unified IP Phones 7900 (except 7940 and 7960) support only the Unified Communications Manager Intercom feature. One manager can have up to ten assigned assistants and one assistant can support up to 33 managers (if each manager has one Unified Communications Manager–controlled line). Only one assistant at a time can assist a manager. Manager Assistant supports up to 3500 managers and 3500 assistants per Unified Communications Manager cluster.
Intercom	After an upgrade, Manager Assistant users that use the incoming intercom line do not get upgraded automatically to the Unified Communications Manager Intercom feature. The system does not support calls between the Unified Communications Manager Intercom feature and regular lines (which may be configured as Manager Assistant Intercom lines).
Single Sign-On	Manager Assistant is not supported in the Single Sign-On environment.
Speed Dial	Cisco Unified IP Phones 7940, 7942, and 7945 support only two lines or speed-dial buttons.

Cisco Unified Communications Manager Assistant Troubleshooting

This section describes the troubleshooting tools for Manager Assistant and the client desktop, and troubleshooting information for Manager Assistant.

Tool Description	Location
Cisco Unified CM Assistant server trace files	The trace files reside on the server that runs the Cisco IP Manager Assistant service. You can download these files from the server using one of the following methods: • Use the CLI command **file get activelog tomcat/logs/ipma/log4j**. • Use the trace collection features in the Cisco Unified Real-Time Monitoring Tool (RTMT). For more information, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. You can enable debug tracing by choosing **Cisco Unified Serviceability** > **Trace** > **Configuration**.
Cisco IPMA client trace files	**$INSTALL_DIR\logs\ACLog*.txt** on the client desktop, in the same location where the Unified CM Assistant assistant console resides. To enable debug tracing, go to the **Settings** dialog box in the Assistant Console. In the **Advanced** panel, check the **Enable Trace** check box. **Note** This check box enables only debug tracing. Error tracing always remains On.
Cisco IPMA client install trace files	**$INSTALL_DIR\InstallLog.txt** on the client desktop, in the same location where the Assistant Console resides.
Cisco IPMA Client AutoUpdater trace files	**$INSTALL_DIR\UpdatedLog.txt** on the client desktop, in the same location where the Unified CM Assistant Console resides.
Install directory	By default—`C:\Program Files\Cisco\Unified Communications Manager Assistant Console\`

Calling Party Gets Reorder Tone

Problem

Calling party gets a reorder tone or a message:

```
This call cannot be completed as dialed.
```

Possible Cause

The calling search space of the calling line may not be configured correctly.

Solution

Check the calling search space of the line. For more information about configuration, see the System Configuration Guide for Cisco Unified Communications Manager.

You can also use the Cisco Dialed Number Analyzer service to check for flaws in the calling search space. For more information, see the *Cisco Unified Communications Manager Dialed Number Analyzer Guide*.

Calls Do Not Get Routed When Filtering Is On or Off

Problem

Calls are not routed properly.

Possible Cause 1

Cisco CTI Manager service may have stopped.

Solution 1

Restart the Cisco CTI Manager and Cisco IP Manager Assistant services from **Cisco Unified Serviceability** > **Tools** > **Control Center—Feature Services**.

Possible Cause 2

The Unified Communications Manager Assistant route point was not configured properly.

Solution 2

Use wildcards to match the directory number of the Unified Communications Manager Assistant CTI route point and the primary directory numbers of all managers that are configured for Unified Communications Manager Assistant.

Possible Cause 3

The status window on the manager phone displays the message `Filtering Down`. This message can indicate that Unified Communications Manager Assistant CTI route point may be deleted or may not be in service.

Solution 3

Use the following procedure to configure the CTI route point and restart the Cisco IP Manager Assistant service:

1. From Cisco Unified CM Administration, choose **Device** > **CTI Route Point**.
2. Find the route point, or add a new route point. For more information about configuration, see the System Configuration Guide for Cisco Unified Communications Manager.
3. Restart the Cisco CTI Manager and Cisco IP Manager Assistant services from **Cisco Unified Serviceability** > **Tools** > **Control Center—Feature Services**.

Cisco IP Manager Assistant Service Unreachable

Problem

After you open the Assistant Console, the following message is displayed:

```
Cisco IPMA Service Unreachable
```

Possible Cause 1

Cisco IP Manager Assistant service may have stopped.

Solution 1

Restart the Unified Communications Manager Assistant from **Cisco Unified Serviceability** > **Tools** > **Control Center—Feature Services**.

Possible Cause 2

The server address for the primary and secondary Unified Communications Manager Assistant servers may be configured as DNS names, but the DNS names are not configured in the DNS server.

Solution 2

Use the following procedure to replace the DNS name.

1. From Cisco Unified CM Administration, choose **System** > **Server**.
2. Replace the DNS name of the server with the corresponding IP address.
3. Restart the Unified Communications Manager Assistant from **Cisco Unified Serviceability** > **Tools** > **Control Center—Feature Services**.

Possible Cause 3

The Cisco CTI Manager service may have stopped.

Solution 3

Restart the Unified Communications Manager Assistant from **Cisco Unified Serviceability** > **Tools** > **Control Center—Feature Services**.

Possible Cause 4

The Unified Communications Manager Assistant service might be configured to open a CTI connection in secure mode, but the security configuration may not be complete.

If this scenario occurs, the following message is displayed in the alarm viewer or in the Unified Communications Manager Assistant service logs:

```
IPMA Service cannot initialize - Could not get Provider.
```

Solution 4

Check the security configuration in the service parameters of Cisco IP Manager Assistant service.

Restart the Unified Communications Manager Assistant from **Cisco Unified Serviceability** > **Tools** > **Control Center—Feature Services**.

Cannot Initialize Cisco IP Manager Assistant Service

Problem

The Cisco IP Manager Assistant service cannot open a connection to CTI Manager, and the following message is displayed:

```
IPMA Service cannot initialize - Could not get Provider
```

Possible Cause

The Cisco IP Manager Assistant service cannot open a connection to CTIManager. You can see the message in the alarm viewer or in the Unified CM Assistant service logs.

Solution

Restart the Cisco CTI Manager and Cisco IP Manager Assistant services from **Cisco Unified Serviceability** > **Tools** > **Control Center—Feature Services**.

Assistant Console Installation from Web Fails

Problem

Assistant Console installation from the web fails. The following message is displayed:

```
Exception: java.lang.ClassNotFoundException: InstallerApplet.class
```

Possible Cause

Using the Sun Java plug-in virtual machine instead of the Microsoft JVM with the standard Unified Communications Manager Assistant Console install causes failures.

Solution

The administrator directs the user to the following URL, which is a JSP page that supports the Sun Java plug-in:

```
https://<servername>:8443/ma/Install/IPMAConsoleInstallJar.jsp
```

HTTP Status 503—This Application Is Not Currently Available

Problem

http://<server-name>:8443/ma/Install/IPMAConsoleInstall.jsp displays the following error message:

```
HTTP Status 503—This application is not currently available
```

Possible Cause

Cisco IP Manager Assistant service has not been activated or is not running.

Solution

Ensure that the Cisco IP Manager Assistant service has been activated by checking the activation status of the service from **Cisco Unified Serviceability** > **Tools** > **Service Activation**.

If the Cisco IP Manager Assistant service has already been activated, restart the Unified Communications Manager Assistant from **Cisco Unified Serviceability** > **Tools** > **Control Center—Feature Services**.

Manager Is Logged Out While the Service Is Still Running

Problem

Although the manager is logged out of Unified Communications Manager Assistant, the service still runs. The display on the manager IP phone disappears. Calls do not get routed, although filtering is On. To verify that the manager is logged out, view the application log using the Cisco Unified Real-Time Monitoring Tool. Look for a warning from the Cisco Java Applications that indicates that the Cisco IP Manager Assistant service logged out.

Possible Cause

The manager pressed the softkeys more than four times per second (maximum limit allowed).

Solution

The Unified Communications Manager administrator must update the manager configuration. Perform the following procedure to correct the problem:

1. From Cisco Unified CM Administration, choose **User Management** > **End User**.

   The **Find and List Users** window is displayed.
2. Enter the manager name in the search field and click **Find**.
3. From the search results list, choose the manager that you want to update.

   The **End User Configuration** window is displayed.
4. From the **Related Links** drop-down list, choose **Cisco IPMA Manager** and click **Go**.
5. Make the necessary changes to the manager configuration and click **Update**.

Manager Cannot Intercept Calls That Are Ringing on the Assistant Proxy Line

Problem

The manager cannot intercept the calls that are ringing on the assistant proxy line.

Possible Cause

The calling search space of the proxy line is not configured properly.

Solution

Check the calling search space of the proxy line for the assistant phone. Perform the following procedure to correct the problem:

1. From Cisco Unified CM Administration, choose **Device** > **Phone**.

   The **Find and List Phones** search window is displayed.

2. Click the assistant phone.

   The **Phone Configuration** window is displayed.

3. Verify the calling search space configuration for the phone and for the directory number (line) and update as appropriate.

No Page Found Error

Problem

`http://<server-name>:8443/ma/Install/IPMAConsoleInstall.jsp` displays the following error message:

```
No Page Found Error
```

Possible Cause 1

Network problems.

Solution 1

Ensure that the client has connectivity to the server. Ping the server name that is specified in the URL and verify that it is reachable.

Possible Cause 2

Misspelled URL.

Solution 2

Because URLs are case sensitive, ensure that the URL matches exactly with the URL in the instructions.

System Error - Contact System Administrator

Problem

After you open the Assistant Console, the following message is displayed:

```
System Error - Contact System Administrator
```

Possible Cause 1

You may have upgraded the Unified Communications Manager. The system does not upgrade the Assistant Console automatically when you upgrade the Unified Communications Manager.

Solution 1

Uninstall the console by choosing `Start > Programs > Cisco Unified Communications Manager Assistant > Uninstall Assistant Console` and reinstall the console from URL **https://<server-name>:8443/ma/Install/IPMAConsoleInstall.jsp**.

Possible Cause 2

The user is not configured correctly in the database.

Solution 2

Ensure that the user ID and the password are run as a Unified Communications Manager user through Cisco Unified CM Administration.

Possible Cause 3

When you deleted a manager from an assistant, Cisco Unified CM Administration left a blank line for the assistant.

Solution 3

From the **Assistant Configuration** window, reassign the proxy lines.

Unable to Call Manager When Cisco IP Manager Assistant Service is Down

Problem

Calls do not get routed properly to managers when Cisco IP Manager Assistant service goes down.

Possible Cause

The Unified Communications Manager Assistant CTI route point does not have Call Forward No Answer enabled.

Solution

Perform the following procedure to properly configure the Unified Communications Manager Assistant route point.

1. From Cisco Unified CM Administration, choose **Device** > **CTI Route Point**.

   The **Find and List CTI Route Point** search window is displayed.

2. Click **Find**.

   A list of configured CTI route points is displayed.

3. Choose the Unified Communications Manager Assistant CTI route point that you want to update.
4. In the **CTI Route Point Configuration** window, click the line to update from the **Association** area.
5. In the **Call Forward and Pickup Settings** section, check the **Forward No Answer Internal** and the **Forward No Answer External** check box and enter the CTI route point DN in the **Coverage/Destination** field (for example, CFNA as 1xxx for the route point DN 1xxx).

6. In the **Calling Search Space** drop-down list, choose **CSS-M-E** (or appropriate calling search space).
7. Click **Update**.

User Authentication Fails

Problem

User authentication fails when you sign in using the login window from the Assistant Console.

Possible Cause

The following probable causes can apply:

- Incorrect management of the user in the database
- Incorrect management of the user as an assistant or a manager

Solution

Ensure that the user ID and the password are ran as a Unified Communications Manager user through Cisco Unified CM Administration.

You must run the user as an assistant or a manager by associating the Unified Communications Manager Assistant user information, which you access through Cisco Unified CM Administration under **User Management** > **End User**.

PART VI

Voice Messaging Features

CHAPTER 13

Audible Message Waiting Indicator

Audible Message Waiting Indicator Overview

You can configure Audible Message Waiting Indicator (AMWI) to play a stutter dial tone on the Cisco Unified IP Phone to notify users of new voice messages. Users hear a stutter dial tone whenever the phone goes off hook on a line on which a voice message was left.

You can configure AMWI for all the phones in a cluster or for only certain directory numbers. The directory-number-level configuration takes precedence over the cluster-wide configuration.

Audible Message Waiting Indicator Prerequisites

You can configure AMWI only on Cisco Unified IP Phone that are running phone firmware Release 8.3(1) or later.

Audible Message Waiting Indicator Configuration Task Flow

Before you begin

- Review Audible Message Waiting Indicator Prerequisites, on page 167.

Procedure

	Command or Action	Purpose
Step 1	Generate a Phone Feature List, on page 3	Generate a report to identify devices that support the Audible Message Waiting Indicator feature.

	Command or Action	Purpose
Step 2	Configure Audible Message Waiting Indicator Service Parameters, on page 168	Configure AMWI default setting for all phones in a cluster.
Step 3	Configure Audible Message Waiting Indicator for a Directory Number, on page 168	Configure AMWI for a directory number that is associated to a device.
Step 4	Configure Audible Message Waiting Indicator for a SIP Profile, on page 169	Configure AMWI for SIP profiles. Perform this procedure to configure AMWI for SIP phones.

Configure Audible Message Waiting Indicator Service Parameters

This procedure describes how to configure AMWI default setting for all the phones in a cluster.

Before you begin

Generate a Phone Feature List, on page 3

Procedure

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

Step 2 From the **Server** drop-down list, choose the server that is running the Cisco CallManager service.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.

Step 4 In the **Clusterwide Parameters (Feature - General)** section, choose the **Audible Message Waiting Indication Policy** service parameter. This parameter determines whether the Audible Message Waiting Indicator is turned on of off for all the devices in the cluster.

Step 5 Click **Save**.

Configure Audible Message Waiting Indicator for a Directory Number

Follow these steps to configure AMWI for a directory number that is associated with a device.

Note The AMWI setting on an individual directory number overrides the clusterwide setting.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 In the **Association** section, click **Add a new DN**.
The **Directory Number Configuration** window appears.

Step 3 Select the **Audible Message Waiting Indicator Policy**. Choose one of the following options:

- **Off**

- **On**—When you select this option, the users will receive a stutter dial tone when the handset is off hook .
- **Default**—When you select this option, the phone uses the default that was set at the system level.

Step 4 Configure the remaining fields in the **Directory Number Configuration** window. See the online help for more information about the fields and their configuration options.

Step 5 Click **Save**.

Configure Audible Message Waiting Indicator for a SIP Profile

Follow these steps to configure Audible Message Waiting Indicator (AMWI) for a SIP profile.

Note The AMWI setting on an individual SIP profile overrides the clusterwide setting.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **SIP Profile**.
The **Find and List SIP Profiles** window appears.

Step 2 Enter the search criteria to use and click **Find**.
The window displays a list of SIP profiles that match the search criteria.

Step 3 Click the SIP profile that you want to update.
The **SIP Profile Configuration** window appears.

Step 4 Check the **Stutter Message Waiting** check box to activate stutter dial tone when the phone is off hook and a message is waiting.

Step 5 Click **Save**.

Step 6 Click **Apply Config**.

Audible Message Waiting Indicator Troubleshooting

Audible Message Waiting Indicator Is Not Heard on the Phone

Problem Phone does not play stutter dial tone to notify the user of new voice messages.

If the user uses an SCCP phone, check the following:

- Ensure that the phone firmware release is 8.3(1) or later.
- Check the AMWI setting for the phone and the line on which the user went off hook.
- Verify that the Cisco CallManager service is running on the server.

- Check the sniffer trace between the phone and Unified Communications Manager. Make sure that the phone receives the StartTone message with tone type equal to 42.

If the user uses a SIP phone, check the following:

- Ensure that the phone firmware release is 8.3(1) or later.
- Check the line (directory number) configuration. The phone must display the settings such as line1_msgWaitingAMWI : 1, line2_msgWaitingAMWI : 0.
- Ensure that the **Stutter Message Waiting** check box is checked in the **SIP Profile Configuration** window in Cisco Unified CM Administration.

Localized AMWI Tone Is Not Played in a Specific Locale

Problem The phone that is configured in a non-English locale does not play the localized tone.

Solution Check the following:

- From Cisco Unified CM Administration, verify the User Locale in the **Device Profile Configuration** window (**Device** > **Device Settings** > **Device Profile**).
- Make sure that the user resets the phone after changing the locale.
- Check `user/local/cm/tftp /<locale name> directory` and verify that the AMWI tone is defined in the localized g3-tones.xml file.

CHAPTER 14

Immediate Divert

Immediate Divert Overview

The Immediate Divert feature is a Unified Communications Manager supplementary service that allows you to immediately divert a call to a voicemail system. When Immediate Divert diverts a call, the line becomes available to make or receive new calls. Access the Immediate Divert feature by using the iDivert or Divert softkey on the IP phone.

Immediate Divert provides the following functions:

- Diverts a call to a voicemail system in the following manner:
  - Legacy iDivert diverts the call to the voice mailbox of the party that invokes the iDivert feature.
  - Enhanced iDivert diverts the call to either the voice mailbox of the party that invokes the iDivert feature or to the voice mailbox of the original called party.
- Diverts inbound calls that are in the Call Offering, Call on Hold, or Call Active states.
- Diverts outbound calls in the Call Active or Call on Hold states.

Note Although the Immediate Divert feature is not available to CTI applications, a CTI redirect operation exists that performs the same function as Immediate Divert. Application developers can use the CTI redirect operation to accomplish Immediate Divert.

Immediate Divert Prerequisites

- You must configure the voicemail profiles and hunt pilots.

For information on how to configure voicemail profiles and hunt pilots, see System Configuration Guide for Cisco Unified Communications Manager

- The following devices support Immediate Divert:
  - Voice-messaging systems such as Cisco Unity Connection that use the Skinny Client Control Protocol (SCCP).
  - QSIG devices (QSIG-enabled H.323 devices, MGCP PRI QSIG T1 gateways, and MGCP PRI QSIG E1 gateways), depending on the setting of the Use Legacy Immediate Divert and Allow QSIG During iDivert clusterwide service parameters.
  - The following table lists the phones that use the Divert or iDivert softkey.

Table 15: Cisco Unified IP Phones That Use Immediate Divert Softkeys

Cisco Unified IP Phone Model	Divert Softkey	iDivert Softkey	What to configure in softkey template
Cisco Unified IP Phone 6900 Series (except 6901 and 6911)	X		iDivert
Cisco Unified IP Phone 7900 Series		X	iDivert
Cisco Unified IP Phone 8900 Series	X		Configured by default
Cisco Unified IP Phone 9900 Series	X		Configured by default

Note Cisco Unified IP Phones 8900 and 9900 series have the Divert softkey assigned by default.

Immediate Divert Configuration Task Flow

Before you begin

- Review Immediate Divert Prerequisites, on page 171.

Procedure

	Command or Action	Purpose
Step 1	Configure Immediate Divert Service Parameters, on page 173	Configure the service parameters to enable Immediate Divert across various devices and applications.

	Command or Action	Purpose
Step 2	Configure a Softkey Template for Immediate Divert, on page 174	Create and configure a softkey template and add the iDivert softkey to that template.
Step 3	To Associate a Softkey Template with a Common Device Configuration, on page 175, complete the following subtasks: • Add a Softkey Template to the Common Device Configuration, on page 176 • Associate a Common Device Configuration with a Phone, on page 176	**Optional**. To make the softkey template available to phones, you must complete either this step or the following step. Follow this step if your system uses a **Common Device Configuration** to apply configuration options to phones. This is the most commonly used method for making a softkey template available to phones.
Step 4	Associate a Softkey Template with a Phone, on page 177	**Optional**. Use this procedure either as an alternative to associating the softkey template with the Common Device Configuration, or in conjunction with the Common Device Configuration. Use this procedure in conjunction with the Common Device Configuration if you need assign a softkey template that overrides the assignment in the Common Device Configuration or any other default softkey assignment.

Configure Immediate Divert Service Parameters

Procedure

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

Step 2 From the **Server** drop-down list, choose the server that is running the Cisco CallManager service.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.

Step 4 Configure the relevant service parameters and click **Save**.

Table 16: Service Parameter Fields for Immediate Divert

Field	Description
Call Park Display Timer	Enter a number from 0 to 100 (inclusive) to control the timer for the Immediate Divert text display on the IP phones. Set this timer for the server or for each server in a cluster that has the Cisco CallManager service and Immediate Divert configured. The default value for this service parameter is 10 seconds.

Field	Description
Use Legacy Immediate Divert	Select one of the following options from the drop-down list: • **True**—The user that invokes the iDivert feature can divert an incoming call only to his own voice mailbox. This is the default setting. • **False**—Immediate Divert allows diversion of an incoming call to either the voice mailbox of the original called party or to the voice mailbox of the user that invokes the iDivert feature.
Allow QSIG During iDivert	Select one of the following options from the drop-down list: • **True**—Immediate Divert diverts calls to voicemail systems that can be reached over QSIG, SIP, and QSIG-enabled H.323 devices. • **False**—Immediate Divert does not support access to voicemail systems over QSIG or SIP trunks. This is the default setting.
Immediate Divert User Response Timer	Enter a number from 5 to 30 (inclusive) to determine the time given to the iDivert softkey user to choose the party to whom to divert a call. If the user does not choose a party, the call remains connected. The default value for this service parameter is 5 seconds.

Configure a Softkey Template for Immediate Divert

To divert incoming calls or outgoing calls, configure a softkey template and assign the iDivert softkey to that template. You can configure the iDivert softkey in the following call states:

- Connected
- On hold
- Ring in

Immediate Divert supports the following call states:

- For incoming calls:
  - Call offering (shown as Ring In on the softkey template).
  - Call on hold
  - Call active
- For outgoing calls:
  - Call on hold
  - Call active

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Softkey Template**.

Step 2 Perform the following steps to create a new softkey template; otherwise, proceed to the next step.

a) Click **Add New**.
b) Select a default template and click **Copy**.
c) Enter a new name for the template in the **Softkey Template Name** field.
d) Click **Save**.

Step 3 Perform the following steps to add softkeys to an existing template.

a) Click **Find** and enter the search criteria.
b) Select the required existing template.

Step 4 Check the **Default Softkey Template** check box to designate this softkey template as the default softkey template.

Note If you designate a softkey template as the default softkey template, you cannot delete it unless you first remove the default designation.

Step 5 Choose **Configure Softkey Layout** from the **Related Links** drop-down list in the upper right corner and click **Go**.

Step 6 From the **Select a Call State to Configure** drop-down list, choose the call state for which you want the softkey to display.

Step 7 From the **Unselected Softkeys** list, choose the softkey to add and click the right arrow to move the softkey to the **Selected Softkeys** list. Use the up and down arrows to change the position of the new softkey.

Step 8 Repeat the previous step to display the softkey in additional call states.

Step 9 Click **Save**.

Step 10 Perform one of the following tasks:

- Click **Apply Config** if you modified a template that is already associated with devices to restart the devices.
- If you created a new softkey template, associate the template with the devices and then restart them. For more information, see *Add a Softkey Template to a Common Device Configuration* and *Associate a Softkey Template with a Phone* sections.

Associate a Softkey Template with a Common Device Configuration

Optional. There are two ways to associate a softkey template with a phone:

- Add the softkey template to the **Phone Configuration**.
- Add the softkey template to the **Common Device Configuration**.

The procedures in this section describe how to associate the softkey template with a **Common Device Configuration**. Follow these procedures if your system uses a **Common Device Configuration** to apply configuration options to phones. This is the most commonly used method for making a softkey template available to phones.

To use the alternative method, see Associate a Softkey Template with a Phone, on page 177

Procedure

	Command or Action	Purpose
Step 1	Add a Softkey Template to the Common Device Configuration, on page 176	
Step 2	Associate a Common Device Configuration with a Phone, on page 176	

Add a Softkey Template to the Common Device Configuration

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Common Device Configuration**.

Step 2 Perform the following steps to create a new Common Device Configuration and associate the softkey template with it; otherwise, proceed to the next step.

a) Click **Add New**.
b) Enter a name for the Common Device Configuration in the **Name** field.
c) Click **Save**.

Step 3 Perform the following steps to add the softkey template to an existing Common Device Configuration.

a) Click **Find** and enter the search criteria.
b) Click an existing Common Device Configuration.

Step 4 In the **Softkey Template** drop-down list, choose the softkey template that contains the softkey that you want to make available.

Step 5 Click **Save**.

Step 6 Perform one of the following tasks:

- If you modified a Common Device Configuration that is already associated with devices, click **Apply Config** to restart the devices.
- If you created a new Common Device Configuration, associate the configuration with devices and then restart them.

Associate a Common Device Configuration with a Phone

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select the phone device to add the softkey template.

Step 3 From the **Common Device Configuration** drop-down list, choose the common device configuration that contains the new softkey template.

Step 4 Click **Save**.

Step 5 Click **Reset** to update the phone settings.

Associate a Softkey Template with a Phone

Optional. Use this procedure as an alternative to associating the softkey template with the Common Device Configuration. This procedure also works in conjunction with the Common Device Configuration. You can use it when you need to assign a softkey template that overrides the assignment in the Common Device Configuration or any other default softkey assignment.

Before you begin

Configure a Softkey Template for Immediate Divert, on page 174

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** to select the phone to add the softkey template.

Step 3 From the **Softkey Template** drop-down list, choose the template that contains the new softkey.

Step 4 Click **Save**.

Immediate Divert Interactions and Restrictions

Immediate Divert Interactions

Feature	Interaction
Multilevel Precedence and Preemption (MLPP)	Immediate Divert diverts calls to voice-messaging mailboxes regardless of the type of call (for example, a precedence call). When Alternate Party Diversion (call precedence) is activated, Call Forward No Answer (CFNA) gets deactivated.
Call Forward	When the Forward No Answer setting on the Directory Number Configuration window is not configured, Call Forward uses the clusterwide CFNA timer service parameter, Forward No Answer Timer. If a user presses the iDivert softkey at the same time as the call is being forwarded, the call gets diverted to an assigned call forward directory number (because the timer was too short), not the voice-messaging mailbox. To resolve this situation, set the CFNA timer service parameter to enough time (for example, 60 seconds).
Call Detail Records (CDR)	Immediate Divert uses the immediate divert code number in the **Onbehalf** of fields (for example, joinOnbehalfOf and lastRedirectRediectOnBehalfOf) in CDR.

Feature	Interaction
Call Park and Directed Call Park	When user A calls user B, and user B parks the call; user B retrieves the call and then decides to send the call to a voice-messaging mailbox by pressing the iDivert or Divert softkey. User A receives the voice-messaging mailbox greeting of user B.
Conference	When a conference participant presses the iDivert softkey, the remaining conference participants receive the voice-messaging mailbox greeting of the immediate divert initiator. Conference types include Ad Hoc, Meet-Me, Barge, cBarge, and Join.
Hunt List	For calls that reach the phone directly through a hunt list pilot (as part of the hunting algorithms), the iDivert softkey appears dimmed if the Use Legacy Immediate Divert clusterwide service parameter is set to True; otherwise, it does not appear dimmed. For calls that do not reach the phone directly through a hunt list pilot (as part of the hunting algorithms), the iDivert softkey does not appear dimmed when the Use Legacy Immediate Divert clusterwide service parameter is set to True or False.
Auto Call Pickup	If the Use Legacy Immediate Divert clusterwide service parameter is set to False, and the Auto Call Pickup Enabled clusterwide service parameter is set to True, and a user of call pickup group uses call pickup to answer a call, the IP phone display will not present any choices to the user when the iDivert softkey is pressed.

Immediate Divert Restrictions

Restriction	Description
Voice Mail Profile	When you use QSIG integration with your voicemail system, a voicemail profile that includes either a voicemail pilot or a voicemail mask or both should leave the **Make this the default Voice Mail Profile for the System** check box unchecked. Ensure the default Voice Mail Profile setting is always set to No Voice Mail.
Call Forward All (CFA) and Call Forward Busy (CFB)	When Call Forward All (CFA) and Call Forward Busy (CFB) are activated, the system does not support Immediate Divert (CFA and CFB have precedence over Immediate Divert).

Restriction	Description
Busy Voicemail System	The iDivert detects a busy condition on the voicemail ports, when iDivert reaches a voicemail system over a local or SCCP connection. **Note** Immediate Divert cannot divert a call to a busy voicemail port; voicemail ports can exist as members of a route or hunt list. The call cannot divert to a busy voicemail system, but the original call gets maintained. The phone displays "Busy" message on which iDivert was invoked to indicate that the call was not diverted. When a voicemail system is reached over a QSIG or SIP trunk, iDivert can be detected, but the call does not get maintained. When the **Allow QSIG During iDivert clusterwide** service parameter is set to **True**, or the **Use Legacy Immediate Divert clusterwide** service parameter is set to **False**, Immediate Divert supports access to voicemail systems that can be reached over QSIG or SIP trunks. When the **Allow QSIG During iDivert clusterwide** service parameter is set to **False**, and the **Use Legacy Immediate Divert clusterwide** service parameter is set to **True**, Immediate Divert does not support access to voicemail systems over QSIG or SIP trunks.
Malicious Caller ID	System does not support using Malicious Caller ID and Immediate Divert features together.
Forward No Answer Timeout	A race condition in connection with the Forward No Answer Timeout exists when you press the iDivert softkey. For example, if a manager presses the iDivert softkey immediately after the Forward No Answer timeout, call forward forwards the call to a preconfigured directory number. However, if the manager presses the iDivert softkey before the Forward No Answer timeout, immediate divert diverts the call to the voice-messaging mailbox of the manager.
Calling Parties and Called Parties	The calling parties and called parties can divert the call to their voice mailboxes if both simultaneously press the iDivert softkey.
Conference Types	When one participant in a conference presses the iDivert softkey, all remaining participants receive an outgoing greeting of the participant who pressed iDivert. Conference types include Meet-Me, Ad Hoc, cBarge, and Join.
Split or Join Operation	If the last action on a call was Auto Pickup, Call Transfer, Call Park, Call Park Reversion, Conference, Meet-Me Conference, or any application that performs a split or join operation, enhanced iDivert does not present a screen to a called party to choose the voice mailbox. Instead, enhanced iDivert immediately diverts the call to the voice mailbox that is associated with the called party.

Immediate Divert Troubleshooting

Key is not active

The phone displays this message when the user presses iDivert:

Key is not active

The voice-messaging profile of the user who pressed iDivert does not have a voice-messaging pilot.

Configure a voice-messaging pilot in the user voice-messaging profile.

Temporary Failure

The phone displays this message when the user presses iDivert:

Temporary Failure

The voice-messaging system does not work, or a network problem exists.

Troubleshoot your voice-messaging system. See troubleshooting or voice-messaging documentation.

Busy

The phone displays this message when the user presses iDivert:

Busy

This message means that the voice-messaging system is busy.

Configure more voice-messaging ports or try again.

PART VII

Conferencing Features

CHAPTER 15

Ad Hoc Conferencing

Ad Hoc Conferencing Overview

Ad Hoc conferences allow the conference controller (or in some cases, another participant) to add participants to the conference.

Ad Hoc conferences comprise two types: basic and advanced. In basic ad hoc conferencing, the originator of the conference acts as the controller of the conference and is the only participant who can add or remove other participants. In advanced Ad Hoc conferencing, any participant can add or remove other participants. Advanced Ad Hoc conferencing also allows you to link multiple ad hoc conferences together.

Advanced Ad Hoc conferencing allows you to link multiple Ad Hoc conferences together by adding an Ad Hoc conference to another Ad Hoc conference as if it were an individual participant. If you attempt to link multiple conferences together when the Advanced Ad Hoc Conference Enabled service parameter is set to False, the IP phone displays a message. You can also use the methods that are available for adding individual participants to an Ad Hoc conference to add another conference to an Ad Hoc conference.

Ad Hoc Conferencing Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure Softkey Template for Conferencing, on page 184	Add the Conference List, Join, and Remove Last Conference Party softkeys to a softkey template.
Step 2	To Associate Softkey Template Common Device, on page 185, complete the following subtasks: • Add a Softkey Template to a Common Device Configuration, on page 186	**Optional**. To make the softkey template available to phones, you must complete either this step or the following step. Follow this step if your system uses a **Common Device Configuration** to apply configuration options to phones. This is the most commonly used

	Command or Action	Purpose
	• Associate a Common Device Configuration with a Phone, on page 187	method for making a softkey template available to phones.
Step 3	Associate a Softkey Template with a Phone, on page 187	**Optional**. Use this procedure either as an alternative to associating the softkey template with the Common Device Configuration, or in conjunction with the Common Device Configuration. Use this procedure in conjunction with the Common Device Configuration if you need assign a softkey template that overrides the assignment in the Common Device Configuration or any other default softkey assignment.
Step 4	Configure Ad Hoc Conferencing, on page 187	Enable advanced conferencing, specify the maximum number of participants, and specify when to drop a conference connection.
Step 5	Configure Join Across Lines, on page 190	Enable Join Across Lines to create a conference.

Configure Softkey Template for Conferencing

Use this procedure to make the following conferencing softkeys available:

Softkey	Description	Call States
Conference List (**ConfList**)	View a list of participant directory numbers that are in an Ad Hoc conference. The name of the participant is displayed if it is configured in Cisco Unified Communications Manager Administration.	On Hook Connected
Join	Join up to 15 established calls (for a total of 16) to create a conference.	On Hold
Remove Last Conference Party (**Remove**)	The conference controller can invoke the conference list and remove any participant in the conference by using the **Remove** softkey.	On Hook Connected

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Softkey Template**.

Step 2 Perform the following steps to create a new softkey template; otherwise, proceed to the next step.

a) Click **Add New**.

b) Select a default template and click **Copy**.
c) Enter a new name for the template in the **Softkey Template Name** field.
d) Click **Save**.

Step 3 Perform the following steps to add softkeys to an existing template.
a) Click **Find** and enter the search criteria.
b) Select the required existing template.

Step 4 Check the **Default Softkey Template** check box to designate this softkey template as the default softkey template.

Note If you designate a softkey template as the default softkey template, you cannot delete it unless you first remove the default designation.

Step 5 Choose **Configure Softkey Layout** from the **Related Links** drop-down list in the upper right corner and click **Go**.

Step 6 From the **Select a Call State to Configure** drop-down list, choose the call state for which you want the softkey to display.

Step 7 From the **Unselected Softkeys** list, choose the softkey to add and click the right arrow to move the softkey to the **Selected Softkeys** list. Use the up and down arrows to change the position of the new softkey.

Step 8 Repeat the previous step to display the softkey in additional call states.

Step 9 Click **Save**.

Step 10 Perform one of the following tasks:

- Click **Apply Config** if you modified a template that is already associated with devices to restart the devices.
- If you created a new softkey template, associate the template with the devices and then restart them. For more information, see *Add a Softkey Template to a Common Device Configuration* and *Associate a Softkey Template with a Phone* sections.

What to do next

Complete one of the following procedures:

- Associate Softkey Template Common Device, on page 185
- Associate a Softkey Template with a Phone, on page 187

Associate Softkey Template Common Device

Optional. There are two ways to associate a softkey template with a phone:

- Add the softkey template to the **Phone Configuration**.
- Add the softkey template to the **Common Device Configuration**.

The procedures in this section describe how to associate the softkey template with a **Common Device Configuration**. Follow these procedures if your system uses a **Common Device Configuration** to apply configuration options to phones. This is the most commonly used method for making a softkey template available to phones.

To use the alternative method, go to Associate a Softkey Template with a Phone, on page 187

Before you begin

Configure Softkey Template for Conferencing, on page 184

Procedure

	Command or Action	Purpose
Step 1	Add a Softkey Template to a Common Device Configuration, on page 186	Perform this step to add a conferencing softkey template to the Common Device Configuration.
Step 2	Associate a Common Device Configuration with a Phone, on page 187	Perform this step to link the conferencing softkey Common Device Configuration to a phone.

Add a Softkey Template to a Common Device Configuration

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Common Device Configuration**.

Step 2 Perform the following steps to create a new Common Device Configuration and associate the softkey template with it; otherwise, proceed to the next step.

a) Click **Add New**.
b) Enter a name for the Common Device Configuration in the **Name** field.
c) Click **Save**.

Step 3 Perform the following steps to add the softkey template to an existing Common Device Configuration.

a) Click **Find** and enter the search criteria.
b) Click an existing Common Device Configuration.

Step 4 In the **Softkey Template** drop-down list, choose the softkey template that contains the softkey that you want to make available.

Step 5 Click **Save**.

Step 6 Perform one of the following tasks:

- If you modified a Common Device Configuration that is already associated with devices, click **Apply Config** to restart the devices.
- If you created a new Common Device Configuration, associate the configuration with devices and then restart them.

Associate a Common Device Configuration with a Phone

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select the phone device to add the softkey template.

Step 3 From the **Common Device Configuration** drop-down list, choose the common device configuration that contains the new softkey template.

Step 4 Click **Save**.

Step 5 Click **Reset** to update the phone settings.

Associate a Softkey Template with a Phone

Optional. Use this procedure as an alternative to associating the softkey template with the Common Device Configuration. This procedure also works in conjunction with the Common Device Configuration. You can use it when you need to assign a softkey template that overrides the assignment in the Common Device Configuration or any other default softkey assignment.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** to select the phone to add the softkey template.

Step 3 From the **Softkey Template** drop-down list, choose the template that contains the new softkey.

Step 4 Click **Save**.

Step 5 Press **Reset** to update the phone settings.

Configure Ad Hoc Conferencing

Configure advanced Ad Hoc conferencing to allow non-controller participants to add and remove other participants and the ability of all participants to link ad hoc conferences together.

Procedure

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

Step 2 From the **Server** drop-down list, choose the server.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.

Step 4 Configure the fields in the **Clusterwide Parameters (Features - Conference)** area. For parameter descriptions, see Ad Hoc Conferencing Service Parameters, on page 188.

Step 5 Click **Save.**

What to do next

Configure Join Across Lines, on page 190

Ad Hoc Conferencing Service Parameters

The following table lists the main service parameters for Ad Hoc conferencing. For additional conferencing service parameters, refer to the **Service Parameter Configuration** window's **Advanced** option. Conferencing service parameters appear under **Clusterwide Parameters (Feature - Conference)**.

Table 17: Ad Hoc Conference Service Parameters

Service Parameters	Description
Drop Ad Hoc Conference	Drop Ad Hoc Conference, prevents toll fraud (where an internal conference controller disconnects from the conference while outside callers remain connected). The service parameter settings specify conditions under which an ad hoc conference gets dropped. • **Never**—The conference does not get dropped. (We recommend that you use the default option to avoid unintentional termination of a conference). • **When No OnNet Parties Remain in the Conference**—The system drops the active conference when the last on-network party in the conference hangs up or drops out of the conference. Unified Communications Manager releases all resources that are assigned to the conference. • **When Conference Controller Leaves**—The active conference terminates when the primary controller (conference creator) hangs up. Unified Communications Manager releases all resources that are assigned to the conference. **Note** We recommend that you set this service parameter to **Never**. Any other setting can result in unintentional termination of a conference. The Drop Ad Hoc Conference service parameter works differently for conference calls that are initiated from a Cisco Unified IP Phone 7940 or 7960 that is running SIP, or a third-party phone that is running SIP .
Maximum Ad Hoc Conference	This parameter specifies the maximum number of participants that are allowed in a single Ad Hoc conference. Default Value: 4
Advanced Ad Hoc Conference Enabled	This parameter determines whether advanced Ad Hoc conference features are enabled. This includes the ability of non-controller participants to add and remove other participants and the ability of all participants to link ad hoc conferences together.

Service Parameters	Description
Non-linear Ad Hoc Conference Linking Enabled	This parameter determines whether more than two Ad Hoc conferences can be linked directly to an Ad Hoc conference in a non-linear fashion (three or more conferences linked to any one conference).
Choose Encrypted Audio Conference Instead Of Video Conference	This parameter determines whether Unified Communications Manager chooses an encrypted audio conference bridge or an unencrypted video conference bridge for an Ad-Hoc conference call when the conference controller's Device Security Mode is set to either Authenticated or Encrypted and at least two conference participants are video-capable. Because encrypted video conference bridges are not supported in this release, Unified Communications Manager must choose between an encrypted audio conference bridge and an unencrypted video conference bridge. The default value is **True**.
Minimum Video Capable Participants To Allocate Video Conference	This parameter specifies the number of video-capable conference participants that must be present in an Ad Hoc conference to allocate a video conference bridge. If the number of video-capable participants is less than the number specified in this parameter, Unified Communications Manager allocates an audio conference bridge. If the number of video-capable participants is equal to, or greater than, the number specified in this parameter, Unified Communications Manager allocates a video conference bridge, when available, from the configured media resource group list (MRGL). Specifying a value of zero means that video conference bridges will always be allocated, even when none of the participants on the conference are video-capable. When a conference has been established using an audio bridge and then additional video-capable participants join the conference, the conference will remain on the audio bridge and will not convert to video. The default value is **2**.
Allocate Video Conference Bridge For Audio Only Conferences When The Video Conference Bridge Has Higher Priority	This parameter determines whether Unified Communications Manager chooses a video conference bridge, when available, for an Ad Hoc audio-only conference call when the video conference bridge has a higher priority than an audio conference bridge in the media resource group list (MRGL). If an audio conference bridge has higher priority than any video conference bridge in the MRGL, Unified Communications Manager ignores this parameter. This parameter proves useful in situations where the local conference bridge is a video bridge (and configured in the MRGL with the highest priority) and audio conference bridges are only available in remote locations; in that situation, enabling this parameter means thatUnified Communications Manager would attempt to use the local video conference bridge first, even for audio-only conference calls. The default value is **False**.
Enable Click-to-Conference for Third-Party Applications	This parameter determines whether the Click-to-Conference functionality over the SIP trunk is enabled on Unified Communications Manager. The Click-to-Conference feature allows third-party applications to setup a conference using the SIP out of dialog REFER method and subscribe to the SIP trunk for Conference Event Package through SIP SUBSCRIBE/NOTIFY. **Warning** Enabling this parameter could negatively affect CTI applications that are not coded to support this feature. Default value: False

Service Parameters	Description
Cluster Conferencing Prefix Identifier	This parameter defines a number, up to 8 digits (e.g. 0001), that is prefixed to a conference identifier generated for Adhoc and Meet-Me conferences that will be hosted on a SIP conference bridge such as Cisco Telepresence MCU or Cisco Telepresence Conductor. This field should be populated by the administrator when there are multiple clusters in a network that will be sharing the SIP conference bridges that Unified Communications Manager manages. Every cluster should be configured with a unique prefix to ensure that the conference identifier for Adhoc and Meet-Me conferences is unique. If conference resources are not being shared across clusters, then this field may not be populated.

Configure Join Across Lines

The Join Across Lines feature allows a user to join calls on multiple phone lines (either on different directory numbers or on the same directory number but on different partitions) to create a conference.

Before you begin

- Ensure the phone model supports Join Across Lines Generate a Phone Feature List, on page 3
- Configure Ad Hoc Conferencing, on page 187

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Default Device Profile**. The **Default Device Profile Configuration** window is displayed.

Step 2 From the **Device Profile Type** drop-down list, choose the phone model.

Step 3 From the **Device Protocol** drop-down list, choose the relevant SCCP or SIP protocol.

Step 4 Set the **Join Across Lines** to **On**.

Step 5 Click **Save**.

Conference Interactions and Restrictions

Conference Interactions

Feature	Interaction
Conference by Using **cBarge**	Initiate a conference by pressing the **cBarge** softkey, or if the Single Button cBarge feature is enabled, by pressing the shared-line button of the active call. When cBarge is initiated, a barge call gets set up by using the shared conference bridge, if available. The original call gets split and then joined at the conference bridge. The call information for all parties gets changed to Conference. The barged call becomes a conference call with the barge target device as the conference controller. It can add more parties to the conference or can drop any party. When any party releases from the call, leaving only two parties in the conference, the remaining two parties experience a brief interruption and then get reconnected as a point-to-point call, which releases the shared conference resource.
Interaction with Call Park, Call Transfer, and Redirect	If the conference controller transfers, parks, or redirects the conference to another party, the party that retrieves the call acts as the virtual controller for the conference. A virtual controller cannot add new parties to the conference nor remove any party that was added to the conference, but a virtual controller can transfer, park, or redirect the conference to another party, who would, in turn, become the virtual controller of the conference. When this virtual controller hangs up the call, the conference ends.
Softkey display on SIP phones	The ConfList and the Remove softkey feature is available only on SCCP phones. The SIP phones have a Show Details button with similar functionality.

Conference Restrictions

The following restrictions apply to ad hoc conferencing:

Feature	Restrictions
Ad Hoc conference	Unified Communications Manager supports a maximum of 100 simultaneous Ad Hoc conferences for each Unified Communications Manager server. Cisco Unified Communications Manager supports a maximum of 64 participants per Ad Hoc conference (provided adequate conference resources are available). In the case of linked Ad Hoc conferences, the system considers each conference as one participant.

Feature	Restrictions
Ad Hoc conference on SIP phones: • Cisco Unified IP Phone 7911 • Cisco Unified IP Phone 7941 • Cisco Unified IP Phone 7961 • Cisco Unified IP Phone 7970 • Cisco Unified IP Phone 7971	Unified Communications Manager uses“ beep” and “beep beep” tones when a new party is added and when the new party drops from the Ad Hoc conference, respectively. When a party is added to an Ad Hoc conference, a user on a phone that is running SIP may not hear the beep; when a participant drops from the Ad Hoc conference, a user on a phone that is running SIP may not hear the “beep beep”. Users might not hear the beeps because of the time it takes Unified Communications Manager to set up and tear down connections during the conferencing process. You can invoke Ad Hoc conference linking for phones that are running SIP only by using the Conference and Transfer functions. The system does not support Direct Transfer and Join. Supported phones that are running SIP comprise Cisco Unified IP Phone 7911, 7941, 7961, 7970, and 7971.
Ad Hoc conference on SIP phones: • Cisco Unified IP Phone 7940 • Cisco Unified IP Phone 7960 • Third-Party Phone	• Phones display individual calls as conference calls. Cisco Unified IP Phones 7940 and 7960 can create local conference calls but not Ad Hoc conference calls. • Conference list (ConfList), is not available. • Remove last conference participant (RmLstC), is not available. • Drop Ad Hoc conference is not supported. • The SIP Profile parameter Conference Join Enabled controls behavior of the phone that is running SIP when the conference controller exits a locally hosted conference. If the Conference Join Enabled check box is unchecked, all legs disconnect when the conference controller exits the Ad Hoc conference call. If the Conference Join Enabled check box is checked, the remaining two parties stay connected. • To achieve the same level of control that the Drop Ad Hoc Conference parameter settings provide for conference calls that a phone that is running SCCP initiates, the administrator can use a combination of the Conference Join Enabled SIP profile parameter and the Block OffNet to OffNet Transfer service parameter for conferences that are initiated on the phone that is running SIP (Cisco Unified IP Phone 7940 or 60). (Because the phone that is running SIP performs a transfer when it drops out of the conference call, the Block OffNet to OffNet Transfer can prevent toll fraud by not allowing two offnet phones to remain in the call.) • Unified Communications Manager uses “beep” and “beep beep” tones when a new party is added and when the new party drops from the Ad Hoc conference, respectively. When a party is added to an Ad Hoc conference, a user on a phone that is running SIP may not hear the beep when a participant drops from the Ad Hoc conference, a user on a phone that is running SIP may not hear the “beep beep”. Users might not hear the beeps because of the time it takes Unified Communications Manager to set up and tear down connections during the conferencing process.

Feature	Restrictions
Phone displaying "To Conference" even when two parties are connected	Configure a Call Manager cluster with Publisher (CmA11) and Subscribers (CmA2). Phones A, B, C are registered with CmA1. Phones D is registered with CmA2. • Setup an consultative or blind ad-hoc conference between A(1000), B(4000), C(5000), D(6000) with A as the controller. • Shutdown Cma2. • Phone D will go to Preservation mode & press end call softkey . • Phone A,B & C are in conference. • Phone A,B & C are in conference. • Disconnect Phone A ,then Phone B & C should be in a Direct call. Issue: Phone B & C are still in conference • Disconnect Phone A ,then Phone B & C should be in a Direct call. Issue: Phone B & C are still in conference • Disconnect Phone B, there should be no call on phone C. Phone B & C are still in conference. Issue: Phone C is still in Conference .

CHAPTER 16

Meet-Me Conferencing

Meet-Me Conferencing Overview

Users can use Meet-Me Conferencing to set up or join conferences. A user that sets up a conference is called the conference controller. A user that joins a conference is called a participant.

Meet-Me Conferencing Task Flow

Before you begin

- Refer to the configuration documentation which came with your router and check for any settings which you may need to configure before proceeding with the Meet-Me Conferencing Task Flow.

Procedure

	Command or Action	Purpose
Step 1	Configure a Softkey Template for Meet-Me Conferencing, on page 196	Add the Meet-Me softkey to a softkey template.
Step 2	To Associate a Softkey Template with a Common Device Configuration, on page 197, complete the following subtasks: • Add a Softkey Template to a Common Device Configuration, on page 197 • Associate a Common Device Configuration with a Phone, on page 198	**Optional**. To make the softkey template available to phones, you must complete either this step or the following step.
Step 3	Common Device ConfigurationAssociate a Softkey Template with a Phone, on page 198	**Optional**. Use this procedure either as an alternative to associating the softkey template with the Common Device Configuration, or in

	Command or Action	Purpose
		conjunction with the Common Device Configuration. Use this procedure in conjunction with the Common Device Configuration if you need assign a softkey template that overrides the assignment in the Common Device Configuration or any other default softkey assignment.
Step 4	Configure a Meet-Me Conferencing Number, on page 199	Enable advanced conferencing, specify the maximum number of participants, and specify when to drop a conference connection.

Configure a Softkey Template for Meet-Me Conferencing

Use this procedure to make the Meet Me softkey available in the off hook call state.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Softkey Template**.

Step 2 Perform the following steps to create a new softkey template; otherwise, proceed to the next step.

a) Click **Add New**.
b) Select a default template and click **Copy**.
c) Enter a new name for the template in the **Softkey Template Name** field.
d) Click **Save**.

Step 3 Perform the following steps to add softkeys to an existing template.

a) Click **Find** and enter the search criteria.
b) Select the required existing template.

Step 4 Check the **Default Softkey Template** check box to designate this softkey template as the default softkey template.

Note If you designate a softkey template as the default softkey template, you cannot delete it unless you first remove the default designation.

Step 5 Choose **Configure Softkey Layout** from the **Related Links** drop-down list in the upper right corner and click **Go**.

Step 6 From the **Select a Call State to Configure** drop-down list, choose the call state for which you want the softkey to display.

Step 7 From the **Unselected Softkeys** list, choose the softkey to add and click the right arrow to move the softkey to the **Selected Softkeys** list. Use the up and down arrows to change the position of the new softkey.

Step 8 Repeat the previous step to display the softkey in additional call states.

Step 9 Click **Save**.

Step 10 Perform one of the following tasks:

- Click **Apply Config** if you modified a template that is already associated with devices to restart the devices.

- If you created a new softkey template, associate the template with the devices and then restart them. For more information, see *Add a Softkey Template to a Common Device Configuration* and *Associate a Softkey Template with a Phone* sections.

Associate a Softkey Template with a Common Device Configuration

Optional. There are two ways to associate a softkey template with a phone:

- Add the softkey template to the **Phone Configuration**.
- Add the softkey template to the **Common Device Configuration**.

The procedures in this section describe how to associate the softkey template with a **Common Device Configuration**. Follow these procedures if your system uses a **Common Device Configuration** to apply configuration options to phones. This is the most commonly used method for making a softkey template available to phones.

To use the alternative method, see Associate a Softkey Template with a Phone, on page 198.

Before you begin

Configure a Softkey Template for Meet-Me Conferencing, on page 196

Procedure

	Command or Action	Purpose
Step 1	Add a Softkey Template to a Common Device Configuration, on page 197	
Step 2	Associate a Common Device Configuration with a Phone, on page 198	

Add a Softkey Template to a Common Device Configuration

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Common Device Configuration**.

Step 2 Perform the following steps to create a new Common Device Configuration and associate the softkey template with it; otherwise, proceed to the next step.

a) Click **Add New**.
b) Enter a name for the Common Device Configuration in the **Name** field.
c) Click **Save**.

Step 3 Perform the following steps to add the softkey template to an existing Common Device Configuration.

a) Click **Find** and enter the search criteria.
b) Click an existing Common Device Configuration.

Step 4 In the **Softkey Template** drop-down list, choose the softkey template that contains the softkey that you want to make available.

Step 5 Click **Save**.

Step 6 Perform one of the following tasks:

- If you modified a Common Device Configuration that is already associated with devices, click **Apply Config** to restart the devices.
- If you created a new Common Device Configuration, associate the configuration with devices and then restart them.

Associate a Common Device Configuration with a Phone

Before you begin

Add a Softkey Template to a Common Device Configuration, on page 197

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select the phone device to add the softkey template.

Step 3 From the **Common Device Configuration** drop-down list, choose the common device configuration that contains the new softkey template.

Step 4 Click **Save**.

Step 5 Click **Reset** to update the phone settings.

Associate a Softkey Template with a Phone

Optional. Use this procedure as an alternative to associating the softkey template with the Common Device Configuration. This procedure also works in conjunction with the Common Device Configuration. You can use it when you need to assign a softkey template that overrides the assignment in the Common Device Configuration or any other default softkey assignment.

Before you begin

Configure a Softkey Template for Meet-Me Conferencing, on page 196

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** to select the phone to add the softkey template.

Step 3 From the **Softkey Template** drop-down list, choose the template that contains the new softkey.

Step 4 Click **Save**.

Step 5 Press **Reset** to update the phone settings.

Configure a Meet-Me Conferencing Number

The Cisco Unified Communications Manager administrator provides the Meet-Me conference directory number range to users, so that they can access the feature. The user chooses a directory number from the range that is specified for the Meet-Me Number or Pattern to establish a Meet-Me conference and becomes the conference controller.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Meet-Me Number/Pattern**.
The **Find and List Meet-Me Numbers** window appears.

Step 2 Enter the appropriate search criteria and click **Find**.
All matching records are displayed.

Step 3 In the list of records, click the link for the record that you want to view.

Step 4 Perform one of the followings tasks:

- To copy a Meet-Me number or pattern, click the Meet-Me number or pattern that you want to copy. The **Meet-Me Number/Pattern Configuration** window appears. Click **Copy**.
- To add a Meet-Me Number or Pattern, click the **Add New** button.
- To update an existing Meet-Me Number or Pattern, click the Meet-Me Number or Pattern that you want to update.

Step 5 Enter the appropriate settings.

See the Related Topics section for information about the fields and their configuration options.

Step 6 Click **Save**.

Meet-Me Number and Pattern Settings

Field	Description
Directory Number or Pattern	Enter a Meet-Me number or a range of numbers. To configure a range, the dash must appear within brackets and follow a digit; for example, to configure the range 1000 to 1050, enter 10[0-5]0.
Description	The description can include up to 50 characters in any language, but it cannot include double quotation marks ("), percentage sign (%), ampersand (&), or angle brackets (<>).

Field	Description
Partition	To use a partition to restrict access to the Meet-Me number or pattern, choose the desired partition from the drop-down list box. If you do not want to restrict access to the Meet-Me number or pattern, choose <None> for the partition. You can configure the number of partitions that are displayed in this drop-down list box by using the Max List Box Items enterprise parameter. If more partitions exist than the Max List Box Items enterprise parameter specifies, the **Find** button is displayed next to the drop-down list box. Click the **Find** button to display the **Find and List Partitions** window. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and update the Max List Box Items field under CCMAdmin Parameters. **Note** Make sure that the combination of Meet-Me number or pattern and partition is unique within the Unified Communications Manager cluster.
Minimum Security Level	Choose the minimum Meet-Me conference security level for this Meet-Me number or pattern from the drop-down list box. • Choose **Authenticated** to block participants with nonsecure phones from joining the conference. • Choose **Encrypted** to block participants with authenticated or nonsecure phones from joining the conference. • Choose **Non Secure** to allow all participants to join the conference. **Note** To use this feature, ensure that you have a secure conference bridge that is configured and available.

Meet-Me Conferencing Restrictions

Unified Communications Manager supports a maximum of 100 simultaneous Meet-Me conferences for each Unified Communications Manager server.

After the maximum number of participants that is specified for that conference is has been exceeded, no other callers can join the conference.

PART VIII

Placing Calls

CHAPTER 17

Call Back

Call Back Overview

The CallBack feature allows you to receive notification when a busy extension is available to receive calls.

You can activate Call Back for a destination phone that is within the same Unified Communications Manager cluster as your phone or on a remote Private Integrated Network Exchange (PINX) over QSIG trunks or QSIG-enabled intercluster trunks.

To receive CallBack notification, press the CallBack softkey or feature button while receiving a busy or ringback tone. You can activate Call Back during reorder tone, which is triggered when the No Answer timer expires.

Suspend/Resume

The Call Back feature enables the system to suspend the call completion service if the user who originated Call Back is busy. When the originating user then becomes available, the call completion service resumes for that user.

Note Call Back supports Suspend/Resume CallBack notification for both intracluster and intercluster QSIG trunks or QSIG-enabled intercluster trunks.

Call Back Prerequisites

To use the Call Back feature, the destination phone must be in one of the following locations:

- In the same Unified Communications Manager cluster as the user phone
- On a remote PINX over QSIG trunks

- On a remote PINX over QSIG-enabled intercluster trunks

If you want to use non-English phone locales or country-specific tones, you must install locales.

- The following devices support the Call Back feature:
  - Cisco Unified IP Phones 6900, 7900, 8900, and 9900 Series (except 6901 and 6911)
  - Cisco IP Phones 7800 and 8800 Series
  - Cisco VGC Phone (uses the Cisco VG248 Gateway)
  - Cisco Analog Telephone Adapter (ATA) 186 and 188
  - Busy Subscriber for Cisco VG224 endpoints
  - No Answer for Cisco VG224 endpoints
- A CTI route point that forwards calls to any of the supported phones.

Call Back Configuration Task Flow

Complete one of the task flows depending on whether your phone supports softkey or buttons.

Use this table to determine whether to configure the CallBack softkey or the button for the Call Back supported IP phones.

Table 18: Cisco IP Phones That Use CallBack Softkeys and Buttons

Cisco Phone Model	CallBack Softkey	CallBack Button
Cisco Unified IP Phone 6900 Series (except 6901 and 6911)	X	X
Cisco Unified IP Phone 7900 Series	X	
Cisco IP Phone 7800 and 8800 Series	X	X
Cisco Unified IP Phone 8900 Series	X	X
Cisco Unified IP Phone 9900 Series	X	X
Cisco IP Communicator	X	

Before you begin

- Review Call Back Prerequisites, on page 203.

Procedure

	Command or Action	Purpose
Step 1	Configure Softkey Template for CallBack, on page 205	Perform this step to add CallBack softkey to template and configure the softkey using the Common Device Configuration or phone.
Step 2	Configure CallBack Button, on page 208	Perform this step to add and configure the CallBack button to a phone.

Configure Softkey Template for CallBack

CallBack softkey has the following call states:

- On Hook
- Ring Out
- Connected Transfer

Use this procedure to make the CallBack softkey available:

Before you begin

Ensure your phone supports Call Back.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Softkey Template**.

Step 2 Perform the following steps to create a new softkey template; otherwise, proceed to the next step.

a) Click **Add New**.
b) Select a default template and click **Copy**.
c) Enter a new name for the template in the **Softkey Template Name** field.
d) Click **Save**.

Step 3 Perform the following steps to add softkeys to an existing template.

a) Click **Find** and enter the search criteria.
b) Select the required existing template.

Step 4 Check the **Default Softkey Template** check box to designate this softkey template as the default softkey template.

Note If you designate a softkey template as the default softkey template, you cannot delete it unless you first remove the default designation.

Step 5 Choose **Configure Softkey Layout** from the **Related Links** drop-down list in the upper right corner and click **Go**.

Step 6 From the **Select a Call State to Configure** drop-down list, choose the call state for which you want the softkey to display.

Step 7 From the **Unselected Softkeys** list, choose the softkey to add and click the right arrow to move the softkey to the **Selected Softkeys** list. Use the up and down arrows to change the position of the new softkey.

Step 8 Repeat the previous step to display the softkey in additional call states.

Step 9 Click **Save**.

Step 10 Perform one of the following tasks:

- Click **Apply Config** if you modified a template that is already associated with devices to restart the devices.
- If you created a new softkey template, associate the template with the devices and then restart them. For more information, see *Add a Softkey Template to a Common Device Configuration* and *Associate a Softkey Template with a Phone* sections.

What to do next

Perform one the following procedures:

- Associate CallBack Softkey Template with a Common Device Configuration, on page 206
- Associate CallBack Softkey Template with Phone, on page 207

Associate CallBack Softkey Template with a Common Device Configuration

Optional. There are two ways to associate a softkey template with a phone:

- Add the softkey template to the **Phone Configuration**.
- Add the softkey template to the **Common Device Configuration**.

The procedures in this section describe how to associate the softkey template with a **Common Device Configuration**. Follow these procedures if your system uses a **Common Device Configuration** to apply configuration options to phones. This is the most commonly used method for making a softkey template available to phones.

To use the alternative method, see Associate CallBack Softkey Template with Phone, on page 207.

Procedure

	Command or Action	Purpose
Step 1	Add CallBack Softkey Template to the Common Device Configuration, on page 206	Perform this step to add CallBack softkey template to the Common Device Configuration.
Step 2	Associate a Common Device Configuration with a Phone, on page 207	Perform this step to link the CallBack softkey Common Device Configuration to a phone.

Add CallBack Softkey Template to the Common Device Configuration

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Common Device Configuration**.

Step 2 Perform the following steps to create a new Common Device Configuration and associate the softkey template with it; otherwise, proceed to the next step.

a) Click **Add New**.
b) Enter a name for the Common Device Configuration in the **Name** field.
c) Click **Save**.

Step 3 Perform the following steps to add the softkey template to an existing Common Device Configuration.

a) Click **Find** and enter the search criteria.
b) Click an existing Common Device Configuration.

Step 4 In the **Softkey Template** drop-down list, choose the softkey template that contains the softkey that you want to make available.

Step 5 Click **Save**.

Step 6 Perform one of the following tasks:

- If you modified a Common Device Configuration that is already associated with devices, click **Apply Config** to restart the devices.
- If you created a new Common Device Configuration, associate the configuration with devices and then restart them.

Associate a Common Device Configuration with a Phone

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select the phone device to add the softkey template.

Step 3 From the **Common Device Configuration** drop-down list, choose the common device configuration that contains the new softkey template.

Step 4 Click **Save**.

Step 5 Click **Reset** to update the phone settings.

Associate CallBack Softkey Template with Phone

Optional: Use this procedure either as an alternative to associating the softkey template with the Common Device Configuration, or in conjunction with the Common Device Configuration. Use this procedure in conjunction with the Common Device Configuration if you need to assign a softkey template that overrides the assignment in the Common Device Configuration or any other default softkey assignment.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** to select the phone to add the softkey template.

Step 3 From the **Softkey Template** drop-down list, choose the template that contains the new softkey.

Step 4 Click **Save**.

Step 5 Press **Reset** to update the phone settings.

Configure CallBack Button

The procedures in this section describe how to configure the CallBack button.

Procedure

	Command or Action	Purpose
Step 1	Configure Phone Button Template for Call Back, on page 208	Perform this step to assign CallBack button features to line or speed dial keys.
Step 2	Associate a Button Template with a Phone, on page 209	Perform this step to configure the CallBack button for a phone.

Configure Phone Button Template for Call Back

Follow this procedure when you want to assign features to line or speed dial keys.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Phone Button Template**.

Step 2 Click **Find** to display list of supported phone templates.

Step 3 Perform the following steps if you want to create a new phone button template; otherwise, proceed to the next step.

a) Select a default template for the model of phone and click **Copy**.
b) In the **Phone Button Template Information** field, enter a new name for the template.
c) Click **Save**.

Step 4 Perform the following steps if you want to add phone buttons to an existing template.

a) Click **Find** and enter the search criteria.
b) Choose an existing template.

Step 5 From the **Line** drop-down list, choose feature that you want to add to the template.

Step 6 Click **Save**.

Step 7 Perform one of the following tasks:

- Click **Apply Config** if you modified a template that is already associated with devices to restart the devices.
- If you created a new softkey template, associate the template with the devices and then restart them.

Associate a Button Template with a Phone

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** to display the list of configured phones.

Step 3 Choose the phone to which you want to add the phone button template.

Step 4 In the **Phone Button Template** drop-down list, choose the phone button template that contains the new feature button.

Step 5 Click **Save**.
A dialog box is displayed with a message to press **Reset** to update the phone settings.

Call Back Interactions and Restrictions

Call Back Interactions

Feature	Interaction
Call Forward	Calls that are made from CallBack notification screen will override all the Call Forward configured values on the target DN. The calls should be made before CallBack recall timer expires otherwise the calls will not override the Call Forward configured values.
CallBack notification with phones running SIP	CallBack notification works differently only for Cisco Unified IP Phones 7960 and 7940. All other SIP phones and all SCCP phones support on-hook and off-hook notification. The only way that Unified Communications Manager knows when a line on a SIP 7960 or 7940 phone becomes available is by monitoring an incoming SIP INVITE message that Unified Communications Manager receives from the phone. After the phone sends the SIP INVITE to Unified Communications Manager and the phone goes on-hook, Unified Communications Manager sends an audio and CallBack notification screen to the Cisco Unified IP Phone 7960 and 7940 (SIP) user.

Feature	Interaction
Do Not Disturb (DND)	CallBack would work normally in case or when **DND-Reject** is set to **Off** at the originating or the terminating end. The behavior differs only when **DND-Reject** is set to **On**. • **DND-Reject On on Originating end**—User A calls User B and invokes Call Back. User A goes on DND-R. After User B is available, the CallBack notification will still be displayed to User A. That is, user will still be notified with the availability of the other party irrespective of the DND status. • **DND-Reject On on Terminating end**—User A calls User B, and User B has set **DND-Reject** to **On**. User A will get a fast busy tone. User A can initiate CallBack on a busy endpoint. If User B is still on DND-Reject and goes Offhook and Onhook, User A will get a notification "User B is available now but on DND-R", and it will not show the Dial option. If User A does not choose to cancel, CallBack will still monitor User B until User B sets **DND-Reject** to **Off**.
Cisco Extension Mobility	When a Cisco Extension Mobility user logs in or logs out, any active call completion that is associated with Call Back is automatically canceled. If a called phone is removed from the system after Call Back is activated on the phone, the caller receives a reorder tone after pressing the Dial softkey. The user may cancel or reactivate Call Back.

Call Back Restrictions

Feature	Restriction
Call Back with video across CUBE	The Call Back feature does not work for video calls when the call is placed between two Unified CM clusters that are connected via CUBE with qsig-enabled SIP trunks. For additional detail, see CSCun46243.
SIP Trunks	Call Back is not supported over SIP trunks but is supported over QSIG-enabled SIP trunks.
Supported characters for name or number of calling or called party	Call Back only supports spaces and digits 0 through 9 for the name or number of the calling or called party. To work with CallBack, the name or number of the calling or called party cannot contain a pound sign (#) or asterisk (*).
Voicemail	You cannot activate Call Back if you forward all calls to Voice-Messaging System.

Call Back Troubleshooting

This section describes the problems, possible causes, and solutions for various scenarios, and error messages that are displayed on the IP phone for Call Back.

Unplug/Reset Phone After Pressing CallBack Softkey but Before CallBack Occurs

Problem

You have unplugged or reset the phone after pressing the CallBack Softkey but before activating CallBack.

Possible Cause

Unified Communications Manager cancels the Call Back activation.

Solution

After the caller phone registers, the caller phone does not display the Call Back activation window after the reset. The caller must press the CallBack Softkey to view the active Call Back service. CallBack notification occurs on the phone.

Caller Misses to View Availability Notification Before Phone Reset

Problem

In an intracluster or intercluster Call Back scenario, a caller initiates Call Back for a user, for example, User B, who is unavailable. When User B becomes available, the availability notification screen displays on the caller phone, and a tone plays. The caller misses the availability notification for some reason, and the phone resets.

The caller contacts a different user, User C, for example, and presses the CallBack softkey because User C appears busy. The replace/retain screen displays on the caller phone, but the screen does not state that the availability notification already occurred for User B.

Possible Cause

The user reset the phone.

Solution

After a phone reset but not during an active call, review the Call Back notifications on the phone. Press the CallBack softkey.

Call Back Error Messages

The following section describes the error messages that display on the IP phone screen.

CallBack Is Not Active

Problem

The following error message is displayed:

```
CallBack is not active. Press Exit to quit this screen.
```

Possible Cause

User pressed the CallBack softkey during the idle state.

Solution

Follow the recommended action provided in the error message.

CallBack Is Already Active

Problem

The following error message is displayed:

```
CallBack is already active on xxxx. Press OK to activate on yyyy. Press Exit to quit this
screen.
```

Possible Cause

A user tried to activate Call Back, but it is already active.

Problem

Follow the recommended action provided in the error message.

CallBack Cannot Be Activated

Problem

The following error message is displayed:

```
CallBack cannot be activated for xxxx.
```

Possible Cause

When a user tried to activate Call Back, either the extension is not available in Unified Communications Manager database or there is no QSIG route to the destination (that is, the extension belongs to remote Proxy which is connected via non-QSIG trunk), and the extension is not found in the database.

Solution

The user must try again, or the administrator must add the directory number to the Cisco Unified CM Administration.

Key Not Active

Problem

During a call, the CallBack softkey displays on the phone and the user presses the CallBack softkey before the phone rings. But, the following error message is displayed on the phone:

```
Key Not Active
```

Possible Cause

User may not be pressing the CallBack softkey at the appropriate time.

Solution

Users must press the CallBack softkey after a ringing or busy signal is received. Pressing the softkey at the wrong time may cause an error message to display on the phone.

CHAPTER 18

Hotline

This chapter describes how to use and configure the Hotline feature.

Hotline Overview

The Hotline feature extends the Private Line Automatic Ringdown (PLAR) feature, which allows you to configure a phone so that when the user goes off hook (or the NewCall softkey or line key gets pressed), the phone immediately dials a preconfigured number. The phone user cannot dial any other number from a phone that is configured for PLAR. Hotline adds the following additional restrictions and administrator controls for phones that use PLAR:

- Hotline devices (devices configured to use hotline) that receive calls will receive calls only from other hotline devices, and will reject non-hotline callers.
- You can configure a Hotline phone to call only, receive only, or both call and receive.
- You can restrict the features available on a Hotline phone by applying a softkey template to the phone.
- Analog hotline phones ignore inbound hookflash signals.

Route Class Signaling

Hotline uses route class signaling to allow Hotline phones to receive calls only from other Hotline phones. A route class is a DSN code that identifies the class of traffic for a call. The route class informs downstream devices about special routing or termination requirements. A Hotline phone can only accept calls from a Hotline phone with the same route class.

Call Screening

Hotline also provides Configurable Call Screening based on caller ID. Configurable Call Screening allows a receiving Hotline phone to screen calls based on caller ID information and allow only callers in a screening list to connect.

System Requirements for Hotline

The following hotline system requirements exist for Unified Communications Manager:

- Unified Communications Manager 8.0(1) or higher on each server in the cluster
- MGCP gateway POTS phones (FXS).
- SCCP gateway POTS phones (FXS).

Tip Cisco Feature Navigator allows you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://cfn.cloudapps.cisco.com/ITDIT/CFN/.

You do not need a Cisco.com account to access Cisco Feature Navigator.

Hotline Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Generate a Phone Feature List, on page 3	Log in to Cisco Unified Reporting and run a phone feature list report to determine which phones support Hotline.
Step 2	Create Custom Softkey Template, on page 216	Optional. If you want to restrict features on a Hotline phone, create a softkey template that allows only the features that you want.
Step 3	Configure Hotline on Phones, on page 217	Enable the phone as a Hotline device.
Step 4	Configure Route Class Signaling Task Flow, on page 218	Configure route class signaling to support the Hotline feature.
Step 5	Configure Hotline to Call Only or Receive Only Task Flow, on page 222	**Optional**. If you want to restrict a Hotline phone to either originating calls only or terminating calls only, configure call and receive settings.
Step 6	Configure Call Screening with a Calling Search Space , on page 224	**Optional**. Use calling search spaces and partitions to configure a call screening list for your Hotline phones.

Create Custom Softkey Template

When configuring Hotline, you can customize a softkey template to display only those features that you want to make available to a Hotline phone.

Unified Communications Manager includes standard softkey templates for call processing and applications. When creating custom softkey templates, copy the standard templates and make modifications as required.

Before you begin

Generate a Phone Feature List, on page 3

Procedure

Step 1 Choose **Device** > **Device Settings** > **Softkey Template**.

Step 2 Click **Add New**.

Step 3 From the drop-down list, select a softkey template and click **Copy** to create a new template.

Step 4 In the **Softkey Template Name** field, enter a unique name to identify the softkey template.

Step 5 Enter a description that describes the use of the template. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), backslash (\), or angle brackets (<>).

Step 6 To designate this softkey template as the standard softkey template, check the **Default Softkey Template** check box.

Note If you designate a softkey template as the default softkey template, you will not be able to delete this softkey template unless you first remove the default designation.

Step 7 Click **Save**.

The softkey template gets copied, and the **Softkey Template Configuration** window redisplays.

Step 8 (Optional) Click the **Add Application** button.

Step 9 Configure the positions of the softkeys on the Cisco Unified IP Phone LCD screen.

Step 10 To save your configuration, click **Save**.

Configure Hotline on Phones

Use this procedure to enable the phone as a Hotline device.

Before you begin

Optional. If you want to create a custom softkey template to display only those features that you want to make available to a Hotline phone, see Create Custom Softkey Template, on page 216.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select the phone that you want to enable as a Hotline device.

Step 3 Check the **Hotline Device** check box.

Step 4 If you have created a custom softkey template specifically for the Hotline phone, from the **Softkey Template** drop-down list, choose the softkey template.

Step 5 Click **Save**.

Note You can also assign a softkey template to a Device Pool and then assign that Device Pool to the phone.

Configure Route Class Signaling Task Flow

Perform this task flow to configure route class signaling for Hotline calls.

Procedure

	Command or Action	Purpose
Step 1	Enable Route Class Signaling in the Cluster, on page 218	Set the route class signaling clusterwide defaults for trunks and gateways to enabled. **Note** The settings for individual trunks and gateways override the clusterwide defaults. If you use this service parameter to enable route class signaling across the cluster, route class signaling can still be disabled on an individual trunk or gateway.
Step 2	Enable Route Class Signaling on Trunks, on page 219	Enable route class signaling on an individual trunk.
Step 3	Enable Route Class Signaling on Gateways, on page 219	Enable route class signaling on an MGCP T1/CAS or MGCP PRI gateway.
Step 4	Configure Signaling Labels for the Hotline Route Class, on page 220	Configure SIP signaling labels for Hotline route classes.
Step 5	Configure the Route Class on Hotline Route Patterns, on page 221	Configure the route class on the route patterns that are routing your Hotline calls.
Step 6	Configure the Route Class on Hotline Translation Patterns, on page 221	**Optional**. If you use translation patterns on your Hotline calls, configure the route class on your translation patterns.

Enable Route Class Signaling in the Cluster

When you set the **Route Class Trunk Signaling Enabled** service parameter to **True**, the default route class signaling setting for all trunks or gateways in the cluster that support route class signaling is set to enabled.

Note The settings for individual trunks and gateways override the clusterwide defaults. If you use this service parameter to enable route class signaling across the cluster, route class signaling can still be disabled on an individual trunk or gateway.

Procedure

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

Step 2 Set the **Route Class Trunk Signaling Enabled** service parameter to **True**.

Step 3 Click **Save**.

What to do next

Use the following procedures to configure route class signaling on individual trunks or gateways.

Enable Route Class Signaling on Trunks, on page 219

Enable Route Class Signaling on Gateways, on page 219

Enable Route Class Signaling on Trunks

Use this procedure to enable route class signaling on an individual trunk. The configuration for individual trunks overrides the clusterwide service parameter setting.

Before you begin

Follow the Enable Route Class Signaling in the Cluster, on page 218 procedure to use a clusterwide service parameter to configure the default route class signaling settings for all trunks in the cluster.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Trunks**.

Step 2 Click **Find** and select the SIP trunk on which you want to enable route class signaling.

Step 3 From the **Route Class Signaling Enabled** drop-down list box, choose one of the following options:

- **Default**—This trunk uses the setting from the **Route Class Signaling Enabled** service parameter.
- **Off**—Route class signaling is disabled for this trunk.
- **On**—Route class signaling is enabled for this trunk.

Step 4 Click **Save**.

Enable Route Class Signaling on Gateways

Use this procedure to enable route class signaling on an individual MGCP PRI or MGCP T1/CAS gateway. The configuration for individual gateways overrides the clusterwide service parameter setting.

Before you begin

Follow the Enable Route Class Signaling in the Cluster, on page 218 procedure to use a clusterwide service parameter to set the default route class signaling setting for gateways in the cluster.

Perform the Enable Route Class Signaling on Trunks, on page 219 procedure to configure route class signaling for individual trunks.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Gateways**.

Step 2 Click **Find** and select the gateway on which you want to configure route class signaling.

Step 3 From the **Route Class Signaling Enabled** drop-down list box, choose one of the following options:

- **Default**—This gateway uses the setting from the clusterwide Route Class Signaling Enabled service parameter.
- **Off**—Route class signaling is disabled on this gateway.
- **On**—Route class signaling is enabled on this gateway.

Step 4 If you want to encode voice route class for voice calls, check the **Encode Voice Route Class** check box.

Step 5 Click **Save**.

Configure Signaling Labels for the Hotline Route Class

You must configure a SIP signaling label value for the Hotline route class that you want to use.

Before you begin

Enable route class signaling on your trunks and gateways. For details, see Enable Route Class Signaling in the Cluster, on page 218.

Procedure

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

Step 2 From the **Server** drop-down list, choose the server on which the CallManager service is running.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.

Step 4 Click **Advanced**.

Step 5 In the **SIP Route Class Naming Authority** service parameter field, enter a value to represent the naming authority and context for the labels used in SIP signaling to represent route class. The default value is **cisco.com**.

Step 6 In the **SIP Hotline Voice Route Class Label** service parameter field, enter a label to represent the Hotline Voice route class. The default value is **hotline**.

Step 7 In the **SIP Hotline Data Route Class Label** service parameter field, enter a lable to represent the Hotline Data route class. The default value is **ccdata**.

Step 8 Click **Save**.

Configure the Route Class on Hotline Route Patterns

This procedure describes call routing instructions that are specific to Hotline devices. For more information on how to configure route patterns and translation patterns in your network, see the System Configuration Guide for Cisco Unified Communications Manager.

For each route pattern that you expect to route a Hotline call, you must set the route class for that route pattern to **Hotline Voice** or **Hotline Data**.

Before you begin

Configure Signaling Labels for the Hotline Route Class, on page 220

Before you perform this procedure, it is expected that your network call routing is set up with route patterns.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Route/Hunt** > **Route Patterns**.

Step 2 Click **Find** to display a list of route patterns in your network.

Step 3 For each T1/CAS route pattern that is used to route a Hotline call:

a) From the **Find and List Route Patterns** window, select the route pattern.

b) From the **Route Class** drop-down list box, choose either **Hotline Voice** or **Hotline Data** as the route class for this route pattern.

c) Click **Save**.

Configure the Route Class on Hotline Translation Patterns

Before you begin

Before you perform this procedure, it is expected that you have set up network call routing with route patterns and translation patterns.

Perform the Configure the Route Class on Hotline Route Patterns, on page 221 procedure.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Translation Pattern**.

Step 2 Click **Find** to display the translation patterns in your cluster.

Step 3 For each translation pattern that you want to use on a Hotline number, perform the following steps:

a) From the **Route Class** drop-down list box, select either **Hotline Voice** or **Hotline Data**.

b) Click **Save**.

Configure Hotline to Call Only or Receive Only Task Flow

The configuration example in this task flow describes how to set up a Hotline phone to either place calls only or receive calls only.

Procedure

	Command or Action	Purpose
Step 1	Configure Partitions for Hotline Call Only Receive Only, on page 222	Create two partitions: one should be empty and the other will be assigned to a new CSS.
Step 2	Configure Calling Search Space for Hotline Call Only Receive Only, on page 222	Create a new calling search space and assign one of the new partitions to this CSS. This CSS will contain no other partition.
Step 3	Perform one of the following procedures: • Configure Call Only on Hotline Phone, on page 223 • Configure Receive Only on Hotline Phone, on page 223	If you want to configure call only, assign the empty partition to the phone line. If you want to configure receive only, assign the new CSS to the phone.

Configure Partitions for Hotline Call Only Receive Only

If you want to configure a Hotline phone to either place calls only, or to receive calls only you must create two partitions.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Partitions**.

Step 2 Click **Add New**.

Step 3 Create a new partition.

Step 4 Enter a unique name and description for the partition. For example, **IsolatedPartition**.

Note This partition will not be assigned to any CSS.

Step 5 Click **Save**

Step 6 Repeat steps 2-5 and create a second partition. For example, **EmptyPartition**.

Note This partition will not be assigned to any phone line, but it will be assigned to the NoRouteCSS.

Configure Calling Search Space for Hotline Call Only Receive Only

You must create a calling search and assign one of the two partitions that you've created to the calling search space.

Before you begin

Configure Partitions for Hotline Call Only Receive Only, on page 222

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Calling Search Space**.

Step 2 Click **Add New**.

Step 3 Enter a **Name** and **Description** for the calling search space.

Step 4 From the **Available Partitions** list box, use the arrows to select the **EmptyPartition** partition.

Note Make sure that the partition is assigned to only this calling search space and to no phone lines.

Step 5 Click **Save**

What to do next

Perform one of the following procedures:

- Configure Call Only on Hotline Phone, on page 223
- Configure Receive Only on Hotline Phone, on page 223

Configure Call Only on Hotline Phone

If you have set up your partitions and calling search spaces, perform these steps to configure the Hotline phone to place calls only.

Before you begin

Configure Calling Search Space for Hotline Call Only Receive Only, on page 222

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Phone**.

Step 2 Click **Find** and select the Hotline phone.

Step 3 From the left navigation pane, click the phone line.
The Directory Number Configuration window displays.

Step 4 From the **Route Partition** drop-down list, select the empty partition that you created.

Step 5 Click **Save**.

Configure Receive Only on Hotline Phone

If you have created your calling search space and partitions already, perform these steps to configure the Hotline phone to receive calls only.

Before you begin

Configure Calling Search Space for Hotline Call Only Receive Only, on page 222

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select the Hotline phone.

Step 3 From the **Calling Search Space** drop-down list, select the new CSS that you created in the previous procedure.

Step 4 Click **Save**.

Configure Call Screening with a Calling Search Space

Configure call screening for any intraswitched (line to line) Hotline calls by assigning a unique CSS where the Hotline phones that are in the partitions are only those Hotline phones that you want to be able to call each other.

Note You can also configure call screening by creating translation patterns where each pattern matches each number pattern that you want to either allow or screen.

Procedure

	Command or Action	Purpose
Step 1	Configure Partitions for Hotline Call Screening, on page 224	Create any new partitions for your Hotline phone lines.
Step 2	Create Calling Search Space for Hotline Call Screening, on page 225	Create a new CSS for the screening list. The CSS must include partitions with only those Hotline numbers that you want to allow.
Step 3	Configure Hotline Phones for Call Screening, on page 226	Assign the new CSS and partition to the Hotline phone.

Configure Partitions for Hotline Call Screening

To configure call screening in Hotline phones using a calling search space, you must set up partitions where the only Hotline numbers are those that you want to allow.

Perform the following procedure if you need to create a new partition for your Hotline call screening list.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Partition**.

Step 2 Click **Add New** to create a new partition.

Step 3 In the **Partition Name, Description** field, enter a name for the partition that is unique to the route plan.

Partition names can contain alphanumeric characters, as well as spaces, hyphens (-), and underscore characters (_). See the online help for guidelines about partition names.

Step 4 Enter a comma (,) after the partition name and enter a description of the partition on the same line.

The description can contain up to 50 characters in any language, but it cannot include double quotes ("), percentage sign (%), ampersand (&), backslash (\), angle brackets (<>), or square brackets ([ ]).

If you do not enter a description, Cisco Unified Communications Manager automatically enters the partition name in this field.

Step 5 To create multiple partitions, use one line for each partition entry.

Step 6 From the **Time Schedule** drop-down list, choose a time schedule to associate with this partition.

The time schedule specifies when the partition is available to receive incoming calls. If you choose **None**, the partition remains active at all times.

Step 7 Select one of the following radio buttons to configure the **Time Zone**:

- **Originating Device**—When you select this radio button, the system compares the time zone of the calling device to the **Time Schedule** to determine whether the partition is available is available to receive an incoming call.
- **Specific Time Zone**—After you select this radio button, choose a time zone from the drop-down list. The system compares the chosen time zone to the **Time Schedule** to determine whether the partition is available is available to receive an incoming call.

Step 8 Click **Save**.

Create Calling Search Space for Hotline Call Screening

Perform the following procedure to create a new calling search space for the Hotline phones in the call screening list. Make sure that the only Hotline numbers in the partitions that you select for this CSS are those Hotline numbers that you want to allow in the call screening list. No Hotline numbers that you want to screen out should be included in the partitions for this CSS.

Before you begin

Configure Partitions for Hotline Call Screening, on page 224

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Calling Search Space**.

Step 2 Click **Add New**.

Step 3 In the **Name** field, enter a name.

Ensure that each calling search space name is unique to the system. The name can include up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_).

Step 4 In the **Description** field, enter a description.

The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).

Step 5 From the **Available Partitions** drop-down list, perform one of the following steps:

- For a single partition, select that partition.
- For multiple partitions, hold down the **Control (CTRL)** key, then select the appropriate partitions.

Step 6 Select the down arrow between the boxes to move the partitions to the **Selected Partitions** field.

Step 7 (Optional) Change the priority of selected partitions by using the arrow keys to the right of the **Selected Partitions** box.

Step 8 Click **Save**.

Configure Hotline Phones for Call Screening

If you have already configured calling search spaces and partitions for Hotline call screening, perform this procedure to assign the calling search spaces and partitions to your Hotline phones.

Before you begin

Create Calling Search Space for Hotline Call Screening, on page 225

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select the Hotline phone.

Step 3 From the **Calling Search Space** drop-down list, select the new calling search space that you created for the Hotline call screening list.

Step 4 Click **Save**.

Step 5 From the left navigation pane, click the phone line that you want to use for Hotline calls.
The Directory Number Configuration window displays.

Step 6 From the **Route Partition** drop-down list, select a partition that is included in the calling search space that you set up.

Step 7 Click **Save**.

Hotline Troubleshooting

The following table provides troubleshooting information for cases where hotline calls do not dial correctly.

Table 19: Troubleshooting Hotline—Calls Do Not Dial Correctly

Problem	Solution
Dial tone	Check PLAR configuration.

Problem	Solution
Reorder tone or VCA (intracluster call)	• Check PLAR configuration. • Verify that the phones on both ends are configured as hotline phones.
Reorder tone or VCA (intercluster or TDM call)	• Check PLAR configuration. • Verify that the phones on both ends are configured as hotline phones. • Verify that route class signalling is enabled on trunks. • Check the configuration of route class translations on CAS gateways.

The following table provides troubleshooting information for cases where call screening based on caller ID does not work.

Table 20: Troubleshooting Hotline—Call Screening Based on Caller ID Problems

Problem	Solution
Call not allowed	• Check Caller ID. • Add pattern to screen CSS.
Call allowed	Remove pattern from screen CSS.

CHAPTER 19

Speed Dial and Abbreviated Dial

Speed Dial and Abbreviated Dial Overview

Administrators can configure speed dial numbers for phones to provide speed dial buttons for users or to configure phones that do not have a specific user that is assigned to them. Users use the Cisco Unified Communications Self Care Portal to change the speed dial buttons on their phones. When configuring speed dial entries, some of the speed dial entries are assigned to the speed dial buttons on the IP phone; the remaining speed dial entries are used for abbreviated dialing. When a user starts dialing digits, the AbbrDial softkey displays, and the user can access any speed dial entry by entering the appropriate index (code) for abbreviated dialing.

The speed dial settings on the phone are associated with a physical button on a phone, whereas the abbreviated dial settings are not associated with a phone button.

Programming Speed Dials with Pauses

You can program commas in your speed dials to reach destinations that require a Forced Authorization Code (FAC), Client Matter Code (CMC), dialing pause, or additional digits (such as a user extension, meeting access number, or voice mail password). Within a speed dial, each comma (,) represents either:

- A delimiter that separates the destination call address from an FAC or CMC code
- A pause of 2 seconds prior to sending post-connect DTMF digits

For example, let's say that you want a speed dial that includes FAC and CMC codes, followed by IVR prompts where:

- The called number is 91886543.
- The FAC code is 8787.
- The CMC code is 5656.
- The IVR response is 987989#, which must be entered 4 seconds after the call connects.

In this case, you would program **91886543,8787,5656,,987989#** as the speed dial.

Speed Dial and Abbreviated Dial Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Generate a Phone Feature List, on page 3	Generate a report to identify devices that support the Speed Dial and Abbreviated Dial feature.
Step 2	Configure Speed Dial and Abbreviated Dial, on page 230	Configure Speed Dial and Abbreviated Dial numbers.

Configure Speed Dial and Abbreviated Dial

You can configure a total of 199 speed dial and abbreviated dial settings. Configure speed dial settings for the physical buttons on the phone. Configure abbreviated dial settings for the speed dial numbers that you access with abbreviated dialing. You can configure speed dial entries and abbreviated dial indexes in the same window.

You can also configure post connect DTMF digits as well as FAC , CMC codes as part of the speed dial.

Follow these steps to configure speed dial and abbreviated dial.

Note Not all Cisco Unified IP Phones support abbreviated dialing. See the phone user guide for information.

Before you begin

Generate a Phone Feature List, on page 3

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**. Enter your search criteria and click **Find**. Choose the phone for which you want to configure speed dial buttons.

Step 2 From the **Phone Configuration** window, choose **Add/Update Speed Dials** from the Related Links drop-down list at the top of the window and click **Go**.
The **Speed Dial and Abbreviated Dial Configuration** window appears for the phone.

Step 3 In the **Number** field, enter the number that you want the system to dial when the user presses the speed dial button or the abbreviated dial index for abbreviated dial. You can enter digits 0 through 9, *, #, and +, which is the international escape character. To include dialing pauses in the speed dial, you can enter comma (,) which can act as a delimiter before sending DTMF digits. Each comma you include represents an additional pause of 2 seconds. For example, two commas (,,) represent a pause of 4 seconds. Use of commas also allows you to separate FAC and CMC from the other digits in the speed dial string.

Note Ensure that the following requirements are met when you include FAC and CMC in the speed dial string:

- FAC must always precede CMC in the speed dial string.
- A speed dial label is required for speed dials with FAC and DTMF digits.
- Only one comma is allowed between FAC and CMC digits in the string.

Step 4 In the **Label** field, Enter the text that you want to display for the speed dial button or abbreviated dial number.

Note This field is not available for all the phones. To determine whether this field is available for your Cisco Unified IP Phone, see the user documentation for your phone model.

Step 5 (Optional) If you are configuring a pause in speed dial, you must add a label so that FAC, CMC, and DTMF digits are not displayed on the phone screen.

CHAPTER 20

WebDialer

WebDialer Overview

Cisco WebDialer is installed on a Unified Communications Manager node and used along with Unified Communications Manager. It allows Cisco Unified IP Phone users to make calls from web and desktop applications.

Cisco WebDialer uses hyperlinked telephone numbers in a company directory to allow users to make calls from a web page by clicking on the telephone number of the person that they are trying to call.

In the Cisco Unified Communications Self-Care Portal, from the Directory window, launch Cisco WebDialer using a URL similar to the following:

```
https://<IP address of Cisco Unified Communications Manager server>:8443/webdialer/
Webdialer
```

WebDialer Prerequisites

Cisco WebDialer requires the following software components:

- CTI-supported Cisco Unified IP Phones

WebDialer Configuration Task Flow

Before you begin

- Review WebDialer Prerequisites, on page 233.

Procedure

	Command or Action	Purpose
Step 1	Activate WebDialer, on page 235	Activate the WebDialer service.
Step 2	(Optional) Enable WebDialer Tracing, on page 235	To view WebDialer traces, enable tracing.
Step 3	(Optional) Configure WebDialer Servlet, on page 236	Configure the WebDialer servlet.
Step 4	(Optional) Configure Redirector Servlet, on page 236	If you have multi cluster applications that you develop using HTML over HTTPS interfaces, configure the Redirector servlet.
Step 5	(Optional) Configure WebDialer Application Server, on page 237	To configure Redirector for Cisco WebDialer.
Step 6	(Optional) To Configure Secure TLS Connection to CTI, on page 237, complete the following sub tasks: • Configure WDSecureSysUser Application User, on page 238 • Configure CAPF Profile, on page 141 • Configure Cisco IP Manager Assistant, on page 143	WebDialer uses WDSecureSysUser application user credentials to establish a secure TLS connection to CTI to make calls. Follow these procedures if your system is running in mixed mode.
Step 7	Configure Language Locale for WebDialer , on page 241	Determine which language WebDialer displays by setting the locale field in the Cisco Unified Communications Self Care Portal menu.
Step 8	Configure WebDialer Alarms, on page 241	If there are any issues with the Web Dialer feature it alerts the administrator.
Step 9	(Optional) Configure Application Dial Rules, on page 242	If your application requires multiple clusters, configure application dial rules.
Step 10	Add Users to Standard CCM End User Group, on page 242	Add each WebDialer user to the Standard End User Group for Cisco Unified Communications Manager.
Step 11	(Optional) To Configure Proxy User, on page 243, complete the following sub tasks: • Add a WebDialer End User, on page 243 • Assign Authentication Proxy Rights, on page 243	If you use makeCallProxy HTML over HTTP interface to develop an application for using Cisco WebDialer, create a proxy user.

Activate WebDialer

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Service Activation**.

Step 2 From the **Servers** drop-down list, choose the Unified Communications Manager server that is listed.

Step 3 From **CTI Services**, check the **Cisco WebDialer Web Service** check box.

Step 4 Click **Save**.

Step 5 From Cisco Unified Serviceability, choose **Tools** > **Control Center - Feature Services** to confirm that the CTI Manager service is active and is in start mode.

For WebDialer to function properly, the CTI Manager service must be active and in start mode.

What to do next

Configure Language Locale for WebDialer , on page 241 or complete any or all of the following optional tasks:

- Enable WebDialer Tracing, on page 235
- Configure WebDialer Servlet, on page 236
- Configure Redirector Servlet, on page 236
- Configure WebDialer Application Server, on page 237
- Configure Secure TLS Connection to CTI, on page 237

Enable WebDialer Tracing

To enable Cisco WebDialer tracing, use the Cisco Unified Serviceability Administration application. Trace settings apply to both the WebDialer and Redirector servlets. To collect traces, use the Real Time Monitoring Tool (RTMT).

To access the WebDialer trace files, use the following CLI commands:

- **file get activelog tomcat/logs/webdialer/log4j**
- **file get activelog tomcat/logs/redirector/log4j**

For more information about traces, see the *Cisco Unified Serviceability Administration Guide*.

Before you begin

Activate WebDialer, on page 235

Procedure

Step 1 From the navigation drop-down list of the Cisco Unified Communications Manager application, choose **Cisco Unified Serviceability** and then click **Go**.

Step 2 Choose **Trace** > **Configuration**.

Step 3 From the **Server** drop-down list, choose the server on which to enable tracing.

Step 4 From the **Service Group** drop-down list, choose CTI Services.

Step 5 From the **Service** drop-down list, choose the **Cisco WebDialer Web Service**.

Step 6 In the **Trace Configuration** window, change the trace settings according to your troubleshooting requirements.

Note For more information about WebDialer trace configuration settings, see the *Cisco Unified Serviceability Administration Guide*.

Step 7 Click **Save**.

Configure WebDialer Servlet

The WebDialer servlet is a Java servlet that allows Cisco Unified Communications Manager users in a specific cluster to make and complete calls.

Before you begin

Activate WebDialer, on page 235

Procedure

Step 1 Choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, choose the Cisco Unified Communications Manager server on which to configure Cisco WebDialer web service parameters.

Step 3 From the **Service** drop-down list, choose **Cisco WebDialer Web Service.**

Step 4 Configure the relevant WebDialer Web Service parameters. For detailed information about the parameters, see online help.

Step 5 Restart the Cisco WebDialer Web Service for new parameter values to take effect.

Configure Redirector Servlet

Redirector servlet is a Java-based Tomcat servlet. When a Cisco WebDialer user makes a request, the Redirector servlet looks for that request in the Cisco Unified Communications Manager cluster and redirects the request to the specific Cisco WebDialer server that is located in the Cisco Unified Communications Manager cluster. The Redirector servlet is available only for multi cluster applications that are developed by using HTML over HTTPS interfaces.

Before you begin

Activate WebDialer, on page 235

Procedure

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

Step 2 From the **Server** drop-down list, choose the Cisco Unified Communications Manager server on which to configure the Redirector Servlet.

Step 3 From the **Service** drop-down list, choose the Cisco WebDialer Web Service.

Step 4 Configure the relevant WebDialer Web Service parameters. For detailed information about the parameters, see online help.

Step 5 Restart the Cisco WebDialer Web Service for new parameter values to take effect.

For more information on WebDialer Web Service, see the *Cisco Unified Serviceability Administration Guide*.

Configure WebDialer Application Server

Application server is required to configure the Redirector Servlet. Redirector is required only when you have multiple Unified Communications Manager servers configured in a cluster.

Before you begin

Activate WebDialer, on page 235

Procedure

Step 1 From Cisco Unified Communications Manager Administration Application server window, choose **System** > **Application Server**.

Step 2 From the **Application Server Type** drop-down list, choose a **Cisco WebDialer application server**.
The server appears in the **List of WebDialers** field in the **Service Parameter Configuration** window for the Cisco WebDialer Web Service.

Configure Secure TLS Connection to CTI

WebDialer uses WDSecureSysUser application user credentials to establish a secure TLS connection to CTI to make calls. To configure the WDSecureSysUser application user to establish a secure TLS connection, complete the following tasks.

Before you begin

- Install and configure the Cisco CTL Client. For more information about CTL Client, see Security Guide for Cisco Unified Communications Manager .

- Verify that the Cluster Security Mode in the Enterprise Parameters Configuration window is 1 (mixed mode). Operating the system in mixed mode impacts other security functions in your system. If your system is not currently running in mixed mode, do not switch to mixed mode until you understand these interactions. For more information, see Security Guide for Cisco Unified Communications Manager.
-
- Activate the Cisco Certificate Authority Proxy Function service on the first node.
- Activate WebDialer, on page 235

Procedure

	Command or Action	Purpose
Step 1	Configure WDSecureSysUser Application User, on page 238	Configure a WDSecureSysUser application user.
Step 2	Configure CAPF Profile, on page 141	Configure a CAPF profile for the WDSecureSysUser application user.
Step 3	Configure Cisco IP Manager Assistant, on page 143	Configure service parameters for the Cisco IP Manager Assistant service.

Configure WDSecureSysUser Application User

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **Application User**.

Step 2 Click **Find**.

Step 3 From the **Find and List Application Users Application** window, choose **WDSecureSysUser**.

Step 4 Configure the fields in the **Application User Configuration** window and click **Save**.

What to do next

Configure CAPF Profile, on page 141

Configure CAPF Profile

Certificate Authority Proxy Function (CAPF) is a component that performs tasks to issue and authenticate security certificates. When you create an application user CAPF profile, the profile uses the configuration details to open secure connections for the application.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **Application User CAPF Profile**.

Step 2 Perform one of the following tasks:

- Click **Add New** in the **Find** window, to add a new CAPF profile.

- Click **Copy** for that record in the **Copy** column, to copy an existing profile, and locate the appropriate profile.

To update an existing entry, locate and display the appropriate profile.

Step 3 Configure or update the relevant CAPF profile fields. See the Related Topics section information about the fields and their configuration options.

Step 4 Click **Save**.

Step 5 Repeat the procedure for each application and end user that you want to use security.

CAPF Profile Settings

Setting	Description
Application User	From the drop-down list, choose the application user for the CAPF operation. This setting displays configured application users. This setting does not appear in the **End User CAPF Profile** window.
End User ID	From the drop-down list, choose the end user for the CAPF operation. This setting displays configured end users. This setting does not appear in the **Application User CAPF Profile** window.
Instance ID	Enter 1 to 128 alphanumeric characters (a-z, A-Z, 0-9). The Instance ID identifies the user for the certificate operation. You can configure multiple connections (instances) of an application. To secure the connection between the application and CTIManager, ensure that each instance that runs on the application PC (for end users) or server (for application users) has a unique certificate. This field relates to the CAPF Profile Instance ID for Secure Connection to CTIManager service parameter that supports web services and applications.
Certificate Operation	From the drop-down list, choose one of the following options: • **No Pending Operation**—This message is displayed when no certificate operation is occurring. (default setting) • **Install/Upgrade**—This option installs a new certificate or upgrades an existing locally significant certificate for the application.
Authentication Mode	The authentication mode for the Install/Upgrade certificate operation specifies By Authentication String, which means CAPF installs, upgrades, or troubleshoots a locally significant certificate only when the user or administrator enters the CAPF authentication string in the **JTAPI/TSP Preferences** window.

Setting	Description
Authentication String	To create your own authentication string, enter a unique string. Each string must contain 4 to 10 digits. To install or upgrade a locally significant certificate, the administrator must enter the authentication string in the JTAPI/TSP preferences GUI on the application PC. This string supports one-time use only; after you use the string for the instance, you cannot use it again.
Generate String	To automatically generate an authentication string, click this button. The 4-to10-digit authentication string appears in the **Authentication String** field.
Key Size (bits)	From the drop-down list, choose the key size for the certificate. The default setting is 1024. The other option for key size is 512. Key generation, which is set at low priority, allows the application to function while the action occurs. Key generation may take up to 30 or more minutes.
Operation Completes by	This field, which supports all certificate operations, specifies the date and time by which you must complete the operation. The values that are displayed apply for the first node. Use this setting with the **CAPF Operation Expires in (days)** enterprise parameter, which specifies the default number of days in which the certificate operation must be completed. You can update this parameter at any time.
Certificate Operation Status	This field displays the progress of the certificate operation, such as pending, failed, or successful. You cannot change the information that is displayed in this field.

Configure Cisco IP Manager Assistant

Procedure

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

Step 2 From the **Server** drop-down list, choose the server on which the Cisco IP Manager Assistantservice is active.

Step 3 From the **Service** drop-down list, choose the **Cisco IP Manager Assistant** service.
A list of parameters appears.

Step 4 Navigate to and update the CTIManager Connection Security Flag and CAPF Profile Instance ID for Secure Connection to CTIManager parameters.

To view parameter descriptions, click the parameter name link.

Step 5 Click **Save**.

Step 6 Repeat the procedure on each server on which the service is active.

What to do next

Refer to the Manager Assistant Task Flow for Shared Lines, on page 134 to determine the next task to complete.

Configure Language Locale for WebDialer

Use the Cisco Unified Communications Self Care Portal to configure a language locale for Cisco WebDialer. The default language is English.

Before you begin

Activate WebDialer, on page 235

Procedure

Step 1 From the Cisco Unified Communications Self Care Portal, click the **General Settings** tab.

Step 2 Click **Language**.

Step 3 From the **Display Language** drop-down list, select a language local, and then click **Save**.

Configure WebDialer Alarms

Cisco WebDialer service uses Cisco Tomcat to generate alarms.

Before you begin

Configure Language Locale for WebDialer , on page 241

Procedure

Step 1 From Cisco Unified Serviceability, choose **Alarm** > **Configuration**.

Step 2 From the **Server** drop-down list, choose the server on which to configure the alarm and then click **Go**.

Step 3 From the **Services Group** drop-down list, choose **Platform Services** and then click **Go**.

Step 4 From the **Services** drop-down list, choose **Cisco Tomcat** and then click **Go**.

Step 5 If your configuration supports clusters, check the **Apply to All Nodes** check box to apply the alarm configuration to all nodes in the cluster.

Step 6 Configure the settings, as described in Alarm configuration settings, which includes descriptions for monitors and event levels.

Note For more information about the Alarm configuration settings, see the *Cisco Unified Serviceability Guide*.

Step 7 Click **Save**.

What to do next

Add Users to Standard CCM End User Group, on page 242 or (optionally) if your application requires multiple clusters, see Configure Application Dial Rules, on page 242.

Configure Application Dial Rules

Before you begin

Configure WebDialer Alarms, on page 241

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Dial Rules** > **Application Dial Rules**.

Step 2 In the **Name** field, enter a name for the dial rule.

Step 3 In the **Description** field, enter a description for the dial rule.

Step 4 In the **Number Begins With** field, enter the initial digits of the directory numbers to which you want to apply this application dial rule.

Step 5 In the **Number of Digits** field, enter the length of the dialed numbers to which you want to apply this application dial rule.

Step 6 In the **Total Digits to be Removed** field, enter the number of digits that you want Unified Communications Manager to remove from the beginning of dialed numbers that apply to this dial rule.

Step 7 In the **Prefix With Pattern** field, enter the pattern to prepend to dialed numbers that apply to this application dial rule.

Step 8 For **Application Dial Rule Priority**, choose the dial rule priority as top, bottom, or middle.

Step 9 Click **Save**.

Add Users to Standard CCM End User Group

To use the Cisco WebDialer links in the User Directory windows in Unified Communications Manager, you must add each user to the Standard Unified Communications Manager End Users Group.

Procedure

Step 1 Choose **User Management** > **User Group**.

Step 2 In the **Find and List User Group** window, click **Find**.

Step 3 Click **Standard CCM End Users**.

Step 4 In the **User Group Configuration** window, click **Add End Users to Group**.

Step 5 In the **Find and List Users** window, click **Find**. You can enter criteria for a specific user.

Step 6 To add one or more users to the user group, complete one of the following steps:

- To add one or more users, check the check box beside each user to add and then click **Add Selected**.
- To add all users, click **Select All** and then click **Add Selected**.

The users appear in the Users in Group table of the **User Group Configuration** window.

Configure Proxy User

If you use makeCallProxy HTML over HTTP interface to develop an application for using Cisco WebDialer, create a proxy user. For information about the makeCallProxy interface, see the makeCallProxy section in the *Cisco WebDialer API Reference Guide*.

Before you begin

Add Users to Standard CCM End User Group, on page 242

Procedure

	Command or Action	Purpose
Step 1	(Optional) Add a WebDialer End User, on page 243	Add a new user. If the user exists, you can proceed to the next task.
Step 2	Assign Authentication Proxy Rights, on page 243	Assign authentication proxy rights to an end user.

Add a WebDialer End User

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **End User**.

Step 2 Click **Add New**.

Step 3 Enter a **Last Name**.

Step 4 Enter and confirm a **Password**.

Step 5 Enter and confirm a **PIN**.

Step 6 Complete any remaining fields in the **End User Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 7 Click **Save**.

Assign Authentication Proxy Rights

Perform the following procedure to enable authentication proxy rights for an existing user.

Procedure

Step 1 Choose **User Management** > **User Group**.
The **Find and List User Group** window appears.

Step 2 Click **Find**.

Step 3 Click the **Standard EM Authentication Proxy Rights** link.
The **User Group Configuration** window appears.

Step 4 Click **Add End Users to Group**.
The **Find and List Users** window appears.

Step 5 Click **Find**. You can also add a criteria for a specific user.

Step 6 To assign proxy rights to one or more users, complete one of the following steps:

Step 7 To add a single user, select the user and then click **Add Selected**.

Step 8 To add all users that appear in the list, click **Select All** and then click **Add Selected**.
The user or users appear in the **Users in Group** table in the **User Group Configuration** window.

WebDialer Interactions and Restrictions

WebDialer Interactions

Feature	Interaction
Client Matter Codes (CMC)	When you use CMCs, you must enter the proper code at the tone; otherwise, the IP phone disconnects and the user receives a reorder tone.
Forced Authorization Codes (FAC)	When you use FACs, you must enter the proper code at the tone; otherwise, the IP phone disconnects and the user receives a reorder tone.
ApplicationDialRule table	Cisco WebDialer uses change notifications on the ApplicationDialRule database table to track and use updated dial rules.
Client Matter Codes and Forced Authorization Codes	Web Dialer supports CMCs and FACs in the following ways: • A user can enter the destination number in the dial text box of the WD HTML page or SOAP request, and then manually enter the CMC or FAC on the phone. • A user can enter the destination number followed by the FAC or CMC in the dial text box of the WD HTML page or SOAP request. For example, if the destination number is 5555, the FAC is 111, and the CMC is 222, a user can make a call by dialing 5555111# (FAC), 5555222# (CMC), or 5555111222# (CMC and FAC). **Note** • WebDialer does not handle any validation for the destination number. The phone handles the required validation. • If a user does not provide a code or provides the wrong code, the call will fail. • If a user makes a call from the WebApp with a DN that contains special characters, the call goes successfully after stripping the special characters. The same rules do not work in SOAP UI.

WebDialer Restrictions

Feature	Restrictions
Phones	Cisco WebDialer supports phones that run Skinny Client Control Protocol (SCCP) and Session Initiation Protocol (SIP) that Cisco Computer Telephony Integration (CTI) supports. **Note** Few older phone models do not support Cisco Web Dialer that run SIP.

WebDialer Troubleshooting

Authentication Error

Problem

Cisco WebDialer displays the following message:

Authentication failed, please try again.

Possible Cause

User entered wrong user ID or password.

Solution

Ensure that you use your Unified Communications ManagerCisco Unified Communications Manager user ID and password to log in.

Service Temporarily Unavailable

Problem

Cisco WebDialer displays the following message:

Service temporarily unavailable, please try again later.

Possible Cause

The Cisco CallManager service became overloaded because it has reached its throttling limit of three concurrent CTI sessions.

Solution

After a short time, retry your connection.

Directory Service Down

Problem

Cisco WebDialer displays the following message:

Service temporarily unavailable, please try again later: Directory service down.

Possible Cause

The Cisco Communications Manager directory service may be down.

Solution

After a short time, retry your connection.

Cisco CTIManager Down

Problem

Cisco WebDialer displays the following message:

Service temporarily unavailable, please try again later: Cisco CTIManager down.

Possible Cause

Cisco CTIManager service that is configured for Cisco Web Dialer went down.

Solution

After a short time, retry your connection.

Session Expired, Please Login Again

Problem

Cisco WebDialer displays the following message:

Session expired, please login again.

Possible Cause

A Cisco Web Dialer session expires:

- After the WebDialer servlet gets configured
- If the Cisco Tomcat Service is restarted.

Solution

Log in by using your Unified Communications Manager User ID and Password.

User Not Logged In on Any Device

Problem

Cisco Web Dialer displays the following message:

User not logged in on any device.

Possible Cause

The user chooses to use Cisco Extension Mobility from the Cisco WebDialer preference window but does not get log in to any IP phone.

Solution

- Log in to a phone before using Cisco WebDialer.
- Choose a device from the Cisco WebDialer preference list in the dialog box instead of choosing the option **Use Extension Mobility**.

Failed to Open Device/Line

Problem

After a user attempts to make a call, Cisco WebDialer displays the following message:

User not logged in on any device.

Possible Cause

- The user chose a Cisco Unified IP Phone that is not registered with Unified Communications Manager. For example, the user chooses a Cisco IP SoftPhone as the preferred device before starting the application.
- The user who has a new phone chooses an old phone that is no longer in service.

Solution

Choose a phone that is in service and is registered with Unified Communications Manager.

Destination Not Reachable

Problem

Cisco WebDialer displays the following message on the End Call window:

Destination not reachable.

Possible Cause

- User dialed the wrong number.
- The correct dial rules did not get applied. For example, the user dials 5550100 instead of 95550100.

Solution

Check the dial rules.

CHAPTER 21

Paging

Paging Overview

Unified Communications Manager can be configured to integrate with Cisco Paging Server to provide basic paging services for Cisco Unified IP Phone and a variety of endpoints. The Cisco Paging Server product is offered through the InformaCast Virtual Appliance and offers the following deployment options:

InformaCast Basic Paging

InformaCast Basic Paging provides phone-to-phone live audio paging to individual Cisco IP phones or groups of up to 50 phones simultaneously. InformaCast Basic Paging is free to all Unified Communications Manager customers and all Cisco Business Edition 6000 and Cisco Business Edition 7000 customers.

InformaCast Advanced Notification

InformaCast Advanced Notification is a full-featured emergency notification and paging solution that allows you to reach an unlimited number of Cisco IP phones and a variety of devices and systems with text and audio messages.

Some of the features include:

- Ability to reach analog PA systems and IP speakers
- Support for Cisco Jabber
- 911 emergency call monitoring, recording, and notification
- Dynamic conference call
- Event accountability with message confirmation and reporting
- Implementation with panic buttons
- Building evacuation or lockdown

- Facilities integration (control lighting, door locks)
- Security integration (motion detectors, access, fire)
- General purpose and shift or bell scheduling

Users must purchase a license key to access InformaCast Advanced Notification features.

InformaCast Mobile

InformaCast Mobile is a cloud-based service that allows users to send images, text, and pre-recorded audio to mobile devices running iOS or Android. It also has bi-directional integration with InformaCast Advanced Notification.

Some of the features include:

- The ability to send and receive InformaCast messages via mobile devices running iOS or Android
- Bi-directional integration with InformaCast Advanced Notification
- Message confirmations and read receipts
- No calling or SMS messaging fees

InformaCast Mobile must be purchased direct from Singlewire Software. Please refer to the Singlewire website for addtional details and downloads.

If you have already configured Unified Communications Manager to integrate with InformaCast Advanced Notification, no further configuration of Unified Communications Manager is required.

Paging Prerequisites

Cisco Paging Server is designed to work in a multicast environment. You must configure your network for multicast.

For a list of Cisco Unified IP Phones that support paging, refer to the **Cisco Unified IP Phones** section of the Singlewire Compatibility Matrix at:

http://www.singlewire.com/compatibility-matrix.html.

Basic Paging Configuration Task Flow

Perform the following tasks to configure Cisco Unified Communications Manager to integrate with Cisco Paging Server for an InformaCast Basic Paging deployment.

Before you begin

- Review Paging Prerequisites, on page 250

Procedure

	Command or Action	Purpose
Step 1	Enable SNMP Service, on page 253	Configure SNMP in Cisco Unified Communications Manager.
Step 2	Set Default Codec to G.711, on page 256	Set the default codec to G.711.
Step 3	Configure a Device Pool for Paging, on page 256	Configure a device pool.
Step 4	Configure Route Partition for InformaCast Paging, on page 258	Configure a route partition for Basic Paging.
Step 5	Configure Calling Search Space for InformaCast Paging, on page 258	Configure a calling search space for Basic Paging.
Step 6	Configure CTI Ports for Paging, on page 261	Configure CTI ports.
Step 7	Configure Access Control Group with AXL Access, on page 263	Configure an AXL access control group.
Step 8	Configure Application User for Paging, on page 263	Configure an application user.
Step 9	Enable web access for the phone using one of the following procedures: • Enable Web Access for a Phone, on page 264 • Enable Web Access for Common Phone Profile, on page 265	You can enable web access on a individual phone or use a Common Phone Profile to enable web access for a group of phones that use that profile.
Step 10	Configure Authentication URL, on page 265	Configure the Cisco Unified Communications Manager authentication URL to point to InformaCast so that when InformaCast pushes broadcasts to Cisco Unified IP Phones, the phones will authenticate with InformaCast.

For detailed procedures on how to configure Cisco Unified Communications Manager and Cisco Paging Server, refer to the *InformaCast Virtual Appliance Basic Paging Installation and User Guide* at: http://www.cisco.com/c/en/us/support/unified-communications/paging-server/products-maintenance-guides-list.html

Advanced Notification Paging Task Flow

Perform the following tasks to configure Cisco Unified Communications Manager to integrate with an InformaCast Advanced Notification paging deployment. An Advanced Notification deployment can include the following features:

- InformaCast paging
- CallAware

- PushToTalk
- Legacy paging devices
- Plugins such as Facebook, Twitter and conferencing

Before you begin

- Review Paging Prerequisites, on page 250

Procedure

	Command or Action	Purpose
Step 1	Configure SNMP for Paging, on page 253	Configure SNMP services in Cisco Unified Communications Manager.
Step 2	Configure Media Resources for Legacy Paging, on page 254	Optional. If you want to connect to legacy paging devices, configure a media resource group that includes an MTP.
Step 3	Configure Region for Paging, on page 256	Configure a region for paging with G.711 as the default codec and a device pool for paging devices.
Step 4	Configure Partitions and Calling Search Spaces for Paging, on page 257	Configure partitions and calling search spaces for your paging deployment.
Step 5	Configure CTI Route Points for CallAware, on page 259	If you are deploying CallAware, configure CTI route points for each CallAware redirect.
Step 6	Enable the Built in Bridge using one of the following procedures: • Enable Built in Bridge for Cluster, on page 260 • Enable Built in Bridge for a Phone, on page 260	If you are deploying CallAware, enable the Built in Bridge using a clusterwide service parameter, or on the phone itself. **Note** The settings in the **Phone Configuration** window for an individual phone override the clusterwide service parameter.
Step 7	Configure CTI Ports for Paging, on page 261	Configure CTI ports for InformaCast paging and CallAware redirects.
Step 8	Configure SIP Trunk for Legacy Paging Devices, on page 262	If you are connecting to legacy paging devices, configure a SIP trunk that connects to your legacy devices.
Step 9	Configure Access Control Group with AXL Access, on page 263	Configure an access control group that includes access to the AXL API.
Step 10	Configure Application User for Paging, on page 263	Configure an application user. You must configure different application users for InformaCast, CallAware, and PushToTalk.

	Command or Action	Purpose
Step 11	Perform one of the following procedures: • Enable Web Access for a Phone, on page 264 • Enable Web Access for Common Phone Profile, on page 265	Enable web access for your phones. You can enable web access on an individual phone, or use a Common Phone Profile to enable web access for a group of phones.
Step 12	Configure Authentication URL, on page 265	Configure the Cisco Unified Communications Manager authentication URL to point to InformaCast so that when InformaCast pushes broadcasts to Cisco Unified IP Phones, the phones will authenticate with InformaCast.
Step 13	Configure PushToTalk Service Integration, on page 267	Configure PushToTalk service integration for your Cisco Unified IP Phones.
Step 14	Assign a Directory URI to a Phone, on page 274	Optional. Assign directory URIs to your paging directory numbers. This allows you to implement URI dialing in your paging deployment.

For detailed information on the InformaCast Advanced Notification deployment options, refer to your InformaCast Advanced Notification product documentation. For help, visit Singlewire's website at http://www.singlewire.com.

Configure SNMP for Paging

Perform the following tasks to configure SNMP services in the cluster for either Basic Paging or Advanced Notification deployments.

Procedure

	Command or Action	Purpose
Step 1	Enable SNMP Service, on page 253	Enable the SNMP and other services in the cluster.
Step 2	Create an InformaCast SNMP Community String, on page 254	Configure an SNMP community string.

Enable SNMP Service

To configure paging in either Basic Paging or Advanced Notification deployments, you must enable SNMP on every node in the cluster. In addition, you must enable the following services:

- Cisco CallManager SNMP Service—Enable on all nodes in the cluster.
- Cisco CallManager—Enable on all nodes in the cluster.
- Cisco AXL Web Services—Enable on at least one node.
- Cisco CTIManager—Enable on at least one node.

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Service Activation**.

Step 2 From the **Server** drop-down list, choose the server on which you want to configure SNMP.

Step 3 Check the check boxes that correspond to the **Cisco CallManager SNMP Service** and **Cisco CallManager**.

Step 4 For at least one server in the cluster, check the check boxes that correspond to the **Cisco CTIManager** and **Cisco AXL Web Service** services.

Step 5 Click **Save**.

Step 6 Click **OK**.

Step 7 Repeat the previous steps for all nodes in the cluster.

Create an InformaCast SNMP Community String

Perform this procedure for Basic Paging or Advanced Notification deployments to set up an SNMP community string.

Before you begin

Enable SNMP Service, on page 253

Procedure

Step 1 From Cisco Unified Serviceability, choose **SNMP** > **V1/V2c** > **Community String**.

Step 2 From the **Server** drop-down list, choose a server and click **Find**.

Step 3 Click **Add New**.

Step 4 In the **Community String Name** field, enter `ICVA`.

Step 5 From the **Access Privileges** drop-down list, select **ReadOnly**.

Step 6 Check the **Apply to All Nodes** check box if the check box is active.

Step 7 Click **Save**.

Step 8 Click **OK**.

What to do next

For Basic Paging, go to Set Default Codec to G.711, on page 256

For Advanced Notification, go to Configure Media Resources for Legacy Paging, on page 254

Configure Media Resources for Legacy Paging

If you are implementing an Advanced Notification deployment that includes legacy paging devices, perform these tasks to configure media resources with an MTP so that InformaCast can send broadcasts to your legacy paging devices.

Procedure

	Command or Action	Purpose
Step 1	Create a Media Resource Group, on page 255	Configure a media resource group that includes an MTP.
Step 2	Create a Media Resource Group List, on page 255	Add your media resource group to a media resource group list.

Create a Media Resource Group

Perform this procedure if you are configuring an Advanced Notification deployment that connects to legacy paging devices. You must configure a media resource group that includes an Media Termination Point (MTP) resource. The MTP is required to connect the legacy paging interface.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **Media Resource Group**.

Step 2 Click **Add New**.

Step 3 Enter a **Name** and **Description** for the group.

Step 4 Use the arrows to move **MTP** from the **Available Media Resources** area to the **Selected Media Resources** area.

Step 5 Click **Save**.

What to do next

Create a Media Resource Group List, on page 255

Create a Media Resource Group List

If you have configured a media resource group with an MTP to connect to a legacy paging interface, configure a media resource group that includes your media resource group.

Before you begin

Create a Media Resource Group, on page 255

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **Media Resource Group List**.

Step 2 Click **Add New**.

Step 3 Enter a **Name** and **Description** for the list.

Step 4 Use the arrows to move the media resource group that you created to the **Selected Media Resource Groups** area.

Step 5 Click **Save**.

What to do next

Set Default Codec to G.711, on page 256

Configure Region for Paging

For either Basic Paging or Advanced Notification deployments, you must set up a region for your paging deployment.

Procedure

	Command or Action	Purpose
Step 1	Set Default Codec to G.711, on page 256	Create a region that uses the G.711 codec for calls to other regions.
Step 2	Configure a Device Pool for Paging, on page 256	Set up a device pool for paging and assign the region that you created to that device pool.

Set Default Codec to G.711

You must create an InformaCast region that uses G.711 as the default codec for calls to other regions.

Before you begin

Configure SNMP for Paging, on page 253

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Region Information** > **Region**.
Step 2 Click **Add New**.
Step 3 In the **Name** field, enter `ICVA`.
Step 4 Click **Save**.
Step 5 In the **Regions** text box, select all regions by pressing the **CTRL** key and clicking all of the selected regions.
Step 6 From the **Maximum Audio Bit Rate** drop-down list, select **64 kbps (G.722, G.711)**.
Step 7 From the **Maximum Session Bit Rate for Video Calls** column click the **None** radio button.
Step 8 Click **Save**.

Configure a Device Pool for Paging

Perform this procedure for both Basic Paging and Advanced Notification deployments to configure a device pool for your paging deployment.

Before you begin

Set Default Codec to G.711, on page 256

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Device Pool**.

Step 2 Click **Add New**.

Step 3 In the **Device Pool Name** field, enter `ICVA`.

Step 4 From the **Cisco Unified Communications Manager Group** drop-down list, select the group that contains the Cisco Unified Communications Manager cluster with which the InformaCast Virtual Appliance will communicate.

Step 5 From the **Date/Time Group** drop-down list, select a date/time group. Select **CMLocal** unless you are performing dialing restrictions by the time of day.

Step 6 From the **Region** drop-down list, choose **ICVA**.

Step 7 If you have an Advanced Notification deployment that includes legacy paging devices, from the **Media Resource Group List** drop-down list box, select the media resource group list that you configured to include an MTP.

Step 8 From the **SRST Reference** drop-down list, select **Disable**.

Step 9 Click **Save**.

Configure Partitions and Calling Search Spaces for Paging

Perform the following tasks to configure a partition and calling search space (CSS) for paging as follows:

- For Basic Paging deployments, create a single partition and CSS for InformaCast paging.
- For Advanced Notification deployments, create a single partition and CSS for InformaCast paging. If you are deploying CallAware, you must also configure a unique partition and CSS combination for each CallAware redirect.

Procedure

	Command or Action	Purpose
Step 1	Configure Route Partition for InformaCast Paging, on page 258	Configure a route partition for InformaCast paging.
Step 2	Configure Calling Search Space for InformaCast Paging, on page 258	Configure a calling search space for InformaCast paging.
Step 3	Configure Route Partitions for CallAware, on page 258	**Optional**. If you are deploying CallAware in an Advanced Notification deployment, configure route partitions for each CallAware redirect.
Step 4	Configure Calling Search Spaces for CallAware, on page 259	**Optional**. If you are deploying CallAware in an Advanced Notification deployment,

	Command or Action	Purpose
		configure calling search spaces for each CallAware redirect.

Configure Route Partition for InformaCast Paging

Create a route partition for InformaCast paging in either a Basic Paging or Advanced Notification deployment.

Before you begin

Configure a Device Pool for Paging, on page 256

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Route Partitions**.

Step 2 Click **Add New**.

Step 3 In the **Name** field, enter the following name and description for the partition: `ICVA-CTIOutbound,ICVA-Do not add to any phone CSS`.

Step 4 Click **Save**.

Configure Calling Search Space for InformaCast Paging

Perform this procedure to configure a calling search space for InformaCast paging in either a Basic Paging or Advanced Notification deployment.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Calling Search Space**.

Step 2 Click **Add New**.

Step 3 In the **Name** field, enter `ICVA`.

Step 4 In the **Available Partitions** list box, use the arrows to move the following partitions to the **Selected Partitions** list box.

- The partition that you created for InformaCast paging
- The partitions that contain your users' extensions and any analog paging extensions

Step 5 Click **Save**.

Configure Route Partitions for CallAware

If you are deploying CallAware in an Advanced Notification paging deployment. perform this procedure to set up a unique partition for each CallAware redirect.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Partition**.

Step 2 Click **Add New**.

Step 3 In the **Name** field, enter the following name and description for the partition: **`ICVA-Redirect1-CA,ICVA Redirect 1 CallAware`**.

Step 4 Click **Save**

Step 5 For each additional call redirect, create a new partition, incrementing the redirect number that you enter in the **Name** field. For example, **`ICVA-Redirect2-CA`**.

Configure Calling Search Spaces for CallAware

If you are deploying CallAware in an Advanced Notification deployment, you must configure a unique calling search space (CSS) for each CallAware redirect.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Calling Search Space**.

Step 2 Click **Add New**.

Step 3 In the **Name** field, enter **`ICVA-Redirect1-CA`**.

Step 4 Click **Save**.

Step 5 Repeat the above steps until you have a separate CSS for each call redirect. For each CSS, increment the redirect number in the **Name** field. For example, **`ICVA-Redirect2-CA`**.

Configure CTI Route Points for CallAware

Perform this procedure only if you have an Advanced Notification paging deployment that includes CallAware. You must configure CTI route points for each CallAware redirect.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **CTI Route Point**.

Step 2 Click **Add New**.

Step 3 In the **Device Name** field, enter a name for your route point. This name must match the corresponding route point name that you configure in the InformaCast Virtual Appliance.

Step 4 Enter a **Description** for the route point. For example, **`ICVA Redirect 1 CallAware`**.

Step 5 From the **Device Pool** drop-down list box, choose **ICVA**.

Step 6 From the **Calling Search Space** drop-down list box, choose the calling search spaces that you set up for this CallAware redirect.

Step 7 Click **Save**.

Step 8 In the **Association** area, click **Line [1] - Add a new DN**.

Step 9 In the **Directory Number** field, enter the directory number that CallAware will monitor.

Step 10 From the **Route Partition** drop-down list box, select the partition that you set up for this CallAware redirect.

Step 11 In the **Call Forward and Call Pickup Settings** area, leave the **Forward All** field empty.

Step 12 For each of the remaining call forward options, configure the following settings:

a) In the **Destination** text box, enter the directory number to which you want to redirect calls.
b) From the **Calling Search Space** drop-down list box, select the CSS that you created for this redirect.
c) Click **Save**.

Step 13 Repeat this procedure for each CallAware redirect.

Note Perform one of the following procedures to enable the Built in Bridge on the phone:

- Enable Built in Bridge for Cluster
- Enable Built in Bridge for a Phone

Enable Built in Bridge for Cluster

Perform this procedure if you have an Advanced Notification paging deployment that includes CallAware. When you use this procedure to enable the Built in Bridge using a clusterwide service parameter, the Built in Bridge default setting for all phones in the cluster is changed to enabled. However, the Built in Bridge setting in the **Phone Configuration** window for an individual phone overrides the clusterwide setting.

Procedure

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

Step 2 From the **Server** drop-down list, choose the server on which the CallManager service is running.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.

Step 4 Set the **Builtin Bridge Enable** service parameter to **On**.

Step 5 Click **Save**.

Enable Built in Bridge for a Phone

If you have an Advanced Notification paging deployment that uses CallAware, perform this procedure to enable an individual phone's Built in Bridge.

You can also use a service parameter to set the Built in Bridge clusterwide default setting to enabled. However, an individual phone's Built in Bridge setting in the **Phone Configuration** window overrides the clusterwide service parameter default.

Before you begin

Enable Built in Bridge for Cluster, on page 260

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** to select the agent phone.

Step 3 From the **Built in Bridge** drop-down list, choose one of the following options:

- **On**—The Built in Bridge is enabled.
- **Off**—The Built in Bridge is disabled.
- **Default**—The setting of the clusterwide **Builtin Bridge Enable** service parameter is used.

Step 4 Click **Save**.

What to do next

Configure CTI Ports for Paging, on page 261

Configure CTI Ports for Paging

Perform this procedure to configure CTI ports for your paging deployment. The number of CTI ports that you need depends on your deployment type and your applications' usage:

- For Basic Paging deployments, you must create a minimum of two CTI ports for InformaCast paging.
- For Advanced Notification deployments, you must create a minimum of two CTI ports for InformaCast paging and two CTI ports for CallAware.

Before you begin

For Basic Paging, Configure Calling Search Space for InformaCast Paging, on page 258

For Advanced Notification, Enable Built in Bridge for a Phone, on page 260

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Add New**.

Step 3 From the **Phone Type** drop-down list, choose **CTI Port**.

Step 4 In the **Device Name** field, enter a name for the CTI Port. For example, `ICVA-IC-001` for an InformaCast port or `ICVA-CA-001` for a CallAware port.

Step 5 In the **Description** field, enter a description for the port. For example, `InformaCast Recording Port` or `CallAware CTI port for Call Monitoring`.

Step 6 From the **Device Pool** drop-down list, select **ICVA**.

Step 7 From the **Calling Search Space** drop-down list, select **ICVA**.

Step 8 From the **Device Security Profile** drop-down list, select **Cisco CTI Port - Standard SCCP Non-Secure Profile**.

Step 9 Click **Save**.

Step 10 Click **OK**.

Step 11 In the left association area, click **Line [1] - Add a new DN**.

Step 12 In the **Directory Number** field, enter a directory number. This directory number should not be used for any purpose other than making paging calls. It should not be assigned to a phone and should not be within a direct-inward-dialing range.

Step 13 In the **Route Partition** drop-down list, select one of the following ports:

- For InformaCast ports, select **ICVA-CTIOutbound**.
- For CallAware ports, select the CallAware partitions. For example, **ICVA-Redirect1-CA**.

Step 14 In the **Display (Internal Caller ID)** text box, enter `InformaCast` or `CallAware` depending on which type of port you are configuring.

Step 15 In the **ASCII Display (Internal Caller ID)** text box, enter `InformaCast` or `CallAware` depending on which type of port you are configuring.

Step 16 If you have an Advanced Notification deployment that includes CallAware, from the **Monitoring Calling Search Space** drop-down list box, select the CSS that you created for the CallAware redirect. For example, **ICVA-Redirect1-CA**.

Step 17 Click **Save**.

Step 18 Repeat this procedure for each CTI port that you need.

What to do next

For Basic Paging, go to

For Advanced Notification, go to Configure SIP Trunk for Legacy Paging Devices, on page 262

Configure SIP Trunk for Legacy Paging Devices

Perform this procedure if you have an Advanced Notification paging deployment and you want to connect to legacy paging devices. You must configure a SIP trunk to enable the Legacy Paging Interface.

Before you begin

Configure CTI Ports for Paging, on page 261

Procedure

Step 1 In Cisco Unified CM Administration, choose **Device** > **Trunk**.

Step 2 Click **Add New**.

Step 3 From the **Trunk Type** drop-down list box, select **SIP Trunk**.

Step 4 Click **Next**.

Step 5 In the **Device Name** text box, enter `ICVA`.

Step 6 In the **Description**, field enter a description for the trunk.

Step 7 From the **Device Pool** drop-down menu, select **ICVA**.

Step 8 From the **Calling Search Space** drop-down list box, select **ICVA**.

Step 9 In the **SIP Information** area, enter the InformaCast Virtual Appliance IP address in the **Destination Address** text box.

Step 10 From the **SIP Trunk Security Profile** drop-down list box, select **Non Secure SIP Trunk Profile**.

Step 11 From the **SIP Profile** drop-down list box, select **Standard SIP Profile**.

Step 12 Click **Save**.

What to do next

Configure Access Control Group with AXL Access, on page 263

Configure Access Control Group with AXL Access

Perform this procedure for either Basic Paging or Advanced Notification deployments to create an access control group that includes AXL access.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Access Control Group**.

Step 2 Click **Add New**.

Step 3 In the **Name** text box, enter `ICVA User Group`.

Step 4 Click **Save**.

Step 5 From the **Related Links** drop-down list, select **Back to Find/List** and click **Go**.

Step 6 In the **Roles** column, click the **i** icon that corresponds to the new access control group.

Step 7 Click **Assign Role to Group**.

Step 8 Click **Find**.

Step 9 Select **Standard AXL API Access** check box, and click **Add Selected**.

Step 10 Click **Save**.

Configure Application User for Paging

Perform this procedure to configure an application user for either Basic Paging or Advanced Notification deployments as follows:

- For Basic Paging, configure an InformaCast application user.
- For Advanced Notification, if you are deploying the InformaCast, CallAware, and PushToTalk features, you must create a separate application user for each feature.

Before you begin

Configure Access Control Group with AXL Access, on page 263

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **Application User**.

Step 2 Click **Add New**.

Step 3 In the **User ID** text box, enter a user ID for the application user. For example, `ICVA InformaCast`, `ICVA CallAware`, or `ICVA PushToTalk`.

Step 4 Enter a password in the **Password** and **Confirm Password** fields.

Step 5 In the **Available Devices** list box, click the CTI ports that you created for your deployment and use the arrows to move the devices to the **Controlled Devices** list box. For example, select **ICVA-IC-001** for InformaCast and **ICVA-CA-001** for CallAware.

Step 6 Click the **Add to Access Control Group**.

Step 7 Click **Find**.

Step 8 Check the following check boxes (unless otherwise indicated, select these permissions for all application users):

- ICVA User Group
- Standard CTI Allow Call Monitoring—for CallAware or PushToTalk application users only
- Standard CTI Allow Control of All Devices
- Standard CTI Allow Control of Phones supporting Connected Xfer and conf
- Standard CTI Allow Control of Phones supporting Rollover Mode
- Standard CTI Enabled

Step 9 Click **Add Selected**.

Step 10 Click **Save**.

Step 11 If you have an Advanced Notification deployment, repeat all the steps in this procedure until you have configured application users for InformaCast, CallAware, and PushToTalk.

What to do next

Perform one of the following procedures to enable web access on your phones:

- Enable Web Access for a Phone, on page 264
- Enable Web Access for Common Phone Profile, on page 265

Enable Web Access for a Phone

Perform this procedure in Basic Paging or Advanced Notification deployments to enable web access for a Cisco Unified IP Phone. You can also use a Common Phone Profile to enable web access for a group of phones that use that profile. For details, see Enable Web Access for Common Phone Profile, on page 265.

Before you begin

Configure Application User for Paging, on page 263

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select the phone for which you want to enable web access.

Step 3 In the **Product Specific Configuration Layout** area, from the **Web Access** drop-down list, select **Enabled**.

Step 4 Click **Save**.

What to do next

For Basic Paging or Advanced Notification , go to Configure Authentication URL, on page 265

Enable Web Access for Common Phone Profile

Perform this procedure in either Basic Paging or Advanced Notification deployments to enable web access for a group of Cisco Unified IP Phones that use a Common Phone Profile. You can also enable web access on an individual phone. For details, see Enable Web Access for a Phone, on page 264.

Before you begin

Configure Application User for Paging, on page 263

Procedure

Step 1 From Cisco Unified CM Administration, chooseI **Device** > **Device Settings** > **Common Phone Profile**.

Step 2 Click **Find** and select the profile that applies to the group of phones for which you want to enable web access.

Step 3 In the **Product Specific Configuration Layout** area, from the **Web Access** drop-down list, select **Enable**.

Step 4 Click **Save**.

Step 5 Click **Apply Config** to reset the phones that use the Common Phone Profile.

Step 6 Click **OK**.

What to do next

For Basic Paging or Advanced Notification, go to Configure Authentication URL, on page 265

Configure Authentication URL

Perform the following tasks to configure an authentication URL that points to InformaCast so that when InformaCast pushes broadcasts to Cisco Unified IP Phones, the phones authenticate with InformaCast instead of Unified Communications Manager.

Procedure

	Command or Action	Purpose
Step 1	Set Authentication URL, on page 266	Set the Unified Communications Manager authentication URL to point InformaCast.
Step 2	Reset Your Phones, on page 266	Reset the phones in your deployment so that your phones use the new settings.
Step 3	Test Your Phones, on page 267	Verify that the phones in your deployment use the new authentication URL settings.

Set Authentication URL

Perform this procedure to set the Unified Communications Manager authentication URL to point to the InformaCast Virtual Appliance.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 Scroll to the **Phone URL Parameters** area, and in the **URL Authentication** field, enter **`http://<IP Address>:8081/InformaCast/phone/auth`** where <IP Address> is the IP Address of the InformaCast Virtual Appliance.

Note Make a note of the existing URL in the **URL Authentication** field. You may need this when you configure InformaCast. See your InformaCast documentation for details.

Step 3 Scroll to the **Secured Phone URL Parameters** area, and in the **Secured Authentication URL** field, enter **`http://<IP Address>:8081/InformaCast/phone/auth`** where <IP Address> is the IP Address of the InformaCast Virtual Appliance.

Step 4 Click **Save**.

Reset Your Phones

After you set the authentication URL to point to the InformaCast Virtual Applicance, you must reset your phones. This procedures describes how to manually reset the phones in device pools. There are many methods for resetting your phones. For example, you can also use Bulk Administration Tool to schedule the reset during off hours. See the *Cisco Unified Communications Manager Bulk Administration Guide* for information on the Bulk Administration Tool.

Before you begin

Set Authentication URL, on page 266

Procedure

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

Step 2 In the **From Phone Where** box, select **Device Pool**.

Step 3 Set the other drop-down menus and field items to settings that will bring up the device pools that you contain your phones.

Step 4 Click **Find**.

Step 5 Select the device pools that you want to reset.

Step 6 Click **Reset Selected**.

Step 7 Click **Reset**.

What to do next

Test Your Phones, on page 267

Test Your Phones

Verify that your phones are authenticating with the InformaCast Virtual Appliance.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Use the drop-down list and fields in the Find and List Phones window to filter your search for a phone that should be using the new authentication URL, and click **Find**.

Step 3 For the phone that should be using the new settings, click the IP Address link in the **IPv4 Address** column.

Step 4 Click Network Configuration.
The Network Configuration page appears.

Step 5 Verify that the **Authentication URL** field displays the InformaCast Virtual Appliance IP address that you entered for the **URL Authentication** enterprise parameter. If the correct URL does not appear, you will need to set the authentication URL.

Configure PushToTalk Service Integration

If you have already configured an Advanced Notification paging deployment in Cisco Unified Communications Manager, perform the following tasks to add PushToTalk services.

Before you begin

If you have not done so, configure an application user specifically for PushToTalk. For details, see Configure Application User for Paging, on page 263

Procedure

	Command or Action	Purpose
Step 1	Create a PushToTalk Service Definition, on page 268	Set up the PushToTalk phone service in Cisco Unified Communications Manager.

	Command or Action	Purpose
Step 2	Configure PhoneGroup Parameter for PushToTalk, on page 269	Configure the Phone Group parameter for the PushToTalk service.
Step 3	Configure SkipConfirm Parameter for PushToTalk, on page 269	Configure the Skip Confirmation parameter for the PushToTalk service.
Step 4	Configure Directory Number Parameter for PushToTalk, on page 270	Configure the Directory Number Parameter for the PushToTalk service.
Step 5	Assign Phones to PushToTalk Service, on page 271	Configure your phones for the PushToTalk service.
Step 6	Configure Wireless Phones for PushToTalk, on page 272	Configure wireless phones for PushToTalk services.
Step 7	Install Audio Files for PushToTalk, on page 273	Download PushToTalk audio files from the InformaCast Virtual Appliance and upload them to Cisco Unified Communications Manager.

Create a PushToTalk Service Definition

If you want to enable PushToTalk services, you must create a service definition for PushToTalk to be able to display interactive content with text and graphics on Cisco Unified IP Phones.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Phone Services**.

Step 2 Click **Add New**.

Step 3 Enter a **Service Name** for the service. For example, **`PushToTalk`**.

Step 4 Enter a **Service Description** for the service. For example, **`Intercom Functionality`**.

Step 5 In the Service URL text box, enter **`http://<InformaCast Virtual Appliance IP Address>:8085/PushToTalk/PhoneMenu.action?sep=#DEVICENAME#`**.

Step 6 Check the **Enable** check box.

Step 7 Click **Save**.

What to do next

Perform the following procedures to configure the parameters by which PushToTalk can be customized for each phone:

- Configure PhoneGroup Parameter for PushToTalk, on page 269
- Configure SkipConfirm Parameter for PushToTalk, on page 269
- Configure Directory Number Parameter for PushToTalk, on page 270

Configure PhoneGroup Parameter for PushToTalk

Use this procedure to configure the PhoneGroup parameter, which allows you to limit a phone subscribed to this service's parameter to only displaying a subset of the phone groups available.

Before you begin

Create a PushToTalk Service Definition, on page 268

Procedure

Step 1 In Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Phone Services**.

Step 2 Click **Find** and select the service that you created for PushToTalk.

Step 3 Click the **New Parameter** button.

Step 4 In the **Parameter Name** text box, enter **`PhoneGroupIds`**.

Step 5 In the **Parameter Display Name** text box, enter **`Phone Group Default`**.

Step 6 In the Parameter Description text box, enter text similar to "**`If you wish to limit the phone to less than all phone groups, enter the phone group ID(s).`**"

Step 7 Uncheck the **Parameter is Required** check box.

Step 8 Uncheck the **Parameter is a Password (mask contents)** check box.

Step 9 Click **Save**.

Step 10 Close the **Configure Cisco IP Phone Service Parameter** window.

Step 11 Click **Update Subscriptions**.

Step 12 Click **Save**.

What to do next

Configure SkipConfirm Parameter for PushToTalk, on page 269

Configure SkipConfirm Parameter for PushToTalk

Use this procedure to configure the SkipConfirm parameter for PushToTalk. The SkipConfirm parameter allows you to (in conjunction with the PhoneGroupIds parameter) immediately enter a PushToTalk session by pressing the side button on wireless phones or the **Services** button on desktop phone.

Before you begin

Configure PhoneGroup Parameter for PushToTalk, on page 269

Procedure

Step 1 In Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Phone Services**.

Step 2 Click **Find** and select the phone service that you created for PushToTalk.

Step 3 Click **New Parameter**.

Step 4 In the **Parameter Name** text box, enter **`SkipConfirm`**.

Step 5 In the **Parameter Display Name** text box, enter `SkipConfirmation`.

Step 6 In the **Default Value** text box, enter `N`.

Step 7 In the **Parameter Description** text box, enter text similar to, "`Skip (Y/N) the confirmation page when limiting to only one specific PushToTalk phone group.`"

Step 8 Uncheck the **Parameter is Required** check box.

Step 9 Uncheck the **Parameter is a Password (mask contents)** check box.

Step 10 Click **Save**.

Step 11 Close the **Configure Cisco IP Phone Service Parameter** window.

Step 12 Click the **Update Subscriptions** button.

Step 13 Click **Save**.

What to do next

Configure Directory Number Parameter for PushToTalk, on page 270

Configure Directory Number Parameter for PushToTalk

Use this procedure to configure the Directory Number parameter for PushToTalk services in an Advanced Notification deployment. The Directory Number parameter allows you to immediately enter a PushToTalk session by pressing the side button on wireless phones or the **Services** button on desktop phone.

Before you begin

Configure SkipConfirm Parameter for PushToTalk, on page 269

Procedure

Step 1 In Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Phone Services.**

Step 2 Click **Find** and select the service that you set up for PushToTalk.

Step 3 Click the **New Parameter** button.

Step 4 In the **Parameter Name** text box, enter `DN`.

Step 5 In the **Parameter Display Name** text box, enter `Directory Number`.

Step 6 In the **Parameter Description** text box, enter text similar to "`If skipping confirmation page when limiting to a specific phone group, use this directory number when starting a one-to-one or intercom session.`"

Step 7 Uncheck the **Parameter is Required** check box.

Step 8 Uncheck the **Parameter is a Password (mask contents)** check box.

Step 9 Click **Save**.

Step 10 Close the **Configure Cisco IP Phone Service Parameter** window.

Step 11 Click the **Update Subscriptions** button.

Step 12 Click **Save**.

What to do next

Assign Phones to PushToTalk Service, on page 271

Assign Phones to PushToTalk Service

Use this procedure to assign a phone to the PushToTalk service and to customize how the Phone Group, Skip Confirmation and Directory Number parameters are set when the user initiates a PushToTalk session.

Before you begin

Configure Directory Number Parameter for PushToTalk, on page 270

Procedure

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

Step 2 Click **Find** and select the phone that you want to use with PushToTalk.
The **Phone Configuration** window opens.

Step 3 From the **Related Links** drop-down list box, select **Subscribe/Unsubscribe** and click **Go**.
The **Cisco IP Phone Services** window opens.

Step 4 From the **Select a Service** drop-down list box, select **PushToTalk** and click **Next**.

Step 5 Leave the **Service Name** and **ASCII Service Name** fields with their default values.

Step 6 If you want to limit the phone to specific phone groups for PushToTalk, in the **Phone Group Default** text box, enter the phone group IDs that you want to include.

Note If you leave the field empty, the **Phone Groups** menu appears whenever you initiate a PushToTalk session.

Step 7 If you want the phone to skip the confirmation screen when entering a PushToTalk session, enter Y in the **Skip Confirmation** field.

Note If you enter N, the Start confirmation appears whenever you initiate a PushToTalk session.

Step 8 If you want the phone to enter a one-to-one or intercom session immediately, in the **Directory Number** text box, enter the directory number for the one-to-one or intercom session.

Note If you leave the field empty, you must enter the directory number in the phone interface when you initiate a one-to-one or intercom PushToTalk session.

Step 9 Click **Subscribe**.

Step 10 Close the **Cisco IP Phone Services** window.

Step 11 Click **Reset**.
The **Device Reset** window appears.

Step 12 Click **Reset**.

What to do next

Configure Wireless Phones for PushToTalk, on page 272

Configure Wireless Phones for PushToTalk

Use this procedure to assign PushToTalk services to a wireless phone and to configure how the Phone Group, Skip Confirmation and Directory Number parameters are set when PushToTalk feature is invoked from a wireless phone.

Before you begin

Assign Phones to PushToTalk Service, on page 271

Procedure

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

Step 2 Click **Find** and select the wireless phone.
The **Phone Configuration** window appears.

Step 3 In the **Application URL** text box, enter a URL to configure the Phone Group, Skip Confirmation and Directory Number parameters and control how PushToTalk behaves when the feature is invoked from the phone. Refer to the following table for the URLs.

Desired Behavior for PushToTalk	URL to Enter
Phone Group menu prompts user to select a phone group.	`http://<InformaCast IP Address>:8085/PushToTalk/PhoneMenu.action?sep=#DEVICENAME#`
Bypass the Phone Group menu. The phone group is limited to the phone groups in the URL.	`http://<InformaCast IP Address>:8085/PushToTalk/PhoneMenu.action?sep=#DEVICENAME#;PhoneGroupIds=x` where **x** represents the phone group. For example, `PhoneGroupIds=3,5`.
Bypass Phone Group menu and bypass the confirmation screen for a standard PushToTalk session.	`http://<InformaCast IP Address>:8085/PushToTalk/PhoneMenu.action?sep=#DEVICENAME#;PhoneGroupIds=x;SkipConfirm=Y` where **x** represents the phone group. For example, `PhoneGroupIds=3,5`
Bypass Phone Group menu, confirmation screen, and directory number selection for a one-to-one or intercom PushToTalk session.	`http://<InformaCast IP Address>:8085/PushToTalk/PhoneMenu.action?sep=#DEVICENAME#;PhoneGroupIds=x;SkipConfirm=Y;DN=xx` where **x** represents the phone group and **xx** represents the directory number for the one-to-one or intercom PushToTalk session. For example, `PhoneGroupIds=3,5;SkipConfirm=Y;DN=2004`

Step 4 Click **Save**.

Step 5 Click **Reset**.
The **Device Reset** window appears.

Step 6 Click **Reset**.

What to do next

Install Audio Files for PushToTalk, on page 273

Install Audio Files for PushToTalk

Perform this procedure to install the following audio files that PushToTalk uses to indicate session activity:

- PTT_start.raw
- PTT_accept.raw
- PTT_change.raw
- PTT_end.raw
- PTT_active.raw

Before you begin

Perform one of the following procedures to set up the PushToTalk service on your phones:

- Assign Phones to PushToTalk Service, on page 271
- Configure Wireless Phones for PushToTalk, on page 272

Procedure

Step 1 Use an SFTP client to access the five PushToTalk audio files from the following default location on the InformaCast Virtual Appliance: `/usr/local/singlewire/PushToTalk/web/sounds`.

Step 2 Use the SFTP client to download the files to a location that the Cisco Unified Communications Manager TFTP server can access.

Step 3 Log in to Cisco Unified Operating System Administration and choose **Software Upgrades** > **TFTP File Management**.

Step 4 Click **Upload File**.

Step 5 **Browse** to the location where you saved the PushToTalk audio files.

Step 6 For each audio file, perform the following steps:

a) Select the audio file.
b) In the **Directory** field, enter the subdirectory where the file will reside.
c) Click **Upload File**.

Step 7 Restart the TFTP service by performing the following steps:

a) From Cisco Unified Serviceability, choose **Tools** > **Control Center - Feature Services**.
b) From the **Server** drop-down list box, select the server on which the TFTP service is running.
c) Click the **Cisco Tftp** radio button.
d) Click the **Restart** button.

e) Click **OK**.

What to do next

Optional. Assign a Directory URI to a Phone, on page 274

Assign a Directory URI to a Phone

Use this procedure if you want to assign a directory URI to a phone, thereby allowing you to use URI dialing for that phone.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select the phone for which you want to assign a directory URI.
The **Phone Configuration** window appears.

Step 3 In the **Association Information** pane that appears on the left, click the phone line.
The **Directory Number Configuration** window appears.

Step 4 In the **Directory URIs** section, enter a directory URI in the **URI** text box.

Step 5 Click **Save**.

CHAPTER 22

Intercom

Intercom Overview

Intercom is a type of phone line that combines the functionality of a traditional line and a speed dial. With an intercom line, a user can call the intercom line of another user, which answers automatically to one-way audio whisper. The recipient can then acknowledge the whispered call and initiate a two-way intercom call.

You can use an intercom line to dial any other intercom line in the intercom partition, or you can preconfigure the line to target an intercom line outside the intercom partition.

Intercom allows a user to place a call to a predefined target. The called destination answers the call automatically in speakerphone mode with mute activated. This sets up a one-way voice path between the initiator and the destination, so the initiator can deliver a short message, regardless of whether the called party is busy or idle.

To ensure that the voice of the called party does not get sent back to the caller when the intercom call is automatically answered, Unified Communications Manager implements whisper intercom. Whisper intercom ensures that only one-way audio exists from the caller to the called party. The called party must manually press a key to talk to the caller.

An auto-answer tone indicates the beginning of the whisper intercom state for both the sender and the recipient.

Intercom and Default Devices

Each intercom line needs a default device. The intercom line is displayed only on the designated default device.

When the administrator assigns an intercom line to a device, the system sets the device as the default device for the intercom line if not set previously. The administrator can modify the default device for the intercom line. When the administrator changes the default device to a different device, the intercom line gets removed from the original device, even though the intercom line may still be assigned to the original device.

You can assign an intercom line to a device profile. Only when a user uses a device profile to log in to the default device that matches the default device of the intercom line does the intercom line become available. Otherwise, no intercom line is displayed when the user logs in.

Intercom Prerequisites

The intercom feature has the following system requirements:

- Cisco Unified IP Phones Firmware Release 8.3(1) or later

Intercom Configuration Task Flow

Before you begin

- Review Intercom Prerequisites, on page 276.

Procedure

	Command or Action	Purpose
Step 1	Configure Intercom Partition, on page 276	To add a new Intercom partition or configure an existing partition.
Step 2	Configure an Intercom Calling Search Space, on page 278	To add a new Intercom Calling Search Space.
Step 3	Configure an Intercom Translation Pattern, on page 279	To add a new Intercom Translation Pattern or to configure an existing Intercom Translation Pattern .
Step 4	Configure an Intercom Directory Number, on page 286	To add or update an Intercom Directory Number.
Step 5	Intercom Line and Speed Dial Configuration, on page 294	Configure Intercom Line and Speed Dial.

Configure Intercom Partition

Before you begin

Ensure the phone model supports the Intercom feature for a particular release and device pack Generate a Phone Feature List, on page 3

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Intercom** > **Intercom Route Partition**.

The **Find and List Intercom Partitions** window appears.

Step 2 Click **Add New**.

An **Add New Intercom Partition** window appears.

Step 3 Under the **Intercom Partition Information** section, in the **Name** box, enter the name and description of the intercom partition that you want to add.

Note To enter multiple partitions, use one line for each partition entry. You can enter up to 75 partitions; the names and descriptions can have up to a total of 1475 characters. The partition name cannot exceed 50 characters. Use a comma (,) to separate the partition name and description on each line. If a description is not entered, Unified Communications Manager uses the partition name as the description.

Step 4 Click **Save**.

Step 5 Locate the partition that you want to configure.
Intercom Partition Configuration window is displayed

Step 6 Configure the fields in the Intercom Partition Configuration field area. See the online help for more information about the fields and their configuration options.

Step 7 Click **Save**.

The **Intercom Partition Configuration** window appears.

Step 8 Enter the appropriate settings. For detailed information about the Intercom Partition Configuration parameters, see online help.

Step 9 Click **Save**.

Step 10 Click **Apply Config**.

Intercom Partition Configuration Fields

Table 21: Intercom Partition Configuration Fields

Field	Description
Name	The name of the intercom partition that you selected displays in this box.
Description	If you entered a description of the intercom partition that you selected, it is displayed here. If you did not enter a description when you added the Intercom partition, you can add it now.
Time Schedule	The drop-down list is populated with time schedules that you can add from **Call Routing** > **Class of Control** > **Time Schedule**.
Time Zone	• If you want the time zone to be the same as the originating device, click the radio button next to Originating Device. • If you want to set a specific time zone, click the Specific Time Zone radio button and select the correct time zone from the drop-down list.

Configure an Intercom Calling Search Space

Before you begin

Configure Intercom Partition, on page 276

Procedure

Step 1 In the menu bar, choose **Call Routing** > **Intercom** > **Intercom Calling Search Space**.

Step 2 Click the **Add New**.

Step 3 Configure the fields in the Intercom Calling Search Space field area. For more information on the fields and their configuration options, see Online Help.

Step 4 Click **Save**.

Intercom Calling Search Space Configuration Fields

Table 22: Intercom Calling Search Space Configuration Fields

Field	Description
Name	Enter a name in the Intercom Calling Search Space Name field. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure each calling search space name is unique to the system. **Note** Use concise and descriptive names for your intercom calling search spaces. The CompanynameLocationCalltype format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a calling search space. For example, CiscoDallasMetroCS identifies a calling search space for toll-free, inter-local access and transport area (LATA) calls from the Cisco office in Dallas.
Description	Enter a description in the Description field. The description can include up to 50 characters in any language, and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_), but it cannot include double-quotes (“), percentage sign (%), ampersand (&), or angle brackets (<>).
Intercom Route Partitions for this Calling Search Space	

Field	Description
Available Intercom Partitions	Choose an intercom partition in the Available Intercom Partitions list box and add it to the Selected Intercom Partitions list box by clicking the arrow button between the two list boxes. To add a range of intercom partitions at once, click the first intercom partition in the range; then, hold down the Shift key while clicking the last intercom partition in the range. Click the arrow button between the two list boxes to add the range of partitions. To add multiple intercom partitions that are not contiguous, hold down the Control (Ctrl) key while clicking multiple intercom partitions. Click the arrow button between the two list boxes to add the chosen intercom partitions. **Note** The length of the intercom partition names limits the maximum number of intercom partitions that can be added to an intercom calling search space. Configure Intercom Partition, on page 276 provides examples of the maximum number of partitions that can be added to an intercom calling search space if intercom partition names are of fixed length.
Selected Intercom Partitions (Ordered by highest priority)	To change the priority of an intercom partition, choose an intercom partition name in the Selected Intercom Partitions list box. Move the intercom partition up or down in the list by clicking the arrows on the right side of the list.

Configure an Intercom Translation Pattern

Before you begin

Configure an Intercom Calling Search Space, on page 278

Procedure

Step 1 Choose **Call Routing** > **Intercom** > **Intercom Translation Pattern**.

The **Find and List Intercom Translation Patterns** window appears.

Step 2 Perform one of the followings tasks:

a) To copy an existing intercom translation pattern, locate the partition to configure, click **Copy** eside the intercom translation pattern to copy.

b) To add a new intercom translation pattern, click the **Add New**.

Step 3 Configure the fields in the Intercom Translation Pattern Configuration field area. For more information on the fields and their configuration options, see Online Help.

Step 4 Click **Save**.

Ensure that the intercom translation pattern that uses the selected partition, route filter, and numbering plan combination is unique. if you receive an error that indicates duplicate entries, check the route pattern or hunt pilot, translation pattern, directory number, call park number, call pickup number, or meet-me number configuration windows.

The **Intercom Translation Pattern Configuration** window displays the newly configured intercom translation pattern.

Intercom Translation Pattern Configuration Fields

Table 23: Translation Pattern Configuration Field Settings

Field	Description
Pattern Definition	
Intercom Translation Pattern	Enter the Intercom Translation Pattern, including numbers and wildcards (do not use spaces), in the Intercom Translation Pattern field. For example, for the NANP, enter 9.@ for typical local access or 8XXX for a typical private network numbering plan. Valid characters include the uppercase characters A, B, C, and D and \+, which represents the international escape character +. If you leave this field blank, you must select a partition from the Partition drop-down list box. **Note** Ensure that the Intercom Translation Pattern, which uses the chosen intercom partition, route filter, and numbering plan combination, is unique. Check the route pattern/hunt pilot, translation pattern, directory number, call park number, call pickup number, or meet-me number if you receive a message that indicates duplicate entries. Alternatively, check the route plan report if you receive a message that indicates duplicate entries.

Field	Description
Partition	Choose an intercom partition. If you do not want to assign an intercom partition, choose <None>. If you choose <None>, you must enter a value in the Intercom Translation Pattern field. You can configure the number of intercom partitions that display in this drop-down list by using the Max List Box Items enterprise parameter. If more intercom partitions exist than the Max List Box Items enterprise parameter specifies, the Find button displays next to the drop-down list. Click the Find button to display the Find and List Partitions window. Find and choose an intercom partition name. **Note** To set the maximum list items, choose **System** > **Enterprise Parameters** and choose **CCMAdmin Parameters**. **Note** Make sure that the combination of intercom translation pattern, route filter, and intercom partition is unique within the Cisco Unified Communications Manager cluster.
Description	Enter a description for the Intercom Translation Pattern. The description can include up to 50 characters in any language, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), or angle brackets (<>).
Numbering Plan	Choose a numbering plan. If your Intercom Translation Pattern includes the @ wildcard, you may choose a numbering plan. The optional act of choosing a numbering plan restricts certain number patterns.

Field	Description
Route Filter	Choosing an optional route filter restricts certain number patterns. See topics related to widlcards and special characters in route patterns and hunt pilots. The route filters that display depend on the numbering plan that you choose from the Numbering Plan drop-down list. If more than 250 route filters exist, the **Find** button displays next to the drop-down list box. Click the **Find** button to display the Select Route Filters window. Enter a partial route filter name in the List items where Name contains field. Click the desired route filter name in the list of route filters that displays in the Select item to use box and click **Add Selected**. **Note** To set the maximum list box items, choose **System** > **Enterprise Parameters** and choose **CCMAdmin Parameters**.
MLPP Precedence	Choose an MLPP precedence setting for this intercom translation pattern from the drop-down list: • Executive Override - Highest precedence setting for MLPP calls. • Flash Override - Second highest precedence setting for MLPP calls. • Flash - Third highest precedence setting for MLPP calls. • Immediate - Fourth highest precedence setting for MLPP calls. • Priority - Fifth highest precedence setting for MLPP calls. • Routine - Lowest precedence setting for MLPP calls. • Default - Does not override the incoming precedence level but rather lets it pass unchanged.
Calling Search Space	From the drop-down list, choose the Intercom Calling Search Space for which you are adding an Intercom Translation Pattern, if necessary. You can configure the number of Intercom Calling Search Spaces that display in this drop-down list by using the Max List Box Items enterprise parameter. If more Intercom Calling Search Spaces exist than the Max List Box Items enterprise parameter specifies, the Find button displays next to the drop-down list. Click the Find button to display the Find and List Calling Search Space window.

Field	Description
Route Option	The Route Option designation indicates whether you want this intercom translation pattern to be used for routing calls (such as 9.@ or 8[2-9]XX) or for blocking calls. Choose the Route this pattern or Block this pattern radio button. If you choose the Block this pattern radio button, you must choose the reason for which you want this intercom translation pattern to block calls. Choose a value from the drop-down list: • No Error • Unallocated Number • Call Rejected • Number Changed • Invalid Number Format • Precedence Level Exceeded
Provide Outside Dial Tone	Outside dial tone indicates that Cisco Unified Communications Manager routes the calls off the local network. Check this check box for each Intercom Translation Pattern that you consider to be off network.
Urgent Priority	If the dial plan contains overlapping patterns, Cisco Unified Communications Manager does not route the call until the interdigit timer expires (even if it is possible to dial a sequence of digits to choose a current match). Check this check box to interrupt interdigit timing when Cisco Unified Communications Manager must route a call immediately. By default, the Urgent Priority check box displays as checked. Unless your dial plan contains overlapping patterns or variable length patterns that contain !, Cisco recommends that you do not uncheck the check box.
Calling Party Transformations	
Use Calling Party's External Phone Number Mask	Check the check box if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls.
Calling Party Transform Mask	Enter a transformation mask value. Valid entries include the digits 0 through 9, the wildcard characters asterisk (*) and octothorpe (#), the international escape character + and blank. If this field is blank and the preceding field is not checked, no calling party transformation takes place.

Field	Description
Prefix Digits (Outgoing Calls)	Enter prefix digits. Valid entries include the digits 0 through 9, the wildcard characters asterisk (*) and octothorpe (#), and the international escape character +. **Note** The appended prefix digit does not affect which directory numbers route to the assigned device.
Calling Line ID Presentation	Cisco Unified Communications Manager uses calling line ID presentation (CLIP/CLIR) as a supplementary service to allow or restrict the originating caller phone number on a call-by-call basis. Choose whether you want the Cisco Unified Communications Manager to allow or restrict the display of the calling party phone number on the called party phone display for this intercom translation pattern. Choose Default if you do not want to change calling line ID presentation. Choose Allowed if you want Cisco Unified Communications Manager to allow the display of the calling number. Choose Restricted if you want Cisco Unified Communications Manager to block the display of the calling number. **Note** Use this parameter and the Connected Line ID Presentation parameter, in combination with the Ignore Presentation Indicators (internal calls only) device-level parameter, to configure call display restrictions. Together, these settings allow you to selectively present or restrict calling and/or connected line display information for each call. See the Cisco Unified Communications Manager Administration Guide for information about the Ignore Presentation Indicators (internal calls only) field.

Field	Description
Calling Name Presentation	Cisco Unified Communications Manager uses calling name presentation (CNIP/CNIR) as a supplementary service to allow or restrict the originating caller name on a call-by-call basis. Choose whether you want the Cisco Unified Communications Manager to allow or restrict the display of the calling party name on the called party phone display for this Intercom Translation Pattern. Choose Default if you do not want to change calling name presentation. Choose Allowed if you want Cisco Unified Communications Manager to display the calling name information. Choose Restricted if you want Cisco Unified Communications Manager to block the display of the calling name information.
Connected Party Transformations	
Connected Line ID Presentation	Cisco Unified Communications Manager uses connected line ID presentation (COLP/COLR) as a supplementary service to allow or restrict the called party phone number on a call-by-call basis. Choose whether you want Cisco Unified Communications Manager to allow or restrict the display of the connected party phone number on the calling party phone display for this Intercom Translation Pattern. Choose Default if you do not want to change the connected line ID presentation. Choose Allowed if you want to display the connected party phone number. Choose Restricted if you want Cisco Unified Communications Manager to block the display of the connected party phone number.

Field	Description
Connected Name Presentation	Cisco Unified Communications Manager uses connected name presentation (CONP/CONR) as a supplementary service to allow or restrict the called party name on a call-by-call basis. Choose whether you want Cisco Unified Communications Manager to allow or restrict the display of the connected party name on the calling party phone display for this Intercom Translation Pattern. Choose Default if you do not want to change the connected name presentation. Choose Allowed if you want to display the connected party name. Choose Restricted if you want Cisco Unified Communications Manager to block the display of the connected party name.
Called Party Transformations	
Discard Digits	Choose the discard digits instructions that you want to be associated with this intercom translation pattern. See the Cisco Unified Communications Manager System Guide for more information. **Note** The discard digits that display depend on the numbering plan that you choose from the Numbering Plan drop-down list.
Called Party Transform Mask	Enter a transformation mask value. Valid entries include the digits 0 through 9, the wildcard characters asterisk (*) and octothorpe (#), the international escape character + and blank. If the field is blank, no transformation takes place. The dialed digits get sent exactly as dialed.
Prefix Digits (Outgoing Calls)	Enter prefix digits. Valid entries include the digits 0 through 9, the wildcard characters asterisk (*) and octothorpe (#), the international escape character + and blank. **Note** The appended prefix digit does not affect which directory numbers route to the assigned device.

Configure an Intercom Directory Number

You can assign patterns to intercom directory numbers; for example, 352XX. To avoid user confusion, when you assign a pattern to an intercom directory number, add text or digits to these intercom DN configuration fields, Line Text Label, Display (Internal Caller ID), and External Phone Number Mask. These fields are

displayed for an intercom directory number only after you add the intercom directory number and you associate the intercom directory number with a phone.

For example, add the username to the line text label and internal caller ID, and add the outside line number to the external number mask, when the calling information is displayed, it says John Chan, not 352XX.

Procedure

Step 1 Choose **Call Routing** > **Intercom** > **Intercom Directory Number**.

The **Find and List Intercom Directory Numbers** window is displayed.

Step 2 To locate a specific intercom directory number, enter search criteria and click **Find.**
A list of intercom directory numbers that match the search criteria displayed.

Step 3 Perform one of the followings tasks:

a) To add an intercom directory number, click **Add New**.
b) To update an intercom directory number, click the intercom directory number to update.

The **Intercom Directory Number Configuration** window displayed.

Step 4 Configure the fields in the Intercom Directory Number Configuration field area. For more information on the fields and their configuration options, see Online Help.

Step 5 Click **Save**.

Step 6 Click **Apply Config**.

Step 7 Click **Reset Phone**.

Step 8 Restart devices.

During the restart, the system may drop calls on gateways.

Intercom Directory Number Configuration Fields

The following table describes the fields that are available in the Intercom Directory Number Configuration window.

Table 24: Intercom Directory Number Configuration Settings

Field	Description
Intercom Directory Number Information	
Intercom Directory Number	Enter a dialable phone number. Values can include numeric characters and route pattern wildcards and special characters except for (.) and (@). The intercom directory number that you enter can appear in more than one intercom partition. At the beginning of the intercom directory number, enter \+ if you want to use the international escape character +. For this field, \+ does not represent a wildcard; instead, entering \+ represents a dialed digit.

Field	Description
Route Partition	Choose the intercom partition to which the intercom directory number belongs. Make sure that the intercom directory number that you enter in the Intercom Directory Number field is unique within the intercom partition that you choose. You can configure the number of intercom partitions that display in this drop-down list by using the Max List Items enterprise parameter. If more intercom partitions exist than the Max List Items enterprise parameter specifies, the Find button displays next to the drop-down list. Click the Find button to display the Find and List Partition window. Enter a partial intercom partition name in the List items where Name contains field. Click the desired intercom partition name in the list of intercom partitions that displays in the Select item to use box and click Add Selected. **Note** To set the maximum list box items, choose **System** > **Enterprise ParametersCCMAdmin** Parameters.
Description	Enter a description of the intercom directory number and intercom route partition. The description can include up to 50 characters in any language, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), or angle brackets (<>).

Field	Description
Alerting Name	Enter a name that you want to display on the phone of the caller. This setting, which supports the Identification Services for the QSIG protocol, applies to shared and nonshared directory numbers. If you configure an alerting name for a directory number with shared-line appearances, when the phone rings at the terminating PINX, the system performs the following tasks: • Forwards the name of the caller that is assigned to the directory number. • Applies the Connected Name Restrictions (CONR) that are configured for the translation pattern (if restrictions exist); the originating PINX may modify the CONR, depending on the route pattern configuration. If you do not configure an alerting name, “Name Not Available” may display on the caller phone. If you do not enter a name for the Display (Internal Caller ID) field, the information in the Alerting Name field displays in the Display (Internal Caller ID) field. If you set the Always Display Original Dialed Number service parameter to True, the alerting name does not display on the calling phone; only the original dialed number displays.
ASCII Alerting Name	This field provides the same information as the Alerting Name field, but you must limit input to ASCII characters. Devices that do not support Unicode (internationalized) characters display the content of the Alerting Name ASCII field.
Allow Control of Device from CTI	Check this check box to allow CTI to control and monitor a line on a device with which this intercom directory number is associated

Field	Description
Associated Devices	After you associate this intercom directory number with a device, this pane displays the device with which this intercom directory number is associated. **Note** An intercom directory number can be associated with at most one device. To edit a device with which this intercom directory number is associated, choose a device name in the Associated Devices pane and click the Edit Device button. The Phone Configuration window or Device Profile Configuration window displays for the device that you choose. To edit a line appearance that has been defined for this intercom directory number, choose a device name in the Associated Devices pane and click the Edit Line Appearance button. The Directory Number Configuration window or Device Profile Configuration window refreshes to show the line appearance for this DN on the device that you choose. To associate a device to this intercom directory number from the list of devices in the Dissociate Devices pane, choose a device in the Dissociate Devices pane and add it to the Associated Devices pane by clicking the up arrow between the two panes.
Dissociate Devices	If you choose to dissociate an intercom directory number from a device, this pane displays the device(s) from which you dissociate this intercom directory number. Choose a device in the Associated Devices pane and add it to the Dissociate Devices pane by clicking the down arrow between the two panes.
Intercom Directory Number Settings	

Field	Description
Calling Search Space	

Field	Description
	From the drop-down list, choose the appropriate intercom calling search space. An intercom calling search space comprises a collection of intercom partitions that are searched for numbers that are called from this intercom directory number. The value that you choose applies to all devices that are using this intercom directory number. Changes result in an update of the numbers that the Call Pickup Group field lists. You can configure calling search space for forward all, forward busy, forward no answer, forward no coverage, and forward on CTI failure directory numbers. The value that you choose applies to all devices that are using this directory number. You must configure either primary forward all calling search space or secondary forward all calling search space or both for call forward all to work properly. The system uses these concatenated fields (Primary CFA CSS + Secondary CFA CSS) to validate the CFA destination and forward the call to the CFA destination. **Note** If the system is using partitions and calling search spaces, Cisco recommends that you configure the other call forward calling search spaces as well. When a call is forwarded or redirected to the call forward destination, the configured call forward calling search space gets used to forward the call. If the forward calling search space is None, the forward operation may fail if the system is using partitions and calling search spaces. For example, if you configure the forward busy destination, you should also configure the forward busy calling search space. If you do not configure the forward busy calling search space and the forward busy destination is in a partition, the forward operation may fail. When you forward calls by using the CFwdAll softkey on the phone, the automatic combination of the line CSS and device CSS does not get used. Only the configured Primary CFA CSS and Secondary CFA CSS get used. If both of these fields are None, the combination results in two null partitions, which may cause the operation to fail.

Field	Description
	If you want to restrict users from forwarding calls on their phones, you must choose a restrictive calling search space from the Forward All Calling Search Space field.
BLF Presence Group	Configure this field with the BLF presence group feature. From the drop-down list box, choose a BLF Presence Group for this intercom directory number. The selected group specifies the devices, end users, and application users that can monitor this intercom directory number. The default value for BLF Presence Group specifies Standard Presence group, configured with installation. BLF Presence groups that are configured in Cisco Unified Communications Manager Administration also appear in the drop-down list. Presence authorization works with BLF presence groups to allow or block presence requests between groups.
Auto Answer	Choose one of the following options to activate the auto answer feature for this intercom directory number: • Auto Answer with Headset • Auto Answer with Speakerphone **Note** Make sure that the headset or speakerphone is not disabled when you choose Auto Answer with headset or Auto Answer with speakerphone. **Note** Do not configure auto answer for devices that have shared lines. **Note** For an intercom line on a CTIPort device, autoanswer-speakerphone and autoanswer-headset means that the autoanswer is on. The speakerphone or headset options do not apply to CTIPort devices; instead, it just indicates that the line is capable of auto-answering. Applications have responsibility for terminating the media on CTIPort devices and can terminate the media on either type of output device.

Field	Description
Default Activated Device	From the drop-down list, choose a default activated device for this intercom directory number. The selected device specifies the phone on which this intercom directory number is activated by default. The drop-down list lists only devices that support intercom. **Note** You must specify a default activated device for this intercom directory number to be active as an intercom line. **Note** If an intercom directory number is specified in a device profile that is configured for Cisco Extension Mobility, that intercom directory number will display as an intercom line only when a user logs in to the specified default activated device by using that device profile, as long as the device supports the intercom feature.

Intercom Line and Speed Dial Configuration

Before you begin

Configure an Intercom Directory Number, on page 286

Procedure

Step 1 Choose **Device** > **Device Settings** > **Phone Button Template** and add the intercom line to an existing phone button template or create a new template.

Note The intercom line cannot be configured as the primary line.

Step 2 From the **Button Information** area, from **Feature** drop-down list, choose **Intercom**.

Step 3 From the **Button Information** area, from **Feature** drop-down list, choose **Speed Dial**.

Note You can configure the intercom line with a predefined destination (speed dial) to allow fast access.

Step 4 Click **Save**.

Step 5 Click **Apply Config**.

Intercom Interactions and Restrictions

Intercom Interactions

Feature	Interaction
Bulk Administration Tool	The Unified Communications Manageradministrator can use the Bulk Administration Tool to add many intercom users at once instead of adding users individually. For more information, see Bulk Administration Guide for Cisco Unified Communications Manager.
Barge	When the intercom destination is a barge target, the Cisco Unified IP Phone can still support whisper intercom. When the destination caller chooses to talk to the intercom caller by pressing the intercom button, the original call is put on hold, and the barge initiator is released.
Do Not Disturb (DND)	The intercom call will override DND on the destination phone.
Call Preservation	When a call is preserved, the end user must hang up before the phone can reregister with Unified Communications Manager. When the intercom call is in whisper mode, it represents a one-way medium, and the terminating side might have no user at all; therefore, only the intercom call in talkback mode will get preserved. (Whisper intercom will not get preserved.)
Cisco Unified Survivable Remote Site Telephony (SRST)	When Cisco Unified IP Phones register with SRST, the phones do not register intercom lines; therefore, the feature will not be available when the phones are registered with SRST.
Cisco Unified Communications Manager Assistant	With the Unified Communications Manager Assistant Configuration Wizard, **Cisco Unified Communications Manager Assistant** configuration takes less time and eliminates errors. The partitions, calling search spaces, route point, and translation pattern automatically get created when the administrator successfully runs and completes the configuration wizard.
CTI	You can use CTI/JTAPI/TSP to set or modify the preconfigured target directory number for an intercom line. You will receive notification if the target directory number is updated or reconfigured through Cisco Unified Communications Manager Administration. Be aware that CTI/JTAPI/TSP is backward compatible if the intercom line is not configured to be controlled by the application. If the intercom line is configured in the application user list, you may have to make changes and test the compatibility.
Cisco Extension Mobility	The intercom feature interacts with Cisco Extension Mobility. The system presents an intercom line to a user who uses Cisco Extension Mobility to log in to a phone that supports the feature if the device profile that the user uses to log in has an intercom line that is provisioned. The phone must be the default device for that intercom line.

Feature	Interaction
Internet Protocol Version 6 (IPv6)	Intercom can support phones with an IP Addressing Mode of IPv4 Only or IPv4 and IPv6. During an intercom call, the talkback mode establishes media streams with the same IP version as the media stream that is used when the caller initiates intercom.
Intercom directory numbers (lines)	Intercom directory numbers (lines) are restricted to one device per intercom line. Cisco Extension Mobility is widely used; mobile users need the intercom feature but need it to be available only on a single device. You can assign intercom lines to either a regular device or to an extension mobility profile, but the system needs to enforce that an intercom line gets associated to either a regular device or to an extension mobility profile.
Extension mobility profile	An extension mobility profile can be used on more than one phone simultaneously, use the **Default Activated Device** field in the **Intercom Directory Number Configuration** window (**Cisco Unified CM Administration** > **Call Routing** > **Intercom** > **ntercom Directory Number Configuration**) to specify which device can display this intercom line. Intercom lines that are not used for Extension Mobility also require configuration of the **Default Activated Device** field.

Intercom Restrictions

The following restrictions apply to the Intercom feature:

Feature	Restrictions
Hold	The system does not allow intercom calls to be placed on hold.
Call Forwarding	Intercom calls cannot be forwarded.
Transfer	The system does not allow an intercom call to be transferred.
iDivert	The system does not allow an intercom call to be diverted.
Call Pickup/Directed Call Pickup	The call pickup groups do not include intercom calls.
DND	Intercom overrides Do Not Disturb (DND).
Bandwidth	If sufficient bandwidth does not exist, the intercom call fails.
Call Target	If two intercom calls are directed to a target, the first one goes through; the second fails with a busy tone.
Barge and cBarge	Intercom does not work with Barge and cBarge.
Conferencing	The system does not allow intercom calls to be in conference.
Monitoring and Recording	When an active call is being monitored or recorded, the user cannot receive nor place intercom calls.
Video	Video is not supported with intercom.

Feature	Restrictions
Intercom Partition	An intercom partition assigned to an item such as calling search space or to a route pattern cannot be deleted.
Intercom Calling Search Spaces	Intercom calling search spaces that devices, lines (DNs), translation patterns, or other items are using cannot be deleted.

Intercom Troubleshooting

Busy Tone When Dialing Out of Intercom Line

Problem

Phone plays busy tone when user is dialing out of intercom line.

Possible Cause

The DN is not in the same intercom partition as the calling number.

Solution

- Ensure that the DN is in the same intercom partition as the calling number.
- I

  f it is, ensure that the dialed-out DN is configured on another phone and that the phone is registered with the same Unified Communications Manager cluster.

Intercom Calls cannot use Talkback with Speaker, Handset or Headset

Problem

User cannot go into talkback mode for intercom calls by using headset, handset, or speaker.

Possible Cause

This situation exists by design. The only way to go into the connected state for intercom calls is by pressing the corresponding line button.

Solution

User can end call by using speaker, handset, or headset.

Troubleshooting SCCP

Intercom Lines Not Showing Up on Phone

Problem

Intercom lines do not display on the phone.

Possible Cause

The phone version may be earlier than 8.3(1), or the button template may not be assigned to the phone.

Solution

- Check the phone version. Ensure that it is 8.3(1) or later.
- Determine whether the button template is assigned to the phone.
- Capture the sniffer trace between Cisco Unified Communications Manager and the phone. In the button template response, see whether intercom lines get sent to the phone (button definition = Ox17).

Intercom Lines Not Showing Up When Phone Falls Back to SRST

Problem

A phone that was configured with Unified Communications Manager Release 6.0(x) or later, includes two intercom lines. Unified Communications Manager stops and falls back to SRST. The intercom lines do not display.

Possible Cause

The SCCP version of SRST does not support SCCP Version 12.

Solution

- Check the SCCP Version of SRST. If SRST supports SCCP Version 12, it will support intercom lines.
- If SRST supports SCCP Version 12, capture a sniffer trace and ensure that the button template that the phone sent includes intercom lines.

Troubleshooting SIP

Debug Phones That Are Running SIP

Use this debug command: **Debug sip-messages sip-task gsmfsmIsm sip-adapter**.

Configuration of Phones That Are Running SIP

Show config —The command on the phone is displayed if intercom lines are configured as regular lines with featureid-->23.

Cisco Extension Mobility User Is Logged In But Intercom Line Does Not Display

Problem

The Cisco Extension Mobility user is logged in to a phone, but the user intercom line does not display.

Possible Cause

Default Activated Device is configured incorrectly.

Solution

- Check that the **Default Activated Device** is configured on the intercom directory number.
- Check that the **Default Activated Device** matches the device to which the user is logged in.

Intercom Line Fails to Display on Phone

Problem

An intercom line has been configured and assigned to a phone but fails to display on the phone.

Possible Cause

Default Activated Device value is set to the intercom line of this device.

Solution

If the configuration has been done, reset the phone.

PART IX

Receiving Calls

CHAPTER 23

Prime Line Support

Prime Line Support Overview

You can configure the Prime Line Support in Cisco Unified CM Administration so that when the phone is off-hook and receives a call on any line, the system always chooses the primary line for the call.

Prime Line Support Prerequisites

The following devices are compatible with the Prime Line Support feature:

Cisco Unified IP Phone 7900 Series, 8900 Series, and 9900 Series

For more information on the supported devices, see the latest version of *Cisco Unified IP Phone Guide* and *Cisco Unified IP Phone Administration Guide*.

Prime Line Support Configuration Task Flow

To configure the Prime Line Support feature for either the Cisco CallManager service or devices and device profiles, perform one of the following procedures.

Before you begin

- Review Prime Line Support Prerequisites, on page 303.

Procedure

	Command or Action	Purpose
Step 1	Configure Clusterwide Prime Line Support, on page 304	**(Optional)**. Configure the Prime Line Support feature for the Cisco CallManager service, which applies to the entire cluster.
Step 2	Configure Prime Line Support for Devices, on page 305	**(Optional)**. Configure the Prime Line Support feature for specific devices within the cluster, if you do not want to enable the feature clusterwide. **Note** When you configure this parameter, going off-hook makes only the first line active on the phone, even when a call rings on another line on the phone. So the call does not get answered on the other line.

Configure Clusterwide Prime Line Support

Procedure

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

Step 2 From the **Server** drop-down list, choose the server that is running the Cisco CallManager service.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.

Step 4 From the **Always Use Prime Line** clusterwide service parameter, choose one of the following options from the drop-down list:

- **True**- When a phone goes off-hook, the primary line gets chosen and becomes the active line.
- **False**- When a phone goes off-hook, the IP phone automatically chooses an available line as the active line.

The default value for this service parameter is **False**.

Step 5 For this change to take effect on the SIP phones, click the **ApplyConfig** button in Cisco Unified CM Administration (for example, on the **Device Configuration** window, the **Device Pool Configuration** window, or any other window on which ApplyConfig is an option).

Note If the new configuration is not applied on the SIP phones, the SIP Prime Line Support feature changes will not be implemented until the next reset of the Cisco CallManager service or reset of each affected device.

Configure Prime Line Support for Devices

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Common Phone Profile**.

Step 2 From the **Find and List** window, choose the phone for which you want to change the Always Use Prime Line setting.
The **Phone Configuration** window appears.

Step 3 From the **Always Use Prime Line** drop-down list, choose one of the following options:

- **Off**- When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received.
- **On**- When the phone is idle (off hook) and receives a call on any line, the primary line is chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls.
- **Default**- Unified Communications Manager uses the configuration from the **Always Use Prime Line** service parameter, which supports the Cisco CallManager service.

Step 4 Click **Save**.

Prime Line Support Interactions

Feature	Interaction
Always Use Prime Line	If you select **On** for the **Always Use Prime Line** parameter in the **Device Profile** or **Default Device Profile Configuration** window, a Cisco Extension Mobility user can use this feature after logging in to the device that supports Cisco Extension Mobility.
Maximum Number of Calls and Busy Trigger Settings	When the phone already has a call on a line, Unified Communications Manager uses the configuration for the Maximum Number of Calls and Busy Trigger settings to determine how to route the call.
Auto Answer	If you choose the Auto Answer with Headset option or Auto Answer with Speakerphone option from the **Auto Answer** drop-down list in Cisco Unified CM Administration, the Auto Answer configuration overrides the configuration for the **Always Use Prime Line** parameter.

Prime Line Support Troubleshooting

Prime Line Support Does Not Work When Set To True

Problem When the cluster-wide service parameter **Always use Prime Line** is set to **True** and the IP phone goes off-hook, the primary line becomes the active line. Even if a call rings on the second line, when the user goes off-hook, it activates only the first line. The phone does not answer the call on the second line. However, when IP phones with multiple line appearances are used with the 7.1.2 phone load, the phone does not use the primary line when a second line rings. If the user picks up the handset, the phone answers the call on the second line.

Solution Press the line button for the primary line so that the secondary line is not engaged when a call is initiated.

Unable To Answer Inbound Calls

Problem The users are unable to automatically answer inbound calls after they go off-hook on IP phones, and must press the Answer softkey to answer the calls.

Solution To resolve the problem, perform the following procedure:

1. From Cisco Unified CM Administration, choose **System** > **Service Parameters**.
2. From the Server drop-down list, choose the server that is running the Cisco CallManager service.
3. From the Service drop-down list, choose **Cisco CallManager**.
4. In Cluster wide parameters (Device - phone), set **Always Use Prime Line** to **False**.

Inbound Calls Are Answered Automatically

Problem When an inbound call is received on a shared line of an IP phone, the call is answered immediately as the handset is lifted, without the option to either answer the call or make an outbound call. This behavior does not change even though **Auto Line Select** is set to disabled.

Solution To resolve the problem, perform the following procedure:

1. From Cisco Unified CM Administration, choose **System** > **Service Parameters**.
2. From the Server drop-down list, choose the server that is running the Cisco CallManager service.
3. From the Service drop-down list, choose **Cisco CallManager**.
4. In Cluster wide parameters (Device - phone), set **Always Use Prime Line** to **False**.

CHAPTER 24

Call Forwarding

Call Forwarding Overview

As a user, you can configure a Cisco Unified IP Phone to forward calls to another phone. The following call forwarding types are supported:

- **Call Forward No Bandwidth**—Forwards calls when a call to a directory number fails due to insufficient bandwidth, and provides forwarding functionality to an Automated Alternate Routing (AAR) destination using public switched telephone network (PSTN) as the alternate route or to a voicemail system.
- **Call Forward with Alternate Destination**—Forwards calls when a call to a directory number and the forwarded destination are not answered. The call gets diverted to an alternate destination as a last resort. This Call Forwarding type is also referred to as "MLPP Alternate Party destination."
- **Call Forward All (CFA)**—Forwards all calls to a directory number.
- **Call Forward Busy (CFB)**—Forwards calls only when the line is in use and the configured Call Forward Busy trigger value is reached.
- **Call Forward No Answer (CFNA)**—Forwards calls when the phone is not answered after the configured No Answer Ring Duration timer is exceeded or the destination is unregistered.
- **Call Forward No Coverage (CFNC)**—Forwards calls when the hunt list is exhausted or timed out, and the associated hunt-pilot for coverage specifies "Use Personal Preferences" for its final forwarding.
- **Call Forward Unregistered (CFU)**—Forwards calls when the phone is unregistered due to a remote WAN link failure, and provides automated rerouting through the Public Switched Telephone Network (PSTN). Calls can also be forwarded based on the type of caller: internal or external.
- **CFA Destination Override**—Forwards calls when the user to whom calls are being forwarded (the target) calls the user whose calls are being forwarded (the initiator). The phone of the initiator rings instead of call forwarding back to the target.

Call Forward All, Including CFA Loop Prevention and CFA Loop Breakout

Call Forward All (CFA) allows a phone user to forward all calls to a directory number.

You can configure CFA for internal and external calls and can forward calls to a voicemail system or a dialed destination number by configuring the calling search space (CSS). Unified Communications Manager includes a secondary Calling Search Space configuration field for CFA. The secondary CSS for CFA combines with the existing CSS for CFA to allow support of the alternate CSS system configuration. When you activate CFA, only the primary and secondary CSS for CFA are used to validate the CFA destination and redirect the call to the CFA destination. If these fields are empty, the null CSS is used. Only the CSS fields that are configured in the primary CSS for CFA and secondary CSS for CFA fields are used. If CFA is activated from the phone, the CFA destination is validated by using the CSS for CFA and the secondary CSS for CFA, and the CFA destination gets written to the database. When a CFA is activated, the CFA destination always gets validated against the CSS for CFA and the secondary CSS for CFA.

Unified Communications Manager prevents CFA activation on the phone when a CFA loop is identified. For example, Unified Communications Manager identifies a call forward loop when the user presses the CFwdALL softkey on the phone with directory number 1000 and enters 1001 as the CFA destination, and 1001 has forwarded all calls to directory number 1002, which has forwarded all calls to directory number 1003, which has forwarded all calls to 1000. In this case, Unified Communications Manager identifies that a loop has occurred and prevents CFA activation on the phone with directory number 1000.

Tip If the same directory number exists in different partitions, for example, directory number 1000 exists in partitions 1 and 2, Unified Communications Manager allows the CFA activation on the phone.

CFA loops do not affect call processing because Unified Communications Manager supports CFA loop breakout, which ensures that if a CFA loop is identified, the call goes through the entire forwarding chain, breaks out of the Call Forward All loop, and the loop is completed as expected, even if CFNA, CFB, or other forwarding options are configured along with CFA for one of the directory numbers in the forwarding chain.

For example, the user for the phone with directory number 1000 forwards all calls to directory number 1001, which has forwarded all calls to directory number 1002, which has forwarded all calls to directory number 1000, which creates a CFA loop. In addition, directory number 1002 has configured CFNA to directory number 1004. The user at the phone with directory number 1003 calls directory number 1000, which forwards to 1001, which forwards to 1002. Unified Communications Manager identifies a CFA loop, and the call, which breaks out of the loop, tries to connect to directory number 1002. If the No Answer Ring Duration timer expires before the user for the phone with directory number 1002 answers the call, Unified Communications Manager forwards the call to directory number 1004.

For a single call, Unified Communications Manager may identify multiple CFA loops and attempt to connect the call after each loop is identified.

Call Forwarding Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure Partitions for Call Forwarding, on page 309	Administrators can configure partitions to restrict Call Forwarding to certain numbers based on the design criteria and requirements.
Step 2	Configure Calling Search Space for Call Forwarding, on page 311	Administrators can configure calling search spaces to restrict Call Forwarding to certain numbers based on the design criteria and requirements.
Step 3	Configure Call Forwarding when Hunt List is Exhausted or Hunt Timer Expires, on page 312	You can forward a call when hunting fails (that is, when hunting is terminated without any hunt party answering, either because no hunt number from the list picked up or because the hunt timer timed out).
Step 4	Configure Call Forward No Bandwidth, on page 314	You can forward a call to an Automated Alternate Routing (AAR) destination using public switched telephone network (PSTN) as the alternate route or to a voicemail system when a call to a called directory number fails due to insufficient bandwidth.
Step 5	Configure Call Forward Alternate Destination, on page 315	You can forward calls that go unanswered to the directory number and the forwarded destination. Calls will get diverted to an alternate destination as a last resort.
Step 6	Configure Other Call Forwarding Types, on page 316	You can configure additional forwarding types such as CFA, CFB, CFNA, CFNC, and CFU. You can configure all these forwarding types from the **Directory Number Configuration** window.
Step 7	Enable Destination Override for Call Forwarding, on page 325	Administrators can override the CFA when the target of the CFA calls the initiator of the CFA. This allows the CFA target can reach the initiator for important calls.

Configure Partitions for Call Forwarding

Configure partitions to create a logical grouping of directory numbers (DNs) and route patterns with similar reachability characteristics. Partitions facilitate call routing by dividing the route plan into logical subsets that are based on organization, location, and call type. You can configure multiple partitions.

Configure partitions to restrict call forwarding to certain numbers based on your design criteria and requirements.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Partition**.

Step 2 Click **Add New** to create a new partition.

Step 3 In the **Partition Name, Description** field, enter a name for the partition that is unique to the route plan.

Partition names can contain alphanumeric characters, as well as spaces, hyphens (-), and underscore characters (_). See the online help for guidelines about partition names.

Step 4 Enter a comma (,) after the partition name and enter a description of the partition on the same line.

The description can contain up to 50 characters in any language, but it cannot include double quotes ("), percentage sign (%), ampersand (&), backslash (\), angle brackets (<>), or square brackets ([ ]).

If you do not enter a description, Cisco Unified Communications Manager automatically enters the partition name in this field.

Step 5 To create multiple partitions, use one line for each partition entry.

Step 6 From the **Time Schedule** drop-down list, choose a time schedule to associate with this partition.

The time schedule specifies when the partition is available to receive incoming calls. If you choose **None**, the partition remains active at all times.

Step 7 Select one of the following radio buttons to configure the **Time Zone**:

- **Originating Device**—When you select this radio button, the system compares the time zone of the calling device to the **Time Schedule** to determine whether the partition is available is available to receive an incoming call.
- **Specific Time Zone**—After you select this radio button, choose a time zone from the drop-down list. The system compares the chosen time zone to the **Time Schedule** to determine whether the partition is available is available to receive an incoming call.

Step 8 Click **Save**.

Partition Name Guidelines for Call Forwarding

The list of partitions in a calling search space is limited to a maximum of 1024 characters. This means that the maximum number of partitions in a CSS varies depending on the length of the partition names. Use the following table to determine the maximum number of partitions that you can add to a calling search space if partition names are of fixed length.

Table 25: Partition Name Guidelines

Partition Name Length	Maximum Number of Partitions
2 characters	340
3 characters	256
4 characters	204

Partition Name Length	Maximum Number of Partitions
5 characters	172
. . .	. . .
10 characters	92
15 characters	64

Configure Calling Search Space for Call Forwarding

A calling search space is an ordered list of route partitions that are typically assigned to devices. Calling search spaces determine the partitions that calling devices can search when they are attempting to complete a call.

Configure calling search spaces to restrict Call Forwarding to certain numbers based on your design criteria and requirements.

Before you begin

Configure Partitions for Call Forwarding, on page 309

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Calling Search Space**.

Step 2 Click **Add New**.

Step 3 In the **Name** field, enter a name.

Ensure that each calling search space name is unique to the system. The name can include up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_).

Step 4 In the **Description** field, enter a description.

The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).

Step 5 From the **Available Partitions** drop-down list, perform one of the following steps:

- For a single partition, select that partition.
- For multiple partitions, hold down the **Control (CTRL)** key, then select the appropriate partitions.

Step 6 Select the down arrow between the boxes to move the partitions to the **Selected Partitions** field.

Step 7 (Optional) Change the priority of selected partitions by using the arrow keys to the right of the **Selected Partitions** box.

Step 8 Click **Save**.

Configure Call Forwarding when Hunt List is Exhausted or Hunt Timer Expires

The concept of hunting differs from that of call forwarding. Hunting allows Unified Communications Manager to extend a call to one or more lists of numbers, where each list specifies a hunting order that is chosen from a fixed set of algorithms. When a call extends to a hunt party from these lists and the party fails to answer or is busy, hunting resumes with the next hunt party. (The next hunt party varies depending on the current hunt algorithm.) Hunting then ignores the Call Forward No Answer (CFNA), Call Forward Busy (CFB), or Call Forward All (CFA) configured values for the attempted party.

Call Forwarding allows detailed control as to how to extend (divert or redirect) a call when a called party fails to answer, or is busy and hunting is not taking place. For example, if the CFNA value for a line is set to a hunt-pilot number, a call to that line that is not answered diverts to the hunt-pilot number and begins hunting.

Before you begin

Configure Calling Search Space for Call Forwarding, on page 311

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Route/Hunt** > **Hunt Pilot**.
The **Find and List Hunt Pilots** window is displayed.

Step 2 Click **Find**.
A list of configured Hunt Pilots is displayed.

Step 3 Choose the pattern for which you want to configure call treatment when hunting fails.
The **Hunt Pilot Configuration** window is displayed.

Step 4 Configure the fields in the **Hunt Pilot Configuration** for the **Hunt Call Treatment Settings** area. For more information on the fields and their configuration options, see Online Help.

Step 5 Click **Save**.

Hunt Call Treatment Fields for Call Forwarding

Field	Description
Hunt Call Treatment Settings	
Note	**Forward Hunt No Answer** or **Forward Hunt Busy** fields are designed to move calls through the route list. Queuing is used to hold callers in a route list. Therefore, if queuing is enabled, both **Forward Hunt No Answer** and **Forward Hunt Busy** are automatically disabled. Conversely, if **Forward Hunt No Answer** or **Forward Hunt Busy** are enabled, queuing is automatically disabled.

Field	Description

Forward Hunt No Answer	When the call that is distributed through the hunt list is not answered in a specific period of time, this field specifies the destination to which the call gets forwarded. Choose one of the following options:
	• **Do Not Forward Unanswered Calls**
	• **Use Forward Settings of Line Group Member** (replaces **Use Personal Preferences** check box)
	• **Forward Unanswered Calls to**
	  • **Destination**—Enter a directory number to which calls must be forwarded to.
	  • **Calling Search Space**—Choose a calling search space from the drop-down list which applies to all devices that use this directory number.
	• **Maximum Hunt Timer**—Enter a value (in seconds) that specifies the maximum time for hunting without queuing.
	Valid values are 1 to 3600. The default value is 1800 seconds (30 minutes).
	This timer is canceled if either a hunt member answers the call or the hunt list gets exhausted before the timer expires. If you do not specify a value for this timer, hunting continues until a hunt member answers or the hunt list is exhausted. If neither event takes place, hunting continues for 30 minutes, after which the call is received for final treatment.
	Note If hunting exceeds the number of hops that the **Forward Maximum Hop Count** service parameter specifies, hunting expires before the 30 minute maximum hunt timer value, and the caller receives a reorder tone.

Forward Hunt Busy	When the call that is distributed through the hunt list is not answered in a specific period of time, this field specifies the destination to which the call gets forwarded. Choose one of the following options:
	• **Do Not Forward Unanswered Calls**
	• **Use Forward Settings of Line Group Member**
	• **Forward Unanswered Calls to**
	  • **Destination**—Enter a directory number to which calls must be forwarded to.
	  • **Calling Search Space**—Choose a calling search space from the drop-down list which applies to all devices that use this directory number.

Configure Call Forward No Bandwidth

Before you begin

Configure Call Forwarding when Hunt List is Exhausted or Hunt Timer Expires, on page 312

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Directory Number Configuration**.
The **Find and List Directory Numbers** window is displayed.

Step 2 Click **Find**.
A list of configured directory numbers is displayed.

Step 3 Choose the directory number for which you want to configure call forward when there is insufficient bandwidth.
The **Directory Number Configuration** window is displayed.

Step 4 Configure the fields In the **AAR Settings** area. See Directory Number Configuration Fields for Call Forwarding, on page 314 for more information about the fields and their configuration options.

Step 5 Click **Save**.

Directory Number Configuration Fields for Call Forwarding

Field	Description
Voice Mail	Check this check box to forward the call to the voicemail. **Note** When you check this check box, Unified Communications Manager ignores the values in the **Destination** and **Calling Search Space** fields.
AAR Destination Mask	Enter a destination mask to determine the AAR destination to dial instead of using the external phone number mask.
AAR Group	Choose an AAR group from the drop-down list. It provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. If you choose **None**, the server does not attempt to reroute the blocked calls. You can also configure this value in the **Precedence Alternate Party Timeout** service parameter from **System** > **Service Parameters**.

Field	Description
Retain this destination in the call forwarding history	By default, the directory number configuration retains the AAR leg of the call in the call history, which ensures that the AAR forward to voicemail system will prompt the user to leave a voice message. If you check the check box, the AAR leg of the call will be present in the call forwarding history.

Configure Call Forward Alternate Destination

Before you begin

Configure Call Forward No Bandwidth, on page 314

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Directory Number Configuration**.
The **Find and List Directory Numbers** window is displayed.

Step 2 Click **Find**.
A list of configured directory numbers is displayed.

Step 3 Choose the directory number for which you want to configure an alternate destination.
The **Directory Number Configuration** window is displayed.

Step 4 Configure the fields in the **MLPP Alternate Party And Confidential Access Level Settings** area. See MLPP Alternate Party And Confidential Access Level Settings Fields for Call Forwarding, on page 315 for more information about the fields and their configuration options.

Step 5 Click **Save**.

MLPP Alternate Party And Confidential Access Level Settings Fields for Call Forwarding

Field	Description
Target (Destination)	Enter the number to which MLPP precedence calls should be diverted if this directory number receives a precedence call and neither this number nor its Call Forward destination answers the precedence call. Values can include numeric characters, octothorpe (#), and asterisk (*).
MLPP Calling Search Space	From the drop-down list, choose a calling search space to associate with the MLPP alternate party target (destination) number.

Field	Description
MLPP No Answer Ring Duration (seconds)	Enter the number of seconds (between 4 and 60) after which an MLPP precedence call will be directed to this directory number alternate party, if this directory number and its Call Forward destination have not answered the precedence call. You can also configure this value in the **Precedence Alternate Party Timeout** service parameter from **System** > **Service Parameters** from Cisco Unified CM Administration.

Configure Other Call Forwarding Types

You can configure Call Forward All (CFA), Call Forward Busy (CFB), Call Forward No Answer (CFNA), Call Forward No Coverage (CFNC), and Call Forward Unregistered (CFU) from the **Directory Number Configuration** window.

Before you begin

- For Call Forwarding functionality to work as intended, Cisco recommends that for the configured phones and the directory numbers in various partitions, the Call Forward Calling Search Spaces also be configured or else the forwarding may fail. When a call is forwarded or redirected to the Call Forward destination, the configured Call Forward Calling Search Space is used to forward the call.
- Configure Call Forward Alternate Destination, on page 315

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Directory Number Configuration**.

The **Find and List Directory Numbers** window is displayed.

Step 2 Configure the **Call Forwarding and Call Pickup Settings** fields in the **Directory Number Configuration** window to configure CFA, CFB, CFNA, CFNC, and CFU. See Call Forwarding Fields, on page 316 for information about the fields and their configuration options.

Step 3 Click **Save**.

Call Forwarding Fields

Field	Description
Call Forward and Call Pickup Settings	

Field	Description
Calling Search Space Activation Policy	Three possible values exist for this option: • **Use System Default**—The **CFA CSS Activation Policy** service parameter determines which Forward All Calling Search Space to use for Call Forwarding. If the **CFA CSS Activation Policy** service parameter is set to **With Configured CSS**, then Forward All Calling Search Space and secondary Calling Search Space for Forward All will be used for Call Forwarding. This is the default setting. • **With Configured CSS**—The Forward All Calling Search Space that is explicitly configured in the **Directory Number Configuration** window controls the Forward All activation and Call Forwarding. If the Forward All Calling Search Space is set to **None**, no CSS is configured for Forward All. A Forward All activation attempt to any directory number with a partition will fail. No change in the Forward All Calling Search Space and secondary Calling Search Space for Forward All occurs during the Forward All activation. • **With Activating Device/Line CSS**—A combination of the Directory Number Calling Search Space and Device Calling Search Space controls the Forward All activation and Call Forwarding without explicitly configuring a Forward All Calling Search Space. When Forward All is activated from the phone, the Forward All Calling Search Space and secondary Calling Search Space for Forward All automatically gets populated with the Directory Number Calling Search Space and Device Calling Search Space for the activating device. If the Forward All Calling Search Space is set to **None**, and when Forward All is activated through the phone, the combination of Directory Number Calling Search Space and activating Device Calling Search Space controls the Forward All attempt. **CFA CSS Activation Policy**—Ensure that you configure this service parameter correctly for Forward All to work as intended in the **Service Parameter Configuration** window. The service parameter includes two possible values: • **With Configured CSS**—The primary and secondary CFA Calling Search Space controls the Call Forwarding attempt. • **With Activating Device/Line CSS**—The primary and secondary CFA Calling Search Space is updated with primary Line Calling Search Space and activating Device Calling Search Space. **Roaming**—When a device is roaming in the same device mobility group, Cisco Unified Communications Manager uses the Device Mobility CSS to reach the local gateway. If a user sets Call Forward All at the phone, the CFA CSS is set to **None**, and the CFA CSS Activation Policy is set to **With Activating Device/Line CSS**, then: • The Device CSS and Line CSS is used as the CFA CSS when the device is in its home location. • If the device is roaming within the same device mobility group, the Device Mobility CSS from the Roaming Device Pool and the Line CSS is used as the CFA CSS. • If the device is roaming within a different device mobility group, the Device CSS and Line CSS is used as the CFA CSS.

Field	Description
Forward All	The fields in this row of fields specify the Call Forwarding treatment for calls to this directory number if the directory number is set to forward all calls. The value in the **Calling Search Space** field is used to validate the Forward All destination that is entered when the user activates Call Forward All from the phone. This field is also used to redirect the call to the Call Forward All destination. Configure the following values: • **Voice Mail**—Check this check box to use the value that is set in the **Voice Mail Profile Configuration** window. **Note** When this check box is checked, Unified Communications Manager ignores the values in the **Destination** and **Calling Search Space** fields. • **Destination**—This field indicates the directory number to which all calls are forwarded. Use any dialable phone number, including an outside destination. • **Calling Search Space**—This value applies to all devices that use this directory number. • **Forward Maximum Hop Count**—Configure this parameter from the Cisco Unified CM Administrator, choose **System** > **Service Parameters**. This service parameter specifies the maximum number of times that a single call can be forwarded or diverted, and has special considerations for QSIG calls. For an incoming QSIG call, the maximum value is 15 (per ISO specifications); if you specify a greater value in this field, the specified value will apply to non-QSIG calls and for an incoming QSIG call, the call will only divert a maximum of 15 times. When QSIG trunks are configured, Cisco recommends setting this parameter to 15. For example, if the value of this parameter is seven, and a Call Forward All chain occurs consecutively from directory numbers 1000 to 007, which comprises seven hops, Cisco Unified Communications Manager prevents a phone user with directory number 2000 from activating CFA to directory number 1000, because no more than seven forwarding hops are supported for a single call.
Secondary Calling Search Space for Forward All	Because Call Forwarding is a line-based feature, in cases where the Device Calling Search Space is unknown, the system uses only the Line Calling Search Space to forward the call. If the Line Calling Search Space is restrictive and not routable, the forward attempt fails. Addition of a secondary calling search space for Call Forward All provides a solution to enable forwarding. The primary calling search space for Call Forward All and secondary calling search space for Call Forward All get concatenated (primary CFA CSS + secondary CFA CSS). Unified Communications Manager uses this combination to validate the CFA destination and to forward the call.

Field	Description
Forward Busy Internal	The fields in this row of fields specify the forwarding treatment for internal calls to this directory number if the directory number is busy. The values in the **Destination** and the **Calling Search Space** fields are used to redirect the call to the forward destination. Configure the following values: • **Voice Mail**—Check this check box to use the configured values in the **Voice Mail Profile Configuration** window for internal calls. **Note** When this check box is checked, the calling search space of the voicemail pilot is used. Unified Communications Manager ignores the values in the **Destination** and the **Calling Search Space** fields. **Note** When this check box is checked for internal calls, the system automatically checks the **Voice Mail** check box for external calls. If you do not want external calls to be forwarded to the voicemail system, you must uncheck the **Voice Mail** check box for external calls. • **Destination**—This field indicates the Call Forward Busy destination for internal calls. Use any dialable phone number, including an outside destination. **Note** When you enter a destination value for internal calls, the system automatically copies this value to the **Destination** field for external calls. If you want external calls to be forwarded to a different destination, you must enter a different value in the **Destination** field for external calls. • **Calling Search Space**—The Forward Busy Internal Calling Search Space is used to forward the call to the Forward Busy Internal destination. It applies to all devices that use this directory number. **Note** If the system is using partitions and calling search spaces, Cisco recommends that you configure the Call Forward Calling Search Spaces. When a call is forwarded or redirected to the Call Forward destination, the configured Call Forward Calling Search Space is used to forward the call. If the **Calling Search Space** field is set to **None**, the forward operation fails if the system uses partitions and calling search spaces. For example, if you configure the Forward Busy destination, you should also configure the Forward Busy Calling Search Space. If you do not configure the Forward Busy Calling Search Space and the Forward Busy destination is in a partition, the forward operation fails. **Note** When you choose a calling search space for internal calls, the system automatically copies this value to the calling search space setting for external calls. If you want external calls to be forwarded to a different calling search space, you must choose a different value in the **Calling Search Space** field for external calls. The Call Forward Busy trigger is configured for each line appearance and cannot exceed the maximum number of calls that are configured for a line appearance. The Call Forward Busy trigger determines how many active calls exist on a line before the Call Forward Busy setting is activated (for example, ten calls). **Tip** Keep the busy trigger slightly lower than the maximum number of calls so that users can make outgoing calls and perform transfers. **Tip** If a call gets forwarded to a directory number that is busy, the call is not completed.

Field	Description
Forward Busy External	The fields in this row of fields specify the forwarding treatment for external calls to this directory number if the directory number is busy. The **Destination** and **Calling Search Space** fields is used to redirect the call to the forward destination. Configure the following values: • **Voice Mail**—Check this check box to use the configured values in the **Voice Mail Profile Configuration** window for external calls. **Note** When this check box is checked, the calling search space of the voicemail pilot is used. Unified Communications Manager ignores the values in the **Destination** and the **Calling Search Space** fields. **Note** When this check box is checked for internal calls, the system automatically checks the **Voice Mail** check box for external calls. If you do not want external calls to be forwarded to the voicemail system, you must uncheck the **Voice Mail** check box for external calls. • **Destination**—This field indicates the Call Forward Busy destination for external calls. Use any dialable phone number, including an outside destination. **Note** When you enter a destination value for internal calls, the system automatically copies this value to the **Destination** field for external calls. If you want external calls to be forwarded to a different destination, you must enter a different value in the **Destination** field for external calls. • **Calling Search Space**—The Forward Busy External Calling Search Space forwards the call to the Forward Busy External destination. It applies to all devices that use this directory number. **Note** If the system is using partitions and calling search spaces, Cisco recommends that you configure the Call Forward Calling Search Spaces. When a call is forwarded or redirected to the Call Forward destination, the configured Call Forward Calling Search Space is used to forward the call. If the **Calling Search Space** field is set to **None**, the forward operation fails if the system uses partitions and calling search spaces. For example, if you configure the Forward Busy destination, you should also configure the Forward Busy Calling Search Space. If you do not configure the Forward Busy Calling Search Space and the Forward Busy destination is in a partition, the forward operation fails. **Note** When you choose a calling search space for internal calls, the system automatically copies this value to the calling search space setting for external calls. If you want external calls to be forwarded to a different calling search space, you must choose a different value in the **Calling Search Space** field for external calls.

Field	Description
Forward No Answer Internal	The fields in this row of fields specify the forwarding treatment for internal calls to this directory number if the directory number does not answer. The **Destination** and **Calling Search Space** fields are used to redirect the call to the forward destination. Configure the following values: • **Voice Mail**—Check this check box to use the configured values in the **Voice Mail Profile Configuration** window. **Note** When this check box is checked, the calling search space of the voicemail pilot is used. Unified Communications Manager ignores the values in the **Destination** and the **Calling Search Space** fields. **Note** When this check box is checked for internal calls, the system automatically checks the **Voice Mail** check box for external calls. If you do not want external calls to be forwarded to the voicemail system, you must uncheck the **Voice Mail** check box for external calls. • **Destination**—This field indicates the directory number to which an internal call is forwarded when the call is not answered. Use any dialable phone number, including an outside destination. **Note** When you enter a destination value for internal calls, the system automatically copies this value to the **Destination** field for external calls. If you want external calls to be forwarded to a different destination, you must enter a different value in the **Destination** field for external calls. • **Calling Search Space**—The Forward No Answer Internal Calling Search Space is used to forward the call to the Forward No Answer Internal destination. It applies to all devices that use this directory number. **Note** If the system is using partitions and calling search spaces, Cisco recommends that you configure the Call Forward Calling Search Spaces. When a call is forwarded or redirected to the Call Forward destination, the configured Call Forward Calling Search Space is used to forward the call. If the **Calling Search Space** field is set to **None**, the forward operation fails if the system uses partitions and calling search spaces. For example, if you configure the Forward No Answer destination, you should also configure the Forward No Answer Calling Search Space. If you do not configure the Forward No Answer Calling Search Space and the Forward No Answer destination is in a partition, the forward operation fails. **Note** When you choose a calling search space for internal calls, the system automatically copies this value to the calling search space setting for external calls. If you want external calls to be forwarded to a different calling search space, you must choose a different value in the **Calling Search Space** field for external calls.

Field	Description
Forward No Answer External	The fields in this row of fields specify the forwarding treatment for external calls to this directory number if the directory number does not answer. The **Destination** and **Calling Search Space** fields are used to redirect the call to the forward destination. Configure the following values: • **Voice Mail**—Check this check box to use the configured values in the **Voice Mail Profile Configuration** window. **Note** When this check box is checked, the calling search space of the voicemail pilot is used. Unified Communications Manager ignores the values in the **Destination** and the **Calling Search Space** fields. **Note** When this check box is checked for internal calls, the system automatically checks the **Voice Mail** check box for external calls. If you do not want external calls to be forwarded to the voicemail system, you must uncheck the **Voice Mail** check box for external calls. • **Destination**—This field indicates the directory number to which an external call is forwarded when the call is not answered. Use any dialable phone number, including an outside destination. **Note** When you enter a destination value for internal calls, the system automatically copies this value to the **Destination** field for external calls. If you want external calls to be forwarded to a different destination, you must enter a different value in the **Destination** field for external calls. • **Calling Search Space**—The Forward No Answer External Calling Search Space is used to forward the call to the Forward No Answer External destination. It applies to all devices that use this directory number. **Note** If the system is using partitions and calling search spaces, Cisco recommends that you configure the Call Forward Calling Search Spaces. When a call is forwarded or redirected to the Call Forward destination, the configured Call Forward Calling Search Space is used to forward the call. If the **Calling Search Space** field is set to **None**, the forward operation fails if the system uses partitions and calling search spaces. For example, if you configure the Forward Busy destination, you should also configure the Forward No Answer Calling Search Space. If you do not configure the Forward No Answer Calling Search Space and the Forward No Answer destination is in a partition, the forward operation fails. **Note** When you choose a calling search space for internal calls, the system automatically copies this value to the calling search space setting for external calls. If you want external calls to be forwarded to a different calling search space, you must choose a different value in the **Calling Search Space** field for external calls.

Field	Description
Forward No Coverage Internal	The **Destination** and **Calling Search Space** fields are used to redirect the call to the forward destination. Configure the following values: • **Voice Mail**—Check this check box to use the configured values in the **Voice Mail Profile Configuration** window. **Note** When this check box is checked, Unified Communications Manager ignores the values in the **Destination** and **Calling Search Space** fields. When this check box is checked for internal calls, the system automatically checks the **Voice Mail** check box for external calls. If you do not want external calls to forward to the voicemail system, you must uncheck the **Voice Mail** check box for external calls. • **Destination**—This field specifies the directory number to which an internal nonconnected call is forwarded when an application that controls that directory number fails. Use any dialable phone number, including an outside destination. **Note** When you enter a destination value for internal calls, the system automatically copies this value to the **Destination** field for external calls. If you want external calls to be forwarded to a different destination, you must enter a different value in the **Destination** field for external calls. • **Calling Search Space**—The Forward No Coverage Internal Calling Search Space is used to forward the call to the Forward No Coverage Internal destination. This value applies to all devices that use this directory number. **Note** If the system is using partitions and calling search spaces, Cisco recommends that you configure the Call Forward Calling Search Spaces. When a call is forwarded or redirected to the Call Forward destination, the configured Call Forward Calling Search Space is used to forward the call. If the **Calling Search Space** field is set to None, the forward operation fails if the system uses partitions and calling search spaces. For example, if you configure the Forward Busy destination, you should also configure the Forward No Coverage Calling Search Space. If you do not configure the Forward No Coverage Calling Search Space and the Forward Busy destination is in a partition, the forward operation fails. **Note** When you choose a calling search space for internal calls, the system automatically copies this value to the calling search space setting for external calls. If you want external calls to be forwarded to a different calling search space, you must choose a different value in the **Calling Search Space** field for external calls.

Field	Description
Forward No Coverage External	The **Destination** and **Calling Search Space** fields are et used to redirect the call to the forward destination. Specify the following values: • **Voice Mail**—Check this check box to use the configured values in the **Voice Mail Profile Configuration** window. **Note** When this check box is checked, Unified Communications Manager ignores the values in the **Destination** and the **Calling Search Space** fields. When this check box is checked for internal calls, the system automatically checks the **Voice Mail** check box for external calls. If you do not want external calls to forward to the voicemail system, you must uncheck the **Voice Mail** check box for external calls. • **Destination**—This field specifies the directory number to which an internal nonconnected call is forwarded when an application that controls that directory number fails. Use any dialable phone number, including an outside destination. **Note** When you enter a destination value for internal calls, the system automatically copies this value to the **Destination** field for external calls. If you want external calls to be forwarded to a different destination, you must enter a different value in the **Destination** field for external calls. • **Calling Search Space**—The Forward No Coverage External Calling Search Space is used to forward the call to the Forward No Coverage External destination. This value applies to all devices that use this directory number. **Note** If the system is using partitions and calling search spaces, Cisco recommends that you configure the Call Forward Calling Search Spaces. When a call is forwarded or redirected to the Call Forward destination, the configured call forward calling search space is used to forward the call. If the **Calling Search Space** is **None**, the forward operation may fail if the system is using partitions and calling search spaces. For example, if you configure the Forward No Coverage destination, you should also configure the Forward No Coverage Calling Search Space. If you do not configure the Forward No Coverage Calling Search Space, and the Forward No Coverage destination is in a partition, the forward operation may fail. **Note** When you choose a calling search space for internal calls, the system automatically copies this value to the calling search space setting for external calls. If you want external calls to be forwarded to a different calling search space, choose a different value in the **Calling Search Space** field for external calls.
Forward on CTI Failure	This field applies only to CTI route points and CTI ports. The fields in this row specify the forwarding treatment for external calls to this CTI route point or CTI port if the CTI route point or CTI port fails. Configure the following values: • **Voice Mail**—Check this check box to use the configured values in the **Voice Mail Profile Configuration** window. **Note** When this check box is checked, Unified Communications Manager ignores the values in the **Destination** and **Calling Search Space** fields. • **Destination**—This field specifies the directory number to which an internal nonconnected call is forwarded when an application that controls that directory number fails. Use any dialable phone number, including an outside destination. • **Calling Search Space**—This value applies to all devices that use this directory number.
Forward Unregistered Internal	This field applies to unregistered internal DN calls. The calls are rerouted to a specified destination or voicemail. **Note** You must also specify the maximum number of forwards in the **Service Parameters Configuration** window for a directory number in the **Max Forward UnRegistered Hops to DN** service parameter. This parameter specifies the maximum number of forward unregistered hops that are allowed for a directory number at the same time. This parameter limits the number of times the call can be forwarded due to unregistered DN when a forwarding loop occurs. Use this count to stop forward loops for external calls that have been Call Forward Unregistered. Unified Communications Manager terminates the call when the value that is specified in this service parameter is exceeded.

Field	Description
Forward Unregistered External	This field applies to unregistered external DN calls. The calls are rerouted to a specified destination or voicemail. **Note** You must also specify the maximum number of forwards in the **Service Parameters Configuration** window for a directory number in the **Max Forward UnRegistered Hops to DN** service parameter. This parameter specifies the maximum number of forward unregistered hops that are allowed for a directory number at the same time. This parameter limits the number of times the call can be forwarded due to unregistered DN when a forwarding loop occurs. Use this count to stop forward loops for external calls that have been Call Forward Unregistered. Unified Communications Manager terminates the call when the value that is specified in this service parameter is exceeded.
No Answer Ring Duration (seconds)	This field specifies the seconds to wait before forwarding the unanswered call to the Call Forward No Answer destination, if specified. Make sure the value that is specified in this parameter is less than the value that is specified in the **T301 Timer** service parameter. If the value in the **Forward No Answer Timer** service parameter is greater than the value that is specified in the **T301 Timer** service parameter, the call is not forwarded and the caller receives a busy signal. Leave this field empty if you want to set the value in the Cisco Unified Communications Manager **Forward No Answer Timer** service parameter.

Enable Destination Override for Call Forwarding

Enable the destination override for call forwarding, Unified Communications Manager ignores the CFA destination when it matches the calling party number. The override applies to both internal and external calls.

In cases where the calling party number has been transformed, the calling party number does not match the CFA destination, no override occurs.

Before you begin

Configure Other Call Forwarding Types, on page 316

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Service Parameters**.
The **Service Parameter Configuration** window is displayed.

Step 2 In the **Clusterwide Parameters (Feature - Hold Reversion)** area, set the **CFA Destination Override** service parameter value to **True**.

Call Forwarding Interactions and Restrictions

Call Forwarding Interactions

Feature	Interaction
Call Back	Calls that are made from the CallBack notification screen will override all the Call Forward configured values on the target DN. The calls should be made before the CallBack recall timer expires, otherwise the calls will not override the Call Forward configured values.
Call Display Restrictions	The Connected Number Display restriction applies to all calls that originate in the system. When this value is set to **True**, this field interacts transparently with existing Unified Communications Manager applications, features, and call processing. The value applies to all calls that terminate inside or outside the system. The Connected Number Display is updated to show the modified number or redirected number when a call is routed to a Call Forward All or Call Forward Busy destination, or gets redirected through a call transfer or CTI application.
Do Not Disturb	On Cisco Unified IP Phones, the message that indicates that the Do Not Disturb (DND) feature is active takes priority over the message that indicates that the user has new voice messages. However, the message that indicates that the Call Forward All feature is active has a higher priority than DND.
External Call Control	External Call Control intercepts calls at the translation pattern level, while Call Forward intercepts calls at the directory number level. External Call Control has higher priority; for calls where call forward is invoked, Unified Communications Manager sends a routing query to the adjunct route server if the translation pattern has an External Call Control profile assigned to it. Call Forwarding is triggered only when the adjunct route server sends a Permit decision with a Continue obligation to the Unified Communications Manager. **Note** The **Call Diversion Hop Count** service parameter that supports External Call Control, and the **Call Forward Call Hop Count** service parameter that supports Call Forwarding are independent of each other; they work separately.
Extension Mobility Cross Cluster	Cisco Extension Mobility Cross Cluster supports Call Forwarding.
Extend and Connect	Extend and Connect supports Call Forward All.

Feature	Interaction
Immediate Divert	When the Forward No Answer field in the **Directory Number Configuration** window is not configured, Call Forward uses the clusterwide CFNA timer service parameter, **Forward No Answer Timer**. If a user presses the iDivert softkey at the same time as the call is being forwarded, the call gets diverted to an assigned call forward directory number (because the amount of time set on the timer was too short), not the voicemail. To resolve this situation, set the CFNA timer service parameter to enough time (for example, 60 seconds).
Logical Partitioning	Unified Communications Manager performs logical partitioning policy check using the geolocation identifier information that associates with the incoming and forwarded devices. This handling applies to all types of call forwarding.

Feature	Interaction
Multilevel Precedence and Preemption (MLPP)	**Call Forward Busy** • You can optionally configure a preconfigured Precedence Alternate Party target for any MLPP-enabled station. • Cisco Unified Communications Manager applies the Call Forward Busy feature to forward a precedence call in the usual manner before it applies to any Precedence Alternate Party Diversion procedures to the call. • The system preserves precedence of calls across multiple forwarded calls. • If the incoming precedence call is of higher precedence than the existing call, preemption occurs. Both the preempted parties in the active call receive a continuous preemption tone until the station to which the precedence call is directed hangs up. After hanging up, the station to which the precedence call is directed receives precedence ringing. The destination station connects to the preempting call when the station goes off hook. **Call Forward No Answer** • For calls of Priority precedence level and above, call processing preserves the precedence level of calls during the forwarding process and may preempt the forwarded-to user. • If an Alternate Party is configured for the destination of a precedence call, call processing diverts the precedence call to the Alternate Party after the Precedence Call Alternate Party timeout expires. If no Alternate Party value is configured for the destination of a precedence call, call processing diverts the precedence call to the Call Forward No Answer value. • Normally, precedence calls are routed to users and not to the voicemail system. The administrator sets the **Use Standard VM Handling For Precedence Calls** enterprise parameter to avoid routing precedence calls to voicemail systems. If the incoming precedence call is of equal or lower precedence than the existing call, call processing invokes normal call-forwarding behavior. If the destination station for a precedence call is nonpreemptable (that is, not MLPP-configured), call processing invokes call-forwarding behavior. Alternate Party Diversion (APD) comprises a special type of call forwarding. If users are configured for APD, APD takes place when a precedence call is directed to a directory number (DN) that is busy or does not answer. MLPP APD applies only to precedence calls. An MLPP APD call disables the DN Call Forward No Answer value for precedence calls.

Feature	Interaction
Originally called party name in Placed Call History	When privacy is configured only in the SIP profile of the called party device and Call Forward All (CFA), or Call Forward Busy (CFB), or Call Forward Unregistered (CFUR) is enabled, the configured alerting name is displayed instead of "private". To ensure that "private" is displayed for call forwarding, Cisco recommends that you configure the name presentation restriction in the translation pattern or the route pattern rather than in the SIP profile.
Rollover Lines	By using call forwarding settings, you can create rollover lines for a shared line. This could be a useful for some call center situations. With rollover lines, when someone dials a number (e.g. 1-800-HOTLINE), the call always is routed to a specific phone line. This may be a shared line that is shared by multiple phones. If line 1 is busy, the call rolls over to line 2, if line 2 is busy it rolls over to line 3, and so on. Line 2 or 3 become available only if line 1 is busy. This type of call functionality is possible via call forwarding busy settings and the Busy Trigger as follows: • On line 1, set the Busy Trigger to 1 and configure Call Forward Busy to the second line in the chain. • On line 2, set the Busy Trigger to 1 and configure Call Forward Busy to the third line in the chain • Continue this for as many lines as meets your needs.
Secure Tone	Call Forward All is supported on protected phones.
Session Handoff	When the user hands off a call, a new call gets presented on the desk phone. While the desk phone is flashing, Call Forward All is not triggered on the desk phone for the call that was handed off.

Call Forwarding Restrictions

Feature	Restriction
Call Forwarding	• If Call Forward All activation occurs in Unified Communications Manager or the Cisco Unified Communications Self Care Portal, Unified Communications Manager does not prevent the CFA loop. • Unified Communications Manager prevents Call Forward All loops if CFA is activated from the phone, if the number of hops for a Call Forward All call exceeds the value that is specified for the Forward Maximum Hop Count service parameter, and if all phones in the forwarding chain have CFA activated (not CFB, CFNA, or any other call forwarding options). For example, if the user with directory number 1000 forwards all calls to directory number 1001, which has CFB and CFNA configured to directory number 1002, which has CFA configured to directory number 1000, Unified Communications Manager allows the call to occur because directory number 1002 acts as the CFB and CFNA (not CFA) destination for directory number 1001. • You cannot activate Call Back if you forward all calls to voicemail system. • An uncommon condition in connection with the Forward No Answer Timeout exists when you press the iDivert softkey. For example, if a manager presses the iDivert softkey immediately after the Forward No Answer timeout, Call Forward forwards the call to a preconfigured directory number. However, if the manager presses the iDivert softkey before the Forward No Answer timeout, Immediate Divert diverts the call to the voicemail of the manager.
Immediate Divert	When Call Forward All (CFA) and Call Forward Busy (CFB) are activated, the system does not support Immediate Divert (CFA and CFB have precedence over Immediate Divert).
Intercom	You cannot forward Intercom calls.
Log Out of Hunt Group	When a phone that is running SIP (7906, 7911, 7941, 7961, 7970, and 7971) is logged in to hunt groups and Call Forward All is activated, the call gets presented to the phone that is running SIP. When 7940 and 7960 IP phones that are running SIP are logged in to hunt groups and Call Forward All is activated, the phone gets skipped and the next phone in the line group is rung.

Feature	Restriction
Logical Partitioning	Logical partitioning handling does not take place in the following circumstances: • When both the caller and forwarded devices are Voice over IP (VoIP) phones. • When geolocation or a geolocation filter is not associated with any device.
Multilevel Precedence and Preemption (MLPP)	Multilevel Precedence and Preemption (MLPP) support for supplementary services specifies the following restrictions for Call Forwarding: • Call Forward All (CFA) support for inbound MLPP calls always forwards the call to the MLPP Alternate Party (MAP) target of the called party, if the MAP target is configured. In the event of an incorrect configuration (that is, if no MAP target is specified), the call gets rejected, and the calling party receives reorder tone. • Call Forward No Answer (CFNA) support for inbound MLPP calls forwards the call once to a CFNA target. After the first hop, if the call remains unanswered, the call is sent to the MAP target of the original called party, if the MAP target is configured. In the event of an incorrect configuration (that is, if no MAP target is specified), the call gets rejected, and the calling party receives reorder tone. • Call Forward Busy (CFB) support for inbound MLPP calls forwards the call up to the maximum number that is configured for forwarding hops. If the maximum hop count is reached, the call is sent to the MAP target of the original called party, if the MAP target is configured. In the event of an incorrect configuration (that is, no MAP target is specified), the call gets rejected, and the calling party receives reorder tone.
Call Forward Classification with Call Transfer	When a call is transferred, the call classification takes on the classification of the transferred leg, rather than the original leg. For example: • Incoming call from PSTN is received by a receptionist. This is an external call. • The receptionist transfers the call to extension 3100. The transferred call is now an internal call. • The user at extension 3100 is busy, but has Call Forward External configured to send external calls back to the receptionist. However, because the call takes on the classification of the second leg (internal), the call goes to voicemail.

CHAPTER 25

Call Pickup

Call Pickup Overview

The Call Pickup feature allows users to answer calls that come in on a directory number other than their own.

Group Call Pickup Overview

The Group Call Pickup feature allows users to pick up incoming calls in another group. Users must dial the appropriate call pickup group number when this feature is activated from a Cisco Unified IP Phone. Use the softkey, GPickUp, for this type of call pickup. When the user invokes the Group Call Pickup phone feature while multiple calls are incoming to a pickup group, the user gets connected to the incoming call that has been ringing the longest. Depending on the phone model, the users can either use the Group Pickup programmable feature button or the Group Pickup softkey to pick up an incoming call. If Auto Group Call Pickup is not enabled, the user must press the GPickUp softkey, dial the group number of another pickup group, and answer the call to make the connection.

Other Group Pickup Overview

The Other Group Pickup feature allows users to pick up incoming calls in a group that is associated with their own group. The Unified Communications Manager automatically searches for the incoming call in the associated groups to make the call connection when the user activates this feature from a Cisco Unified IP Phone. Users use the softkey, OPickUp, for this type of call pickup. If Auto Other Group Pickup is not enabled, the user must press the softkeys, OPickUp and Answer, to make the call connection. Depending on the phone model, the users can either use the Call Pickup programmable feature button or the Call Pickup softkey to pick up an incoming call.

When more than one associated group exists, the first associated group has the highest the priority of answering calls for the associated group. For example, groups A, B, and C associate with group X, the group A has the highest priority and the group C has the lowest priority of answering calls. The group X picks up incoming call in group A, though a call may have come in earlier in group C than the incoming call in group A.

Note The longest alerting call (longest ringing time) gets picked up first if multiple incoming calls occur in that group. For other group call pickup, priority takes precedence over the ringing time if multiple associated pickup groups are configured.

Directed Call Pickup Overview

The Directed Call Pickup feature allows a user to pick up a ringing call on a DN directly by pressing the GPickUp or Group Pickup softkeys and entering the directory number of the device that is ringing. If Auto Directed Call Pickup is not enabled, the user must press the GPickUp softkey, dial the DN of the ringing phone, and answer the call that will now ring on the user phone to make the connection. Unified Communications Manager uses the associated group mechanism to control the privilege of a user who wants to pick up an incoming call by using Directed Call Pickup. The associated group of a user specifies one or more call pickup groups that are associated to the pickup group to which the user belongs.

If a user wants to pick up a ringing call from a DN directly, the associated groups of the user must contain the pickup group to which the DN belongs. If two users belong to two different call pickup groups and the associated groups of the users do not contain the call pickup group of the other user, the users cannot invoke Directed Call Pickup to pick up calls from each other.

When the user invokes the Directed Call Pickup feature and enters a DN to pick up an incoming call, the user connects to the call that is incoming to the specified phone whether or not the call is the longest ringing call in the call pickup group to which the DN belongs. If multiple calls are ringing on a particular DN and the user invokes Directed Call Pickup to pick up a call from the DN, the user connects to the incoming call that has been ringing the specified DN the longest.

BLF Call Pickup Overview

The BLF Call Pickup feature allows Unified Communications Manager to notify a phone user when a call is waiting to be picked up from a BLF DN. The BLF call pickup initiator (the phone that picks up the call) is selected as the next available line or as a specified line. To use a specified line, the line must remain off hook before the BLF SD button is pressed. You can configure a hunt list member DN as the BLF DN to allow an incoming call to a hunt list member to be picked up by the BLF call pickup initiator. The incoming call on the hunt list member can come from the hunt list or be a directed call. The behavior in each case depends on how you configure call pickup for the hunt list member DN, the BLF DN, and the hunt pilot number. When a Call Pickup occurs with the service parameter Auto Call Pickup Enabled set to false, the phone must remain off hook or the user must press the answer key to pick up the call.

The BLF SD button on the phone can exist in any of the following states:

- Idle—Indicates that no call exists on the BLF DN.
- Busy—Indicates that at least one active call exists on the BLF DN, but no alerts exist.
- Alert— Indicates by flashing that at least one incoming call exists on the BLF DN.

When there is an incoming call to the BLF DN, the BLF SD button flashes on the BLF call pickup initiator phone to indicate that an incoming call to the BLF DN exists. If Auto Call Pickup is configured, the user presses the BLF SD button on the call pickup initiator phone to pick up the incoming call. If auto call pickup is not configured, the phone must remain off hook, or the user must press the answer key to pick up the call.

Call Pickup Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure a Call Pickup Group, on page 337	Configure a call pickup group for each of the call pickup features that you want to use: • Call Pickup • Group Call Pickup • Other Call Pickup • Directed Call Pickup • BLF Call Pickup You must define groups with unique names and numbers.
Step 2	Assign a Call Pickup Group to Directory Numbers, on page 337	Assign each of the call pickup groups that you created to the directory numbers that are associated with phones on which you want to enable call pickup. Directory numbers must be assigned to a call pickup group to use this feature. Repeat this procedure for each call pickup group that you create.
Step 3	Create another call pickup group and associate it with the BLF call pickup group that you created in Step 1, on page 335. You can associate a call pickup group with multiple BLF DN call pickup groups.	Perform this step if you are configuring BLF Call Pickup. **Note** You do not always need to create another call pickup group. For example, you can have a single call pickup group that includes both the initiator DN and the destination DN. In such cases, associate the BLF call pickup group with itself.
Step 4	Configure Partitions for Call Pickup, on page 338	Configure partitions to create a logical grouping of directory numbers (DN) with similar reachability characteristics. You can use partitions to restrict access to call pickup groups. If you assign call pickup group numbers to a partition, only those phones that can dial numbers in that partition can use the call pickup group.

	Command or Action	Purpose
		You must complete this procedure for directed call pickup. It is optional for other types of call pickup.
Step 5	Configure Calling Search Space, on page 339	If you configure partitions, you must also configure calling search spaces. Configure calling search spaces to identify the partitions that calling devices can search when they attempt to complete a call. You must complete this procedure for directed all pickup. It is optional for other types of call pickup.
Step 6	Assign a Call Pickup Group to Hunt Pilots, on page 340	**(Optional).** Assign a call pickup group to a hunt pilot DN so that users can pick up calls that are alerting in the line group members. Hunt lists that are assigned to a call pickup group can use Call Pickup, Group Call pickup, BLF Call Pickup, Other Group Pickup, and Directed call pickup.
Step 7	Configure notifications: • Configure Call Pickup Notification, on page 340 • Configure Call Pickup Notification for a Directory Number, on page 343 • Configure BLF Call Pickup Notification, on page 341	**(Optional).** Configure notifications when other members of a pickup group receive a call. You can configure audio or visual notifications, or both.
Step 8	Configure Directed Call Pickup: • Configure a Time Period, on page 344 • Configure Time Schedule, on page 344 • Associate a Time Schedule with a Partition, on page 344	Before you configure directed call pickup, you must configure partitions and calling search spaces. With directed call pickup, the calling search space of the user who requests the Directed Call Pickup feature must contain the partition of the DN from which the user wants to pick up a call. Time periods and time schedules specify the times when members in the associated group are available to accept calls.
Step 9	Configure automatic call answering: • Configure Auto Call Pickup, on page 345 • Configure BLF Auto Pickup, on page 346	**(Optional).** Enable automatic call answering and configure timers for automatic call answering.
Step 10	Configure phone button templates: • Configure Call Pickup Phone Button Template, on page 347	Configure phone button templates for any of the call pickup features that you want to use: • Speed Dial BLF

	Command or Action	Purpose
	• Associate Call Pickup Button Template with Phone, on page 347 • Configure BLF Speed Dial Number for the BLF Call Pickup Initiator, on page 348	• Call Pickup • Group Call Pickup • Other Group Pickup For Directed Call Pickup, use the Group Call Pickup button.
Step 11	Configure Softkeys for Call Pickup, on page 348 • Configure a Softkey Template for Call Pickup, on page 349 • Associate a Softkey Template with a Common Device Configuration, on page 350 • Associate a Softkey Template with a Phone , on page 351	Configure softkeys for any of the call pickup features that you want to use: • Call Pickup (Pickup) • Group Call Pickup (GPickup) • Other Group Pickup (OPickup) For Directed Call Pickup, use the Group Call Pickup softkey.

Configure a Call Pickup Group

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Call Pickup Group**.
The **Find and List Call Pickup Groups** window appears.

Step 2 Click **Add New**.
The **Call Pickup Group Configuration** window appears.

Step 3 Configure the fields in the **Call Pickup Group Configuration** window. For more information on the fields and their configuration options, see Online Help.

Assign a Call Pickup Group to Directory Numbers

This section describes how to assign a call pickup group to a directory number. Only directory numbers that are assigned to a call pickup group can use call pickup, group call pickup, BLF call pickup, other group pickup, and directed call pickup. If partitions are used with call pickup numbers, make sure that the directory numbers that are assigned to the call pickup group have a calling search space that includes the appropriate partitions.

Before you begin

Configure a Call Pickup Group, on page 337

Procedure

Step 1 Choose **Device** > **Phone or Call Routing** > **Directory Number**.

Step 2 Enter the appropriate search criteria to find the phone or directory number that you want to assign to a call pickup group and click **Find.**

A list of phones or directory numbers that match the search criteria displays.

Step 3 Choose the phone or directory number to which you want to assign a call pickup group.

Step 4 From the **Association Information** list in the **Phone Configuration** window, choose the directory number to which the call pickup group will be assigned.

Step 5 From the **Call Pickup Group** drop-down list that displays in the Call Forward and Call Pickup Settings area, choose the desired call pickup group.

Step 6 To save the changes in the database, click **Save.**

What to do next

Perform the following tasks:

- Configure Partitions for Call Pickup, on page 338
- Configure Calling Search Space, on page 339

Configure Partitions for Call Pickup

You can restrict access to call pickup groups by assigning a partition to the call pickup group number. When this configuration is used, only the phones that have a calling search space that includes the partition with the call pickup group number can participate in that call pickup group. Make sure that the combination of partition and group number is unique throughout the system. You can create multiple partitions.

If you assign call pickup group numbers to a partition, only those phones that can dial numbers in that partition can use the call pickup group. If partitions represent tenants in a multitenant configuration, make sure that you assign the pickup groups to the appropriate partition for each tenant.

Before you begin

Assign a Call Pickup Group to Directory Numbers, on page 337

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Partition**.

Step 2 In the **Partition Name, Description** field, enter a name for the partition that is unique to the route plan.

Partition names can contain alphanumeric characters, as well as spaces, hyphens (-), and underscore characters (_). See the online help for guidelines about partition names.

Step 3 Enter a comma (,) after the partition name and enter a description of the partition on the same line.

The description can contain up to 50 characters in any language, but it cannot include double quotes ("), percentage sign (%), ampersand (&), backslash (\), angle brackets (<>), or square brackets ([ ]).

If you do not enter a description, Cisco Unified Communications Manager automatically enters the partition name in this field.

Step 4 To create multiple partitions, use one line for each partition entry.

Step 5 From the **Time Schedule** drop-down list, choose a time schedule to associate with this partition.

The time schedule specifies when the partition is available to receive incoming calls. If you choose **None**, the partition remains active at all times.

Step 6 Select one of the following radio buttons to configure the **Time Zone**:

- **Originating Device**—When you select this radio button, the system compares the time zone of the calling device to the **Time Schedule** to determine whether the partition is available is available to receive an incoming call.
- **Specific Time Zone**—After you select this radio button, choose a time zone from the drop-down list. The system compares the chosen time zone to the **Time Schedule** to determine whether the partition is available is available to receive an incoming call.

Step 7 Click **Save**.

Configure Calling Search Space

A calling search space is an ordered list of route partitions that are typically assigned to devices. Calling search spaces determine the partitions that calling devices can search when they are attempting to complete a call.

Before you begin

Configure Partitions for Call Pickup, on page 338

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Calling Search Space**.

Step 2 Click **Add New**.

Step 3 In the **Name** field, enter a name.

Ensure that each calling search space name is unique to the system. The name can include up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_).

Step 4 In the **Description** field, enter a description.

The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).

Step 5 From the **Available Partitions** drop-down list, perform one of the following steps:

- For a single partition, select that partition.
- For multiple partitions, hold down the **Control (CTRL)** key, then select the appropriate partitions.

Step 6 Select the down arrow between the boxes to move the partitions to the **Selected Partitions** field.

Step 7 (Optional) Change the priority of selected partitions by using the arrow keys to the right of the **Selected Partitions** box.

Step 8 Click **Save**.

Assign a Call Pickup Group to Hunt Pilots

Only hunt lists that are assigned to a call pickup group can use Call Pickup, Group Call Pickup, BLF Call Pickup, Other Group Pickup, and Directed Call Pickup. Follow these steps to assign a call pickup group to hunt pilots:

Before you begin

Configure Calling Search Space, on page 339

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Route/Hunt** > **Hunt Pilot**.

Step 2 Enter the appropriate search criteria to find the hunt pilot that you want to assign to a call pickup group and click **Find**. A list of hunt pilots that match the search criteria appears.

Step 3 Choose the hunt pilot to which you want to assign a call pickup group.

Step 4 From the **Call Pickup Group** drop-down list that appears in the **Hunt Forward Settings** area, choose the desired call pickup group.

Step 5 Click **Save**.

Configure Call Pickup Notification

You can configure Call Pickup Notification at the system level, call pickup group level, or individual phone level.

Before you begin

Assign a Call Pickup Group to Hunt Pilots, on page 340

Procedure

	Command or Action	Purpose
Step 1	Configure Call Pickup Notification for a Call Pickup Group, on page 342	To allow the original called party to pick up the call prior to the audio and/or visual alert being sent to the pickup group.
Step 2	Configure Call Pickup Notification for a Directory Number, on page 343	To configure the type of audio alert to be provided when phone is idle or has an active call.
Step 3	Configure BLF Call Pickup Notification, on page 341	

Configure BLF Call Pickup Notification

Before you begin

Configure Call Pickup Notification for a Directory Number, on page 343

Procedure

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

Step 2 From the **Server** drop-down list, choose the server that is running the Cisco CallManager service.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.

Step 4 Configure the fields from **Clusterwide Parameters (Device - Phone** section in the **Service Parameter Configuration** window. See Service Parameter Fields for BLF Call Pickup Notification, on page 341 for more information about the fields and their configuration options.

Service Parameter Fields for BLF Call Pickup Notification

Field	Description
Call Pickup Group Audio Alert Setting of Idle Station	This parameter determines the kind of audio notification that is provided when a phone is idle (not in use) and it needs to be alerted regarding an incoming call on its Call Pickup Group. Valid values are as follows: • Disable • Ring Once
Call Pickup Group Audio Alert Setting of Busy Station	This parameter determines the kind of audio notification that is provided when a phone is busy (in use) and it needs to be alerted regarding an incoming call on its Call Pickup Group. Valid values are as follows: • Disable • Beep Only
BLF Pickup Group Audio Alert Setting of Idle Station	This parameter determines the kind of audio notification that is provided when a phone is idle and it needs to be alerted regarding an incoming call on the BLF Pickup Button. Valid values are as follows: • No Ring • Ring Once

Field	Description
BLF Pickup Group Audio Alert Setting of Busy Station	This parameter determines the kind of audio notification that is provided when a phone is busy and it needs to be alerted regarding an incoming call on the BLF Pickup Button. Valid values are as follows: • No Ring • Beep Only

Configure Call Pickup Notification for a Call Pickup Group

Before you begin

Assign a Call Pickup Group to Hunt Pilots, on page 340

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Call Pickup Group**.
The **Call Pickup Group** window appears.

Step 2 Configure the fields in the **Call Pickup Group Notification Settings** section in the **Call Pickup Group Configuration** window. See Call Pickup Notification Fields for Call Pickup, on page 342 for details about the fields and their configuration options.

Note Refer to **Call Pickup Interactions and Restrictions** for feature interactions and restrictions that will affect your Call Pickup configuration.

Call Pickup Notification Fields for Call Pickup

Field	Description
Call Pickup Group Notification Policy	From the drop-down list, select the notification policy. The available are options are No Alert, Audio Alert, Visual Alert, and Audio and Visual Alert.
Call Pickup Group Notification Timer	Enter the seconds of delay (integer in the range of 1 to 300) between the time that the call first comes into the original called party and the time that the notification to the rest of the call pickup group is sent.
Calling Party Information	Check the check box if you want the visual notification message to the call pickup group to include identification of the calling party. The system only makes this setting available when the Call Pickup Group Notification Policy is set to Visual Alert or Audio and Visual Alert.

Field	Description
Called Party Information	Check the check box if you want the visual notification message to the call pickup group to include identification of the original called party. The system makes this setting available when the Call Pickup Group Notification Policy is set to Visual Alert or Audio and Visual Alert.

Configure Call Pickup Notification for a Directory Number

Perform these steps to configure the type of audio notification that is provided when a phone is idle or in use.

Before you begin

Configure Call Pickup Notification for a Call Pickup Group, on page 342

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Directory Number**.
The **Find and List Directory Numbers** window appears.

Step 2 Enter the search criteria and click **Find**.

Step 3 Click the directory number for which you want to configure the Call Pickup Notification.
The **Directory Number Configuration** window appears.

Step 4 Choose a device name in the **Associated Devices** pane and click the **Edit Line Appearance** button.
The **Directory Number Configuration** window refreshes to show the line appearance for this DN on the device that you choose.

Step 5 From the **Call Pickup Group Audio Alert Setting(Phone Idle)** drop-down list, choose one of the following:

- Use System Default
- Disable
- Ring Once

Step 6 From the **Call Pickup Group Audio Alert Setting(Phone Active)** drop-down list, choose one of the following:

- Use System Default
- Disable
- Beep Only

Step 7 Click **Save**.

Configure Directed Call Pickup

Procedure

	Command or Action	Purpose
Step 1	Configure a Time Period, on page 344	Configure time period for members of the associated groups to your group.
Step 2	Configure Time Schedule, on page 344	Configure time schedule for members of the associated groups to your group.
Step 3	Associate a Time Schedule with a Partition, on page 344	Associate time schedules with partitions to determine where calling devices search when they are attempting to complete a call during a particular time of a day.

Configure a Time Period

Use this procedure to define time periods. You can define a start time and an end time, and also specify repetition interval either as days of the week or a specified date on the yearly calendar.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Time Period**.

Step 2 Configure the fields in the **Time Period Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 3 Click **Save**.

Configure Time Schedule

Before you begin

Configure a Time Period, on page 344

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Time Schedule**.

Step 2 Configure the fields in the **Time Schedule Configuration** window. For more information on the fields and their configuration options, see Online Help.

Associate a Time Schedule with a Partition

Associate time schedules with partitions to determine where calling devices search when they are attempting to complete a call during a particular time of day.

Before you begin

Configure Time Schedule, on page 344

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Partition**.

Step 2 From the **Time Schedule** drop-down list, choose a time schedule to associate with this partition.
The time schedule specifies when the partition is available to receive incoming calls. If you choose **None**, the partition remains active at all times.

Step 3 Click **Save**.

Configure Automatic Call Answering

Procedure

	Command or Action	Purpose
Step 1	Configure Auto Call Pickup, on page 345	You can automate call pickup, group pickup, other group pickup, directed call pickup, and BLF call pickup. If you do not enable automatic call answering, users must press additional softkeys or dial group numbers to complete the connection.
Step 2	Configure BLF Auto Pickup, on page 346	

Configure Auto Call Pickup

Auto call pickup connects the user to an incoming call. When the user presses the softkey on the phone, Unified Communications Manager locates the incoming call in the group and completes the call connection. You can automate call pickup, group pickup, other group pickup, directed call pickup, and BLF call pickup. If you do not enable automatic call answering, users must press additional softkeys or dial group numbers to complete the connection.

Before you begin

Associate a Time Schedule with a Partition, on page 344

Procedure

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

Step 2 From the Server drop-down list, choose the server that is running the Cisco CallManager service.

Step 3 From the Service drop-down list, choose **Cisco CallManager**.

Step 4 In the **Clusterwide Parameters (Feature – Call Pickup)** section, select **True** or **False** from the **Auto Call Pickup Enabled** drop-down list to enable or disable automatic call answering for call pickup groups.

Step 5 If the **Auto Call Pickup Enabled** service parameter is False, enter a value from 12 to 300 in the **Call Pickup No Answer Timer** field. This parameter controls the time that a call takes to get restored if the call is picked up but not answered by using call pickup, group call pickup, or other group call pickup.

Step 6 In the **Pickup Locating Timer** field, enter a value from 1 to 5. This service parameter specifies the maximum time, in seconds, for Cisco Unified Communications Manager to identify all alerting calls from all nodes in the cluster. This information is then used to help ensure that the call that has been waiting longest in the queue is delivered to the next user who presses the PickUp, GPickUp, or OPickUp softkey.

Step 7 Click **Save**.

Configure BLF Auto Pickup

Before you begin

Configure Auto Call Pickup, on page 345

Procedure

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

Step 2 From the **Server** drop-down list, choose the server that is running the Cisco CallManager service.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.

Step 4 Configure values for the following clusterwide service parameters.

- BLF Pickup Audio Alert Setting of Idle Station—Select **True** or **False** from the drop-down list to enable or disable automatic call answering for call pickup groups. The default value for this service parameter is False.
- BLF Pickup Audio Alert Setting of Busy Station—If the Auto Call Pickup Enabled service parameter is False, enter a value from 12 to 300 (inclusive). This parameter controls the time that a call takes to get restored if the call is picked up but not answered by using call pickup, group call pickup, or other group call pickup.

Configure Call Pickup Phone Buttons

Procedure

	Command or Action	Purpose
Step 1	Configure Call Pickup Phone Button Template, on page 347	Add Call Pickup feature to the phone button template.
Step 2	Associate Call Pickup Button Template with Phone, on page 347	
Step 3	Configure BLF Speed Dial Number for the BLF Call Pickup Initiator, on page 348	

Configure Call Pickup Phone Button Template

Follow these steps to add Call Pickup feature to the phone button template.

Before you begin

Configure Automatic Call Answering, on page 345

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Phone Button Template**.

Step 2 Click **Find** to display list of supported phone templates.

Step 3 Perform the following steps if you want to create a new phone button template; otherwise, proceed to the next step.

a) Select a default template for the model of phone and click **Copy**.
b) In the **Phone Button Template Information** field, enter a new name for the template.
c) Click **Save**.

Step 4 Perform the following steps if you want to add phone buttons to an existing template.

a) Click **Find** and enter the search criteria.
b) Choose an existing template.

Step 5 From the **Line** drop-down list, choose feature that you want to add to the template.

Step 6 Click **Save**.

Step 7 Perform one of the following tasks:

- Click **Apply Config** if you modified a template that is already associated with devices to restart the devices.
- If you created a new softkey template, associate the template with the devices and then restart them.

Associate Call Pickup Button Template with Phone

Before you begin

Configure Call Pickup Phone Button Template, on page 347

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** to display the list of configured phones.

Step 3 Choose the phone to which you want to add the phone button template.

Step 4 In the **Phone Button Template** drop-down list, choose the phone button template that contains the new feature button.

Step 5 Click **Save**.

A dialog box is displayed with a message to press **Reset** to update the phone settings.

Configure BLF Speed Dial Number for the BLF Call Pickup Initiator

Before you begin

Associate Call Pickup Button Template with Phone, on page 347

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Select the phone that you want to use as the BLF call pickup initiator.

Step 3 In the **Association** pane, **Add a new BLF SD** link.
The **Busy Lamp Field Speed Dial Configuration** window appears.

Step 4 Select a **Directory Number** (BLF DN) that should be monitored by the BLF SD button.

Step 5 Check the **Call Pickup** check box to use the BLF SD button for BLF Call Pickup and BLF Speed Dial. If you do not check this check box, the BLF SD button will be used only for BLF Speed Dial.

Step 6 Click **Save**.

Configure Softkeys for Call Pickup

Procedure

	Command or Action	Purpose
Step 1	Configure a Softkey Template for Call Pickup, on page 349	Add the Pickup, GPickup, and OPickup softkeys to a softkey template.
Step 2	To Associate a Softkey Template with a Common Device Configuration, on page 350, complete the following subtasks: • Add a Softkey Template to Common Device Configuration, on page 350 • Associate a Common Device Configuration with a Phone, on page 351	**Optional**. To make the softkey template available to phones, you must complete either this step or the following step. Follow this step if your system uses a Common Device Configuration to apply configuration options to phones. This is the most commonly used method for making a softkey template available to phones.
Step 3	Associate a Softkey Template with a Phone , on page 351	**Optional**. Use this procedure either as an alternative to associating the softkey template with the Common Device Configuration, or in conjunction with the Common Device Configuration. Use this procedure in conjunction with the Common Device Configuration if you need assign a softkey template that overrides the assignment in the

	Command or Action	Purpose
		Common Device Configuration or any other default softkey.

Configure a Softkey Template for Call Pickup

Use this procedure to make the following call pickup softkeys available:

Softkey	Description	Call States
Call Pickup (**Pickup**)	Allows you to answer a call on another extension in your group.	On Hook Off Hook
Group Call Pickup (**GPickup**)	Allows you to answer a call on extension outside your group.	On Hook Off Hook
Other Group Pickup (**OPickup**)	Allows you to answer a call ringing in another group that is associated with your group.	On Hook Off Hook

Before you begin

Configure Call Pickup Phone Buttons, on page 346

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Softkey Template**.

Step 2 Perform the following steps to create a new softkey template; otherwise, proceed to the next step.

a) Click **Add New**.
b) Select a default template and click **Copy**.
c) Enter a new name for the template in the **Softkey Template Name** field.
d) Click **Save**.

Step 3 Perform the following steps to add softkeys to an existing template.

a) Click **Find** and enter the search criteria.
b) Select the required existing template.

Step 4 Check the **Default Softkey Template** check box to designate this softkey template as the default softkey template.

Note If you designate a softkey template as the default softkey template, you cannot delete it unless you first remove the default designation.

Step 5 Choose **Configure Softkey Layout** from the **Related Links** drop-down list in the upper right corner and click **Go**.

Step 6 From the **Select a Call State to Configure** drop-down list, choose the call state for which you want the softkey to display.

Step 7 From the **Unselected Softkeys** list, choose the softkey to add and click the right arrow to move the softkey to the **Selected Softkeys** list. Use the up and down arrows to change the position of the new softkey.

Step 8 Repeat the previous step to display the softkey in additional call states.

Step 9 Click **Save**.

Step 10 Perform one of the following tasks:

- Click **Apply Config** if you modified a template that is already associated with devices to restart the devices.
- If you created a new softkey template, associate the template with the devices and then restart them. For more information, see *Add a Softkey Template to a Common Device Configuration* and *Associate a Softkey Template with a Phone* sections.

What to do next

Perform one of the following tasks:

- Associate a Softkey Template with a Common Device Configuration, on page 350
- Associate a Softkey Template with a Phone , on page 351

Associate a Softkey Template with a Common Device Configuration

Optional. There are two ways to associate a softkey template with a phone:

- Add the softkey template to the **Phone Configuration**.
- Add the softkey template to the **Common Device Configuration**.

The procedures in this section describe how to associate the softkey template with a **Common Device Configuration**. Follow these procedures if your system uses a **Common Device Configuration** to apply configuration options to phones. This is the most commonly used method for making a softkey template available to phones.

To use the alternative method, see Associate a Softkey Template with a Phone , on page 351.

Procedure

Step 1 Add a Softkey Template to Common Device Configuration, on page 350

Step 2 Associate a Common Device Configuration with a Phone, on page 351

Add a Softkey Template to Common Device Configuration

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Common Device Configuration**.

Step 2 Perform the following steps to create a new Common Device Configuration and associate the softkey template with it; otherwise, proceed to the next step.

a) Click **Add New**.
b) Enter a name for the Common Device Configuration in the **Name** field.
c) Click **Save**.

Step 3 Perform the following steps to add the softkey template to an existing Common Device Configuration.

a) Click **Find** and enter the search criteria.
b) Click an existing Common Device Configuration.

Step 4 In the **Softkey Template** drop-down list, choose the softkey template that contains the softkey that you want to make available.

Step 5 Click **Save**.

Step 6 Perform one of the following tasks:

- If you modified a Common Device Configuration that is already associated with devices, click **Apply Config** to restart the devices.
- If you created a new Common Device Configuration, associate the configuration with devices and then restart them.

Associate a Common Device Configuration with a Phone

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select the phone device to add the softkey template.

Step 3 From the **Common Device Configuration** drop-down list, choose the common device configuration that contains the new softkey template.

Step 4 Click **Save**.

Step 5 Click **Reset** to update the phone settings.

Associate a Softkey Template with a Phone

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** to select the phone to add the softkey template.

Step 3 From the **Softkey Template** drop-down list, choose the template that contains the new softkey.

Step 4 Click **Save**.

Call Pickup Interactions and Restrictions

Call Pickup Interactions

Feature	Interaction
Route Plan Report	The route plan report displays the patterns and DNs that are configured in Unified Communications Manager. Use the route plan report to look for overlapping patterns and DNs before assigning a DN to call pickup group.
Calling search space and partitions	Assigning a partition to the Call Pickup Group number limits call pickup access to users on the basis of the device calling search space.
Time of Day (TOD)	Time of Day (TOD) parameter for members in the associated group enable them to accept calls within the same time period as their own group. TOD associates a time stamp to the calling search space and partition.
Call Accounting	When a call pickup occurs through auto call pickup, the system generates two call detail records (CDRs). One CDR applies to the original call that is cleared, and another CDR applies to the requesting call that is connected. When a call pickup occurs via non-auto call pickup, the system generates one call detail record, which applies to the requesting call that is connected. A CDR search returns all CDRs that match a specific time range and other search criteria. You can also search for a type of call that is associated with a particular CDR. The search result displays a call type field that indicates whether the call is a pickup call.
Call Forwarding	When a call pickup occurs with the service parameter Auto Call Pickup Enabled set to false, the call forward that is configured on the phone gets ignored when one of the pickup softkeys is pressed. If the call pickup requestor does not answer the call, the original call gets restored after the pickup no answer timer expires.

Call Pickup Restrictions

Restriction	Description
Different phone lines to different call pickup groups	Although you can assign different lines on a phone to different call pickup groups, Cisco does not recommend this setup because it can be confusing to users.

Restriction	Description
Call Pickup Group Number	• You cannot delete a call pickup group number when it is assigned to a line or DN. To determine which lines are using the call pickup group number, use Dependency Records in **Call Pickup Configuration** window. To delete a call pickup group number, reassign a new call pickup group number to each line or DN. • When you update a call pickup group number, Cisco Unified Communications Manager automatically updates all directory numbers that are assigned to that call pickup group.
SIP Phones	• The system does not support Call Pickup Notification on a few Cisco Unified IP Phones that run SIP. • Call Pickup Notification is only supported on licensed, third-party phones that run SIP.
Directed Call Pickup	• If a device that belongs to a hunt list rings due to a call that was made by calling the hunt pilot number, users cannot use the Directed Call Pickup feature to pick up such a call. • Users cannot pick up calls to a DN that belongs to a line group by using the Directed Call Pickup feature.
BLF Pickup	The system does not support Call Pickup Notification on a few Cisco Unified IP Phones that run SIP.
Incoming Calling Party International Number Prefix - Phone	If you have configured a prefix in the “Incoming Calling Party International Number Prefix - Phone ” service parameter, and an international call is placed to a member in the Call Pickup Group, the prefix does not get invoked in the calling party field if the call gets picked up by another member of the Call Pickup Group.

CHAPTER 26

Call Park and Directed Call Park

Call Park Overview

The Call Park feature allows you to place a call on hold so that can be retrieved from another phone in the Unified Communications Manager system (for example, a phone in another office or in a conference room). If you are on an active call, you can park the call to a call park extension by pressing the Park softkey. Another phone in your system can then dial the call park extension to retrieve the call.

You can define either a single directory number or a range of directory numbers for use as Call Park extension numbers. You can park only one call at each Call Park extension number.

The Call Park feature works within a Unified Communications Manager cluster, and each Unified Communications Manager node in a cluster must have Call Park extension numbers defined. You can define either a single directory number or a range of directory numbers for use as Call Park extension numbers. Ensure that the directory number or range of numbers is unique.

Users can dial the assigned route pattern (for example, a route pattern for an intercluster trunk could be 80XX) and the Call Park number (for example, 8022) to retrieve parked calls from another Unified Communications Manager cluster. You must ensure that calling search spaces and partitions are properly configured. Call Park works across clusters.

Valid Call Park extension numbers comprise integers and the wildcard character X. You can configure a maximum of XX in a Call Park extension number (for example, 80XX), which provides up to 100 Call Park extension numbers. When a call gets parked,Unified Communications Manager chooses the next Call Park extension number that is available and displays that number on the phone.

Park Monitoring

Park Monitoring is an optional Call Park feature where Cisco Unified Communications Manager monitors the status of a parked call until a timer expires. After the timer expires, the call is forwarded to a preassigned number, sent to voicemail, or returned to the call parker. You can apply park monitoring to phone lines and to hunt pilots.

Call Park Prerequisites

If you are using call park across clusters, you must have partitions and calling search spaces configured.

Table 26: Cisco Unified IP Phones that Support Park Softkey Template and Call Park Button Template

Phone Model	Supported in Softkey Template	Supported in Phone Button Template
Cisco Unified IP Phones 6900 series (except 6901 and 6911)	X	X
Cisco IP Phone 7800 Series	X	X
Cisco Unified IP Phones 7900 series (except 7921, 7925, 7935, 7936, 7937)	X	
Cisco IP Phone 8800 Series	X	X
Cisco Unified IP Phones 8900 series	X	X
Cisco Unified IP Phones 9900 series	X	X
Cisco Unified IP Phones 7900 series (except 7906, 7911, 7921, 7925, 7935, 7936, 7937)		X

Note You can configure Call Park on any line (except line 1) or button by using the programmable line key feature.

Call Park Configuration Task Flow

Before you begin

- Review Call Park Prerequisites, on page 356

Procedure

	Command or Action	Purpose
Step 1	Configure Clusterwide Call Park, on page 357	**(Optional).** Configure Call Park for the entire cluster, or use the procedure in step 3 to configure Call Park on servers within the cluster
Step 2	Configure a Partition for Call Park, on page 358	Create a partition to add a Call Park Number
Step 3	Configure a Call Park Number, on page 359	Configure a Call Park Number to use Call Park across servers in a cluster.
Step 4	Configure a Softkey Template for Call Park, on page 361	Add the Park softkey to a softkey template.
Step 5	To Associate a Softkey Template with a Common Device Configuration , on page 362, complete the following subtasks: • Add a Softkey Template to a Common Device Configuration , on page 362 • Associate a Common Device Configuration with a Phone, on page 363	**Optional.** To make the softkey template available to phones, you must complete either this step or the following step. Follow this step if your system uses a **Common Device Configuration** to apply configuration options to phones. This is the most commonly used method for making a softkey template available to phones.
Step 6	Associate a Softkey with a Phone, on page 363	**Optional.** Use this procedure either as an alternative to associating the softkey template with the Common Device Configuration, or in conjunction with the Common Device Configuration. Use this procedure in conjunction with the Common Device Configuration if you need assign a softkey template that overrides the assignment in the Common Device Configuration or any other default softkey assignment.
Step 7	To Configure Call Park Button, on page 364, complete the following subtasks: • Configure a Phone Button Template for Call Park, on page 364 • Associate a Button Template with a Phone, on page 364	
Step 8	Configure Park Monitoring, on page 365	Complete this optional task flow to add Park Monitoring to your Call Park configuration.

Configure Clusterwide Call Park

Procedure

Step 1 Choose **System** > **Service Parameters**.

Step 2 Select the desired node as **Server** and the service as **Cisco CallManager** (active).

Step 3 Click the **Advanced**.

The advanced service parameters are displayed in the window.

Step 4 In Clusterwide Parameter(Feature- General) section set the **Enable cluster-wide Call Park Number/Ranges** to **True**.

The default value is False. This parameter determines whether the Call Park feature is implemented clusterwide or restricted to a specific Unified CM node.

Step 5 Set the **Call Park Display Timer** for each server in a cluster that has the Cisco CallManager service and Call Park configured.

The default is 10 seconds. This parameter determines how long a Call Park number displays on the phone that parked the call.

Step 6 Set the **Call Park Reversion Timer** for each server in a cluster that has the Unified Communications Manager service and Call Park configured.

The default is 60 seconds. This parameter determines the time that a call remains parked. When this timer expires, the parked call returns to the device that parked the call. If a hunt group member parks a call that comes through a hunt pilot, the call goes back to the hunt pilot when the Call Park Reversion Timer expires.

Note If you enter a Call Park Reversion Timer value that is less than the Call Park Display Timer, Call Park numbers may not display on the phone.

Step 7 Click **Save**.

Step 8 Restart all Unified Communications Manager and CTI Manager services.

Configure a Partition for Call Park

Configure partitions to create a logical grouping of directory numbers (DNs) and route patterns with similar reachability characteristics. Partitions facilitate call routing by dividing the route plan into logical subsets that are based on organization, location, and call type. You can configure multiple partitions.

Before you begin

(Optional) Configure Clusterwide Call Park, on page 357

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Partition**.

Step 2 Click **Add New** to create a new partition.

Step 3 In the **Partition Name, Description** field, enter a name for the partition that is unique to the route plan.

Partition names can contain alphanumeric characters, as well as spaces, hyphens (-), and underscore characters (_). See the online help for guidelines about partition names.

Step 4 Enter a comma (,) after the partition name and enter a description of the partition on the same line.

The description can contain up to 50 characters in any language, but it cannot include double quotes ("), percentage sign (%), ampersand (&), backslash (\), angle brackets (<>), or square brackets ([ ]).

If you do not enter a description, Cisco Unified Communications Manager automatically enters the partition name in this field.

Step 5 To create multiple partitions, use one line for each partition entry.

Step 6 From the **Time Schedule** drop-down list, choose a time schedule to associate with this partition.

The time schedule specifies when the partition is available to receive incoming calls. If you choose **None**, the partition remains active at all times.

Step 7 Select one of the following radio buttons to configure the **Time Zone**:

- **Originating Device**—When you select this radio button, the system compares the time zone of the calling device to the **Time Schedule** to determine whether the partition is available is available to receive an incoming call.
- **Specific Time Zone**—After you select this radio button, choose a time zone from the drop-down list. The system compares the chosen time zone to the **Time Schedule** to determine whether the partition is available is available to receive an incoming call.

Step 8 Click **Save**.

Configure a Call Park Number

If you want to use Call Park across servers in a cluster, you must configure Call Park extension numbers on each server.

Ensure that each Call Park directory number, partition, and range is unique within the Unified Communications Manager. Each Unified Communications Manager to which devices are registered requires its own unique Call Park directory number and range. Cisco Unified Communications Manager Administration does not validate the Call Park numbers or range that you use to configure Call Park. To help identify invalid numbers or ranges and potential range overlaps, use the Unified Communications Manager Dialed Number Analyzer tool.

Before you begin

Configure a Partition for Call Park, on page 358

Procedure

Step 1 Choose **Call Routing** > **Call Park**.

Step 2 Perform one of the following tasks:

- To add a new Call Park number, click **Add New**.
- To copy a Call Park number, find the Call Park number or range of numbers and then click the **Copy** icon.
- To update a Call Park number, find the Call Park number or range of numbers.

The Call Park number configuration window displays.

Step 3 Configure the fields in the Call Park configuration fields. See Call Park Configuration Fields, on page 360 for more information about the fields and their configuration options.

Step 4 To save the new or changed Call Park numbers in the database, click **Save.**

Call Park Configuration Fields

Field	Description
Call Park Number/Range	Enter the Call Park extension number. You can enter digits or the wildcard character X (the system allows one or two Xs). For example, enter 5555 to define a single Call Park extension number of 5555 or enter 55XX to define a range of Call Park extension numbers from 5500 to 5599. **Note** You can create a maximum of 100 Call Park numbers with one call park range definition. Make sure that the call park numbers are unique. **Note** You cannot overlap call park numbers between Unified Communications Manager servers. Ensure that each Unified Communications Manager server has its own number range. **Note** The call park range is selected from the list of servers where the call originates. For example, if phone A (registered to node A) calls phone B (registered to node B) and the phone B user presses Park, phone B requires a call park range in the CSS that resides on node A. In a multinode environment where phones and gateways communicate with various nodes and where calls that originate from any server may need to be parked, the phones require a CSS that contains call park ranges from all servers.
Description	Provide a brief description of this call park number. The description can include up to 50 characters in any language, but it cannot include double-quotes (“), percentage sign (%), ampersand (&), or angle brackets (<>).

Field	Description
Partition	If you want to use a partition to restrict access to the call park numbers, choose the desired partition from the drop-down list. If you do not want to restrict access to the call park numbers, choose <None> for the partition. **Note** Make sure that the combination of call park extension number and partition is unique within the Unified Communications Manager.
Unified Communications Manager	Using the drop-down list, choose the Cisco Unified Communications Manager to which these call park numbers apply.

Configure a Softkey Template for Call Park

Use this procedure to make the **Park** softkey available.

Park softkey has the following call states:

- On Hook
- Ring Out
- Connected Transfer

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Softkey Template**.

Step 2 Perform the following steps to create a new softkey template; otherwise, proceed to the next step.

a) Click **Add New**.
b) Select a default template and click **Copy**.
c) Enter a new name for the template in the **Softkey Template Name** field.
d) Click **Save**.

Step 3 Perform the following steps to add softkeys to an existing template.

a) Click **Find** and enter the search criteria.
b) Select the required existing template.

Step 4 Check the **Default Softkey Template** check box to designate this softkey template as the default softkey template.

Note If you designate a softkey template as the default softkey template, you cannot delete it unless you first remove the default designation.

Step 5 Choose **Configure Softkey Layout** from the **Related Links** drop-down list in the upper right corner and click **Go**.

Step 6 From the **Select a Call State to Configure** drop-down list, choose the call state for which you want the softkey to display.

Step 7 From the **Unselected Softkeys** list, choose the softkey to add and click the right arrow to move the softkey to the **Selected Softkeys** list. Use the up and down arrows to change the position of the new softkey.

Step 8 Repeat the previous step to display the softkey in additional call states.

Step 9 Click **Save**.

Step 10 Perform one of the following tasks:

- Click **Apply Config** if you modified a template that is already associated with devices to restart the devices.
- If you created a new softkey template, associate the template with the devices and then restart them. For more information, see *Add a Softkey Template to a Common Device Configuration* and *Associate a Softkey Template with a Phone* sections.

Associate a Softkey Template with a Common Device Configuration

Optional. There are two ways to associate a softkey template with a phone:

- Add the softkey template to the **Phone Configuration**.
- Add the softkey template to the **Common Device Configuration**.

The procedures in this section describe how to associate the softkey template with a **Common Device Configuration**. Follow these procedures if your system uses a **Common Device Configuration** to apply configuration options to phones. This is the most commonly used method for making a softkey template available to phones.

To use the alternative method, see the section *Associate a Softkey Template with a Phone* .

Procedure

Step 1 Add a Softkey Template to a Common Device Configuration , on page 362

Step 2 Associate a Common Device Configuration with a Phone, on page 363

Add a Softkey Template to a Common Device Configuration

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Common Device Configuration**.

Step 2 Perform the following steps to create a new Common Device Configuration and associate the softkey template with it; otherwise, proceed to the next step.

a) Click **Add New**.
b) Enter a name for the Common Device Configuration in the **Name** field.
c) Click **Save**.

Step 3 Perform the following steps to add the softkey template to an existing Common Device Configuration.

a) Click **Find** and enter the search criteria.

b) Click an existing Common Device Configuration.

Step 4 In the **Softkey Template** drop-down list, choose the softkey template that contains the softkey that you want to make available.

Step 5 Click **Save**.

Step 6 Perform one of the following tasks:

- If you modified a Common Device Configuration that is already associated with devices, click **Apply Config** to restart the devices.
- If you created a new Common Device Configuration, associate the configuration with devices and then restart them.

Associate a Common Device Configuration with a Phone

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select the phone device to add the softkey template.

Step 3 From the **Common Device Configuration** drop-down list, choose the common device configuration that contains the new softkey template.

Step 4 Click **Save**.

Step 5 Click **Reset** to update the phone settings.

Associate a Softkey with a Phone

Optional. Use this procedure as an alternative to associating the softkey template with the Common Device Configuration. This procedure also works in conjunction with the Common Device Configuration. You can use it when you need to assign a softkey template that overrides the assignment in the Common Device Configuration or any other default softkey assignment.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** to select the phone to add the softkey template.

Step 3 From the **Softkey Template** drop-down list, choose the template that contains the new softkey.

Step 4 Click **Save**.

Step 5 Press **Reset** to update the phone settings.

Configure Call Park Button

Configure a Phone Button Template for Call Park

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Phone Button Template**.

Step 2 Click **Find** to display list of supported phone templates.

Step 3 Perform the following steps if you want to create a new phone button template; otherwise, proceed to the next step.

a) Select a default template for the model of phone and click **Copy**.
b) In the **Phone Button Template Information** field, enter a new name for the template.
c) Click **Save**.

Step 4 Perform the following steps if you want to add phone buttons to an existing template.

a) Click **Find** and enter the search criteria.
b) Choose an existing template.

Step 5 From the **Line** drop-down list, choose feature that you want to add to the template.

Step 6 Click **Save**.

Step 7 Perform one of the following tasks:

- Click **Apply Config** if you modified a template that is already associated with devices to restart the devices.
- If you created a new softkey template, associate the template with the devices and then restart them.

Associate a Button Template with a Phone

Before you begin

Configure a Phone Button Template for Call Park, on page 364

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** to display the list of configured phones.

Step 3 Choose the phone to which you want to add the phone button template.

Step 4 In the **Phone Button Template** drop-down list, choose the phone button template that contains the new feature button.

Step 5 Click **Save**.
A dialog box is displayed with a message to press **Reset** to update the phone settings.

Configure Park Monitoring

Complete these optional tasks to add Park Monitoring to your Call Park configuration.

Before you begin

Park Monitoring is supported on only a subset of phones that support Call Park. The following Cisco Unified IP Phones support Park Monitoring:

- Cisco IP Phone 8811
- Cisco IP Phone 8841
- Cisco IP Phone 8845
- Cisco IP Phone 8851
- Cisco IP Phone 8851NR
- Cisco IP Phone 8861
- Cisco IP Phone 8865
- Cisco IP Phone 8865NR
- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

Procedure

	Command or Action	Purpose
Step 1	Configure Park Monitoring System Timers, on page 365	Configure system-level timers for the Park Monitoring feature.
Step 2	Configure Park Monitoring for Hunt Pilots, on page 366	**Optional.** If you have hunt pilots deployed, assign a Park Monitoring destination to a hunt pilot.
Step 3	Configure Park Monitoring for a Directory Number, on page 367	Assign a Park Monitoring destination for an individual phone line.
Step 4	Configure Park Monitoring via Universal Line Template, on page 368	If you have an LDAP directory sync configured, you can use universal line templates to provision directory number settings for multiple users with park monitoring configured.

Configure Park Monitoring System Timers

Use this procedure to configure system-level timers for the Park Monitoring feature.

Procedure

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

Step 2 From the **Server** drop-down list, select the publisher node.

Step 3 From the **Service** drop-down list, select **Cisco CallManager**.

Step 4 Configure values for the following service parameters:

- **Park Monitoring Reversion Timer**—The number of seconds that Cisco Unified Communications Manager waits before prompting the user to retrieve a parked call. For individual phone lines, this setting can be overridden by the same setting in the **Directory Number Configuration** window. When the call park reversion timer expires, the call will be forwarded to the hunt pilot.
- **Park Monitoring Periodic Reversion Timer**—The number of seconds between reversion attempts when a call has been parked. Cisco Unified Communications Manager prompts the user about the parked call by ringing, beeping, or flashing the parker's phone. When the park monitoring reversion timer expires, the call will be forwarded to the parked party and not the hunt pilot.
- **Park Monitoring Forward No Retrieve Timer**—The number of seconds that park reminder notifications occur before the parked call is forwarded to the **Park Monitoring Forward No Retrieve** destination specified in the call parker's Directory Number configuration. When park monitoring forward no retrieve timer expires, the call will be forwarded to the hunt pilot.

Note For additional details on these fields, see the service parameter online help.

Step 5 Click **Save**.

What to do next

Use any of these optional tasks to assign how expired timers get handled for individual phones lines and hunt pilots:

- Configure Park Monitoring for Hunt Pilots, on page 366
- Configure Park Monitoring for a Directory Number, on page 367
- Configure Park Monitoring via Universal Line Template, on page 368

Configure Park Monitoring for Hunt Pilots

If your deployment uses hunt pilots, use this optional procedure to assign a Park Monitoring destination to a hunt pilot.

Note For general information on setting up hunt pilots, see the "Configure Hunt Pilots" chapter of the System Configuration Guide for Cisco Unified Communications Manager.

Before you begin

Configure Park Monitoring System Timers, on page 365

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Route/Hunt** > **Hunt Pilot**.

Step 2 Click **Find** and select the hunt pilot on which you want to configure a Park Monitoring destination.

Step 3 In the **Park Monitoring No Retrieve Destination** field, assign a **Destination** directory number and **Calling Search Space**.

Step 4 Complete any remaining fields in the **Hunt Pilot Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 5 Click **Save.**

Configure Park Monitoring for a Directory Number

Use this procedure to assign a Park Monitoring destination for an individual phone line. You can forward calls to another number, send to voicemail, or return to the call parker.

Note The following tools are available to provision settings for multiple phone lines:

- Use a universal line template to provision park monitoring settings for multiple phone lines via an LDAP directory sync. For details, see Configure Park Monitoring via Universal Line Template, on page 368.
- Use the Bulk Administration Tool to import a CSV file with settings for a large number of phone lines. For more information, see the Bulk Administration Guide for Cisco Unified Communications Manager.

Before you begin

Configure Park Monitoring System Timers, on page 365

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Directory Number**.

Step 2 Click **Find** and select the directory number that you want to configure.

Step 3 Enter values for the following **Park Monitoring** fields:

- **Park Monitoring Forward No Retrieve Destination External**—When the Park Monitoring Forward No Retrieve Timer expires, and the parkee is an external party, the call is forwarded either to voicemail or to a specified directory number. If this field s empty, the call is redirected to the call parker's line.
- **Park Monitoring Forward No Retrieve Destination Internal**—When the Park Monitoring Forward No Retrieve Timer expires, and the parkee is an internal party, the call is forwarded either to voicemail or to a specified directory number. If this field s empty, the call is redirected to the call parker's line.
- **Park Monitor Reversion Timer**—The number of seconds that Cisco Unified Communications Manager waits before prompting the user to retrieve a call parked on this phone line. If the value is 0 or empty, then Cisco Unified Communications Manager uses the value of the **Park Monitor Reversion Timer** service parameter.

Step 4 Complete any remaining fields in the **Directory Number Configuration** window.For more information on the fields and their configuration options, see Online Help.

Step 5 Click **Save**.

Configure Park Monitoring via Universal Line Template

Use this procedure to assign park monitoring settings to a universal line template. If you have an LDAP directory sync configured, you can use the universal line template configuration to provision directory number settings with park monitoring configured for multiple users.

Before you begin

Configure Park Monitoring System Timers, on page 365

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User Phone/Add** > **Universal Line Template**.

Step 2 Perform one of the following steps:

- Click **Find** and select an existing template.
- Click **Add New** to create a new template.

Step 3 Expand the **Park Monitoring Settings** section and complete the fields. For field descriptions, see Park Monitoring Settings for Universal Line Templates, on page 368.

Step 4 Click **Save**.

What to do next

To apply the universal line template to individual directory numbers, you must assign the template to a user profile, feature group template, and LDAP directory sync. When the sync occurs, the template settings get applied to the phone lines that are a part of the sync. For LDAP setup, see the "Configure End Users" chapters in the System Configuration Guide for Cisco Unified Communications Manager.

Park Monitoring Settings for Universal Line Templates

The following table contains the Park Monitoring fields in the **Universal Line Template Configuration** window of Cisco Unified Communications Manager.

Table 27: Park Monitoring Settings for Universal Line Templates

Field	Description
Forward Destination for External Calls When Not Retrieved	When the person whose call is parked is an external party and the **Park Monitoring Forward No Retrieve Timer** expires, the system sends the call to one of these destinations: • **Voicemail**—Uses the configuration in Voice Mail Profile to determine where to send the call. • **Revert to Originator**—Returns the call to the call parker. • To forward calls to another number, input the other number in the text box. If no option is selected, the call returns to the call parker.
Calling Search Space for Forwarding External Calls When Not Retrieved	If you have configured parked calls to be redirected to a configured number, select the calling search space for the forward destination.
Forward Destination for Internal Calls When Not Retrieved	When the person whose call is parked is an internal party and the **Park Monitoring Forward No Retrieve Timer** expires, the system sends the call to one of these destinations: • **Voicemail**—Uses the configuration in Voice Mail Profile to determine where to send the call. • **Revert to Originator**—Returns the call to the call parker. • To forward calls to another number, input the other number in the text box. If no option is selected, the call returns to the call parker.
Calling Search Space for Forwarding Internal Calls When Not Retrieved	If you have configured parked calls to be redirected to a configured number, select the calling search space for the forward destination.
Park Monitor Reversion Timer (seconds)	This timer determines the number of seconds that Unified Communications Manager waits before prompting the user to retrieve a call that the user parked. This timer starts when the user presses the Park softkey on the phone, and a reminder is issued when the timer expires. The default value is 60 seconds. **Note** If you select 0 for the timer then phone lines that use this template will use the value of the **Park Monitor Reversion Timer** cluster-wide service parameter.

Call Park Interactions and Restrictions

Call Park Interactions

Feature	Interaction
CTI Applications	CTI applications access call park functionality, including monitoring activity on call park DNs. To monitor a call park DN, add an application or end user that is associated with the CTI application to the Standard CTI Allow Call Park Monitoring user group.
Music On Hold	Music On Hold allows users to place calls on hold with music that a streaming source provides. The Music On Hold audio source for Call Park is selected by the setting of the **Network Hold MOH Audio Source** setting within the **Phone Configuration** window. If you do not choose an audio source within the device configuration, Cisco Unified CM uses the audio source that is defined in the device pool or the system default if the device pool does not specify an audio source ID.
Route Plan Report	The route plan report displays the patterns and directory numbers that are configured in Unified Communications Manager. Use the route plan report to look for overlapping patterns and directory numbers before assigning a directory number to Call Park.
Calling Search Space and Partitions	Assign the call park directory number or range to a partition to limit call park access to users on the basis of the device calling search space.
Immediate Divert	Call Park supports Immediate Divert (iDivert or Divert softkey). For example, user A calls user B, and user B parks the call. User B retrieves the call and then decides to send the call to a voice-messaging mailbox by pressing the iDivert or Divert softkey. User A receives the voice mail greeting of user B.
Barge	• Barge with Call Park–The target phone (the phone that is being barged upon) controls the call. The barge initiator “piggybacks” on the target phone. The target phone includes most of the common features, even when the target is being barged; therefore, the barge initiator has no feature access. When the target parks a call, the barge initiator then must release its call (the barge). • cBarge with Call Park–The target and barge initiator act as peers. The cBarge feature uses a conference bridge, which causes it to function like a MeetMe conference. Both phones (target and barge initiator) have full access to their features.
Directed Call Park	We recommend that you do not configure both Directed Call Park and the Park softkey for Call Park, but the possibility exists to configure both. If you configure both, ensure that the call park and directed call park numbers do not overlap.

Feature	Interaction
QSIG Intercluster Trunks	When a user parks a call across a QSIG intercluster trunk or a QSIG gateway trunk, the caller who has been parked (the parkee) does not see the To parked number message. The phone continues to display the original connected number. The call has been parked, and the user who parked the call can retrieve it. When the call is retrieved from the parked state, the call continues, but the caller who was parked does not see the newly connected number.

Call Park Restrictions

Feature	Restriction
Call Park	Unified Communications Manager can park only one call at each call park extension number.
Shared Line	For shared line devices across nodes, the line registers to the node on which the device registers first. For example, if a device from subscriber2 registers first and the line is created in subscriber2 and the publisher node, the line belongs to subscriber2. Each node must be configured with the call park number.
Backup	To achieve failover or fallback, configure call park numbers on the publisher node and subscriber nodes. With this configuration, when the primary node is down, the line device association gets changed to the secondary node, and the secondary node call park number gets used.
Directed Call Park	If a directed call park (or call park) is initiated from a shared line and the call is not retrieved from any device, the parked call does not always get reverted to the recipient in the shared line (parker).
Conference	When a conference call is set up between both the shared line and the caller on park reversion or park reversion fails causing a two-party call (between the other shared line and caller). The reason is that, on park reversion, Unified Communications Manager extends the call to both devices sharing the line and tries to add either party in conference (party already in conference or party that hit the park). If the party attempts to add the party who is already in the conference first, then the park reversion fails. When park reversion fails, the shared line can still barge into the call as usual.
Delete Server	If any call park numbers are configured for Unified Communications Manager on a node that is being deleted in the **Server Configuration** window (**System** > **Server**), the node deletion fails. Before you can delete the node, you must delete the call park numbers in Cisco Unified Communications Manager Administration.

Troubleshooting Call Park

User Cannot Park Calls

Problem

User cannot park calls. When the user presses the Park softkey or feature button, the call does not get parked.

Solution

Ensure that a unique call park number is assigned to each Unified Communications Manager in the cluster.

The partition that is assigned to the call park number does not match the partition that is assigned to the phone directory number. For more information on partition, see the System Configuration Guide for Cisco Unified Communications Manager.

Call Park Number is Not Displayed Long Enough

Problem

The call park number is not displayed long enough for the user.

Solution

Set the Call Park Display Timer to a longer duration. See Configure Clusterwide Call Park, on page 357 for more information about the Timer.

Directed Call Park Overview

Directed Call Park allows a user to transfer a call to an available user-selected directed call park number. Configured Directed Call Park numbers exist cluster-wide. You can configure phones that support the directed call park Busy Lamp Field (BLF) to monitor the busy or idle status of specific directed call park numbers. Users can also use the BLF to speed dial a directed call park number.

Unified Communications Manager can park only one call at each directed call park number. To retrieve a parked call, a user must dial a configured retrieval prefix followed by the directed call park number at which the call is parked.

Directed Call Park Prerequisites

Make sure that the phones in your deployment support Directed Call Park. For a list of supported phones, run the **Phone Feature List** report from Cisco Unified Reporting, selecting **Assisted Directed Call Park** as the feature. For details, see Generate a Phone Feature List, on page 3.

Directed Call Park Configuration Task Flow

Before you begin

- Review Directed Call Park Prerequisites, on page 372

Procedure

	Command or Action	Purpose
Step 1	Configure ClusterWide Directed Call Park, on page 373	To configure clusterwide parameter for directed call park.
Step 2	Configure a Directed Call Park Number, on page 373	To add, copy, and update a single Directed Call Park extension number or range of extension numbers.
Step 3	Configure BLF/Directed Call Park Buttons, on page 375	Configure a phone button template for BLF/Directed Call Park.
Step 4	Synchronize Directed Call Park with Affected Devices, on page 376	Synchronize Directed Call Park with Affected Devices

Configure ClusterWide Directed Call Park

Procedure

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

Step 2 To set the timer, update the **Call Park Reversion Timer** fields in the Clusterwide Parameter(Feature- General) section.

The default is 60 seconds. This parameter determines the time that a call remains parked. When this timer expires, the parked call returns to the device that parked the call or to another specified number, depending on what you configure in the **Directed Call Park Configuration** window.

Configure a Directed Call Park Number

Before you begin

Ensure that each directed call park directory number, partition, and range is unique within the Unified Communications Manager. Before you begin, generate a route plan report. If the Park softkey is also activated (not recommended), ensure that no overlap exists between call park numbers and directed call park numbers. If reversion number is not configured, the call reverts to the parker (parking party) after the Call Park Reversion Timer expires.

Configure ClusterWide Directed Call Park, on page 373

Procedure

Step 1 Choose **Call Routing** > **Directed Call Park**.

Step 2 Perform one of the following tasks:

- To add a new directed call park number, click **Add New**.
- To copy a directed call park number, find the directed call park number or range of numbers and then click the **Copy** icon.
- To update a directed call park number, find the directed call park number or range of numbers.

The **directed call park number configuration** window is displayed.

Step 3 Configure the fields in the Directed Call Park settings area. See Directed Call Park Configuration Settings, on page 374 for more information about the fields and their configuration options.

Step 4 To save the new or changed call park numbers in the database, click **Save.**

If you update a directed call park number, Unified Communications Manager reverts any call that is parked on that number only after the Call Park Reversion Timer expires.

Step 5 Click **Apply Config**.

The **Apply Configuration Information** dialog is displayed.

Step 6 Click **OK.**

Step 7 If you are using BLF to monitor directed Call Park numbers, click **Restart Devices** on the **Directed Call Park Configuration** window. This step is optional if you are using change notification.

Directed Call Park Configuration Settings

Field	Description
Number	Enter the directed call park number. You can enter digits (0-9) or the wildcard character ([], - , *, ^, #) and X (the system allows one or two Xs). For example, enter 5555 to define a single call park number of 5555 or enter 55XX to define a range of directed call park extension numbers from 5500 to 5599. Make sure that the directed call park numbers are unique and that they do not overlap with call park numbers.
Description	Provide a brief description of this directed call park number or range. The description can include up to 50 characters in any language, but it cannot include double quotation marks (“), percentage sign (%), ampersand (&), or angle brackets (<>) and tabs.

Field	Description
Partition	If you want to use a partition to restrict access to the directed call park numbers, choose the desired partition from the drop-down list. If you do not want to restrict access to the directed call park numbers, leave the partition as the default of <None>. **Note** Make sure that the combination of directed call park number and partition is unique within Unified Communications Manager.
Reversion Number	Enter the number to which you want the parked call to return if not retrieved, or leave the field blank. **Note** A reversion number can comprise digits only; you cannot use wildcards.
Reversion Calling Search Space	Using the drop-down list, choose the calling search space or leave the calling search space as the default of <None>.
Retrieval Prefix	For this required field, enter the prefix for retrieving a parked call. The system needs the retrieval prefix to distinguish between an attempt to retrieve a parked call and an attempt to initiate a directed park.

Configure BLF/Directed Call Park Buttons

Before you begin

Configure ClusterWide Directed Call Park, on page 373

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Phone Button Template**.

Step 2 After the configuration window displays, click the **Add a new BLF Directed Call Park** link in the Association Information pane.

Note The link does not display in the Association Information pane if the phone button template that you applied to the phone or device profile does not support BLF/Directed Call Park.

Step 3 Configure the fields in the BLF/Directed Call Park fields area. See BLF/Directed Call Park Configuration Fields, on page 376 for more information about the fields and their configuration options.

Step 4 After you complete the configuration, click **Save** and close the window.

The directory numbers are displayed in the Association Information pane of the Phone Configuration Window.

BLF/Directed Call Park Configuration Fields

Table 28: BLF/Directed Call Park Button Configuration Fields

Field	Description
Directory Number	The Directory Number drop-down list displays a list of Directed Call Park number that exist in the Unified Communications Manager database. For phones that are running SCCP or phones that are running SIP, choose the number (and corresponding partition, if it is displayed) that you want the system to dial when the user presses the speed-dial button; for example, 6002 in 3. Directory numbers that display without specific partitions belong to the default partition.
Label	Enter the text that you want to display for the BLF/Directed Call Park button. This field supports internationalization. If your phone does not support internationalization, the system uses the text that displays in the Label ASCII field.
Label ASCII	Enter the text that you want to display for the BLF/Directed Call Park button. The ASCII label represents the noninternationalized version of the text that you enter in the Label field. If the phone does not support internationalization, the system uses the text that displays in this field. **Note** If you enter text in the Label ASCII field that differs from the text in the Label field, Cisco Unified Communications Manager Administration accepts the configuration for both fields, even though the text differs.

Synchronize Directed Call Park with Affected Devices

Procedure

Step 1 Choose **Call Routing** > **Directed Call Park**.

The **Find and List Directed Call Parks** window is displayed.

Step 2 Choose the search criteria to use.

Step 3 Click **Find.**

The window displays a list of directed call parks that match the search criteria.

Step 4 Click the directed call park to which you want to synchronize applicable devices. The **Directed Call Park Configuration** window is displayed.

Step 5 Make any additional configuration changes.

Step 6 Click **Save.**

Step 7 Click **Apply Config**.

The **Apply Configuration Information** dialog is displayed.

Step 8 Click **OK.**

Directed Call Park Interactions and Restrictions

Directed Call Park Interactions

The following table describes feature interactions with the Directed Call Park feature.

Feature	Interaction
Music On Hold	The Music On Hold Audio Source for directed call park is assigned via the **Default Network Hold MOH Audio Source** service parameter. To assign the parameter: **1.** From Cisco Unified CM Administration, choose **System** > **Service Parameters**. **2.** From the **Server** drop-down list, choose a Unified Communications Manger cluster node. **3.** From the **Service** drop-down list, select **Cisco CallManager**. **4.** Under **Clusterwide Paramters (Service)**, assign a MOH audio source to the **Default Network Hold MOH Audio Source ID** parameter. The default is **1**. **5.** Click **Save**. **Note** For detailed information on adding MOH audio sources to the system, refer to the "Configure Music On Hold" section of this guide.
Calling Search Space and Partitions	Assign the Directed Call Park Directory number or range to a partition to limit Directed Call Park access to users on the basis of the device calling search space.
Immediate Divert	Directed call park supports Immediate Divert (iDivert or Divert softkey). For example, user A calls user B, and user B parks the call. User B retrieves the call and then decides to send the call to a voice-messaging mailbox by pressing the iDivert or Divert softkey. User A receives the voicemail greeting of user B.
Barge	• Barge with Directed Call Park–The target phone (the phone that is being barged upon) controls the call. The barge initiator “piggybacks” on the target phone. The target phone includes most of the common features, even when the target is being barged; therefore, the barge initiator has no feature access. When the target parks a call by using directed call park, the barge initiator then must release its call (the barge). • cBarge with Directed Call Park–The target and barge initiator act as peers. The cBarge feature uses a conference bridge that makes it behave like to a meet-me conference. Both phones (target and barge initiator) retain full access to their features.

Feature	Interaction
Call Park	We recommend that you do not configure both directed call park and the Park softkey for call park, but the possibility exists to configure both. If you configure both, ensure that the call park and directed call park numbers do not overlap. A caller who has been parked (the parkee) by using the directed call park feature cannot, while parked, use the standard call park feature.

Directed Call Park Restrictions

Feature	Restriction
Directed Call Park number	Cisco Unified Communications Manager one party can park only one call at each Directed Call Park number. You cannot delete a Directed Call Park number that a device is configured to monitor (using the BLF button). A message indicates that the Directed Call Park number or range cannot be deleted because it is in use. To determine which devices are using the number, click the Dependency Records link on the **Directed Call Park Configuration** window.
Standard Call Park feature	A caller who has been parked (the parkee) by using the Directed Call Park feature cannot, while parked, use the standard call park feature.
Directed Call Park BLF	The Directed Call Park BLF cannot monitor a range of Directed Call Park numbers. A user can monitor only individual Directed Call Park numbers by using the Directed Call Park BLF. For example, if you configure a Directed Call Park number range 8X, you cannot use the Directed Call Park BLF to monitor that whole range of 80 to 89.
Directed Call Park for phones that are running SIP	The following limitations apply to Directed Call Park for phones that are running SIP: • Directed Call Park gets invoked by using the Transfer softkey on Cisco Unified IP Phones 7940 and 7960 that are running SIP. • The system does not support directed call park when the Blind Transfer softkey is used on Cisco Unified IP Phones 7940 and 7960 that are running SIP. • The system does not support directed call park BLF on Cisco Unified IP Phones 7940 and 7960 that are running SIP, and third-party phones that are running SIP.

Troubleshooting Directed Call Park

User Cannot Retrieve Parked Calls

User cannot retrieve parked calls. After dialing the directed call park number to retrieve a parked call, the user receives a busy tone, and the IP phone displays the message, “Park Slot Unavailable”.

Ensure that the user dials the retrieval prefix followed by the directed call park number.

User Cannot Park Calls

User cannot park calls. After the Transfer softkey (or Transfer button if available) is pressed and the directed call park number is dialed, the call does not get parked.

Ensure that the partition that is assigned to the call park number matches the partition that is assigned to the phone directory number. Ensure that the partition and calling search space are configured correctly for the device. For more information about the partition, see the *System Configuration Guide for Cisco Unified Communications Manager*.

User Receives a Reorder Tone After the Reversion Timer Expires

User cannot park calls. The user receives a reorder tone after the reversion timer expires.

Ensure that the user presses the Transfer softkey (or Transfer button if available) before dialing the directed call park number, and then presses the Transfer softkey (or Transfer button) again or goes on hook after dialing the directed call park number. Because directed call park is a transfer function, the directed call park number cannot be dialed alone.

Note You can complete the transfer only by going on hook rather than pressing the Transfer softkey (or Transfer button) a second time if the Transfer On-hook Enabled service parameter is set to True.

User Receives a Reorder Tone or Announcement

User cannot park calls. After pressing the Transfer softkey (or Transfer button if available) and dialing the directed call park number, the user receives a reorder tone or announcement.

Ensure that the dialed number is configured as a directed call park number.

User Cannot Park a Call at a Number Within The Range

After configuring a range of directed call park numbers, the user cannot park a call at a number within the range.

Review the syntax for entering a range of directed call park numbers. If incorrect syntax is used, the system may appear to configure the range when it actually does not.

Parked Calls Revert Too Quickly

Parked calls revert too quickly.

Set the Call Park Reversion Timer to a longer duration.

Park Slot Unavailable

User cannot park calls. After pressing the Transfer softkey (or Transfer button if available) and dialing the directed call park number, the user receives a busy tone, and the IP phone displays the message, “Park Slot Unavailable".

Ensure that the dialed directed call park number is not already occupied by a parked call or park the call on a different directed call park number.

Parked Calls Do Not Revert to the Parked Call Number

Parked calls do not revert to the number that parked the call.

Check the configuration of the directed call park number to ensure that it is configured to revert to the number that parked the call rather than to a different directory number.

Number or Range Cannot Be Deleted Because It Is in Use

When an attempt is made to delete a directed call park number or range, a message displays that indicates that the number or range cannot be deleted because it is in use.

You cannot delete a directed call park number that a device is configured to monitor (by using the BLF button). To determine which devices are using the number, click the Dependency Records link in the Directed Call Park Configuration window.

CHAPTER 27

Extension Mobility

Extension Mobility Overview

Cisco Extension Mobility allows users to temporarily access their phone settings, such as line appearances, services, and speed dials, from other phones within your system. If you have a single phone that will be used by multiple workers, for example, you can configure extension mobility so that individual users can log in to the phone and access their settings without affecting settings on other user accounts.

Extension Mobility Prerequisites

- A TFTP server that is reachable.
- Extension mobility functionality extends to most Cisco Unified IP Phones. Check the phone documentation to verify that Cisco Extension Mobility is supported.

Extension Mobility Configuration Task Flow

Before you begin

Procedure

	Command or Action	Purpose
Step 1	Generate a Phone Feature List, on page 3	Generate a report to identify devices that support the extension mobility feature.

	Command or Action	Purpose
Step 2	Activate Extension Mobility Services, on page 382	
Step 3	Configure the Cisco Extension Mobility Phone Service, on page 383	Configure the extension mobility IP phone service to which users can later subscribe to access extension mobility.
Step 4	Create an Extension Mobility Device Profile for Users, on page 383	Configure an extension mobility device profile. This profile acts as a virtual device that maps onto a physical device when a user logs in to extension mobility. The physical device takes on the characteristics in this profile.
Step 5	Associate a Device Profile to a User, on page 389	Associate a device profile to users so that they can access their settings from a different phone. You associate a user device profile to a user in the same way that you associate a physical device.
Step 6	Subscribe to Extension Mobility, on page 389	Subscribe IP phones and device profiles to the extension mobility service so that users can log in, use, and log out of extension mobility.
Step 7	Configure the Change Credential IP Phone Service, on page 390	To allow users to change their PINs on their phones, you must configure the change credential Cisco Unified IP Phone service and associate the user, the device profile, or the IP phone with the change credential phone service.
Step 8	(Optional) Configure Service Parameters for Extension Mobility, on page 390	If you want to modify the behavior of extension mobility, configure the service parameters.

Activate Extension Mobility Services

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Service Activation**.

Step 2 From the **Server** drop-down list, choose the publisher node.

Step 3 Activate the following services as needed:

a) Cisco CallManager
b) Cisco Tftp
c) Cisco Extension Mobility

Step 4 Click **Save**.

Step 5 Click **OK**.

Configure the Cisco Extension Mobility Phone Service

Configure the extension mobility IP phone service to which users can later subscribe to access extension mobility.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Phone Services**.

Step 2 Click **Add New**.

Step 3 In the **Service Name** field, enter a name for the service.

Step 4 In the **Service URL** field, enter the Service URL.

The format is `http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#`. `IP Address` is the IP address of the Unified Communications Manager where Cisco Extension Mobility is activated and running.

Example:

`http://123.45.67.89:8080/emapp/EMAppServlet?device=#DEVICENAME#`

Note If you append the Extension Mobility Cross Cluster suffix `&EMCC=#EMCC#` in the service URL for Extension Mobility, the Extension Mobility login fails with an HTTP 400 error on phones that do not support Extension Mobility Cross Cluster. Users will see a blank screen on the phone when the Extension Mobility service is not selected.

Step 5 In the **Service Type** field, choose whether the service is provisioned to the Services, Directories, or Messages button.

Step 6 Click **Save**.

Create an Extension Mobility Device Profile for Users

Configure an extension mobility device profile. This profile acts as a virtual device that maps onto a physical device when a user logs in to extension mobility. The physical device takes on the characteristics in this profile.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Device Profile**.

Step 2 Perform one of the following tasks:

- Click **Find** to modify the settings and choose an existing device profile from the resulting list.
- Click **Add New** to add a new device profile and choose an option from the **Device Profile Type**. Click **Next**.
- Choose a device protocol from the **Device Protocol** drop-down list and click **Next**.

Step 3 Configure the fields. For more information on the fields and their configuration options, see Online Help.

Step 4 Click **Save**.

Step 5 From the **Association Information** section, click **Add a new DN**.

Step 6 In the **Directory Number** field, enter the directory number and click **Save**.

Step 7 Click **Reset** and follow the prompts.

Device Profile Fields for Extension Mobility

Table 29: Device Profile Settings

Field	Description
Product Type	Displays the product type to which this device profile applies.
Device Protocol	Displays the device protocol to which this device profile applies.
Device Profile Name	Enter a unique name. This name can comprise up to 50 characters in length.
Description	Enter a description of the device profile. For text, use anything that describes this particular user device profile.
User Hold MOH Audio Source	Specifies the audio source that plays when a user initiates a hold action, choose an audio source from the User Hold MOH Audio Source drop-down list. If you do not choose an audio source, Unified Communications Manager uses the audio source that is defined in the device pool or the system default if the device pool does not specify an audio source ID. **Note** You define audio sources in the Music On Hold Audio Source Configuration window. For access, choose **Media Resources** > **Music On Hold Audio Source**.
User Locale	From the drop-down list, choose the locale that is associated with the phone user interface. The user locale identifies a set of detailed information, including language and font, to support users. Unified Communications Manager makes this field available only for phone models that support localization. **Note** If no user locale is specified, Unified Communications Manager uses the user locale that is associated with the device pool. If the users require information to display (on the phone) in any language other than English, verify that the locale installer is installed before configuring user locale. See the Unified Communications Manager Locale Installer documentation.
Phone Button Template	From the Phone Button Template drop-down list, choose a phone button template. **Tip** If you want to configure BLF/SpeedDials for the profile for presence monitoring, choose a phone button template that you configured for BLF/SpeedDials. After you save the configuration, the Add a New BLF SD link displays in the Association Information pane. For more information on BLF/SpeedDials, see the Feature Configuration Guide for Cisco Unified Communications Manager.

Field	Description
Softkey Template	From the Softkey Template drop-down list, choose the softkey template from the list that displays.
Privacy	From the Privacy drop-down list, choose On for each phone on which you want privacy. For more information, see the Feature Configuration Guide for Cisco Unified Communications Manager.
Single Button Barge	From the drop-down list, choose from the following options: • Off—This device does not allow users to use the Single Button Barge/cBarge feature. • Barge—Choosing this option allows users to press the Single Button Barge shared-line button on the phone to barge into a call using Barge. • Default—This device inherits the Single Button Barge/cBarge setting from the service parameter and device pool settings. **Note** If the server parameter and device pool settings are different, the device will inherit the setting from the service parameter setting. For more information, see the Feature Configuration Guide for Cisco Unified Communications Manager.
Join Across Lines	From the drop-down list, choose from the following options: • Off—This device does not allow users to use the Join Across Lines feature. • On—This device allows users to join calls across multiple lines. • Default—This device inherits the Join Across Lines setting from the service parameter and device pool settings. **Note** If the server parameter and device pool settings are different, the device will inherit the setting from the service parameter setting. For more information, see the System Configuration Guide for Cisco Unified Communications Manager.
Always Use Prime Line	From the drop-down list, choose one of the following options: • Off—When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received. • On—When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls. • Default—Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco CallManager service.

Field	Description
Always Use Prime Line for Voice Message	From the drop-down list, choose one of the following options: • On—If the phone is idle, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone. • Off—If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. Unified Communications Manager always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when the phone user presses the Messages button. • Default—Unified Communications Manager uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco CallManager service.
Ignore Presentation Indicators (internal calls only)	To configure call display restrictions and ignore any presentation restriction that is received for internal calls, check the "Ignore Presentation Indicators (internal calls only)" check box. **Tip** Use this configuration in combination with the calling line ID presentation and connected line ID presentation configuration at the translation pattern level. Together, these settings allow you to configure call display restrictions to selectively present or block calling and/or connected line display information for each call. For more information about call display restrictions, see the Feature Configuration Guide for Cisco Unified Communications Manager.
Do Not Disturb	Check this check box to enable Do Not Disturb.
DND Option	When you enable DND on the phone, this parameter allows you to specify how the DND feature handles incoming calls: • Call Reject—This option specifies that no incoming call information gets presented to the user. Depending on how you configure the DND Incoming Call Alert parameter, the phone may play a beep or display a flash notification of the call. • Ringer Off—This option turns off the ringer, but incoming call information gets presented to the device, so that the user can accept the call. • Use Common Phone Profile Setting—This option specifies that the DND Option setting from the Common Phone Profile window will get used for this device. **Note** For 7940/7960 phones that are running SCCP, you can only choose the Ringer Off option. For mobile devices and dual-mode phones, you can only choose the Call Reject option. When you activate DND Call Reject on a mobile device or dual-mode phone, no call information gets presented to the device.

Field	Description
DND Incoming Call Alert	When you enable the DND Ringer Off or Call Reject option, this parameter specifies how a call displays on a phone. From the drop-down list, choose one of the following options: • None—This option specifies that the DND Incoming Call Alert setting from the Common Phone Profile window will get used for this device. • Disable—This option disables both beep and flash notification of a call but for the DND Ringer Off option, incoming call information still gets displayed. For the DND Call Reject option, no call alerts display and no information gets sent to the device. • Beep Only—For an incoming call, this option causes the phone to play a beep tone only. • Flash Only—For an incoming call, this option causes the phone to display a flash alert.
Extension Mobility Cross Cluster CSS	From the drop-down list, choose an existing Calling Search Space (CSS) to use for this device profile for the Extension Mobility Cross Cluster feature. (To configure a new CSS or modify an existing CSS, choose **Call Routing** > **Class of Control** > **Calling Search Space** in Unified Communications Manager.) Default value specifies None. The home administrator specifies this CSS, which gets used as the device CSS that gets assigned to the phone when the user logs in to this remote phone. For more information, see the Feature Configuration Guide for Cisco Unified Communications Manager.
Module 1	You can configure one or two expansion modules for this device profile by choosing phone templates from the expansion module drop-down list in the expansion module fields. **Note** You can view a phone button list at any time by choosing the View button list link next to the phone button template fields. A separate dialog box pops up and displays the phone buttons for that particular expansion module. Choose the appropriate expansion module or None.
Module 2	Choose the appropriate expansion module or None.
MLPP Domain	If this user device profile will be used for MLPP precedence calls, choose the MLLP Domain from the drop-down list. **Note** You define MLPP domains in the MLPP Domain Configuration window. For access, choose **System** > **MLPP Domain**.

Field	Description
MLPP Indication	If this user device profile will be used for MLPP precedence calls, assign an MLPP Indication setting to the device profile. This setting specifies whether a device that can play precedence tones will use the capability when it places an MLPP precedence call. From the drop-down list, choose a setting to assign to this device profile from the following options: **1.** Default—This device profile inherits its MLPP indication setting from the device pool of the associated device. **2.** Off—This device does not handle nor process indication of an MLPP precedence call. **3.** On—This device profile does handle and process indication of an MLPP precedence call. **Note** Do not configure a device profile with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.
MLPP Preemption	If this user device profile will be used for MLPP precedence calls, assign an MLPP Preemption setting to the device profile. This setting specifies whether a device that can preempt calls in progress will use the capability when it places an MLPP precedence call. From the drop-down list, choose a setting to assign to this device profile from the following options: **1.** Default—This device profile inherits its MLPP preemption setting from the device pool of the associated device. **2.** Disabled—This device does not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. **3.** Forceful—This device allows preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. **Note** Do not configure a device profile with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.
Login User Id	From the Login User ID drop-down list, choose a valid login user ID. **Note** If the device profile is used as a logout profile, specify the login user ID that will be associated with the phone. After the user logs out from this user device profile, the phone will automatically log in to this login user ID.

Associate a Device Profile to a User

Associate a device profile to users so that they can access their settings from a different phone. You associate a user device profile to a user in the same way that you associate a physical device.

Tip You can use the Bulk Administration Tool (BAT) to add and delete several user device profiles for Cisco Extension Mobility at one time. See the Bulk Administration Guide for Cisco Unified Communications Manager.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **End User**.

Step 2 Perform one of the following tasks:

- Click **Find** to modify the settings for an existing user, enter search criteria, and choosing an existing user from the resulting list.
- Click **Add New** to add a new user.

Step 3 Under **Extension Mobility**, locate the device profile that you created and move it from **Available Profiles** to **Controlled Profiles**.

Step 4 Check the **Home Cluster** check box.

Step 5 Click **Save**.

Subscribe to Extension Mobility

Subscribe IP phones and device profiles to the extension mobility service so that users can log in, use, and log out of extension mobility.

Procedure

Step 1 Perform one of the following tasks from Cisco Unified CM Administration:

- Choose **Device** > **Phone**, specify search criteria, click **Find**, and choose a phone which users will use for extension mobility.
- Choose **Device** > **Device Settings** > **Device Profile**, specify search criteria, click **Find**, and choose the device profile that you created.

Step 2 From the **Related Links** drop-down list, choose **Subscribe/Unsubscribe Services**, and then click **Go**.

Step 3 From the **Select a Service** drop-down list, choose the **Extension Mobility** service.

Step 4 Click **Next**.

Step 5 Click **Subscribe**.

Step 6 Click **Save** and close the popup window.

Configure the Change Credential IP Phone Service

To allow users to change their PINs on their phones, you must configure the change credential Cisco Unified IP Phone service and associate the user, the device profile, or the IP phone with the change credential phone service.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Phone Services**.

Step 2 Click **Add New**.

Step 3 In the **Service Name** field, enter **`Change Credential`**.

Step 4 In the **Service URL** field, enter the following value, where `server` designates the server where the Change Credential IP phone service runs:

```
http://server:8080/changecredential/ChangeCredentialServlet?device=#DEVICENAME#
```

Step 5 (Optional) In the **Secure-Service URL** field, enter the following value, where `server` is the server where the Change Credential IP phone service runs:

```
https://server:8443/changecredential/ChangeCredentialServlet?device=#DEVICENAME#
```

Step 6 Configure the remaining fields in the **IP Phone Services Configuration** window, and choose **Save**.

Step 7 To subscribe the Cisco Unified IP Phone to the Change Credential IP phone service, choose **Device** > **Phone**.

Step 8 In the **Phone Configuration** window, go to the **Related Links** drop-down list and choose **Subscribe/Unsubscribe Services**.

Step 9 Click **Go**.

Step 10 From the **Select a Service** drop-down list, choose the **Change Credential IP phone service**.

Step 11 Click **Next**.

Step 12 Click **Subscribe**.

Step 13 Click **Save**.

Configure Service Parameters for Extension Mobility

(Optional)

If you want to modify the behavior of extension mobility, configure the service parameters.

Procedure

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

Step 2 From the **Server** field, choose the node that is running the Cisco Extension Mobility service.

Step 3 From the **Service** field, choose **Cisco Extension Mobility**.

Step 4 Click **Advanced** to show all service parameters.

See Extension Mobility Service Parameters, on page 391 for more information about these service parameters and their configuration options.

Step 5 Click **Save**.

Extension Mobility Service Parameters

Table 30: Extension Mobility Service Parameters

Service Parameter	Description
Enforce Intra-cluster Maximum Login Time	Select **True** to specify a maximum time for local logins. After this time, the system automatically logs out the device. **False**, which is the default setting, means that no maximum time for logins exists. To set an automatic logout, you must choose **True** for this service parameter and also specify a system maximum login time for the **Intra-cluster Maximum Login Time** service parameter. Cisco Unified Communications Manager then uses the automatic logout service for all logins.
Intra-cluster Maximum Login Time	This parameter sets the maximum time that a user can be locally logged in to a device, such as 8:00 (8 hours) or :30 (30 minutes). The system ignores this parameter and set the maximum login time to 0:00, if the **Enforce Intra-cluster Maximum Login Time** parameter is set to **False**. Valid values are between 0:01 and 168:00 in the format HHH:MM, where HHH represents the number of hours and MM represents the number of minutes.
Maximum Concurrent Requests	Specify the maximum number of login or logout operations that can occur simultaneously. This number prevents the Cisco Extension Mobility service from consuming excessive system resources. The default value of 5 is acceptable in most cases.
Intra-cluster Multiple Login Behavior	Choose one of the following options: • Multiple Logins Allowed—A user can log in to more than one device at a time. • Multiple Logins Not Allowed—The second and subsequent login attempts after a user successfully logs in once will fail. • Auto Logout—After a user logs in to a second device, the Cisco Unified Communications Manager automatically logs the user out of the first device. For EMCC, multiple logins are always allowed.
Alphanumeric User ID	Choose **True** to allow the user ID to contain alphanumeric characters. Choosing **False** allows the user ID to contain only numeric characters. **Note** The Alphanumeric User ID parameter applies systemwide. You can have a mix of alphanumeric and numeric user IDs. The system supports only user IDs that can be entered by using the alphanumeric keypad. The case-sensitive userid field requires the characters to be lowercase.

Service Parameter	Description
Remember the Last User Logged In	When you choose **False**, the system does not remember the last user who logged in to the phone. Use this option when the user access the phone on a temporary basis only. Choose True to remember the last user that logged into the phone. Use this option when a phone has only one user. For example, Cisco Extension Mobility is used to enable the types of calls that are allowed from a phone. Individuals who are not logged in and who are using their office phone can make only internal or emergency calls. But after logging in using Cisco Extension Mobility, the user can make local, long-distance, and international calls. In this scenario, only this user regularly logs in to the phone. It makes sense to set the Cisco Extension Mobility to remember the last user ID that logged in.
Clear Call Logs on Intra-cluster EM	Choose **True** to specify that the call logs are cleared during the Cisco Extension Mobility manual login and logout process. While a user is using the Cisco Extension Mobility service on an IP phone, all calls (placed, received, or missed) appear in a call log and can be retrieved and seen on the IP phone display. To ensure privacy, set the Clear Call Log service parameter to **True**. This ensures that the call logs are cleared when a user logs out and another user logs in. For extension mobility cross cluster (EMCC), the call log is always cleared when the user logs in or out of a phone. **Note** Call logs are cleared only during manual login/logout. If a Cisco Extension Mobility logout occurs automatically or any occurrence other than a manual logout, the call logs are not cleared.
Validate IP Address	This parameter sets whether validation occurs on the IP address of the source that is requesting login or logout. If the parameter is set to **True**, the IP address from which a Cisco Extension Mobility log in or log out request occurs and is validated to ensure that it is trusted. Validation is first performed against the cache for the device that will log in or log out. If the IP address is found in the cache or in the list of trusted IP addresses or is a registered device, the device can log in or log out. If the IP address is not found, the log in or log out attempt is blocked. If the parameter is set to **False**, the Cisco Extension Mobility log in or log out request is not validated. Validation of IP addresses can affect the time that is required to log in or log out a device, but it offers additional security that prevents unauthorized log in or log out attempts. This function is recommended, especially when used with logins from separate trusted proxy servers for remote devices.
Trusted List of IPs	This parameter appears as a text box (the maximum length is 1024 characters). You can enter strings of trusted IP addresses or hostnames which are separated by semicolons, in the text box. IP address ranges and regular expressions are not supported.

Service Parameter	Description
Allow Proxy	If the parameter is **True**, the Cisco Extension Mobility log in and log out operations that use a web proxy are allowed. If the parameter is **False**, the Cisco Extension Mobility log in and log out requests coming from behind a proxy get rejected. The setting that you select takes effect only if the Validate IP Address parameter specifies true.
Extension Mobility Cache Size	In this field, enter the size of the device cache that is maintained by Cisco Extension Mobility. The minimum value for this field is 1000 and the maximum is 20000. The default value is 10000. The value that you enter takes effect only if the Validate IP Address parameter is **True**.

Extension Mobility Interactions and Restrictions

Cisco Extension Mobility Interactions

Table 31: Cisco Extension Mobility Interactions

Feature	Interaction
Assistant	A manager who uses Cisco Extension Mobility can simultaneously use Cisco Unified Communications Manager Assistant. The manager logs in to the Cisco Unified IP Phone by using Cisco Extension Mobility and then chooses the Cisco IP Manager Assistant service. When the Cisco IP Manager Assistant service starts, the manager can access assistants and all Cisco Unified Communications Manager Assistant features (such as call filtering and Do Not Disturb).
BLF Presence	When you configure BLF/speed dial buttons in a user device profile, a phone that supports Cisco Extension Mobility displays BLF presence status on the BLF/SpeedDial buttons after you log in to the device. When the extension mobility user logs out, a phone that supports Cisco Extension Mobility displays BLF presence status on the BLF/SpeedDial buttons for the logout profile that is configured.
Call Display Restrictions	When you enable call display restrictions, Cisco Extension Mobility functions as usual: when a user is logged in to the device, the presentation or restriction of the call information depends on the user device profile that is associated with that user. When the user logs out, the presentation or restriction of the call information depends on the configuration that is defined for that phone type in the Phone Configuration window. To use call display restrictions with Cisco Extension Mobility, check the **Ignore Presentation Indicators (internal calls only)** check obx in both the **Device Profile Configuration** window and the **Phone Configuration** window.

Feature	Interaction
Call Forward All Calling Search Space	An enhancement to call forward all calling search space (CSS) lets you upgrade to later releases of Cisco Unified Communications Manager without loss of functionality. The **CFA CSS Activation Policy** service parameter supports this enhancement. In the **Service Parameter Configuration** window, this parameter displays in the **Clusterwide Parameters (Feature - Forward)** section with two options: • With Configured CSS (default) • With Activating Device/Line CSS
Do Not Disturb	For extension mobility, the device profile settings include do not disturb (DND) incoming call alert and DND status. When a user logs in and enables DND, the DND incoming call alert and DND status settings are saved, and these settings are used when the user logs in again. **Note** When a user who is logged in to extension mobility modifies the DND incoming call alert or DND status settings, this action does not affect the actual device settings.
Intercom	Cisco Extension Mobility supports the intercom feature. To support intercom, Cisco Extension Mobility uses a default device that is configured for an intercom line. An intercom line is presented on only the default device. You can assign an intercom line to a device profile. When a user logs in to a device that is not the default device, the intercome line is not presented. The following additional considerations apply to intercom for Cisco Extension Mobility: • When Unified Communications Manager assigns an intercom line to a device and the default device value is empty, the current device is selected as the default device. • When AXL programatically assigns an intercom DN, you must update the intercom DN separately by using Cisco Unified Communications Manager Administration to set the default device. • When you delete a device that is set as the intercom default device for an intercom line, the intercom default device is no longer set to the deleted device.
Internet Protocol Version 6 (IPv6)	Cisco Extension Mobility supports IPv4, so you cannot use phones with an IP Addressing Mode of IPv6 Only for Cisco Extension Mobility. If you want to use Cisco Extension Mobility with the phone, you must configure the phone with an IP Addressing Mode of IPv4 Only or IPv4 and IPv6.
Prime Line	If you select **On** for the **Always Use Prime Line** parameter in the **Device Profile** or **Default Device Profile Configuration** window, a Cisco Extension Mobility user can use this feature after logging in to the device that supports Cisco Extension Mobility.

Cisco Extension Mobility Restrictions

Table 32: Cisco Extension Mobility Restrictions

Feature	Restriction
Cache	Cisco Extension Mobility maintains a cache of all logged-in user information for 2 minutes. If a request comes to extension mobility regarding a user who is represented in the cache, the user is validated with information from the cache. For example, if a user changes the password, logs out, and then logs back in within 2 minutes, both the old and new passwords are recognized.
Call Back	When a Cisco Extension Mobility user logs out of a device, all call back services that are active for the Cisco Extension Mobility user are automatically cancelled.
Character Display	The characters that display when a user logs in depend on the current locale of the phone. For example, if the phone is currently in the English locale (based on the Logout profile of the phone), the user can only enter English characters in the UserID.
Hold Reversion	Cisco Extension Mobility does not support the hold reversion feature.
IP Phones	Cisco Extension Mobility requires a physical Cisco Unified IP Phone for login. Users of office phones that are configured with Cisco Extension Mobility cannot remotely log in to their phones.
Locale	If the user locale that is associated with the user or profile is not the same as the locale or device, after a successful login, the phone will restart and then reset. This behavior occurs because the phone configuration file is rebuilt. Addon-module mismatches between profile and device can cause the same behavior.
Log Out	If Cisco Extension Mobility is stopped or restarted, the system does not automatically log out users who are already logged in after the logout interval expires. Those phones automatically log out users only once a day. You can manually log out these users from either the phones or from Cisco Unified CM Administration.
Secure Tone	Cisco Extension Mobility and join across line services are disabled on protected phones.
User Group	Although you can add users to the Standard EM authentication proxy rights user group, those users are not authorized to authenticate by proxy.

Extension Mobility Troubleshooting

Troubleshoot Extension Mobility

Procedure

- Configure the Cisco Extension Mobility trace directory and enable debug tracing by performing the following steps:
  a) From Cisco Unified Serviceability, choose **Trace** > **Trace Configuration**.
  b) From the **Servers** drop-down list, select a server.

c) From the **Configured Services** drop-down-list, select **Cisco Extension Mobility**.

- Make sure that you entered the correct URL for the Cisco Extension Mobility service. Remember that the URL is case sensitive.
- Check that you have thoroughly and correctly performed all the configuration procedures.
- If a problem occurs with authentication of a Cisco Extension Mobility user, go to the user pages and verify the PIN.

Authentication Error

Problem "Error 201 Authentication Error" appears on the phone.

Solution The user should check that the correct user ID and PIN were entered; the user should check with the system administrator that the user ID and PIN are correct.

Blank User ID or PIN

Problem "Error 202 Blank User ID or PIN" appears on the phone.

Solution Enter a valid user ID and PIN.

Busy Please Try Again

Problem "Error 26 Busy Please Try Again" appears on the phone.

Solution Check whether the number of concurrent login and logout requests is greater than the **Maximum Concurrent requests** service parameter. If so, lower the number of concurrent requests.

Note To verify the number of concurrent login and logout requests, use the Cisco Unified Real-Time Monitoring Tool to view the Requests In Progress counter in the Extension Mobility object. For more information, see the Cisco Unified Real-Time Monitoring Tool Administration Guide at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

Database Error

Problem "Error 6 Database Error" appears on the phone.

Solution Check whether a large number of requests exists. If a large number of requests exists, the Requests In Progress counter in the Extension Mobility object counter shows a high value. If the requests are rejected because of a large number of concurrent requests, the Requests Throttled counter also shows a high value. Collect detailed database logs.

Dev Logon Disabled

Problem "Error 22 Dev Logon Disabled" appears on the phone.

Solution Verify that you checked the **Enable Extension Mobility** check box in the **Phone Configuration** window (**Device** > **Phone**).

Device Name Empty

Problem "Error 207 Device Name Empty" appears on the phone.

Solution Check that the URL that is configured for Cisco Extension Mobility is correct. See the Related Topics section for more information.

Related Topics

Configure the Cisco Extension Mobility Phone Service, on page 383

EM Service Connection Error

Problem "Error 207 EM Service Connection Error" appears on the phone.

Solution Verify that the Cisco Extension Mobility service is running by selecting **Tools** > **Control Center—Feature** in Cisco Unified Serviceability.

Host Not Found

Problem The "Host Not Found" error message appears on the phone.

Solution Check that the Cisco Tomcat service is running by selecting **Tools** > **Control Center—Network Services** in CIsco Unified Serviceability.

HTTP Error

Problem HTTP Error (503) appears on the phone.

Solution

- If you get this error when you press the **Services** button, check that the Cisco IP Phone Services service is running by selecting **Tools** > **Control Center—Network Services** in Cisco Unified Serviceability.
- If you get this error when you select Extension Mobility service, check that the Cisco Extension Mobility Application service is running by selecting **Tools** > **Control Center—Network Services** in Cisco Unified Serviceability.

Phone Resets

Problem After users log in or log out, their phones reset instead of restarting.

Possible Cause Locale change is the probable cause of the reset.

Solution No action is required. If the user locale that is associated with the logged-in user or profile is not the same as the locale or device, after a successful login the phone will restart and then reset. This pattern occurs because the phone configuration file is rebuilt.

Phone Services Unavailable After Login

Problem After logging in, the user finds that the phone services are not available.

Possible Cause This problem occurs because the user profile had no services associated with it when it was loaded on the phone.

Solution

- Ensure that the user profile includes the Cisco Extension Mobility service.
- Change the configuration of the phone where the user is logged in to include Cisco Extension Mobility. After the phone is updated, the user can access the phone services.

Phone Services Unavailable After Logout

Problem After a user logs out and the phone reverts to the default device profile, the phone services are no longer available.

Solution

- Verify that the **Synchronization Between Auto Device Profile and Phone Configuration** enterprise parameter is set to **True**.
- Subscribe the phone to the Cisco Extension Mobility service.

User Logged in Elsewhere

Problem “Error 25 User Logged in Elsewhere” appears on the phone.

Solution Check whether the user is logged in to another phone. If multiple logins must be allowed, ensure that the **Multiple Login Behavior** service parameter is set to **Multiple Logins Allowed**.

User Profile Absent

Problem “Error 205 User Profile Absent” appears on the phone.

Solution Associate a device profile to the user.

CHAPTER 28

Extension Mobility Cross Cluster

Extension Mobility Cross Cluster Overview

The extension mobility cross cluster (EMCC) feature provides users with the same functionality as extension mobility, but also allows them to move from one cluster (the home cluster) and log in to a temporary phone on another remote cluster (the visiting cluster). From there, they can access their phone settings from any location as if the they were using an IP phone at the home office.

Extension Mobility Cross Cluster Prerequisites

- Other call-control entities that support and use the extension mobility cross cluster (EMCC) configuration; for example, other Cisco Unified Communications Manager clusters, EMCC intercluster service profiles, and EMCC remote cluster services
- Clusters that are set to nonsecure or mixed mode. See Extension Mobility Cross Cluster and Security Mode for Different Cluster Versions, on page 422 for more information.
- Supported phones in secure or nonsecure mode

Extension Mobility Cross Cluster Configuration Task Flow

Before you begin

- Review Extension Mobility Cross Cluster Prerequisites, on page 399
- Review **Extension Mobility Cross Cluster Interaction and Restriction**

Procedure

	Command or Action	Purpose
Step 1	Generate a Phone Feature List, on page 3	Generate a report to identify devices that support the extension mobility cross cluster feature.
Step 2	To Configure Extension Mobility, on page 401, perform the following subtasks: • Activate Services for Extension Mobility Cross Cluster, on page 402 • Configure the Extension Mobility Phone Service, on page 402 • Configure a Device Profile for Extension Mobility Cross Cluster, on page 403 • Enable Extension Mobility Cross Cluster for a User, on page 408 • Subscribe Devices to Extension Mobility, on page 409	Configure extension mobility to allow users to temporarily access their phone settings, such as line appearances, services, and speed dials, from other phones in one cluster. Perform this task flow on both home and remote clusters, so that users will be able to access settings from either a home or visiting cluster.
Step 3	To Configure Certificates for Extension Mobility Cross Cluster, on page 409, perform the following subtasks: • Activate the Bulk Provisioning Service, on page 410 • Configure Bulk Certificate Management and Export Certificates, on page 410 • Consolidate the Certificates, on page 411 • Import the Certificates into the Clusters, on page 412	To configure the home and remote clusters properly, you must export certificates on each cluster to the same SFTP server and SFTP directory and consolidate them on one of the participating clusters. This procedure ensures that trust is established between the two clusters.
Step 4	To Configure Extension Mobility Cross Cluster Devices and Templates, on page 412, perform the following subtasks: • Create a Common Device Configuration, on page 413 • Configure an Extension Mobility Cross Cluster Template, on page 413 • Set the Default Template, on page 414 • Add Extension Mobility Cross Cluster Devices, on page 414	
Step 5	Configure a Geolocation Filter for Extension Mobility Cross Cluster, on page 414	Configure a geolocation filter to specify criteria for device location matching, such as country, state, and city values. Geolocations are used to identify the location of a device, and the filter indicates what parts of the geolocation are significant.

	Command or Action	Purpose
Step 6	Configure Feature Parameters for Extension Mobility Cross Cluster, on page 415	Select values for the feature parameters that you configured, such as the geolocation filter.
Step 7	Configure Intercluster SIP Trunk for Extension Mobility Cross Cluster, on page 418	Configure trunks to process inbound or outbound traffic for intercluster PSTN access and RSVP agent services. You can configure one trunk for both PSTN access and RSVP agent services or one trunk for each service. You do not need more than two SIP trunks for extension mobility cross cluster.
Step 8	Configure an Intercluster Service Profile for Extension Mobility Cross Cluster, on page 418	Configure the intercluster service profile to activate extension mobility cross cluster. The profile collects all the configuration that precedes and provides a results report.
Step 9	Configure Remote Cluster Services, on page 419	Configure the remote cluster for extension mobility cross cluster. This step completes the link between the home cluster with remote (visiting) cluster.

Configure Extension Mobility

Configure extension mobility to allow users to temporarily access their phone settings, such as line appearances, services, and speed dials, from other phones in one cluster. Perform this task flow on both home and remote clusters, so that users will be able to access settings from either a home or visiting cluster.

Procedure

	Command or Action	Purpose
Step 1	Activate Services for Extension Mobility Cross Cluster, on page 402	
Step 2	Configure the Extension Mobility Phone Service, on page 402	Create the Extension Mobility phone service to which you can subscribe your users.
Step 3	Configure a Device Profile for Extension Mobility Cross Cluster, on page 403	Create a device profile to map settings onto a real device when a user logs in to Extension Mobility cross cluster.
Step 4	Enable Extension Mobility Cross Cluster for a User, on page 408	
Step 5	Subscribe Devices to Extension Mobility, on page 409	Enable Extension Mobility on devices and subscribe to the service if you have not set up an enterprise subscription for all devices.

Activate Services for Extension Mobility Cross Cluster

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Service Activation**.

Step 2 From the **Server** drop-down list, choose the publisher node.

Step 3 Activate the following services as needed:

a) Cisco CallManager
b) Cisco Tftp
c) Cisco Extension Mobility

Step 4 Click **Save**.

Step 5 Click **OK**.

Configure the Extension Mobility Phone Service

Create the Extension Mobility phone service to which you can subscribe your users.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Phone Services**.

Step 2 Click **Add New**.

Step 3 In the **Service Name** field, enter a name for the service.

For example, enter a name such as Extension Mobility or EM. For Java MIDlet services, the service name must exactly match the name that is defined in the Java Application Descriptor (JAD) file.

Step 4 In the **Service URL** field, enter the service URL in the following format:

```
http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&EMCC=#EMCC#.
```

Step 5 (Optional) If you want to create a secure URL using HTTPS, enter the secure service URL in the following format:

```
https://<IP
Address>:8443/emapp/EMAppServlet?device=#DEVICENAME#&EMCC=#EMCC#
```

Step 6 Use the default values for the **Service Category** and **Service Type** fields.

Step 7 Check the **Enable** check box.

Step 8 (Optional) Check the **Enterprise Subscription** check box to subscribe all phones and device profiles to this phone service.

Note If you check this check box when configuring the service for the first time, you will set up this IP phone service as an enterprise subscription service. All phones and device profiles in the enterprise will automatically subscribe to this IP phone service, removing the need for you to subscribe them individually.

Step 9 Click **Save**.

Configure a Device Profile for Extension Mobility Cross Cluster

Create a device profile to map settings onto a real device when a user logs in to Extension Mobility cross cluster.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Device Profile**.

Step 2 Perform one of the following tasks:

- Click **Find** to modify an existing device profile, enter search criteria. Click a device profile name in the resulting list.
- Click **Add New** to add a new device profile and click **Next** to choose a device profile type. Click **Next** to choose a protocol, then click **Next**.

Step 3 Configure the fields on the **Device Profile Configuration** window. See Device Profile Fields for Extension Mobility Cross Cluster, on page 403 for more information about the fields and their configuration options.

Step 4 Click **Save**.

Step 5 Add a directory number (DN) to the new device profile.

Device Profile Fields for Extension Mobility Cross Cluster

Table 33: Device Profile Settings

Field	Description
Product Type	Displays the product type to which this device profile applies.
Device Protocol	Displays the device protocol to which this device profile applies.
Device Profile Name	Enter a unique name. This name can comprise up to 50 characters in length.
Description	Enter a description of the device profile. For text, use anything that describes this particular user device profile.
User Hold MOH Audio Source	Specifies the audio source that plays when a user initiates a hold action, choose an audio source from the User Hold MOH Audio Source drop-down list. If you do not choose an audio source, Unified Communications Manager uses the audio source that is defined in the device pool or the system default if the device pool does not specify an audio source ID. **Note** You define audio sources in the Music On Hold Audio Source Configuration window. For access, choose **Media Resources** > **Music On Hold Audio Source**.

Field	Description
User Locale	From the drop-down list, choose the locale that is associated with the phone user interface. The user locale identifies a set of detailed information, including language and font, to support users. Unified Communications Manager makes this field available only for phone models that support localization. **Note** If no user locale is specified, Unified Communications Manager uses the user locale that is associated with the device pool. If the users require information to display (on the phone) in any language other than English, verify that the locale installer is installed before configuring user locale. See the Unified Communications Manager Locale Installer documentation.
Phone Button Template	From the Phone Button Template drop-down list, choose a phone button template. **Tip** If you want to configure BLF/SpeedDials for the profile for presence monitoring, choose a phone button template that you configured for BLF/SpeedDials. After you save the configuration, the Add a New BLF SD link displays in the Association Information pane. For more information on BLF/SpeedDials, see the Feature Configuration Guide for Cisco Unified Communications Manager.
Softkey Template	From the Softkey Template drop-down list, choose the softkey template from the list that displays.
Privacy	From the Privacy drop-down list, choose On for each phone on which you want privacy. For more information, see the Feature Configuration Guide for Cisco Unified Communications Manager.
Single Button Barge	From the drop-down list, choose from the following options: • Off—This device does not allow users to use the Single Button Barge/cBarge feature. • Barge—Choosing this option allows users to press the Single Button Barge shared-line button on the phone to barge into a call using Barge. • Default—This device inherits the Single Button Barge/cBarge setting from the service parameter and device pool settings. **Note** If the server parameter and device pool settings are different, the device will inherit the setting from the service parameter setting. For more information, see the Feature Configuration Guide for Cisco Unified Communications Manager.

Field	Description
Join Across Lines	From the drop-down list, choose from the following options: • Off—This device does not allow users to use the Join Across Lines feature. • On—This device allows users to join calls across multiple lines. • Default—This device inherits the Join Across Lines setting from the service parameter and device pool settings. **Note** If the server parameter and device pool settings are different, the device will inherit the setting from the service parameter setting. For more information, see the System Configuration Guide for Cisco Unified Communications Manager.
Always Use Prime Line	From the drop-down list, choose one of the following options: • Off—When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received. • On—When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls. • Default—Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco CallManager service.
Always Use Prime Line for Voice Message	From the drop-down list, choose one of the following options: • On—If the phone is idle, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone. • Off—If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. Unified Communications Manager always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when the phone user presses the Messages button. • Default—Unified Communications Manager uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco CallManager service.

Field	Description
Ignore Presentation Indicators (internal calls only)	To configure call display restrictions and ignore any presentation restriction that is received for internal calls, check the "Ignore Presentation Indicators (internal calls only)" check box. **Tip** Use this configuration in combination with the calling line ID presentation and connected line ID presentation configuration at the translation pattern level. Together, these settings allow you to configure call display restrictions to selectively present or block calling and/or connected line display information for each call. For more information about call display restrictions, see the Feature Configuration Guide for Cisco Unified Communications Manager.
Do Not Disturb	Check this check box to enable Do Not Disturb.
DND Option	When you enable DND on the phone, this parameter allows you to specify how the DND feature handles incoming calls: • Call Reject—This option specifies that no incoming call information gets presented to the user. Depending on how you configure the DND Incoming Call Alert parameter, the phone may play a beep or display a flash notification of the call. • Ringer Off—This option turns off the ringer, but incoming call information gets presented to the device, so that the user can accept the call. • Use Common Phone Profile Setting—This option specifies that the DND Option setting from the Common Phone Profile window will get used for this device. **Note** For 7940/7960 phones that are running SCCP, you can only choose the Ringer Off option. For mobile devices and dual-mode phones, you can only choose the Call Reject option. When you activate DND Call Reject on a mobile device or dual-mode phone, no call information gets presented to the device.
DND Incoming Call Alert	When you enable the DND Ringer Off or Call Reject option, this parameter specifies how a call displays on a phone. From the drop-down list, choose one of the following options: • None—This option specifies that the DND Incoming Call Alert setting from the Common Phone Profile window will get used for this device. • Disable—This option disables both beep and flash notification of a call but for the DND Ringer Off option, incoming call information still gets displayed. For the DND Call Reject option, no call alerts display and no information gets sent to the device. • Beep Only—For an incoming call, this option causes the phone to play a beep tone only. • Flash Only—For an incoming call, this option causes the phone to display a flash alert.

Field	Description
Extension Mobility Cross Cluster CSS	From the drop-down list, choose an existing Calling Search Space (CSS) to use for this device profile for the Extension Mobility Cross Cluster feature. (To configure a new CSS or modify an existing CSS, choose **Call Routing** > **Class of Control** > **Calling Search Space** in Unified Communications Manager.) Default value specifies None. The home administrator specifies this CSS, which gets used as the device CSS that gets assigned to the phone when the user logs in to this remote phone. For more information, see the Feature Configuration Guide for Cisco Unified Communications Manager.
Module 1	You can configure one or two expansion modules for this device profile by choosing phone templates from the expansion module drop-down list in the expansion module fields. **Note** You can view a phone button list at any time by choosing the View button list link next to the phone button template fields. A separate dialog box pops up and displays the phone buttons for that particular expansion module. Choose the appropriate expansion module or None.
Module 2	Choose the appropriate expansion module or None.
MLPP Domain	If this user device profile will be used for MLPP precedence calls, choose the MLLP Domain from the drop-down list. **Note** You define MLPP domains in the MLPP Domain Configuration window. For access, choose **System** > **MLPP Domain**.
MLPP Indication	If this user device profile will be used for MLPP precedence calls, assign an MLPP Indication setting to the device profile. This setting specifies whether a device that can play precedence tones will use the capability when it places an MLPP precedence call. From the drop-down list, choose a setting to assign to this device profile from the following options: **1.** Default—This device profile inherits its MLPP indication setting from the device pool of the associated device. **2.** Off—This device does not handle nor process indication of an MLPP precedence call. **3.** On—This device profile does handle and process indication of an MLPP precedence call. **Note** Do not configure a device profile with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.

Field	Description
MLPP Preemption	If this user device profile will be used for MLPP precedence calls, assign an MLPP Preemption setting to the device profile. This setting specifies whether a device that can preempt calls in progress will use the capability when it places an MLPP precedence call. From the drop-down list, choose a setting to assign to this device profile from the following options: **1.** Default—This device profile inherits its MLPP preemption setting from the device pool of the associated device. **2.** Disabled—This device does not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. **3.** Forceful—This device allows preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. **Note** Do not configure a device profile with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.
Login User Id	From the Login User ID drop-down list, choose a valid login user ID. **Note** If the device profile is used as a logout profile, specify the login user ID that will be associated with the phone. After the user logs out from this user device profile, the phone will automatically log in to this login user ID.

Enable Extension Mobility Cross Cluster for a User

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **End User**.

Step 2 Perform one of the following tasks:

- Click **Find** to modify the settings for an existing user and choosing an existing user from the resulting list.
- Click **Add New** to add a new user.

Step 3 In the **Extension Mobility** pane, check the **Enable Extension Mobility Cross Cluster** check box.

Step 4 Choose the device profile from the **Available Profiles** list pane in the **Extension Mobility** pane.

Step 5 Move the device profile to the **Controlled Profiles** list pane.

Step 6 Click **Save**.

Subscribe Devices to Extension Mobility

Enable Extension Mobility on devices and subscribe to the service if you have not set up an enterprise subscription for all devices.

Procedure

Step 1 From From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Find the phone on which users can use Extension Mobility Cross Cluster.

Step 3 For this device, check the **Enable Extension Mobility** check box in the **Extension Information** pane.

Step 4 In the **Phone Configuration** window, choose the **Subscribe/Unsubscribe Services** option in the **Related Links** drop-down list.

Step 5 Click **Go**.

Step 6 In the popup window that opens, choose the **Extension Mobility** service in the **Select a Service** drop-down list.

Step 7 Click **Next**.

Step 8 Click **Subscribe**.

Step 9 From the popup window, click **Save**, and then close the window.

Step 10 In the **Phone Configuration** window, click **Save**.

Step 11 Click **OK** if prompted.

Configure Certificates for Extension Mobility Cross Cluster

To configure the home and remote clusters properly, you must export certificates on each cluster to the same SFTP server and SFTP directory and consolidate them on one of the participating clusters. This procedure ensures that trust is established between the two clusters.

Before you begin

Configure Extension Mobility, on page 401

Procedure

	Command or Action	Purpose
Step 1	Activate the Bulk Provisioning Service, on page 410	
Step 2	Configure Bulk Certificate Management and Export Certificates, on page 410	Configure bulk certificate management in Cisco Unified OS Administration to export the certificates from both the home and remote clusters.
Step 3	Consolidate the Certificates, on page 411	Consolidate certificates when all participating clusters have exported their certificates. This option is available only if two or more clusters exported their certificates to the SFTP server.

	Command or Action	Purpose
Step 4	Import the Certificates into the Clusters, on page 412	Import the certificates back into the home and remote (visiting) clusters.

Activate the Bulk Provisioning Service

Before you begin

Configure Extension Mobility, on page 401

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Service Activation**.

Step 2 From the **Server** drop-down list, choose the publisher node.

Step 3 Check the **Cisco Bulk Provisioning Service** check box.

Step 4 Click **Save**.

Step 5 Click **OK**.

Configure Bulk Certificate Management and Export Certificates

Configure bulk certificate management in Cisco Unified OS Administration to export the certificates from both the home and remote clusters.

This procedure creates a PKCS12 file that contains certificates for all nodes in the cluster.

Note

- Every participating cluster must export certificates to the same SFTP server and SFTP directory.
- You must export certificates on the cluster whenever the Tomcat, TFTP, or CAPF certificates are regenerated on any of the cluster nodes.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Bulk Certificate Management**.

Step 2 Configure the settings for a TFTP server that both the home and remote clusters can reach. See the online help for information about the fields and their configuration options.

Step 3 Click **Save**.

Step 4 Click **Export**.

Step 5 In the **Bulk Certificate Export** window, choose **All** for the **Certificate Type** field.

Step 6 Click **Export**.

Step 7 Click **Close**.

Note When the bulk certificate export is performed, the certificates are then uploaded to the remote cluster as follows:

- CAPF certificate gets uploaded as a CallManager-trust
- Tomcat certificate gets uploaded as a Tomcat-trust
- CallManager certificate gets uploaded as a CallManager-trust
- CallManager certificate gets uploaded as a Phone-SAST-trust
- ITLRecovery certificate gets uploaded as a PhoneSast-trust and CallManager-trust

The above steps are performed when certificates are self-signed and there is no common trust in another cluster. If there is a common trust or the same signer then the export of ALL certificates is not needed.

Consolidate the Certificates

Consolidate certificates when all participating clusters have exported their certificates. This option is available only if two or more clusters exported their certificates to the SFTP server.

This procedure consolidates all PKCS12 files in the SFTP server to form a single file.

Note If you export new certificates after consolidation, you must perform this procedure again to include the newly exported certificates.

Procedure

Step 1 From From Cisco Unified OS Administration, choose **Security** > **Bulk Certificate Management** > **Consolidate** > **Bulk Certificate Consolidate**.

Step 2 In the **Certificate Type** field, choose **All**.

Step 3 Click **Consolidate**.

Note When the bulk certificate consolidate is performed, the certificates are then uploaded to the remote cluster as follows:

- CAPF certificate gets uploaded as a CallManager-trust
- Tomcat certificate gets uploaded as a Tomcat-trust
- CallManager certificate gets uploaded as a CallManager-trust
- CallManager certificate gets uploaded as a Phone-SAST-trust
- ITLRecovery certificate gets uploaded as a PhoneSast-trust and CallManager-trust

Import the Certificates into the Clusters

Import the certificates back into the home and remote (visiting) clusters.

Note After an upgrade, these certificates are preserved. You do not need to reimport or reconsolidate certificates.

Caution After you import the certificates, the phones on the cluster will automatically restart.

Procedure

Step 1 From From Cisco Unified OS Administration, choose **Security** > **Bulk Certificate Management** > **Import** > **Bulk Certificate Import**.

Step 2 From the **Certificate Type** drop-down list, choose **All**.

Step 3 Choose **Import**.

Note When the bulk certificate import is performed, the certificates are then uploaded to the remote cluster as follows:

- CAPF certificate gets uploaded as a CallManager-trust
- Tomcat certificate gets uploaded as a Tomcat-trust
- CallManager certificate gets uploaded as a CallManager-trust
- CallManager certificate gets uploaded as a Phone-SAST-trust
- ITLRecovery certificate gets uploaded as a PhoneSast-trust and CallManager-trust

Note The following types of certificates determines phones that are restarted:

- Callmanager - ALL phones only IF TFTP service is activated on the node the certificate belongs.
- TVS - SOME phones based on Callmanager group membership.
- CAPF - ALL phones only IF CAPF is activated.

Configure Extension Mobility Cross Cluster Devices and Templates

Procedure

	Command or Action	Purpose
Step 1	Create a Common Device Configuration, on page 413	Configure a common device configuration to specify the services or features that will be associated with a particular user.

	Command or Action	Purpose
Step 2	Configure an Extension Mobility Cross Cluster Template, on page 413	Create an extension mobility cross cluster template to link the common device configuration with this feature.
Step 3	Set the Default Template, on page 414	Set the extension mobility cross cluster template that you created as the default template.
Step 4	Add Extension Mobility Cross Cluster Devices, on page 414	Insert extension mobility cross cluster device entries into your system database. Each device is identified with a unique name in the format EMCC1, EMCC2, and so on. The Bulk Administration Tool assigns device numbers by obtaining the last one used.

Create a Common Device Configuration

Configure a common device configuration to specify the services or features that will be associated with a particular user.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Common Device Configuration**.

Step 2 Perform one of the following tasks:

- Click **Find** to modify an existing common device configuration and choose a common device configuration from the resulting list.
- Click **Add New** to add a new common device configuration.

Step 3 Configure the fields on the **Common Device Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 4 Click **Save**.

Configure an Extension Mobility Cross Cluster Template

Create an extension mobility cross cluster template to link the common device configuration with this feature.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Bulk Administration** > **EMCC** > **EMCC Template**.

Step 2 Click **Add New**.

Step 3 Configure the fields on the **EMCC Template Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 4 Click **Save**.

Set the Default Template

Set the extension mobility cross cluster template that you created as the default template.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Bulk Administration** > **EMCC** > **Insert/Update EMCC**.

Step 2 Click **Update EMCC Devices**.

Step 3 From the **Default EMCC Template** drop-down list, choose the extension mobility cross cluster device template that you configured.

Step 4 Click **Run Immediately**.

Step 5 Click **Submit**.

Step 6 Verify the success of the job:

a) Choose **Bulk Administration** > **Job Scheduler**.

b) Locate the Job ID of your job.

Add Extension Mobility Cross Cluster Devices

Insert extension mobility cross cluster device entries into your system database. Each device is identified with a unique name in the format EMCC1, EMCC2, and so on. The Bulk Administration Tool assigns device numbers by obtaining the last one used.

Procedure

Step 1 From From Cisco Unified CM Administration, choose **Bulk Administration** > **EMCC** > **Insert/Update EMCC**.

Step 2 Click **Insert EMCC Devices**.

Step 3 Enter the number of devices you are adding in the **Number of EMCC Devices to be added** field.

Step 4 Click **Run Immediately** and click **Submit**.

Step 5 Refresh the window and verify that the **Number of EMCC Devices already in database** value shows the number of devices that you added.

Configure a Geolocation Filter for Extension Mobility Cross Cluster

Configure a geolocation filter to specify criteria for device location matching, such as country, state, and city values. Geolocations are used to identify the location of a device, and the filter indicates what parts of the geolocation are significant.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Geolocation Filter**.

Step 2 Click **Add New**.

Step 3 Configure the fields on the **Geolocation Filter Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 4 Click **Save**.

Configure Feature Parameters for Extension Mobility Cross Cluster

Select values for the feature parameters that you configured, such as the geolocation filter.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advanced Features** > **EMCC** > **EMCC Feature Configuration**.

Step 2 Configure the fields on the **EMCC Feature Configuration** window. See Feature Parameter Fields for Extension Mobility Cross Cluster, on page 415 for more information about the fields and their configuration options.

Step 3 Click **Save**.

Feature Parameter Fields for Extension Mobility Cross Cluster

Table 34: Feature Parameter Fields for Extension Mobility Cross Cluster

EMCC Parameter	Description
Default TFTP Server for EMCC Login Device	Choose the computer name or IP address of the default TFTP server that devices logging into extension mobility cross cluster (EMCC) from a remote cluster should use.
Backup TFTP Server for EMCC Login Device	Choose the computer name or IP address of the backup TFTP server that devices logging into EMCC from a remote cluster should use.
Default Interval for Expired EMCC Device Maintenance	Specify the number of minutes that elapse between system checks for expired EMCC devices. An expired EMCC device is a device that logged in to EMCC from a remote cluster, but that, because of a WAN failure or a connectivity issue, the phone logged out of the visiting cluster. When connectivity was restored, the device logged back into the visiting cluster. During this maintenance job, the Cisco Extension Mobility service checks the Unified Communications Manager database for any expired EMCC devices and automatically logs them out. The default value is 1440 minutes. Valid values range from 10 minutes to 1440 minutes.

EMCC Parameter	Description
Enable All Remote Cluster Services When Adding A New Remote Cluster	Choose whether you want all services on a new remote cluster to be automatically enabled when you add a new cluster. Valid values are True (enable all services on the remote cluster automatically) or False (manually enable the services on the remote cluster via the Remote Cluster Configuration window in Unified Communications Manager). You can enable the services manually so that you have time to configure the EMCC feature completely before enabling the remote services. The default value is False.
CSS for PSTN Access SIP Trunk	Choose the calling search space (CSS) that the PSTN Access SIP trunk for processing EMCC calls uses. The PSTN Access SIP trunk is the SIP trunk that you configured for PSTN access in the **Intercluster Service Profile** window. Calls over this trunk are intended for and are routed to only the local PSTN that is co-located with the EMCC logged-in phone that initiates the call. Valid values are the following: • Use Trunk CSS (PSTN calls use the local route group, which can prove useful for properly routing emergency service calls) • Use phone's original device CSS (PSTN calls are routed using the configured calling search space on the remote phone, that is, the CSS that is used when the phone is not logged into EMCC). The default value is Use trunk CSS.
EMCC Geolocation Filter	Choose the geolocation filter that you have configured for use EMCC. Based on the information in the geolocation that associates with a phone that is logged in through Extension Mobility from another cluster, as well as the selected EMCC geolocation filter, Cisco Unified Communications Manager places the phone into a roaming device pool. Cisco Unified Communications Manager determines which roaming device pool to use by evaluating which device pool best matches the phone geolocation information after the EMCC geolocation filter is applied.
EMCC Region Max Audio Bit Rate	This parameter specifies the maximum audio bit rate for all EMCC calls, regardless of the region associated with the other party. The default value is 8 kbps (G.729). **Note** All participating EMCC clusters must specify the same value for the EMCC region max audio bit rate.

EMCC Parameter	Description
EMCC Region Max Video Call Bit Rate (Includes Audio)	This parameter specifies the maximum video call bit rate for all EMCC video calls, regardless of the maximum video call bit rate of the region associated with the other party. The default value is 384. Valid values range from 0 to 8128. **Note** All participating EMCC clusters must specify the same value for the EMCC region max video call bit rate.
EMCC Region Link Loss Type	This parameter specifies the link loss type between any EMCC phone and devices in any remote cluster. **Note** To allow two-way audio on EMCC calls, all participating EMCC clusters must use the same EMCC region link loss type. Based on the option that you choose, Cisco Unified Communications Manager attempts to use the optimal audio codec for the EMCC call while observing the configured EMCC region max audio bit rate. Valid values are the following: • **Lossy**—A link where some packet loss can or may occur, for example, DSL. • **Low Loss**—A link where low packet loss occurs, for example, T1. When you set this parameter to **Lossy**, Cisco Unified Communications Manager chooses the optimal codec within the limit that is set by the EMCC Region Max Audio Bit Rate, based on audio quality. Some packet loss will occur. When this parameter is set to **Low Loss**, Cisco Unified Communications Manager chooses the optimal codec within the limit that is set by the EMCC Region Max Audio Bit Rate, based on audio quality. Little or no packet loss will occur. The only difference in the audio codec preference ordering between the low loss and lossy options is that G.722 is preferred over Internet Speech Audio Codec (iSAC) when the link loss type is set as low loss, whereas iSAC is preferred over G.722 when the link loss type is set as lossy. The default value is **Low Loss**.
RSVP SIP Trunk KeepAlive Timer	Specify the number of seconds that Unified Communications Manager waits between sending or receiving KeepAlive messages or acknowledgments between two clusters over EMCC RSVP SIP trunks. An EMCC RSVP SIP trunk is a SIP trunk that has Cisco Extension Mobility Cross Cluster configured as the Trunk Service Type and that has been selected as the SIP Trunk for RSVP Agent in the Intercluster Service Profile window. When two of these intervals elapse without receipt of a KeepAlive message or an acknowledgment, Unified Communications Manager releases the RSVP resources with the remote cluster. The default value is 15 seconds. Valid values range from 1 second to 600 seconds.

EMCC Parameter	Description
Default Server For Remote Cluster Update	Choose the default server name or IP address of the primary node in this local cluster that has the Cisco Extension Mobility service activated. The remote cluster accesses this node to get information about this local cluster.
Backup Server for Remote Cluster Update	Choose the default server name or IP address of the secondary node in this local cluster that has the Cisco Extension Mobility service activated. The remote cluster accesses this node when the primary node is down to retrieve information about this local cluster.
Remote Cluster Update Interval	Specify an interval, in minutes, during which the Cisco Extension Mobility service on the local node collects information about the remote EMCC cluster. Collected information includes such details as the remote cluster Unified Communications Manager version and service information. The default value is 30. Valid values range from 15 minutes to 10,080 minutes.

Configure Intercluster SIP Trunk for Extension Mobility Cross Cluster

Configure trunks to process inbound or outbound traffic for intercluster PSTN access and RSVP agent services. You can configure one trunk for both PSTN access and RSVP agent services or one trunk for each service. You do not need more than two SIP trunks for extension mobility cross cluster.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Trunk**.

Step 2 Click **Add New**.

Step 3 From the **Trunk Type** drop-down list, choose **SIP Trunk**.

Step 4 From the **Trunk Service Type** drop-down list, choose **Extension Mobility Cross Clusters**.

Step 5 Click **Next**.

Step 6 Configure the fields in the **Trunk Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 7 Click **Save**.

Configure an Intercluster Service Profile for Extension Mobility Cross Cluster

Configure the intercluster service profile to activate extension mobility cross cluster. The profile collects all the configuration that precedes and provides a results report.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advance Features** > **EMCC** > **EMCC Intercluster Service Profile**.

Step 2 Configure the fields on the **EMCC Intercluster Service Profile Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 3 If no failure messages appear in the popup window, click **Save**.

Configure Remote Cluster Services

Configure the remote cluster for extension mobility cross cluster. This step completes the link between the home cluster with remote (visiting) cluster.

Procedure

Step 1 From From Cisco Unified CM Administration, choose **Advanced Features** > **Cluster View**.

Step 2 Click **Find** to show a list of known remote clusters.

Step 3 Perform one of the following steps:

- Click the remote cluster name and verify the fields if the remote cluster that you want to configure appears.
- Click **Add New** if the remote cluster that you want to configure does not appear and configure the following fields:

  a. For the **Cluster Id** field, ensure that the ID matches the enterprise parameter value of the cluster ID of the other clusters.

  b. n the **Fully Qualified Name** field, enter the IP address of the remote cluster or a domain name that can resolve to any node on the remote cluster.

  c. Click **Save**.

Note For extension mobility cross cluster, the **TFTP** check box should always be disabled.

Extension Mobility Cross Cluster Interactions and Restrictions

- Extension Mobility Cross Cluster Restrictions, on page 420

Extension Mobility Cross Cluster Interactions

Table 35: Extension Mobility Cross Cluster Interactions

Feature	Interaction
Audio	The default maximum audio bit-rate for EMCC login device is set to 8 kbps (G.729).

Feature	Interaction
Call Admission Control (CAC)	• The home cluster is unaware of visiting cluster locations and regions. • The system cannot apply Cisco Unified Communications Manager locations and regions across the cluster boundaries. • RSVP agent-based CAC uses RSVP agents in the visiting cluster.
Call Forwarding	EMCC supports call forwarding.
Cisco Extension Mobility login and logout	User authentication takes place across clusters.
Media resources for the visiting phone	Examples include RSVP agent, TRP, music on mold (MOH), MTP, transcoder, and conference bridge. Media resources are local to the visiting phone (other than RSVP agents).
PSTN access for the visiting phone	• E911 calls are routed to the local gateways of the PSTN. • Local calls are routed to the local gateways of the PSTN. • Calls terminating to local route groups route to local gateways in the visiting cluster.
Other call features and services	Example restriction: Intercom configuration specifies configuration to a static device, so EMCC does not support the intercom feature.
Security	• Cross-cluster security is provided by default. • Cisco Unified IP Phones with secure and nonsecure phone security profiles are supported.

Extension Mobility Cross Cluster Restrictions

Table 36: Extension Mobility Cross Cluster Restrictions

Restriction	Description
Unsupported Features	• EMCC does not support the intercom feature, because intercom configuration requires a static device. • Location CAC is not supported, but RSVP-based CAC is supported.
EMCC Device Cannot Be Provisioned in More Than One Cluster	For EMCC to function properly, you cannot configure the same phone (device name) in two clusters. Otherwise, login will fail due to the duplicate device error (37). For this reason, for cluster deployed with EMCC you should disable Autoregistration on all Unified Communication Manager nodes to prevent a new device being created in the home cluster after EMCC logout.

Restriction	Description
Number of EMCC Devices	Cisco Unified Communications Manager can support a MaxPhones value of 60,000. Include EMCC in the total number of devices that are supported in the cluster by using the following calculation: Phones + (2 x EMCC devices) = MaxPhones **Note** EMCC login does not affect the number of licenses that are used in the home cluster.
Visiting Device Logout Limitations	• If the home cluster administrator disables EMCC for a user while the user is logged in with EMCC, the system does not automatically log this user out. Instead, the system does not allow future EMCC attempts by this user. The current EMCC session continues until the user logs out. • In the visiting cluster, the **Phone Configuration** window has a Log Out button for extension mobility. This button is also used by the visiting cluster administrator to log out an EMCC phone. Because the EMCC phone is not currently registered with the visiting Cisco Unified Communications Manager, this operation is like a database cleanup in the visiting cluster. The EMCC phone remains registered with the home Cisco Unified Communications Manager until the phone returns to the visiting cluster because of a reset or a logout from the home cluster.
Visiting Device Login Limitations	The extension mobility service in participating clusters performs a periodic remote cluster update. The **Remote Cluster Update Interval** feature parameter controls the update interval. The default interval is 30 minutes. If the extension mobility service on cluster A does not receive a reply from a remote cluster (such as cluster B) for this update, the Remote Cluster window for cluster A shows that the Remote Activated service is set to False for cluster B. In this case, the visiting cluster does not receive any response from the home cluster and sets the Remote Activated values for the home cluster to False. During this interval, a visiting phone may not be able to log in by using EMCC. The visiting phone receives the “Login is unavailable” error message. At this point, a login attempt to EMCC from a visiting phone can fail; the phone displays the “Login is unavailable” error message. This error occurs because the visiting cluster has not yet detected the change of the home cluster from out-of-service to in-service. Remote cluster status change is based on the value of the Remote Cluster Update Interval EMCC feature parameter and on when the visiting extension mobility service performed the last query or update. You can select **Update Remote Cluster Now** in the **Remote Cluster Service Configuration** window (**Advanced Features** > **EMCC** > **EMCC Remote Cluster**) to change Remote Activate values to True, which also allows EMCC logins. Otherwise, after the next periodic update cycle, EMCC logins by visiting phones will return to normal.

Extension Mobility Cross Cluster and Security Mode for Different Cluster Versions

Note Phone configuration files can be encrypted only if both the home cluster and visiting cluster versions are 9.x or later, and when the TFTP encryption configuration flag is enabled.

During EMCC login, if both the visiting cluster and home cluster versions are in 9.x or later, the phone will behave in various modes as shown in the following table.

Table 37: Supported Security Modes When Both Visiting Cluster and Home Cluster Are In 9.x or later Versions

Home Cluster Version	Home Cluster Mode	Visiting Cluster Version	Visiting Cluster Mode	Visiting Phone Mode	EMCC Status
9.x or later	Mixed	9.x or later	Mixed	Secure	Secure EMCC
9.x or later	Mixed	9.x or later	Mixed	Non-secure	Non-secure EMCC
9.x or later	Mixed	9.x or later	Non-secure	Non-secure	Non-secure EMCC
9.x or later	Non-secure	9.x or later	Mixed	Secure	Login fails
9.x or later	Non-secure	9.x or later	Non-secure	Non-secure	Non-secure EMCC

During EMCC login, if the visiting cluster version is 8.x and the home cluster version is 9.x or later, the phone will behave in various modes as shown in the following table.

Table 38: Supported Security Modes When Visiting Cluster Is In 8.x and Home Cluster Is In 9.x or later Version

Home Cluster Version	Home Cluster Mode	Visiting Cluster Version	Visiting Cluster Mode	Visiting Phone Mode	EMCC Status
9.x or later	Mixed	8.x	Mixed	Secure	Not supported
9.x or later	Mixed	8.x	Mixed	Non-secure	Non-secure EMCC
9.x or later	Mixed	8.x	Non-secure	Non-secure	Non-secure EMCC
9.x or later	Non-secure	8.x	Mixed	Secure	Not supported
9.x or later	Non-secure	8.x	Non-secure	Non-secure	Non-secure EMCC

During EMCC login, if the visiting cluster version is 9.x or later and the home cluster version is 8.x, the phone will behave in various modes as shown in the following table.

Table 39: Supported Security Modes When Visiting Cluster Is In 9.x or later and Home Cluster Is In 8.x Version

Home Cluster Version	Home Cluster Mode	Visiting Cluster Version	Visiting Cluster Mode	Visiting Phone Mode	EMCC Status
8.x	Mixed	9.x or later	Mixed	Secure	Login fails
8.x	Mixed	9.x or later	Mixed	Non-secure	Non-secure EMCC
8.x	Mixed	9.x or later	Non-secure	Non-secure	Non-secure EMCC
8.x	Non-secure	9.x or later	Mixed	Secure	Login fails
8.x	Non-secure	9.x or later	Non-secure	Secure	Non-secure EMCC

Extension Mobility Cross Cluster Troubleshooting

Extension Mobility Application Error Codes

Table 40: Extension Mobility Application Error Codes

Error Code	Phone Display	Quick Description	Reason
201	Please try to login again (201)	Authentication Error	If the user is an EMCC user, this error can occur if "EMCC" is not activated on the **Intercluster Service Profile** window.
202	Please try to login again (202)	Blank userid or pin	The user enters a blank user ID or PIN.
204	Login is unavailable (204)	Directory server error	The EMApp sends this error to the phone when IMS could not authenticate the user with the given PIN.
205	Login is unavailable (205) Logout is unavailable (205)	User Profile Absent	Occurs when the user profile information cannot be retrieved from the cache or the database.

Error Code	Phone Display	Quick Description	Reason
207	Login is unavailable(207) Logout is unavailable(207)	Device Name Empty	Occurs when the device or name tag is missing in the request URI. This cannot happen with real devices and can occur only if the request is sent from third-party applications.
208	Login is unavailable(208) Logout is unavailable(208)	EMService Connection Error	The visiting EMApp cannot connect to any Visiting EMService. (The service is down or not activated.) The visiting EMService cannot connect to the Home EMService (the WAN is down or certificates are not trusted.)
210	Login is unavailable(210) Logout is unavailable(210)	Init Fail-Contact Admin	An error (such as a database connection failure) occurred while initializing EMApp. The error can occur because of a failure to connect to the database during startup.
211	Login is unavailable(211) Logout is unavailable(211)	EMCC Not Activated	Occurs when the PSTN is not activated in the **Intercluster Service Profile** window of the visiting cluster.
212	Login is unavailable(212)	Cluster ID is invalid	Occurs when a remote cluster update fails by sending an incorrect cluster ID to the remote cluster.
213	Login is unavailable(213) Logout is unavailable(213)	Device does not support EMCC	Occurs when a device does not support EMCC.

Extension Mobility Service Error Codes

Table 41: Extension Mobility Service Error Codes

Error Code	Phone Display	Quick Description	Reason
0	Login is unavailable(0) Logout is unavailable(0)	Unknown Error	The EMService failed for an unknown reason.
1	Login is unavailable(1) Logout is unavailable(1)	Error on parsing	When the EMService cannot parse the XML request from the EMApp or EMService. This error occurs when third-party applications send an incorrect query to login XML (EM API). The error can also occur because of a version mismatch between home and visiting clusters.
2	Login is unavailable(2)	EMCC Authentication Error	The EMCC user credentials cannot be authenticated because the user entered an incorrect PIN.
3	Login is unavailable(3) Logout is unavailable(3)	Invalid App User	Invalid application user. This error commonly occurs because of the EM API.
4	Login is unavailable(4) Logout is unavailable(4)	Policy Validation error	The EM Service sends this error when it cannot validate the login or logout request because of an unknown reason, an error while querying the database or an error while retrieving information from the cache.
5	Login is unavailable(5) Logout is unavailable(5)	Dev. logon disabled	A user logs into a device that has **Enable Extension Mobility** unchecked in the **Phone Configuration** window.

Error Code	Phone Display	Quick Description	Reason
6	Login is unavailable(6) Logout is unavailable(6)	Database Error	Whenever the database returns an exception while executing the query or stored procedure that the EM Service requests (login/logout or device/user query), the EM Service sends this error code to EMApp.
8	Login is unavailable(8) Logout is unavailable(8)	Query type undetermined	No valid query was sent to the EMService (DeviceUserQuery and UserDeviceQuery are valid ones). This error occurs because of the EM API or incorrect XML input.
9	Login is unavailable(9) Logout is unavailable(9)	Dir. User Info Error	This error appears in two cases: **1.** IMS returns an exception when it attempts to authenticate a user. **2.** When information about a user cannot be retrieved either from the cache or database.
10	Login is unavailable(10) Logout is unavailable(10)	User lacks app proxy rights	The user tries to log in on behalf of another user. By default, a CCMSysUser has administrative rights.
11	Login is unavailable(11) Logout is unavailable(11)	Device Does not exist	The phone record entry is absent in the device table.
12	Phone record entry is absent in the device table	Dev. Profile not found	No device profile is associated with the remote user.
18	Login is unavailable(18)	Another user logged in	Another user is already logged in on the phone.

Error Code	Phone Display	Quick Description	Reason
19	Logout is unavailable(19)	No user logged in	The system attempted to log out a user who has not logged in. This error occurs when sending logout requests from third-party applications (EM API).
20	Login is unavailable(20) Logout is unavailable(20)	Hoteling flag error	**Enable Extension Mobility** is unchecked in the **Phone Configuration** window.
21	Login is unavailable(21) Logout is unavailable(21)	Hoteling Status error	The current user status was not retrieved from either the local cache or database.
22	Login is unavailable(22)	Dev. logon disabled	Occurs when EM is not enabled on device and the request is sent via EM API or when the services button is pressed on phone.
23	Login is Unavailable (23) Logout is Unavailable (23)	User does not exist	Occurs when the given user ID is not found (in any of the remote clusters).
25	Login is unavailable(25)	User logged in elsewhere	The user is currently logged in to some other phone.
26	Login is unavailable(26) Logout is unavailable(26)	Busy, please try again	Occurs when the EMService has currently reached the threshold level of Maximum Concurrent Requests service parameter.

Error Code	Phone Display	Quick Description	Reason
28	Login is unavailable(28) Logout is unavailable(28)	Untrusted IP Error	Occurs when the Validate IP Address service parameter is set to **True** and the user tries to log in or log out from a machine whose IP address is not trusted. For example, a third-party application or EM API from a machine is not listed in the Trusted List of Ips service parameter.
29	Login is unavailable(29) Logout is unavailable(29)	ris down-contact admin	The Real-Time Information Server Data Collector (RISDC) cache is not created or initialized, and the EMService is unable to connect to RISDC.
30	Login is unavailable(30) Logout is unavailable(30)	Proxy not allowed	When login and logout occur through proxy (“Via” is set in HTTP header) and the Allow Proxy service parameter is set to **False**.
31	Login is unavailable(31) Logout is unavailable(31)	EMCC Not Activated for the user	Occurs when the **Enable Extension Mobility Cross Cluster** check box is not checked in the **End User Configuration** window of the home cluster.
32	Login is unavailable(32) Logout is unavailable(32)	Device does not support EMCC	Occurs when a device model does not have EMCC capability.
33	Login is unavailable(33) Logout is unavailable(33)	No free EMCC dummy device	Occurs when all the EMCC dummy devices are in use by other EMCC logins.
35	Login is unavailable(35) Logout is unavailable(35)	Visiting Cluster Information is not present in Home Cluster	Occurs when the home cluster does not have an entry for this visiting cluster.

Error Code	Phone Display	Quick Description	Reason
36	Login is unavailable(36) Logout is unavailable(36)	No Remote Cluster	Occurs when the administrator has not added a remote cluster.
37	Login is Unavailable (37) Logout is Unavailable (37)	Duplicate Device Name	Occurs when the same device name exists in both the home cluster and visiting cluster.
38	Login is unavailable(38) Logout is unavailable(38)	EMCC Not Allowed	Occurs when the home cluster does not want to allow EMCC login (The **Enable Extension Mobility Cross Cluster** check box is not checked in the home cluster).
43	Login is unavailable(43)	Device Security mode error	The Device Security Profile that is associated to the EMCC device should be set to Nonsecure for its Device Security Mode.
45	Login is unsuccessful(45)	Remote Cluster version not supported	Occurs during EMCC login when the visiting cluster version is 9.x and is in mixed mode, the phone is in secure mode, and the home cluster version is 8.x.
46	Login is unsuccessful(46)	Remote Cluster security mode not supported	Occurs during EMCC login when the visiting cluster security mode is in mixed mode, the phone is in secure mode, and the home cluster is in nonsecure mode.

CHAPTER 29

Hold Reversion

This chapter provides information about the hold reversion feature which alerts a phone user when a held call exceeds a configured time limit.

Hold Reversion Overview

When you place a call on hold, the Hold Reversion feature alerts you when the held call exceeds a configured time limit. When the configured time limit expires, an alert is generated on your phone to remind you to handle the call.

The following alerts are available:

- The Phone rings or beeps once
- The status line displays “Hold Reversion”
- The LED next to the line button flashes continuously
- A vibrating handset icon displays

Note The type of alert that you receive depends on the capabilities of your phone.

To retrieve a reverted call, you can:

- Pick up the handset
- Press the speaker button on the phone
- Press the headset button
- Select the line that is associated with the reverted call
- Press the Resume softkey

For details, see the user guide for your particular phone model.

Hold Reversion Prerequisites

- Cisco CallManager service must be running on at least one node in the cluster
- Cisco CTIManager service must be running on at least one node in the cluster
- Cisco Database Layer Monitor service must be running on the same node as the Cisco CallManager service
- Cisco RIS Data Collector service must be running on the same node as the Cisco CallManager service
- Cisco Tftp service must be running on at least one node in the cluster
- Cisco Unified Communications Manager Locale Installer must be installed, if you want to use non-English phone locales or country-specific tones

Hold Reversion Configuration Task Flow

Perform the following steps to configure Hold Reversion for your phones. This procedure assumes that you have configured directory numbers for phones, or that you are using auto-registration.

Before you begin

- If phone users want the hold reversion messages to display in a language other than English, or if you want the user to receive country-specific tones for calls, verify that you have installed the locale installer.
- Review Hold Reversion Prerequisites, on page 432

Procedure

	Command or Action	Purpose
Step 1	Generate a Phone Feature List, on page 3	Run a phone feature list report to determine which phones support the Hold Reversion feature.
Step 2	Configure Call Focus Priority for Hold Reversion, on page 432	Configure the call focus priority setting against the device pool for your phones.
Step 3	Perform one of the following procedures: • Configure Hold Reversion Timer Defaults for Cluster, on page 433 • Configure Hold Reversion Timer Settings for Phone, on page 434	Configure the Hold Reversion timer settings. You can configure the timer using a clusterwide service parameter, or configure the settings on an individual phone line. **Note** The settings on an individual phone line override the clusterwide service parameter settings.

Configure Call Focus Priority for Hold Reversion

As an administrator, you can prioritize incoming calls and reverted calls. By default, all incoming calls are handled before reverted calls, however you can change the call focus priority so that reverted calls take precedence.

Before you begin

Generate a Phone Feature List, on page 3

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Device Pool** and open the device pool that applies to your phones.

Step 2 In the **Reverted Call Focus Priority** field, choose one of the following options and click **Save**:

- **Default**—Incoming calls have priority over reverted calls.
- **Highest**—Reverted calls have priority over incoming calls.

Step 3 Click **Save**.

Step 4 Reset any devices in the Device Pool by performing the following steps:

a) Click **Reset**. The **Device Reset** window displays.

b) In the **Device Reset** window, click **Reset**.

What to do next

Perform one of the following procedures to configure Hold Reversion Timer Settings:

- Configure Hold Reversion Timer Defaults for Cluster, on page 433
- Configure Hold Reversion Timer Settings for Phone, on page 434

Configure Hold Reversion Timer Defaults for Cluster

Perform this procedure to configure clusterwide service parameters that apply hold reversion timer default settings for all phones in the cluster.

Note When you configure the clusterwide service parameters, the configuration is applied as the default hold reversion setting for all phones in the cluster. However, the settings on an individual phone line can override the clusterwide defaults.

Before you begin

Configure Call Focus Priority for Hold Reversion, on page 432

Procedure

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

Step 2 From the **Server** drop-down list, choose the server that is running the **CallManager** service.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.

Step 4 Configure values for the following clusterwide service parameters:

- **Hold Reversion Duration**—Enter a number from 0 to 1200 (inclusive) to specify the wait time in seconds before Cisco Unified Communications Manager issues a reverted call alert to the holding party phone. If you enter 0, Cisco Unified Communications Manager does not issue reverted call alerts, unless it is configured on a phone line.
- **Hold Reversion Interval Notification**—Enter a number from 0 to 1200 (inclusive) to specify the wait time in seconds before Cisco Unified Communications Manager sends periodic reminder alerts to the holding party phone. If you enter 0, Cisco Unified Communications Manager does not send periodic reminder alerts unless the timer is configured on a phone line.

Step 5 Click **Save**.

Configure Hold Reversion Timer Settings for Phone

Perform this procedure to configure Hold Reversion timer settings for a phone and phone line.

Note You can also configure Hold Reversion timer settings using a clusterwide service parameter. However, the settings on an individual phone line override the clusterwide service parameter setting.

Before you begin

Perform Configure Hold Reversion Timer Defaults for Cluster, on page 433 to configure Hold Reversion clusterwide defaults.

Procedure

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

Step 2 Click **Find** and select the phone on which you want to configure Hold Reversion.

Step 3 In the **Association** pane on the left, click the phone line on which you want to configure Hold Reversion.

Step 4 Configure values for the following fields:

- **Hold Reversion Ring Duration**—Enter a number from 0 to 1200 (inclusive) to specify the wait time in seconds before Cisco Unified Communications Manager issues a reverted call alert. If you enter 0, Cisco Unified Communications Manager does not issue reverted call alerts to this DN. If you leave the field empty (the default setting), Cisco Unified Communications Manager applies the setting from the Hold Reversion Duration service parameter.
- **Hold Reversion Ring Interval Notification**—Enter a number from 0 to 1200 (inclusive) to specify the wait time in seconds before Cisco Unified Communications Manager sends periodic reminder alerts. If you enter 0, Cisco Unified Communications Manager does not send periodic reminder alerts to this DN. If you leave the field empty (the default setting), Cisco Unified Communications Manager applies the setting from the Hold Reversion Interval Notification service parameter.

Step 5 Click **Save**.

Step 6 Reset the phone by performing the following steps:

a) Click **Reset**. The **Reset Device** window displays.

b) Click **Reset**.

Hold Reversion Interactions

Table 42: Hold Reversion Feature Interactions

Feature	Interactions
Music on Hold	MOH is supported on a reverted call if MOH is configured for a normal held call.
Call Park	If hold reversion is invoked and the held party presses the **Park** softkey, the holding party still receives hold reversion alerts and can retrieve the call. When the holding party retrieves the call, the holding party receives MOH, if configured. If the held party parks before the hold duration exceeds the configured time limit, the system suppresses all hold reversion alerts until the call is picked up or redirected.
MLPP	When a multilevel precedence and preemption (MLPP) call is put on hold and reverts, the MLPP call loses its preemption status, and the reverted call gets treated as a routine call. After the call reverts, the system does not play a preemption ring. If a high precedence call becomes a reverted call, the system does not play a precedence tone.
CTI Applications	CTI applications can access hold reversion functionality when the feature is enabled for a line or the system. Cisco-provided applications such as Cisco Unified Communications Manager Assistant and attendant console provide hold reversion functionality using the CTI interface. When hold reversion gets invoked, the CTI port receives event notification instead of the audible tone presented on Cisco Unified IP Phones. CTI ports and route points receive the event notification once only, whereas Cisco Unified IP Phones receive alerts at regular intervals. See the following API documents for information about CTI requirements and interactions with hold reversion: • *Cisco Unified Communications JTAPI Developer Guide* • *Cisco Unified Communications TAPI Developer Guide*
Hold Reversion Interval for SCCP phones when interacting with SIP Phones	SCCP phones support a minimum Hold Reversion Notification Interval (HRNI) of 5 seconds, whereas SIP phones support a minimum of 10 seconds. SCCP phones set for the minimum HRNI of 5 seconds may experience a Hold Reversion Notification ring delay of 10 seconds when handling calls involving SIP phones.
Shared Lines	If a Cisco Unified IP Phone that supports hold reversion shares a line with a phone device that does not support hold reversion, the hold reversion configuration settings display only for the line on the supporting device. If a shared line device disables the feature, hold reversion gets disabled on all other devices that share the line.

Feature	Interactions
Ring Settings	If the ring settings that are configured for the phone specify Disabled, the phone does not ring, flash, or beep for the hold reversion feature.

Hold Reversion Restrictions

Feature	Restriction
Cisco Extension Mobility and Cisco Web Dialer	Cisco Extension Mobility and Cisco Web Dialer features do not support the hold reversion feature.
SCCP phones	This feature does not support SCCP analog phone types, such as ATA 186, DPA-7610, and DPA-7630. Only certain on-net phone devices that are running SCCP on a node can invoke the hold reversion feature.
Directory numbers	If a directory number is associated to a phone that does not support hold reversion, the feature settings do not display for that directory number in the **Directory Number Configuration** window.
Shared lines	If a Cisco Unified IP Phone that supports hold reversion shares a line with a phone device that does not support hold reversion, the hold reversion configuration settings display only for the line on the supporting device. If a shared-line device disables this feature, hold reversion gets disabled on all other devices that share this line.
Ring settings	Hold reversion ring uses the ring settings that Cisco Unified Communications Manager Administration defines for that user (disable, flash only, ring once, ring, beep only) except that flash gets converted to flash once, and ring gets converted to ring once. **Note** When an IP Phone call is on normal hold, the ring settings (Phone Idle) from the Call Manager is applied.
Maximum number of reverted calls	The maximum number of reverted calls on a line equals the maximum number of calls on your system.
CTI Applications	To enable this feature with CTI applications, ensure that the CTI application is certified to work with this feature and this release. Otherwise, the CTI application may fail because the hold reversion feature may affect existing CTI applications. This feature gets disabled by default. See the following API documents for information about CTI requirements: • *Cisco Unified TAPI Developers Guide for Cisco Unified Communications Manager* • *Cisco Unified JTAPI Developers Guide for Cisco Unified Communications Manager*

Feature	Restriction
Cisco Unified IP Phones	You cannot configure hold reversion settings for DNs that are associated with phones that do not support this feature. Only Cisco Unified IP Phones that support the hold reversion feature display the hold reversion timer settings in the Directory Number Configuration window. When Hold Reversion is configured for the system, the phone must support the feature or the feature does not activate. See Cisco Unified IP Phone administration guides for Cisco Unified IP Phone models that support hold reversion and this version of Unified Communications Manager for any phone restrictions with hold reversion.

CHAPTER 30

Accessing Hunt Groups

Hunt Group Overview

A Hunt Group is a group of lines that are organized hierarchically, so that if the first number in the hunt group list is busy, the system dials the second number. If the second number is busy, the system dials the next number, and so on.

The phone users can log in to or log out of the hunt groups by using the HLog softkey or the Hunt Group line button on the IP phone. The phone provides a visual status of the login state, so that the user can determine whether they are logged in to one or more of their line groups.

The Hunt Group feature provides the following functions:

- The HLog softkey on the IP phone allows the user to toggle between login and logout of phone.
- A hunt group allows a caller to automatically find an available line from amongst a group of extensions.
- The Hunt Group Log Off feature allows phone users to prevent their phones from receiving incoming calls that get routed to directory numbers. Regardless of the phone status, the phone rings normally for incoming calls that are not calls to one or more line groups associated with the phone.

  Note The directory numbers (DNs) belong to line groups that are associated with the phone.

- System administrators can log in or log out the users from the phones that are automatically logged into hunt groups.
- The HLog softkey allows a phone user to log a phone out of all line groups to which the phone directory numbers belong.
- From Cisco Unified Communications Manager Release 9.0 onward, the Hunt Group Log Off feature enables the use of mobile device as a desk phone. When you use the Hlog softkey through your mobile client, you no longer receive calls that are placed to the hunt pilot.

Hunt Group Prerequisites

- The phones must be running Skinny Client Control Protocol (SCCP) or Session Initiation Protocol (SIP).
- The phone ringtone file must be located in the TFTP directory (/usr/local/cm/tftp).

Hunt Group Configuration Task Flow

Before you begin

- Review Hunt Group Prerequisites, on page 440

Procedure

	Command or Action	Purpose
Step 1	Configure a Softkey Template for Hunt Group, on page 440	Configure a softkey template for the HLog softkey.
Step 2	To Associate a Softkey Template with a Common Device Configuration, on page 442, complete the following subtasks: • Add a Softkey Template to a Common Device Configuration, on page 442 • Associate a Common Device Configuration with a Phone, on page 443	Optional. To make the softkey template available to phones, you must complete either this step or the following step. Follow this step if your system uses a Common Device Configuration to apply configuration options to phones. This is the most commonly used method for making a softkey template available to phones.
Step 3	Associate a Softkey Template with a Phone, on page 443	Optional. Use this procedure either as an alternative to associating the softkey template with the Common Device Configuration, or in conjunction with the Common Device Configuration. Use this procedure in conjunction with the Common Device Configuration if you need to assign a softkey template that overrides the assignment in the Common Device Configuration or any other default softkey assignment.
Step 4	Configure Phones for Hunt Group, on page 444	Configure phones to automatically log in to or log out of hunt groups and hunt lists.

Configure a Softkey Template for Hunt Group

The HLog softkey appears on the phone when the phone is in the following call states:

- Connected

- On Hook
- Off Hook

Note You must create a new softkey template to configure the HLog softkey. You cannot configure the HLog softkey in a standard softkey template.

Use this procedure to make the HLog softkey available:

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Softkey Template**.

Step 2 Perform the following steps to create a new softkey template; otherwise, proceed to the next step.

a) Click **Add New**.
b) Select a default template and click **Copy**.
c) Enter a new name for the template in the **Softkey Template Name** field.
d) Click **Save**.

Step 3 Perform the following steps to add softkeys to an existing template.

a) Click **Find** and enter the search criteria.
b) Select the required existing template.

Step 4 Check the **Default Softkey Template** check box to designate this softkey template as the default softkey template.

Note If you designate a softkey template as the default softkey template, you cannot delete it unless you first remove the default designation.

Step 5 Choose **Configure Softkey Layout** from the **Related Links** drop-down list in the upper right corner and click **Go**.

Step 6 From the **Select a Call State to Configure** drop-down list, choose the call state for which you want the softkey to display.

Step 7 From the **Unselected Softkeys** list, choose the softkey to add and click the right arrow to move the softkey to the **Selected Softkeys** list. Use the up and down arrows to change the position of the new softkey.

Step 8 Repeat the previous step to display the softkey in additional call states.

Step 9 Click **Save**.

Step 10 Perform one of the following tasks:

- Click **Apply Config** if you modified a template that is already associated with devices to restart the devices.
- If you created a new softkey template, associate the template with the devices and then restart them. For more information, see *Add a Softkey Template to a Common Device Configuration* and *Associate a Softkey Template with a Phone* sections.

What to do next

Perform one of the following procedures:

- Add a Softkey Template to a Common Device Configuration, on page 442
- Associate a Softkey Template with a Phone, on page 443

Associate a Softkey Template with a Common Device Configuration

Optional. There are two ways to associate a softkey template with a phone:

- Add the softkey template to the **Phone Configuration**.
- Add the softkey template to the **Common Device Configuration**.

The procedures in this section describe how to associate the softkey template with a **Common Device Configuration**. Follow these procedures if your system uses a **Common Device Configuration** to apply configuration options to phones. This is the most commonly used method for making a softkey template available to phones.

To use the alternative method, see Associate a Softkey Template with a Phone, on page 443.

Before you begin

Configure a Softkey Template for Hunt Group, on page 440

Procedure

	Command or Action	Purpose
Step 1	Add a Softkey Template to a Common Device Configuration, on page 442	
Step 2	Associate a Common Device Configuration with a Phone, on page 443	

Add a Softkey Template to a Common Device Configuration

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Common Device Configuration**.

Step 2 Perform the following steps to create a new Common Device Configuration and associate the softkey template with it; otherwise, proceed to the next step.

a) Click **Add New**.
b) Enter a name for the Common Device Configuration in the **Name** field.
c) Click **Save**.

Step 3 Perform the following steps to add the softkey template to an existing Common Device Configuration.

a) Click **Find** and enter the search criteria.
b) Click an existing Common Device Configuration.

Step 4 In the **Softkey Template** drop-down list, choose the softkey template that contains the softkey that you want to make available.

Step 5 Click **Save**.

Step 6 Perform one of the following tasks:

- If you modified a Common Device Configuration that is already associated with devices, click **Apply Config** to restart the devices.
- If you created a new Common Device Configuration, associate the configuration with devices and then restart them.

Associate a Common Device Configuration with a Phone

Before you begin

Add a Softkey Template to a Common Device Configuration, on page 442

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select the phone device to add the softkey template.

Step 3 From the **Common Device Configuration** drop-down list, choose the common device configuration that contains the new softkey template.

Step 4 Click **Save**.

Step 5 Click **Reset** to update the phone settings.

Associate a Softkey Template with a Phone

This procedure is optional. You can use this procedure as an alternative to associating the softkey template with the Common Device Configuration. This procedure also works in conjunction with the Common Device Configuration: use it when you need to assign a softkey template that overrides the assignment in the Common Device Configuration or any other default softkey assignment.

Before you begin

Configure a Softkey Template for Hunt Group, on page 440

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.
The **Find and List Phones** window appears.

Step 2 Choose the phone to which you want to add the softkey template.
The **Phone Configuration** window appears.

Step 3 From the **Softkey Template** drop-down list, choose the template that contains the new softkey.

Step 4 Click **Save**.
A dialog box appears with a message to press **Reset** to update the phone settings.

Configure Phones for Hunt Group

Use this procedure to configure phones to automatically log in to or log out of hunt groups and hunt lists.

Before you begin

Ensure the phone directory numbers belong to one or more hunt groups.

See the Administration Guide for Cisco Unified Communications Manager for information on hunt groups and hunt lists.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Perform one of the following tasks:

a) To modify the fields for an existing phone, enter search criteria and choose a phone from the resulting list. The **Phone Configuration** window appears.

b) To add a new phone, click **Add New**.

The **Add a New Phone** window appears.

Step 3 In the **Phone Configuration** window, perform one of the following tasks:

a) To log out the phone from the hunt group, uncheck the **Logged Into Hunt Group** check box.

b) To log in the phone to the hunt group, ensure that the **Logged Into Hunt Group** check box is checked.

Note The **Logged Into Hunt Group** check box remains checked by default for all phones.

Step 4 Click **Save**.

Configure Hunt Group Service Parameter

The **Hunt Group Logoff Notification** service parameter provides the option to turn audible ringtones on or off when calls that come in to a line group arrive at a phone that is currently logged out. This ringtone alerts a logged-out user that there is an incoming call to a hunt list to which the line is a member, but the call will not ring at the phone of that line group member because of the logged-out status.

To configure the **Hunt Group Logoff Notification** service parameter, perform the following steps.

Procedure

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

Step 2 From the **Server** drop-down list, choose the server that is running the Cisco CallManager service.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.

The **Service Parameter Configuration** window appears.

Step 4 In the Clusterwide Parameters (**Device - Phone**) section, configure values for the following Hunt Group Logoff Notification service parameter:

Enter a name for the ringtone file that Cisco IP Phones play when a member of a line group (hunt group) has logged out. The default value for this service parameter is None, which indicates no ringtone. You can enter a maximum of 255 characters.

Step 5 Click **Save**.
The window refreshes, and Cisco Unified Communications Manager updates the service parameter with your changes.

Hunt Group Interactions and Restrictions

Hunt Group Interactions

Feature	Interaction
Non-shared-line Directory Number	If a phone is logged out of a line group and an extension on the phone is not shared, the line group does not ring that directory number (DN) in the line group. When the line group would normally offer the call to the DN, call processing skips the DN and acts as if the DN does not belong to the line group.
Shared-line Directory Number	Because the Log Out of Hunt Group feature is device-based, when a user logs a phone out, the feature affects only the logged-out phone. Calls to a line group that contains a shared-line directory number behave as follows: • The DN does not ring if all phones that share that DN are logged out. • The DN does ring if one or more phones that share the DN are logged in. • The audible ring on a phone that is logged out is turned off by default. Cisco Unified Communications Manager provides a system parameter that can be set, so that a different ring tone plays when a call comes in to a logged-out hunt group member.

Hunt Group Restrictions

Restriction	Description
Multiple Line Groups	When the user enables the Hunt Group Log Off feature by pressing the HLog softkey, the phone gets logged out from all associated line groups. This is because Hunt Group Log Off is a device-based feature. If a phone has DNs that belong to multiple line groups, pressing the HLog softkey logs the phone out of all associated line groups.

Restriction	Description
7940, 7960, and third-party SIP phones	• When a phone that is running SIP (7906, 7911, 7941, 7961, 7970, and 7971) is logged in to hunt groups and Call Forward All is activated, the call gets presented to the phone that is running SIP. • When 7940 and 7960 phones that are running SIP are logged in to hunt groups and Call Forward All is activated, the phones get skipped and the next phone in the line group rings. • 7940 and 7960 phones that are running SIP and third-party phones that are running SIP can be logged in to or logged out of hunt groups by using the **Phone Configuration** window, but no softkey support exists. • 7940 and 7960 phones that are running SIP and third-party phones that are running SIP do not show “Logged out of hunt groups” on the status line. • 7940 and 7960 phones that are running SIP and third-party phones that are running SIP do not play the Hunt Group Logoff Notification tone regardless of whether the tone is configured.

CHAPTER 31

Malicious Call Identification

Malicious Call Identification Overview

You can configure the Malicious Call Identification (MCID) feature to track troublesome or threatening calls. Users can report these calls by requesting that Cisco Unified Communications Manager identify and register the source of the incoming call in the network.

When the MCID feature is configured, the following actions take place:

1. The user receives a threatening call and presses Malicious call (or enters the feature code *39 if using a POTS phone that is connected to an SCCP gateway).
2. Cisco Unified Communications Manager sends the user a confirmation tone and a text message, if the phone has a display, to acknowledge receiving the MCID notification.
3. Cisco Unified Communications Manager updates the call details record (CDR) for the call with an indication that the call is registered as a malicious call.
4. Cisco Unified Communications Manager generates the alarm and local syslogs entry that contains the event information.
5. Cisco Unified Communications Manager sends an MCID invocation through the facility message to the connected network. The facility information element (IE) encodes the MCID invocation.
6. After receiving this notification, the PSTN or other connected network can take actions, such as providing legal authorities with the call information.

Malicious Call Identification Prerequisites

- Gateways and connections that support MCID:
  - PRI gateways that use the MGCP PRI backhaul interface for T1 (NI2) and E1 (ETSI) connections
  - H.323 trunks and gateways
- IP Phones that support MCID

Malicious Call Identification Configuration Task Flow

Before you begin

- Review Malicious Call Identification Prerequisites, on page 447

Procedure

	Command or Action	Purpose
Step 1	Generate a Phone Feature List, on page 3	Generate a report to identify devices that support the MCID feature.
Step 2	Set Malicious Call ID Service Parameter, on page 449	Enable Cisco Unified Communications Manager to flag a call detail record (CDR) with the MCID indicator.
Step 3	Configure Malicious Call ID Alarms, on page 449	Configure alarms to ensure that alarm information displays in the system logs.
Step 4	Configure a Softkey Template for Malicious Call Identification, on page 450	Configure a softkey template with MCID. **Note** The Cisco Unified IP Phones 8900 and 9900 Series support MCID with feature button only.
Step 5	To Associate a Softkey Template with a Common Device Configuration, on page 450, complete the following subtasks: • Add a Softkey Template to a Common Device Configuration, on page 451 • Associate a Common Device Configuration with a Phone, on page 452	Optional. To make the softkey template available to phones, you must complete either this step or the following step. Follow this step if your system uses a **Common Device Configuration** to apply configuration options to phones. This is the most commonly used method for making a softkey template available to phones.
Step 6	Associate a Softkey Template with a Phone, on page 452	Optional. Use this procedure either as an alternative to associating the softkey template with the Common Device Configuration, or in conjunction with the Common Device Configuration. Use this procedure in conjunction with the Common Device Configuration if you need assign a softkey template that overrides the assignment in the Common Device Configuration or any other default softkey assignment.
Step 7	To Configure Malicious Call Identification Button, on page 452, complete the following subtasks: • Configure Malicious Call ID Phone Button Template, on page 453	Perform this step to add and configure the MCID button to a phone.

	Command or Action	Purpose
	• Associate a Button Template with a Phone , on page 453	

Set Malicious Call ID Service Parameter

To enable Unified Communications Manager to flag a CDR with the MCID indicator, you must enable the CDR flag.

Before you begin

Configure Malicious Call ID Alarms, on page 449

Procedure

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

Step 2 From the **Server** drop-down list, choose the Unified Communications Manager server name.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.
The **Service Parameter Configuration** window displays.

Step 4 In the System area, set the **CDR Enabled Flag** field to **True**.

Step 5 Click **Save**.

Configure Malicious Call ID Alarms

In the Local Syslogs, you must set the alarm event level and activate alarms for MCID.

Before you begin

Set Malicious Call ID Service Parameter, on page 449

Procedure

Step 1 From Cisco Unified Serviceability, choose **Alarm** > **Configuration**.
The **Alarm Configuration** window displays.

Step 2 From the **Server** drop-down list, choose the Unified Communications Manager server and click **Go**.

Step 3 From the **Service Group** drop-down list, choose **CM Services**. The **Alarm Configuration** window updates with configuration fields.

Step 4 From the **Service** drop-down list, choose **Cisco CallManager**.

Step 5 Under Local Syslogs, in the **Alarm Event Level** drop-down list, choose **Informational**.
The **Alarm Configuration** window updates with configuration fields.

Step 6 Under Local Syslogs, check the **Enable Alarm** check box.

Step 7 If you want to enable the alarm for all nodes in the cluster, check the **Apply to All Nodes** check box.

Step 8 To turn on the informational alarm, click **Update**.

Configure a Softkey Template for Malicious Call Identification

Note Skinny Client Control Protocol (SCCP) IP phones use a softkey to invoke the MCID feature.

Before you begin

Configure Malicious Call ID Alarms, on page 449

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Softkey Template**.

Step 2 Perform the following steps to create a new softkey template; otherwise, proceed to the next step.

a) Click **Add New**.
b) Select a default template and click **Copy**.
c) Enter a new name for the template in the **Softkey Template Name** field.
d) Click **Save**.

Step 3 Perform the following steps to add softkeys to an existing template.

a) Click **Find** and enter the search criteria.
b) Select the required existing template.

Step 4 Check the **Default Softkey Template** check box to designate this softkey template as the default softkey template.

Note If you designate a softkey template as the default softkey template, you cannot delete it unless you first remove the default designation.

Step 5 Choose **Configure Softkey Layout** from the **Related Links** drop-down list in the upper right corner and click **Go**.

Step 6 In the **Select a call state to configure** field, choose **Connected**.
The list of Unselected Softkeys changes to display the available softkeys for this call state.

Step 7 In the **Unselected Softkeys** drop-down list, choose **Toggle Malicious Call Trace (MCID)**.

Step 8 From the **Unselected Softkeys** list, choose the softkey to add and click the right arrow to move the softkey to the **Selected Softkeys** list. Use the up and down arrows to change the position of the new softkey.

Step 9 Click **Save.**

Associate a Softkey Template with a Common Device Configuration

Optional. There are two ways to associate a softkey template with a phone:

- Add the softkey template to the **Phone Configuration**.

- Add the softkey template to the **Common Device Configuration**.

The procedures in this section describe how to associate the softkey template with a **Common Device Configuration**. Follow these procedures if your system uses a **Common Device Configuration** to apply configuration options to phones. This is the most commonly used method for making a softkey template available to phones.

To use the alternative method, see Associate a Softkey Template with a Phone, on page 452.

Before you begin

Configure a Softkey Template for Malicious Call Identification, on page 450

Procedure

	Command or Action	Purpose
Step 1	Add a Softkey Template to a Common Device Configuration, on page 451	
Step 2	Associate a Common Device Configuration with a Phone, on page 452	

Add a Softkey Template to a Common Device Configuration

Before you begin

Configure a Softkey Template for Malicious Call Identification, on page 450

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Common Device Configuration**.

Step 2 Perform the following steps to create a new Common Device Configuration and associate the softkey template with it; otherwise, proceed to the next step.

a) Click **Add New**.
b) Enter a name for the Common Device Configuration in the **Name** field.
c) Click **Save**.

Step 3 Perform the following steps to add the softkey template to an existing Common Device Configuration.

a) Click **Find** and enter the search criteria.
b) Click an existing Common Device Configuration.

Step 4 In the **Softkey Template** drop-down list, choose the softkey template that contains the softkey that you want to make available.

Step 5 Click **Save**.

Step 6 Perform one of the following tasks:

- If you modified a Common Device Configuration that is already associated with devices, click **Apply Config** to restart the devices.

- If you created a new Common Device Configuration, associate the configuration with devices and then restart them.

Associate a Common Device Configuration with a Phone

Before you begin

Add a Softkey Template to a Common Device Configuration, on page 451

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select the phone device to add the softkey template.

Step 3 From the **Common Device Configuration** drop-down list, choose the common device configuration that contains the new softkey template.

Step 4 Click **Save**.

Step 5 Click **Reset** to update the phone settings.

Associate a Softkey Template with a Phone

Optional. Use this procedure as an alternative to associating the softkey template with the Common Device Configuration. This procedure also works in conjunction with the Common Device Configuration. You can use it when you need to assign a softkey template that overrides the assignment in the Common Device Configuration or any other default softkey assignment.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** to select the phone to add the softkey template.

Step 3 From the **Softkey Template** drop-down list, choose the template that contains the new softkey.

Step 4 Click **Save**.

Step 5 Press **Reset** to update the phone settings.

Configure Malicious Call Identification Button

The procedures in this section describe how to configure the Malicious Call Identification button.

Before you begin

Configure Malicious Call ID Alarms, on page 449

Procedure

	Command or Action	Purpose
Step 1	Configure Malicious Call ID Phone Button Template, on page 453.	Perform this step to assign Malicious Call Identification button features to line or speed dial keys.
Step 2	Associate a Button Template with a Phone , on page 453	Perform this step to configure the Malicious Call Identification button for a phone.

Configure Malicious Call ID Phone Button Template

Before you begin

Configure Malicious Call ID Alarms, on page 449

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Phone Button Template**.

Step 2 Click **Find** to display list of supported phone templates.

Step 3 Perform the following steps if you want to create a new phone button template; otherwise, proceed to the next step.

a) Select a default template for the model of phone and click **Copy**.
b) In the **Phone Button Template Information** field, enter a new name for the template.
c) Click **Save**.

Step 4 Perform the following steps if you want to add phone buttons to an existing template.

a) Click **Find** and enter the search criteria.
b) Choose an existing template.

Step 5 From the **Line** drop-down list, choose feature that you want to add to the template.

Step 6 Click **Save**.

Step 7 Perform one of the following tasks:

- Click **Apply Config** if you modified a template that is already associated with devices to restart the devices.
- If you created a new softkey template, associate the template with the devices and then restart them.

Associate a Button Template with a Phone

Before you begin

Configure Malicious Call ID Phone Button Template, on page 453

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** to display the list of configured phones.

Step 3 Choose the phone to which you want to add the phone button template.

Step 4 In the **Phone Button Template** drop-down list, choose the phone button template that contains the new feature button.

Step 5 Click **Save**.
A dialog box is displayed with a message to press **Reset** to update the phone settings.

Malicious Call Identification Interactions and Restrictions

Malicious Call Identification Interactions

Table 43: Malicious Call Identification Interactions

Feature	Interaction
Conference Calls	When a user is connected to a conference, the user can use the MCID feature to flag the call as a malicious call. Cisco Unified Communications Manager sends the MCID indication to the user, generates the alarm, and updates the CDR. However, Cisco Unified Communications Manager does not send an MCID invoke message to the connected network that might be involved in the conference.
Extension Mobility	Extension Mobility users can have the MCID softkey as part of their user device profile and can use this feature when they are logged on to a phone.
Call Detail Records	To track malicious calls by using CDR, you must set the **CDR Enabled Flag** to **True** in the Cisco CallManager service parameter. When the MCID feature is used during a call, the CDR for the call contains **CallFlag=MALICIOUS** in the Comment field.

Feature	Interaction
Alarms	To record alarms for the MCID feature in the Local Syslogs, you must configure alarms in Cisco Unified Serviceability. Under **Local Syslogs**, enable alarms for the **Informational** alarm event level. When the MCID feature is used during a call, the system logs an SDL trace and a Cisco Unified Communications Manager trace in alarms. You can view the **Alarm Event Log** by using Cisco Unified Serviceability. The traces provide the following information: • Date and time • Type of event: Information • Information: The Malicious Call Identification feature is invoked in Cisco Unified Communications Manager • Called Party Number • Called Device Name • Called Display Name • Calling Party Number • Calling Device Name • Calling Display Name • Application ID • Cluster ID • Node ID For more information about alarms and traces, see the *Cisco Unified Serviceability Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.
Cisco ATA 186 analog phone ports	The Cisco ATA 186 analog phone ports support MCID by using the feature code (*39).

Malicious Call Identification Restrictions

Table 44: Malicious Call Identification Restrictions

Feature	Restriction
Malicious Call Identification Terminating (MCID-T) function	Cisco Unified Communications Manager supports only the malicious call identification originating function (MCID-O). Cisco Unified Communications Manager does not support the malicious call identification terminating function (MCID-T). If Cisco Unified Communications Manager receives a notification from the network of a malicious call identification, Cisco Unified Communications Manager ignores the notification.

Feature	Restriction
Intercluster trunks	MCID does not work across intercluster trunks because Cisco Unified Communications Manager does not support the MCID-T function.
Cisco MGCP FXS gateways	Cisco MGCP FXS gateways do not support MCID. No mechanism exists for accepting the hookflash and collecting the feature code in MGCP.
QSIG trunks	MCID does not work over QSIG trunks because MCID is not a QSIG standard.
Cisco VG248 Analog Phone Gateway	Cisco VG248 Analog Phone Gateway does not support MCID.
SIP trunks	MCID does not support SIP trunks.
Immediate Divert	System does not support using MCID and Immediate Divert features together.

Malicious Call ID Troubleshooting

To track and troubleshoot Malicious Call ID, you can use Cisco Unified Communications Manager SDL traces and alarms. For information about setting traps and traces for MCID, see the *Cisco Unified Serviceability Administration Guide*. For information about how to generate reports for MCID, see the *Cisco Unified CDR Analysis and Reporting Administration Guide*.

CHAPTER 32

Call Transfer

Call Transfer Overview

The transfer feature allows you to redirect a connected call from your phone to another number. After call transfer, your call is disconnected and the transferred call is established as a new call connection.

Following are the different types of call transfers:

- **Consult Transfer and Blind Transfer**—In Consult Transfer, a transferring phone user can redirect the caller to a different target address, after consulting with the target phone user that answers the call. That is, the transferring phone user will stay on the call until the target phone user answers the call. In Blind Transfer, the transferring phone user connects the caller to a destination line before the target of the transfer answers the call.

  Most phones use hard keys or softkeys for Transfer. Both Consult Transfer and Blind Transfer do not require separate configuration. The difference between the two types of transfer depends on when the transferring party presses the **Transfer** button a second time. For a consult transfer, the transferring party presses the **Transfer** button after the target answers, while for a Blind Transfer, the transferring party presses the **Transfer** button before the target answers.

  For SCCP-initiated blind transfers, Cisco Unified Communications Manager provides call progress indications in the form of ring-back to the transferred user.

- **Transfer On-Hook**—In this type of call transfer, the user presses the **Transfer** softkey, dials the number to which the call will be transferred, and then presses the **Transfer** softkey again, or simply goes on-hook to complete the transfer operation. You must set the **Transfer On-Hook** service parameter to **True**. This service parameter determines whether a call transfer is completed as a result of the user going on-hook after initiating a transfer operation.

  Both Consult Transfer and Blind Transfer use the Transfer On-Hook option.

- **Direct Transfer**—This type of transfer allows a user to join two established calls (the two calls can either be on hold or in the connected state) into one call and then drop the initiator from the transfer. Direct Transfer does not initiate a consultation call and does not put the active call on hold. The user uses the **DirTrfr** softkey to join any two established calls and remove the initiator.

Call Transfer Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure Consult and Blind Transfer, on page 458	Transfer allows you to redirect a single call to a new number with or without consulting the transfer recipient. Perform this step to configure Trnsfer as a softkey and/or button.
Step 2	Configure Transfer On-Hook, on page 463	(Optional) Transfer On-Hook is an option to complete call transfers. Press Trnsfer, dial the number to which the call should be transferred to, and go on-hook to complete the transfer. Perform this step to configure the service parameter.
Step 3	Configure Direct Transfer, on page 463	(Optional) Direct Transfer allows you to transfer two calls to each other (without you remaining on the line). Perform this step to configure DirTrfr as a softkey and/or button.

Configure Consult and Blind Transfer

Complete one of the task flows depending on whether your phone supports softkey or buttons.

Procedure

	Command or Action	Purpose
Step 1	Configure a Softkey Template for Transfer, on page 458	
Step 2	Configure Transfer Button, on page 461	

Configure a Softkey Template for Transfer

Trnsfer softkey is used for consult and blind transfer of a call. The trnsfer sofkey has the following call states:

- connected
- on hold

Use this procedure to make the Trnsfer softkey available:

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Softkey Template**.

Step 2 Perform the following steps to create a new softkey template; otherwise, proceed to the next step.

a) Click **Add New**.
b) Select a default template and click **Copy**.
c) Enter a new name for the template in the **Softkey Template Name** field.
d) Click **Save**.

Step 3 Perform the following steps to add softkeys to an existing template.

a) Click **Find** and enter the search criteria.
b) Select the required existing template.

Step 4 Check the **Default Softkey Template** check box to designate this softkey template as the default softkey template.

Note If you designate a softkey template as the default softkey template, you cannot delete it unless you first remove the default designation.

Step 5 Choose **Configure Softkey Layout** from the **Related Links** drop-down list in the upper right corner and click **Go**.

Step 6 From the **Select a Call State to Configure** drop-down list, choose the call state for which you want the softkey to display.

Step 7 From the **Unselected Softkeys** list, choose the softkey to add and click the right arrow to move the softkey to the **Selected Softkeys** list. Use the up and down arrows to change the position of the new softkey.

Step 8 Repeat the previous step to display the softkey in additional call states.

Step 9 Click **Save**.

Step 10 Perform one of the following tasks:

- Click **Apply Config** if you modified a template that is already associated with devices to restart the devices.
- If you created a new softkey template, associate the template with the devices and then restart them. For more information, see *Add a Softkey Template to a Common Device Configuration* and *Associate a Softkey Template with a Phone* sections.

What to do next

Perform one the following procedures:

- Associate Transfer Softkey Template with a Common Device Configuration, on page 459
- Associate Transfer Softkey Template with a Phone, on page 461

Associate Transfer Softkey Template with a Common Device Configuration

Optional. There are two ways to associate a softkey template with a phone:

- Add the softkey template to the **Phone Configuration**.
- Add the softkey template to the **Common Device Configuration**.

The procedures in this section describe how to associate the softkey template with a **Common Device Configuration**. Follow these procedures if your system uses a **Common Device Configuration** to apply

configuration options to phones. This is the most commonly used method for making a softkey template available to phones.

To use the alternative method, see Associate Transfer Softkey Template with a Phone, on page 461.

Before you begin

Configure a Softkey Template for Transfer, on page 458

Procedure

	Command or Action	Purpose
Step 1	Add Transfer Softkey Template to the Common Device Configuration, on page 460	Perform this step to add Trnsfer softkey template to the Common Device Configuration.
Step 2	Associate a Common Device Configuration with a Phone, on page 461	Perform this step to link the Trnsfer softkey Common Device Configuration to a phone.

What to do next

Configure Transfer Button, on page 461

Add Transfer Softkey Template to the Common Device Configuration

Before you begin

Configure a Softkey Template for Transfer, on page 458

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Common Device Configuration**.

Step 2 Perform the following steps to create a new Common Device Configuration and associate the softkey template with it; otherwise, proceed to the next step.

a) Click **Add New**.
b) Enter a name for the Common Device Configuration in the **Name** field.
c) Click **Save**.

Step 3 Perform the following steps to add the softkey template to an existing Common Device Configuration.

a) Click **Find** and enter the search criteria.
b) Click an existing Common Device Configuration.

Step 4 In the **Softkey Template** drop-down list, choose the softkey template that contains the softkey that you want to make available.

Step 5 Click **Save**.

Step 6 Perform one of the following tasks:

- If you modified a Common Device Configuration that is already associated with devices, click **Apply Config** to restart the devices.

- If you created a new Common Device Configuration, associate the configuration with devices and then restart them.

Associate a Common Device Configuration with a Phone

Before you begin

Add Transfer Softkey Template to the Common Device Configuration, on page 460

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select the phone device to add the softkey template.

Step 3 From the **Common Device Configuration** drop-down list, choose the common device configuration that contains the new softkey template.

Step 4 Click **Save**.

Step 5 Click **Reset** to update the phone settings.

Associate Transfer Softkey Template with a Phone

Optional. Use this procedure as an alternative to associating the softkey template with the Common Device Configuration. This procedure also works in conjunction with the Common Device Configuration. You can use it when you need to assign a softkey template that overrides the assignment in the Common Device Configuration or any other default softkey assignment.

Before you begin

Configure a Softkey Template for Transfer, on page 458

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** to select the phone to add the softkey template.

Step 3 From the **Softkey Template** drop-down list, choose the template that contains the new softkey.

Step 4 Click **Save**.

Step 5 Press **Reset** to update the phone settings.

Configure Transfer Button

The procedures in this section describe how to configure the Transfer button.

Procedure

	Command or Action	Purpose
Step 1	Configure a Phone Button Template for Transfer, on page 462	Perform this step to assign Transfer button features to line or speed dial keys.
Step 2	Associate Transfer Button Template with a Phone, on page 462	Perform this step to configure the Transfer button for a phone.

Configure a Phone Button Template for Transfer

Optional. Follow this procedure when you want to assign features to line or speed dial keys.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Phone Button Template**.

Step 2 Click **Find** to display list of supported phone templates.

Step 3 Perform the following steps if you want to create a new phone button template; otherwise, proceed to the next step.

a) Select a default template for the model of phone and click **Copy**.
b) In the **Phone Button Template Information** field, enter a new name for the template.
c) Click **Save**.

Step 4 Perform the following steps if you want to add phone buttons to an existing template.

a) Click **Find** and enter the search criteria.
b) Choose an existing template.

Step 5 From the **Line** drop-down list, choose feature that you want to add to the template.

Step 6 Click **Save**.

Step 7 Perform one of the following tasks:

- Click **Apply Config** if you modified a template that is already associated with devices to restart the devices.
- If you created a new softkey template, associate the template with the devices and then restart them.

Associate Transfer Button Template with a Phone

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** to display the list of configured phones.

Step 3 Choose the phone to which you want to add the phone button template.

Step 4 In the **Phone Button Template** drop-down list, choose the phone button template that contains the new feature button.

Step 5 Click **Save**.

A dialog box is displayed with a message to press **Reset** to update the phone settings.

Configure Transfer On-Hook

Before you begin

Configure Consult and Blind Transfer, on page 458

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Service Parameters**.
The **Service Parameter Configuration** window is displayed.

Step 2 From the **Server** drop-down list, choose the server on which you want to configure the parameter.

Step 3 From the **Service** drop-down list, choose the **Cisco CallManager (Active)** service.

Step 4 In the **Clusterwide Parameters (Device - Phone)**, choose **True** for the **Transfer On-Hook Enabled** service parameter.

Step 5 Click **Save**.

Configure Direct Transfer

Complete one of the task flows depending on whether your phone supports softkey or buttons.

Procedure

	Command or Action	Purpose
Step 1	Configure a Softkey Template for Direct Transfer, on page 463	Perform this step to add Direct Transfer softkey to template and configure the softkey using the Common Device Configuration or phone.
Step 2	Configure Direct Transfer Button, on page 466	Perform this step to add and configure the Direct Transfer button to a phone.

Configure a Softkey Template for Direct Transfer

Direct Transfer softkey has the following call states:

- Connected
- On hold

Use this procedure to make the Direct Transfer softkey available:

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Softkey Template**.

Step 2 Perform the following steps to create a new softkey template; otherwise, proceed to the next step.

a) Click **Add New**.
b) Select a default template and click **Copy**.
c) Enter a new name for the template in the **Softkey Template Name** field.
d) Click **Save**.

Step 3 Perform the following steps to add softkeys to an existing template.

a) Click **Find** and enter the search criteria.
b) Select the required existing template.

Step 4 Check the **Default Softkey Template** check box to designate this softkey template as the default softkey template.

Note If you designate a softkey template as the default softkey template, you cannot delete it unless you first remove the default designation.

Step 5 Choose **Configure Softkey Layout** from the **Related Links** drop-down list in the upper right corner and click **Go**.

Step 6 From the **Select a Call State to Configure** drop-down list, choose the call state for which you want the softkey to display.

Step 7 From the **Unselected Softkeys** list, choose the softkey to add and click the right arrow to move the softkey to the **Selected Softkeys** list. Use the up and down arrows to change the position of the new softkey.

Step 8 Repeat the previous step to display the softkey in additional call states.

Step 9 Click **Save**.

Step 10 Perform one of the following tasks:

- Click **Apply Config** if you modified a template that is already associated with devices to restart the devices.
- If you created a new softkey template, associate the template with the devices and then restart them. For more information, see *Add a Softkey Template to a Common Device Configuration* and *Associate a Softkey Template with a Phone* sections.

What to do next

Perform one the following procedures:

- Associate Direct Transfer Softkey Template with a Common Device Configuration, on page 464
- Associate Direct Transfer Softkey Template with a Phone, on page 466

Associate Direct Transfer Softkey Template with a Common Device Configuration

Optional. There are two ways to associate a softkey template with a phone:

- Add the softkey template to the **Phone Configuration**.

- Add the softkey template to the **Common Device Configuration**.

The procedures in this section describe how to associate the softkey template with a **Common Device Configuration**. Follow these procedures if your system uses a **Common Device Configuration** to apply configuration options to phones. This is the most commonly used method for making a softkey template available to phones.

To use the alternative method, see Associate Direct Transfer Softkey Template with a Phone, on page 466

Before you begin

Configure a Softkey Template for Direct Transfer, on page 463

Procedure

	Command or Action	Purpose
Step 1	Add Direct Transfer Softkey Template to the Common Device Configuration, on page 465	Perform this step to add Direct Transfer softkey template to the Common Device Configuration.
Step 2	Associate a Common Device Configuration with a Phone, on page 466	Perform this step to add Direct Transfer softkey template to the Common Device Configuration.

Add Direct Transfer Softkey Template to the Common Device Configuration

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Common Device Configuration**.

Step 2 Perform the following steps to create a new Common Device Configuration and associate the softkey template with it; otherwise, proceed to the next step.

a) Click **Add New**.
b) Enter a name for the Common Device Configuration in the **Name** field.
c) Click **Save**.

Step 3 Perform the following steps to add the softkey template to an existing Common Device Configuration.

a) Click **Find** and enter the search criteria.
b) Click an existing Common Device Configuration.

Step 4 In the **Softkey Template** drop-down list, choose the softkey template that contains the softkey that you want to make available.

Step 5 Click **Save**.

Step 6 Perform one of the following tasks:

- If you modified a Common Device Configuration that is already associated with devices, click **Apply Config** to restart the devices.
- If you created a new Common Device Configuration, associate the configuration with devices and then restart them.

Associate a Common Device Configuration with a Phone

Before you begin

Add Direct Transfer Softkey Template to the Common Device Configuration, on page 465

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select the phone device to add the softkey template.

Step 3 From the **Common Device Configuration** drop-down list, choose the common device configuration that contains the new softkey template.

Step 4 Click **Save**.

Step 5 Click **Reset** to update the phone settings.

Associate Direct Transfer Softkey Template with a Phone

Optional. Use this procedure as an alternative to associating the softkey template with the Common Device Configuration. This procedure also works in conjunction with the Common Device Configuration. You can use it when you need to assign a softkey template that overrides the assignment in the Common Device Configuration or any other default softkey assignment.

Before you begin

Configure a Softkey Template for Direct Transfer, on page 463

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** to select the phone to add the softkey template.

Step 3 From the **Softkey Template** drop-down list, choose the template that contains the new softkey.

Step 4 Click **Save**.

Step 5 Press **Reset** to update the phone settings.

Configure Direct Transfer Button

The procedures in this section describe how to configure the Direct Transfer button.

Procedure

	Command or Action	Purpose
Step 1	Configure Phone Button Template for Direct Transfer, on page 467	Perform this step to assign Direct Transfer button features to line or speed dial keys.

	Command or Action	Purpose
Step 2	Associate Direct Transfer Button Template with a Phone, on page 467	Perform this step to configure the Direct Transfer button for a phone.

Configure Phone Button Template for Direct Transfer

Optional. Follow this procedure when you want to assign features to line or speed dial keys.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Phone Button Template**.

Step 2 Click **Find** to display list of supported phone templates.

Step 3 Perform the following steps if you want to create a new phone button template; otherwise, proceed to the next step.

a) Select a default template for the model of phone and click **Copy**.
b) In the **Phone Button Template Information** field, enter a new name for the template.
c) Click **Save**.

Step 4 Perform the following steps if you want to add phone buttons to an existing template.

a) Click **Find** and enter the search criteria.
b) Choose an existing template.

Step 5 From the **Line** drop-down list, choose feature that you want to add to the template.

Step 6 Click **Save**.

Step 7 Perform one of the following tasks:

- Click **Apply Config** if you modified a template that is already associated with devices to restart the devices.
- If you created a new softkey template, associate the template with the devices and then restart them.

Associate Direct Transfer Button Template with a Phone

Before you begin

Configure Phone Button Template for Direct Transfer, on page 467

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** to display the list of configured phones.

Step 3 Choose the phone to which you want to add the phone button template.

Step 4 In the **Phone Button Template** drop-down list, choose the phone button template that contains the new feature button.

Step 5 Click **Save**.

A dialog box is displayed with a message to press **Reset** to update the phone settings.

Call Transfer Interactions and Restrictions

Call Transfer Interactions

Feature	Interaction
Logical Partitioning	The logical partitioning policy check is performed between the geolocation identifier of the device that is acting as a transferred party and the geolocation identifier of the device that is acting as a transferred destination. Logical partitioning handling takes place in the following circumstances: • When a phone user uses Transfer softkey to transfer the call, the second press of the softkey invokes and processes the Call Transfer feature. • When other transfer mechanisms, such as Direct Transfer, On-Hook Transfer, Hook Flash Transfer, and CTI-application-initiated Transfer results in invoking the Call Transfer feature. • When the transferred and the transferred destination specifies a PSTN participant. • When Cisco Unified Communications Manager uses the geolocation identifier information that associates with the transferred and transferred destination device to perform logical partitioning policy checking. • Before splitting of the primary and secondary calls, and before joining. Logical partitioning handles a denied call as follows: • Sends External Transfer Restricted message to the VoIP phone. • Normal Transfer—For a phone that is running SCCP, the primary call remains on hold, and the consultation call remains active. For a phone that is running SIP, both primary and consultation calls remain on hold and must be resumed manually after the failure. • On-Hook, Hook-Flash and Analog-Phone-Initiated Transfer—Both the primary and secondary calls are cleared by using the cause code=63 “Service or option not available” with a reorder tone from Cisco Unified Communications Manager. • The Number of Transfer Failures perfmon counter is incremented.

Feature	Interaction
Multilevel Precedence and Preemption (MLPP)	When a switch initiates a call transfer between two segments that have the same precedence level, the segments maintain the precedence level upon transfer. When a call transfer is made between call segments that are at different precedence levels, the switch that initiates the transfer marks the connection at the segment that has the higher precedence level. Cisco Unified Communications Manager supports this requirement by upgrading the precedence level of a call leg that is involved in a Call Transfer operation. For example, party A calls party B with Priority precedence level. Party B then initiates a transfer to party C and dials the Flash precedence digits when dialing. When the transfer is complete, the precedence level of party A gets upgraded from Priority to Flash. The Call Transfer feature is enabled automatically when MLPP is enabled, and the phones support the Transfer softkey. **Note** The precedence level upgrade does not work over a trunk device such as an intercluster trunk (ICT) or a PRI trunk.

Call Transfer Restrictions

Feature	Restriction
Logical Partitioning	Logical partitioning handling does not take place when both the transferred and the transferred destination devices are VoIP phones. Logical partitioning handling does not take place when geolocation or a geolocation filter is not associated with any device.
External Call Transfer Restrictions	To restrict transfer for external call scenarios, see the “External Call Transfer Restrictions” chapter.
Hunt Pilot	If a call transfer to a hunt pilot is initiated when an announcement is in progress, the call is redirected only after the announcement is complete.

CHAPTER 33

External Call Transfer Restrictions

External Call Transfer Restrictions Overview

External Call Transfer Restrictions is a feature that you can use to configure gateways, trunks, and route patterns as OnNet (internal) or OffNet (external) devices at the system level. By setting the devices as OffNet, you can restrict the transferring of an external call to an external device and thus help prevent toll fraud.

If you try to transfer a call on an OffNet gateway or trunk when the service parameter Block OffNet to OffNet Transfer is set to True, a message displays on the user phone to indicate that the call cannot be transferred.

This chapter uses the following terms:

Term	Description
OnNet Device	A device that is configured as OnNet and considered to be internal to the network.
OffNet Device	A device that is considered as OffNet and, when routed, is considered to be external to the network.
Network Location	The location of the device, which is considered as OnNet or OffNet, with respect to the network.
Originating End	The device that gets transferred. The system considers this device as OnNet or OffNet.
Terminating End	The device that receives the transferred call. The system considers this device as OnNet or OffNet.
Incoming Call	A call for which only gateways and trunks call classification settings get used to classify it as OnNet or OffNet. Route Pattern call classification settings do not apply.

Term	Description
Outgoing Call	A call for which the call classification setting of the trunk, gateway, and route pattern gets considered. The Allow Device Override setting on the route pattern determines whether the trunk or gateway call classification setting gets used instead of the route pattern call classification setting.

Configure External Call Transfer Restrictions Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure the Service Parameter for Call Transfer Restrictions, on page 472	Block external calls from being transferred to another external device or number.
Step 2	To configure incoming calls perform the following procedures: • Configure the Clusterwide Service Parameter, on page 473 • Configure Gateways for Call Transfer Restrictions, on page 474 • Configure Trunks for Call Transfer Restrictions, on page 474	Configure gateways and trunks as OnNet (internal) or OffNet (external) by using Gateway Configuration or Trunk Configuration or by setting a clusterwide service parameter.
Step 3	Configure Outgoing Calls, on page 475	Configure transfer capabilities with route pattern configuration.

Configure the Service Parameter for Call Transfer Restrictions

To block external calls from being transferred to another external device or number:

Procedure

Step 1 From the Cisco Unified CM Administration user interface choose **System** > **Service Parameters**.

Step 2 On the Service Parameter Configuration window choose the Cisco Unified CM server you want to configure from the Server drop-down list.

Step 3 Choose **Cisco CallManager (Active)** from the Service drop-down list.

Step 4 Choose **True** from the Block OffNet to OffNet Transfer drop-down list. The default value specifies False.

Step 5 Click **Save**.

Configure Incoming Calls Task Flow

Procedure

	Command or Action	Purpose
Step 1	(Optional) Configure the Clusterwide Service Parameter, on page 473	Configure all gateways or trunks in the Cisco Unified Communications Manager cluster to be OffNet (external) or OnNet (internal).
Step 2	Configure Gateways for Call Transfer Restrictions, on page 474	Configure gateways as OnNet (internal) or OffNet (external) by using Gateway Configuration. When the feature is used in conjunction with the clusterwide service parameter Block OffNet to OffNet Transfer, the configuration determines whether calls can transfer over a gateway. You can configure the following devices as internal and external to Cisco Unified Communications Manager: • H.323 gateway • MGCP FXO trunk • MGCP T1/E1 trunk
Step 3	Configure Trunks for Call Transfer Restrictions, on page 474	Configure trunks as OnNet (internal) or OffNet (external) by using Trunk Configuration. When the feature is used in conjunction with the clusterwide service parameter Block OffNet to OffNet Transfer, the configuration determines whether calls can transfer over a trunk. You can configure the following devices as internal and external to Cisco Unified Communications Manager: • Intercluster trunk • SIP trunk

Configure the Clusterwide Service Parameter

To configure all gateways or trunks in the Cisco Unified Communications Manager cluster to be OffNet (external) or OnNet (internal), perform the following steps:

Before you begin

Configure the Service Parameter for Call Transfer Restrictions, on page 472

Procedure

Step 1 From the Cisco Unified CM Administration user interface choose **System** > **Service Parameters**.

Step 2 On the Service Parameter Configuration window choose the Cisco Unified CM server you want to configure from the Server drop-down list.

Step 3 Choose **Cisco CallManager (Active)** from the Service drop-down list.

Step 4 Choose either OffNet or OnNet (the default specifies OffNet) from the Call Classification drop-down list.

Configure Gateways for Call Transfer Restrictions

To configure the gateway as OffNet, OnNet, or Use System Default, perform the following procedure. The system considers calls that come to the network through that gateway as OffNet or OnNet, respectively.

Before you begin

Configure the Clusterwide Service Parameter, on page 473

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Gateway**.

The Find and List Gateways window displays.

Step 2 To list the configured gateways, click **Find**.

The gateways that are configured in Unified Communications Manager display.

Step 3 Choose the gateway that you want to configure as OffNet or OnNet.

Step 4 In the Call Classification field choose OffNet or OnNet. If you have enabled clusterwide restrictions an all gateways, configure each gateway to Use System Default (this reads the setting in the Call Classification service parameter and uses that setting for the gateway).

Step 5 Click **Save**.

Configure Trunks for Call Transfer Restrictions

To configure the trunk as OffNet, OnNet, or Use System Default, perform the following procedure. The system considers calls that come to the network through that trunk as OffNet or OnNet, respectively.

Before you begin

Configure Gateways for Call Transfer Restrictions, on page 474

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Trunk.**

The Find and List Trunk window displays.

Step 2 To list the configured trunks, click **Find.**

The trunks that are configured in Unified Communications Manager display.

Step 3 Choose the trunk that you want to configure as OffNet or OnNet.

Step 4 From the Call Classification drop-down list, choose one of the following fields:

- **OffNet -** When you choose this field, this identifies the gateway as an external gateway. When a call comes in from a gateway that is configured as OffNet, the system sends the outside ring to the destination device.
- **OnNet -** When you choose this field, this identifies the gateway as an internal gateway. When a call comes in from a gateway that is configured as OnNet, the system sends the inside ring to the destination device.
- **Use System Default -** When you choose this field, this uses the Unified Communications Manager clusterwide service parameter Call Classification.

Note If you have enabled clusterwide restrictions an all trunks, configure each trunk to Use System Default (this reads the setting in the Call Classification service parameter and uses that setting for the trunk)

Step 5 Click **Save.**

Configure Outgoing Calls

To classify a call as OnNet or OffNet, administrators can set the **Call Classification** field to OnNet or OffNet, respectively, on the **Route Pattern Configuration** window. Administrators can override the route pattern setting and use the trunk or gateway setting by checking the **Allow Device Override** check box on the **Route Pattern Configuration** window.

Before you begin

Configure Trunks for Call Transfer Restrictions, on page 474

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Route/Hunt** > **Route Pattern** and click **Find** to list all route patterns.

Step 2 Choose the route pattern you want to configure, or click **Add New**.

Step 3 In the **Route Pattern Configuration** window, use the following fields to configure transfer capabilities with route pattern configuration:

a) **Call Classification**—Use this drop-down list to classify the call that uses this route Pattern as OffNet or OnNet.

b) **Provide Outside Dial Tone**—If Call Classification is set to OffNet, this check box gets checked.

c) **Allow Device Override**—When this check box is checked, the system uses the Call Classification setting of the trunk or gateway that is associated with the route pattern instead of the Call Classification setting on the Route Pattern Configuration window.

Step 4 Click **Save**.

External Call Transfer Interactions and Restrictions

External Call Transfer Restrictions Interactions

Feature	Interaction
Drop Conference	The Drop Conference feature determines whether an existing ad hoc conference should be dropped by checking whether the conference parties are configured as OffNet or OnNet. You use the service parameter Drop Ad Hoc Conference and choose the option When No OnNet Parties Remain in the Conference to configure the feature. You determine OnNet status for each party by checking the device or route pattern that the party is using. For more information, see topics related to Ad Hoc Conference linking in the "Ad Hoc Conferencing" chapter.
Bulk Administration	Bulk Administration inserts gateway configuration (OffNet or OnNet) on the Gateway Template. For more information, see the *Cisco Unified Communications Manager Bulk Administration Guide*.
Dialed Number Analyzer (DNA)	When used to perform digit analysis on a gateway, DNA displays the Call Classification that is configured for the gateway and the route pattern. For more information, see the *Cisco Unified Communications Manager Dialed Number Analyzer Guide*.

External Call Transfer Restrictions Restrictions

Restriction	Description
FXS Gateways	FXS gateways such as Cisco Catalyst 6000 24 Port do not have a Call Classification field on the Gateway Configuration window; therefore, the system always considers them as OnNet.
Cisco VG248 Gateway	The system does not support the Cisco VG248 Gateway which does not have a Call Classification field.

Restriction	Description
FXS Ports	Cisco Unified Communications Manager considers all Cisco Unified IP Phones and FXS ports as OnNet (internal) that cannot be configured as OffNet (external).

PART X

Presence and Privacy Features

CHAPTER 34

Barge

Barge Overview

Barge allows a user to be added to a remotely active call that is on a shared line. Remotely active calls for a line are the active (connected) calls that are made to or from another device that shares a directory number with the line.

If you configure party entrance tone, a tone plays on the phone when a basic call changes to a barged call or cbarged call. In addition, a different tone plays when a party leaves the multiparty call.

Phones support Barge in the following conference modes:

- Built-in conference bridge at the phone that is barged—This mode uses the Barge softkey. Most Cisco Unified IP Phones include the built-in conference bridge capability.
- Shared conference bridge—This mode uses the cBarge softkey.

By pressing the Barge or cBarge softkey in the remote-in-use call state, the user is added to the call with all parties, and all parties receive a barge beep tone (if configured). If Barge fails, the original call remains active. If no conference bridge is available (built-in or shared), the barge request gets rejected, and a message displays on the Barge initiator device. When network or Unified Communications Manager failure occurs, the Barge call is preserved.

Note To display the softkey option for both Barge and cBarge, disable the **Privacy** option in Unified Communications Manager user interface for those devices that have shared line appearances.

For a list of Cisco Unified IP Phones that support Barge, log in to Cisco Unified Reporting and run the Unified CM Phone Feature List report. Make sure to select Built In Bridge as the feature. For details, see Generate a Phone Feature List, on page 3.

Single-Button Barge and Single-Button cBarge

The Single-Button Barge and Single-Button cBarge features allow a user to press the shared-line button of the remotely active call, to be added to the call. All parties receive a barge beep tone (if configured). If barge fails, the original call remains active.

Phones support Single-Button Barge and Single-Button cBarge in two conference modes:

- Built-in conference bridge at the phone that is barged—This mode uses the Single-Button Barge feature.
- Shared conference bridge—This mode uses the Single-Button cBarge feature.

By pressing the shared-line button of the remote-in-use call, the user is added to the call with all parties, and all parties receive a barge beep tone (if configured). If barge fails, the original call remains active. If no conference bridge is available (built-in or shared), the barge request gets rejected, and a message is displayed at the Barge initiator device.

Built-In Conference

When the user presses the Barge softkey or a shared-line button, a Barge call is set up by using the built-in conference bridge, if available. A built-in conference bridge is advantageous because neither a media interruption nor display changes to the original call occur when the Barge is being set up.

Shared Conference

When the user presses the cBarge softkey, or a shared-line button, a barge call is set up by using the shared conference bridge, if available. The original call is split and then joined at the conference bridge, which causes a brief media interruption. The call information for all parties changes to “Barge”. The barged call becomes a conference call with the barge target device as the conference controller. It can add more parties to the conference or can drop any party. When any party releases the call, the remaining two parties experience a brief interruption and then get reconnected as a point-to-point call, which releases the shared conference resource.

Built-In and Shared Conference Differences

This table describes the differences between barge with built-in conference bridge and shared conference.

Feature	Barge with Built-In Conference	Barge with Shared Conference
The standard softkey template includes the Barge/cBarge softkey. **Note** If the single button Barge/cBarge feature is enabled, the softkey is not used.	Yes	No
A media break occurs during barge setup.	No	Yes
If configured, a user receives a barge setup tone.	Yes	Yes

Feature	Barge with Built-In Conference	Barge with Shared Conference
Text displays at the barge initiator phone.	To barge XXX	To Conference
Text displays at the target phone.	To/From Other	To Conference
Text displays at the other phones.	To/From Target	To Conference
Bridge supports a second barge setup to an already barged call.	No	Yes
Initiator releases the call.	No media interruption occurs for the two original parties.	Media break occurs to release the shared conference bridge when only two parties remain and to reconnect the remaining parties as a point-to-point call.
Target releases the call.	Media break occurs to reconnect initiator with the other party as a point-to-point call.	Media break occurs to release the shared conference bridge when only two parties remain and to reconnect the remaining parties as a point-to-point call.
Other party releases the call.	All three parties get released.	Media break occurs to release the shared conference bridge when only two parties remain and to reconnect the remaining parties as a point-to-point call.
Target puts call on hold and performs Direct Transfer, Join, or Call Park.	Initiator gets released.	Initiator and the other party remain connected.

Barge Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure Softkey Template for Built-In Conferencing, on page 484	Add the Barge softkey to a softkey template. Follow this procedure when you are configuring barge for built-in conference bridges.
Step 2	Configure Softkey Template for Shared Conferencing, on page 485	Add the cBarge softkey to a softkey template. Follow this procedure when you are configuring barge for shared conference bridges.
Step 3	To Associate a Softkey Template with Common Device Configuration, on page 486, complete the following subtasks:	Optional. To make the softkey template available to phones, you must complete either this step or the following step. Follow this step

	Command or Action	Purpose
	• Add a Softkey Template to Common Device Configuration, on page 487 • Associate Common Device Configuration with Phone, on page 488	if your system uses a Common Device Configuration to apply configuration options to phones. This is the most commonly used method for making a softkey template available to phones.
Step 4	Associate Softkey Template with Phone, on page 486	Optional. Use this procedure either as an alternative to associating the softkey template with the Common Device Configuration, or in conjunction with the Common Device Configuration. Use this procedure in conjunction with the Common Device Configuration if you need assign a softkey template that overrides the assignment in the Common Device Configuration or any other default softkey.
Step 5	Configure Barge for Built-In Conferencing, on page 488	Configure barge for built-in conference bridges.
Step 6	Configure Barge for Shared Conferencing, on page 489	Configure barge for shared conference bridges.
Step 7	Associate User with Device, on page 54	Associate users with devices.

Configure Softkey Template for Built-In Conferencing

Configure a softkey template for Barge and assign the Barge softkey to that template. You can configure the Barge softkey in the **Remote In Use** call state.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Softkey Template**.

Step 2 Perform the following steps to create a new softkey template; otherwise, proceed to the next step.

a) Click **Add New**.
b) Select a default template and click **Copy**.
c) Enter a new name for the template in the **Softkey Template Name** field.
d) Click **Save**.

Step 3 Perform the following steps to add softkeys to an existing template.

a) Click **Find** and enter the search criteria.
b) Select the required existing template.

Step 4 Check the **Default Softkey Template** check box to designate this softkey template as the default softkey template.

Note If you designate a softkey template as the default softkey template, you cannot delete it unless you first remove the default designation.

Step 5 Choose **Configure Softkey Layout** from the **Related Links** drop-down list in the upper right corner and click **Go**.

Step 6 From the **Select a Call State to Configure** drop-down list, choose the call state for which you want the softkey to display.

Step 7 From the **Unselected Softkeys** list, choose the softkey to add and click the right arrow to move the softkey to the **Selected Softkeys** list. Use the up and down arrows to change the position of the new softkey.

Step 8 Repeat the previous step to display the softkey in additional call states.

Step 9 Click **Save**.

Step 10 Perform one of the following tasks:

- Click **Apply Config** if you modified a template that is already associated with devices to restart the devices.
- If you created a new softkey template, associate the template with the devices and then restart them. For more information, see *Add a Softkey Template to a Common Device Configuration* and *Associate a Softkey Template with a Phone* sections.

What to do next

Perform one of the following procedures:

- Add a Softkey Template to Common Device Configuration, on page 487
- Associate Common Device Configuration with Phone, on page 488

Configure Softkey Template for Shared Conferencing

Configure a softkey template for shared conferencing and assign the cBarge softkey to that template. You can configure the cBarge softkey in the **Remote In Use** call state.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Softkey Template**.

Step 2 Perform the following steps to create a new softkey template; otherwise, proceed to the next step.

a) Click **Add New**.
b) Select a default template and click **Copy**.
c) Enter a new name for the template in the **Softkey Template Name** field.
d) Click **Save**.

Step 3 Perform the following steps to add softkeys to an existing template.

a) Click **Find** and enter the search criteria.
b) Select the required existing template.

Step 4 Check the **Default Softkey Template** check box to designate this softkey template as the default softkey template.

Note If you designate a softkey template as the default softkey template, you cannot delete it unless you first remove the default designation.

Step 5 Choose **Configure Softkey Layout** from the **Related Links** drop-down list in the upper right corner and click **Go**.

Step 6 From the **Select a Call State to Configure** drop-down list, choose the call state for which you want the softkey to display.

Step 7 From the **Unselected Softkeys** list, choose the softkey to add and click the right arrow to move the softkey to the **Selected Softkeys** list. Use the up and down arrows to change the position of the new softkey.

Step 8 Repeat the previous step to display the softkey in additional call states.

Step 9 Click **Save**.

Step 10 Perform one of the following tasks:

- Click **Apply Config** if you modified a template that is already associated with devices to restart the devices.
- If you created a new softkey template, associate the template with the devices and then restart them. For more information, see *Add a Softkey Template to a Common Device Configuration* and *Associate a Softkey Template with a Phone* sections.

Associate Softkey Template with Phone

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.
The **Find and List Phones** window is displayed.

Step 2 Find the phone to which you want to add the softkey template.

Step 3 Perform one of the following tasks:

- From the **Common Device Configuration** drop-down list, choose the common device configuration that contains the required softkey template.
- In the **Softkey Template** drop-down list, choose the softkey template that contains the Barge or cBarge softkey.

Step 4 Click **Save**.
A dialog box is displayed with a message to press **Reset** to update the phone settings.

Associate a Softkey Template with Common Device Configuration

Optional. There are two ways to associate a softkey template with a phone:

- Add the softkey template to the **Phone Configuration**.
- Add the softkey template to the **Common Device Configuration**.

The procedures in this section describe how to associate the softkey template with a **Common Device Configuration**. Follow these procedures if your system uses a **Common Device Configuration** to apply

configuration options to phones. This is the most commonly used method for making a softkey template available to phones.

To use the alternative method, see Associate Softkey Template with Phone, on page 486.

Procedure

Step 1 Add a Softkey Template to Common Device Configuration, on page 350

Step 2 Associate a Common Device Configuration with a Phone, on page 351

Add a Softkey Template to Common Device Configuration

Before you begin

Perform one or both of the following as needed:

- Configure Softkey Template for Built-In Conferencing, on page 484
- Configure Softkey Template for Shared Conferencing, on page 485

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Common Device Configuration**.

Step 2 Perform the following steps to create a new Common Device Configuration and associate the softkey template with it; otherwise, proceed to the next step.

a) Click **Add New**.
b) Enter a name for the Common Device Configuration in the **Name** field.
c) Click **Save**.

Step 3 Perform the following steps to add the softkey template to an existing Common Device Configuration.

a) Click **Find** and enter the search criteria.
b) Click an existing Common Device Configuration.

Step 4 In the **Softkey Template** drop-down list, choose the softkey template that contains the softkey that you want to make available.

Step 5 Click **Save**.

Step 6 Perform one of the following tasks:

- If you modified a Common Device Configuration that is already associated with devices, click **Apply Config** to restart the devices.
- If you created a new Common Device Configuration, associate the configuration with devices and then restart them.

Associate Common Device Configuration with Phone

Before you begin

Perform one or both of the following as needed:

- Configure Softkey Template for Built-In Conferencing, on page 484
- Configure Softkey Template for Shared Conferencing, on page 485

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select the phone device to add the softkey template.

Step 3 From the **Common Device Configuration** drop-down list, choose the common device configuration that contains the new softkey template.

Step 4 Click **Save**.

Step 5 Click **Reset** to update the phone settings.

What to do next

Perform one or both of the following:

- Configure Barge for Built-In Conferencing, on page 488
- Configure Barge for Shared Conferencing, on page 489

Configure Barge for Built-In Conferencing

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Service Parameters** and set the **Built In Bridge Enable** clusterwide service parameter to **On**.

Note If this parameter is set to **Off**, configure barge for each phone by setting the **Built in Bridge** field in the **Phone Configuration** window.

Step 2 Set the **Party Entrance Tone** clusterwide service parameter to **True** (required for tones) or configure the **Party Entrance Tone** field in the **Directory Number Configuration** window.

Step 3 Set the **Single Button Barge/CBarge Policy** to **Barge**.

Note If this parameter is set to **Off**, configure single-button barge for each phone by setting the **Single Button Barge** field in the **Phone Configuration** window.

Step 4 Set the **Allow Barge When Ringing** service parameter to **True**.

Step 5 Click **Save**.

Configure Barge for Shared Conferencing

Cisco recommends that you do not configure Barge for shared conferencing (cBarge) for a user who has Barge configured. Choose only one barge method for each user.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Service Parameters** and set the **Built In Bridge Enable** clusterwide service parameter to **On**.

Note If this parameter is set to **Off**, configure cBarge for each phone by setting the **Built in Bridge** field in the **Phone Configuration** window.

Step 2 Set the **Party Entrance Tone** clusterwide service parameter to **True** (required for tones) or configure the **Party Entrance Tone** field in the **Directory Number Configuration** window.

Step 3 Set the **Single Button Barge/CBarge Policy** to **cBarge**.

Note If this parameter is set to **Off**, configure Single-button cBarge for each phone by setting the **Single Button cBarge** field in the **Phone Configuration** window.

Step 4 Set the **Allow Barge When Ringing** service parameter to True.

Step 5 Click **Save**.

Associate User with Device

Before you begin

Perform one or both of the following:

- Configure Barge for Built-In Conferencing, on page 488
- Configure Barge for Shared Conferencing, on page 489

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **End User**.

Step 2 Specify the appropriate filters in the **Find User Where** field to and then click **Find** to retrieve a list of users.

Step 3 Select the user from the list.
The **End User Configuration** window appears.

Step 4 Locate the **Device Information** section.

Step 5 Click **Device Association**.
The **User Device Association** window appears.

Step 6 Find and select the CTI remote device.

Step 7 To complete the association, click **Save Selected/Changes**.

Step 8 From **Related Links** drop-down list, choose **Back to User**, and then click **Go**.
The **End User Configuration** window appears, and the associated device that you chose appears in the **Controlled Devices** pane.

Barge Interactions and Restrictions

This section describes the interactions and restrictions for barge and privacy features.

Barge Interactions

Feature	Interaction
cBarge	Cisco recommends that you assign either the Barge or cBarge softkey to a softkey template. By having only one of these softkeys for each device, you can prevent confusion for users and avoid potential performance issues. **Note** You can enable Single-Button Barge or Single-Button cBarge for a device, but not both.
Call Park	When the target parks the call, the barge initiator gets released (if using the built-in bridge), or the barge initiator and the other party remain connected (if using the shared conference).
Join	When the target joins the call with another call, the barge initiator gets released (if using the built-in bridge), or the barge initiator and the other party remain connected (if using the shared conference).
Private Line Automatic Ringdown (PLAR)	A Barge, cBarge, or Single-Button Barge initiator can barge into a call through a shared line that is configured for Barge and Private Line Automatic Ringdown (PLAR). The initiator can barge into the call if the barge target uses the preconfigured number that is associated with the PLAR line while on the call. Cisco Unified Communications Manager does not send the barge invocation to the PLAR line before connecting the barge call, so the barge occurs regardless of the state of the PLAR destination. To make Barge, cBarge, or Single-Button Barge function with PLAR, you must configure Barge, cBarge, or Single-Button Barge. In addition, you must configure the PLAR destination, a directory number that is used specifically for PLAR.

Barge Restrictions

Restriction	Description
Additional callers	The Barge initiator cannot conference in additional callers.

Restriction	Description
Computer Telephony Interface (CTI)	CTI does not support Barge through APIs that TAPI and JTAPI applications invoke. CTI generates events for Barge when it is invoked manually from an IP phone by using the Barge or cBarge softkey.
G.711 codec	The original call requires G.711 codec. If G.711 is not available, use cBarge instead.
Cisco Unified IP Phones	You can assign a softkey template that contains the Barge softkey to any IP phone that uses softkeys; however, some IP phones do not support the Barge feature.
Encryption	If you configure encryption for Cisco Unified IP Phones 7960 and 7940, those encrypted devices cannot accept a barge request when they are participating in an encrypted call. When the call is encrypted, the barge attempt fails. A tone plays on the phone to indicate that the Barge failed.
Maximum number of calls	If the number of shared-line users in the conference is equal to or greater than the configuration for the Maximum Number of Calls setting for the device from which you are attempting to barge, the phone displays the message, `Error: Past Limit`.

Barge Troubleshooting

No Conference Bridge Available

When the Barge softkey is pressed, the message `No Conference Bridge Available` is displayed on the IP phone.

The **Built In Bridge** field in the **Phone Configuration** window for the target phone is not set properly.

To resolve the problem, perform the following steps:

1. From Cisco Unified CM Administration, choose **Device** > **Phone** and click **Find the phone** to find the phone configuration of the phone that is having the problem.
2. Set the **Built In Bridge** field to **On**.
3. Click **Update**.
4. Reset the phone.

Error: Past Limit

The phone displays the message, `Error: Past Limit`.

The number of shared-line users in the conference is equal to or greater than the configuration for the **Maximum Number of Calls** field for the device from which you are attempting to barge.

- Go to **Service Parameter Configuration** window and locate the **Clusterwide Parameters (Feature - Conference)** section. Increase the value of **Maximum Ad Hoc Conference** parameter as required.
- Check the **Maximum Number of Calls** value for the shared lines on the device from which you are attempting to barge and increase the value as required.

Error: Past Limit

CHAPTER 35

BLF Presence

BLF Presence Overview

The Busy Lamp Field (BLF) presence feature allows a user who is a watcher to monitor the real-time status of another user at a directory number or Session Initiation Protocol (SIP) uniform resource identifier (URI) from the device of the watcher.

A watcher can monitor the status of the user or BLF presence entity (also called presentity) by using the following options:

- BLF and SpeedDial buttons
- Missed call, placed call, or received call lists in the directories window
- Shared directories, such as the corporate directory

Call lists and directories display the BLF status for existing entries. When you configure BLF and SpeedDial buttons, the BLF presence entity appears as a speed dial on the device of the watcher.

To view the status of a BLF presence entity, watchers send BLF presence requests to Cisco Unified Communications Manager. After administrators configure BLF presence features, real-time status icons appear on the watcher device to indicate whether the BLF presence entity is on the phone, is not on the phone, the status is unknown, and so on.

Extension mobility users can use BLF presence features on phones with extension mobility support.

BLF presence group authorization ensures that only authorized watchers can access the BLF presence status for a destination. Because the administrator ensures that the watcher is authorized to monitor the destination when a BLF or Speed Dial is configured, BLF presence group authorization does not apply to BLF or Speed Dials.

BLF Presence Prerequisites

- Configure the phones that you want to use with the BLF presence feature.
- Configure the SIP trunks that you want to use with the BLF presence feature.

BLF Presence Configuration Task Flow

Before you begin

- Review BLF Presence Prerequisites, on page 493

Procedure

	Command or Action	Purpose
Step 1	Configure and synchronize cluster-wide enterprise parameters for Busy Lamp Field (BLF). See Configure/Synchronize Cluster-Wide Enterprise Parameters for BLF, on page 495.	Configure BLF options that apply to all devices and services in the same cluster. You can synchronize enterprise-parameter configuration changes with the configured devices in the least-intrusive manner. For example, a reset or restart may not be required on some affected devices.
Step 2	Configure cluster-wide service parameters for BLF. See Configure Cluster-Wide Service Parameters for BLF, on page 496.	Configure presence service parameters to configure different services on selected servers in Cisco Unified Communications Manager Administration.
Step 3	Configure BLF presence groups. See Configure BLF Presence Groups, on page 496.	Configure BLF presence groups to control the destinations that watchers can monitor.
Step 4	To associate BLF presence group with devices and users, perform the following subtasks: • Associate BLF presence groups with phones. See Associate BLF Presence Groups with Phone, on page 498. • Associate BLF presence groups with SIP trunks. See Associate BLF Presence Groups with SIP Trunk, on page 499. • Associate BLF presence groups with an end user. See Associate BLF Presence Groups with End User, on page 500. • Associate BLF presence groups with an application user. See Associate BLF Presence Groups with Application User, on page 501.	Apply a BLF presence group to a directory number, SIP trunk, phone that is running SIP, phone that is running SCCP, application user (for application users that are sending presence requests over the SIP trunk), or end user.
Step 5	Accept BLF presence requests from external trunks and applications. See Accept BLF Presence Requests from External Trunks and Applications, on page 501.	To enable application-level authorization for a SIP trunk application in addition to trunk-level authorization.
Step 6	Configure Calling Search Space. See Configure a Calling Search Space for Presence Requests, on page 502.	Apply a SUBSCRIBE Calling Search Space to the SIP trunk, phone, or end user. The SUBSCRIBE Calling Search Space determines

	Command or Action	Purpose
		how Cisco Unified Communications Manager routes presence requests that come from the trunk or the phone. Calling search spaces determine the partitions that calling devices search when they are attempting to complete a call. If you do not select a different calling search space for presence requests, the SUBSCRIBE Calling Search Space selects the default option, which is **None**.
Step 7	Configure a phone button template for BLF and SpeedDial buttons. See Configure a Phone Button Template for BLF and SpeedDial Buttons, on page 503.	Configure a phone button template for BLF and SpeedDial buttons for a phone, or user device profile. **Note** If the template does not support BLF and SpeedDials, the **Add a new BLF SD** link appears in the Unassigned Associated Items pane.
Step 8	Associate button template with a device. See Associate Button Template with a Device, on page 504.	Use a button template with a configured device for the BLF presence.
Step 9	Configure user device profile. See Configure User Device Profile, on page 504.	Configure the user device profiles for BLF presence.

Configure/Synchronize Cluster-Wide Enterprise Parameters for BLF

Use enterprise parameters for default configuration that apply to all devices and services in the same cluster. A cluster consists of a set of Cisco Unified Communications Managers that share the same database. When you install a new Cisco Unified Communications Manager, it uses the enterprise parameters to set the initial values of its device defaults.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 Configure the fields in the **Enterprise Parameters Configuration** window. For more information on the fields and their configuration options, see Online Help.

Tip For details about an enterprise parameter, click the parameter name or the question mark that appears in the **Enterprise Parameter Configuration** window.

Step 3 Click **Save**.

Step 4 (Optional) Click **Apply Config** to synchronize cluster-wide parameters.

The Apply Configuration Information dialog box appears.

Step 5 Click **OK**.

Configure Cluster-Wide Service Parameters for BLF

You can configure one or multiple services available in the **Service Parameter Configuration** window for BLF.

Before you begin

Configure/Synchronize Cluster-Wide Enterprise Parameters for BLF, on page 495

Procedure

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

Step 2 From the **Server** drop-down list, choose the server where you want to configure the parameter.

Step 3 Configure the fields in the **Service Parameters Configuration** window. For more information on the fields and their configuration options, see Online Help.

Tip For details about the service parameters, click the parameter name or the question mark that appears in the **Service Parameter Configuration** window.

Step 4 Click **Save**.

Note The Default Inter-Presence Group Subscription parameter does not apply to BLF and SpeedDials.

Configure BLF Presence Groups

You can use BLF presence groups to control the destinations that watchers can monitor. To configure a BLF presence group, create the group in Cisco Unified Communications Manager Administration and assign one or more destinations and watchers to the same group.

When you add a new BLF presence group, Unified Communications Manager defines all group relationships for the new group with the default cluster field as the initial permission fields. To apply different permissions, configure new permissions between the new group and existing groups for each permission that you want to change.

Note The system always allows BLF presence requests within the same BLF presence group.

To view the status of a presence entity, watchers send presence requests to Unified Communications Manager. The system requires watchers to be authorized to initiate status requests for a presence entity with these requirements:

- The watcher BLF presence group be authorized to obtain the status for the presence entity presence group, whether inside or outside of the cluster.
- Unified CM must be authorized to accept BLF presence requests from an external presence server or application.

Before you begin

Configure Cluster-Wide Service Parameters for BLF, on page 496

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **BLF Presence Group**.

Step 2 Configure the fields in the **BLF Presence Group Configuration** window. See BLF Presence Group Fields for BLF, on page 497 for details about the fields and their configuration options.

Note Use the **Default Inter-Presence Group Subscription** service parameter for the Cisco CallManager service. It sets the clusterwide permissions parameter for BLF presence groups to allow subscription or disallow subscription. This field enables administrators to set a system default and configure BLF presence group relationships by using the default field for the cluster.

Step 3 Click **Save**.

Note The permissions that you configure for a BLF presence group appear in the **BLF Presence Group Relationship** pane. Permissions that use the system default permission field for the group-to-group relationship do not appear.

What to do next

Associate BLF presence group with devices and users by performing the following subtasks:

- Associate BLF Presence Groups with Phone, on page 498
- Associate BLF Presence Groups with SIP Trunk, on page 499
- Associate BLF Presence Groups with End User, on page 500
- Associate BLF Presence Groups with Application User, on page 501

BLF Presence Group Fields for BLF

Presence authorization works with BLF presence groups. The following table describes the BLF presence group configuration fields.

Field	Description
Name	Enter the name of the BLF presence group that you want to configure. For example, Executive_Group.
Description	Enter a description for the BLF presence group that you are configuring.
Modify Relationship to Other Presence Groups	Select one or more BLF presence groups to configure the permission fields for the named group to the selected groups.

Field	Description
Subscription Permission	For the selected BLF presence groups, choose one of the following options from the drop-down list: • **Use System Default**—Set the permissions field to the Default Inter-Presence Group Subscription clusterwide service parameter field (Allow Subscription or Disallow Subscription). • **Allow Subscription**—Allow members in the named group to view the real-time status of members in the selected groups. • **Disallow Subscription**—Block members in the named group from viewing the real-time status of members in the selected groups. The permissions that you configure appear in the BLF Presence Group relationship pane when you click **Save**. All groups that use system default permission field do not appear.

BLF Presence Group Association with Devices and Users

Perform the following procedures to apply a BLF presence group to the phone, SIP trunk, phone that is running SIP, phone that is running SCCP, directory number, application user (for application users that are sending presence requests over the SIP trunk), and end user.

Note The system allows presence requests between members in the same BLF presence group.

Associate BLF Presence Groups with Phone

You can use BLF presence for phones and trunks when the phones and trunks have permission to send and receive presence requests.

Cisco Unified Communications Manager handles the BLF presence requests for Cisco Unified Communications Manager users, whether inside or outside the cluster. For a Cisco Unified Communications Manager watcher that sends a BLF presence request through the phone, Cisco Unified Communications Manager responds with the BLF presence status if the phone and BLF presence entity are colocated

Before you begin

Configure BLF Presence Groups, on page 496

Procedure

Step 1 In the Cisco Unified CM Administration, choose **Device** > **Phone**, and click **Add New**.
The **Add a New Phone** window appears.

Step 2 From the **Phone Type** drop-down list, select the type of phone that you want to associate BLF presence group to.

Step 3 Click **Next**.

Step 4 Configure the fields in the **Phone Configuration** window. See the online help for information about the fields and their configuration options.

Note From the **SUBSCRIBE Calling Search Space** drop-down list, select a SUBSCRIBE calling search space to use for presence requests for the phone. All calling search spaces that you configure in Cisco Unified Communications Manager Administration appear in the **SUBSCRIBE Calling Search Space** drop-down list. If you do not select a different calling search space for the end user from the drop-down list, the value of this field applies the default value as **None**. To configure a SUBSCRIBE calling search space specifically for this purpose, configure a calling search space as you configure all calling search spaces.

Step 5 Click **Save**.

What to do next

Associate BLF presence group with devices and users by performing the following subtasks:

- Associate BLF Presence Groups with SIP Trunk, on page 499
- Associate BLF Presence Groups with End User, on page 500
- Associate BLF Presence Groups with Application User, on page 501

Associate BLF Presence Groups with SIP Trunk

If digest authentication is not configured for the SIP trunk, you can configure the trunk to accept incoming subscriptions, but application-level authorization cannot be initiated, and Unified CM accepts all incoming requests before performing group authorization. When digest authentication is used with application-level authorization, Unified CM also authenticates the credentials of the application that is sending the BLF presence requests.

When there is a BLF presence request for a device that exists outside of the cluster, Unified Communications Manager queries the external device through the SIP trunk. If the watcher has permission to monitor the external device, the SIP trunk sends the BLF presence request to the external device, and returns BLF presence status to the watcher.

Tip To use BLF presence group authorization with incoming presence requests on a SIP trunk, configure a presence group for the trunk, such as External_Presence_Serv_Group1, and configure the appropriate permissions to other groups inside the cluster.

If you configure both levels of authorization for SIP trunk presence requests, the BLF presence group for the SIP trunk gets used only when no BLF presence group is identified in the incoming request for the application.

Before you begin

Configure BLF Presence Groups, on page 496

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Trunk**, and click **Add New**.

Step 2 From the **Trunk Type** drop-down list, select the type of phone that you want to associate BLF presence group. The value in the **Device Protocol** drop-down list populates automatically.

Step 3 Click **Next**.

Step 4 Configure the fields in the **Trunk Configuration** window. See the online help for information about the fields and their configuration options.

Note To authorize the Unified CM system to accept incoming BLF presence requests from the SIP trunk, check the **Accept Presence Subscription** check box in the SIP Trunk Security Profile Configuration window. To block incoming presence requests on a SIP trunk, uncheck the check box. When you allow SIP trunk BLF presence requests, Unified CM accepts requests from the SIP user agent (SIP proxy server or external BLF presence server) that connects to the trunk. Consider digest authentication as optional when Unified CM is configured to accept BLF presence requests from a SIP trunk.

Step 5 Click **Save**.

What to do next

Associate BLF presence group with devices and users by performing the following subtasks:

- Associate BLF Presence Groups with Phone, on page 498
- Associate BLF Presence Groups with End User, on page 500
- Associate BLF Presence Groups with Application User, on page 501

Associate BLF Presence Groups with End User

An administrator associates BLF presence groups with end user for user directories and call lists and to configure extension mobility settings.

Before you begin

Configure BLF Presence Groups, on page 496

Procedure

Step 1 In the Cisco Unified CM Administration, choose **User Management** > **End User**, and click **Add New**. The **End User Configuration** window appears.

Step 2 Configure the fields in the **End User Configuration** window. See the online help for information about the fields and their configuration options.

Step 3 Click **Save**.

What to do next

Associate BLF presence group with devices and users by performing the following subtasks:

- Associate BLF Presence Groups with Phone, on page 498
- Associate BLF Presence Groups with SIP Trunk, on page 499
- Associate BLF Presence Groups with Application User, on page 501

Associate BLF Presence Groups with Application User

An administrator associates BLF Presence groups with an application user for external applications. These external applications send BLF presence requests that is SIP trunk or home on a proxy server which is connected on SIP trunk. For example, Web Dial, Meeting Place, conference servers, and presence servers.

Before you begin

Configure BLF Presence Groups, on page 496

Procedure

Step 1 In the Cisco Unified CM Administration, choose **User Management** > **Application User**, and click **Add New**.
The **Application User Configuration** window appears.

Step 2 Configure the fields in the **Application User Configuration** window. See the online help for information about the fields and their configuration options.

Step 3 Click **Save**.

What to do next

Associate BLF presence group with devices and users by performing the following subtasks:

- Associate BLF Presence Groups with Phone, on page 498
- Associate BLF Presence Groups with SIP Trunk, on page 499
- Associate BLF Presence Groups with End User, on page 500

Accept BLF Presence Requests from External Trunks and Applications

To allow BLF presence requests from outside the cluster, configure the system to accept BLF presence requests from the external trunk or application. You can assign BLF presence groups to trunks and applications outside the cluster to invoke BLF presence group authorization.

Before you begin

Associate BLF presence group with devices and users by performing the following subtasks:

- Associate BLF Presence Groups with Phone, on page 498

- Associate BLF Presence Groups with SIP Trunk, on page 499
- Associate BLF Presence Groups with End User, on page 500
- Associate BLF Presence Groups with Application User, on page 501

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Trunk**, and click **Add New**.
The **Trunk Configuration** window appears.

Step 2 To allow BLF presence requests from a SIP trunk, check the **Accept Presence Subscription** check box in the **SIP Trunk Security Profile Configuration** window.

Step 3 To enable application-level authorization for a SIP trunk application in addition to trunk-level authorization, check the following check boxes in the **SIP Trunk Security Profile Configuration** window:

- **Enable Digest Authentication**
- **Enable Application Level Authorization**

Note You cannot check **Enable Application Level Authorization** unless **Enable Digest Authentication** is checked.

Step 4 Apply the profile to the trunk. Click **Reset** so that the changes to the trunk can take effect.

Note If you checked **Enable Application Level Authorization**, check the **Accept Presence Subscription** check box in the **Application User Configuration** window for the application.

Configure a Calling Search Space for Presence Requests

The SUBSCRIBE Calling Search space option allows you to apply a calling search space separate from the call-processing Calling Search Space for BLF presence requests. Select a different calling search space for presence requests, else the SUBSCRIBE Calling Search Space selects the **None** default option. The SUBSCRIBE Calling Search Space that is associated with an end user is used for extension mobility calls.

You apply the SUBSCRIBE Calling Search Space to the SIP trunk, phone, or end user. The SUBSCRIBE Calling Search Space that is associated with an end user is used for extension mobility calls.

Before you begin

Accept BLF Presence Requests from External Trunks and Applications, on page 501

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Calling Search Space**.

Step 2 In the **Calling Search Space configuration** window, choose the calling search space from the **SUBSCRIBE Calling Search Space** drop-down list.

Step 3 Click **Add New**.

Step 4 In the **Name** field, enter a name.

Step 5 (Optional) In the **Description** field, enter a description to identify the calling search space.

Step 6 From the **Available Partitions** list, select one or multiple partitions, and click the arrow keys.
The selected partitions appear in the **Selected Partitions** list.

Step 7 (Optional) To add or remove a partition from the **Selected Partitions** list, click the arrow keys next to the list box.

Step 8 Click **Save**.

All calling search spaces that you configure in Cisco Unified Communications Manager Administration appear in the **SUBSCRIBE Calling Search Space** drop-down list in the **Trunk Configuration** or **Phone Configuration** window.

Configure a Phone Button Template for BLF and SpeedDial Buttons

You can configure BLF and SpeedDial buttons for a phone or user device profile. After you apply the template to the phone or device profile (and save the phone or device profile configuration), the Add a new BLF SD link appears in the **Association Information** pane in Cisco Unified Communications Administration.

Note If the template does not support BLF and SpeedDials, the Add a new BLF SD link appears in the **Unassigned Associated Items** pane.

When an administrator decides to add or change a BLF and SpeedDial button for a SIP URI, the administrator ensures that the watcher is authorized to monitor that destination. If the system uses a SIP trunk to reach a SIP URI BLF target, the BLF presence group associated with the SIP trunk applies.

Note You do not need to configure BLF presence groups or the Default Inter-Presence Group Subscription parameter for BLF and SpeedDials.

Before you begin

Configure a Calling Search Space for Presence Requests, on page 502

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Phone Button Template**.

Step 2 Click the **Add New** button.
The **Phone Button Template Configuration** window appears.

Step 3 In the **Button Template Name** field, enter a name for the template.

Step 4 From the **Phone Button Template** drop-down list, select a template of phone button.

Step 5 Click **Copy** to create a new button template based on the layout of the selected button template.

Step 6 Click **Save**.

Associate Button Template with a Device

You configure BLF and SpeedDial buttons for a phone or user device profile. The BLF value does not have to be on the cluster. For information on the Busy Lamp Field (BLF) status icons that display on the phone, see the Cisco Unified IP Phone documentation that supports your phone. To identify whether your phone supports BLF presence, see the Cisco Unified IP Phone documentation that supports your phone and this version of Unified Communications Manager.

Before you begin

Configure a Phone Button Template for BLF and SpeedDial Buttons, on page 503

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Device Profile**.

Step 2 Enter the search parameters to find the configured phone button templates, and click **Find**.
The records matching all the search criteria appear.

Step 3 Click one of the records.
The **Device Profile Configuration** window appears.

Step 4 From the **Phone Button Template** list, select a configured phone button template.

Step 5 (Optional) Modify the values of the configured device.

Step 6 Click **Save**.

Configure User Device Profile

See the "BLF Presence with Extension Mobility" section of BLF Presence Interactions, on page 505 for details.

Before you begin

Associate Button Template with a Device, on page 504

Procedure

Step 1 In the Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Device Profile**.

Step 2 Click **Add New**.
The **Device Profile Configuration** window appears.

Step 3 Configure the fields in **Device Profile Configuration** window. See the online help for information about the fields and their configuration options.

Note If the phone button template that you applied to the phone or device profile does not support BLF and SpeedDials, the link does not appear in the **Association Information** pane, but appears in the **Unassigned Associated Items** pane.

Step 4 Click **Save**.

BLF Presence Interactions and Restrictions

BLF Presence Interactions

Feature	Interaction
Presence BLF with DNs on H.323 phones when the H.323 phone device serves as presence entity	When the H.323 phone is in the RING IN state, the BLF status gets reported as Busy. For the presence entities of phones that are running either SCCP or SIP and that are in the RING IN state, the BLF status gets reported as Idle.
Presence BLF with DNs on H.323 phones when the H.323 phone device serves as presence entity	When the H.323 phone is not connected to Cisco Unified Communications Manager for any reason, such as the Ethernet cable is unplugged from the phone, the BLF status gets reported as Idle all the time. For presence entities of phones that are running either SCCP or SIP and that are not connected to Cisco Unified Communications Manager, the BLF status gets reported as Unknown.
BLF Presence with Extension Mobility	When you configure BLF and SpeedDial buttons in a user device profile in Cisco Unified Communications Manager Administration, a phone that supports Cisco Extension Mobility displays BLF presence status on the BLF and SpeedDial buttons after you log in to the device. When the extension mobility user logs out, a phone that supports Cisco Extension Mobility displays BLF presence status on the BLF and SpeedDial buttons for the logout profile that is configured.

BLF Presence Restrictions

Restriction	Description
SIP Presence	Cisco Unified Communications Manager Assistant does not support SIP presence.
BLF Presence Requests	Cisco Unified Communications Manager Administration rejects BLF presence requests to a directory number that is associated with a hunt pilot.
BLF on Call List Feature	The BLF on call list feature is not supported on the Cisco Unified IP Phone 7940 and Cisco Unified IP Phone 7960.

Restriction	Description
BLF and SpeedDials	The administrator ensures that the watcher is authorized to monitor the destination when configuring a BLF and SpeedDial. BLF presence group authorization does not apply to BLF and SpeedDials. **Note** BLF presence group authorization does not apply to any directory number or SIP URI that is configured as a BLF and Speed Dial that appears in a call list for phones that are running SIP. If there is an overlapping DN, where there is the same extension in different partitions, the presence notifications are selected based on the order of the partitions configured within the SUBSCRIBE CSS assigned to the device. For example, two BLF speed dials are configured on a phone. • Extension 1234 in the "internal" partition • Extension 1234 in the "external" partition Whichever partition is listed first within the SUBSCRIBE CSS is the one that will provide BLF presence to the subscribed devices.
BLF Presence Authorization	For Cisco Unified IP Phones with multiple lines, the phone uses the cached information that is associated with the line directory number for missed and placed calls to determine BLF presence authorization. If this call information is not present, the phone uses the primary line as the subscriber for BLF presence authorization. For BLF and SpeedDial buttons on Cisco Unified IP Phones with multiple lines, the phone uses the first available line as the subscriber.
Cisco Unified IP Phone	When a user monitors a directory number that is configured for Cisco Unified IP Phones 7960, 7940, 7905, and 7912 that are running SIP, the system displays a status icon for ‘not on the phone’ on the watcher device when the presence entity is off-hook (but not in a call connected state). These phones do not detect an off-hook status. For all other phone types, the system displays the status icon for ‘on the phone’ on the watcher device for an off-hook condition at the presence entity.
SIP Trunks	BLF presence requests and responses must route to SIP trunks or routes that are associated with SIP trunks. The system rejects BLF presence requests routing to MGCP and H323 trunk devices.
BLF Presence-supported Phones that are running SIP	For BLF presence-supported phones that are running SIP, you can configure directory numbers or SIP URIs as BLF and SpeedDial buttons. For BLF presence-supported phones that are running SCCP, you can only configure directory numbers as BLF and SpeedDial buttons.
Phones that are running SIP	For phones that are running SIP, BLF presence group authorization also does not apply to any directory number or SIP URI that is configured as a BLF and Speed Dial that appears in a call list.

CHAPTER 36

Call Display Restrictions

Call Display Restrictions Overview

Cisco Unified Communications Manager provides flexible configuration options that allow and also restrict the display of the number and name information for both calling and connected users. You can restrict connected numbers and names independently of each other.

You can configure connected number and name restrictions on the SIP trunk level or on a call-by-call basis. The SIP trunk level configuration overrides a call-by-call configuration.

For example, in a hotel environment, you may want to see the display information for calls that are made between a guest room and the front desk. However, for calls between guest rooms, you can restrict the call information to display on either phone.

Call Display Restrictions Configuration Task Flow

Before you begin

- Review Call Display Restrictions Interactions, on page 516

Procedure

	Command or Action	Purpose
Step 1	Generate a Phone Feature List, on page 3	Generate a report to identify endpoints that support the Call Display Restrictions feature.
Step 2	Configure Partitions for Call Display Restrictions, on page 508	Configure partitions to create a logical grouping of directory numbers (DN) and route patterns with similar reachability characteristics. For example, in a hotel environment, you can a

	Command or Action	Purpose
		configure a partition for dialing between rooms, and a partition for dialing the public switched telephone network (PSTN).
Step 3	Configure Calling Search Spaces for Call Display Restrictions, on page 509.	Configure calling search spaces to identify the partitions that calling devices can search when they attempt to complete a call. Create calling search spaces for rooms, the front desk, other hotel extensions, the PSTN, and the room park range (for call park).
Step 4	Configure the Service Parameter for Connected Number Display Restriction, on page 510.	Configure the service parameter to display the connected line ID as dialed digits only.
Step 5	Configure Translation Patterns, on page 511.	Configure translation patterns with different levels of display restrictions.
Step 6	Configure Phones for Call Display Restrictions, on page 512	Associate endpoints with the partitions and the calling search spaces that you want to use for call display restrictions.
Step 7	Configure the PSTN Gateway for Call Display Restrictions, on page 514	Associate the PSTN gateway with the partitions and the calling search spaces that you want to use for call display restrictions.
Step 8	Optional. Configure Call Display Restrictions on SIP Trunks, on page 514	Use this procedure to configure connected number and name restrictions on the SIP trunk level. The SIP trunk level configuration overrides call-by-call configuration.

Configure Partitions for Call Display Restrictions

Configure partitions to create a logical grouping of directory numbers (DNs) and route patterns with similar reachability characteristics. Partitions facilitate call routing by dividing the route plan into logical subsets that are based on organization, location, and call type. You can configure multiple partition

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Partition**.

Step 2 Click **Add New** to create a new partition.

Step 3 In the **Partition Name, Description** field, enter a name for the partition that is unique to the route plan.

Partition names can contain alphanumeric characters, as well as spaces, hyphens (-), and underscore characters (_). See the online help for guidelines about partition names.

Step 4 Enter a comma (,) after the partition name and enter a description of the partition on the same line.

The description can contain up to 50 characters in any language, but it cannot include double quotes ("), percentage sign (%), ampersand (&), backslash (\), angle brackets (<>), or square brackets ([ ]).

If you do not enter a description, Cisco Unified Communications Manager automatically enters the partition name in this field.

Step 5 To create multiple partitions, use one line for each partition entry.

Step 6 From the **Time Schedule** drop-down list, choose a time schedule to associate with this partition.

The time schedule specifies when the partition is available to receive incoming calls. If you choose **None**, the partition remains active at all times.

Step 7 Select one of the following radio buttons to configure the **Time Zone**:

- **Originating Device**—When you select this radio button, the system compares the time zone of the calling device to the **Time Schedule** to determine whether the partition is available is available to receive an incoming call.
- **Specific Time Zone**—After you select this radio button, choose a time zone from the drop-down list. The system compares the chosen time zone to the **Time Schedule** to determine whether the partition is available is available to receive an incoming call.

Step 8 Click **Save**.

Partition Name Guidelines

The list of partitions in a calling search space is limited to a maximum of 1024 characters. This means that the maximum number of partitions in a CSS varies depending on the length of the partition names. Use the following table to determine the maximum number of partitions that you can add to a calling search space if partition names are of fixed length.

Table 45: Partition Name Guidelines

Partition Name Length	Maximum Number of Partitions
2 characters	340
3 characters	256
4 characters	204
5 characters	172
. . .	. . .
10 characters	92
15 characters	64

Configure Calling Search Spaces for Call Display Restrictions

Configure calling search spaces to identify the partitions that calling devices can search when they attempt to complete a call. Create calling search spaces for rooms, the front desk, other hotel extensions, the PSTN, and the room park range (for call park).

Before you begin

Configure Partitions for Call Display Restrictions, on page 508

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Calling Search Space**.

Step 2 Click **Add New**.

Step 3 In the **Name** field, enter a name.

Ensure that each calling search space name is unique to the system. The name can include up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_).

Step 4 In the **Description** field, enter a description.

The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).

Step 5 From the **Available Partitions** drop-down list, perform one of the following steps:

- For a single partition, select that partition.
- For multiple partitions, hold down the **Control (CTRL)** key, then select the appropriate partitions.

Step 6 Select the down arrow between the boxes to move the partitions to the **Selected Partitions** field.

Step 7 (Optional) Change the priority of selected partitions by using the arrow keys to the right of the **Selected Partitions** box.

Step 8 Click **Save**.

Configure the Service Parameter for Connected Number Display Restriction

The connected number display restriction restricts the connected line ID display to dialed digits only. This option addresses customer privacy issues as well as connected number displays that are meaningless to phone users.

Before you begin

Configure Calling Search Spaces for Call Display Restrictions, on page 509

Procedure

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

Step 2 Select the server where the Cisco CallManager service runs, and then select the Cisco CallManager service.

Step 3 Set the **Always Display Original Dialed Number** service parameter to **True** to enable this feature.

The default value is **False**.

Step 4 (Optional) Set the **Name Display for Original Dialed Number When Translated** service parameter.

The default field shows the alerting name of the original dialed number before translation. You can change this parameter to show the alerting name of the dialed number after translation. This parameter is not applicable if the **Always Display Original Number** service parameter is set to **False**.

Step 5 Click **Save**.

Configure Translation Patterns

Unified Communications Manager uses translation patterns to manipulate dialed digits before it routes a call. In some cases, the system does not use the dialed number. In other cases, the public switched telephone network (PSTN) does not recognize the dialed number. For the Call Display Restrictions feature, calls are routed through different translation patterns before the calls are extended to the actual device.

Before you begin

Configure the Service Parameter for Connected Number Display Restriction, on page 510

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Translation Pattern**.

Step 2 Configure the fields in the **Translation Pattern Configuration** window. See Translation Pattern Fields for Call Display Restrictions, on page 511 for more information about the fields and their configuration options.

Step 3 Click **Save**.

Translation Pattern Fields for Call Display Restrictions

Field	Description
Translation Pattern	Enter the translation pattern, including numbers and wildcards. Do not use spaces. For example, for the NANP, enter 9.@ for typical local access or 8XXX for a typical private network numbering plan. Valid characters include the uppercase characters A, B, C, and D and \+, which represents the international escape character +.
Description	Enter a description for the translation pattern. The description can include up to 50 characters in any language, but it cannot include double quotes ("), percentage sign (%), ampersand (&), or angle brackets (<>).
Partition	From the drop-down list, choose the partition to associate with this translation pattern.
Calling Search Space	From the drop-down list, choose the calling search space to associate with this translation pattern.

Field	Description
Calling Line ID Presentation	From the drop-down list, choose one of the following options: • **Default**—Choose this option if you do not want to change the presentation of the calling line ID. • **Allowed**—Choose this option if you want to display the phone number of the calling party. • **Restricted**—Choose this option if you want Cisco Unified Communications Manager to block the display of the calling party phone number.
Calling Name Presentation	From the drop-down list, choose one of the following options: • **Default**—Choose this option if you do not want to change the presentation of the calling name. • **Allowed**—Choose this option if you want to display the name of the calling party. • **Restricted**—Choose this option if you want Cisco Unified Communications Manager to block the display of the calling name.
Connected Line ID Presentation	From the drop-down list, choose one of the following options: • **Default**—Choose this option if you do not want to change the presentation of the connected line ID. • **Allowed**—Choose this option if you want to display the phone number of the connected party. • **Restricted**—Choose this option if you want Cisco Unified Communications Manager to block the display of the connected party phone number.
Connected Name Presentation	From the drop-down list, choose one of the following options: • **Default**—Choose this option if you do not want to change the presentation of the connected name. • **Allowed**—Choose this option if you want to display the name of the connected party. • **Restricted**—Choose this option if you want Cisco Unified Communications Manager to block the display of the connected name.

Configure Phones for Call Display Restrictions

Use this procedure to associate phones with the partitions and the calling search spaces used for call display restrictions.

Before you begin

Configure Translation Patterns, on page 511

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Perform one of the following tasks:

a) To modify the fields for an existing phone, enter search criteria and choose a phone from the resulting list. The **Phone Configuration** window appears.

b) To add a new phone, click **Add New**.

The **Add a New Phone** window appears.

Step 3 From the **Calling Search Space** drop-down list, choose the calling search space that you want the system to use when it determines how to route a dialed number.

Step 4 Check the **Ignore presentation indicators (internal calls only)** check box to ignore any presentation restriction on internal calls.

Step 5 Click **Save**.
The phone is added to the database.

Step 6 To associate the added phone to a directory number, choose **Device** > **Phone**, enter search parameters to search the phone that you added.

Step 7 In the **Find and List Phones** window, click the phone name.
The **Phone Configuration window** appears.

Step 8 From the **Association** pane, click the phone name to add or modify the directory number.
The **Directory Number Configuration** window appears.

Step 9 In the **Directory Number Configuration** window, add or modify the value of directory number in the **Directory Number** text box, and select a value in the **Route Partition** drop-down list.

Step 10 Click **Save**.

Phone Configuration Example

Configure phone A (Room-1) with partition P_Room and device/line calling search space CSS_FromRoom

{ P_Phones, CSS_FromRoom} : 221/Room-1

Configure phone B (Room-2) with partition P_Room and device/line calling search space CSS_FromRoom

{ P_Phones, CSS_FromRoom} : 222/Room-2

Configure phone C (Front Desk-1) with partition P_FrontDesk and device/line calling search space

CSS_FromFrontDesk and Ignore Presentation Indicators check box enabled

{ P_FrontDesk, CSS_FromFrontDesk, IgnorePresentationIndicators set} : 100/Reception

Configure phone D (Front Desk-2) with partition P_FrontDesk and device/line calling search space

CSS_FromFrontDesk and Ignore Presentation Indicators check box enabled

{ P_FrontDesk, CSS_FromFrontDesk, IgnorePresentationIndicators set} : 200/Reception

Configure phone E (Club) with partition P_Club and calling search space CSS_FromClub

{ P_Club, CSS_FromClub) : 300/Club

Configure the PSTN Gateway for Call Display Restrictions

Associate the PSTN gateway with the partitions and the calling search spaces that you want to use for call display restrictions.

Before you begin

Configure Phones for Call Display Restrictions, on page 512

Procedure

Step 1 In Cisco Unified CM Administration, choose **Device** > **Gateway**.

Step 2 Enter search criteria and choose the PSTN gateway from the resulting list.
The **Gateway Configuration** window appears.

Step 3 From the **Calling Search Space** drop-down list, choose the calling search space that you want the system to use when it determines how to route an incoming call from the PSTN.

Step 4 Click **Save** and **Reset** to apply the configuration changes.

Step 5 (Optional) To associate the available trunk or gateway, in Cisco Unified Communications Manager Administration, choose **SIP Route Pattern**, and select a SIP trunk or route list from the **SIP Trunk/Route List** drop-down list.

Gateway Configuration Example

Configure PSTN Gateway E with route pattern P_PSTN and calling search space CSS_FromPSTN

{CSS_FromPSTN}, RoutePattern {P_PSTN}

Configure Call Display Restrictions on SIP Trunks

You can configure connected number and name restrictions on the SIP trunk level. The SIP trunk-level configuration overrides call-by-call configuration.

Before you begin

(Optional) Configure the PSTN Gateway for Call Display Restrictions, on page 514

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Trunk**.
The **Find and List Trunks** window appears.

Step 2 Enter search criteria and click **Find**.

Step 3 Select the name of the trunk that you want to update.

Step 4 Configure the fields in the **SIP Trunk Configuration** window. See SIP Trunk Fields for Call Display Restrictions, on page 515 for more information about the fields and their configuration options.

Step 5 Click **Save**.

SIP Trunk Fields for Call Display Restrictions

Table 46: Inbound Calls

Field	Description
Calling Line ID Presentation	From the drop-down list, choose one of the following options: • **Default**—Choose this option if you do not want to change the presentation of the calling line ID. • **Allowed**—Choose this option if you want to display the phone number of the calling party. • **Restricted**—Choose this option if you want Cisco Unified Communications Manager to block the display of the calling party phone number.
Calling Name Presentation	From the drop-down list, choose one of the following options: • **Default**—Choose this option if you do not want to change the presentation of the calling name. • **Allowed**—Choose this option if you want to display the name of the calling party. • **Restricted**—Choose this option if you want Cisco Unified Communications Manager to block the display of the calling name.
Calling Search Space	From the drop-down list, choose the calling search space to associate with this translation pattern.

Table 47: Outbound Calls

Field	Description
Connected Line ID Presentation	From the drop-down list, choose one of the following options: • **Default**—Choose this option if you do not want to change the presentation of the connected line ID. • **Allowed**—Choose this option if you want to display the phone number of the connected party. • **Restricted**—Choose this option if you want Cisco Unified Communications Manager to block the display of the connected party phone number.
Connected Name Presentation	From the drop-down list, choose one of the following options: • **Default**—Choose this option if you do not want to change the presentation of the connected name. • **Allowed**—Choose this option if you want to display the name of the connected party. • **Restricted**—Choose this option if you want Cisco Unified Communications Manager to block the display of the connected name.

Call Display Restrictions Interactions

This section describes how the Call Display Restrictions feature interacts with Cisco Unified Communications Manager applications and call processing features.

Feature	Interaction
Call Park	When you use the Call Display Restrictions feature with Call Park, you must configure an associated translation pattern for each individual call park number to preserve the Call Display Restrictions feature. You cannot configure a single translation pattern to cover a range of call park numbers. Consider the following scenario as an example: **1.** The system administrator creates a call park range of 77x and places it in a partition called P_ParkRange. (The phones in the guest rooms can see that the P_ParkRange partition is made visible to the phones in the guest rooms by inclusion of it in the calling search space of the phones [CSS_FromRoom]). **2.** The administrator configures a separate translation pattern for each call park directory number and configures the display fields to Restricted. (In the current scenario, the administrator creates translations patterns for 770, 771, 772...779.) **Note** For the Call Display Restrictions feature to work correctly, the administrator must configure separate translation patterns and not a single translation pattern for a range of numbers (such as 77x or 77[0-9]). **3.** Room-1 calls Room-2. **4.** Room-2 answers the call, and Room-1 parks the call. **5.** When Room-1 retrieves the call, Room-2 does not see Room-1 call information display. See Call Park Overview
Conference List	When you use Call Display Restrictions, you restrict the display information for the list of participants in a conference. See Ad Hoc Conferencing Overview
Conference and Voice Mail	When you use Call Display Restrictions with features, such as conference and voice mail, the call information display on the phones reflects that status. For example, when the conference feature is invoked, the call information display shows **To Conference**. When voice mail is accessed by choosing the Messages button, the call information display shows **To Voicemail**.
Extension Mobility	To use Call Display Restrictions with Extension Mobility, enable the **Ignore Presentation Indicators (internal calls only)** parameter in both the Cisco Unified Communications Manager Administration Phone Configuration window and the Cisco Unified Communications Manager Administration Device Profile Configuration window. When you enable Call Display Restrictions with Extension Mobility, the presentation or restriction of the call information depends on the line profile that is associated with the user who is logged in to the device. The configuration that is entered in the user device profile (associated with the user) overrides the configuration that is entered in the phone configuration (of the phone that is enabled for Extension Mobility).

Feature	Interaction
Call Forwarding	The Connected Number Display restriction applies to all calls that originate in the system. When this value is set to **True**, this field interacts with existing Cisco Unified Communications Manager applications, features, and call processing. This value applies to all calls that terminate inside or outside the system. The Connected Number Display is updated to show the modified number or redirected number when a call is routed to a Call Forward All or Call Forward Busy destination, or gets redirected through a call transfer or CTI application.

Call Display Restrictions Feature Restrictions

Translation Patterns—Duplicate entries are not allowed in translation patterns.

CHAPTER 37

Do Not Disturb

This chapter provides details on the Do Not Disturb feature.

Do Not Disturb Overview

Do Not Disturb (DND) provides the following options:

- Call Reject—This option specifies that the incoming call gets rejected. Depending on how you configure the DND Incoming Call Alert parameter, the phone may play a beep, or display a flash notification of the call.
- Ringer Off—This option turns off the ringer, but incoming call information gets presented to the device, so that the user can accept the call.

When DND is enabled, all new incoming calls with normal priority honor the DND settings for the device. High-priority calls, such as Cisco Emergency Responder (CER) calls, or calls with Multilevel Precedence and Preemption (MLPP), ring on the device. Also, when you enable DND, the Auto Answer feature gets disabled.

Users can activate Do Not Disturb on the phone in the following ways:

- Softkey
- Feature button
- Cisco Unified Communications Self-Care Portal

Note You can also enable or disable the feature on a per-phone basis from within Cisco Unified Communications Manager.

Phone Behavior

When you enable Do Not Disturb, the Cisco Unified IP Phone displays the message "Do Not Disturb is active". Some Cisco Unified IP Phones display DND status icons. For details on how individual phone models use Do Not Disturb, consult the user guide for that particular phone model.

When you activate DND, you can still receive incoming call notifications on the phone as specified by the Incoming Call Alert settings in Cisco Unified Communications Manager Administration, but the phone will not ring, except for high-priority calls (such as Cisco Emergency Responder and MLPP calls). Also, if you enable DND while the phone is ringing, the phone stops ringing.

Status Notifications

Do Not Disturb is supported on both SIP and Cisco Skinny Call Control Protocol (SCCP) devices.

SIP phones use the SIP PUBLISH method to signal a DND status change to Cisco Unified Communications Manager. Cisco Unified Communications Manager uses a Remote-cc REFER request to signal a DND status change to the SIP phone.

SCCP phones use SCCP messaging to signal a DND status change to Cisco Unified Communications Manager.

Do Not Disturb Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Generate a Phone Feature List, on page 3	Run a Phone Feature List report from Cisco Unified Reporting to determine which phones support Do Not Disturb. **Note** Cisco Unified IP Phones 7940 and 7960 that are running SIP use their own backwards-compatible implementation of Do Not Disturb, which you configure on the SIP Profile.
Step 2	Configure Busy Lamp Field Status, on page 521	Configure the Busy Lamp Field status service parameter.
Step 3	Configure Do Not Disturb on a Common Phone Profile, on page 521	Optional. Configure Do Not Disturb against a Common Phone Profile. The profile allows you to apply Do Not Disturb settings to a group of phones in your network.
Step 4	Apply Do Not Disturb Settings to the Phone, on page 522.	Apply Do Not Disturb settings to the phone.
Step 5	Depending on whether your phone uses softkeys or feature buttons, perform either of the following tasks:	Add a Do Not Disturb feature button or softkey to your phone.

	Command or Action	Purpose
	• Configure a Do Not Disturb Feature Button, on page 523 • Configure a Do Not Disturb Softkey, on page 524	

Configure Busy Lamp Field Status

Configure how the Busy Lamp Field (BLF) status depicts Do Not Disturb by setting the **BLF Status Depects DND** service parameter. To set the BLF status, do the following:

Before you begin

Generate a Phone Feature List, on page 3

Procedure

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

Step 2 Choose the **Cisco CallManager** service for the server that you want to configure.

Step 3 In the Clusterwide Parameters (System - Presence) pane, specify one of the following values for the **BLF Status Depicts DND** service parameter:

- **True**—If Do Not Disturb is activated on the device, the BLF status indicator for the device or line appearance reflects the Do Not Disturb state.
- **False**—If Do Not Disturb is activated on the device, the BLF status indicator for the device or line appearance reflects the actual device state.

What to do next

Perform one of the following procedures:

Configure Do Not Disturb on a Common Phone Profile, on page 521

Apply Do Not Disturb Settings to the Phone, on page 522

Configure Do Not Disturb on a Common Phone Profile

Common Phone Profiles allow you to configure Do Not Disturb settings and then apply those settings to a group of phones in your network that use that profile.

Before you begin

Configure Busy Lamp Field Status, on page 521

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Common Phone Profile**.

Step 2 From the **DND Option** drop-down list, choose how you want the Do Not Disturb feature to handle incoming calls.

- **Call Reject**—No incoming call information gets presented to the user. Depending on how you configure the DND Incoming Call Alert parameter, the phone may play a beep or display a flash notification of the call.
- **Ringer Off**—This option turns off the ringer, but incoming call information gets presented to the device, so the user can accept the call.

Note For mobile phones and dual-mode phones, you can only choose the Call Reject option.

Step 3 From the **Incoming Call Alert** drop-down list, choose how you want to alert phone users of incoming calls while Do Not Disturb is turned on.

- **Disable**—Both beep and flash notification of a call are for disabled. If you configured the DND Ringer Off option, incoming call information still gets displayed. However, for the DND Call Reject option, no call alerts display, and no information gets sent to the device.
- **Flash Only**—The phone flashes for incoming calls.
- **Beep Only**—The phone displays a flash alert for incoming calls.

Step 4 Click **Save**.

Apply Do Not Disturb Settings to the Phone

This procedure describes how to apply Do Not Disturb settings on your Cisco Unified IP Phones. You can apply DND settings through the **Phone Configuration** window in Cisco Unified CM Administration, or you can apply DND settings to a Common Phone Profile and then apply that profile to your phone.

Before you begin

If you are using a Common Phone Profile, complete Configure Do Not Disturb on a Common Phone Profile, on page 521.

Otherwise, complete Configure Busy Lamp Field Status, on page 521

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**

Step 2 Click **Find** and select the phone on which you want to configure Do Not Disturb.

Step 3 If you want to apply Do Not Disturb settings from a Common Phone Profile, from the **Common Phone Profile** drop-down list, choose the profile on which you have configured Do Not Disturb.

Step 4 Check the **Do Not Disturb** check box to enable Do Not Disturb on the phone.

Step 5 In the **DND Option** drop-down list, specify from the following options how you want the DND feature to handle incoming calls.

- **Call Reject**—No incoming call information gets presented to the user. Depending on the configuration, the phone either plays a beep or displays a flash notification.
- **Ringer Off**—Incoming call information gets presented to the device so that the user can accept the call, but the ringer is turned off.
- **Use Common Profile Setting**—The Do Not Disturb setting for the Common Phone Profile that is specified for this device gets used.

Note For 7940/7960 phones that are running SCCP, you can only choose the Ringer Off option. For mobile devices and dual-mode phones, you can only choose the Call Reject option. When you activate DND Call Reject on a mobile device or dual-mode phone, no call information gets presented to the device.

Step 6 In the **DND Incoming Call Alert** drop-down list, specify from the following options how you want the phone to display an incoming call when DND is turned on.

- **None**—The DND Incoming Call Alert setting from the Common Phone Profile gets used for this device.
- **Disable**—For DND Ringer Off, both beep and flash notifications are disabled, but incoming call information is still displayed. For Call Reject, beep and flash notifications are disabled, and no incoming call information gets passed to the device.
- **Beep only**—For incoming calls, the phone plays a beep tone only.
- **Flash only**—For incoming calls, the phone displays a flash alert.

Step 7 Click **Save**.

What to do next

Complete either of the following procedures:

Configure a Do Not Disturb Feature Button, on page 523

Configure a Do Not Disturb Softkey, on page 524

Configure a Do Not Disturb Feature Button

Follow these steps to add a Do Not Disturb feature button to your Cisco Unified IP Phone.

Procedure

	Command or Action	Purpose
Step 1	Configure Phone Button Template for Do Not Disturb, on page 523	Create a phone button template that includes the Do Not Disturb button.
Step 2	Associate a Button Template with a Phone, on page 209	Associate the Do Not Disturb button template to a phone.

Configure Phone Button Template for Do Not Disturb

Follow this procedure to configure a phone button template that includes the Do Not Disturb button.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Phone Button Template**.

Step 2 Click **Find** to display list of supported phone templates.

Step 3 Perform the following steps if you want to create a new phone button template; otherwise, proceed to the next step.

a) Select a default template for the model of phone and click **Copy**.
b) In the **Phone Button Template Information** field, enter a new name for the template.
c) Click **Save**.

Step 4 Perform the following steps if you want to add phone buttons to an existing template.

a) Click **Find** and enter the search criteria.
b) Choose an existing template.

Step 5 From the **Line** drop-down list, choose feature that you want to add to the template.

Step 6 Click **Save**.

Step 7 Perform one of the following tasks:

- Click **Apply Config** if you modified a template that is already associated with devices to restart the devices.
- If you created a new softkey template, associate the template with the devices and then restart them.

Associate a Button Template with a Phone

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** to display the list of configured phones.

Step 3 Choose the phone to which you want to add the phone button template.

Step 4 In the **Phone Button Template** drop-down list, choose the phone button template that contains the new feature button.

Step 5 Click **Save**.
A dialog box is displayed with a message to press **Reset** to update the phone settings.

Configure a Do Not Disturb Softkey

Optional. If your phone uses softkeys, perform the tasks in the following task flow to add a Do Not Disturb softkey to the phone.

Procedure

	Command or Action	Purpose
Step 1	Configure Softkey Template for Do Not Disturb, on page 525	Create a softkey template that includes the Do Not Disturb softkey.
Step 2	Perform either of the following procedures: • Associate a Softkey Template with a Common Device Configuration, on page 526 • Associate Softkey Template with a Phone, on page 527	You can associate the softkey to a Common Device Configuration and then associate that configuration to a group of phones, or you can associate the softkey template directly to a phone.

Configure Softkey Template for Do Not Disturb

Perform these steps to configure a softkey template that includes the Do Not Disturb softkey.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Softkey Template**.

Step 2 Perform the following steps to create a new softkey template; otherwise, proceed to the next step.

a) Click **Add New**.
b) Select a default template and click **Copy**.
c) Enter a new name for the template in the **Softkey Template Name** field.
d) Click **Save**.

Step 3 Perform the following steps to add softkeys to an existing template.

a) Click **Find** and enter the search criteria.
b) Select the required existing template.

Step 4 Check the **Default Softkey Template** check box to designate this softkey template as the default softkey template.

Note If you designate a softkey template as the default softkey template, you cannot delete it unless you first remove the default designation.

Step 5 Choose **Configure Softkey Layout** from the **Related Links** drop-down list in the upper right corner and click **Go**.

Step 6 From the **Select a Call State to Configure** drop-down list, choose the call state for which you want the softkey to display.

Step 7 From the **Unselected Softkeys** list, choose the softkey to add and click the right arrow to move the softkey to the **Selected Softkeys** list. Use the up and down arrows to change the position of the new softkey.

Step 8 Repeat the previous step to display the softkey in additional call states.

Step 9 Click **Save**.

Step 10 Perform one of the following tasks:

- Click **Apply Config** if you modified a template that is already associated with devices to restart the devices.

- If you created a new softkey template, associate the template with the devices and then restart them. For more information, see *Add a Softkey Template to a Common Device Configuration* and *Associate a Softkey Template with a Phone* sections.

What to do next

Perform one of the following procedures to add the softkey template to a phone.

Associate a Softkey Template with a Common Device Configuration, on page 526

Associate Softkey Template with a Phone, on page 527

Associate a Softkey Template with a Common Device Configuration

When you associate the Do Not Disturb (DND) softkey template to a Common Device Configuration you can add the DND softkey to a group of Cisco Unified IP Phones that use that Common Device Configuration.

Before you begin

Configure Softkey Template for Do Not Disturb, on page 525

Procedure

	Command or Action	Purpose
Step 1	Add Softkey Template to Common Device Configuration, on page 526	Associate the DND softkey template to a Common Device Configuration.
Step 2	Associate Common Device Configuration with Phone, on page 527	Add the DND softkey to a phone by associating the Common Device Configuration to the phone.

Add Softkey Template to Common Device Configuration

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Common Device Configuration**.

Step 2 Perform the following steps to create a new Common Device Configuration and associate the softkey template with it; otherwise, proceed to the next step.

a) Click **Add New**.
b) Enter a name for the Common Device Configuration in the **Name** field.
c) Click **Save**.

Step 3 Perform the following steps to add the softkey template to an existing Common Device Configuration.

a) Click **Find** and enter the search criteria.
b) Click an existing Common Device Configuration.

Step 4 In the **Softkey Template** drop-down list, choose the softkey template that contains the softkey that you want to make available.

Step 5 Click **Save**.

Step 6 Perform one of the following tasks:

- If you modified a Common Device Configuration that is already associated with devices, click **Apply Config** to restart the devices.
- If you created a new Common Device Configuration, associate the configuration with devices and then restart them.

Associate Common Device Configuration with Phone

Before you begin

Associate a Softkey Template with a Common Device Configuration, on page 526

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select the phone device to add the softkey template.

Step 3 From the **Common Device Configuration** drop-down list, choose the common device configuration that contains the new softkey template.

Step 4 Click **Save**.

Step 5 Click **Reset** to update the phone settings.

Associate Softkey Template with a Phone

Perform this procedure if you have configured a softkey template with the Do Not Disturb softkey and you want to associate that softkey template to a phone.

Before you begin

Configure Softkey Template for Do Not Disturb, on page 525

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** to select the phone to add the softkey template.

Step 3 From the **Softkey Template** drop-down list, choose the template that contains the new softkey.

Step 4 Click **Save**.

Step 5 Press **Reset** to update the phone settings.

Do Not Disturb Interactions and Restrictions

This section provides information about Do Not Disturb interactions and restrictions.

Interactions

The following table describes feature interactions with the Do Not Disturb (DND) feature. Unless otherwise stated, the interactions apply to both the DND Ringer Off and the DND Call Reject option.

Feature	Interaction with Do Not Disturb
Call Forward All	On Cisco Unified IP Phones, the message that indicates that the Do Not Disturb (DND) feature is active takes priority over the message that indicates that the user has new voice messages. However, the message that indicates that the Call Forward All feature is active has a higher priority than DND.
Park Reversion	For locally parked calls, Park Reversion overrides DND. If Phone A has DND turned on, and a call is parked, the park reversion to Phone A occurs and Phone A rings. For remotely parked calls, DND overrides Park Reversion: • If Phone A activates DND Ringer Off and shares a line with Phone A-prime, when Phone A-prime parks the call, park reversion on Phone A honors the DND settings and does not ring. • If Phone A activated DND Call Reject, the park reversion is not presented to Phone A.
Pickup	For locally placed Pickup requests, Pickup overrides DND. If Phone A has DND turned on, and has initiated any type of Pickup, the Pickup call presents normally, and Phone A rings. For remotely placed Pickup requests, DND overrides Pickup as follows: • If Phone A is in DND Ringer Off mode and shares a line with Phone A-prime, when Phone A-prime initiates Pickup, the Pickup call to Phone A honors the DND settings and Phone A does not ring. • If Phone A is in DND Call Reject mode, the Pickup call is not presented to Phone A.
Hold Reversion and Intercom	Hold Reversion and Intercom override DND, and the call gets presented normally.
MLPP and CER	Multilevel Precedence and Preemption (phones that are running SCCP) and Cisco Emergency Responder calls override DND. Multilevel Precedence and Preemption and Cisco Emergency Responder calls get presented normally, and the phone rings.

Feature	Interaction with Do Not Disturb
Call Back	For the originating side, callback overrides DND. When the activating device is on DND mode, the callback notification (both audio and visual) is still presented to the user. For the terminating side, DND overrides callback as follows: • When the terminating side is on DND Ringer Off, the Callback Available screen is sent after the terminating side goes off hook and on hook. • When the terminating side is on DND Call Reject, and is available, a new screen is sent to the activating device as "<DirectoryNumber> has become available but is on DND-R" if the activating device is in same cluster. Callback available notification is sent only after the terminating side disables DND Call Reject.
Pickup Notification	For the DND Ringer Off option, only visual notification gets presented to the device. For the DND Call Reject option, no notification gets presented to the device.
Hunt List	If a device in a Hunt List has DND Ringer Off activated, the call is still presented to the user. However, the DND Incoming Call Alert settings would still apply. If a device in a Hunt List has DND Call Reject activated, any calls to that Hunt List will go to the next member and will not get sent to this device.
Extension Mobility	For Extension Mobility, the device profile settings include DND incoming call alert and DND status. When a user logs in and enables DND, the DND incoming call alert and DND status settings get saved, and these settings get used when the user logs in again. **Note** When a user who is logged in to Extension Mobility modifies the DND incoming call alert or DND status settings, this action does not affect the actual device settings.

Restrictions

Some restrictions apply to DND usage, depending on the phone or device type in use.

- The following phone models and devices that are running SCCP support only the DND Ringer Off option:
  - Cisco Unified IP Phone 7940
  - Cisco Unified IP Phone 7960
  - Cisco IP Communicator

Note Cisco Unified IP Phones 7940 and 7960 that run SIP use their own implementation of Do Not Disturb, which is backward compatible.

- The following phone models and devices support only the DND Call Reject option:

- Mobile devices (dual mode)
- Remote Destination Profile
- Cisco Unified Mobile Communicator

Do Not Disturb Troubleshooting

This section provides troubleshooting information for Cisco Unified IP Phones (SCCP and SIP).

For SIP phones, use the following information for troubleshooting:

- debugs: sip-dnd, sip-messages, dnd-settings
- show: config, dnd-settings
- sniffer traces

For SCCP phones, use the following information for troubleshooting:

- debug: jvm all info
- sniffer traces

Troubleshooting Errors

The following table describes how to troubleshoot errors with Do No Disturb.

Symptom	Actions
DND softkey does not display or DND feature button does not display	• Verify that the softkey or button template for this phone includes DND. • Capture a sniffer trace and verify that the phone gets the correct softkey or button template. • Verify that the phone firmware is Version 8.3(1) or later.
BLF speed dial does not show DND status	• Verify that the BLF DND is set to enabled in Enterprise parameters. • Capture a sniffer trace and verify that the phone gets the correct notification message. • Verify that the phone firmware is Version 8.3(1) or later.

CHAPTER 38

Privacy

Privacy Overview

The Privacy feature allows you to enable or disable the capability of users with phones that share the same line (DN) to view call status and to barge into the call. You can enable or disable privacy for each phone or for all phones. By default, the system enables privacy for all phones in the cluster.

When the device that is configured for privacy registers with Cisco Unified Communications Manager, the feature button on the phone that is configured with privacy gets labeled, and the status is indicated through an icon. If the button has a lamp, it comes on.

When the phone receives an incoming call, the user makes the call private (so the call information does not display on the shared line) by pressing the Privacy feature button. The Privacy feature button toggles between On and Off.

To verify if your Cisco Unified IP Phone supports Privacy, see the user documentation for your phone model.

Privacy on Hold

Privacy on Hold allows you to enable or disable the capability of users with phones that share the same line (DN) to view call status and retrieve calls on hold.

You can enable or disable Privacy on Hold for specific phones or all the phones. Privacy on Hold activates automatically on all private calls when Privacy on Hold is enabled. By default, the system disables Privacy on Hold for all phones in the cluster.

To activate Privacy on Hold, users press the **Hold** softkey or **Hold** button while on a private call. To return to the call, users press the **Resume** softkey. The phone that puts the call on hold displays the status indicator for a held call; shared lines display the status indicators for a private and held call.

Privacy Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Generate a Phone Feature List, on page 3	Generate a report to identify devices that support the Privacy feature.
Step 2	Enable Privacy Cluster-wide, on page 532	Enable Privacy by default for all the phones in the cluster.
Step 3	Enable Privacy for a Device, on page 532	Enable Privacy for specific devices.
Step 4	Configure Privacy Phone Button Template, on page 533	Configure Privacy phone button template for a device.
Step 5	Associate Privacy Phone Button Template with a Phone, on page 533	Associate the phone button template with a user.
Step 6	Configure Shared Line Appearance, on page 534	Configure the shared line appearance.
Step 7	(Optional) Configure Privacy on Hold, on page 535	Configure Privacy on Hold.

Enable Privacy Cluster-wide

Perform these steps to enable Privacy by default for the entire cluster.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Service Parameters**.
The **Service Parameter Configuration** window appears.

Step 2 From the **Server** drop-down list, choose the server that is running the **Cisco CallManager** service.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.

Step 4 From the **Privacy Setting** drop-down list, choose **True**.

Step 5 Click **Save**.

Enable Privacy for a Device

Before you begin

Ensure that the phone model supports Privacy. For more information, see Generate a Phone Feature List, on page 3.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Specify search criteria and click **Find**.
The phone search results appear.

Step 3 Select the phone.

Step 4 From the **Privacy** drop-down list, select **Default**.

Step 5 Click **Save**.

Configure Privacy Phone Button Template

Before you begin

Enable Privacy for a Device, on page 532

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Phone Button Template**.

Step 2 Click **Find** to display list of supported phone templates.

Step 3 Perform the following steps if you want to create a new phone button template; otherwise, proceed to the next step.

a) Select a default template for the model of phone and click **Copy**.
b) In the **Phone Button Template Information** field, enter a new name for the template.
c) Click **Save**.

Step 4 Perform the following steps if you want to add phone buttons to an existing template.

a) Click **Find** and enter the search criteria.
b) Choose an existing template.

Step 5 From the **Line** drop-down list, choose feature that you want to add to the template.

Step 6 Click **Save**.

Step 7 Perform one of the following tasks:

- Click **Apply Config** if you modified a template that is already associated with devices to restart the devices.
- If you created a new softkey template, associate the template with the devices and then restart them.

Associate Privacy Phone Button Template with a Phone

Before you begin

Configure Privacy Phone Button Template, on page 533

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** to display the list of configured phones.

Step 3 Choose the phone to which you want to add the phone button template.

Step 4 In the **Phone Button Template** drop-down list, choose the phone button template that contains the new feature button.

Step 5 Click **Save**.
A dialog box is displayed with a message to press **Reset** to update the phone settings.

Configure Shared Line Appearance

Before you begin

Associate Privacy Phone Button Template with a Phone, on page 533

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.
The **Find and List Phones** window appears.

Step 2 To locate a specific phone, enter search criteria and click **Find**.
A list of phones that match the search criteria is displayed.

Step 3 Choose the phone for which you want to configure shared line appearance.
The **Phone Configuration** window is displayed.

Step 4 Click **Add a new DN link** in the Association Information area on the left side of the **Phone Configuration** window.
The **Directory Number Configuration** window appears.

Step 5 Enter the **Directory Number** and choose the **Route Partition** to which the directory number belongs.

Step 6 Configure the remaining fields in the **Directory Number Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 7 Repeat Step 3, on page 534 to Step 6, on page 534 for all the phones for which you want to create a shared line appearance.

Note Ensure that you assign the same directory number and route partition to all the phones that are part of the shared line appearance.

Configure Privacy on Hold

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Service Parameters**.
The **Service Parameter Configuration** window appears.

Step 2 From the **Server** drop-down list, choose the server that is running the Cisco CallManager service.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.

Step 4 Set the **Enforce Privacy Setting on Held Calls** service parameter to **True**.

Step 5 Click **Save**.

Privacy Restrictions

Restriction	Description
CTI	• CTI does not support Privacy through APIs that TAPI and JTAPI applications invoke. CTI generates events when Privacy is enabled or disabled from an IP phone by using the Privacy feature button. • CTI does not support Privacy on Hold through APIs that TAPI/JTAPI applications invoke. CTI generates events when a Privacy-enabled call is put on hold and when Privacy gets enabled or disabled on held calls from an IP phone by using the Privacy feature button.

CHAPTER 39

Private Line Automatic Ringdown

Private Line Automatic Ringdown Overview

The Private Line Automatic Ringdown (PLAR) feature configures a phone so that when the user goes off hook (or the NewCall softkey or line key gets pressed), the phone immediately dials a preconfigured number. The phone user cannot dial any other number from the phone line that gets configured for PLAR.

PLAR works with features such as Barge, cBarge, or single button Barge. If you use PLAR with a feature, you must configure the feature as described in the feature documentation, and you must configure the PLAR destination, which is a directory number that is used specifically for PLAR.

Private Line Automatic Ringdown Configuration Task Flow for SCCP Phones

Perform the following tasks to configure Private Line Automatic Ringdown (PLAR) on SCCP phones.

Procedure

	Command or Action	Purpose
Step 1	Create Partition, on page 538	Create a partition for the PLAR destination. The only directory number that you can assign to this partition is the PLAR destination.
Step 2	Assign Partitions to Calling Search Spaces, on page 538	Assign the partition to a unique CSS, and a CSS that includes the PLAR destination device.
Step 3	Assign Partition to the Private Line Automatic Ringdown Destination, on page 539	Assign the null partition and a CSS to your PLAR destination directory number.

	Command or Action	Purpose
Step 4	Configure Translation Pattern for Private Line Automatic Ringdown on Phones, on page 539	Create a null translation pattern and assign it to your PLAR destination directory number.

Create Partition

Create a new partition for the Private Line Automatic Ringdown (PLAR) destination. For the feature to work, only the null translation pattern that you configure for PLAR can be assigned to this partition.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **Partition**.

Step 2 Click **Add New**.

Step 3 In the **Name** field, enter a partition name and a description separated by a comma.

Step 4 Click **Save**.

Assign Partitions to Calling Search Spaces

For Private Line Automatic Ringdown (PLAR) on SCCP phones, you must configure two calling search spaces (CSS):

- The first CSS should include the new partition for the null translation pattern as well as a partition that routes to the destination phone.
- The second CSS should include only the new partition for the null translation pattern.

Before you begin

Create Partition, on page 538

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Control** > **Class of Control** > **Calling Search Space**.

Step 2 Click **Find** and select the calling search space for the PLAR destination device.

Step 3 Use the arrows to move both of the following partitions to the **Selected Partitions** list box: the new partition that you created for the null translation pattern and a partition that routes to the destination device.

Step 4 Click **Save**.

Step 5 Click **Add New**.

Step 6 Enter a name and description for the calling search space.

Step 7 Use the arrows to move the new partition to the **Selected Partitions** list box.

Step 8 Click **Save**.

Assign Partition to the Private Line Automatic Ringdown Destination

When configuring Private Line Automatic Ringdown (PLAR) on SCCP phones, assign a null partition to the directory number that you want to use as the PLAR destination.

Note Each PLAR destination directory number must have its own unique partition. Do not add any other directory numbers to the null partition that you created for the PLAR destination.

Before you begin

Assign Partitions to Calling Search Spaces, on page 538

Procedure

Step 1 In Cisco Unified CM Administration, choose **Call Routing** > **Directory Number**.

Step 2 Click **Find** and select the directory number that you want to use as the PLAR destination.

Step 3 In the **Route Partition** field, select a partition that you created for your PLAR destination.

Step 4 In the **Calling Search Space** drop-down list, select the CSS that includes both the null partition and the destination device.

Step 5 Click **Save**.

Configure Translation Pattern for Private Line Automatic Ringdown on Phones

To configure Private Line Automatic Ringdown (PLAR) on phones, configure a null translation pattern and assign the PLAR destination number to that translation pattern.

Before you begin

Assign Partition to the Private Line Automatic Ringdown Destination, on page 539

Procedure

Step 1 In Cisco Unified CM Administration, choose **Call Routing** > **Translation Pattern**.

Step 2 Click **Add New** to create a new translation pattern.

Step 3 Leave the **Translation Pattern** field empty.

Step 4 From the **Partition** drop-down list, select the new partition that you created for the null translation pattern.

Step 5 From the **Calling Search Space** drop-down list, select a calling search space that includes both the new partition and the partition for the PLAR destination device.

Step 6 In the **Called Party Transformation Mask** field, enter the PLAR destination directory number.

Step 7 Click **Save**.

Private Line Automatic Ringdown Configuration Task Flow for SIP Phones

Perform these tasks to configure Private Line Automatic Ringdown (PLAR) on SIP Phones.

Procedure

	Command or Action	Purpose
Step 1	Create SIP Dial Rule for Private Line Automatic Ringdown, on page 540	Create a SIP dial rule for PLAR.
Step 2	Assign Private Line Automatic Ringdown Dial Rule to SIP Phone, on page 540	Assign the PLAR dial rule to the phone.

Create SIP Dial Rule for Private Line Automatic Ringdown

To configure Private Line Automatic Ringdown (PLAR) on SIP phones, you must configure a SIP dial rule for your PLAR destination number.

Before you begin

Create Partition, on page 538

Assign Partitions to Calling Search Spaces, on page 538

Assign Partition to the Private Line Automatic Ringdown Destination, on page 539

Configure Translation Pattern for Private Line Automatic Ringdown on Phones, on page 539

Procedure

Step 1 In Cisco Unified CM Administration, choose **Call Routing** > **Class of Control** > **SIP Dial Rules**.

Step 2 Click **Add New**.

Step 3 From the **Dial Pattern** drop-down list, choose **7940_7960_OTHER**.

Step 4 Click **Next**.

Step 5 Enter a name and description for the dial rule.

Step 6 Click **Next**.

Step 7 In the **Pattern** field, enter a pattern that matches the PLAR destination number and click **Add PLAR**.

Step 8 Click **Save**.

Assign Private Line Automatic Ringdown Dial Rule to SIP Phone

You can configure Private Line Automatic Ringdown (PLAR) on SIP phones by assigning a PLAR-enabled SIP Dial Rule to the phone.

Before you begin

Create SIP Dial Rule for Private Line Automatic Ringdown, on page 540

Procedure

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

Step 2 Click **Find** and select the phone on which you want to configure PLAR.

Step 3 From the **SIP Dial Rules** drop-down list, choose the dial rule that you created for PLAR.

Step 4 Click **Save**.

Private Line Automatic Ringdown Troubleshooting

Troubleshooting Private Line Automatic Ringdown on SCCP Phones

Symptom	Solution
The phone goes off hook and the user hears a fast busy (reorder) tone.	Make sure that the CSS that is assigned to the PLAR translation pattern contains the partition of the PLAR destination.
The phone goes off hook and receives dial tone.	Make sure that the CSS that is assigned to the phone contains the partition of the null PLAR translation pattern.

Troubleshooting Private Line Automatic Ringdown on SIP Phones

Symptom	Solution
The phone goes off hook and the user hears fast busy (reorder) tone.	Make sure that the CSS of the SIP phone can reach the PLAR destination.
The phone goes off hook and receives a dial tone.	Make sure that the SIP Dial Rule has been created and is assigned to the phone.

CHAPTER 40

Secure Tone

Secure Tone Overview

The Secure Tone feature can configure a phone to play a secure indication tone when a call is encrypted. The tone indicates that the call is protected and that confidential information may be exchanged. The 2-second tone comprises three long beeps. If the call is protected, the tone begins to play on a protected phone as soon as the called party answers.

When the call is not protected, the system plays a nonsecure indication tone, which comprises six short beeps, on a protected phone.

Note Only callers on protected phones can hear secure and nonsecure indication tones. Callers on phones that are not protected cannot hear these tones.

The secure and nonsecure indication tones are supported on the following types of calls:

- Intracluster to IP-to-IP calls
- Intercluster protected calls
- IP-to-Time-Division-Multiplexing (TDM) calls through a protected MGCP E1 PRI gateway

For video calls, the system plays secure and nonsecure indication tones on protected devices.

Note For video calls, the user may first hear secure indication tone for the audio portion of the call and then nonsecure indication tone for overall nonsecure media.

A lock icon that is displayed on a Cisco Unified IP Phone indicates that the media are encrypted, but does not indicate that the phone has been configured as a protected device. However, the lock icon must be present for a protected call to occur.

Protected Device Gateways

You can configure only supported Cisco Unified IP Phones and MGCP E1 PRI gateways as protected devices in Cisco Unified Communications Manager.

Cisco Unified Communications Manager can also direct an MGCP Cisco IOS gateway to play secure and nonsecure indication tones when the system determines the protected status of a call.

Protected devices provide these functions:

- You can configure phones that are running SCCP or SIP as protected devices.
- Protected devices can call nonprotected devices that are either encrypted or nonencrypted. In such cases, the call specifies nonprotected and the system plays nonsecure indication tone to the phones on the call.
- When a protected phone calls another protected phone, but the media is not encrypted, the system plays a nonsecure indication tone to the phones on the call.

Secure Tone Prerequisites

- You must configure the MGCP gateway for SRTP encryption. Configure the gateway with this command: **mgcp package-capability srtp-package**.
- The MGCP gateway must specify an Advanced IP Services or Advanced Enterprise Services image (for example, c3745-adventerprisek9-mz.124-6.T.bin).

Secure Tone Configuration Task Flow

Before you begin

- Review Secure Tone Prerequisites, on page 544

Procedure

	Command or Action	Purpose
Step 1	Generate a Phone Feature List, on page 3	Generate a report to identify devices that support the Secure Tone feature.
Step 2	Configure Phone As a Protected Device, on page 545	Configure the phone as a protected device.
Step 3	Configure Directory Number for Secure Tones, on page 545	Configure multiple calls and call waiting settings for the protected device.
Step 4	Configure Secure Tone Service Parameters, on page 546	Configure service parameters.
Step 5	(Optional) Configure MGCP E1 PRI Gateway, on page 546	This configuration allows the system to pass protected status of the call between Cisco Unified IP Phone endpoints and the protected PBX phones that connect to the MGCP gateway.

Configure Phone As a Protected Device

Before you begin

Generate a Phone Feature List, on page 3

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click the phone for which you want to set secure tone parameters.
The **Phone Configuration** window is displayed.

Step 3 From the **Softkey Template** drop-down list in the Device Information portion of the window, choose **Standard Protected Phone**.

Note You must use a new softkey template without supplementary service softkeys for a protected phone.

Step 4 Set the **Join Across Lines** option to Off.

Step 5 Check the **Protected Device** check box.

Step 6 From the **Device Security Profile** drop-down list (in the Protocol Specific Information portion of the window), choose a secure phone profile that is already configured in the **Phone Security Profile Configuration** window (**System** > **Security Profile** > **Phone Security Profile**.

Step 7 Click **Save**.

What to do next

Perform one of the following procedures:

- Configure Directory Number for Secure Tones, on page 545
- Configure MGCP E1 PRI Gateway, on page 546

Configure Directory Number for Secure Tones

Before you begin

Configure Phone As a Protected Device, on page 545

Procedure

Step 1 Locate the **Association** section on the **Phone Configuration** window.

Step 2 Select **Add a new DN**.
The **Directory Number Configuration** window is displayed.

Step 3 Specify a directory number in the **Directory Number** field.

Step 4 In the **Multiple Call/Call Waiting Settings on Device [device name]** area of the **Directory Number Configuration** window, set the **Maximum Number of Calls** and **Busy Trigger** options to 1.

Step 5 Configure the remaining fields in the **Directory Number Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 6 Click **Save**.

Configure Secure Tone Service Parameters

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **System** > **Service Parameters**.

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

Step 3 From the **Service** drop-down list, choose **Cisco CallManager** .

Step 4 In the **Clusterwide Parameters (Feature - Secure Tone)** area, set the **Play Tone to Indicate Secure/Non-Secure Call Status** option to True.

Step 5 Click **Save**.

Configure MGCP E1 PRI Gateway

If you want the system to pass the protected status of the call between Cisco Unified IP Phone endpoints and the protected PBX phones that connect to the MGCP gateway, follow these steps:

Before you begin

Configure Phone As a Protected Device, on page 545

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Gateway**.

Step 2 Specify the appropriate search criteria and click **Find**.

Step 3 Choose a MGCP gateway.
The **Gateway Configuration** window appears.

Step 4 Set **Global ISDN Switch Type** to Euro.

Step 5 Configure the fields in the **Gateway Configuration** window. See the online help for more information about the fields and their configuration options.

Step 6 Click **Save**.

Step 7 Click the **Endpoint** icon that appears to the right of subunit 0 in the window. The **Enable Protected Facility IE** check box appears. Check this check box.

Secure Tone Interactions and Restrictions

Secure Tone Interactions

Feature	Interaction
Call Transfer, Conference, and Call Waiting	When the user invokes these features on a protected phone, the system plays a secure or nonsecure indication tone to indicate the updated status of the call.
Hold/Resume and Call Forward All	These features are supported on protected calls.

Secure Tone Restrictions

Restriction	Description
Cisco Extension Mobility and Join Across Line services	Cisco Extension Mobility and Join Across Line services are disabled on protected phones.
Shared-line configuration	Shared-line configuration is not available on protected phones.
Non-encrypted media	If the media between the Cisco Unified IP Phone and the MGCP E1 PRI gateway are not encrypted, the call drops.

PART XI

Custom Features

CHAPTER 41

Client Matter Codes and Forced Authorization Codes

Client Matter Codes and Forced Authorization Codes Overview

With client matter codes (CMCs) and forced authorization codes (FACs), you can effectively manage call access and accounting. CMCs assist with call accounting and billing for clients, and FACs regulate the types of calls that certain users can place.

CMCs force the user to enter a code; this action specifies that the call relates to a specific client matter. You can assign client matter codes to customers, students, or other populations for call accounting and billing purposes. FACs force the user to enter a valid authorization code that is assigned at a certain access level before the call is completed.

Client Matter Codes and Forced Authorization Codes Prerequisites

- Cisco Unified IP Phones that are running SCCP and SIP support CMC and FAC.
- The CMC and FAC tones play only on Cisco Unified IP Phones that are running SCCP or SIP; TAPI/JTAPI ports; and MGCP FXS ports.

Client Matter Codes and Forced Authorization Codes Configuration Task Flow

You can implement CMCs and FACs separately or together. For example, you may authorize users to place certain classes of calls, such as long distance calls, and also assign the class of calls to a specific client. CMC

and FAC tones sound the same to the user; if you configure both codes, the feature prompts the user to enter the FAC after the first tone and enter the CMC after the second tone.

Before you begin

- Review Client Matter Codes and Forced Authorization Codes Prerequisites, on page 551

Procedure

	Command or Action	Purpose
Step 1	To Configure Client Matter Codes, on page 552, complete the following subtasks: • Add Client Matter Codes, on page 552 • Enable Client Matter Codes, on page 553	After you finalize the list of CMCs that you plan to use, add those codes to the database and enable the CMC feature in route patterns.
Step 2	To Configure Forced Authorization Codes, on page 553, complete the following subtasks: • Add Forced Authorization Codes, on page 554 • Enable Forced Authorization Codes, on page 554	After you finalize the list of FACs and authorization levels that you plan to use, add those codes to the database and enable the FAC feature in route patterns.

Configure Client Matter Codes

Procedure

	Command or Action	Purpose
Step 1	Add Client Matter Codes, on page 552	Determine unique client matter codes that you want to use and add them to your system. Because the number of CMCs directly affects the time that is required for your system to start up, limit the number of CMCs to a maximum of 60,000. If you configure more CMCs than the maximum number, expect significant delays.
Step 2	Enable Client Matter Codes, on page 553	Enable client matter codes through a route pattern.

Add Client Matter Codes

Determine unique client matter codes that you want to use and add them to your system. Because the number of CMCs directly affects the time that is required for your system to start up, limit the number of CMCs to a maximum of 60,000. If you configure more CMCs than the maximum number, expect significant delays.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Client Matter Codes**.

Step 2 Click **Add New**.

Step 3 In the **Client Matter Code** field, enter a unique code of no more than 16 digits that the user will enter when placing a call.

Step 4 In the **Description** field, enter a client name if you want to identify the client matter code.

Step 5 Click **Save**.

Enable Client Matter Codes

Enable client matter codes through a route pattern.

Before you begin

Add Client Matter Codes, on page 552

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Route/Hunt** > **Route Pattern**.

Step 2 Perform one of the following tasks:

- To update an existing route pattern, enter search criteria, click **Find**, and choose a route pattern from the resulting list.
- To create a new route pattern, click **Add New**.

Step 3 In the **Route Pattern Configuration** window, check the **Require Client Matter Code** check box.

Step 4 Click **Save**.

Configure Forced Authorization Codes

Procedure

	Command or Action	Purpose
Step 1	Add Forced Authorization Codes, on page 554	Determine unique forced authorization codes that you want to use and add them to your system.
Step 2	Enable Forced Authorization Codes, on page 554	Enable forced authorization codes through a route pattern.

Add Forced Authorization Codes

Use this procedure to determine unique forced authorization codes that you want to use and add them to your system. To successfully route a call, the user authorization level must be equal to or greater than the authorization level that is specified for the route pattern for the call.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Forced Authorization Codes**.

Step 2 In the **Authorization Code Name** field, enter a unique name that is no more than 50 characters.

This name ties the authorization code to a specific user or group of users.

Step 3 In the **Authorization Code** field, enter a unique authorization code that is no more than 16 digits.

Users enter this code when they place a call through an FAC-enabled route pattern.

Step 4 In the **Authorization Level** field, enter a three-digit authorization level in the range of 0 to 255.

Step 5 Click **Save**.

Enable Forced Authorization Codes

Use this procedure to enable forced authorization codes through a route pattern.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Call Routing** > **Route/Hunt** > **Route Pattern**.

Step 2 Perform one of the following tasks:

- Click **Find**, and then choose a route pattern from the resulting list to update an existing route pattern.
- Click **Add New** to create a new route pattern.

Step 3 In the **Route Pattern Configuration** window, check the **Require Forced Authorization Code** check box.

Step 4 In the **Authorization Level** field, enter the authorization level value between 0 and 255.

The FAC level for the user must be greater than or equal to the configured level for the call to route successfully.

Step 5 Click **Save**.

Client Matter Codes and Forced Authorization Codes Interactions and Restrictions

Client Matter Codes and Forced Authorization Codes Interactions

Table 48: Client Matter Codes and Forced Authorization Codes Interactions

Feature	Interaction
CDR Analysis and Reporting (CAR)	CDR Analysis and Reporting (CAR) allows you to run reports that provide call details for client matter codes (CMCs), forced authorization codes (FACs), and authorization levels.
CTI, JTAPI, and TAPI applications	In most cases, your system can alert a CTI, JTAPI, or TAPI application that the user must enter a code during a call. When a user places a call, creates an ad hoc conference, or performs a consult transfer through a CMC- or FAC-enabled route pattern, the user must enter a code after receiving the tone. When a user redirects or blind transfers a call through a CMC- or FAC-enabled route pattern, the user receives no tone, so the application must send the codes to Cisco Unified Communications Manager. If your system receives the appropriate codes, the call connects to the intended party. If your system does not receive the appropriate codes, Cisco Unified Communications Manager sends an error to the application that indicates which code is missing.
Cisco Web Dialer	Web Dialer supports CMCs and FACs in the following ways: • A user can enter the destination number in the dial text box of the WD HTML page or SOAP request, and then manually enter the CMC or FAC on the phone. • A user can enter the destination number followed by the FAC or CMC in the dial text box of the WD HTML page or SOAP request. For example, if the destination number is 5555, the FAC is 111, and the CMC is 222, a user can make a call by dialing 5555111# (FAC), 5555222# (CMC), or 5555111222# (CMC and FAC). **Note** • WebDialer does not handle any validation for the destination number. The phone handles the required validation. • If a user does not provide a code or provides the wrong code, the call will fail. • If a user makes a call from the WebApp with a DN that contains special characters, the call goes successfully after stripping the special characters. The same rules do not work in SOAP UI.
Speed Dial and Abbreviated Speed Dial	You can use speed dial to reach destinations that require a FAC, CMC, dialing pauses, or additional digits (such as a user extension, a meeting access code, or a voicemail password). When the user presses the configured speed dial, the phone establishes the call to the destination number and sends the specified FAC, CMC, and additional digits with dialing pauses inserted.

Client Matter Codes and Forced Authorization Codes Restrictions

Table 49: Client Matter Codes and Forced Authorization Codes Restrictions

Restriction	Description
Analog gateways	H.323 analog gateways do not support CMCs or FACs because these gateways cannot play tones.
Call forwarding	Calls that are forwarded to a CMC- or FAC-enabled route pattern fail because no user is present to enter the code. When a user presses the CFwdALL softkey and enters a number that has CMC or FAC enabled on the route pattern, call forwarding fails. To minimize call-processing interruptions, test the number before you configure call forwarding. To do this, dial the intended forwarding number; if you are prompted for a code, do not configure call forwarding for that number. Advise users of this practice to reduce the number of complaints that result from forwarded calls that do not reach the intended destination.
Cisco Unified Mobility	Calls that originate from a SIP trunk, H.323 gateway, or MGCP gateway fail if they encounter a route pattern that requires CMCs or FACs and the caller is not configured with Cisco Unified Mobility.
Dial via Office callback number	The CMC and FAC feature on Cisco Mobility does not support an alternative number as its dial via office (DVO) callback number. The DVO callback number must be the number that is registered on the **Mobility Identity** window.
Failover calls	CMCs and FACs do not work with failover calls.
Hearing-impaired users	After dialing the phone number, hearing-impaired users should wait one or two seconds before entering the authorization or client matter code.
Localization	Cisco does not localize CMCs or FACs. The CMC and FAC features use the same default tone for any locale that is supported with Cisco Unified Communications Manager. **Note** For Cisco Mobility, CMCs and FACs are localized.
Overlap sending	The CMC and FAC features do not support overlap sending because Cisco Unified Communications Manager cannot determine when to prompt the user for the code. If you check the **Require Forced Authorization Code** or the **Require Client Matter Code** check box in the **Route Pattern Configuration** window, the **Allow Overlap Sending** check box is automatically unchecked and vice-versa.
Speed-dial buttons	You cannot configure CMCs or FACs for speed-dial buttons. You must enter the code when the system prompts you to do so.

CHAPTER 42

Custom Phone Rings

This chapter describes how to configure and upload customized phone ring types for your Cisco Unified IP Phones.

Custom Phone Rings Overview

Custom Phone Rings allows you to create customized phone rings and upload the customized files to the Cisco Unified Communications Manager TFTP server where they can be accessed by Cisco Unified IP Phones.

Cisco Unified IP Phones ship with default ring types that are implemented in hardware: Chirp1 and Chirp2. In addition, Cisco Unified Communications Manager provides the capability of uploading the following files to phones:

PCM Files

Cisco Unified Communications Manager provides a default set of phone ring sounds that are implemented in software as pulse code modulation (PCM) audio files. Each PCM file specifies a single ring type.

Ringlist.xml File

The Ringlist.xml file describes the list of ring options that are available for phones.

You can upload customized PCM audio files, such as custom ring tones and call back tones, as well as the modified Ringlist.xml file to the TFTP directory in Cisco Unified Communications Manager.

Custom Phone Rings Prerequisites

The following prerequisites apply to Custom Phone Rings:

- In order to upload your custom phone rings, the Cisco TFTP service must be running.
- Any PCM files that you want to upload must meet a set of file requirements in order to be compatible with Cisco Unified IP Phones. For details, review the topic PCM File Format Requirements, on page 559.

- The Ringlist.xml file must meet a set of formatting guidelines. For details, review the topic Ringlist.xml File Format Requirements, on page 559.

Custom Phone Rings Configuration Task Flow

Before you begin

- Review Custom Phone Rings Prerequisites, on page 557

Procedure

	Command or Action	Purpose
Step 1	Prepare Custom Phone Rings for Upload, on page 558	Create your customized PCM and Ringlist.xml files.
Step 2	Upload Custom Phone Rings to TFTP Server, on page 558	Upload customized files to the Cisco Unified Communications Manager TFTP server.
Step 3	Restart TFTP Service, on page 559	After the upload completes, restart the Cisco TFTP service.

Prepare Custom Phone Rings for Upload

Procedure

Step 1 Use the `file get tftp <tftp path>` CLI command to download the existing Ringlist.xml file, in addition to any PCM files that you want to modify.

Step 2 Create a PCM file for each ring type that you want to upload. For guidelines on PCM file compatibility with Cisco Unified Communications Manager, see PCM File Format Requirements, on page 559.

Step 3 Use an ASCII editor to update the Ringlist.xml file with your new phone rings. For details on Ringlist.xml file formatting requirements, see Ringlist.xml File Format Requirements, on page 559.

Upload Custom Phone Rings to TFTP Server

Before you begin

Prepare Custom Phone Rings for Upload, on page 558

Procedure

Step 1 From Cisco Unified OS Administration, choose **Software Upgrades** > **TFTP** > **File Management**.

Step 2 Click **Upload File**.

Step 3 Click **Browse** and select the Ringlist.xml file, as well as any PCM files that you want to upload.

Step 4 Click **Upload File**.

Restart TFTP Service

Before you begin

Upload Custom Phone Rings to TFTP Server, on page 558

Procedure

Step 1 Log in to Cisco Unified Serviceability and choose **Tools** > **Control Center - Feature Services**.

Step 2 From the **Server** drop-down list, choose the server on which the Cisco TFTP service is running.

Step 3 Click the radio button that corresponds to the **Cisco TFTP** service.

Step 4 Click **Restart**.

PCM File Format Requirements

PCM files for phone rings must meet a set of requirements for proper playback on Cisco Unified IP Phones. When creating or modifying your PCM files, you can use any standard audio editing packages that support the following file format requirements:

- Raw PCM
- 8000 samples per second
- 8 bits per sample
- mu-law compression
- Maximum ring size: 16080 samples
- Number of samples in the ring must be evenly divisible by 240
- Ring starts and ends at the zero crossing

Ringlist.xml File Format Requirements

The Ringlist.xml file defines an XML object that contains a list of phone ring types. Each ring type contains a pointer to the PCM file that is used for that ring type and the text that will display on the Ring Type menu on a Cisco Unified IP Phone for that ring.

The CiscoIPPhoneRinglist XML object uses the following simple tag set to describe the information:

```
<CiscoIPPhoneRinglist>   <Ring>
      <DisplayName/>
      <FileName/>
   </Ring>
</CiscoIPPhoneRinglist>
```

The following characteristics apply to the definition names:

- DisplayName defines the name of the custom ring for the associated PCM file that will display on the Ring Type menu of the Cisco Unified IP Phone.
- FileName specifies the name of the PCM file for the custom ring to associate with DisplayName.

Tip The DisplayName and FileName fields must not exceed 25 characters.

The following example shows a Ringlist.xml file that defines two phone ring types:

```
<CiscoIPPhoneRinglist>   <Ring>
      <DisplayName>Analog Synth 1</DisplayName>
      <FileName>Analog1.raw</FileName>
   </Ring>
   <Ring>
      <DisplayName>Analog Synth 2</DisplayName>
      <FileName>Analog2.raw</FileName>
   </Ring>
</CiscoIPPhoneRinglist>
```

Tip You must include the required DisplayName and FileName for each phone ring type. The Ringlist.xml file can include up to 50 ring types.

CHAPTER 43

Music On Hold

Music On Hold Overview

Use the integrated Music On Hold (MOH) feature to place on-net and off-net users on hold with music from a streaming source. This source makes music available to any on-net or off-net device that you place on hold. On-net devices include station devices and applications that an interactive voice response (IVR) or call distributor places on hold, consult hold, or park hold. Off-net users include those users who are connected through Media Gateway Control Protocol (MGCP) or Skinny Call Control Protocol (SCCP) gateways, Cisco IOS H.323 gateways, and Cisco IOS Media Gateway Control Protocol gateways. The system also makes the Music On Hold feature available for Cisco IP POTS phones that connect to the Cisco IP network through Foreign Exchange Station (FXS) ports on Cisco IOS H.323 or MGCP and for Cisco MGCP or SCCP gateways.

Start Cisco Unified Communications Manager to create a media resource manager. Music On Hold server registers to the media resource manager with its music on hold resources. Music On Hold server is a software application that provides music on hold audio sources and connects a music on hold audio source to multiple streams.

When an end device or feature places a call on hold, Cisco Unified Communications Manager connects the held device to a music resource. When the held device is retrieved, it disconnects from the music on hold resource and resumes normal activity.

Caller-Specific Music On Hold

For SIP calls that a phone receives over the SIP trunk, Cisco Unified Communications Manager can use a different MOH audio source.

An external application, such as the Cisco Unified Customer Voice Portal (CVP) contact center solution, determines the most appropriate MOH audio source based on the caller ID, dialed number, or IVR interaction when a call is received from the public switched telephone network (PSTN).

For details, see the Cisco Unified Customer Voice Portal documentation at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html.

Increased Capacity of IP Voice Media Streaming Application and Expanded MOH Audio Source

Cisco IP Voice Media Streaming application is installed automatically when you install Cisco Unified Communications Manager. Activate this application to enable the Music On Hold (MOH) feature.

With this release, the capacity of Cisco Unified Communications Manager to support unique and concurrent MOH audio sources, while the Music On Hold service is running on the MOH server, is increased from 51 to 501. The MOH audio sources are numbered from 1 to 501 with the fixed MOH audio source remaining at the number 51.

The fixed MOH device cannot use an audio source that connects through a USB MOH device, because Cisco Unified Communications Manager does not support USB when running on VMware. Use of the fixed MOH USB device is not supported on VMware. However, provision the external sound device for use with deployments that utilize Cisco Unified Survivable Remote Site Telephony (SRST) multicast MOH.

You can configure each MOH audio source to use a custom announcement as an initial greeting and/or an announcement that is played periodically to callers who are hearing the music. Cisco Unified Communications Manager provides 500 custom announcements that you can use on one or multiple MOH audio sources. These announcements are not distributed between the Cisco Unified Communications Manager servers within a cluster. You have to upload these custom announcement files to each server that provides the MOH and announcement services. You must also upload each custom music file for MOH audio sources to each server.

Performance Impact of Media Devices with Services

The Cisco IP Voice Media Streaming application runs as a service for four media devices—annunciator (ANN), software conference bridge, Music On Hold (MOH), and software media termination point. Activate this service on a Cisco Unified Communications Manager server as coresident with call processing. When you activate this service, ensure that you configure these media devices for limited capacity to avoid any impact on the call processing. The default settings for the media devices are defined based on this coresident operation. You can adjust these settings by reducing the use of one or more media devices to increase other settings.

For example, if you are not using software media termination point devices, you can choose the **Run Flag** setting for the SW MTP to **False**, select **System** > **Service Parameters** > **Cisco IP Voice Media Streaming App service** > **MTP Parameters** , and add the **MTP Call Count** setting to **Media Resource** > **MOH Server** > **Maximum Half Duplex Streams** configuration. Depending on the call traffic, you can modify the default settings. However, monitor the server performance activity for CPU, memory, and IO wait. For higher capacity clusters, such as the ones using 7500 user OVA configuration, it is possible to increase the default media device settings for Call Count by 25%.

For installations where you expect high usage of the media devices, such as Music On Hold, or where high call volumes require higher number of media connections, activate the Cisco IP Voice Media Streaming application service on one or more of the Cisco Unified Communications Manager servers which do not have call processing activated. Activating this service limits the impact of media device usage to other services, such as call processing. Then, you can increase the configuration settings for maximum number of calls for the media devices.

When you activate Cisco IP Voice Media Streaming application as co-resident with Cisco Unified Communications Manager service, it can impact call processing performance. To increase the capacity settings for Music On Hold or annunciator from the default settings, it is suggested to activate Cisco IP Voice Media Streaming application on a server without activating Cisco Unified Communications Manager.

The CPU performance is impacted by MOH when active callers are on hold or when multicast MOH audio streams are configured.

Table 50: General Performance Results

Configuration Notes	CPU Performance
Dedicated MOH server, 1000 held calls, 500 MOH sources with greeting and periodic announcements.	25–45% (7500 user OVA configuration)
Native call queuing with dedicated MOH server and annunciator server, 1000 queued calls, 500 MOH sources with greeting and periodic announcements. An annunciator can play up to 300 simultaneous greeting announcements.	25–45% (7500 user OVA configuration)
Dedicated MOH server, 500 held calls, 500 MOH sources with greeting and periodic announcements.	15–35% (7500 user OVA configuration)

Table 51: Extrapolated Recommendations

Configuration	Recommendation Limit
When Cisco IP Voice Media Streaming application is co-resident with Cisco Unified Communications Manager on 2500 OVA (moderate call processing).	MOH: 500 held callers, 100 MOH sources, and 48 to 64 annunciator callers.
When Cisco IP Voice Media Streaming application is a dedicated server on 2500 OVA.	MOH: 750 held callers, 250 MOH sources, and 250 annunciator callers.
When Cisco IP Voice Media Streaming application is co-resident with Cisco Unified Communications Manager on 7500/10K OVA (moderate call processing).	MOH: 500 held callers, 250 MOH sources, and 128 annunciator callers.
When Cisco IP Voice Media Streaming application is a dedicated server on 7500/10K OVA.	MOH: 1000 held callers, 500 MOH sources, and 300-700 annunciator callers (with 1 MOH codec). **Note** Reduce annunciator to 300 for two MOH codecs.

Note These recommendations are specific to MOH/ANN devices. If you combine these devices with the software media termination point (MTP) and call forward busy (CFB) devices, reduce the limits to provide streams.

Configuration Limitations for Capacity Planning

The Cisco IP Voice Media Streaming application and Self Provisioning IVR services use a media kernel driver to create and control Real-time Transfer Protocol (RTP) streams. This media kernel driver has a capacity of 6000 streams. These streams allow the media devices and IVR to make resource reservations.

These reservations are based on the following capacity calculations:

Media Device	Capacity
Annunciator	(Call Count service parameter) * 3 Where 3 indicates total of receiving (RX) and transmitting (TX) calls for endpoint and 1 for .wav file.
Software Conference Bridge	(Call Count service parameter) * 2 Where 2 indicates total streams of RX and TX endpoints.
Software Media Termination Point	(Call Count service parameter) * 2 Where 2 indicates total streams of RX and TX endpoints.
Music On Hold	((Maximum Half Duplex Streams) * 3) + (501 * 2 * [number of enabled MOH codecs]) Where: • (Maximum Half Duplex Streams) is a configuration setting on the MOH device configuration administration web page. • 3 indicates total steams of RX, TX, and greeting announcement .wav file. • 501 indicates the maximum number of Music On Hold (MOH) sources. • 2 indicates music .wav stream and possible multicast TX stream. • [number of enabled MOH codecs] is based on how many MOH codecs are enabled in the Cisco IP Voice Media Streaming application service parameters.
Self Provisioning IVR Service	(500 * 2) Where 500 indicates callers, and 2 indicates total streams from RX and TX streams.

Hence, to enable MOH to support a maximum of 1000 callers, use the following equation: `1000 * 3 + 501 * 2 * 1 = 4002` driver streams with one enabled codec and `1000 * 3 +501 * 2 * 2 = 5004` with two enabled codecs. Reduce the remaining devices and deactivate the Self Provisioning IVR service to limit total reservations to 6000, which allows the MOH device to make these reservations. It may also require that you do not activate the Self Provisioning IVR service on the same server with Cisco IP Voice Media Streaming application.

If configuration settings of the media devices exceed the capacity of the media device driver, the media devices that register with the device driver first will be able to reserve their required stream resources. The media devices that register later are restricted to fewer than requested stream resources. The later registered media devices result in logging some alarm messages and automatically reducing the call count for the restricted media device.

Note A media kernel driver with a capacity of 6000 streams might not support that many simultaneous media device connections.

Music On Hold Prerequisites

- Before you configure multicast, ensure that you configure MOH server and audio sources. If you want to use fixed audio source, configure it before you configure multicast.
- Make sure to decide whether you are going to do unicast or multicast Music On Hold
- It is crucial to plan the capacity of the deployed and configured hardware and ensure that it can support the anticipated call volume of the network. You need to know the hardware capacity for MOH resources and consider the implications of multicast and unicast MOH in relation to this capacity. Ensure that network call volumes do not exceed these limits. When MOH sessions reach these limits, an additional load can result in poor MOH quality, erratic MOH operation, or loss of MOH functionality.
- If you use multicast MOH and the devices that listen to multicast MOH streams are not in the same IP network, you must enable multicast routing in the IP network. Take care when you enable the multicast routing to avoid the potential flooding of parts of the network with wrongly sent multicast packets (specially, across WAN links). Disable multicasts on interfaces on which the multicast MOH packets are not required and use the Max Hops parameter.
- For detailed information on planning your Music On Hold deployment, including server capacities, refer to the Music On Hold capacities topics in the *Cisco Collaboration System Solution Reference Network Design*.

Music On Hold Configuration Task Flow

Before you begin

- Review Music On Hold Prerequisites, on page 565

Procedure

	Command or Action	Purpose
Step 1	Enable Music On Hold. See Activate Cisco IP Voice Media Streaming, on page 567.	Enable the Music On Hold service.
Step 2	Configure Music On Hold server. See Configure Music On Hold Server, on page 567.	Stream Music on Hold from Music On Hold data source files that are stored on their disks or external audio source.
Step 3	Configure MOH audio. See Music On Hold Audio Source Configuration, on page 571, and perform the following subtasks: • Upload an MOH audio file. See Upload Audio File for Music On Hold, on page 571. • Convert MOH Files. See Convert Music On Hold Files, on page 572.	• Upload a Music On Hold audio file to make it available for use as a Music on Hold audio source. • Convert the Music On Hold file to the appropriate formats for use by the Music On Hold server.

	Command or Action	Purpose
	• Configure MOH audio source. See Configure Music On Hold Audio Source, on page 572.	• To place on-net and off-net users on hold (end user hold or network hold) with music streamed from a streaming source.
Step 4	(Optional) Configure fixed MOH audio source. See Configure Fixed Music On Hold Audio Source, on page 577.	Configure the fixed MOH audio source in addition to the file stream sources.
Step 5	Configure Media Resource Group. See Add MOH to Media Resource Group, on page 579.	Define logical groupings of media servers.
Step 6	Configure Media Resource Group list. See Configure Media Resource Group List, on page 579.	Specify a list of prioritized media resource groups.
Step 7	View MOH audio file. See View Music on Hold Audio File, on page 580.	View a list of Music On Hold audio files that are stored on the system.
Step 8	Enable security for MOH. See Enable Security for Music On Hold, on page 580.	Enable security for Music On Hold devices through the **Cluster Security Mode** enterprise parameter.
Step 9	(Optional) Enable secured MOH through SRTP. See Enable Secured Music On Hold through SRTP, on page 581.	When you enable the Cisco Unified Communications Manager cluster or system for security, the MOH server registers with the Cisco Unified Communications Manager as an SRTP-capable device.
Step 10	Configure multicast by performing the following subtasks: • Plan MOH Server capacity. See Plan Music On Hold Server Capacity, on page 583. • Verify Music On Hold service parameters. See Configure MOH Service Parameters, on page 584. • Configure multicast Music On Hold audio sources or fixed MOH audio source. See Configure Multicast Music On Hold Audio Sources/Fixed MOH Audio Source, on page 585. • Configure multicast Music On Hold server. See Configure Multicast Music On Hold Server, on page 585. • Configure a multicast-enabled media resource group. See Configure a Multicast-Enabled Media Resource Group, on page 587. • Configure multicast Music On Hold over H.323 intercluster trunks. See Configure	Configure the various Cisco Unified Communications Manager services to allow multicasting. For details on unicast and multicast audio sources, see Unicast and Multicast Audio Sources, on page 582.

	Command or Action	Purpose
	Multicast Music On Hold over H.323 Intercluster Trunks, on page 587.	
Step 11	(Optional) Reset or restart a Music On Hold server. See Reset or Restart a Music On Hold Server, on page 588.	Reset or restart a music on hold server for changes to take effect, if required.
Step 12	(Optional) Synchronize Music On Hold server. See Synchronize Music On Hold Server, on page 588.	Apply configuration to the selected music on hold servers.

Activate Cisco IP Voice Media Streaming

The **Cisco IP Voice Media Streaming Application** service must be **Activated** in order to use Music On Hold.

Note During installation, Unified Communications Manager installs and configures a default Music On Hold audio source. Music On Hold functionality can proceed by using the default audio source.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Tools** > **Service Activation**.

Step 2 Choose a server from the **Server** drop-down list.

Step 3 Under **CM Services** , make sure the **Cisco IP Voice Media Streaming App** service is **Activated**. If the service is deactivated, check the service and click **Save**.

Configure Music On Hold Server

Before you begin

Make sure one or multiple Music On Hold (MOH) servers are available.

Note The Cisco Unified Communications Manager MOH server is automatically added when the **Cisco IP Voice Media Streaming Application** service is activated.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **Music On Hold Server**.

Step 2 Click **Find** and select the Music On Hold server that you want to update.

Step 3 Select the **Host Server**.

Step 4 Enter a descriptive **Music On Hold Server Name** along with a **Description**.

Step 5 Select the **Device Pool** you want to use for this server.

Step 6 Configure server capacity by configuring the following fields:

- **Maximum Half Duplex Stream**—Set this to the maximum number of devices that can be on unicast music on hold that is streamed from this music on hold server at any given time. You can use the following formula to calculate the maximum:

  Note `(Server and deployment capacity) - ([Number of multicast MOH sources] * [Number of enabled MOH codecs])`

- **Maximum Multi-cast Connections**—Set this to a value that is greater than or equal to the number of devices that might be placed on multicast MOH at any given time.

Step 7 (Optional) To enable multi-casting, check the **Enable Multi-cast Audio Sources on this MOH Server** check box, and configure the multicast IP address ranges.

Step 8 Configure the additional fields in the **Music On Hold Server Configuration** window. For help with the fields and their settings, see the online help.

Step 9 Click **Save**.

Music On Hold Server Fields for Music On Hold

Table 52: Device Information

Field	Description
Registration	Displays the registration information of the device.
IPv4 Address	Displays the IPv4 address.
IPv6 Address	Displays the IPv6 address.
Device is trusted	If the device is trusted, a green checkmark appears.
Host Server	Displays the IP address of the existing host server.
Music On Hold Server Name	Enter a unique name for the MOH server. The name can comprise up to 15 characters. You can form the name by using letters, numbers, spaces, dashes, dots (periods), and underscores.
Description	Enter a description for the MOH server. The description can include up to 50 characters. Ensure that this field does not contain ampersand (&), double quotes (“), brackets ([]), less than (<), greater than (>), or the percentage (%).
Device Pool	Choose a device pool for the Music On Hold server from the drop-down arrow and choose a device pool from the list that appears.

Field	Description
Location	Use locations to implement call admission control (CAC) in a centralized call-processing system. CAC enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between locations. The location specifies the total bandwidth that is available for calls to and from this location. From the drop-down list, choose the appropriate location for this MOH server. The **Hub_None** location field indicates that the locations feature does not keep track of the bandwidth that this MOH server consumes. The **Phantom** location field indicates a location that enables successful CAC across intercluster trunks that use H.323 or SIP protocol. To configure a new location, use the **System** > **Location** menu option.
Maximum Half Duplex Streams	Enter a number in this required field for the maximum number of unicast Music On Hold streams that this Music On Hold server supports. This value determines the maximum number of devices that can be on unicast Music On Hold that is streamed from this Music On Hold server at any given time. Valid values range from 0 to 1000.
Maximum Multi-cast Connections	Enter a number in this required field for the maximum number of multicast Music On Hold streams that this Music On Hold server supports. This value determines the maximum number of devices that can be on multicast music on hold that is streamed from this Music On Hold server at any given time. Valid values range from 1 to 999999.
Fixed Audio Source Device	Enter the device name of the fixed audio source device. This device serves as the per-server override that is used if the server has a special sound device installed.

Field	Description
Use Trusted Relay Point	From the drop-down list, enable or disable whether Cisco Unified Communications Manager inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values: • **Off**—Disables the use of a TRP with this device. • **On**—Enables the use of a TRP with this device. A trusted relay point (TRP) device designates an Media Transfer Protocol (MTP) or transcoder device that is labeled as Trusted Relay Point. Cisco Unified Communications Manager places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent). If both TRP and MTP are required for the endpoint, TRP is used as the required MTP. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified Communications Manager first tries to find an RSVPAgent that can also be used as a TRP. If both TRP and transcoder are needed for the endpoint, Cisco Unified Communications Manager first tries to find a transcoder that is also designated as a TRP.
Run Flag	Use this required field to choose a run flag for the Music On Hold server. To do so, click the drop-down arrow and choose Yes or No. Choosing No disables the music on hold server.

Table 53: Multicast Audio Source Information

Field	Description
Enable Multicast Audio Sources on this MOH Server	Check or uncheck this check box to enable or disable the multicast of audio sources for this Music On Hold server. **Note** If this MOH server belongs to a multicast media resource group, a message asks you to enable multicast on this MOH server or to update the specified media resource groups either by removing this MOH server or by changing the multicast field of each listed group.
Base Multicast IP Address	If multicast support is needed, enter the base multicast IP address in this field. Valid IP addresses for multicast range from 224.0.1.0 to 239.255.255.255. **Note** IP addresses between 224.0.1.0 and 238.255.255.255 are in the reserved range of IP multicast addresses for public multicast applications. Use of these addresses may interfere with existing multicast applications on the Internet. We strongly recommend using IP addresses that are in the range that is reserved for administratively controlled applications on private networks (239.0.0.0 – 239.255.255.255).

Field	Description
Base Multicast Port Number	If multicast support is needed, enter the base multicast port number in this field. Valid multicast port numbers include even numbers that range from 16384 to 32766.
Increment Multicast on	Click **Port Number** to increment multicast on port number. Click **IP Address** to increment multicast on IP address. **Note** Use multicast by incrementing IP address as the preferred method in firewall situations. This results in a unique IP address for each multicast audio source and helps to avoid network saturation.

Table 54: Selected Multicast Audio Sources

Field	Description
No.	This field designates Music On Hold audio stream number that is associated with a particular multicast audio source. Only audio sources that are defined as allowing multicasting appear.
Audio Source Name	This field designates the name of the audio source that is defined to allow multicasting.
Max Hops	For each multicast audio source, enter the maximum number of router hops through which multicast packets should pass. Valid values range from 1 to 127. **Note** Using high values can lead to network saturation. This field also gets identified as Time to Live.

Music On Hold Audio Source Configuration

Upload Audio File for Music On Hold

Use this procedure if you want to upload customized audio files that you can make available as Music On Hold audio streams.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **MOH Audio File Management**.

Step 2 Click **Upload File**.

Step 3 Click **Choose File** and browse to the file you want to upload. Once you've selected the file, click **Open**.

Step 4 Click **Upload**.

The **Upload Result** window shows the result of the upload. The uploading procedure uploads the file and performs audio conversions to create codec-specific audio files for MOH. Depending on the size of the original file, processing may take several minutes to complete.

Step 5 Click **Close** to close the **Upload Result** window.

Step 6 Repeat this procedure if you want to upload additional audio files.

Note When you import an audio source file, Cisco Unified Communications Manager processes the file and converts the file to the proper formats for use by the Music On Hold server. Followoing are examples of valid input audio source files:

- 16-bit PCM .wav file
- Stereo or mono
- Sample rates of 48 kHz, 44.1 kHz, 32 kHz, 16 kHz, or 8 kHz

Note MOH audio source files do not automatically propagate to other MOH servers in a cluster. You must upload an audio source file to each MOH server or each server in a cluster separately

Convert Music On Hold Files

When you import an audio source file, Cisco Unified Communications Manager processes the file and converts the file to the proper formats for use by the Music On Hold server.

These are some examples of a valid input audio source files:

- 16-bit PCM .wav file
- Stereo or mono
- Sample rates of 48 kHz, 44.1 kHz, 32 kHz, 16 kHz, or 8 kHz

Before you begin

Upload Audio File for Music On Hold, on page 571

What to do next

- Configure Music On Hold Audio Source, on page 572

Configure Music On Hold Audio Source

Use this procedure to configure Music On Hold audio sources. You can configure audio streams and associate uploaded files to an audio stream. You can configure up to 500 audio streams.

Note If a new version of an audio source file is available, perform the update procedure to use the new version.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **Music On Hold Audio Source**.

Step 2 Do either of the following:

- Click **Find** and select an existing audio stream.
- Click **Add New** to configure a new stream.

Step 3 From the **MOH Audio Stream Number**, select an audio stream.

Step 4 Enter a unique name in the **MOH Audio Source Name** field.

Step 5 Optional. Check the **Allow Multi-casting** check box if you want to allow this file to be multi-casted.

Step 6 Configure the audio source:

- Check the **Use MOH WAV file** source radio button and from the **MOH Audio Source File**, select the file you want to assign.
- Check the **Rebroadcast External Multicast Source** radio button and enter the multicast source IP Address details.

Step 7 In the **Announcement Settings for Held and Hunt Pilot Calls** section, assign the announcements that you want to use for this audio source.

Step 8 Configure the remaining fields in the **Music On Hold Audio Source Configuration** window. For help with the fields and their settings, see the online help.

Step 9 Click **Save**.

Audio Source Fields for Music On Hold

Table 55: Music On Hold Audio Source Information

Field	Description
MOH Audio Stream Number	Use this field to choose the stream number for this MOH audio source. Click the drop-down arrow and choose a value from the list. For existing MOH audio sources, the value appears in the MOH Audio Source title.
MOH Audio Source File	Use this field to choose the file for this MOH audio source. Click the drop-down arrow and choose a value from the list.
MOH Audio Source Name	Enter a unique name in this field for the MOH audio source. This name includes up to 50 valid characters, such as letters, numbers, spaces, dashes, dots (periods), and underscores.
Allow Multicasting	Check this check box to specify that the selected MOH audio source allows multicasting.

Field	Description
MOH Audio Source File Status	This pane displays the following information about the source file for the selected MOH audio source: • InputFileName • ErrorCode • ErrorText • DurationSeconds • DiskSpaceKB • LowDateTime • HighDateTime • OutputFileList • MOH Audio Translation completion date **Note** OutputFileList includes information on ULAW, ALAW, G.729, and Wideband wav files and status options.

Table 56: Announcement Settings

Field	Description
Initial Announcement	Choose an initial announcement from the drop-down list. **Note** To select MoH with no initial announcement, choose the **Not Selected** option. Click the **View Details** link to view the following Initial Announcement information: • Announcement Identifier • Description • Default Announcement **Note** • Played by MOH server only when the Audio Source has “Allow Multi-casting” unchecked and “Initial Announcement Played” set to 'Only for queued calls'. • Played by ANN if “Allow Multi-casting” is checked or if “Initial Announcement Played” is set to 'Always.'

Field	Description
Initial Announcement Played	Choose one of the following to determine when to play the initial announcement: • Play announcement before routing to Hunt Member • Play announcement if call is queued
Periodic Announcement	Choose a periodic announcement from the drop-down list. **Note** To select MoH with no periodic announcement, choose the **Not Selected** option. Click the **View Details** link to view the following Periodic Announcement information: • Announcement Identifier • Description • Default Announcement **Note** Initial announcements are always simulcast to each new caller. Periodic announcements are multicast to queued callers at the specified time interval. Callers who join the queue after the periodic announcement has begun to play may only hear a portion of the announcement.
Periodic Announcement Interval	Enter a value (in seconds) that specifies the periodic announcement interval. Valid values are 10 to 300. The default value is 30.
Locale Announcement	Locale Announcement depends upon the locale installation package that has been installed. **Note** • Prompts played by MOH will use the setting for Locale Announcement. • Prompts played by ANN will use the User Locale of the calling party.

Table 57: Music On Hold Audio Sources

Field	Description
(list of MoH audio sources)	This list box shows the MOH audio source that you add. Select the audio stream number of an MOH audio source to configure that MoH audio source. Audio source ID is an ID that represents an audio source in the Music On Hold server. The audio source can include either a file on a disk or a fixed device from which a source stream Music On Hold server obtains the streaming data. An MOH server can support up to 51 audio source IDs. Each audio source, represented by an audio source ID, can stream as unicast and multicast mode, if needed. **Note** If you select **<None>** , the system default MoH audio source service parameter (**Default Network Hold MoH Audio Source ID**) is used for the MoH audio source.
Upload File	To upload an MOH audio source file that does not appear in the drop-down list, click **Upload File**. In the **Upload File** window, either enter the path of an audio source file or navigate to the file by clicking **Browse**. After you locate the audio source file, click the **Upload File** button to complete the upload. After the audio file gets uploaded, the Upload Result window displays the result of the upload. Click **Close** to close this window. **Note** When you upload a file, the file is uploaded to the Cisco Unified Communications Manager server and performs audio conversions to create codec-specific audio files for MOH. Depending on the size of the original file, processing may take several minutes to complete. **Note** Uploading an audio source file to an MOH server uploads the file only to one MOH server. You must upload an audio source file to each MOH server in a cluster by using Cisco Unified Communications Manager Administration on each server. MOH audio source files do not automatically propagate to other MOH servers in a cluster.

Configure Fixed Music On Hold Audio Source

For each cluster, you may define one fixed audio source (Source 51). You must set up the fixed audio source that is configured per cluster on each MOH server. The fixed audio source originates from a fixed device that uses the local computer audio driver.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **Fixed MOH Audio Source**.

Step 2 Optional. Check the **Allow Multi-casting** check box if you want to allow this audio source to be multi-casted.

Step 3 Check the **Enable** check box to enable the fixed audio source. When you check this check box, a **Name** is required.

Step 4 In the **Announcement Settings for Held and Hunt Pilot Calls** area, configure announcements for this audio source.

Step 5 Configure the fields in the **Fixed MOH Audio Source Configuration** window. For help with the fields and their settings, see the online help.

Step 6 Click **Save**.

Fixed Music on Hold Audio Source Fields for Music On Hold

Table 58: Fixed MOH Audio Source Information

Field	Description
Source ID	This field displays the stream number for this fixed MOH audio source.
Name	Enter a unique name in this field for the fixed MOH audio source. This name can comprise up to 50 characters. Valid characters include letters, numbers, spaces, dashes, dots (periods), and underscores. **Note** For virtual servers, the fixed Music On Hold device cannot specify an audio source that connects through a Universal Serial Bus (USB), because Cisco Unified Communications Manager does not support USB when running on VMware. Internal Music On Hold is supported on VMware.
Allow Multi-casting	Check this check box to specify that this fixed MOH audio source allows multicasting.
Enable (If checked, Name is required.)	To enable this fixed MOH audio source, check this check box.

Table 59: Announcement Settings for Held and Hunt Pilot Calls

Field	Description
Initial Announcement	Choose an initial announcement from the drop-down list box. **Note** To select MOH with no initial announcement, choose the default option, which is **`Not Selected`**. Select **View Details** to view the following Initial Announcement information: • Announcement Identifier • Description • Default Announcement **Note** To disable Initial Announcement completely, set Initial Announcement to **`Not Selected`** and set Initial Announcement Played to **`Only for Queued Calls`**.
Initial Announcement for queuing-enabled Hunt Pilot calls	Choose one of the following options from the drop-down list: • Play announcement before routing to Hunt Member • Play announcement if call is queued
Periodic Announcement	Choose a periodic announcement from the drop-down list: **Note** To select MOH with no periodic announcement, choose the default option, which is **`Not Selected`**. Click the **View Details** link to view the following Periodic Announcement information: • Announcement Identifier • Description • Default Announcement
Periodic Announcement Interval	Enter a value (in seconds) that specifies the periodic announcement interval. Valid values specify 10 to 300. The default value is 30.
Locale Announcement	Locale Announcement depends upon the locale installation package that has been installed.

Add MOH to Media Resource Group

A Media Resource Group is a logical grouping of media resources. You may associate a media resource group with a geographical location or a site, as required. You can also form media resource groups to control server usage, or unicast or multicast service type.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **Media Resource Group**.

Step 2 Do either of the following:

- Click **Find** and select an existing group.
- Click **Add New** to create a new group.

Step 3 Enter a **Name** and **Description**.

Step 4 In the **Available Media Resources** list, select the Music On Hold resource and use the down arrow to add the resource to the **Selected Media Resources**. Repeat this step for the other media resources you want to assign to this group.

Step 5 (Optional) Check the **Use Multi-cast for MOH Audio** check box if you want to allow Music On Hold multi-casting.

Step 6 Click **Save**.

Configure Media Resource Group List

Media Resource Group List lists the prioritized media resource groups. An application can select required media resources from among ones that are available according to the priority order that is defined in a media resource group list.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **Media Resource Group List**.

Step 2 Do either of the following:

- Click **Find** and select an existing media resource group list.
- Click **Add New** to create a new media resource group list.

Step 3 Enter a **Name** for the list.

Step 4 From the **Available Media Resource Groups** list, select the groups you want to add to this list and use the down arrow to move them to **Selected Media Resource Groups**.

Step 5 In the **Selected Media Resource Groups** list use the up and down arrows to the right of the list to edit the prioritized order of groups.

Step 6 Click **Save**.

View Music on Hold Audio File

View existing Music On Hold audio files that are stored on the system.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Media Resources** > **MOH Audio File Management**. The **Music On Hold Audio File Management** window appears.

Step 2 View the following information for each record:

- **Check box**—If the audio file can be deleted, a check box appears before the **File Name** column.
- **File Name**—This column displays the audio file name.
- **Length**—This column displays the audio file length in minutes and seconds.
- **File Status**—This column displays one of the following statuses of an audio file:
  - **Translation Complete**—This status appears after a file is uploaded successfully and is available for use as audio files for a music on hold audio source.
  - **In Use**—This status appears after you add a Music On Hold audio source that uses this audio file as its MOH audio source file.

    Note You cannot a delete a file with **In Use** status.

Enable Security for Music On Hold

You can enable the security mode of an MOH server in a cluster. Select a value in the **Cluster Security Mode** enterprise parameter so that the Music On Hold devices are automatically enabled for security. Enter one of the following values for this parameter:

- **0**—Implies Non Secure, which means that the cluster allows the phones to register with no security.
- **1**—Implies Mixed, which means that the cluster allows the registration of both secure devices and non-secure devices.

Note The **Cluster Security Mode** enterprise parameter is a noneditable parameter. To change the cluster security mode, you must run the Certificate Trust List (CTL) Client plugin. Then, you must restart Cisco Unified Communications Manager for the parameter change to take effect.

Before you begin

View Music on Hold Audio File, on page 580

Procedure

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

Step 2 In the **Security Parameters** section, set the **Cluster Security Mode** option to `1`.

What to do next

(Optional) Enable Secured Music On Hold through SRTP, on page 581

Configure multicast by performing the following subtasks:

- Plan Music On Hold Server Capacity, on page 583
- Configure MOH Service Parameters, on page 584
- Configure Multicast Music On Hold Audio Sources/Fixed MOH Audio Source, on page 585
- Configure Multicast Music On Hold Server, on page 585
- Configure a Multicast-Enabled Media Resource Group, on page 587
- Configure Multicast Music On Hold over H.323 Intercluster Trunks, on page 587

Enable Secured Music On Hold through SRTP

Cisco Unified Communications Manager enhances the Cisco IP Voice Media Streaming application service to support Secure Real-Time Protocol (SRTP). Hence, when you enable the Cisco Unified Communications Manager cluster or system for security, the MOH server registers with Cisco Unified Communications Manager as an SRTP capable device. If the receiving device is also SRTP-capable, the music media is encrypted before streaming to the receiving device.

Note In a secure mode, the Cisco Unified Communications Manager Administration device page for Music On Hold displays a **Device is trusted** message with a green check box, indicating that it is a trusted device.

Before you begin

Enable Security for Music On Hold, on page 580

Procedure

Step 1 In the Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 In **Enterprise Parameters** window, set the **Cluster Security Mode** parameter to **Mixed Mode**.

Note The media streaming between the devices is done through SRTP. When calls are secure, an icon with a secured lock appears on the Cisco Unified IP Phone, indicating that the call is protected for both signaling and media.

This parameter indicates the security mode of the cluster. A value of `0` indicates Non Secure (phones register in nonsecure mode); `1` indicates Mixed (the cluster allows the registration of both secure devices and nonsecure devices). Because this parameter is read-only, to change the cluster security mode, you must run the CTL Client plugin.

Step 3 Click **Save**, and restart Cisco Unified Communications Manager for the parameter change to take effect.

What to do next

Configure multicast by performing the following subtasks:

- Plan Music On Hold Server Capacity, on page 583
- Configure MOH Service Parameters, on page 584
- Configure Multicast Music On Hold Audio Sources/Fixed MOH Audio Source, on page 585
- Configure Multicast Music On Hold Server, on page 585
- Configure a Multicast-Enabled Media Resource Group, on page 587
- Configure Multicast Music On Hold over H.323 Intercluster Trunks, on page 587

Unicast and Multicast Audio Sources

Unicast Music On Hold is the system default option. However, you need to configure for multicast, if required. Both multicast and unicast configurations present the same audio-source behavior to held parties. Each audio source is used once, and the stream is split internally and is sent to the held parties. The only difference between multicast and unicast, in this case, is how the data is sent over the network.

Table 60: Differences Between Unicast and Multicast Audio Sources

Unicast Audio Source	Multicast Audio Source
Consists of streams that are sent directly from the MOH server to the endpoint that requests an MOH audio stream.	Consists of streams that are sent from the MOH server to a multicast group IP address. Endpoints that request an MOH audio stream can join multicast MOH, as needed.
A unicast MOH stream is a point-to-point, one-way audio RTP stream between the server and the endpoint device.	A multicast MOH stream is a point-to-multipoint, one-way audio RTP stream between the MOH server and the multicast group IP address.
Unicast MOH uses a separate source stream for each user or connection. As more endpoint devices go on hold through a user or network event, the number of MOH streams increases.	Enables multiple users to use the same audio source stream to provide MOH.
An MOH audio source may be configured with an initial (greeting) announcement, which will be played to unicast held parties. For unicast MOH users, this announcement is heard from the beginning.	For multicast users, this announcement is not heard.

Unicast Audio Source	Multicast Audio Source
The additional MOH streams can have a negative effect on network throughput and bandwidth.	Multicast MOH conserves system resources and bandwidth.
Extremely useful in networks in which multicast is not enabled or devices are incapable of multicast.	Can be problematic in situations in which a network is not enabled for multicast or the endpoint devices are incapable of processing multicast.
Includes managing devices only.	Includes managing devices, IP addresses, and ports.
No requirement to define the Music On Hold server.	Administrators must define at least one audio source to allow multicasting. To define Music On Hold servers for multicast, first define the server to allow multicasting.
Functions without configuring MOH audio source, MOH server, or media resource group list.	Functions only if both media resource groups and media resource group lists are defined to include a multicast Music On Hold server. For media resource groups, you must include a Music On Hold server that is set up for multicast. These servers are labeled as (MOH) [Multicast]. Also, check the **Use Multicast for MOH Audio** check box when you define a media resource group for multicast.

Note The Multicast MOH Direction Attribute for SIP service parameter determines whether Cisco Unified Communications Manager sets the direction attribute of the Session Description Protocol (SDP) in its multicast Music On Hold (MOH) INVITE message to sendOnly or recvOnly.

If your deployment uses SIP phone uses Release 8.4 and earlier for Cisco Unified IP Phones 7940 and 7960, or SIP phone uses Release 8.1(x) and earlier for Cisco Unified IP Phones 7906, 7911, 7941, 7961, 7970, and 7971, set this parameter to **sendOnly**. Otherwise, leave this parameter set to the default value, **recvOnly**.

Multicast Configuration

Plan Music On Hold Server Capacity

It is crucial to plan the capacity of the deployed and configured hardware and to ensure the support it can provide for the anticipated call volume of the network. You need to know the hardware capacity for MOH resources and consider the implications of multicast and unicast MOH in relation to this capacity. Ensure that network call volumes do not exceed these limits. When MOH sessions reach these limits, an additional load can result in poor MOH quality, erratic MOH operation, or loss of MOH functionality.

Before you begin

- Enable Security for Music On Hold, on page 580
- (Optional) Enable Secured Music On Hold through SRTP, on page 581

Procedure

Step 1 In Cisco Unified CM Administration, choose **Media Resources** > **Music on Hold Server**.

Step 2 In the **Find and List Music On Hold Servers** window, enter the search parameters and click **Find**.
The system displays the records that match all the criteria.

Step 3 Check the check box of the MOH Server for which you want to plan the capacity.
The **Music On Hold (MOH) Server Configuration** window appears.

Step 4 Configure the following fields in the **Music On Hold (MOH) Server Configuration** window:

- **Maximum Half Duplex Streams**—This parameter determines the number of devices that you can place on unicast MOH. By default, this value is set to 250. Set this parameter to the value that is derived from the following formula:

  ```
  (Server and deployment capacity) - ([Number of multicast MOH sources] * [Number of
  enabled MOH codecs])
  ```

  The value of this parameter should be set according to the platform and deployment type (coresident or standalone).

  Note Regarding the maximum suggested number of MOH streams (250 MOH streams on Cisco MCS 7815 and 7825 Series and 500 MOH streams on Cisco MCS 7835 and 7845 Series) – Count each multicast audio source as two MOH streams. For example, for Cisco MCS 7835 and 7845 Series, if three multicast MOH audio sources and four codecs are enabled, no more than 476 unicast MOH streams should be generated at the same time (2 * 3 * 4 + 476 = 500).

- **Maximum Multi-cast Connections**—This parameter determines the number of devices that you can place on multicast MOH. By default, this value is set to 30,000. Set this parameter to a value that ensures that all devices can be placed on multicast MOH, if necessary. Although the MOH server can generate only a finite number of multicast streams (a maximum of 204), many held devices can join each multicast stream. This parameter should be set to a number that is greater than or equal to the number of devices that might be placed on multicast MOH at any given time.

Step 5 Click **Save**.
The changes take place when the streaming to the device is idle.

What to do next

Configure MOH Service Parameters, on page 584

Configure MOH Service Parameters

Use this procedure to configure optional service parameters for Music On Hold (MOH). For many deployments the default settings will be sufficient.

Procedure

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

Step 2 From the **Server** drop-down list, select the server.

Step 3 From the **Service** drop-down list, select **Cisco IP Voice Media Streaming**.

Step 4 From the **Clusterwide Parameters (Parameters that apply to all servers)** area, configure optional MOH service parameters.

Step 5 Click **Save**.

Step 6 From the **Service** drop-down list, select **Cisco CallManager**.

Step 7 Configure optional MOH parameters. For example, under **Clusterwide Parameters (Service)**, you can assign the default audio sources for Hold.

Step 8 Click **Save**.

Note All parameters apply only to the current server except parameters that are in the cluster-wide group.

Configure Multicast Music On Hold Audio Sources/Fixed MOH Audio Source

For multicast to be available, configure the Cisco Unified Communications Manager services to allow multicasting on MOH audio sources or fixed MOH audio source.

Before you begin

Configure MOH Service Parameters, on page 584

Procedure

Step 1 In Cisco Unified CM Administration, choose **Media Resources** > **Music On Hold Audio Source**.

Step 2 Enter search parameters to find a Music On Hold audio source.
The system displays the records that match all the criteria.

Step 3 In the **Music On Hold Audio Source Configuration** window, check the **Allow Multi-casting** checkbox to allow multicasting.

Step 4 Click **Save**.

What to do next

Configure Multicast Music On Hold Server, on page 585

Configure Multicast Music On Hold Server

After you allow multicast Music On Hold (MOH) on audio sources, you must enable the MOH server for multicast Music on Hold.

When you use multicast MOH and when the devices that listen to multicast MOH streams are not in the same IP network, you must enable multicast routing in the IP network. Take care when you enable the multicast routing to avoid the potential flooding of parts of the network with wrongly sent multicast packets (specially, across WAN links). Disable multicasts on interfaces on which the multicast MOH packets are not required and use the **Max Hops** parameter.

Note To use multicast MOH when you use Media Resource Group and Media Resource Group Lists to implement media-resources access control and when you assign a multicast MOH server to a Media Resource Group, you must also enable multicast MOH for the Media Resource Group.

Before you begin

Configure Multicast Music On Hold Audio Sources/Fixed MOH Audio Source, on page 585

Procedure

Step 1 In Cisco Unified CM Administration, choose **Media Resources** > **Music On Hold Server**.

Step 2 Enter search parameters to find a Music On Hold server.
The system displays the records that match all the criteria.

Step 3 In the **Music On Hold (MOH) Server Configuration** window, check the **Enable Multi-cast Audio Sources on this MOH Server** checkbox.
The **Base Multi-cast IP Address**, **Base Multi-cast Port Number**, and **Increment Multi-cast On** fields are populated automatically. You can modify these values as desired.

Step 4 (Optional) Configure the following fields in the **Music On Hold (MOH) Server Configuration** window:

- **Base Multi-cast IP Address**—Enter the multicast IP addresses that range from 224.0.1.0 to 239.255.255.255.

  Note IP addresses between 224.0.1.0 and 238.255.255.255 fall in the reserved range of IP multicast addresses for public multicast applications. Use of such addresses may interfere with existing multicast applications on the Internet. Use IP addresses in the range that is reserved for administratively controlled applications on private networks (239.0.0.0 - 239.255.255.255).

- **Base Multi-cast Port Number**—Enter the multicast port numbers that include even numbers and range from 16384 to 32766.

  Note Increment multicast on IP address instead of on port number. Doing so results in each multicast audio source to have a unique IP address and helps to avoid network saturation in firewall situations.

- **Increment Multi-cast On**—Click `Port Number` to increment multicast on port number or click **IP Address** to increment multicast on IP address.

Note All MOH audio sources that you configure to allow multicasting are listed in the **Selected Multicast Audio Sources** section of the **Music On Hold (MOH) Server Configuration** window.

Step 5 Click **Save**.

What to do next

Configure a Multicast-Enabled Media Resource Group, on page 587

Configure a Multicast-Enabled Media Resource Group

Multicast Music On Hold (MOH) works only if you assign the Multicast-enabled MOH server to a Multicast-enabled Media Resource Group. Configure this Media Resource Group to be a member of a Media Resource Group List. Then, you can associate the Media Resource Group List with devices, such as phones.

Before you begin

- Assign a multicast-enabled MOH server to a multicast-enabled Media Resource Group for the multicast MOH to work.
- Configure Multicast Music On Hold Server, on page 585

Procedure

Step 1 In Cisco Unified CM Administration, choose **Media Resources** > **Media Resource Group**.

Step 2 Enter search parameters to find a Media Resource Group.
The system displays the records that match all the criteria.

Step 3 Configure the following fields in the **Media Resource Group Configuration** window:

- **Name**—Enter a name for the media resource group
- **Available Media Resources**—From this list, select one or multiple media resources.
- **Selected Media Resources**—Using the arrow key, select one or multiple media resources to use for multicasting.

Step 4 Check the **Use Multi-cast for MOH Audio** check box, if at least one multicast resource is available.

Step 5 Click **Save**.
This media resource group is then configured to be a member of a Media Resource Group List (MRGL). The MRGL is associated with devices, such as phones.

What to do next

Configure Multicast Music On Hold over H.323 Intercluster Trunks, on page 587

Configure Multicast Music On Hold over H.323 Intercluster Trunks

Using the multicast MOH over H.323 intercluster trunk feature, you can multicast MOH to work over H.323 intercluster trunks (ICT).

Consider these guidelines for configuring multicast MOH:

- This feature does not work if any middle box between Cisco Unified Communications Managers does not pass the new fields in Terminal Capability Set (TCS) and OLC message.
- This feature requires no additional configuration for field up multicast MOH, and applies only between Cisco Unified Communications Managers that support single-transmitter multicast.
- The feature remains active by default. To turn off the feature, set the value of the **Send Multicast MOH in H.245 OLC Message** service parameter to **False**. Setting this value can resolve interoperability issues that the feature might cause.

Procedure

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

Step 2 In the **Service Parameter Configuration** window, select a server and the CallManager service.

Step 3 In the **Clusterwide Parameters (Service)** section, set the value of **Send Multicast MOH in H.245 OLC Message** service parameter to **True**.

Step 4 Click **Save**.

Reset or Restart a Music On Hold Server

Perform the following procedure to reset or restart an existing Music On Hold server.

Before you begin

Configure multicast by performing the following subtasks:

- Plan Music On Hold Server Capacity, on page 583
- Configure MOH Service Parameters, on page 584
- Configure Multicast Music On Hold Audio Sources/Fixed MOH Audio Source, on page 585
- Configure Multicast Music On Hold Server, on page 585
- Configure a Multicast-Enabled Media Resource Group, on page 587
- Configure Multicast Music On Hold over H.323 Intercluster Trunks, on page 587

Procedure

Step 1 In Cisco Unified CM Administration, choose **Media Resources** > **Music On Hold Server**.

Step 2 Check the check box for the Music On Hold server that you want to reset, and click **Reset**.
A popup window shows an information message.

Step 3 Click **Restart** to restart the Music On Hold server, or click **Reset** to reset the Music On Hold server.

What to do next

(Optional) Synchronize Music On Hold Server, on page 588

Synchronize Music On Hold Server

To synchronize a Music on Hold Server with the most recent configuration changes, perform the following procedure. After you perform this procedure any outstanding configuration is applied in the least-intrusive manner possible. For example, a reset or restart may not be required on few affected devices.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Media Resources** > **Music On Hold Server**.

Step 2 Enter search parameters to find a Music On Hold server, and click **Find**.
The system displays the search results for the records that match all the criteria.

Step 3 Check the check boxes next to the Music On Hold servers that you want to synchronize. To select all MOH servers in the window, check the check box in the matching records title bar.

Step 4 Click **Apply Config to Selected**.

Step 5 Click **OK**.

Music On Hold Interactions and Restrictions

Music On Hold Interactions

Feature	Interaction
Multicast Music On Hold over H.323 Intercluster Trunks	Using the multicast MOH over H.323 intercluster trunk feature, you can multicast MOH to work over H.323 intercluster trunks (ICT). When a call connects over an intercluster trunk and one of the parties presses the Hold key, MOH streams over the intercluster trunk. If you have turned on the multicast MOH and have configured the holding party and trunk to use the multicast MOH server, MOH streams with multicast. Only one multicast MOH stream streams over the trunk regardless of the number of calls that are put on hold on this trunk. Additional points regarding this feature: • This feature does not work if any middle box between Cisco Unified Communications Managers does not pass the new fields in Terminal Capability Set (TCS) and OLC message. • This feature requires no additional configuration for field up multicast MOH, and applies only between Cisco Unified Communications Managers that support single-transmitter multicast. • The feature is On by default, but can be turned off by setting the **Send Multicast MOH in H.245 OLC Message** service parameter to **False**. Setting this value can resolve interoperability issues that the feature might cause.
Music On Hold Failover and Fallback	The MOH server supports Cisco Unified Communications Manager lists and failover as implemented by the software conference bridge and media termination point. Upon failover, the system maintains connections to a backup Cisco Unified Communications Manager, if available. When a Music On Hold server fails during an active Music On Hold session, the held party hears no music from this point. However, this situation does not affect normal call functions.

Feature	Interaction
Call Park and Directed Call Park	Music On Hold allows users to place calls on hold with music that a streaming source provides. Music On Hold allows two types of hold: • User hold—The system invokes this type of hold when a user presses the Hold button or Hold softkey. • Network hold—This type of hold takes place when a user activates the Transfer, Conference, or Call Park feature, and the hold automatically gets invoked. This hold type applies to directed call park because directed call park is a transfer function. However, Directed Call Park uses the Cisco Call Manager service parameter, Default Network Hold MOH Audio Source, for the audio source.
Extension Mobility Cross Cluster—Media resources for the visiting phone	Examples include RSVP Agent, TRP, Music On Hold (MOH), MTP, transcoder, and conference bridge. Media resources are local to the visiting phone (other than RSVP Agents).
Hold Reversion	Cisco Unified Communications Manager supports MOH on a reverted call if MOH is configured for a normal held call.
Media Resource Selection	Held parties determine the media resource group list that a Cisco Unified Communications Manager uses to allocate a Music On Hold resource.
Secured Music On Hold with SRTP	Cisco Unified Communications Manager enhances the Cisco IP Voice Media Streaming application service to support Secure Real-Time Protocol (SRTP). Hence, when you enable the Cisco Unified Communications Manager cluster or system for security, the MOH server registers with Cisco Unified Communications Manager as an SRTP capable device. If the receiving device is also SRTP-capable, the music media is encrypted before streaming to the receiving device. Make sure of the following: • Cluster security should be mixed mode—Run the `utils ctl set-cluster mixed-mode` CLI command • SIP trunks in the path support SRTP—The **SRTP Allowed** check box must be checked in the **Trunk Configuration** window for SRTP to work over the trunk. • Devices support SRTP—In the Phone Security Profile used by the endpoint, the **Device Security Mode** must be **Encrypted**.

Music On Hold Restrictions

Restriction	Description
Multicast Music On Hold Support	Computer Telephony Integration (CTI) and media termination point (MTP) devices do not support the multicast Music On Hold feature. If you configure CTI or MTP devices with a multicast MoH device in the media resource group list of the CTI device, call control issues may result. CTI and MTP devices do not support multicast media streaming.
Internet Protocol Support	Multicast Music On Hold supports only IPv4. The Cisco IP Voice Media Streaming Application, which is a component of Music On Hold, supports both IPv4 and IPv6 audio media connections for unicast Music On Hold. Multicast Music On Hold supports IPv4 only. Devices with an IP addressing mode of IPv6 only cannot support multicast.
Distribution of fixed-device audio sources	Cisco Unified Communications Manager does not support distribution of fixed-device (hardware) audio sources across Music On Hold servers within a media resource group.
Unacceptable Audio Quality with G.729a codec	Because the G.729a codec is designed for human speech, if you use it with Music On Hold for music, it may not provide acceptable audio quality.
Cisco Unified Communications Manager System Support	A Cisco Unified Communications Manager cluster or system supports only virtualized deployments on Cisco Unified Computing System (UCS) servers or other Cisco-approved third-party server configurations. You cannot use the Music On Hold feature with an external source (USB audio dongle) for the nodes that provide MOH from an external source.
Multicast Support	The administrator can designate a Music On Hold server as either unicast or multicast, provided that resources exist to support multicast.
Caller-specific MOH Support	Caller-specific MOH is not supported when calls are received or transferred over QSIG tunneling-enabled SIP trunks.
MP3 Format Support	The Music On Hold feature does not support the MP3 format.
Interoperability between H.323 and SIP Protocols	Multicast MOH does not support interoperability between H.323 and SIP protocols.
SRTP Support	Multicast MoH audio streams are not encrypted and do not support SRTP.
Multicast Streams	MTPs do not support multicast streams.
Encryption of Multicast Music On Hold RTP Streams	Cisco Unified Communications Manager does not support encryption of multicast Music On Hold RTP streams. For secure MOH audio, you should not configure multicast audio sources.
Fixed Music On Hold Device	The fixed Music On Hold device cannot specify an audio source that connects through a USB, because Cisco Unified Communications Manager does not support USB when running on VMware. However, VMware supports internal Music On Hold.

Restriction	Description
MOH Server Failure	Cisco Unified Communications Manager takes no action when a Music On Hold server fails during an active Music On Hold session.
Multicast MOH	When an MTP resource gets invoked in a call leg at a site that is using multicast MOH, Cisco Unified Communications Manager falls back to unicast MOH instead of multicast MOH.
Provisioning	If you do not provision the user and network MOH audio source identifiers, or if one or both values are invalid, the caller-specific MOH information in the SIP header is ignored. The call reverts to tone on hold and an invalid MOH audio source alarm is raised.
Header Values	• When both the user and network MOH audio source identifiers are present in the header, any invalid value is replaced by the default value (0). • If both values are zero, or the only value is zero, the header in the incoming INVITE is ignored.
MOH Audio Source Identifier	• If you provide only one MOH audio source identifier in the SIP header, including if a comma appears before or after the MOH audio source identifier value, the same MOH ID is used for both user and network MOH. The SIP trunk populates both the user and the network MOH audio source identifiers in the SIP header so that Call Control always receive both values. • If there are more than two MOH audio source identifier values separated by a comma in the header, then the first two values are used. Subsequent values are ignored.
Administrators for Consistent Caller-specific MOH Configurations	Administrators are responsible to maintain consistent caller-specific MOH configurations when multiple Cisco Unified Communications Manager clusters are involved.
Original Incoming Caller	The original incoming caller to the call center cannot change during the course of the entire call.
MOH Information	The Music On Hold information is shared only across SIP trunks.

Music On Hold Troubleshooting

Music On Hold Does Not Play on Phone

Phone user cannot hear Music On Hold.

- G.729a codec is used with MOH for music, which may not provide acceptable audio quality.
- An MTP resource is invoked in a call leg at a site that is using multicast MoH.

- Verify the IP addressing mode of the device where Music On Hold is played. If the IP addressing mode for the device is IPv6 Only and if Music On Hold is configured for unicast Music On Hold, ensure that a dual-stack MTP is configured and available for media translation.
- When an MTP resource gets invoked in a call leg at a site that is using multicast MoH, the caller receives silence instead of Music On Hold. To avoid this scenario, configure unicast MoH or Tone on Hold instead of multicast MoH.

CHAPTER 44

Self Care Portal

Self Care Portal Overview

From the Cisco Unified Communications Self Care Portal, users can customize features and settings for their phones. As the administrator, you control access to the portal. Before an end user can access the portal, you must add the user to the default **Standard CCM End Users** access control group, or to any access control group that has the **Standard CCM End Users** role assignment. In addition, users require their user ID, password, and the URL with which to access the portal. Users can access the portal via the following URL:

```
http(s)://<server_name>:<port_number>/ucmuser/
```

where:

- **`<server_name>`** represents the Unified Communications Manager IP address, hostname or fully qualified domain name
- **`<port_number>`** represents the port on which to connect. The port is optional, but is useful in firewall situations.
- **`ucmuser`** is a mandatory subpath that points to Self Care

Optionally, you can also configure enterprise parameters within Cisco Unified Communications Manager in order to assign which phone settings are available for end users to configure. For example, the **Show Call Forwarding** enterprise parameter determines whether users can configure Call Forward via the portal.

Self Care Portal Task Flow

Procedure

	Command or Action	Purpose
Step 1	Grant User Access to the Self Care Portal, on page 596	To access the portal, end users must be assigned to the **Standard CCM End Users** access control group or to any group that has the **Standard CCM End Users** role assignment.

	Command or Action	Purpose
Step 2	Configure the Self Care Portal Options, on page 596	Configure enterprise parameters in order to control what configuration options are available to users whom access the portal.

Grant User Access to the Self Care Portal

To access the portal, end users must be assigned to the **Standard CCM End Users** access control group or to any group that has the **Standard CCM End Users** role assignment.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **End User**.

Step 2 Search for the user for whom you want to provide Self-Care access.

Step 3 In the **End User** section, ensure that the user has a password and PIN configured.

Usually these credentials are entered when a new user is added.

Step 4 In the **Permission Information** section, click **Add to Access Control Group**.

Step 5 Click **Find** and select the **Standard CCM End Users** group or a customized group that contains the **Standard CCM End Users** role.

Note For information on editing and configuring access control groups, and role assignments for access control groups, refer to the "Configure User Access" chapter of the System Configuration Guide for Cisco Unified Communications Manager.

Step 6 Select **Save**.

Configure the Self Care Portal Options

Use this procedure to configure Self Care Portal enterprise parameters in order to control what configuration options are available to users whom access the portal.

Before you begin

Grant User Access to the Self Care Portal, on page 596

Procedure

Step 1 From Cisco Unified Communications Manager Administration, select **System** > **Enterprise Parameters**.

Step 2 Under **Self Care Portal Parameters**, set the **Self Care Portal Default Server** by selecting one of the available servers from the drop-down list.

This parameter determines which Cisco Unified CM server Jabber uses to display embedded Self Care options pages. If you select **None**, Jabber defaults to the Publisher.

Step 3 Configure any of the remaining Self Care Portal Parameters to enable or disable features for the portal. For help with the fields, refer to the enterprise parameters help.

Step 4 Select **Save**.